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。

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ルータは、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、ルータ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。ルータは、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、ルータは再度 CA または Lightweight Directory Access Protocol（LDAP）サーバあるいは HTTP サーバに連絡して、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）。

（注） Cisco IOS リリースに応じて、LDAP がサポートされます。

設定によっては、有効またはルーティング可能な 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 接続を実行できる場合があります。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。この要件の具体例としてケーブル モデムがあります。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アドレスがないためです。ただし、ユーザインターフェイス（通常は FastEthernet）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 pki 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 pki 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **source interface** *interface-address*
6. **interface** *type slot / port*

7. **description** *string*
8. **ip address** *ip-address mask*
9. **interface** *type slot / port*
10. **description** *string*
11. **ip address** *ip-address mask*
12. **crypto map** *map-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 pki trustpoint** *name* 例： `Router (config)# crypto pki trustpoint ms-ca`	ルータが使用する認証局（CA）を宣言し、CA トラストポイント 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 url** *url* 例： `Router (ca-trustpoint)# enrollment url http://yourname:80/certsrv/mscep/mscep.dll`	CA の登録パラメータを指定します。
ステップ 5	**source interface** *interface-address* 例： `Router (ca-trustpoint)# interface fastethernet1/0`	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	**interface** *type slot / port* 例： `Router (ca-trustpoint)# interface fastethernet1/0`	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 7	**description** *string* 例： `Router (config-if)# description inside interface`	インターフェイスの設定に説明を加えます。

	コマンドまたはアクション	目的
ステップ 8	**ip address** *ip-address mask* 例： `Router (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 9	**interface** *type slot / port* 例： `Router (config-if)# interface fastethernet1/0`	インターフェイス タイプを設定します。
ステップ 10	**description** *string* 例： `Router (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 11	**ip address** *ip-address mask* 例： `Router (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 12	**crypto map** *map-name* 例： `Router (config-if)# crypto map mymap`	インターフェイスに対して以前に定義されたクリプト マップ セットを適用します。

トラブルシューティングのヒント

コマンドで指定されたインターフェイスのアドレスが有効であることを確認します。指定されたインターフェイスのアドレスを使用して別のデバイス（可能性としては CRL を処理している HTTP または LDAP サーバ）からルータに ping を実行します。外部デバイスからルータへのトレースルートを使用しても同じことができます。

Cisco IOS XE コマンドライン インターフェイス（CLI）を使用して、ルータと CA または LDAP サーバ間の接続をテストすることもできます。**ping ip** コマンドを入力し、プロンプトに回答します。「Extended commands [n]:」プロンプトに「はい」と回答すると、送信元アドレスまたはインターフェイスが指定できるようになります。

また、Cisco IOS XE CLI を使用して traceroute コマンドを入力できます。**traceroute ip** コマンド（EXEC モード）を入力すると、宛先および送信元アドレスを求めるプロンプトが表示されます。CA または LDAP サーバを、宛先および送信元アドレスの「送信元インターフェイス」として指定されたインターフェイスのアドレスとして指定する必要があります。

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

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例

次に、ルータが支社にある例を示します。ルータは IP セキュリティ（IPSec）を使用して本社と通信します。FastEthernet 1 は、ISP（インターネット サービス プロバイダー）に接続する「外部」インターフェイスです。FastEthernet 0 は、支社の LAN に接続されたインターフェイスです。本社にある CA サーバにアクセスするには、ルータは IPSec トンネルを使用してその IP データグラムを外部インターフェイスである FastEthernet 1（アドレス 10.2.2.205）に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 から発信されたメッセージを確認しますが、応答はできません（つまり、CA は、ルータが支社の到達可能なアドレス 10.1.1.1 にあることを認識していません）。

source interface コマンドを追加すると、ルータはアドレス 10.1.1.1 を CA に送信される IP データグラムの送信元アドレスとして使用するよう指示されます。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。

```
crypto pki trustpoint ms-ca
 enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
 source interface fastethernet0
!
interface fastethernet 0
 description inside interface
 ip address 10.1.1.1 255.255.255.0
!
interface fastethernet 1
 description outside interface
 ip address 10.2.2.205 255.255.255.0
 crypto map main-office
```

その他の参考資料

次に、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の機能に関する資料を示します。

関連資料

関連項目	マニュアル タイトル
IPsec と認証局の設定	「Security for VPNs with IPsec」

関連項目	マニュアル タイトル
IPsec と認証局に関するコマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	-

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。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索し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
この機能でサポートが追加または変更された RFC 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/techsupport

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情報

表 *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の機能情報

機能名	リリース	機能情報
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	Cisco IOS XE Release 2.1	この機能により、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。 次のコマンドが導入されました。**source interface**

用語集

認証：IDの証明書およびIDがもたらす秘密を使用してエンティティのIDを証明すること（通常は、秘密キーは証明書の公開キーに対応します）。

CA：認証局。CAはデジタル証明書を発行するエンティティ（特にX.509証明書）で、証明書のデータ項目間のバインディングを保証します。

CA authentication：ユーザーはルート CA からの証明書を手動で承認します。通常は、証明書のフィンガープリントがユーザに提示され、ユーザはフィンガープリントに基づく証明書を承認するよう求められます。ルート CA の証明書は、通常の証明書確認プロセスで自動的に認証できないよう、自ら署名（自己署名）されます。

CRL：証明書失効リスト。CRL は、発行者により無効にされたデジタル証明書をそれらの期限満了予定までに列挙するデータ構造です。

enrollment：ルータは登録プロセス経由でその証明書を受信します。ルータは、（PKCS#10 と呼ばれる）特定の形式で証明書の要求を生成します。その要求は CA に転送され、CA は要求を許可し、要求と同じ形式に符号化された証明書を生成します。ルータは許可された証明書を受信し、通常操作中に使用するため、内部データベースに保管します。

certificate：エンティティ（マシンまたはユーザー）をそのエンティティの公開キーと関連付けるため国際標準化機構（ISO）規格 X.509 で定義されたデータ構造。証明書には、エンティティの名前など特定のフィールドが含まれています。証明書は通常は、エンティティに代わって CA により発行されます。この場合は、ルータが CA としての役割を果たします。証明書内の共通フィールドには、エンティティの認定者名（DN）、証明書を発行している認証局の DN、およびエンティティの公開キーがあります。

LDAP：Lightweight Directory Access Protocol。LDAP は、X.500 ディレクトリに読み書きインタラクティブ アクセスできる、管理アプリケーションおよびブラウザ アプリケーションにアクセスできるプロトコルです。

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。