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

Certificate Authority（CA; 認証局）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仕様

機能の履歴	
リリース	**変更点**
12.2(15)T	この機能が追加されました。
サポートされているプラットフォーム	
Cisco 1600、Cisco 1600R、Cisco 1710、Cisco 1720、Cisco 1750、Cisco 1751、Cisco 1760、Cisco 2400、Cisco 2610–2613、Cisco 2610XM–2611XM、Cisco 2620–2621、Cisco 2620XM–2621XM、Cisco 2650–2651、Cisco 2650XM–2651XM、Cisco 2691、Cisco 3620、Cisco 3631、Cisco 3640、Cisco 3660、Cisco 3725、Cisco 3745、Cisco 7100、Cisco 7200、Cisco 7400、Cisco 7500、Cisco 801–Cisco 806、Cisco 811、Cisco 813、Cisco 828、Cisco 8850-RPM、Cisco AS5300、Cisco AS5350、Cisco AS5400、Cisco AS5800、Cisco MC3810、Cisco ubr7200、Cisco ubr905、Cisco ubr925	

プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明の場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

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

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を設定するには、次の概念を理解しておく必要があります。

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 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、Certificate Revocation List（CRL; 証明書失効リスト）のチェックとも呼ばれています）。

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

ここでは、次の手順について説明します。

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 ca 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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
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 ca trustpoint** *name* **例：** `Router (config)# crypto ca 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。

	コマンドまたはアクション	目的
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 ethernet 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 ethernet 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 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。
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 ethernet1/0`	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 Command-Line Interface（CLI; コマンドライン インターフェイス）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 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

ここでは、次の例について説明します。

- 「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例」（P.5）

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例

次に、ルータが支社にある例を示します。ルータは IP Security（IPSec; IP セキュリティ）を使用して本社と通信します。イーサネット 1 は、Internet Service Provider（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。イーサネット 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イーサネット 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 ca trustpoint ms-ca
 enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
 source interface ethernet0
!
interface ethernet 0
 description inside interface
 ip address 10.1.1.1 255.255.255.0
!
interface ethernet 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

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関するその他の情報については、次の関連資料を参照してください。

関連資料

内容	参照先
IPsec と認証局の設定	「*Security for VPNs with IPsec*」
IPsec と認証局に関するコマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格や変更された規格はありません。	–

MIB

MIB	MIB 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。	プラットフォームおよび Cisco IOS ソフトウェア リリースによりサポートされている MIB のリストを入手し、MIB モジュールをダウンロードするには、Cisco.com の次のシスコ MIB Web サイトの URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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://tools.cisco.com/ITDIT/MIBS/servlet/index

Cisco MIB Locator で必要な MIB 情報がサポートされていない場合、サポート対象 MIB のリストを取得し、次の URL にある Cisco MIB ページから MIB をダウンロードすることもできます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cisco MIB Locator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E メールで届きます。資格のあるユーザは、Cisco.com のアカウントを作成できます。次の URL にある指示に従ってください。

http://www.cisco.com/register

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **source interface**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『*Master Command List*』を参照してください。

用語集

CA : Certificate Authority（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 認証：ユーザはルート 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：Certificate Revocation List（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。

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。

証明書：エンティティ（マシンまたはユーザ）をそのエンティティの公開鍵と関連付けるため International Organization for Standardization（ISO; 国際標準化機構）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 Distinguished Name（DN; 認定者名）、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鍵があります。

登録：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。

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、公開鍵は証明書の公開鍵に対応します）。

（注） この用語集に記載されていない用語については、『*Internetworking Terms and Acronyms*』を参照してください。