



# プラットフォームイベントフィルタの設定

この章の内容は、次のとおりです。

- [プラットフォーム イベント フィルタ, 1 ページ](#)
- [プラットフォーム イベント アラートのイネーブル化, 2 ページ](#)
- [プラットフォーム イベント アラートのディセーブル化, 2 ページ](#)
- [プラットフォーム イベント フィルタの設定, 3 ページ](#)
- [SNMP トラップ設定の指定, 5 ページ](#)
- [テスト SNMP トラップ メッセージの送信, 6 ページ](#)
- [プラットフォーム イベント トラップの解釈, 7 ページ](#)

## プラットフォーム イベント フィルタ

プラットフォーム イベント フィルタ (PEF) は、ハードウェア関連の重要なイベントが発生したときに、アクションをトリガーしたりアラートを生成したりできます。PEF ごとに、プラットフォーム イベントが発生したときに実行するアクション (またはアクションを実行しないこと) を選択できます。また、プラットフォーム イベントが発生したときにアラートを生成して送信することもできます。アラートは SNMP トラップとして送信されるので、アラートを送信するには、先に SNMP トラップの宛先を設定する必要があります。

プラットフォーム イベント アラートの生成はグローバルにイネーブルまたはディセーブルにできます。ディセーブルにすると、PEF がアラートを送信するように設定されていても、アラートは送信されません。

## プラットフォーム イベント アラートのイネーブル化

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope fault</b>	障害コマンド モードを開始します。
ステップ 2	Server /fault # <b>set platform-event-enabled yes</b>	プラットフォーム イベント アラートをイネーブルにします。
ステップ 3	Server /fault # <b>commit</b>	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /fault # <b>show [detail]</b>	(任意) プラットフォーム イベント アラートの設定を表示します。

次に、プラットフォーム イベント アラートをイネーブルにする例を示します。

```
Server# scope fault
Server /fault # set platform-event-enabled yes
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
-----
public                               yes
Server /fault #
```

## プラットフォーム イベント アラートのディセーブル化

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope fault</b>	障害コマンド モードを開始します。
ステップ 2	Server /fault # <b>set platform-event-enabled no</b>	プラットフォーム イベント アラートをディセーブルにします。
ステップ 3	Server /fault # <b>commit</b>	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /fault # <b>show [detail]</b>	(任意) プラットフォーム イベント アラートの設定を表示します。

次に、プラットフォーム イベント アラートをディセーブルにする例を示します。

```
Server# scope fault
Server /fault # set platform-event-enabled no
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
-----
public                no
Server /fault #
```

## プラットフォーム イベント フィルタの設定

次のプラットフォーム イベント フィルタに対する処理とアラートを設定できます。

ID	プラットフォーム イベント フィルタ
1	温度緊急アサート フィルタ
2	温度警告アサート フィルタ
3	電圧緊急アサート フィルタ
4	電流アサート フィルタ
5	ファン緊急アサート フィルタ
6	プロセッサ アサート フィルタ
7	電源緊急アサート フィルタ
8	電源警告アサート フィルタ
9	電源冗長性損失フィルタ
10	ディスクリット電源アサート フィルタ
11	メモリ アサート フィルタ
12	ドライブ スロット アサート フィルタ

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope fault</b>	障害コマンド モードを開始します。
ステップ 2	Server /fault # <b>scope pef id</b>	指定したイベントに対してプラットフォーム イベントフィルタ コマンド モードを開始します。 イベント ID 番号に対応するプラットフォーム イベントフィルタの表を参照してください。
ステップ 3	Server /fault/pef # <b>set action {none   reboot   power-cycle   power-off}</b>	このイベントが発生した場合に必要なシステムの処理を選択します。 次のいずれかの処理を選択できます。 <ul style="list-style-type: none"> <li>• <b>none</b> : システム アクションは実行されません。</li> <li>• <b>reboot</b> : サーバがリブートされます。</li> <li>• <b>power-cycle</b> : サーバの電源が再投入されます。</li> <li>• <b>power-off</b> : サーバの電源がオフになります。</li> </ul>
ステップ 4	Server /fault/pef # <b>set send-alert {yes   no}</b>	このイベントに対するプラットフォーム イベントアラートの送信をイネーブルまたはディセーブルにします。 (注) 送信するアラートについて、フィルタトラップを正しく設定し、プラットフォーム イベントアラートをイネーブルにする必要があります。
ステップ 5	Server /fault/pef # <b>commit</b>	トランザクションをシステムの設定にコミットします。

次に、イベントに対するプラットフォーム イベント アラートを設定します。

```
Server# scope fault
Server /fault # scope pef 13
Server /fault/pef # set action reboot
Server /fault/pef *# set send-alert yes
Server /fault/pef *# commit
Server /fault/pef # show
Platform Event Filter Event Action Send Alert
-----
13 Memory Assert Filter reboot yes

Server /fault/pef #
```

## 次の作業

PEF を設定してアラートを送信する場合は、次のタスクを完了させます。

- プラットフォーム イベント アラートのイネーブル化

- SNMP トラップ設定の実行

## SNMP トラップ設定の指定

### はじめる前に

- このタスクを実行するには、admin 権限を持ってログインする必要があります。
- トラップの設定を実行する前に、SNMP をイネーブルにして保存する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope snmp</b>	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # <b>set trap-community-str</b> <i>string</i>	トラップ情報の送信先となる SNMP コミュニティの名前を入力します。
ステップ 3	Server /snmp # <b>set trap-ver</b> {1   2   3}	必要なトラップ メッセージの SNMP バージョンを指定します。  (注) SNMPv3 トラップは SNMPv3 ユーザおよびキー値が正しく設定されている場所だけに配信されます。
ステップ 4	Server /snmp # <b>set inform-type</b> {trap   inform}	SNMP 通知メッセージを単純なトラップとして送信するのか、レシーバによる確認応答が必要なインフォーム要求として送信するかを指定します。
ステップ 5	Server /snmp # <b>scope trap-destination</b> <i>number</i>	指定した宛先に対して SNMP トラップ宛先コマンドモードを開始します。4 つの SNMP トラップ宛先を使用できます。宛先の <i>number</i> は、1 ~ 4 の範囲の整数です。
ステップ 6	Server /snmp/trap-destination # <b>set enabled</b> {yes   no}	SNMP トラップ宛先をイネーブルまたはディセーブルにします。
ステップ 7	Server /snmp/trap-destination # <b>set addr</b> <i>ip-address</i>	SNMP トラップ情報を送信する宛先 IP アドレスを指定します。
ステップ 8	Server /snmp/trap-destination # <b>commit</b>	トランザクションをシステムの設定にコミットします。

次に、汎用の SNMP トラップとトラップの宛先番号 1 を設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # set trap-community-str public
Server /snmp # set trap-ver 3
Server /snmp # set inform-type inform
Server /snmp *# scope trap-destination 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set addr 192.0.20.41
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show
Trap Destination IP Address      Enabled
-----
1                                192.0.20.41    yes
Server /snmp/trap-destination #
```

## テスト SNMP トラップ メッセージの送信

### はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope snmp</b>	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # <b>scope trap-destination number</b>	指定した宛先に対して SNMP トラップ宛先コマンドモードを開始します。4つの SNMP トラップ宛先を使用できます。宛先の <i>number</i> は、1 ~ 4 の範囲の整数です。
ステップ 3	Server /snmp/trap-destination # <b>sendSNMPtrap</b>	設定済みの SNMP トラップ宛先に SNMPv1 テストトラップを送信します。  (注) テストメッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

次の例では、SNMP トラップ宛先 1 にテストメッセージが送信されます。

```
Server# scope snmp
Server /snmp # scope trap-destination 1
Server /snmp/trap-destination # sendSNMPtrap
SNMP Test Trap sent to Destination:1
Server /snmp/trap-destination #
```

# プラットフォーム イベント トラップの解釈

SNMP トラップとして送信された CIMC プラットフォーム イベント アラートには、エンタープライズオブジェクト ID (OID) が 1.3.6.1.4.1.3183.1.1.0.event の形式で含まれています。OID の最初の 10 個のフィールドは、

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired\_for\_management(3183).PET(1).version(1).version(0) を表し、IPMI プラットフォーム イベント トラップ (PET) バージョン 1.0 メッセージであることを示しています。最後のフィールドはイベント番号であり、通知されている特定の状態またはアラートを示しています。

## プラットフォーム イベント トラップの説明

次の表に、プラットフォーム イベント トラップ メッセージで通知されるイベントの説明を示します。これらは、トラップ OID のイベント番号に基づいています。

イベント番号 [注記 1]	プラットフォーム イベントの説明	
0	0h	テスト トラップ
65799	010107h	温度に関する警告
65801	010109h	温度が重大な状態
131330	020102h	電圧不足、緊急
131337	020109h	電圧が重大な状態
196871	030107h	電流に関する警告
262402	040102h	ファンが重大な状態
459776	070400h	プロセッサ関連 (IOH-Thermalert/Caterr センサー) : 予測障害非アサート
459777	070401h	プロセッサ関連 (IOH-Thermalert/Caterr センサー) : 予測障害アサート
460032	070500h	プロセッサ電力警告: 制限未超過
460033	070501h	プロセッサ電力警告: 制限超過
524533	0800F5h	電源が重大な状態
524551	080107h	電源に関する警告
525313	080401h	個々の電源に関する警告
527105	080B01h	電源冗長性の損失
527106	080B02h	電源冗長性復元
552704	086F00h	電源挿入済み

イベント番号 [注記 1]	プラットフォーム イベントの説明
552705	086F01h 電源モジュール障害
552707	086F03h 電源 AC の損失
786433	0C0001h 修正可能な ECC メモリ エラー、リリース 1.3(1) 以降のリリース、すべての読み取りタイプを受け入れるように設定されたフィルタ [注記 4]
786439	0C0007h DDR3_INFO センサー LED : RED ビットアサート (DIMM での ECC エラーの可能性が高い) 、汎用センサー [注記 2、3]
786689	0C0101h 修正可能な ECC メモリ エラー、リリース 1.3(1) 以降のリリース
818945	0C7F01h 修正可能な ECC メモリ エラー、リリース 1.2(x) 以前のリリース
818951	0C7F07h DDR3_INFO センサー LED : RED ビットアサート (DIMM での ECC エラーの可能性が高い) 、1.2(x) 以前のリリース [注記 3]
851968	0D0000h HDD センサーで障害が示されない、汎用センサー [注記 2]
851972	0D0004h HDD センサーで障害が示される、汎用センサー [注記 2]
854016	0D0800h HDD が存在しない、汎用センサー [注記 2]
854017	0D0801h HDD が存在する、汎用センサー [注記 2]
880384	0D6F00h HDD あり、障害の兆候なし
880385	0D6F01h HDD の障害
880512	0D6F80h HDD が存在しない
880513	0D6F81h HDD がアサート解除されたが障害状態ではない
884480	0D7F00h ドライブ スロット LED オフ
884481	0D7F01h ドライブ スロット LED オン
884482	0D7F02h ドライブ スロット LED 高速で点滅
884483	0D7F03h ドライブ スロット LED 低速で点滅
884484	0D7F04h ドライブ スロット LED 緑
884485	0D7F05h ドライブ スロット LED オレンジ
884486	0D7F01h ドライブ スロット LED 青
884487	0D7F01h ドライブ スロット LED 読み取り
884488	0D7F08h ドライブ スロット オンライン



イベント番号 [注記 1]		プラットフォーム イベントの説明
884489	0D7F09h	ドライブ スロット低下
注記 1： イベント番号の書式の基本情報については、次の URL にある『 <i>IPMI Platform Event Trap Format Specification v1.0</i> 』を参照してください。 <a href="ftp://download.intel.com/design/servers/ipmi/pet100.pdf">ftp://download.intel.com/design/servers/ipmi/pet100.pdf</a>		
注記 2： 一部のプラットフォームおよびリリースでは汎用センサー実装が使用され、一部のプラットフォームおよびリリースではシスコ独自のセンサー実装が使用されます。		
注記 3： リリース 1.3(1) 以降のリリースでは、ECC センサーによって LED はアクティブ化されなくなりました。		
注記 4： すべての読み取りタイプを受け入れるようにイベントフィルタが設定された場合は、16 進のイベント番号のビット 15:8 は 0 にマスクされます。たとえば、イベント番号 786689 (0C0101h) は 786433 (0C0001h) になります。		

