ネットワーク管理用 IPv6 の実装

このマニュアルでは、IPv6 でのシスコ アプリケーションの管理およびネットワーク管理用 IPv6 の実装の概念とコマンドについて説明します。IPv6 に管理機能を提供するために、**copy**、**ping**、**telnet**、および **traceroute** コマンドが変更されました。Secure Shell（SSH; セキュア シェル）の拡張により、IPv6 アドレスがサポートされるため、Cisco ルータは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。

Cisco IOS IPv6 組み込み管理コンポーネントは、IPv6 ネットワークおよび IPv6 と IPv4 のハイブリッド ネットワークにおいて IPv6 に対応した操作性を実現します。Cisco IOS 組み込み管理コンポーネントとして、system message logging（syslog; システム メッセージ ロギング）、Cisco Networking Services（CNS）エージェント、設定ロガー、Hypertext Transfer Protocol server（HTTP(S); ハイパーテキスト転送プロトコル サーバ）、Tool Command Language（TCL; ツール コマンド言語）、Network Configuration Protocol（NETCONF）、Service-Oriented Access Protocol（SOAP）、および IP Service Level Agreements（SLA; サービス レベル契約）があります。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「ネットワーク管理用 IPv6 の実装の機能情報」（P.20）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

ネットワーク管理用 IPv6 の実装の前提条件

- デフォルトでは、IPv6 ルーティングは Cisco IOS ソフトウェアでディセーブルになっています。IPv6 ルーティングをイネーブルにするには、まずルータで IPv6 トラフィックの転送をイネーブルにし、IPv6 アドレスをルータの個々のインターフェイスに割り当てる必要があります。少なくとも 1 つのインターフェイスに IPv6 を設定する必要があります。
- ルータへの Telnet アクセスをイネーブルにするには、vty インターフェイスとパスワードを作成する必要があります。
- このマニュアルでは、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンドリファレンス情報については、「その他の関連資料」に記載されている資料を参照してください。

ネットワーク管理用 IPv6 の実装に関する情報

ネットワーク管理用 IPv6 を実装するには、次の概念を理解する必要があります。

IPv6 を介した Telnet アクセス

Cisco IOS ソフトウェアの Telnet クライアントとサーバでは、IPv6 接続がサポートされています。IPv6 Telnet クライアントを使用してルータへの Telnet セッションを直接確立するか、またはルータから IPv6 Telnet 接続を開始できます。IPv6 ルータへの Telnet アクセスをイネーブルにするには、vty インターフェイスとパスワードを作成する必要があります。

IPv6 での TFTP ファイルのダウンロード

IPv6 では、**copy** コマンドを使用した TFTP ファイルのダウンロードとアップロードがサポートされています。次に示すように、**copy** コマンドは、引数として宛先の IPv6 アドレスまたは IPv6 ホスト名を受け入れ、ルータの実行コンフィギュレーションを IPv6 TFTP サーバに保存します。

```
Router# copy running-config tftp://[3ffe:xxxx:c18:1:290:27ff:fe3a:9e9a]/running-config
```

（注） Cisco IOS Release 12.2(8)T 以降のリリースでは、ポート番号とともに指定されたリテラル IPv6 アドレスを TFTP の送信元または宛先 URL で使用する場合、角カッコ（[ ]）で囲む必要があります。ポート番号のないリテラル IPv6 アドレスは、角カッコで囲む必要はありません。URL でリテラル IPv6 アドレスに角カッコを使用する方法の詳細については、RFC 2732 の『*Format for Literal IPv6 Addresses in URLs*』を参照してください。

IPv6 における ping および traceroute コマンド

ping コマンドは、引数として宛先の IPv6 アドレスまたは IPv6 ホスト名を受け入れ、Internet Control Message Protocol version 6（ICMPv6; インターネット制御メッセージ プロトコル バージョン 6）エコー要求メッセージを指定された宛先に送信します。ICMPv6 エコー応答メッセージは、コンソールに表示されます。拡張 ping 機能も IPv6 でサポートされています。

traceroute コマンドは、引数として宛先の IPv6 アドレスまたは IPv6 ホスト名を受け入れ、IPv6 トラフィックを生成して、宛先アドレスに到達するために使用された各 IPv6 ホップを報告します。

IPv6 トランスポートを介した SSH

IPv6 における SSH は、IPv4 における SSH と同じように機能し、同じ利点があります。SSH サーバ機能を使用すると、SSH クライアントは Cisco ルータへのセキュアな暗号化された接続を確立できます。SSH クライアント機能を使用すると、Cisco ルータは別の Cisco ルータまたは SSH サーバが稼動する他のデバイスへのセキュアな暗号化された接続を確立できます。SSH への IPv6 の機能拡張により、IPv6 アドレスがサポートされるため、Cisco ルータは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。

IPv6 トランスポートを介した SNMP

IPv6 ホストが SNMP クエリーを実行したり、Cisco IOS IPv6 を実行しているデバイスから SNMP 通知を受信したりできるように、IPv6 トランスポートを介した Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を設定できます。SNMP エージェントおよび関連する MIB が拡張され、IPv6 アドレッシングがサポートされるようになりました。

SNMP for IPv6 は、メッセージの暗号化用に 3DES と AES を提供します。

Cisco IOS IPv6 MIB

シスコは長い間 IPv4 の IP-MIB と IP-FORWARD-MIB をサポートしてきました。CISCO-IETF-IP-MIB と CISCO-IETF-IP-FORWARDING-MIB は、プロトコルに依存しない MIB として定義されている IPv6 MIB ですが、IPv6 オブジェクトとテーブルについてだけ実装されています。Cisco IOS Release 12.2(33)SRC では、IP-MIB と IP-FORWARD-MIB が RFC 4293 および RFC 4292 標準に準拠するように更新されました。

- アップグレードには下位互換性があります。つまり、すべての IP-MIB と IP-FORWARD-MIB のオブジェクトやテーブルは引き続き表示されます。
- IP-MIB と IP-FORWARD-MIB には、新しい IPv6 専用、IPv4 専用、および Protocol-Version Independent（PVI）のオブジェクトとテーブルが含まれます。ただし、IPv6 では、これらの MIB 内の PVI オブジェクトとテーブルの IPv6 専用部分および新しい IPv6 部分がサポートされています。

CISCO-IETF-IP-MIB と CISCO-IETF-IP-FORWARDING-MIB は、Cisco IOS Release 12.2(33)SRC から削除されました。これらの MIB 内の情報は、新しい MIB の IP-MIB と IP-FORWARD-MIB に含まれるようになりました。

IPv6 でサポートされる MIB

IPv6 では、次の MIB がサポートされます。

- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DATA-COLLECTION-MIB
- CISCO-FLASH-MIB
- CISCO-IETF-IP-FORWARDING-MIB（Cisco IOS Release 12.2(33)SRC 以降使用不能）
- CISCO-IETF-IP-MIB（Cisco IOS Release 12.2(33)SRC 以降使用不能）
- IP-FORWARD-MIB
- IP-MIB
- ENTITY-MIB
- NOTIFICATION-LOG-MIB
- SNMP-TARGET-MIB

TFTP、remote copy protocol（rcp; リモート コピー プロトコル）、または FTP が使用されている場合、CISCO-CONFIG-COPY-MIB と CISCO-FLASH-MIB では IPv6 アドレッシングがサポートされます。

SNMP を介した IPv6 をサポートするために、次の MIB が追加されました。

- CISCO-SNMP-TARGET-EXT-MIB

SNMP を介した IPv6 をサポートするために、次の MIB が変更されました。

- CISCO-FLASH-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONFIG-COPY-MIB

Cisco IOS IPv6 組み込み管理コンポーネント

ここでは、IPv6 ネットワークおよび IPv6 と IPv4 のハイブリッド ネットワークで IPv6 に対応した操作性を実現する Cisco IOS 組み込み管理コンポーネントについて説明します。ここで説明する Cisco IOS 組み込み管理コンポーネントには、次の IPv6 機能があります。

- 「syslog」（P.5）
- 「CNS エージェント」（P.5）
- 「設定ロガー」（P.6）
- 「HTTP(S) の IPv6 サポート」（P.6）
- 「TCL」（P.6）
- 「NETCONF」（P.7）
- 「SOAP メッセージ フォーマット」（P.7）
- 「IP SLA for IPv6」（P.7）

syslog

IPv6 における Cisco IOS system message logging（syslog; システム メッセージ ロギング）プロセスを使用すると、ユーザは IPv6 アドレスを指定して syslog メッセージを外部の syslog サーバやホストに記録できます。この実装では、ホストの IP アドレスを IPv4 形式（たとえば、192.168.0.0）または IPv6 形式（たとえば、2001:0DB8:A00:1::1/64）で指定して、IPv4 ベースのロギング ホスト（syslog サーバ）を指定できます。

Cisco IOS Release 12.4(4)T および 12.2(33)SRC 以降では、この機能は既存の IPv4 および新しい IPv6 のアドレスやホスト名と下位互換性があります。

CNS エージェント

Cisco Networking Services（CNS）サブシステムでは、IPv6 アドレッシングがサポートされています。CNS は、ユーザをネットワーク サービスにリンクするための基盤テクノロジーであり、多数のネットワーク デバイスの自動設定に対応するインフラストラクチャを提供します。多くの IPv6 ネットワークは複雑で多くのデバイスが存在し、各デバイスを個別に設定する必要があります。標準設定が存在しない場合、または変更されている場合は、初期インストールとその後のアップグレードにかなりの時間がかかります。Internet Service Providers（ISP; インターネット サービス プロバイダー）には、部分的な設定を送信して新しいサービスを導入するための手段が必要です。

これらのすべての問題に対処するために、CNS は、中央のディレクトリ サービスと分散型エージェントを使用した「プラグアンドプレイ」ネットワーク サービスを提供するように設計されました。CNS 機能には、CNS エージェントとフロースルー プロビジョニング構造が含まれます。CNS フロースルー プロビジョニングは、CNS の設定エージェントとイベント エージェントを使用してワークフローを自動化するため、オンサイト技術者は必要なくなります。

IPv6 アドレッシングでは、ここで説明する CNS エージェントがサポートされます。

- 「CNS 設定エージェント」（P.5）
- 「CNS イベント エージェント」（P.5）
- 「CNS EXEC エージェント」（P.6）
- 「CNS イメージ エージェント」（P.6）

CNS 設定エージェント

CNS 設定エージェントは、Cisco IOS デバイスにおける初期設定とその後の部分的な設定に関与します。CNS 設定エンジンを使用して、Cisco IOS デバイスの初期設定、増分設定、および同期された設定アップデートを自動化するための手段を提供します。設定エンジンは、設定のロード ステータスをイベントとして報告し、ネットワーク モニタリングまたはワークフロー アプリケーションはそのイベントをサブスクライブできます。

CNS イベント エージェント

CNS イベント エージェントは、他のすべての CNS エージェントに対して CNS イベント バスへのトランスポート接続を提供します。CNS イベント エージェントが動作し、設定エンジンとルータ間の接続が正常に確立されるまでは、イベントを設定エンジンによってルータに送信できません。

イベント エージェントは CNS 設定エンジンを使用して、Cisco IOS デバイスの初期設定、増分設定、および同期された設定アップデートを自動化するための手段を提供します。

CNS EXEC エージェント

CNS EXEC エージェントを使用すると、リモート アプリケーションは、コマンドが含まれるイベント メッセージを送信することによって、Cisco IOS デバイス上で CLI コマンドを EXEC モードで実行できます。

CNS イメージ エージェント

Cisco IOS デバイスの大規模なネットワークを保持する管理者には、イメージ ファイルを多数のリモート デバイスにロードするための自動化されたメカニズムが必要です。ネットワーク管理アプリケーションを使用すると、実行するイメージやシスコ オンライン ソフトウェア センターから受信したイメージの管理方法を決定できます。他のイメージ配布ソリューションは、数千のデバイスに対応するように拡張されず、ファイアウォールの背後にあるデバイスや Network Address Translation（NAT; ネットワーク アドレス変換）を使用したデバイスにイメージを配布できません。CNS イメージ エージェントを使用すると、管理対象デバイスは、ネットワーク接続を開始したり、イメージ ダウンロードを要求したりできるため、NAT を使用したデバイスやファイアウォールの背後にあるデバイスはイメージ サーバにアクセスできます。

CNS イメージ エージェントは、CNS イベント バスを使用するように設定できます。CNS イベント バスを使用するには、CNS 設定エンジンで CNS イベント エージェントをイネーブルにし、CNS イベント ゲートウェイに接続する必要があります。CNS イメージ エージェントは、CNS イメージ エージェント プロトコルを認識する HTTP サーバを使用することもできます。CNS イメージ エージェント動作の展開では、CNS イベント バスと HTTP サーバの両方を使用できます。

CNS エージェントの詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Cisco Networking Services」を参照してください。

設定ロガー

設定ロガーは、変更を追跡したり報告したりします。設定ロガーでは、次の 2 つのコンテンツ タイプがサポートされています。

- プレーン テキスト：プレーン テキスト形式を使用すると、設定ロガーは設定変更だけを報告します。
- XML：設定ロガーは、Extensible Markup Language（XML; 拡張マークアップ言語）を使用して設定変更の詳細（変更内容、変更者、変更日時、Parser Return Code（PRC）値、増分の NVGEN 結果など）を報告します。

HTTP(S) の IPv6 サポート

この機能は、IPv6 アドレスをサポートするように HTTP(S) クライアントとサーバを拡張します。Cisco IOS ソフトウェアの HTTP サーバは、IPv6 と IPv4 の両方の HTTP クライアントからの要求を処理できます。Cisco IOS ソフトウェアの HTTP クライアントは、IPv4 と IPv6 の両方の HTTP サーバへの要求の送信をサポートします。HTTP クライアントを使用する場合、リテラル IPv6 アドレスを含む URL を RFC 2732 のルールに従った形式にする必要があります。

TCL

Tool Command Language（TCL; ツール コマンド言語）は、Embedded Syslog Manager（ESM）、Embedded Event Manager（EEM）、Interactive Voice Response（IVR; 自動音声応答）、tclsh パーサー モードなどの機能をサポートするために Cisco IOS IPv6 で使用されます。TCL では、送信側（クライアント）と受信側（サーバ）の両方のソケットがサポートされています。

NETCONF

Network Configuration Protocol（NETCONF）では、ネットワーク デバイスの管理、設定データ情報の取得、および新しい設定データのアップロードと操作に使用できるメカニズムが定義されています。NETCONF は、設定データとプロトコル メッセージに XML ベースのデータ符号化を使用します。

NETCONF の詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Network Configuration Protocol」を参照してください。

SOAP メッセージ フォーマット

Service-Oriented Access Protocol（SOAP）を使用すると、CNS メッセージのレイアウトを一貫性のある形式でフォーマットできます。SOAP は、非集中型の分散型環境で構造化された情報を交換するためのプロトコルです。XML テクノロジーを使用して、基礎となるさまざまなプロトコルを介して交換できるメッセージ フォーマットを提供する拡張メッセージ フレームワークを定義します。

SOAP メッセージ構造内にはセキュリティ ヘッダーがあり、CNS 通知メッセージによってユーザ クレデンシャルを認証できます。

CNS メッセージは、要求、応答、および通知の 3 つのメッセージ タイプに分類されます。SOAP の詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Cisco Networking Services」を参照してください。

IP SLA for IPv6

Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）は、Cisco IOS ソフトウェアを実行するほとんどのデバイスに組み込まれているテクノロジーのポートフォリオであり、シスコのカスタマーは IPv6 アプリケーションやサービスの IPv6 サービス レベルの分析、生産性の向上、運用コストの削減、およびネットワーク停止頻度の低減が可能になります。IP SLA では、ネットワーク パフォーマンスの測定にアクティブなトラフィック モニタリング（継続的で信頼性のある予測可能な方法によるトラフィックの生成）を使用します。

IPv6 では、次の Cisco IOS IP SLA がサポートされています。

- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）エコー動作：IPv4 または IPv6 を使用する Cisco ルータとデバイス間でエンドツーエンドの応答時間を監視するために使用されます。ICMP エコーは、ネットワーク接続問題のトラブルシューティングに役立ちます。
- TCP 接続動作：IPv4 または IPv6 を使用する Cisco ルータとデバイス間で TCP 接続動作の実行にかかった応答時間を測定するために使用されます。
- User Datagram Protocol（UDP; ユーザ データグラム プロトコル）エコー動作：IPv4 または IPv6 を使用する Cisco ルータとデバイス間でエンドツーエンドの応答時間を監視するために使用されます。
- UDP ジッタ動作：IPv4 または IPv6 ネットワークで UDP トラフィックを伝送するネットワークのラウンドトリップ遅延、一方向遅延、一方向ジッタ、一方向パケット損失、および接続を分析するために使用されます。
- UDP ジッタ動作：ネットワークにおける VoIP 品質レベルを予防的に監視するために使用されます。これにより、IPv4 または IPv6 ネットワーク内のユーザに対して VoIP 品質レベルを保証できます。

ネットワーク管理用 IPv6 の実装方法

ここでは、次の各手順について説明します。

- 「IPv6 ルータへの Telnet アクセスのイネーブル化と Telnet セッションの確立」（P.8）（任意）
- 「IPv6 ルータでの SSH のイネーブル化」（P.9）（任意）
- 「IPv6 を介した SNMP 通知サーバの設定」（P.11）（任意）
- 「Cisco IOS IPv6 組み込み管理コンポーネントの設定」（P.13）（任意）

IPv6 ルータへの Telnet アクセスのイネーブル化と Telnet セッションの確立

この作業では、IPv6 ルータへの Telnet アクセスをイネーブルにし、Telnet セッションを確立する方法を示します。IPv4 または IPv6 トランスポートを使用すると、Telnet を使用して、ホストからルータ、ルータからルータ、およびルータからホストに接続できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 host** *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]
4. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **password** *password*
6. **login** [**local** | **tacacs**]
7. **ipv6 access-class** *ipv6-access-list-name* {**in** | **out**}
8. **telnet** *host* [*port*] [*keyword*]

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。 • 必要に応じて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	**ipv6 host** *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*] **例：** `Router(config)# ipv6 host cisco-sj 2001:0DB8:20:1::12`	ホスト名からアドレスへのスタティック マッピングをホスト名キャッシュに定義します。

	コマンドまたはアクション	目的
ステップ 4	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] **例：** `Router(config)# line vty 0 4`	**vty** キーワードを指定して vty インターフェイスを作成します。
ステップ 5	**password** *password* **例：** `Router(config)# password hostword`	Telnet をイネーブルにするパスワードを作成します。
ステップ 6	**login** [**local** | **tacacs**] **例：** `Router(config)# login tacacs`	（任意）ログイン時のパスワード チェックをイネーブルにします。
ステップ 7	**ipv6 access-class** *ipv6-access-list-name* {**in** | **out**} **例：** `Router(config)# ipv6 access-list hostlist`	（任意）回線インターフェイスに IPv6 アクセス リストを追加します。 • このコマンドを使用すると、アクセス リストに一致するセッションへのリモート アクセスが制限されます。
ステップ 8	**telnet** *host* [*port*] [*keyword*] **例：** `Router(config)# telnet cisco-sj`	ホスト名または IPv6 アドレスを使用して、ルータからリモート ホストへの Telnet セッションを確立します。 • Telnet セッションは、ルータ名または IPv6 アドレスに対して確立できます。

IPv6 ルータでの SSH のイネーブル化

この作業では、使用する IPv6 トランスポートを介した SSH をイネーブルにする方法を示します。SSH パラメータを設定しない場合は、デフォルト値が使用されます。

前提条件

IPv6 トランスポートを介した SSH を設定する前に、次の条件が満たされていることを確認してください。

- Cisco IOS Release 12.2(8)T 以降のリリースまたは Cisco IOS Release 12.0(22)S 以降のリリースの IPsec（Data Encryption Standard（DES; データ暗号規格）または 3DES）暗号化ソフトウェア イメージがルータにロードされている。SSH サーバと SSH クライアントの IPv6 トランスポートには、IPsec 暗号化ソフトウェア イメージが必要です。
- ルータにホスト名とホスト ドメインが設定されている。IPv6 アドレスへのホスト名の割り当ておよび IPv4 と IPv6 の両方で使用できるデフォルト ドメイン名の指定については、「*Implementing IPv6 Addressing and Basic Connectivity*」の章の「Mapping Host Names to IPv6 Addresses」の項を参照してください。
- SSH を自動的にイネーブルにする Rivest, Shamir, and Adelman（RSA; Rivest、Shamir、および Adelman）キー ペアがルータに生成されている。

（注） RSA は公開鍵暗号化システムで、Ron Rivest、Adi Shamir、Leonard Adelman の 3 名によって開発されました。RSA キーは、1 つの公開鍵と 1 つの秘密鍵のペアになっています。

- ルータでローカル アクセスまたはリモート アクセスのユーザ認証メカニズムが設定されている。

制約事項

『*Cisco IOS Security Configuration Guide*』の「Configuring Secure Shell」に記載されている、IPv4 トランスポートを介した SSH の基本的な制約事項は、IPv6 トランスポートを介した SSH にも適用されます。その章に記載されている制約事項以外に、ローカルに格納されているユーザ名とパスワードを使用できるのは、IPv6 トランスポートを介した SSH によってサポートされているユーザ認証メカニズムだけです。IPv6 トランスポートを介した TACACS+ および RADIUS ユーザ認証メカニズムはサポートされません。

（注） SSH クライアントを認証するには、IPv4 トランスポートを介した TACACS+ または RADIUS を設定し、IPv6 トランスポートを介した SSH サーバに接続します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*]
4. **exit**
5. **ssh** [**-v 1** | **2**] [**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-l** *userid* | **-l** *userid*:*number ip-address* | **-l** *userid*:**rotary** *number ip-address*] [**-m** {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*]

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。 • 必要に応じて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。

	コマンドまたはアクション	目的
ステップ 3	**ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*] **例：** `Router(config)# ip ssh timeout 100 authentication-retries 2`	ルータに SSH 制御変数を設定します。 • 120 秒以内のタイムアウトを秒数で指定できます。デフォルトは 120 です。この設定は、SSH ネゴシエーション フェーズに適用されます。EXEC セッションが開始すると、vty に設定された標準のタイムアウトが適用されます。 デフォルトでは、5 本の vty 回線（0 ～ 4）が定義されています。したがって、5 本のターミナル セッションを確立できます。SSH でシェルが実行されると、vty タイムアウトが始動します。vty タイムアウトのデフォルトは 10 分です。 • 認証の再試行回数（5 回以内）も指定できます。デフォルトは 3 です。
ステップ 4	**exit** **例：** `Router(config)# exit`	コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 5	**ssh** [**-v** {**1** | **2**}] [**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-l** *userid* | **-l** *userid*:*number ip-address* | **-l** *userid*:**rotary***number ip-address*] [**-m** {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**-o** **numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*] **例：** `Router# ssh`	リモート ネットワーク デバイスとの暗号化されたセッションを開始します。

IPv6 を介した SNMP 通知サーバの設定

SNMP マネージャとエージェントとの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、パスワードと同じように機能して、ルータ上でのエージェントへのアクセスを制限します。ストリングに関連付ける特性を次の中から 1 つ以上指定することもできます。

- コミュニティ ストリングを使用したエージェントへのアクセスが許可される SNMP マネージャの IP アドレスのアクセス リスト
- 特定のコミュニティへのアクセスが可能なすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティへのアクセスが可能な MIB オブジェクトに対する読み書きアクセス権または読み取り専用アクセス権

1 つ以上のコミュニティ ストリングを設定できます。特定のコミュニティ ストリングを削除するには、**no snmp-server community** コマンドを使用します。

snmp-server host コマンドでは、SNMP 通知を受信するホスト、および通知をトラップまたは応答要求として送信するかどうかを指定します。**snmp-server enable traps** コマンドでは、指定された通知タイプの生成メカニズム（Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）トラップ、設定トラップ、エンティティ トラップ、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）トラップなど）をグローバルにイネーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]
4. **snmp-server engineID remote** {*ipv4-ip-address* | *ipv6 address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*
5. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*]{*acl-number* | *acl-name*}]
6. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
7. **snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128 | 192 |256**}} *privpassword*] {*acl-number* | *acl-name*}]
8. **snmp-server enable traps** [*notification-type*] [**vrrp**]

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。 • 必要に応じて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	**snmp-server community** *string* [**view** *view-name*] [**ro**	**rw**] [**ipv6** *nacl*] [*access-list-number*] **例：** `Router(config)# snmp-server community mgr view restricted rw ipv6 mgr2`	コミュニティ アクセス ストリングを定義します。
ステップ 4	**snmp-server engineID remote** {*ipv4-ip-address*	*ipv6-address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string* **例：** `Router(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6`	（任意）リモート SNMP エンジン（または SNMP のコピー）の名前を指定します。

	コマンドまたはアクション	目的
ステップ 5	**snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*]{*acl-number* | *acl-name*}] **例：** `Router(config)# snmp-server group public v2c access ipv6 public2`	（任意）新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマッピングするテーブルを設定します。
ステップ 6	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **例：** `Router(config)# snmp-server host host1.com 2c vrf trap-vrf`	SNMP 通知動作の受信者を指定します。 • SNMP 通知をトラップまたは応答要求として送信するかどうか、使用する SNMP のバージョン、通知のセキュリティ レベル（SNMPv3 の場合）、および通知の受信者（ホスト）を指定します。
ステップ 7	**snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** | **256**}} *privpassword*] {*acl-number* | *acl-name*}] **例：** `Router(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6 public2`	（任意）既存の SNMP グループの新しいユーザを設定します。 **（注）** アドレスのリモート ユーザを設定するには、まずそのリモート ホストのエンジン ID を設定する必要があります。これは、これらのコマンドの設計に適用される制限事項です。ホストよりも前にユーザを設定しようとすると、警告メッセージが表示され、コマンドは実行されません。
ステップ 8	**snmp-server enable traps** [*notification-type*] [**vrrp**] **例：** `Router(config)# snmp-server enable traps bgp`	トラップと応答要求の送信をイネーブルにし、送信する通知のタイプを指定します。 • *notification-type* が指定されていない場合は、サポートされているすべての通知がルータでイネーブルになります。 • ルータで使用可能な通知を確認するには、**snmp-server enable traps ?** コマンドを入力します。

Cisco IOS IPv6 組み込み管理コンポーネントの設定

IPv6 をイネーブルにすると、ほとんどの IPv6 組み込み管理コンポーネントは自動的にイネーブルになり、それ以上の設定は必要ありません。IPv6 を介した syslog を設定したり、ルータへの HTTP アクセスをディセーブルにしたりする場合は、次の各項で説明する作業を参照してください。

- 「IPv6 を介した syslog の設定」（P.13）
- 「IPv6 ルータへの HTTP アクセスのディセーブル化」（P.14）

IPv6 を介した syslog の設定

この作業では、IPv6 を介した syslog の設定方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **logging host** {{*ip-address* | *hostname*} | {**ipv6** *ipv6-address* | *hostname*}} [**transport** {**udp** [**port** *port-number*] | **tcp** [**port** *port-number*] [**audit**]}] [**xml** | **filtered** [**stream** *stream-id*]] [**alarm** [*severity*]]

手順の詳細

	コマンド	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。 • 必要に応じて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	**logging host** {{*ip-address* | *hostname*} | {**ipv6** *ipv6-address* | *hostname*}} [**transport** {**udp** [**port** *port-number*] | **tcp** [**port** *port-number*] [**audit**]}] [**xml** | **filtered** [**stream** *stream-id*]] [**alarm** [*severity*]] **例：** `Router(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF`	システム メッセージとデバッグ出力をリモート ホストに記録します。

IPv6 ルータへの HTTP アクセスのディセーブル化

HTTP サーバをイネーブルにし、ルータに IPv6 アドレスが設定されている場合、IPv6 を介した HTTP アクセスは自動的にイネーブルになります。HTTP サーバが必要ない場合は、この項の説明に従ってディセーブルにしてください。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip http server**

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。 • 必要に応じて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	**no ip http server** **例：** `Router(config)# no ip http server`	HTTP アクセスをディセーブルにします。

ネットワーク管理用 IPv6 の実装の設定例

ここでは、次の設定例について説明します。

- 「IPv6 ルータへの Telnet アクセスのイネーブル化：例」（P.15）
- 「ルータへの HTTP アクセスのディセーブル化：例」
- 「IPv6 を介した SNMP 通知サーバの設定：例」（P.17）

IPv6 ルータへの Telnet アクセスのイネーブル化：例

次に、Telnet をイネーブルにし、IPv6 ルータとの間のセッションを開始する例を示します。次の例では、IPv6 アドレス 2001:0db8:20:1::12 とホスト名 cisco-sj が指定されています。この情報を確認するために、**show host** コマンドが使用されています。

```
Router# configure terminal
Router(config)# ipv6 host cisco-sj 2001:0db8:20:1::12
Router(config)# end
Router# show host

Default domain is not set
Name/address lookup uses static mappings

Codes:UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                 Port  Flags      Age Type   Address(es)
cisco-sj             None  (perm, OK)  0  IPv6 2001:0db8:20:1::12
```

ルータへの Telnet アクセスをイネーブルにするには、vty インターフェイスとパスワードを作成します。

```
Router(config)# line vty 0 4

password lab
login
```

Telnet を使用してルータにアクセスするには、パスワードを入力する必要があります。

```
Router# telnet cisco-sj

Trying cisco-sj (2001:0db8:20:1::12)... Open

User Access Verification

Password:
cisco-sj
.
.
.
verification
```

telnet コマンドを使用する必要はありません。次の例に示すように、ホスト名またはアドレスを指定するだけで十分です。

```
Router# cisco-sj
```

または

```
Router# 2001:0db8:20:1::12
```

接続先ルータ上の IPv6 接続ユーザ（回線 130）を表示するには、**show users** コマンドを使用します。

```
Router# show users

    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
 130 vty 0                idle                 00:00:22   8800::3
```

表示されるアドレスは、接続元の IPv6 アドレスです。Domain Name Server（DNS; ドメイン ネーム サーバ）またはローカルのホスト キャッシュで接続元のホスト名が既知の場合は、代わりにホスト名が表示されます。

```
Router# show users

    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
 130 vty 0                idle                 00:02:47   cisco-sj
```

接続ルータのユーザが ^6x とのセッションを一時停止して **show sessions** コマンドを入力すると、IPv6 接続が表示されます。

```
Router# show sessions

Conn Host               Address             Byte  Idle Conn Name
*  1 cisco-sj 2001:0db8:20:1::12      0     0 cisco-sj
```

Conn Name フィールドには、宛先のホスト名（既知の場合だけ）が表示されます。ホスト名が不明な場合、出力は次のようになります。

```
Router# show sessions

Conn Host               Address             Byte  Idle Conn Name
*  1 2001:0db8:20:1::12 2001:0db8:20:1::12      0     0 2001:0db8:20:1::12
```

ルータへの HTTP アクセスのディセーブル化：例

次の例では、**show running-config** コマンドを使用すると、ルータで HTTP アクセスがディセーブルになっていることが示されています。

```
Router# show running-config

Building configuration...
!
Current configuration : 1490 bytes
!
version 12.2
!
hostname Router
!
no ip http server
!
line con 0
line aux 0
line vty 0 4
```

IPv6 を介した SNMP 通知サーバの設定：例

次に、コミュニティ ストリング public を使用して、SNMP が読み取り専用アクセス権ですべてのオブジェクトにアクセスすることを許可する例を示します。また、ルータは、BGP トラップを SNMPv1 を使用して IPv4 ホスト 172.16.1.111 と IPv6 ホスト 3ffe:b00:c18:1::3/127 に送信し、SNMPv2c を使用してホスト 172.16.1.27 に送信します。トラップとともにコミュニティ ストリング public が送信されます。

```
Router(config)# snmp-server community public
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host 172.16.1.27 version 2c public
Router(config)# snmp-server host 172.16.1.111 version 1 public
Router(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

SNMP サーバ グループを指定したビューに関連付ける例

次に、SNMP コンテキスト A を SNMPv2c グループ GROUP1 のビューと IPv6 の名前付きアクセス リスト public2 に関連付ける例を示します。

```
Router(config)# snmp-server context A
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp mib target list commAVpn vrf CustomerA
Router(config)# snmp-server view viewA ciscoPingMIB included
Router(config)# snmp-server view viewA ipForward included
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify
  access ipv6 public2
```

SNMP 通知サーバの作成例

次に、IPv6 ホストを通知サーバとして設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Router(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Router(config)# snmp-server group public v2c access ipv6 public2
Router(cofig)# snmp-server host host1.com 2c vrf trap-vrf
Router(cofig)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6
public2
Router(config)# snmp-server enable traps bgp
Router(config)# exit
```

関連情報

IPv6 ルーティング プロトコルを実装する場合は、「*Implementing RIP for IPv6*」、「*Implementing IS-IS for IPv6*」、または「*Implementing Multiprotocol BGP for IPv6*」の章を参照してください。

その他の関連資料

ここでは、IPv6 を介した Cisco IOS アプリケーションの管理に関する関連資料について説明します。

関連資料

関連項目	参照先
IPv6 でサポートされる機能	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
基本的な IPv6 の設定作業	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
SSH 設定情報	『*Cisco IOS Security Command Reference*』
IPv4 CNS、SOAP	『*Cisco IOS Network Management Configuration Guide*』の「Cisco Networking Services」
NETCONF	『*Cisco IOS Network Management Configuration Guide*』の「Network Configuration Protocol」
IP SLA for IPv6	• 『*IP SLAs—Analyzing IP Service Levels Using the ICMP Echo Operation*』 • 『*IP SLAs—Analyzing IP Service Levels Using the TCP Connect Operation*』 • 『*IP SLAs—Analyzing IP Service Levels Using the UDP Echo Operation*』 • 『*IP SLAs—Analyzing IP Service Levels Using the UDP Jitter Operation*』 • 『*IP SLAs—Analyzing VoIP Service Levels Using the UDP Jitter Operation*』

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または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-DATA-COLLECTION-MIB • CISCO-FLASH-MIB • CISCO-RTTMON-IPv6-MIB • CISCO-SNMP-TARGET-EXT-MIB • ENTITY-MIB • IP-FORWARD-MIB • IP-MIB • NOTIFICATION-LOG-MIB • SNMP-TARGET-MIB	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://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2732	『*Format for Literal IPv6 Addresses in URLs*』
RFC 3414	『*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*』
RFC 3484	『*Default Address Selection for Internet Protocol version 6 (IPv6)*』
RFC 4292	『*IP Forwarding Table MIB*』
RFC 4293	『*Management Information Base for the Internet Protocol (IP)*』

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/en/US/support/index.html

ネットワーク管理用 IPv6 の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表に示されているのは、Cisco IOS Release 12.2(2)T または 12.0(3)S 以降のリリースで導入または変更された機能だけです。

ここに記載されていないこのテクノロジーの機能情報については、「*Start Here: Cisco IOS Software Release Specifics for IPv6 Features*」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア 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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IPv6 を介した Cisco IOS アプリケーションの管理の機能情報

機能名	リリース	機能情報
IPv6 を介した Telnet アクセス	12.0(22)S 12.2(2)T 12.2(14)S 12.2(28)SB 12.3 12.3(2)T 12.4 12.4(2)T	Cisco IOS ソフトウェアの Telnet クライアントとサーバでは、IPv6 接続がサポートされています。IPv6 Telnet クライアントを使用してルータへの Telnet セッションを直接確立するか、またはルータから IPv6 Telnet 接続を開始できます。 この機能に関する詳細については、次の各項を参照してください。 • 「ネットワーク管理用 IPv6 の実装の前提条件」（P.2） • 「IPv6 を介した Telnet アクセス」（P.2） • 「IPv6 ルータへの Telnet アクセスのイネーブル化と Telnet セッションの確立」（P.8） • 「IPv6 ルータへの Telnet アクセスのイネーブル化 : 例」（P.15）
IPv6 での TFTP ファイルのダウンロード	12.0(22)S 12.2(2)T 12.2(14)S 12.2(28)SB 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 では、TFTP ファイルのダウンロードとアップロードがサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 での TFTP ファイルのダウンロード」（P.2）
IPv6 トランスポートを介した SSH	12.0(22)S 12.2(8)T 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 における SSH は、IPv4 における SSH と同じように機能し、同じ利点があります。SSH サーバ機能を使用すると、SSH クライアントは Cisco ルータへのセキュアな暗号化された接続を確立できます。SSH クライアント機能を使用すると、Cisco ルータは別の Cisco ルータまたは SSH サーバが稼動する他のデバイスへのセキュアな暗号化された接続を確立できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SSH」（P.3） • 「IPv6 ルータでの SSH のイネーブル化」（P.9）

表 1　IPv6 を介した Cisco IOS アプリケーションの管理の機能情報（続き）

機能名	リリース	機能情報
IPv6 を介した SNMP	12.0(27)S 12.2(33)SRB 12.2(33)SXI 12.3(14)T 12.4 12.4(2)T	IPv6 ホストが SNMP クエリーを実行したり、Cisco IOS IPv6 を実行しているデバイスから SNMP 通知を受信したりできるように、IPv6 トランスポートを介した SNMP を設定できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SNMP」（P.3） • 「IPv6 を介した SNMP 通知サーバの設定」（P.11） • 「IPv6 を介した SNMP 通知サーバの設定：例」（P.17）
IPv6 サービス：IP-FORWARD-MIB のサポート	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	MIB は、デバイス上の管理可能なオブジェクトのデータベースです。管理対象オブジェクト、つまり変数を設定したり読み取ったりして、ネットワーク デバイスやインターフェイスに関する情報を提供できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SNMP」（P.3）
IPv6 サービス：IP-MIB のサポート	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	MIB は、デバイス上の管理可能なオブジェクトのデータベースです。管理対象オブジェクト、つまり変数を設定したり読み取ったりして、ネットワーク デバイスやインターフェイスに関する情報を提供できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SNMP」（P.3）
SNMPv3：3DES および AES 暗号化のサポート	12.2(33)SB 12.2(33)SRB 12.2(33)SXI 12.4(2)T	SNMP for IPv6 では、3DES および AES 暗号化がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SNMP」（P.3） • 「IPv6 ルータでの SSH のイネーブル化」（P.9）
IPv6 サービス：RFC 4293 IP-MIB（IPv6 だけ）および RFC 4292 IP-FORWARD-MIB（IPv6 だけ）	12.2(33)SB 12.2(33)SRC	IP-FORWARD-MIB と IP-MIB は、それぞれ RFC 4292 標準と RFC 4293 標準に準拠するように更新されました。 この機能に関する詳細については、次の項を参照してください。 • 「Cisco IOS IPv6 MIB」（P.3）
IPv6 サービス：RFC 4293 IP-MIB（IPv6 だけ）	12.2(33)SB	IP-MIB は、RFC 4293 標準に準拠するように更新されました。 この機能に関する詳細については、次の項を参照してください。 • 「Cisco IOS IPv6 MIB」（P.3）

表 1　IPv6 を介した Cisco IOS アプリケーションの管理の機能情報（続き）

機能名	リリース	機能情報
IPv6：IPv6 での syslog	12.2(33)SB 12.2(33)SRC 12.2(33)SXI 12.4(4)T	IPv6 における Cisco IOS syslog プロセスを使用すると、ユーザは IPv6 アドレスを指定して syslog メッセージを外部の syslog サーバやホストに記録できます。 この機能に関する詳細については、次の項を参照してください。 • 「syslog」（P.5）
CNS エージェント for IPv6	12.2(33)SB 12.2(33)SRC 12.4(20)T	CNS 設定エージェントとイベント エージェントは、CNS 設定エンジンを使用して、Cisco IOS デバイスの初期設定、増分設定、および同期された設定アップデートを自動化するための手段を提供します。設定エンジンは、設定のロード ステータスをイベントとして報告し、ネットワーク モニタリングまたはワークフロー アプリケーションはそのイベントをサブスクライブできます。 この機能に関する詳細については、次の項を参照してください。 • 「CNS エージェント」（P.5）
設定ロガーでの IPv6	12.2(33)SB 12.2(33)SRC 12.4(20)T	設定ロガーは、変更を追跡したり報告したりします。 この機能に関する詳細については、次の項を参照してください。 • 「設定ロガー」（P.6）
HTTP(S) の IPv6 サポート	12.2(33)SB 12.2(33)SRC 12.4(20)T	この機能は、IPv6 アドレスをサポートするように HTTP(S) クライアントとサーバを拡張します。 この機能に関する詳細については、次の項を参照してください。 • 「HTTP(S) の IPv6 サポート」（P.6）
IPv6 での TCL のサポート	12.2(33)SRC 12.4(20)T	IPv6 では、TCL がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「TCL」（P.6）
IPv6 NETCONF のサポート	12.2(33)SB 12.2(33)SRC 12.4(20)T	Network Configuration Protocol（NETCONF）では、ネットワーク デバイスの管理、設定データ情報の取得、および新しい設定データのアップロードと操作に使用できる簡単なメカニズムが定義されています。 この機能に関する詳細については、次の項を参照してください。 • 「NETCONF」（P.7）

表 1　IPv6 を介した Cisco IOS アプリケーションの管理の機能情報（続き）

機能名	リリース	機能情報
SOAP での IPv6 のサポート	12.2(33)SB 12.2(33)SRC 12.4(20)T	SOAP は、非集中型の分散型環境で構造化された情報を交換するためのプロトコルです。この機能に関する詳細については、次の項を参照してください。 • 「SOAP メッセージ フォーマット」（P.7）
IP SLA for IPv6	12.2(33)SB 12.2(33)SRC 12.4(20)T	IPv6 では IP SLA がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「IP SLA for IPv6」（P.7）