LISP とゾーンベース ファイアウォールの統合と相互運用性

LISP およびゾーンベース ファイアウォールの統合および相互運用性の機能により、デバイスをパス スルーするすべての Locator/ID Separation Protocol（LISP）データ パケットの内部パケット インスペクションが可能になります。LISP 内部パケットインスペクションを有効にするには、**lisp inner-packet inspection** コマンドを設定する必要があります。LISP 内部パケット インスペクションが行われないと、LISP ネットワーク内のエンドポイント ID（EID）デバイスはファイアウォールで保護されません。

このモジュールでは、この機能を設定する方法を説明します。

- LISP とゾーンベース ファイアウォールの統合と相互運用性に関する機能情報 （1 ページ）
- LISP およびゾーンベース ファイアウォールの統合と相互運用性の前提条件 （2 ページ）
- LISP およびゾーンベース ファイアウォールの統合と相互運用性に関する制約事項 （3 ページ）
- LISP とゾーンベース ファイアウォールの統合と相互運用性に関する情報 （3 ページ）
- LISP とゾーンベース ファイアウォールの統合と相互運用性の設定方法 （6 ページ）
- LISP とゾーンベース ファイアウォールの統合と相互運用性の設定例 （13 ページ）
- LISP とゾーンベース ファイアウォールの統合と相互運用性に関する追加情報 （14 ページ）

LISP とゾーンベース ファイアウォールの統合と相互運用性に関する機能情報

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 : LISP* とゾーンベース ファイアウォールの統合と相互運用性に関する機能情報

機能名	リリース	機能情報
LISP とゾーンベース ファイアウォールの統合と相互運用性	Cisco IOS XE リリース 3.13S	LISP およびゾーンベース ファイアウォールの統合および相互運用性の機能により、デバイスをパス スルーするすべての Locator/ID Separation Protocol（LISP）データ パケットの内部パケット インスペクションが可能になります。LISP 内部パケット インスペクションを有効にするには、lisp inner-packet inspection コマンドを設定する必要があります。LISP 内部インスペクションを使用しない場合は、LISP ネットワーク内のエンドポイント識別子（EID）デバイスにファイアウォール保護が設定されません。 この機能により、次のコマンドが導入または変更されました。**lisp inner-packet-inspection**、**show parameter-map type inspect-global**、および **show parameter-map type inspect global**。
ゾーンベース ファイアウォールおよび LISP 統合のシャーシ内およびシャーシ間ハイ アベイラビリティ	Cisco IOS XE リリース 3.14S	Cisco IOS XE リリース 3.14S では、LISP およびゾーンベース ファイアウォール統合および相互運用性機能により、シャーシ内ハイ アベイラビリティとシャーシ間ハイ アベイラビリティの両方がサポートされています。 この機能によって導入または変更されたコマンドはありません。

LISP およびゾーンベース ファイアウォールの統合と相互運用性の前提条件

- アクティブ デバイスとスタンバイ デバイスのシャーシ間高可用性設定は同一でなければなりません。

LISP およびゾーンベース ファイアウォールの統合と相互運用性に関する制約事項

次の機能はサポートされていません。

- Locator ID Separator Protocol（LISP）モビリティ
- ゾーンベース ファイアウォール、LISP 、および Web Cache Control Protocol（WCCP）の相互運用性
- VRF 相互運用性を備えたゾーンベース ファイアウォールと LISP サブインターフェイス

LISP 内部パケットインスペクションが有効な場合、次の機能はサポートされません。

- 非対称ルーティング
- LISP 制御メッセージ インスペクション
- LISP 内部パケット フラグメンテーション
- ネットワーク アドレス変換（NAT）および NAT 64
- TCP リセット
- VPN ルーティングおよび転送（VRF）
- 仮想 TCP（vTCP）
- VRF 対応ソフトウェア インフラストラクチャ（VASI）
- Web Cache Communication Protocol（WCCP）

LISP とゾーンベース ファイアウォールの統合と相互運用性に関する情報

LISP の概要

Locator/ID Separation Protocol（LISP）は、ネットワーク アーキテクチャ兼プロトコルです。LISP は、単一の IP アドレスを 2 つのナンバリング スペースで置き換えます。ナンバリング スペースの一方は、ネットワーク接続ポイントにトポロジ的に割り当てられ、そのネットワーク経由のパケットのルーティングおよび転送に使用されるルーティング ロケータ（RLOC）です。もう一方は、ネットワーク トポロジとは関係なく割り当てられ、ナンバリング デバイスに使用されて管理境界で集約されるエンドポイント ID です。

LISP が定義しているのは、これら 2 つのナンバリング スペースをマッピングし、ルーティング不可能な EID を使用してデバイスから発信されたトラフィックを、ルーティングと転送に RLOC を使用するネットワーク インフラストラクチャで転送できるようにカプセル化するための機能です。LISP では、デバイスがルーティング不可能な EID をルーティング可能な RLOC にマップする際に使用する情報を交換するための一連の機能を提供しています。

LISP を使用するには、LISP 関連の 1 つ以上のデバイス（LISP 出力トンネル ルータ（ETR）、入力トンネル ルータ（ITR）、プロキシ ETR（PETR）、Proxy Ingress Tunnel Router（PITR）、マップ リゾルバ（MR）、マップ サーバ（MS）、LISP 代替論理トポロジ（ALT）デバイスなど）からなる LISP 固有の構成が必要です。

ゾーンベース ファイアウォールと LISP の相互運用性の概要

ゾーンベース ファイアウォールは、ネットワーク内でのエッジ ルータ（Cisco ASR 1000 アグリゲーション サービス ルータなどのルータ）の配置場所に応じて、Locator/ID Separation Protocol（LISP）xTR デバイスのサウスバウンドまたはノースバウンドに導入できます。入力トンネル ルータ（ITR）と出力トンネル ルータ（ETR）は xTR デバイスと総称されています。

ゾーンベース ファイアウォールが xTR デバイスのノースバウンドに位置する場合、ファイアウォールはネットワークをパス スルーする LISP カプセル化パケット（LISP トンネル化パケットなど）を確認できます。

ゾーンベース ファイアウォールが xTR デバイスのサウスバウンドに位置する場合、ファイアウォールはオリジナル パケットを確認できます。ただし、ゾーンベース ファイアウォールが LISP xTR 処理を認識したり、LISP ヘッダーを確認することはできません。出力パケットについては、xTR デバイスはファイアウォール インスペクションの後に LISP カプセル化を行い、LISP ヘッダーをオリジナル パケットの先頭に追加します。入力パケットについては、xTR デバイスはファイアウォール インスペクションの前に LISP カプセル化解除（LISP ヘッダーの削除）を行うため、ファイアウォール インスペクションではオリジナル パケットだけを検査します。したがって、LISP との対話はありません。

この項では、LISP xTR デバイスのサウスバウンドでゾーンベース ファイアウォールを導入する場合のシナリオを説明します:

LISP カプセル化およびカプセル化解除機能を実行する LISP xTR としてエッジ ルータを設定する場合、ゾーンベース ファイアウォールは、LISP インターフェイスと同じエッジ ルータ上の LISP ローカル エンドポイント ID（EID）デバイスに対応するインターフェイスとの間に設定できます。LISP ヘッダーのカプセル化解除は、LISP インターフェイスに位置するゾーンベース ファイアウォールにヘッダーが入力される前に実行されます。LISP ヘッダーのカプセル化は、LISP インターフェイスに位置するゾーンベース ファイアウォールからパケットが出力された後に実行されます。ファイアウォールは EID スペースのネイティブ トラフィックだけを検査します。

この項では、LISP xTR デバイスのノースバウンドでゾーンベース ファイアウォールを導入する場合のシナリオを説明します。

xTR デバイスのノースバウンドでロード シェアリング ルータとして複数のエッジ ルータを導入する場合、エッジ ルータ上のファイアウォールは xTR デバイスのノースバウンドと見なされます。この場合、ゾーンベース ファイアウォールをパス スルーするすべてのパケットが、

LISP カプセル化パケットになります。パケットが到着すると、ファイアウォールは LISP パケットの内部ヘッダーまたは外部ヘッダーのいずれかを検査します。デフォルトでは、外部ヘッダーだけが検査されます。内部ヘッダーのインスペクションを有効にするには、**lisp inner-packet-inspection** コマンドを使用します。

Cisco IOS XE リリースでは、LISP 内部パケット インスペクションが有効にされていると、ファイアウォールはフラグメント化された最初の内部パケットだけを検査し、後続の内部パケットはインスペクションされずにファイアウォールをパス スルーします。LISP 内部パケット インスペクションが有効になっている場合、LISP インスタンス ID が Virtual Routing and Forwarding（VRF）ID として扱われ、異なるインスタンス ID に属する LISP パケットは別のゾーンベース ファイアウォール セッションに関連付けられます。

LISP 機能の相互運用性

Cisco IOS XE リリース 3.13S では LISP およびゾーンベース ファイアウォール統合および相互運用性機能が次の機能と連携します。

- IPv4 内部ヘッダーおよび外部ヘッダー
- IPv6 内部ヘッダーおよび外部ヘッダー
- LISP マルチテナンシー
- アプリケーション レイヤ ゲートウェイ（ALG）
- アプリケーション インスペクションおよびコントロール（AIC）
- マルチプロトコル ラベル スイッチング（MPLS）
- インサービス ソフトウェア アップグレード（ISSU）
- PxTR ケース

ゾーンベース ファイアウォールおよび LISP 統合のシャーシ内およびシャーシ間ハイ アベイラビリティ

Cisco IOS XE リリース 3.14S では、LISP およびゾーンベース ファイアウォール統合および相互運用性機能により、シャーシ内ハイ アベイラビリティとシャーシ間ハイ アベイラビリティの両方がサポートされています。Location/ID Separation Protocol（LISP）内部パケット インスペクションが有効な場合、xTR ノースバウンド デバイスでシャーシ内およびシャーシ間冗長性がサポートされています。

ノースバウンド デバイスでの LISP 内部パケット インスペクションでは、LISP インスタンス ID が Virtual Routing and Forwarding（VRF）インスタンスとして使用されます。LISP 内部パケット インスペクションが有効な場合、ノースバウンド デバイスの VRF 設定は無視されます。

2 つのデバイスが xTR デバイスのノースバウンドに配置されており、xTR デバイスがクラウド内部に配置されている場合、この両方のデバイスで LISP 内部パケット インスペクションが有

効であると、LISP 内部パケット フローに対して作成されたゾーンベース ファイアウォール セッションがスタンバイ デバイスと同期されます。

一般的なシャーシ間（ボックスツーボックス）ハイ アベイラビリティ トポロジでは、xTR デバイスのノースバウンドのルーティング ロケータ（RLOC）スペースに 2 つのデバイスがあります。xTR デバイスは、内部ネットワークに配置されます。LISP 内部パケット インスペクションがこの両方のデバイスで有効であると、LISP 内部パケットに対して作成されたゾーンベース ファイアウォール セッションがスタンバイ デバイスと同期されます。

シャーシ内冗長性については設定の変更はありません。

LISP とゾーンベース ファイアウォールの統合と相互運用性の設定方法

LISP 内部パケット インスペクションの有効化

parameter-map type inspect global コマンドまたは **parameter-map type inspect-global** コマンドを設定した後で、LISP 内部パケットインスペクションを設定できます。

（注） これらのコマンドの両方を同時には設定できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **lisp inner-packet-inspection**
5. **end**
6. **show parameter-map type** {**inspect global** | **inspect-global**}

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： `Device`	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	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	接続しきい値、タイムアウト、およびその他の検査アクションに関連するパラメータのグローバル検査タイプパラメータ マップを設定し、パラメータ マップ タイプ検査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	**lisp inner-packet-inspection** 例： `Device(config-profile)# lisp inner-packet-inspection`	LISP 内部パケット インスペクションをイネーブルにします。
ステップ 5	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show parameter-map type** {**inspect global** | **inspect-global**} 例： `Device# show parameter-map type inspect-global`	グローバル検査タイプ パラメータ マップ情報を表示します。

例

次に示す **show parameter-map type inspect-global** コマンドの出力例は、LISP 内部パケットインスペクションが有効であることを表示します。

```
Device# show parameter-map type inspect-global

parameter-map type inspect-global
  log dropped-packet off
  alert on
  aggressive aging disabled
  syn_flood_limit  unlimited
  tcp window scaling enforcement loose off
  max incomplete unlimited  aggressive aging disabled
  max_incomplete TCP unlimited
  max_incomplete UDP unlimited
  max_incomplete ICMP unlimited
  application-inspect all
  vrf default inspect vrf-default
  vrf vrf2 inspect vrf-default
  vrf vrf3 inspect vrf-default
  lisp inner-packet-inspection
```

LISP 内部パケット インスペクションのシャーシ間ハイ アベイラビリティの設定

シャーシ間ハイ アベイラビリティのための xTR サウスバウンド インターフェイスの設定

始める前に

前提条件

- ゾーンとゾーン ペアを設定する必要があります。
- 冗長性と冗長グループを設定する必要があります。詳細については、『*Zone-Based Policy Firewall Configuration Guide*』の「Configuring Firewall Stateful Interchassis Redundancy」モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **description** *string*
6. **ip address** *ip-address mask*
7. **exit**
8. **interface** *type number*
9. **description** *string*
10. **zone-member security** *zone-name*
11. **exit**
12. **interface** *type number*
13. **description** *string*
14. **ip address** *ip-address mask*
15. **zone-member security** *zone-name*
16. **cdp enable**
17. **end**

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： `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）。

	コマンドまたはアクション	目的
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。
ステップ 3	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet 1/3/0`	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 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding lower`	VRF インスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。
ステップ 5	**description** *string* 例： `Device(config-if)# description facing RLOC and the LISP cloud; has a LISP header.`	インターフェイスの設定に説明を加えます。 • ゾーンベース ファイアウォールは、このインターフェイスには設定できません。
ステップ 6	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.0.1.27 255.255.255.0`	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 7	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface LISP 0`	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。 • これは LISP 仮想インターフェイスです。

ステップ 9	**description** *string*
	例：
	`Device(config-if)# description LISP virtual interface.`
	`Adds LISP header after firewall inspection or removes LISP header before firewall inspection.`
		インターフェイスの設定に説明を加えます。

ステップ 10	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security ge0-0-3a`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 11	**exit** 例：	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# exit`	
ステップ 12	**interface** *type number* 例： `Device(config)# interface tengigabitethernet 0/3/0`	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 13	**description** *string* 例： `Device(config-if)# description facing internal network, does not have a LISP header.`	インターフェイスの設定に説明を加えます。
ステップ 14	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.0.2.5 255.255.255.0`	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 15	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security ge0-0-0`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 16	**cdp enable** 例： `Device(config-if)# cdp enable`	インターフェイスで Cisco Discovery Protocol（CDP）を有効にします。
ステップ 17	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

LISP 内部パケット インスペクションのための xTR ノースバウンド インターフェイスの設定

この設定では、ノースバウンドで LISP ヘッダーが検査されないので、Locator ID Separation Protocol（LISP）仮想インターフェイスは必要ありません。ただし、ゾーンベースのファイアウォールを設定して、LISP 内部パケットまたは外部パケットのどちらかを検査できます。

始める前に

- ゾーンとゾーン ペアを設定する必要があります。
- 冗長性と冗長グループを設定する必要があります。詳細については、『*Zone-Based Policy Firewall Configuration Guide*』の「Configuring Firewall Stateful Interchassis Redundancy」モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **ip address** *ip-address mask*
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **redundancy rii** *id*
9. **redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value*
10. **exit**
11. **interface** *type number*
12. **description** *string*
13. **ip address** *ip-address mask*
14. **zone-member security** *zone-name*
15. **negotiation auto**
16. **redundancy rii** *id*
17. **redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value*
18. **ip virtual-reassembly**
19. **end**

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： `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。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/2/1`	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。 • このインターフェイスは LISP パケット全体を認識できます。
ステップ 4	**description** *string* 例： `Device(config-if)# description RLOC-space/north LAN`	インターフェイスの設定に説明を加えます。
ステップ 5	**ip address** *ip-address mask* 例：	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。

	コマンドまたはアクション	目的
	`Device(config-if)# ip address 198.51.100.8 255.255.255.0`	
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security ge0-0-3`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 7	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 8	**redundancy rii** *id* 例： `Device(config-subif)# redundancy rii 200`	冗長グループが保護するトラフィック インターフェイス用に冗長インターフェイス識別子（RII）を設定します。
ステップ 9	**redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value* 例： `Device(config-if)# redundancy group 1 ip 198.51.100.12 exclusive decrement 50`	冗長グループ（RG）トラフィック インターフェイス設定をイネーブルにします。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 11	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/3`	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。 • このインターフェイスは LISP パケット全体を認識できます。
ステップ 12	**description** *string* 例： `Device(config-if)# description RLOC-space/south LAN`	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 198.51.100.27 255.255.255.0`	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	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security ge0-0-0`	インターフェイスをセキュリティ ゾーンにアタッチします。

	コマンドまたはアクション	目的
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 16	**redundancy rii** *id* 例： `Device(config-subif)# redundancy rii 300`	冗長グループが保護するトラフィック インターフェイス用に冗長インターフェイス識別子（RII）を設定します。
ステップ 17	**redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value* 例： `Device(config-if)# redundancy group 1 ip 194.88.4.1 exclusive decrement 50`	RG トラフィック インターフェイス設定を有効にします。
ステップ 18	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイス上の仮想フラグメント再構成（VFR）を有効にします。
ステップ 19	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

LISP とゾーンベース ファイアウォールの統合と相互運用性の設定例

例：LISP 内部パケット インスペクションの有効化

```
Device# configure terminal
Device(config)# parameter-map type inspect-global
Device(config-profile)# lisp inner-packet-inspection
Device(config-profile)# end
```

次に、LISP 内部パケット インスペクションを有効にしたゾーンベース ファイアウォール設定の例を示します。

```
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

class-map type inspect match-any c-ftp-tcp
```

```
 match protocol ftp
 match protocol telnet
 match protocol http
 match protocol tcp
 match protocol udp
!
policy-map type inspect p1
 class type inspect c-ftp-tcp
  inspect
 class class-default
!
zone security ge0-0-0
!
zone security ge0-0-3
!
zone-pair security zp-ge000-ge003 source ge0-0-0 destination ge0-0-3
 service-policy type inspect p1
!
zone-pair security zp-ge003-ge000 source ge0-0-3 destination ge0-0-0
 service-policy type inspect p1
!
interface TenGigabitEthernet 1/3/0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address 2001:DB8:100::2/64
 zone-member security ge0-0-0
!
interface TenGigabitEthernet 0/3/0
 ip address 192.168.2.1 255.255.255.0
 ipv6 address 2001:DB8:200::2/64
 zone-member security ge0-0-3
!
parameter-map type inspect global
 lisp inner-packet-inspection
 log dropped-packet off
  alert on
!
```

LISP 内部パケット インスペクションのシャーシ間ハイ アベイラビリティの設定

LISP とゾーンベース ファイアウォールの統合と相互運用性に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco コマンド	『Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
LISP コマンド	『Cisco IOS IP Routing: LISP Command Reference』
LISP 設定ガイド	『*IP Routing: LISP Configuration Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6830	『*The Locator/ID Separation Protocol (LISP)*』

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/support

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。