IPv6 ネットワーク コンフィギュレーション ガイド

初版：2012 年 10 月 09 日

最終更新：2012 年 10 月 09 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと発展しています。これにより、スイッチングおよびルーティング ポートフォリオの幅広い範囲のアクセスおよびエッジ製品に 1 つのリリースで対応できます。

（注） 技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディング ページに表示されている場合は、その機能がプラットフォームでサポートされていることを示します。

第 2 章

IPv6 を介した Telnet アクセス

Cisco 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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

IPv6 を介した Telnet アクセスの前提条件

デバイスへの IPv6 を介した 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 を介した Telnet アクセスに関する情報

IPv6 を介した Telnet アクセス

Cisco 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デバイスへの Telnet セッションを直接確立するか、またはデバイスから IPv6 Telnet 接続を開始できます。IPv6 デバイスへの 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 を介した Telnet アクセスをイネーブルにする方法

IPv6 デバイスへの Telnet アクセスのイネーブル化と Telnet セッションの確立

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6host***name* [*port*] *ipv6-address*
4. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **password***password*
6. **login** [**local** | **tacacs**]
7. **ipv6access-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configureterminal** 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	**ipv6host***name* [*port*] *ipv6-address* 例： `Device(config)# ipv6 host cisco-sj 2001:DB8:20:1::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。
ステップ 4	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Device(config)# line vty 0 4`	vty インターフェイスを作成します。
ステップ 5	**password***password* 例： `Device(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： `Device(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	**ipv6access-class***ipv6-access-list-name* {**in** | **out**] 例： `Device(config)# ipv6 access-list hostlist`	（任意）ライン 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して、アクセス リストに一致するセッションへのリモート アクセスを制限します。
ステップ 8	**telnet***host* [*port*] [*keyword*] 例： `Device(config)# telnet cisco-sj`	ホスト名または IPv6 アドレスを使用して、デバイスからリモート ホストへの Telnet セッションを確立します。 • Telnet セッションは、デバイス名または IPv6 アドレス向けに確立することができます。

IPv6 を介した Telnet アクセスの設定例

例：IPv6 デバイスへの Telnet アクセスのイネーブル化

次に、Telnet をイネーブルにし、IPv6 デバイス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 アドレスは 2001:DB8:20:1::12、ホスト名は as cisco-sj に指定されています。この情報を確認するために、**showhost** コマンドが使用されています。

```
Device# configure terminal
Device(config)# ipv6 host cisco-sj 2001:DB8:20:1::12
Device(config)# end
Device# 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:DB8:20:1::12
```

デバイスへの 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。

```
Device(config)# line vty 0 4
password lab
login
```

Telnet を使用してデバイス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。

```
Device# telnet cisco-sj
Trying cisco-sj (2001:DB8:20:1::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。

```
Device# cisco-sj
```

または

```
Device# 2001:DB8:20:1::12
```

接続先デバイス上の IPv6 接続ユーザ（回線 130）を表示するには、**showusers** コマンドを使用します。

```
Device# 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。ドメイン ネーム サーバ（DNS）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。

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

接続デバイスのユーザが ^6x とのセッションを一時停止して **showsessions** コマンドを入力すると、IPv6 接続が表示されます。

```
Device# show sessions
Conn Host                Address              Byte  Idle Conn Name
*   1 cisco-sj 2001:DB8:20:1::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。

```
Device# show sessions
Conn Host                Address              Byte  Idle Conn Name
*   1 2001:DB8:20:1::12 2001:DB8:20:1::12      0     0 2001:DB8:20:1::12
```

IPv6 ソース ガードおよびプレフィックス ガードに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
IPv4 アドレス指定	『*IP Addressing: IPv4 Addressing Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

IPv6 を介した Telnet アクセスの機能情報

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*：*IPv6* を介した *Telnet* アクセスの機能情報

機能名	リリース	機能情報
IPv6 を介した Telnet アクセス	12.2(2)T 12.2(18)SXE 12.2(25)SEA 12.2(25)SG 12.2(33)SRA 15.0(2)SG Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2SG	IPv6 を介した Telnet アクセスがサポートされています。 次の各コマンドが導入または変更されました。**ipv6 access-class**、**ipv6 host**。

第 3 章

TFTP に対する IPv6 サポート

TFTP は自身のトランスポートとして IPv4 または IPv6を介した UDP を使用し、IPv4 および IPv6 ネットワーク レイヤを介して動作できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

TFTP に対する IPv6 サポートに関する情報

TFTP IPv6 サポート

TFTP は、可能な限り最小限の機能セットを使用して、1 つのホストから別のホストへネットワーク経由でファイルを転送するように設計されています。TFTP は、クライアントがサーバとの間でファイルのコピーを要求可能なクライアント/サーバ モデルを使用します。TFTP は自身のトラン

スポートとして IPv4 または IPv6を介した UDP を使用し、IPv4 および IPv6 ネットワーク レイヤを介して動作できます。

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および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、デバイス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。

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

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

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。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

TFTP の IPv6 サポートの機能情報

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 *2*：*TFTP の IPv6* サポートの機能情報

機能名	リリース	機能情報
TFTP IPv6 サポート		TFTP の IPv6 サポートがサポートされています。 追加または変更されたコマンドはありません。

第 4 章

IPv6 を介した SSH サポート

セキュア シェル（SSH）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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

IPv6 を介した SSH サポートの前提条件

- IPSec（データ暗号規格（DES）または3DES）暗号ソフトウェア イメージがデバイスにロードされている。SSH サーバおよび SSH クライアントへの 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。
- デバイスのホスト名およびホスト ドメインが設定されている。
- SSH を自動的にイネーブルにする Rivest、Shamir、および Adelman（RSA）キー ペアがデバイスに生成されている。
- ローカル アクセスまたはリモート アクセス用にユーザ認証メカニズムがデバイスに設定されている。
- IPv4 トランスポートを介した TACACS+ または RADIUS を設定した後に IPv6 トランスポートを介して SSH サーバ に接続し、SSH クライアントを認証する。

IPv4 トランスポートを介した SSH 用の基本的な制限は、IPv6 トランスポートを介した SSH に適用されます。ローカルに保存されたユーザ名とパスワードの使用は、IPv6 トランスポートを介した SSH によってサポートされる唯一のユーザ認証メカニズムです。TACACS+ および RADIUS ユーザ認証メカニズムは、IPv6 トランスポートを介してサポートされていません。

IPv6 を介した SSH サポートに関する情報

IPv6 トランスポートを介した SSH

IPv6 におけるセキュア シェル（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 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 クライアント機能を使用すると、Cisco デバイスは別の Cisco デバイスまたは SSH サーバが稼働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 デバイスは 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 を介した SSH サポートをイネーブルにする方法

IPv6 デバイスでの SSH のイネーブル化

このタスクはオプションです。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。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipssh**[**timeout***seconds* | **authentication-retries***integer*]
4. **exit**
5. **ssh** [**-v** { **1** | **2** } | **c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** } | **-l** *userid* | **-l** *userid:vrfname number ip-address 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** | **-vrf**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**ipssh**[**timeout***seconds* | **authentication-retries***integer*] 例： `Device(config)# IP ssh timeout 100 authentication-retries 2`	デバイス上で SSH 制御変数を設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	コンフィギュレーションモードを終了して、デバイスが特権 EXEC モードに戻ります。
ステップ 5	**ssh** [**-v** { **1** | **2** } | **c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** } | **-l** *userid* | **-l** *userid:vrfname number ip-address 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** | **-vrf**] 例： `Device# ssh -l userid1 2001:db8:2222:1044::72`	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 SSH サポートの設定例

例：IPv6 デバイスでの SSH のイネーブル化

```
Device# configure terminal
Device(config)# ip ssh
Device(config)# exit
Device(config)# ssh -l userid1 2001:db8:2222:1044::72
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

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。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

IPv6 を介した SSH サポートの機能情報

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 *3* : *IPv6* を介した *SSH* サポートの機能情報

機能名	リリース	機能情報
IPv6 を介した SSH サポート	12.2(8)T 12.2(17a)SX1 12.2(25)SEE 12.2(25)SG 12.2(33)SRA 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	SSH 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。 次の各コマンドが導入または変更されました。**ip ssh**、**ssh**。

第 5 章

SNMP over IPv6

簡易ネットワーク管理プロトコル（SNMP）を IPv6 トランスポート経由で設定し、IPv6 ホストが SNMP クエリーを実行し、IPv6 を実行しているデバイスから SNMP 通知を受信できるようにすることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

SNMP over IPv6 に関する情報

SNMP over an IPv6 Transport

簡易ネットワーク管理プロトコル（SNMP）を IPv6 トランスポート経由で設定し、IPv6 ホストが SNMP クエリーを実行し、IPv6 ソフトウェアを実行しているデバイスから SNMP 通知を受信できるようにすることができます。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。この機能は、Data Encryption Standard（3DES）および Advanced Encryption Standard（AES）のメッセージ暗号化規格を使用します。

SNMP over IPv6 を設定する方法

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、デバイス上のエージェントへのアクセスを制御するパスワードのように機能します。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。

- エージェントへのアクセスを取得するためにコミュニティ ストリングを使用することを許可された 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、**nosnmp-servercommunity** コマンドを使用します。

snmp-serverhost コマンドでは、どのホストで SNMP 通知を受信するか、および通知がトラップとインフォーム要求のどちらで送信されるようにするかを指定します。**snmp-serverenabletraps** コマンドは、指定された通知タイプ（ボーダー ゲートウェイ プロトコル（BGP）トラップ、設定トラップ、エンティティ トラップ、ホットスタンバイ ルータ プロトコル（HSRP）トラップ）の生成メカニズムをグローバルにイネーブルにします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **snmp-servercommunity***string* [**view***view-name*] [**ro** | **rw**] [**ipv6***nacl*] [*access-list-number*]
4. **snmp-serverengineIDremote** {*ipv4-ip-address* | *ipv6-address*} [**udp-port***udp-port-number*] [**vrf***vrf-name*] *engineid-string*
5. **snmp-servergroup***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-serverhost** {*hostname* | *ip-address*} [**vrf***vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port***port*] [*notification-type*]
7. **snmp-serveruser***usernamegroup-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-serverenabletraps** [*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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**snmp-servercommunity***string* [**view***view-name*] [**ro** | **rw**] [**ipv6***nacl*] [*access-list-number*] 例： `Device(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-serverengineIDremote** {*ipv4-ip-address* | *ipv6-address*} [**udp-port***udp-port-number*] [**vrf***vrf-name*] *engineid-string* 例： `Device(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-servergroup***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： `Device(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-serverhost** {*hostname* | *ip-address*} [**vrf***vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port***port*] [*notification-type*] 例： `Device(config)# snmp-server host host1.com 2c vrf trap-vrf`	SNMP 通知動作の指定 • 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-serveruser***usernamegroup-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： `Device(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6 public2`	（任意）既存の SNMP グループに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として課された制限です。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-serverenabletraps** [*notification-type*] [**vrrp**] 例： `Device(config)# snmp-server enable traps bgp`	トラップまたはインフォームの送信をイネーブルにして、送信される通知のタイプを指定します。 • *notification-type* 引数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デバイスでイネーブルになります。 • デバイスで使用可能な通知を確認するには、**snmp-serverenabletraps?** コマンドを入力します。

SNMP over IPv6 の設定例

例：IPv6 を介した SNMP 通知サーバの設定

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、デバイスは、ボーダー ゲートウェイ プロトコル（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。

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

例：SNMP サーバ グループと指定されたビューとの関連付け

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。

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

例：SNMP 通知サーバの作成

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。

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

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

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。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

SNMP over IPv6 の機能情報

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 *4*：***SNMP over IPv6*** の機能情報

機能名	リリース	機能情報
SNMP over IPv6	12.2(33)SRB 12.2(33)SXI 12.2(44)SE 12.2(44)SG 12.3(14)T 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	SNMP を IPv6 転送上で設定できるため、IPv6 ホストは SNMP クエリーを実行でき、IPv6 を実行するデバイスから SNMP 通知を受信できます。 次の各コマンドが導入または変更されました。**snmp-server community**、**snmp-server enable traps**、**snmp-server engineID remote**、**snmp-server group**、**snmp-server host**、**snmp-server user**。

機能名	リリース	機能情報
SNMPv3--3DES および AES 暗号化サポート	12.2(33)SRB 12.2(33)SXI 12.2(50)SG 12.2(52)SE 12.4(2)T 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	IPv6 は NMPv3--3DES および AES 暗号化サポート機能をサポートしています。 追加または変更されたコマンドはありません。

第 6 章

IPv6 MIB

このマニュアルでは、IPv6 用に実装された MIB について説明しています。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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

IPv6 MIB に関する情報

Cisco 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。IP-MIB および IP-FORWARD-MIB は、次のとおり RFC 4293 および RFC 4292 基準に準拠します。

- 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の定義が含まれます。

CISCO-IETF-IP-MIB および CISCO-IETF-IP-FORWARDING-MIB は、CISCO-IETF-IP-MIB および CISCO-IETF-IP-FORWARDING-MIB が適用された Cisco リリースから削除されました。CISCO-IETF-IP-MIB および CISCO-IETF-IP-FORWARDING-MIB の情報は、IP-MIB および IP-FORWARD-MIB に含まれます。

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-SNMP-TARGET-EXT-MIB
- ENTITY-MIB
- IP-FORWARD-MIB
- IP-MIB
- NOTIFICATION-LOG-MIB
- SNMP-TARGET-MIB

TFTP、リモート コピー プロトコル（RCP）、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。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

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。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

IPv6 MIB の機能情報

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 5：***IPv6 MIB* の機能情報**

機能名	リリース	機能情報
IPv6 MIB	12.0(22)S 12.2(14)S 12.2(15)T 12.2(28)SB 12.2(33)SRA 12.2(50)SY 15.0(1)SY Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.9S	この機能は、IPv6 でサポートされます。 追加または変更されたコマンドはありません。 Cisco IOS XE Release 3.9S では、Cisco ISR 4400 シリーズ ルータのサポートが追加されました。
IPv6 サービス：RFC 4293 IP-MIB（IPv6 のみ）および RFC 4292 IP-FORWARD-MIB（IPv6 のみ）	12.2(33)SRC 12.2(50)SY 12.2(54)SG 12.2(58)SE 15.0(2)SG 15.0(1)SY 15.1(3)T Cisco IOS XE Release 2.1 3.2SG	IP-FORWARD-MIB および IP-MIB は、それぞれ RFC 4292 および RFC 4293 規格に準拠するように更新されました。 追加または変更されたコマンドはありません。

第 7 章

IPv6 組み込み管理コンポーネント

Cisco 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。このマニュアルでは、次の組み込み管理コンポーネントについて説明しています。syslog、config logger、TCL、NETCONF、SOAP メッセージ フォーマット。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

IPv6 組み込み管理コンポーネントに関する情報

Syslog

IPv6 における Cisco システム メッセージ ロギング（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。この実装では、ユーザはホストの 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:DB8: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。

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、XML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。

TCL

IPv6 用の Cisco ソフトウェアでは Tool Command Language（TCL）が使用され、Embedded Syslog Manager（ESM）、Embedded Event Manager（EEM）、Interactive Voice Response（IVR）、および tclsh パーサー モードなどの機能をサポートします。TCL は、開始（クライアント）およびリスニング（サーバ）ソケットの両方をサポートします。

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可能な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。

Service-Oriented Access Protocol（SOAP）メッセージ フォーマット

Service-Oriented Access Protocol（SOAP）を使用すると、Cisco Networking Service（CNS）メッセージのレイアウトを一貫性のある方法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の交換を目的としています。SOAP は XML テクノロジーを使用し、さまざま

な基本プロトコルで交換可能なメッセージ フォーマットを提供する、拡張性のあるメッセージング フレームワークを定義します。

SOAP メッセージ構造には、CNS 通知メッセージがユーザ クレデンシャルを認証できるセキュリティ ヘッダーがあります。

IPv6 組み込み管理コンポーネントの設定方法

Syslog over IPv6 の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **logginghost** {{*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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**logginghost** {{*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： `Device(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF`	リモート ホストへのシステム メッセージおよびデバッグ出力を記録します。

IPv6 組み込み管理コンポーネントの設定例

例：Syslog over IPv6 の設定

```
Device(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF transport tcp port 1470
```

IPv6 組み込み管理コンポーネントに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco_IOS_IPv6_Feature_Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

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。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

IPv6 組み込み管理コンポーネントの機能情報

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 *6*：*IPv6* 組み込み管理コンポーネントの機能情報

機能名	リリース	機能情報
IPv6：設定ロガー	12.2(33)SB 12.2(33)SRC 12.2(50)SG 12.2(50)SY 12.4(20)T 15.0(1)SY 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	IPv6 は、この機能をサポートします。 追加または変更されたコマンドはありません。

機能名	リリース	機能情報
IPv6：NETCONF	12.2(33)SB 12.2(33)SRC 12.2(50)SG 12.2(50)SY 12.4(20)T 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	IPv6は、この機能をサポートします。 追加または変更されたコマンドはありません。
SOAP での IPv6 サポート	12.2(33)SB 12.2(33)SRC 12.2(50)SG 12.2(50)SY 12.4(20)T 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	IPv6は、この機能をサポートします。 追加または変更されたコマンドはありません。
IPv6：TCL	12.2(33)SB 12.2(33)SRC 12.2(50)SG 12.2(50)SY 12.4(20)T 15.0(1)SY 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	IPv6は、この機能をサポートします。 追加または変更されたコマンドはありません。

機能名	リリース	機能情報
IPv6 での Syslog	12.2(33)SB 12.2(33)SRC 12.2(33)SXI 12.2(44)SE 12.2(44)SG 12.4(4)T 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	IPv6 における Cisco 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。 次のコマンドが導入されました。**logging host**。

第 8 章

IPv6 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。このマニュアルでは、IPv6 でサポートされる CNS エージェントについて説明しています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

IPv6 CNS エージェントに関する情報

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。ISP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

CNS 設定エージェントは、Cisco 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 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、設定エンジンとデバイス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デバイスに送信できません。

イベント エージェントは CNS 設定エンジンを使用して、Cisco 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 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

シスコ 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ネットワーク アドレス変換（NAT）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。

IPv6 IOS ファイアウォールの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

IPv6 CNS エージェントの機能情報

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 *7*：***IPv6 CNS*** エージェントの機能情報

機能名	リリース	機能情報
IPv6 CNS エージェント	12.2(33)SB 12.2(33)SRC 12.2(50)SY 12.4(20)T Cisco IOS XE Release 3.9S	CNS 設定エージェントおよびイベントエージェントは、CNS 設定エンジンを使用してデバイスの初期設定、差分設定、および同期設定の更新を自動化するための方法を提供し、設定エンジンは、設定ロードのステータスをネットワーク モニタリングまたはワークフロー アプリケーションが加入できるイベントとして報告します。 追加または変更されたコマンドはありません。 Cisco IOS XE Release 3.9S では、Cisco CSR 1000V のサポートが追加されました。

第 9 章

IPv6 HTTP（S）

Hypertext Transfer Protocol サーバ HTTP（S）は、Cisco IPv6 組み込み管理コンポーネントです。Cisco 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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

IPv6 HTTP（S）に関する情報

Cisco IPv6 組み込み管理コンポーネント

シスコの組み込み管理コンポーネントは、IPv6 ネットワークおよびデュアル スタックの IPv6 と IPv4 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。

HTTP（S）の IPv6 サポート

この機能は、HTTP（S）クライアントとサーバで IPv6 アドレスをサポートするようにします。

Cisco 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。HTTP（S）サーバがクライアントからの接続を受け入れると、サーバはそのクライアントが IPv4 であるか IPv6 ホストであるかを決定します。それに応じて、ソケット コールを受け入れる IPv4 または IPv6 のアドレス ファミリが選択されます。リスニング ソケットは、IPv4 と IPv6 の両方の接続を待ち受け続けます。

Cisco ソフトウェアの HTTP クライアントは、IPv4 と IPv6 の両 HTTP サーバへの要求を送信できます。

IPv6 HTTP クライアントを使用すると、実際の IPv6 アドレスの URL は、RFC 2732 のルールを使用してフォーマットする必要があります。

IPv6 HTTP（S）の設定方法

IPv6 デバイスへの 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、デバイスに 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 サーバが必要でない場合は、ディセーブルにする必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **noiphttpserver**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**noiphttpserver** 例： `Device(config)# no ip http server`	HTTP アクセスをディセーブルにします。

IPv6 HTTP（S）の設定例

例：デバイスへの HTTP アクセスのディセーブル化

次の例では、**showrunning-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。

```
Device# show running-config

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

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP アクセス リスト コマンド	『*Cisco IOS Security Command Reference*』
IP アクセス リストの設定	『IP アクセス リストの作成とインターフェイスへの適用』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

IPv6 HTTP（S）の機能情報

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 *8*：*IPv6 HTTP*（*S*）の機能情報

機能名	リリース	機能情報
IPv6 HTTP（S）	12.2(33)SB 12.2(33)SRC 12.2(50)SY 12.4(20)T 15.0(1)SY Cisco IOS XE Release 3.8S	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有効にします。 次のコマンドが変更されました。**ip http server**。

第 10 章

IPv6 用 IP SLA

Cisco IP サービス レベル契約（SLA）は、シスコの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たテクノロジーのポートフォリオです。SLA により、IPv6 アプリケーションとサービスの IPv6 サービス レベルを分析するとともに、生産性の向上、運用コストの削減、ネットワーク停止頻度の低減を実現できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

IP SLA for IPv6 に関する情報

Cisco IPv6 組み込み管理コンポーネント

シスコの組み込み管理コンポーネントは、IPv6 ネットワークおよびデュアル スタックの IPv6 と IPv4 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。

IPv6 用 IP SLA

Cisco IP サービス レベル契約（SLA）は、Cisco 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 ポートフォリオです。シスコのソフトウェアにより、IPv6 アプリケーションとサービスの IPv6 サービス レベルを分析するとともに、生産性の向上、運用コストの削減、ネットワーク停止頻度の低減を実現できます。IP SLA は、アクティブ トラフィック モニタリングを使用します。これにより、継続的で信頼性のある予測可能な方法でトラフィックが生成され、ネットワーク パフォーマンスを測定できます。

IPv6 では、次の Cisco IP SLA がサポートされています。

- インターネット制御メッセージ プロトコル（ICMP）エコー動作：IPv4 または IPv6 を使用する Cisco デバイスとその他の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 デバイスとその他のデバイス間で TCP が接続されるまでの応答時間を測定するために使用されます。
- ユーザ データグラム プロトコル（UDP）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。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

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。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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/cisco/web/support/index.html

IP SLA for IPv6 の機能情報

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 *9*：*IP SLA for IPv6* の機能情報

機能名	リリース	機能情報
IPv6 用 IP SLA	12.2(33)SRC 12.2(50)SG 12.2(50)SY 12.4(20)T 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	IPv6 は、この機能をサポートします。 追加または変更されたコマンドはありません。

第 11 章

IPv6 の RFC

標準規格および RFC

RFC	タイトル
RFC 1195	『*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*』
RFC 1267	『*A Border Gateway Protocol 3 (BGP-3)*』
RFC 1305	『*Network Time Protocol (Version 3) Specification, Implementation and Analysis*』
RFC 1583	『*OSPF version 2*』
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1886	『*DNS Extensions to Support IP version 6*』
RFC 1918	『*Address Allocation for Private Internets*』
RFC 1981	『*Path MTU Discovery for IP version 6*』
RFC 2080	『*RIPng for IPv6*』
RFC 2281	『*Cisco Hot Standby Router Protocol (HSRP)*』
RFC 2332	『*NBMA Next Hop Resolution Protocol (NHRP)*』
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2374	『*An Aggregatable Global Unicast Address Format*』

RFC	タイトル
RFC 2375	『*IPv6 Multicast Address Assignments*』
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2404	『*The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2407	『*The Internet Security Domain of Interpretation for ISAKMP*』
RFC 2408	『*Internet Security Association and Key Management Protocol*』
RFC 2409	『*Internet Key Exchange (IKE)*』
RFC 2427	『*Multiprotocol Interconnect over Frame Relay*』
RFC 2428	『*FTP Extensions for IPv6 and NATs*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2461	『*Neighbor Discovery for IP Version 6 (IPv6)*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 2463	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 2464	『*Transmission of IPv6 Packets over Ethernet*』
RFC 2467	『*Transmission of IPv6 Packets over FDDI*』
RFC 2472	『*IP Version 6 over PPP*』
RFC 2473	『*Generic Packet Tunneling in IPv6 Specification*』
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』

RFC	タイトル
RFC 2475	『*An Architecture for Differentiated Services Framework*』
RFC 2492	『*IPv6 over ATM*』
RFC 2545	『*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Specification*』
RFC 2597	『*Assured Forwarding PHB*』
RFC 2598	『*An Expedited Forwarding PHB*』
RFC 2640	『*Internet Protocol, Version 6 Specification*』
RFC 2684	『*Multiprotocol Encapsulation over ATM Adaptation Layer 5*』
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』
RFC 2710	『*Multicast Listener Discovery (MLD) for IPv6*』
RFC 2711	『*IPv6 Router Alert Option*』
RFC 2732	『*Format for Literal IPv6 Addresses in URLs*』
RFC 2765	『*Stateless IP/ICMP Translation Algorithm (SIIT)*』
RFC 2766	『*Network Address Translation-Protocol Translation (NAT-PT)*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2893	『*Transition Mechanisms for IPv6 Hosts and Routers*』
RFC 3056	『*Connection of IPv6 Domains via IPv4 Clouds*』
RFC 3068	『*An Anycast Prefix for 6to4 Relay Routers*』

RFC	タイトル
RFC 3095	『*RObust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP, ESP, and Uncompressed*』
RFC 3107	『*Carrying Label Information in BGP-4*』
RFC 3137	『*OSPF Stub Router Advertisement*』
RFC 3147	『*Generic Routing Encapsulation over CLNS*』
RFC 3152	『*Delegation of IP6.ARPA*』
RFC 3162	『*RADIUS and IPv6*』
RFC 3315	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3319	『*Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
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 3513	『*Internet Protocol Version 6 (IPv6) Addressing Architecture*』
RFC 3576	『*Change of Authorization*』
RFC 3587	『*IPv6 Global Unicast Address Format*』
RFC 3590	『*Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*』
RFC 3596	『*DNS Extensions to Support IP Version 6*』
RFC 3633	『*DHCP IPv6 Prefix Delegation*』

RFC	タイトル
RFC 3646	『*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3697	『*IPv6 Flow Label Specification*』
RFC 3736	『*Stateless DHCP Service for IPv6*』
RFC 3756	『*IPv6 Neighbor Discovery (ND) Trust Models and Threats*』
RFC 3759	『*RObust Header Compression (ROHC): Terminology and Channel Mapping Examples*』
RFC 3775	『*Mobility Support in IPv6*』
RFC 3810	『*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*』
RFC 3846	『*Mobile IPv4 Extension for Carrying Network Access Identifiers*』
RFC 3879	『*Deprecating Site Local Addresses*』
RFC 3898	『*Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』
RFC 3956	『*Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*』
RFC 3963	『*Network Mobility (NEMO) Basic Support Protocol*』
RFC 3971	『*SEcure Neighbor Discovery (SEND)*』
RFC 3972	『*Cryptographically Generated Addresses (CGA)*』
RFC 4007	『*IPv6 Scoped Address Architecture*』
RFC 4075	『*Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6*』

RFC	タイトル
RFC 4087	『*IP Tunnel MIB*』
RFC 4091	『*The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework*』
RFC 4092	『*Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)*』
RFC 4109	『*Algorithms for Internet Key Exchange version 1 (IKEv1)*』
RFC 4191	『*Default Router Preferences and More-Specific Routes*』
RFC 4193	『*Unique Local IPv6 Unicast Addresses*』
RFC 4214	『*Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*』
RFC 4242	『*Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 4282	『*The Network Access Identifier*』
RFC 4283	『*Mobile Node Identifier Option for Mobile IPv6*』
RFC 4285	『*Authentication Protocol for Mobile IPv6*』
RFC 4291	『*IP Version 6 Addressing Architecture*』
RFC 4292	『*IP Forwarding Table MIB*』
RFC 4293	『*Management Information Base for the Internet Protocol (IP)*』
RFC 4302	『*IP Authentication Header*』
RFC 4306	『*Internet Key Exchange (IKEv2) Protocol*』
RFC 4308	『*Cryptographic Suites for IPsec*』
RFC 4364	『*BGP MPLS/IP Virtual Private Networks (VPNs)*』

RFC	タイトル
RFC 4382	『*MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*』
RFC 4443	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 4552	『*Authentication/Confidentiality for OSPFv3*』
RFC 4594	『*Configuration Guidelines for DiffServ Service Classes*』
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification*』
RFC 4610	『*Anycast-RP Using Protocol Independent Multicast (PIM)*』
RFC 4649	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*』
RFC 4659	『*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*』
RFC 4724	『*Graceful Restart Mechanism for BGP*』
RFC 4798	『*Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*』
RFC 4818	『*RADIUS Delegated-IPv6-Prefix Attribute*』
RFC 4861	『*Neighbor Discovery for IP version 6 (IPv6)*』
RFC 4862	『*IPv6 Stateless Address Autoconfiguration*』
RFC 4884	『*Extended ICMP to Support Multi-Part Messages*』
RFC 4885	『*Network Mobility Support Terminology*』
RFC 4887	『*Network Mobility Home Network Models*』
RFC 5015	『*Bidirectional Protocol Independent Multicast (BIDIR-PIM)*』

RFC	タイトル
RFC 5059	『*Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*』
RFC 5072	『*IPv6 over PPP*』
RFC 5095	『*Deprecation of Type 0 Routing Headers in IPv6*』
RFC 5120	『*M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*』
RFC 5130	『*A Policy Control Mechanism in IS-IS Using Administrative Tags*』
RFC 5187	『*OSPFv3 Graceful Restart*』
RFC 5213	『*Proxy Mobile IPv6*』
RFC 5308	『*Routing IPv6 with IS-IS*』
RFC 5340	『*OSPF for IPv6*』
RFC 5460	『*DHCPv6 Bulk Leasequery*』
RFC 5643	『*Management Information Base for OSPFv3*』
RFC 5838	『*Support of Address Families in OSPFv3*』
RFC 5844	『*IPv4 Support for Proxy Mobile IPv6*』
RFC 5845	『*Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6*』
RFC 5846	『*Binding Revocation for IPv6 Mobility*』
RFC 5881	『*Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*』
RFC 5905	『*Network Time Protocol Version 4: Protocol and Algorithms Specification*』
RFC 5969	『*IPv6 Rapid Deployment on IPv4 Infrastructures (6RD) -- Protocol Specification*』
RFC 6105	『*IPv6 Router Advertisement Guard*』

RFC	タイトル
RFC 6620	『*FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses*』