

サポート対象の Cisco IOS SNMP トラップとその設定方法

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[snmp-server host コマンド](#)

[構文の説明](#)

[デフォルト設定](#)

[コマンドモード](#)

[使用ガイドライン](#)

[インフォームの設定](#)

[例](#)

[snmp-server enable traps コマンド](#)

[構文の説明](#)

[デフォルト設定](#)

[コマンドモード](#)

[使用ガイドライン](#)

[関連情報](#)

[はじめに](#)

注: このドキュメントは Cisco IOS(R) ソフトウェア リリース 12.1(3)T を使用して作成されたものです。これより前の Cisco IOS ソフトウェア リリースを使用している場合は、すべてのオプションがサポートされていないことがあります。Cisco IOS ソフトウェア 12.1(3)T よりも後のバージョンを使用する場合は、追加の [notification-type] オプションがサポートされる場合があります。このドキュメントには、Cisco IOS ソフトウェアで現在サポートされている Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) トラップの Object Identifiers (OID; オブジェクト識別子) のリストが記載されています。

Cisco の標準的な IOS ソフトウェアが稼働する Cisco のデバイス (ルータ、Asynchronous Transfer Mode (ATM; 非同期転送モード) のスイッチ、リモート アクセス サーバ) では、多数の SNMP トラップを作成できます。

[前提条件](#)

[要件](#)

この文書の読者は、次のことについて理解する必要があります。

シスコのデバイスで送信方法が認識されているすべての SNMP トラップを送信する必要はありません。たとえば、64 本のダイヤルイン回線が接続されたリモート アクセス サーバですべてのトラップを使用可能にすると、ユーザのダイヤルインや接続終了のたびにトラップが発生します。この結果、大量のトラップが作成されます。Cisco IOS ソフトウェアには、トラップのグループを定義して、グループごとに使用可能または使用不可にする機能があります。Cisco IOS ソフトウェアが稼働するデバイスに SNMP トラップを設定するのに使用されるグローバル設定コマンドには、次の 2 つがあります。

- ```
snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}}
community-string [udp-port port] [notification-type]
```

SNMP 通知処理の受信者を指定するには、**snmp-server host** グローバル設定コマンドを発行します。指定のホストを削除するには、このコマンドの **no** 形式を発行します。

- ```
snmp-server enable traps [notification-type] [notification-option]
```

ルータに SNMP トラップを送信させるには、**snmp-server enable traps** グローバル設定コマンドを使用します。SNMP 通知を無効にする場合は、このコマンドの **no** 形式を使用します。

トラップのタイプは、両方のコマンドで指定できます。トラップの送信先となるネットワーク管理システムを定義するには **snmp-server host** コマンドを発行する必要があります。すべてのトラップを送信するわけではない場合は、トラップのタイプも指定する必要があります。その場合は、**snmp host** コマンドで使用したトラップ タイプごとに 1 つずつ、複数の **snmp-server enable traps** コマンドを発行します。

注: [notification-type] オプションの中には、このコマンドの両方でサポートされていないものがあります。たとえば、[notification-type] x25 および teletype (tty) は、**snmp-server enable trap** には使用されません。x25 および tty トラップはデフォルトで有効になっています。

1 つの例として、Cisco IOS ソフトウェアのデバイスに、設定、Border Gateway Protocol (BGP; ボーダーゲートウェイプロトコル)、および tty のトラップだけをネットワーク管理システム、10.10.10.10 に報告させるには、次のコマンドを使用します。

```
snmp-server host 10.10.10.10 public config bgp tty  
snmp-server enable traps config  
snmp-server enable traps bgp
```

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

snmp-server host コマンド

SNMP 通知処理の受信者を指定するには、`snmp-server host` グローバル設定コマンドを発行します。指定のホストを削除するには、このコマンドの `no` 形式を発行します。

```
snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port] [notification-type] no snmp-server host host [traps | informs]
```

構文の説明

host-addr	ホスト (ターゲットの受信者) の名前またはインターネット アドレス。
traps	(オプション) このホストに SNMP トラップを送信します。これはデフォルトです。
informs	(オプション) このホストに SNMP インフォームを送信します。
version	<p>(オプション) トラップの送信に使用する SNMP バージョン。バージョン 3 は、<code>priv</code> キーワードによってパケットを暗号化できるため、最もセキュアなモデルです。バージョンのキーワードを使用する場合は、次のいずれか 1 つのオプションを指定する必要があります。</p> <ul style="list-style-type: none"> • 1 : SNMPv1 このオプションは、<code>inform</code> とともに使用できません。 • 2c : SNMPv2C • 3 : SNMPv3 バージョン 3 のキーワードの後に、次の 3 つのオプション キーワードを付けることができます。<code>auth</code> : (オプション) Message Digest 5 (MD5) と Secure Hash Algorithm (SHA) パケット認証を使用可能にします。<code>noauth</code> : (デフォルト) <code>noAuthNoPriv</code> セキュリティレベル。これは次の場合にデフォルトとなります : <code>[auth noauth priv]</code> キーワードを選択していない場合 <code>priv</code> : (オプション) Data Encryption Standard (DES; データ暗号規格) パケット認証 (別名「プライバシー」) を使用可能にします。
community-string	通知処理で送られる、パスワードに似たコミュニティ スtring。この String は、 <code>snmp-server host</code> コマンドだけを使っても設定できますが、 <code>snmp-server host</code> コマンドを使用する前に、 <code>snmp-server community</code> コマンドで String を定義することを推奨します。
udp-port port	使用するホストの User Datagram Protocol (UDP) ポート。デフォルトは 162 です。
notification-	(オプション) ホストに送信される通知のタイプ。タイプを指定しない場合、すべての通知が

type

送信されます。通知タイプには、次のキーワードを1つ以上指定できます。

- **aaa-server** : AAA 通知を送信します。
- **bgp** : ボーダー ゲートウェイ プロトコル (BGP) 状態変化通知を送信します。
- **bstun** : Block Serial Tunneling (BSTUN; ブロック シリアル トンネリング) 通知を送信します。
- **calltracker** : CallTracker 通知を送信します。
- **config** : コンフィギュレーション通知を送信します。
- **dls** : Data-Link Switching (DLSw; データ リンク スイッチング) 通知を送信します。
- **ds0-busyout** : ds0-busyout 通知を送信します。
- **ds1-loopback** : ds1-loopback 通知を送信します。
- **dspu** : DSPU (downstream physical unit; 下流物理ユニット) 通知を送信します。
- **dsp** : digital signal processing (DSP; デジタル信号処理) 通知を送信します。
- **entity** : Management Information Base (MIB; 管理情報ベース) 変更通知を送信します。
- **envmon** : 環境のしきい値が設定値を超えたときに、Cisco Enterprise に固有の環境 モニタリング通知を送信します。
- **frame-relay** : フレームリレー通知を送信します。
- **hsrp** : Hot Standby Router Protocol (HSRP) 通知を送信します。
- **isdn** : ISDN 通知を送信します。
- **msdp** : Multicast Source Discovery Protocol (MSDP) 通知を送信します。
- **llc2** : Logical Link Control, type 2 (LLC2; 論理リンク制御タイプ 2) 通知を送信します。
- **repeater** : 標準リピータ (ハブ) 通知を送信します。
- **rsrb** : Remote Source-Route Bridging (RSRB; リモート ソースルートブリッジング) 通知を送信します。
- **rsvp** : Resource Reservation Protocol (RSVP; リソース予約プロトコル) 通知を送信します。
- **rtr** : SA エージェント (RTR) 通知を送信します。

- **sdhc** : Synchronous Data Link Control (SDLC) 通知を送信します。
- **snmp** : SNMP 通知を RFC 1157 の定義に従って送信します。
- **stun** : Serial Tunnel (STUN; シリアルトンネル) 通知を送信します。
- **syslog** : エラーメッセージ通知を送信します (Cisco Syslog MIB)。 **logging history level** コマンドを使って、送信されるメッセージのレベルを指定します。
- **ttty** : Transmission Control Protocol (TCP; 伝送制御プロトコル) 接続が閉じた際に、Cisco Enterprise に固有の通知を送信します。
- **voice** : 音声通知を送信します。
- **x25** : X.25 イベント通知を送信します。
- **xgcp** : External Media Gateway Control Protocol (XGCP; 外部メディアゲートウェイコントロールプロトコル) 通知を送信します。

デフォルト設定

デフォルトでは、**snmp-server host** コマンドは無効になっています。通知は送信されません。

キーワードを付けずにこのコマンドを入力すると、デフォルトでは全トラップタイプがホストに送信されます。

このホストには、インフォームは送信されません。バージョンキーワードがない場合、デフォルトはバージョン 1 になります。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップは無効になりますが、インフォームは無効になりません。インフォームを送信しないようにするには、**no snmp-server host informs** コマンドを発行します。

注: **snmp-server community** コマンドで *community-string* を定義せずにこのコマンドを使用すると、**snmp-server community** コマンドのデフォルト形式が自動的に設定に挿入されます。**snmp-server community** の自動設定時に使われるパスワード (*community-string*) は、**snmp-server host** コマンドに指定されたパスワードと同じです。これは、Cisco IOS ソフトウェア リリース 12.0(3) 以降のデフォルト動作です。

コマンドモード

グローバル設定 : コマンド履歴

Cisco IOS ソフトウェアリリース	変更箇所
10.0	コマンドが導入されました。
12.0(3)T	次のキーワードが追加されました。

- | |
|---|
| <ul style="list-style-type: none">• version 3 [auth noauth priv]• hsrp |
|---|

使用ガイドライン

SNMP 通知は、トラップまたはインフォーム要求として送信できます。このデバイスでトラップが受信されても受信側は確認応答を送信しないので、トラップの信頼性は高くありません。送信側は、トラップが受信されたかどうかを判断できません。しかし、SNMP エンティティはインフォーム要求を受信すると、SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット) によって要求に応答します。送信側が応答をまったく受け取っていないければ、インフォーム要求を再送信できます。このため、インフォームは、目的の宛先に到達できる可能性が高くなります。

ただし、インフォームは、エージェントやネットワークでより多くのリソースを消費します。トラップは、送信されると同時に破棄されますが、インフォーム要求の場合は、応答が受信されるか、要求時間がタイムアウトになるまでメモリ内に残る必要があります。トラップの送信回数は 1 回だけですが、インフォームは数回、繰り返し送信される場合があります。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。

`snmp-server host` コマンドを入力しなければ、通知はまったく送信されません。ルータが SNMP 通知を送信するように設定するには、少なくとも 1 回は `snmp-server host` コマンドを入力する必要があります。キーワードを付けずにコマンドを入力すると、すべてのトラップタイプがホストで有効になります。

複数のホストを有効にするには、各ホストに対して `snmp-server host` コマンドを個別に発行する必要があります。各ホスト宛てのコマンドに、複数の通知タイプを指定することもできます。

同じホストや通知タイプ (トラップやインフォーム) に複数の `snmp-server host` コマンドを発行すると、コマンドを発行するたびに前のコマンドに上書きされます。最後の `snmp-server host` コマンドだけが有効です。たとえば、あるホストに `snmp-server host inform` コマンドを入力してから、同じホストに別の `snmp-server host inform` コマンドを入力したとします。その場合は、2 番目のコマンドが最初のコマンドと入れ替わります。

`snmp-server host` コマンドは、`snmp-server enable` コマンドと組み合わせて使用します。`snmp-server enable` コマンドを発行して、グローバルに送信する SNMP 通知を指定します。最も多くの通知を受信するホストについては、少なくとも 1 つの `snmp-server enable` コマンドと `snmp-server host` コマンドを有効にする必要があります。

しかし、`snmp-server enable` コマンドで制御できない通知タイプもあります。たとえば、一部の通知タイプは常に有効です。また、`snmp-server enable` 以外のコマンドで使用可能になる通知タイプもあります。たとえば、linkUpDown 通知は、`snmp trap link-status` コマンドにより制御されます。これらの通知タイプには、`snmp-server enable` コマンドを発行する必要はありません。

使用可能な通知タイプのオプションは、ルータのタイプおよびルータ上でサポートされる Cisco IOS ソフトウェア機能により異なります。たとえば、`envmon` 通知タイプは、環境モニタリングがシステムの一部となっている場合に限り使用可能です。

インフォームの設定

インフォームの送信を可能にするには、次の手順を実行します。

1. リモート エンジンの ID を設定する。
2. リモート ユーザを設定する。
3. リモート装置でグループを設定する。
4. リモート装置でトラップを使用可能にする。
5. SNMP マネージャを使用可能にする。

例

トラップに一意の SNMP コミュニティ スtring を設定する場合に、この String による SNMP ポーリング アクセスを防止するには、設定に access-list を含める必要があります。次の例では、コミュニティ String 名に「comaccess」を、アクセス リストには 10 をそれぞれ指定しています。

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

次の例では、名前 myhost.cisco.com で指定されたホストに SNMP トラップを送信します。コミュニティ String を comaccess と定義しています。

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、SNMP および Cisco Enterprise に固有の環境モニタリングのトラップをアドレス 172.30.2.160 に送信しています。

```
snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

次の例では、ルータが、コミュニティ String の public を使用して、ホストの myhost.cisco.com にすべてのトラップを送信できるようにします。

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

次の例では、どのホストにもトラップがまったく送信されません。BGP トラップはすべてのホストで送信可能にできますが、ISDN トラップだけは 1 つのホストにだけ送信できます。

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

次の例では、ルータが、コミュニティ String の public を使用して、ホストの myhost.cisco.com にすべてのインフォーム要求を送信できるようにします。

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version
```

次の例では、名前 myhost.cisco.com で指定されたホストに HSRP SNMPv2c トラップを送信します。コミュニティストリングを、public と定義しています。

```
snmp-server enable traps
snmp-server host myhost.cisco.com traps version 2c public hsrp
```

snmp-server enable traps

ルータに SNMP トラップを送信させるには、**snmp-server enable traps** グローバル設定コマンドを発行します。SNMP 通知を送信しないようにするには、このコマンドの **n no** 形式を使用します。

```
snmp-server enable traps [notification-type] [notification-option]
```

```
no snmp-server enable traps [notification-type] [notification-option]
```

構文の説明

<i>notification-type</i>	<p>(オプション) 使用可能な通知タイプ。通知タイプを指定しない場合、envmon および repeater などの通知を含めて、すべての通知が送信されます。通知タイプは、次のキーワードのいずれかになります。</p> <ul style="list-style-type: none">• aaa-server : AAA サーバ通知を送信します。このキーワードは、Cisco IOS ソフトウェア リリース 12.1(3)T 以降、Cisco AS5300 および AS5800 のプラットフォームだけに追加されています。これは CISCO-AAA-SERVER-MIB によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange• bgp : ボーダー ゲートウェイ プロトコル (BGP) 状態変化通知を送信します。これは BGP4-MIB によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.2.1.15.7 1 bgpEstablished 2 bgpBackwardTransition• calltracker : 新しいアクティブ コール エントリが cctActiveTable に作成されるか、新しい履歴 コール エントリが cctHistoryTable に作成されるたびに、通知を送信します。このキーワードは、CISCO-CALL-TRACKER-MIB によるものであり、通知は次のとおりです。 enterprise
--------------------------	--

1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification
2 cctCallTerminateNotification

- **config** : コンフィギュレーション通知を送信します。これは [CISCO-CONFIG-MAN-MIB](#) によるものであり、通知は次のとおりです。

enterprise 1.3.6.1.4.1.9.9.43.2 1
ciscoConfigManEvent

- **dial** : 正常に接続されたコールをクリアするか、あるいは接続に失敗したコールが最終的に接続失敗と判断されるか、またはコール設定メッセージが送受信されるたびに、通知を送信します。これは [DIAL-CONTROL-MIB](#) によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation
2 dialCtlPeerCallSetup

- **dls** : DLSw エージェントから通知を送信します。キーワード **dls** を使用すると、*notification-option* の値を指定できます。これは [CISCO-DLSW-MIB](#) によるものであり、通知は次のとおりです。 enterprise

1.3.6.1.4.1.9.10.9.1.7 1
ciscoDlsTrapTConnPartnerReject 2
ciscoDlsTrapTConnProtViolation 3
ciscoDlsTrapTConnUp 4
ciscoDlsTrapTConnDown 5
ciscoDlsTrapCircuitUp 6
ciscoDlsTrapCircuitDown

- **ds0-busyout** : DS0 インターフェイスの busyout の状態が変わるたびに、通知を送信します。このキーワードは、Cisco IOS ソフトウェア リリース 12.1(3)T 以降で、Cisco AS5300 プラットフォームに限定して追加されています。これは [CISCO-POP-MGMT-MIB](#) によるものであり、通知は次のとおりです。 enterprise

1.3.6.1.4.1.9.10.19.2 1
cpmDS0BusyoutNotification

- **ds1-loopback** : DS1 インターフェイスがループバック モードになるたびに通知を送信します。このキーワードは、Cisco IOS ソフトウェア リリース 12.1(3)T 以降で、Cisco AS5300 プラットフォームに限定して追加されています。これは [CISCO-POP-MGMT-MIB](#) によるものであり、通知は次のとおりです。 enterprise

1.3.6.1.4.1.9.10.19.2 2
cpmDS1LoopbackNotification

- **dspu** : physical unit (PU; 物理ユニット) または logical unit (LU; 論理ユニット) の稼働状態

の変更、または起動の失敗が検出されたときに通知を送信します。これは [CISCO-DSPU-MIB](#) によるものであり、通知は次のとおりです。

enterprise 1.3.6.1.4.1.9.9.24.1.4.4

1newdspuPuStateChangeTrap 2

newdspuPuActivationFailureTrap enterprise

1.3.6.1.4.1.9.9.24.1.5.3 1

newdspuLuStateChangeTrap 2

dspuLuActivationFailureTrap

- **dsp** : DSP カードがアップまたはダウンするたびに通知を送信します。これは [CISCO-DSP-MGMT-MIB](#) によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.4.1.9.9.86.2 1 cdspMIBCardStateNotification
- **entity** : エンティティ MIB 変更通知を送信します。これは [ENTITY-MIB](#) によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.2.1.47.2 1 entConfigChange
- **envmon** : 環境のしきい値が設定値を超えたときに、Cisco Enterprise に固有の環境モニタリング通知を送信します。キーワード **envmon** が使用されている場合は、*notification-option* の値を設定できます。これは [CISCO-ENVMON-MIB](#) によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonShutdownNotification 2 ciscoEnvMonVoltageNotification 3 ciscoEnvMonTemperatureNotification 4 ciscoEnvMonFanNotification 5 ciscoEnvMonRedundantSupplyNotification
- **frame-relay** : フレームリレー通知を送信します。これは [RFC1315-MIB](#) によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.2.1.10.32 1 frDLCIStatusChange
- **hsrp** : Hot Standby Router Protocol (HSRP) 通知を送信します。この機能は Cisco IOS ソフトウェア リリース 12.0(3)T からサポートされています。これは [CISCO-HSRP-MIB](#) によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange
- **isdn** : ISDN 通知を送信します。キーワード **isdn** が使用されている場合は、*notification-option* の値を設定できます。これは [CISCO-ISDN-MIB](#) によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.4.1.9.9.26.2 1 demandNbrCallInformation 2

demandNbrCallDetails 3
demandNbrLayer2Change [supported since
Cisco IOS Software Release 12.1(1)T] 4
demandNbrCNANotification [supported since
Cisco IOS Software Release 12.1(5)T] これは
[CISCO-ISDNU-IF-MIB](#) によるものであり、通知
は次のとおりです。 enterprise
1.3.6.1.4.1.9.9.18.2 1
ciulfLoopStatusNotification

- **msdp** : Multicast Source Discovery
Protocol (MSDP) 通知を送信します。 これは
[MSDP-MIB](#) によるものであり、通知は次のと
おりです。 enterprise 1.3.6.1.3.92.1.1.7 1
msdpEstablished 2 msdpBackwardTransition
- **repeater** : イーサネットのハブ **repeater** 通知を
送信します。 キーワード **repeater** が選択され
ている場合は、*notification-option* の値を指定で
きます。 これは [CISCO-REPEATER-MIB](#) によ
るものであり、通知は次のとおりです。
enterprise 1.3.6.1.4.1.9.9.22.3 1
ciscoRptrIllegalSrcAddrTrap
- **rsvp** : Resource Reservation Protocol (RSVP;
リソース予約プロトコル) 通知を送信します。
この機能は Cisco IOS ソフトウェア リリース
12.0(2)T からサポートされています。 これは
[RSVP-MIB](#) によるものであり、通知は次のと
おりです。 enterprise 1.3.6.1.3.71.2 1 newFlow 2
lostFlow
- **rtr** : SA エージェント RTR (RTR) 通知を送信
します。 これは [CISCO-RTTMON-MIB](#) による
ものであり、通知は次のとおりです。
enterprise 1.3.6.1.4.1.9.9.42.2 1
rttMonConnectionChangeNotification 2
rttMonTimeoutNotification 3
rttMonThresholdNotification 4
rttMonVerifyErrorNotification
- **snmp** : SNMP 通知を送信します。 キーワード
snmp が使用されている場合は、*notification-
option* の値を指定できます。 これは [CISCO-
GENERAL-TRAPS](#) によるものであり、通知は
次のとおりです。 enterprise 1.3.6.1.2.1.11 0
coldStart 2 linkDown 3 linkUp 4
authenticationFailure 5 egpNeighborLoss
enterprise 1.3.6.1.4.1.9 0 reload 注: このトラッ
プは、通知タイプの「tty」により制御されます
。注: 1 tcpConnectionClose
- **syslog** : エラー メッセージ通知を送信します

	<p>(Cisco Syslog MIB)。 logging history level コマンドを使って、送信されるメッセージのレベルを指定します。これは CISCO-SYSLOG-MIB によるものであり、通知は次のとおりです。</p> <p>enterprise 1.3.6.1.4.1.9.9.41.2 1 clogMessageGenerated</p> <ul style="list-style-type: none"> • voice : 音声の品質がよくないことを示す通知を送信します。これは CISCO-VOICE-DIAL-CONTROL-MIBSMI によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVNotification • xgcp : External Media Gateway Control Protocol (XGCP; 外部メディア ゲートウェイ コントロール プロトコル) 通知を送信します。これは XGCP-MIB によるものであり、通知は次のとおりです。 enterprise 1.3.6.1.3.90.2 1 xgcpUpDownNotification
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">notification - option</p>	<p>(オプション)</p> <ul style="list-style-type: none"> • dls [circuit tconn] : dls キーワードを使用すると、特定の通知タイプを使用可能または使用禁止と指定できます。キーワードを何も指定しない場合、すべての DLSw 通知タイプが使用可能になります。オプションとして、次のキーワードを 1 つ以上使用できます。 circuit : DLSw 回線トラップを使用可能にします。 tconn : DLSw ピア転送接続トラップを使用可能にします。 • envmon [voltage shutdown supply fan temperature] : envmon キーワードを使用すると、特定の環境通知タイプを使用可能にしたり、環境モニタリング システムから全通知タイプを受け入れることができます。オプションを指定しない場合、すべての環境通知が使用可能になります。オプションとして、次のキーワードを 1 つ以上使用できます。 voltage、shutdown、supply、fan、および temperature。 • isdn [call-information isdn u-interface chan-not-avail layer2] : isdn キーワードを使用すると、call-information キーワードを指定して、ISDN MIB サブシステムに SNMP ISDN コール情報通知を使用可能にしたり、isdn u-interface キーワードを指定して ISDN U インターフェースの MIB サブシステムに SNMP ISDN U インターフェイス通知を使用可能にすることができます。 • repeater [health reset] : repeater キーワードを使用すると、リピータのオプションを指定できます。タイプを指定しない場合、すべての

リピータ通知が使用可能になります。オプションとして、次のキーワードを1つ以上使用できます。ヘルス--Internet Engineering Task Force (IETF; インターネット技術特別調査委員会)のリピータ ハブ MIB (RFC 1516)のヘルス通知を使用可能にします。リセット--IETFリピータ ハブ MIB (RFC 1516)リセット通知を使用可能にします。health : Internet Engineering Task Force (IETF; インターネット技術特別調査委員会)リピータ ハブ MIB (RFC 1516)の状態通知を使用可能にします。reset : IETFリピータ ハブ MIB (RFC 1516)リセット通知を使用可能にします。

- `snmp [authentication | linkup | linkdown | coldstart]` keywords `linkup | linkdown | coldstart` は Cisco IOS ソフトウェア リリース 12.1(3)T から追加されています。snmp キーワードを使用すると、特定の通知タイプを使用可能または使用禁止と指定できます。キーワードを指定しない場合、すべての SNMP 通知タイプが使用可能になります (または no 形式を使用すれば使用禁止となります)。次の通知タイプが使用できます。authentication : SNMP 認証失敗通知の配布を制御します。authenticationFailure(4)トラップは、送信側のプロトコル エンティティが、正式に認証されていないプロトコル メッセージの受信者であることを意味します。linkup : SNMP リンクアップ通知の送信を制御します。linkUp(3)トラップは、エージェントの設定に示されている通信リンクの1つがアップしたことが、送信側のプロトコル エンティティで認識されたことを示します。linkdown : SNMP リンクダウン通知の送信方法を制御します。linkDown(2)トラップは、エージェントの設定に示されている通信リンクの1つに障害が発生したことが、送信側のプロトコル エンティティで認識されたことを示します。coldstart : SNMP coldstart 通知の送信を制御します。coldStart(0)トラップは、送信側のプロトコル エンティティ自体が再初期化されるので、エージェントやプロトコル エンティティの実装が変わる可能性があることを示します。

デフォルト設定

SNMP 通知は使用禁止です。

notification-type キーワードを指定せずにこのコマンドを入力すると、デフォルト設定により、このコマンドで制御できる全通知タイプが使用可能になります。

コマンドモード

グローバル設定：コマンド履歴

Cisco IOS ソフトウェア リリース	変更箇所
11.1	このコマンドが導入されました。
12.0(2)T	キーワードの rsvp が追加されました。
12.0(3)T	キーワードの hsrp が追加されました。
12.1(3)T	次のキーワードが、このコマンドの snmp-server enable traps snmp 形式に追加されています。 <ul style="list-style-type: none">• linkup• linkdown• coldstart 次の通知タイプのキーワードは、Cisco AS5300 プラットフォームに限定して追加されています。 <ul style="list-style-type: none">• ds0-busyout• isdn chan-not-avail• modem-health• ds1-loopback 次の通知タイプのキーワードは、Cisco AS5300 および AS5800 プラットフォームに限定して追加されています。 <ul style="list-style-type: none">• aaa-server

使用ガイドライン

このコマンドの **snmp-server enable traps snmp [linkup] [linkdown]** 形式が、**snmp trap link-status interface** 設定コマンドを置き換えます。

snmp-server enable traps コマンドの **no** 形式が役立つのは、ネットワーク上で不必要な大量のノイズを生成する通知を使用禁止にする場合です。

SNMP 通知は、トラップまたはインフォーム要求として送信できます。このコマンドは、特定の通知タイプのトラップおよびインフォーム要求の両方を使用可能にします。

snmp-server enable traps コマンドを入力しないと、このコマンドで制御する通知はまったく送信されません。ルータがこれらの SNMP 通知を送信するように設定するには、少なくとも 1 回は **snmp-server enable traps** コマンドを入力する必要があります。キーワードを指定せずにコマンドを入力すると、すべてのトラップタイプが使用可能になります。キーワードを指定してコマンドを入力した場合は、そのキーワードに関連した通知タイプだけが使用可能になります。複数の通知タイプを使用可能にするには、通知タイプと通知オプションごとに **snmp-server enable traps** コマンドを個別に発行する必要があります。

snmp-server enable traps コマンドは、**snmp-server host** コマンドと組み合わせて使用します。**snmp-server host** コマンドを発行すると、どのホストが SNMP 通知を受信するのかを指定できま

す。通知を送信するには、少なくとも 1 回は `snmp-server host` コマンドを設定する必要があります。

`snmp-server enable traps` コマンドで制御する通知を受信するホストに対しては、このコマンドと `snmp-server host` コマンドの両方を使用可能にする必要があります。通知タイプが `snmp-server enable traps` コマンドの制御対象外である場合は、適切な `snmp-server host` コマンドだけを使用可能にする必要があります。

`snmp-server enable traps` コマンドで使用する通知タイプにはすべて、対応する MIB オブジェクトが設定されており、そのオブジェクトによって通知タイプは使用可能または使用禁止となります (たとえば、HSRP トラップは、HSRP MIB によって、リピータトラップの場合は、Repeater Hub MIB によってそれぞれ定義されます)。ただし、`snmp-server host` コマンドに使用可能なすべての通知タイプに `notificationEnable` MIB オブジェクトが設定されているとは限らないため、`snmp-server enable` コマンドによって制御できない通知タイプがあります。

関連情報

- [ATM SNMP トラップと OAM 拡張](#)
- [テクニカルサポート - Cisco Systems](#)