



## **IPv6 ネットワーク管理コンフィギュレーションガイド、Cisco IOS XE Release 3S (Cisco ASR 1000)**

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/](http://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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2013 Cisco Systems, Inc. All rights reserved.



## 目次

### IPv6 を介した Telnet アクセス 1

機能情報の確認 1

IPv6 を介した Telnet アクセスの前提条件 1

IPv6 を介した Telnet アクセスに関する情報 2

IPv6 を介した Telnet アクセス 2

IPv6 を介した Telnet アクセスをイネーブルにする方法 2

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 2

IPv6 を介した Telnet アクセスの設定例 4

例：IPv6 デバイスへの Telnet アクセスのイネーブル化 4

IPv6 のソースガードおよびプレフィックスガードのその他の関連資料 5

IPv6 を介した Telnet アクセスの機能情報 6

### IPv6 の TFTP サポート 9

機能情報の確認 9

IPv6 の TFTP サポートに関する情報 9

TFTP IPv6 サポート 9

IPv6 での TFTP ファイルのダウンロード 10

その他の関連資料 10

TFTP に対する IPv6 サポートに関する機能情報 11

### IPv6 を介した SSH のサポート 13

機能情報の確認 13

IPv6 を介した SSH のサポートの前提条件 14

IPv6 を介した SSH のサポートに関する情報 14

IPv6 トランスポートを介した SSH 14

IPv6 を介した SSH のサポートをイネーブルにする方法 14

IPv6 デバイスでの SSH のイネーブル化 14

IPv6 を介した SSH のサポートの設定例 16

例：IPv6 デバイスでの SSH のイネーブル化 16

その他の関連資料	16
IPv6 を介した SSH のサポートに関する機能情報	17
<b>SNMP over IPv6</b>	<b>19</b>
機能情報の確認	19
SNMP over IPv6 に関する情報	20
IPv6 トランスポートを介した SNMP	20
SNMP over IPv6 の設定方法	20
IPv6 を介した SNMP 通知サーバの設定	20
SNMP over IPv6 の設定例	23
例：IPv6 を介した SNMP 通知サーバの設定	23
その他の関連資料	24
SNMP over IPv6 に関する機能情報	25
<b>IPv6 MIB</b>	<b>27</b>
機能情報の確認	27
IPv6 MIB について	27
Cisco IPv6 MIB	27
IPv6 でサポートされる MIB	28
その他の関連資料	28
IPv6 MIB に関する機能情報	30
<b>IPv6 組み込み管理コンポーネント</b>	<b>31</b>
機能情報の確認	31
IPv6 組み込み管理コンポーネントに関する情報	32
Syslog	32
設定ロガー	32
TCL	32
NETCONF	32
Service-Oriented Access Protocol (SOAP) メッセージフォーマット	32
IPv6 組み込み管理コンポーネントの設定方法	33
IPv6 を介した Syslog の設定	33
IPv6 組み込み管理コンポーネントの設定例	34
例：IPv6 を介した Syslog の設定	34
IPv6 組み込み管理コンポーネントに関するその他の関連資料	34
IPv6 組み込み管理コンポーネントに関する機能情報	35

<b>IPv6 CNS エージェント</b>	<b>39</b>
機能情報の確認	39
IPv6 CNS エージェントに関する情報	39
CNS エージェント	39
CNS 設定エージェント	40
CNS イベント エージェント	40
CNS EXEC エージェント	40
CNS イメージ エージェント	40
その他の関連資料	41
IPv6 CNS エージェントに関する機能情報	42
<b>IPv6 用 IP SLA</b>	<b>45</b>
機能情報の確認	45
IPv6 用 IP SLA に関する情報	45
シスコ IPv6 組み込み管理コンポーネント	45
IPv6 用 IP SLA	46
その他の関連資料	46
IPv6 用 IP SLA に関する機能情報	47
<b>IPv6 RFCs</b>	<b>49</b>





# 第 1 章

## IPv6 を介した Telnet アクセス

シスコ 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, 1 ページ](#)
- [IPv6 を介した Telnet アクセスの前提条件, 1 ページ](#)
- [IPv6 を介した Telnet アクセスに関する情報, 2 ページ](#)
- [IPv6 を介した Telnet アクセスをイネーブルにする方法, 2 ページ](#)
- [IPv6 を介した Telnet アクセスの設定例, 4 ページ](#)
- [IPv6 のソース ガードおよびプレフィックス ガードのその他の関連資料, 5 ページ](#)
- [IPv6 を介した Telnet アクセスの機能情報, 6 ページ](#)

### 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。最新の警告および機能情報については、『[Bug Search Tool](#)』および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](http://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

シスコ 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. **enable**
2. **configure terminal**
3. **ipv6 host** *name* [*port*] *ipv6-address*
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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ipv6 host</b> <i>name</i> [ <i>port</i> ] <i>ipv6-address</i>  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	<b>line</b> [ <i>aux</i>   <i>console</i>   <i>tty</i>   <i>vty</i> ] <i>line-number</i> [ <i>ending-line-number</i> ]  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	<b>password</b> <i>password</i>  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	<b>login</b> [ <i>local</i>   <i>tacacs</i> ]  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	<b>ipv6 access-class</b> <i>ipv6-access-list-name</i> [ <i>in</i>   <i>out</i> ]  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。  <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 8	<b>telnet</b> <i>host</i> [ <i>port</i> ] [ <i>keyword</i> ]  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。  <ul style="list-style-type: none"> <li>Telnet セッションは、デバイス名または IPv6 アドレスに対して確立できます。</li> </ul>

# 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、`show host` 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、`vtty` 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、`show users` 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        idle        00:00:00
 130 vty 0      idle        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 **show sessions** 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 のソース ガードおよびプレフィックス ガードのその他の関連資料

### 関連資料

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

## 標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『IPv6 RFCs』

## シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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](http://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。  <b>ipv6 access-class</b> 、 <b>ipv6 host</b> の各コマンドが導入または変更されました。





## 第 2 章

# IPv6 の TFTP サポート

TFTP は、IPv4 または IPv6 を介した UDP をトランスポートプロトコルとして使用し、IPv4 および IPv6 ネットワーク層を介して機能することができます。

- [機能情報の確認, 9 ページ](#)
- [IPv6 の TFTP サポートに関する情報, 9 ページ](#)
- [その他の関連資料, 10 ページ](#)
- [TFTP に対する IPv6 サポートに関する機能情報, 11 ページ](#)

## 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。最新の警告および機能情報については、『[Bug Search Tool](#)』および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](http://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 の TFTP サポートに関する情報

### TFTP IPv6 サポート

TFTP は可能な限り最小の機能セットを使用して、あるホストから別のホストにネットワークを介してファイルを転送するように設計されています。TFTP は、サーバとの間でファイルをコピーするようにクライアントが要求できるクライアント/サーバモデルを使用します。TFTP は、IPv4

または IPv6 を介した UDP をトランスポートプロトコルとして使用し、IPv4 および IPv6 ネットワーク層を介して機能することができます。

## IPv6 での TFTP ファイルのダウンロード

IPv6 は、**copy** コマンドを使用した TFTP によるファイルのダウンロードとアップロードをサポートします。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
```

## その他の関連資料

### 関連資料

関連項目	マニュアルタイトル
IPv6 のアドレス指定と接続	『 <a href="#">IPv6 Configuration Guide</a> 』
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
IPv6 コマンド	『 <a href="#">Cisco IOS IPv6 Command Reference</a> 』
Cisco IOS IPv6 の機能	『 <a href="#">Cisco IOS IPv6 Feature Mapping</a> 』

### 標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	<i>IPv6 の RFC</i>

## 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。  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## TFTP に対する IPv6 サポートに関する機能情報

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](http://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 に対する IPv6 サポートに関する機能情報

機能名	リリース	機能情報
TFTP IPv6 サポート	12.0(22)S 12.2(2)T 12.2(14)S 12.2(28)SB 15.1(1)SY Cisco IOS XE Release 2.1	TFTP に対する 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 3 章

# IPv6 を介した SSH のサポート

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、シスコデバイスは 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。

- [機能情報の確認, 13 ページ](#)
- [IPv6 を介した SSH のサポートの前提条件, 14 ページ](#)
- [IPv6 を介した SSH のサポートに関する情報, 14 ページ](#)
- [IPv6 を介した SSH のサポートをイネーブルにする方法, 14 ページ](#)
- [IPv6 を介した SSH のサポートの設定例, 16 ページ](#)
- [その他の関連資料, 16 ページ](#)
- [IPv6 を介した SSH のサポートに関する機能情報, 17 ページ](#)

## 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。最新の警告および機能情報については、『[Bug Search Tool](#)』および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](http://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 のサポートの前提条件

- IPsec (Data Encryption Standard (DES) または 3DES) 暗号化ソフトウェア 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 クライアントに対する 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。
- ホスト名およびホスト ドメインがデバイスに設定されている。
- 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。
- ローカルまたはリモート アクセスのユーザ認証のメカニズムがデバイスで設定されている。
- SSH クライアントを認証するために、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て SSH サーバに接続している。

IPv4 トランスポートを介した SSH 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 でサポートされてい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た SSH ではサポートされていません。

## IPv6 を介した SSH の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 サーバ機能により、SSH クライアントはシスコデバイスにセキュアな暗号化された接続を確立できます。また、SSH クライアント機能により、シスコデバイスは他のシスコデバイスや SSH サーバを実行するその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、シスコ 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 の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ていない場合、デフォルト値が使用されます。

## 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: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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip ssh [timeout seconds   authentication-retries integer]</b>  例 : Device(config)# IP ssh timeout 100 authentication-retries 2	デバイスに SSH 制御変数を設定します。
ステップ 4	<b>exit</b>  例 : Device(config)# exit	コンフィギュレーションモードを終了し、デバイスを特権 EXEC モードに戻します。
ステップ 5	<b>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]</b>  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 のサポートの設定例

### 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
```

## その他の関連資料

### 関連資料

関連項目	マニュアル タイトル
IPv6 のアドレス指定と接続	『 <a href="#">IPv6 Configuration Guide</a> 』
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
IPv6 コマンド	『 <a href="#">Cisco IOS IPv6 Command Reference</a> 』
Cisco IOS IPv6 の機能	『 <a href="#">Cisco IOS IPv6 Feature Mapping</a> 』

### 標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	<a href="#">IPv6 の RFC</a>

## 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。  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## IPv6 を介した SSH のサポートに関する機能情報

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](http://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 のサポートに関する機能情報

機能名	リリース	機能情報
IPv6 を介した SSH のサポート	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、シスコ 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。  <b>ip ssh、ssh</b> の各コマンドが導入または変更されました。



## 第 4 章

# SNMP over IPv6

IPv6 ホストが SNMP クエリーを実行したり、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簡易ネットワーク管理プロトコル (SNMP) を設定できます。

- [機能情報の確認, 19 ページ](#)
- [SNMP over IPv6 に関する情報, 20 ページ](#)
- [SNMP over IPv6 の設定方法, 20 ページ](#)
- [SNMP over IPv6 の設定例, 23 ページ](#)
- [その他の関連資料, 24 ページ](#)
- [SNMP over IPv6 に関する機能情報, 25 ページ](#)

## 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。最新の警告および機能情報については、『[Bug Search Tool](#)』および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](http://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

## 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、IPv6 ソフトウェアを実行しているデバイスから SNMP 通知を受信したりできるように、IPv6 トランスポートを介した簡易ネットワーク管理プロトコル (SNMP) 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。この機能は、データ暗号規格 (3DES) および Advanced Encryption Standard (AES) メッセージ暗号化を使用します。

## SNMP over IPv6 の設定方法

### 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、**no snmp-server community** コマンドを使用します。

**snmp-server host** 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いずれで送信されるようにするかを指定します。**snmp-server enable traps** 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. **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 nacl**] {*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**}}] [*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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b>   <b>rw</b> ] [ <b>ipv6 nacl</b> ] [ <i>access-list-number</i> ]  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	<b>snmp-server engineID remote</b> { <i>ipv4-ip-address</i>   <i>ipv6-address</i> } [ <b>udp-port</b> <i>udp-port-number</i> ] [ <b>vrf</b> <i>vrf-name</i> ] <i>engineid-string</i>  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	<p><b>snmp-server group</b> <i>group-name</i> {<b>v1</b>   <b>v2c</b>   <b>v3</b> {<b>auth</b>   <b>noauth</b>   <b>priv</b>}} [<b>context</b> <i>context-name</i>] [<b>read</b> <i>read-view</i>] [<b>write</b> <i>write-view</i>] [<b>notify</b> <i>notify-view</i>] [<b>access</b> [<b>ipv6</b> <i>named-access-list</i>] {<i>acl-number</i>   <i>acl-name</i>}]</p> <p>例 :</p> <pre>Device(config)# snmp-server group public v2c access ipv6 public2</pre>	<p>(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。</p>
ステップ 6	<p><b>snmp-server host</b> {<i>hostname</i>   <i>ip-address</i>} [<b>vrf</b> <i>vrf-name</i>] [<b>traps</b>   <b>informs</b>] [<b>version</b> {<b>1</b>   <b>2c</b>   <b>3</b> {<b>auth</b>   <b>noauth</b>   <b>priv</b>}}] [<b>community-string</b> <i>community-string</i>] [<b>udp-port</b> <i>port</i>] [<b>notification-type</b>]</p> <p>例 :</p> <pre>Device(config)# snmp-server host host1.com 2c vrf trap-vrf</pre>	<p>SNMP 通知動作の指定</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>
ステップ 7	<p><b>snmp-server user</b> <i>username</i> <i>group-name</i> [<b>remote</b> <i>host</i>] [<b>udp-port</b> <i>port</i>] {<b>v1</b>   <b>v2c</b>   <b>v3</b> [<b>encrypted</b>] [<b>auth</b> {<b>md5</b>   <b>sha</b>} <i>auth-password</i>]} [<b>access</b> [<b>ipv6</b> <i>nacl</i>] [<b>priv</b> {<b>des</b>   <b>3des</b>   <b>aes</b> {<b>128</b>   <b>192</b>   <b>256</b>} } <i>privpassword</i>] {<i>acl-number</i>   <i>acl-name</i>} ]</p> <p>例 :</p> <pre>Device(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6 public2</pre>	<p>(任意) 既存の SNMP グループに新しいユーザを設定します。</p> <p>(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で課された制限です。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。</p>
ステップ 8	<p><b>snmp-server enable traps</b> [<i>notification-type</i>] [<b>vrrp</b>]</p> <p>例 :</p> <pre>Device(config)# snmp-server enable traps bgp</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• <i>notification-type</i> 引数に値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されます。</li> <li>• デバイスで使用可能な通知を確認するには、<b>snmp-server enable traps ?</b> コマンドを使用します。</li> </ul>

# 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：指定されたビューに SNMP サーバグループを関連付ける

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 通知サーバを作成する

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
```

## その他の関連資料

### 関連資料

関連項目	マニュアル タイトル
IPv6 のアドレス指定と接続	『 <i>IPv6 Configuration Guide</i> 』
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
IPv6 コマンド	『 <i>Cisco IOS IPv6 Command Reference</i> 』
Cisco IOS IPv6 の機能	『 <a href="#">Cisco IOS IPv6 Feature Mapping</a> 』

### 標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	<i>IPv6 の RFC</i>

### 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 <a href="#">Cisco MIB Locator</a> を使用します。  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## SNMP over IPv6 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](http://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* に関する機能情報

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。  <b>snmp-server community、snmp-server enable traps、snmp-server engineID remote、snmp-server group、snmp-server host、snmp-server user</b> の各コマンドが導入または変更されました。

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 SNMPv3 - 3DES および AES 暗号化サポート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 5 章

# IPv6 MIB

このマニュアルでは、IPv6 に対して実装されている MIB について説明します。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, 27 ページ](#)
- [IPv6 MIB について, 27 ページ](#)
- [その他の関連資料, 28 ページ](#)
- [IPv6 MIB に関する機能情報, 30 ページ](#)

## 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。最新の警告および機能情報については、『[Bug Search Tool](#)』および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](http://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 について

### 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。次に示すように、IP-MIB と IP-FORWARD-MIB は、RFC 4293 および RFC 4292 規格に従っています。

- 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 と CISCO-IETF-IP-FORWARDING-MIB は、CISCO-IETF-IP-MIB と CISCO-IETF-IP-FORWARDING-MIB が適用されていたシスコ リリースから削除されました。CISCO-IETF-IP-MIB と CISCO-IETF-IP-FORWARDING-MIB の情報は、IP-MIB と IP-FORWARD-MIB に含まれています。

## 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。

## その他の関連資料

### 関連資料

関連項目	マニュアル タイトル
IPv6 のアドレス指定と接続	『 <i>IPv6 Configuration Guide</i> 』
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』

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 の機能	『Cisco IOS IPv6 Feature Mapping』

## 標準および RFC

標準/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。	<p>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。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## IPv6 MIB 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](http://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 に関する機能情報

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 規格に従って 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 6 章

# IPv6 組み込み管理コンポーネント

シスコ 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、syslog、設定ロガー、TCL、NETCONF および SOAP メッセージフォーマットの各組み込み管理コンポーネントについて説明します。

- [機能情報の確認, 31 ページ](#)
- [IPv6 組み込み管理コンポーネントに関する情報, 32 ページ](#)
- [IPv6 組み込み管理コンポーネントの設定方法, 33 ページ](#)
- [IPv6 組み込み管理コンポーネントの設定例, 34 ページ](#)
- [IPv6 組み込み管理コンポーネントに関するその他の関連資料, 34 ページ](#)
- [IPv6 組み込み管理コンポーネントに関する機能情報, 35 ページ](#)

## 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。最新の警告および機能情報については、『[Bug Search Tool](#)』および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](http://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 におけるシスコ 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 が Embedded Syslog Manager (ESM)、Embedded Event Manager (EEM)、音声自動応答装置 (IVR)、および tclsh パーサーモードなどの機能をサポートできるように、シスコソフトウェアでは Tool Command Language (TCL) が使用されます。TCL は開始ソケット (クライアント) とリスニングソケット (サーバ) 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。

## 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を交換することを目的としています。XML テクノロジーを使用して、さま

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

### IPv6 を介した Syslog の設定

#### 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

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  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	<b>configure terminal</b>  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	<b>logging host</b> <code>{{ip-address   hostname}   {ipv6 ipv6-address   hostname}}</code> [ <b>transport</b> <code>{udp [port port-number]   tcp [port port-number] [audit]}</code> ] [ <b>xml   filtered [stream stream-id]</b> ] [ <b>alarm [severity]</b> ]  例： Device(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF	システム メッセージおよびデバッグ出力をリモート ホストにロギングします。

## IPv6 組み込み管理コンポーネントの設定例

### 例：IPv6 を介した Syslog 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関連資料

#### 関連資料

関連項目	マニュアル タイトル
IPv6 のアドレス指定と接続	『 <a href="#">IPv6 Configuration Guide</a> 』
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
IPv6 コマンド	『 <a href="#">Cisco IOS IPv6 Command Reference</a> 』
Cisco IOS IPv6 の機能	『 <a href="#">Cisco IOS IPv6 Feature Mapping</a> 』

#### 標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	<i>IPv6 の RFC</i>

#### 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。  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## IPv6 組み込み管理コンポーネントに関する機能情報

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](http://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に関する機能情報

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 におけるシスコ 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。  <b>logging host</b> コマンドが導入されました。





## 第 7 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 でサポートされている CNS エージェントについて説明します。

- [機能情報の確認, 39 ページ](#)
- [IPv6 CNS エージェントに関する情報, 39 ページ](#)
- [その他の関連資料, 41 ページ](#)
- [IPv6 CNS エージェントに関する機能情報, 42 ページ](#)

## 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。最新の警告および機能情報については、『[Bug Search Tool](#)』および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](http://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、シスコ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せん。CNS設定エンジンを使用して、シスコ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、シスコ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、シスコデバイス上で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の動作の展開では、CNS イベントバスと HTTP サーバの両方を使用できます。

## その他の関連資料

### 関連資料

関連項目	マニュアルタイトル
IPv6 のアドレス指定と接続	『 <i>IPv6 Configuration Guide</i> 』
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
IPv6 コマンド	『 <i>Cisco IOS IPv6 Command Reference</i> 』
Cisco IOS IPv6 の機能	『 <a href="#">Cisco IOS IPv6 Feature Mapping</a> 』

### 標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	<i>IPv6 の RFC</i>

### MIB

MIB	MIB のリンク
	<p>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。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## IPv6 CNS エージェントに関する機能情報

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](http://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 エージェントに関する機能情報

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	<p>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シスコ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。</p> <p>追加または変更されたコマンドはありません。</p> <p>Cisco IOS XE Release 3.9S では、Cisco CSR 1000V のサポートが追加されました。</p>





## 第 8 章

# IPv6 用 IP SLA

Cisco IP サービス レベル契約 (SLA) は、シスコ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す。SLAを使用することで、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。

- [機能情報の確認, 45 ページ](#)
- [IPv6 用 IP SLA に関する情報, 45 ページ](#)
- [その他の関連資料, 46 ページ](#)
- [IPv6 用 IP SLA に関する機能情報, 47 ページ](#)

## 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。最新の警告および機能情報については、『[Bug Search Tool](#)』および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](http://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 用 IP SLA に関する情報

### シスコ IPv6 組み込み管理コンポーネント

シスコ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 のデュアルスタック 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 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 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 を使用するシスコデバイスと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 を使用するシスコデバイスと他のデバイス間で 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。
- 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 を使用するシスコ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。

## その他の関連資料

### 関連資料

関連項目	マニュアル タイトル
IPv6 のアドレス指定と接続	『 <a href="#">IPv6 Configuration Guide</a> 』
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
IPv6 コマンド	『 <a href="#">Cisco IOS IPv6 Command Reference</a> 』
Cisco IOS IPv6 の機能	『 <a href="#">Cisco IOS IPv6 Feature Mapping</a> 』

## 標準および RFC

標準/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。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## IPv6 用 IP SLA 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](http://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 用 IP SLA に関する機能情報

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 9 章

# IPv6 RFCs

### 標準および RFC

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

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

RFC	タイトル
RFC 3095	『 <i>RObust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP, ESP, and Uncompressed</i> 』
RFC 3107	『 <i>Carrying Label Information in BGP-4</i> 』
RFC 3137	『 <i>OSPF Stub Router Advertisement</i> 』
RFC 3147	『 <i>Generic Routing Encapsulation over CLNS</i> 』
RFC 3152	『 <i>Delegation of IP6.ARPA</i> 』
RFC 3162	『 <i>RADIUS and IPv6</i> 』
RFC 3315	『 <i>Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</i> 』
RFC 3319	『 <i>Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers</i> 』
RFC 3392	『 <i>Capabilities Advertisement with BGP-4</i> 』
RFC 3414	『 <i>User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)</i> 』
RFC 3484	『 <i>Default Address Selection for Internet Protocol version 6 (IPv6)</i> 』
RFC 3513	『 <i>Internet Protocol Version 6 (IPv6) Addressing Architecture</i> 』
RFC 3576	『 <i>Change of Authorization</i> 』
RFC 3587	『 <i>IPv6 Global Unicast Address Format</i> 』
RFC 3590	『 <i>Source Address Selection for the Multicast Listener Discovery (MLD) Protocol</i> 』
RFC 3596	『 <i>DNS Extensions to Support IP Version 6</i> 』
RFC 3633	『 <i>DHCP IPv6 Prefix Delegation</i> 』

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

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

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

