

# Zabbixを使用した IBM Flex System 障害検知 検証報告書

2013年4月11日  
ミラクル・リナックス株式会社

## 1. はじめに

本書は OSS の統合監視ソフトウェア Zabbix を使用して、IBM Flex System の障害検知を行う検証を実施した際の報告書です。

IBM Flex System ではシャーシ全体を管理するための CMM (Chassis Manager Module) が標準で搭載されており、ブラウザベースの管理 GUI によってブレードサーバ・スイッチモジュール・電源モジュール・ファンモジュールといった各コンポーネントを一元的に管理することが可能となっています。

また、ブレードサーバには IMM (Integrated Management Module) v2 が搭載されており、サーバ単体の管理もブラウザベースの管理 GUI によって行うことが可能となっています。

これら (CMM および IMM2) が検知した障害情報を SNMP Trap を使用して送信、Zabbix サーバで受信して、障害として通知する方法を紹介します。

## 2. 概要

IBM Flex System ではセキュリティレベルの向上を鑑み、初期状態では Agent, Trap いずれも SNMPv3 のみ有効として設定されています。CMM, IMM2 から送出される SNMPv3 Trap を、Zabbix サーバ上で動作する snmptrapd で受信し、MySQL Database に受信データを格納したうえ障害通知を行います。

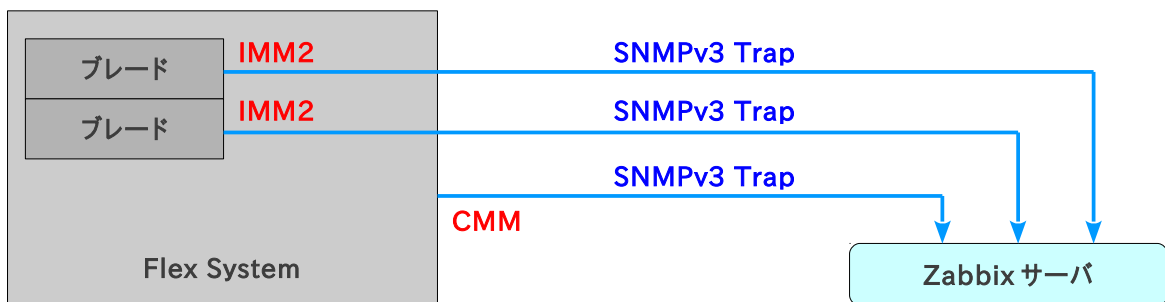


図 1: Flex System - Zabbix サーバ間の通信概念図

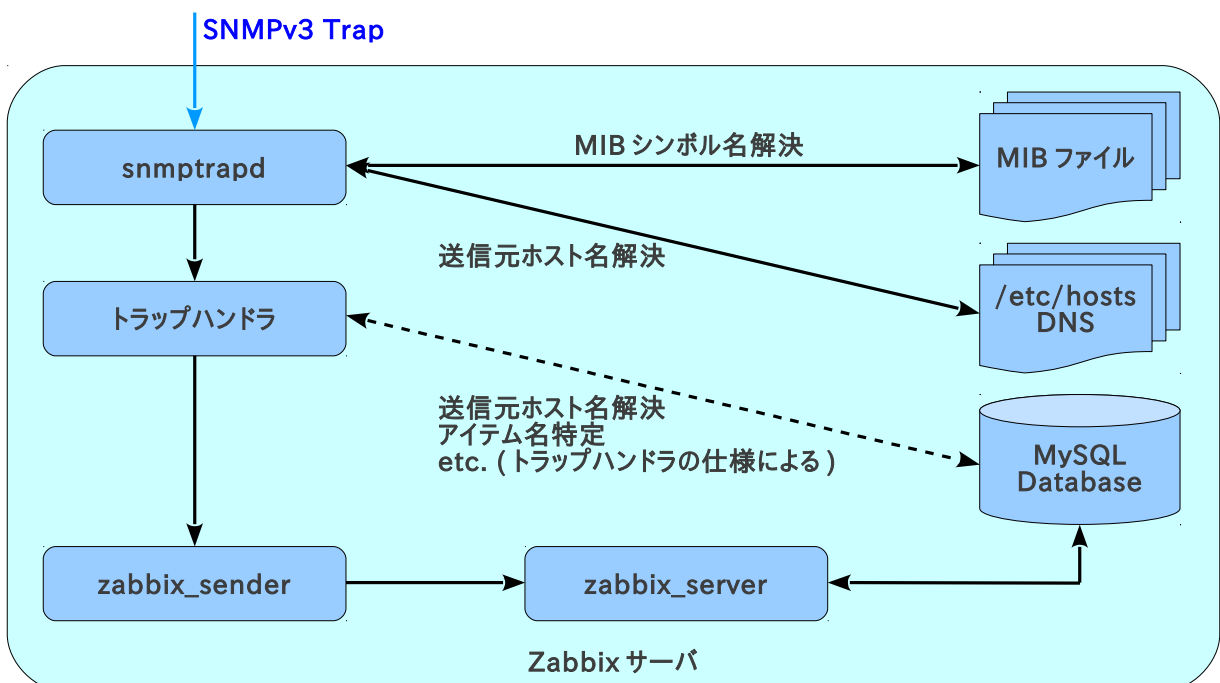


図 2: Zabbix サーバ内の動作概念図

なお、snmptrapd を使用する構成を採用したことから、本書の内容は Zabbix 2.0.x および 1.8.x で同様に使用することができます。

### 3. 検証環境

以下の環境で検証を行いました。

#### 【Zabbix サーバ】

- H/W: x3550 M4
- OS: Red Hat Enterprise Linux 6.3 Server (x86\_64)
- Zabbix: 2.0.4 (MIRACLE ZBX® 2.0.4 パッケージを使用)
- MySQL: 5.1.61 (OS 付属パッケージを使用)
- Apache: 2.2.15 (OS 付属パッケージを使用)

#### 【IBM Flex System】

- シャーシ: IBM Flex System Enterprise シャーシ
- ブレード: IBM Flex System x240

### 4. 設定手順

#### 4-1. Zabbix Server に MIB 定義ファイルを追加

IBM の提供する MIB 定義ファイル群 (imm.mib, immalert.mib, cme.mib, mmalert.mib ※) を /usr/share/snmp/mibs にコピーします。これらが正常に組み込まれ、使用可能な状態にあるかどうかを、追加した MIB ファイルに定義されている OID とシンボル名の相互変換を行うことで確認します。

```
$ export MIBS=ALL
$ snmptranslate .1.3.6.1.4.1.2.6.158.3.0.22 2> /dev/null
BLADESPALT-MIB::mmTrapAppS
$ snmptranslate -On BLADESPALT-MIB::mmTrapAppS 2> /dev/null
.1.3.6.1.4.1.2.6.158.3.0.22
```

※ MIB 定義ファイルは CMM および IMM2 の Firmware に同梱されて提供されています。  
CMM および IMMv2 の Firmware は IBM のダウンロードサイト(Fix Central)から入手することが可能です。

## 4-2. CMM の Security Policies を Legacy へ変更

SNMPv3 で SNMP Trap を受信できるように設定するためには、EngineID を特定する必要があります。このため、項番 4-2～4-4 にて一時的に SNMPv1 を有効化する方法を説明します。項番 4-5 の作業が終了した後、必要に応じて元に戻してください。

なお、CMM の Security Policies の変更は、Flex System に搭載されているブレードの IMM2 セキュリティ設定に影響を及ぼします。本項の操作を行った後は、4-4 に記載されている IMM2 の再起動を行ってください。

CMM に Web ブラウザでアクセスし、下図にて赤枠で囲まれているメニュー “Mgt Module Management” / “Security” を選択してください。

The screenshot shows the IBM Chassis Management Module web console. The top navigation bar includes 'System Status', 'Multi-Chassis Monitor', 'Events', 'Service and Support', and 'Chassis Management'. The 'Mgt Module Management' dropdown menu is expanded, showing options like 'User Accounts', 'Firmware', 'Security' (highlighted with a red box), 'Network', 'Configuration', 'Properties', 'License Key Management', 'Restart', 'Reset to Defaults', and 'File Management'. The main content area displays 'Chassis' information with a 'Table View' of hardware components.

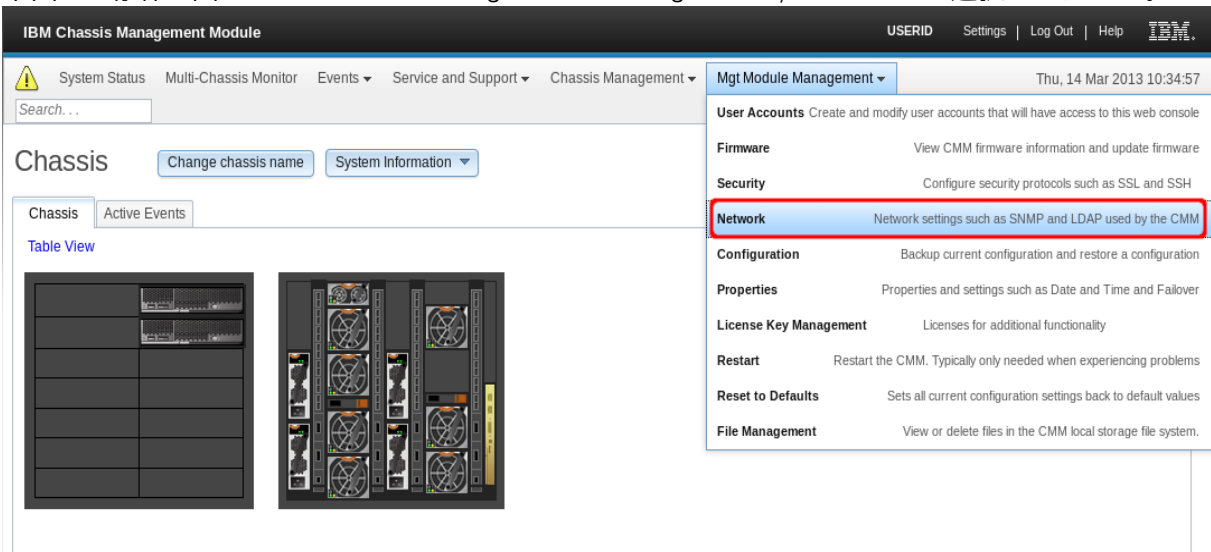
画面左側に表示されているスライダーを “Legacy” に合わせ、ボタン “Apply” をクリックして変更状態を保存してください。

The screenshot shows the 'Security' configuration page in the IBM Chassis Management Module web console. The 'Security Policies' tab is selected, and the 'Policy Setting' is set to 'Legacy' on a vertical slider. The 'Apply' button is visible. The page content includes a description of the Legacy security policy level and a list of attributes:

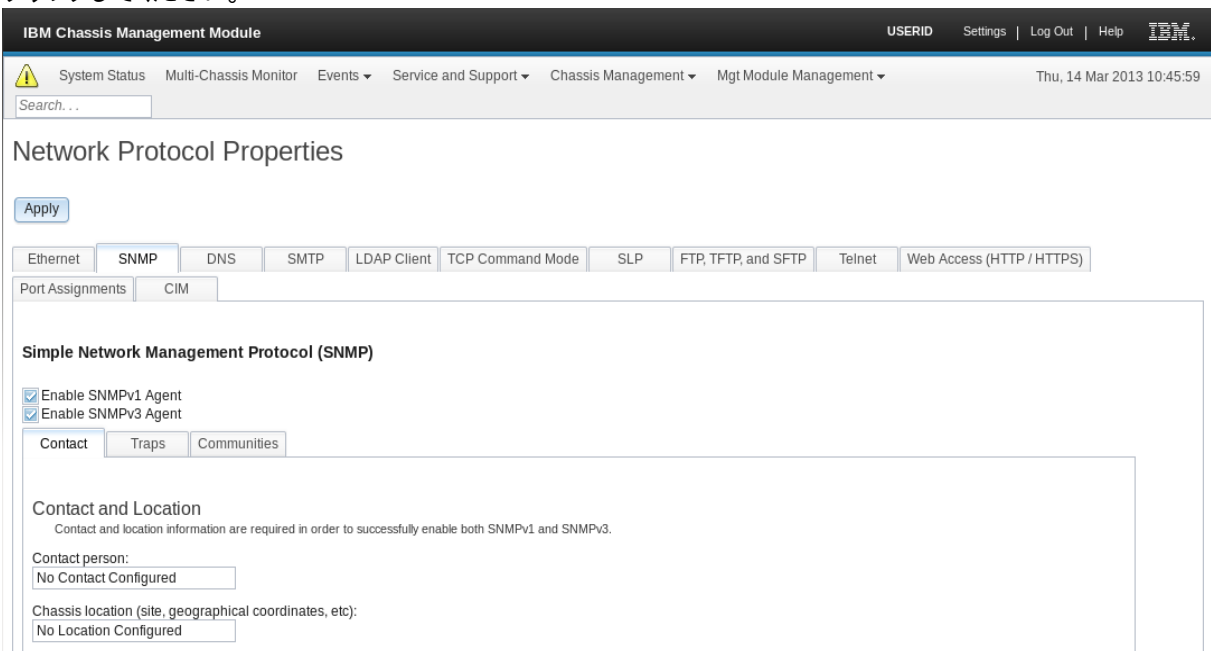
- Weak password policies are permitted
- Well-known passwords for network login are not required to be changed
- Unencrypted communication protocols may be enabled

### 4-3. CMM の SNMPv1 Agent を有効化

下図にて赤枠で囲まれているメニュー “Mgt Module Management” / “Network” を選択してください。



タブ “SNMP” をクリックして表示を切り替え、“Enable SNMPv3 Agent” にチェックを入れてボタン “Apply” をクリックしてください。



2 段目のタブ “Communities” をクリックして表示を切り替え、SNMP のコミュニティ名を確認してください。以降の例示では “public” が設定されていると仮定しています。

#### 4-4. IMM2 の SNMPv1 Agent を有効化

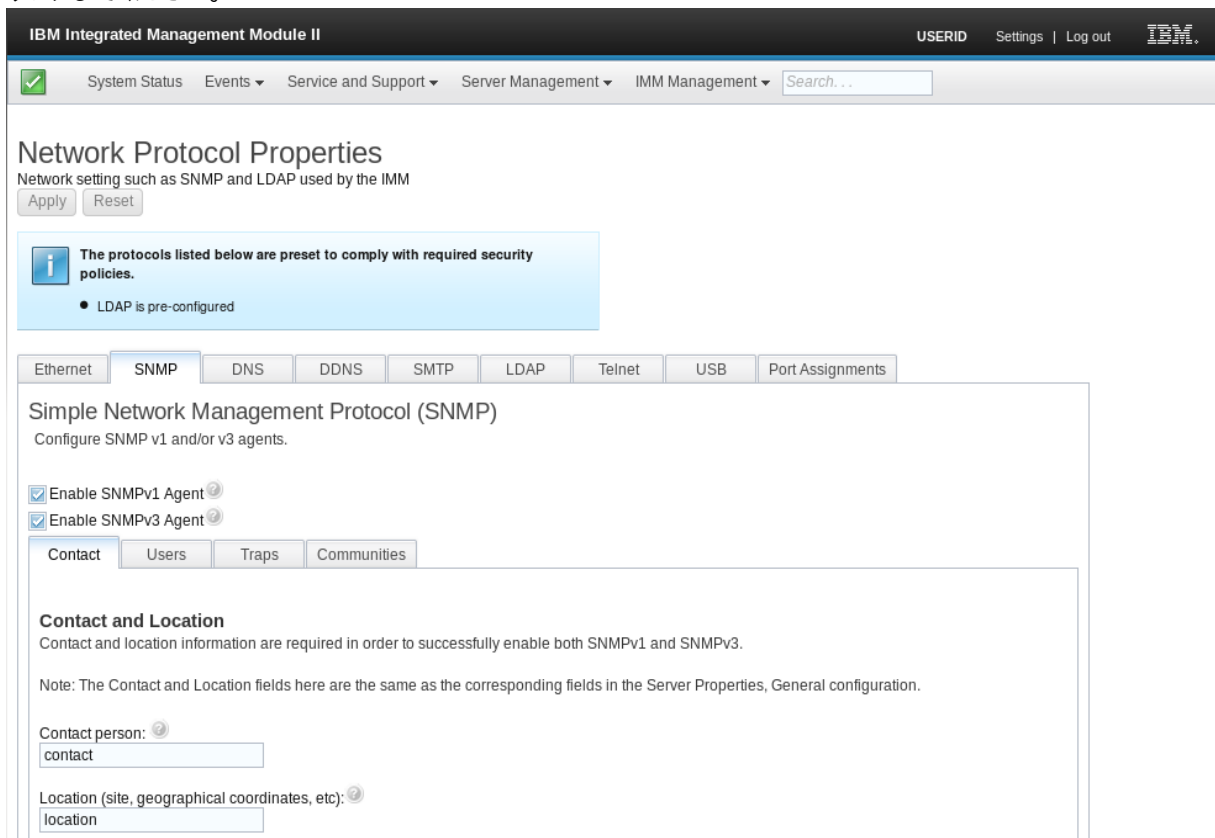
4-2.を実行したのち本手順(4-4)を実施する前に、IMM2 を再起動させてください。SNMPv1 を有効化することができるようになります。再起動を行うにはメニュー “IMM Management” / “Restart IMM” を選択してください。

The screenshot shows the IBM Integrated Management Module II web interface. The main content area displays system information for an IBM Flex System x240 with 10Gb, including system status (Power: On, System state: System power off/State unknown) and hardware health (Disks, Processors, Memory, System, all Normal). The 'IMM Management' dropdown menu is open, showing options like IMM Properties, Users, Network, Security, IMM Configuration, Restart IMM, Reset IMM to factory defaults, and Activation Key Management. The 'Restart IMM' option is highlighted with a red rectangle.

再起動後、メニュー “IMM Management” / “Network” を選択してください。

The screenshot shows the IBM Integrated Management Module II web interface. The main content area displays system information for an IBM Flex System x240 with 10Gb, including system status (Power: On, System state: System power off/State unknown) and hardware health (Disks, Processors, Memory, System, all Normal). The 'IMM Management' dropdown menu is open, showing options like IMM Properties, Users, Network, Security, IMM Configuration, Restart IMM, Reset IMM to factory defaults, and Activation Key Management. The 'Network' option is highlighted with a red rectangle.

タブ”SNMP”をクリックして表示を切り替え、”Enable SNMPv1 Agent”チェックを入れてボタン”Apply”をクリックしてください。



IBM Integrated Management Module II

System Status Events Service and Support Server Management IMM Management Search...

### Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Apply Reset

The protocols listed below are preset to comply with required security policies.

- LDAP is pre-configured

Ethernet **SNMP** DNS DDNS SMTP LDAP Telnet USB Port Assignments

#### Simple Network Management Protocol (SNMP)

Configure SNMP v1 and/or v3 agents.

Enable SNMPv1 Agent

Enable SNMPv3 Agent

Contact Users Traps Communities

##### Contact and Location

Contact and location information are required in order to successfully enable both SNMPv1 and SNMPv3.

Note: The Contact and Location fields here are the same as the corresponding fields in the Server Properties, General configuration.

Contact person: contact

Location (site, geographical coordinates, etc): location

2 段目のタブ”Communities”をクリックして表示を切り替え、SNMP のコミュニティ名を確認してください。以降の例示では”public”が設定されていると仮定しています。

#### 4-5. CMM, IMM2 の EngineID を取得する

Zabbix サーバから CMM, IMM2 の SNMPv1 Agent へ通信し、SNMPv3 Trap の受信に必要な EngineID の情報を取得します。Zabbix サーバのターミナルまたはコンソール上で、次のコマンドを実行してください。

```
$ export MIBS=ALL
$ snmpget -v1 -c public 192.168.70.100 SNMP-FRAMEWORK-MIB::snmpEngineID.0
SNMP-FRAMEWORK-MIB::snmpEngineID.0 = Hex-STRING: 80 00 04 50 01 34 40 B5
DF 04 72
$ snmpget -v1 -c public 192.168.70.112 SNMP-FRAMEWORK-MIB::snmpEngineID.0
SNMP-FRAMEWORK-MIB::snmpEngineID.0 = Hex-STRING: 80 00 1F 88 80 56 A0 BF
79 AD 41 41 51
```

Hex-STRING として返された文字列からスペースを取り除いた値が EngineID です。上記例では、192.168.70.100 の EngineID が 80000450013440B5DF0472、192.168.70.112 の EngineID が 80001F888056A0BF79AD414151 となります。

なお、EngineID はハードウェア固有の値です。CMM のハードウェア交換などが発生した場合には再取得が必要となりますので、ご注意ください。

## 4-6. CMM の SNMP Trap 送出に関する設定を行う

下図にて赤枠で囲まれているメニュー “Mgt Module Management” / “User Accounts” を選択してください。

The screenshot shows the IBM Chassis Management Module interface. At the top, the user is logged in as 'USERID'. The navigation menu includes 'System Status', 'Multi-Chassis Monitor', 'Events', 'Service and Support', 'Chassis Management', and 'Mgt Module Management'. The 'Mgt Module Management' dropdown menu is open, and 'User Accounts' is highlighted with a red box. Below the menu, there are options for 'Firmware', 'Security', 'Network', 'Configuration', 'Properties', 'License Key Management', 'Restart', 'Reset to Defaults', and 'File Management'. The main content area shows 'Chassis' management options and a hardware diagram.

タブ “Accounts” をクリックして表示を切り替え、SNMPv3 Trap を送信する際に使用するユーザを作成または既存ユーザの設定を変更します。以下の例では既存ユーザ “USERID” の設定を変更する場合があります。

The screenshot shows the 'User Accounts' page in the IBM Chassis Management Module. The 'Accounts' tab is selected. The page title is 'User Accounts' and the subtitle is 'Configure user accounts for all chassis elements.' There are buttons for 'Create User', 'Global Login Settings', 'Currently Logged in Users', and 'Delete'. A table lists the existing users:

User Name	Permission Group	# Active Sessions	Last Login	Dormant	Days to Expiration	State
USERID	supervisor	3	03/14/13 09:56:52		67	Active
test	operator	0	02/25/13 17:22:57		74	Disabled



ユーザ名”USERID”をクリックすると、下図のようにポップアップウィンドウ”USER Properties”が表示されます。タブ”SNMPv3”をクリックし、各項目を設定します。パスワードには適切な文字列を設定してください。入力終了後にボタン”OK”をクリックし、設定を保存してください。

- Authentication Protocol:  
Hash-based Message Authentication Code (HMAC) – Secure Hash Algorithm (SHA)
- Use a privacy protocol  
Advanced Encryption Standard (AES)
- Access Type:  
Trap 以上の権限
- IP address or host name for traps:  
Zabbix サーバの IP アドレス

The screenshot shows the 'User Properties' dialog box with the following settings:

- Context name: (empty)
- Authentication Protocol: Hash-based Message Authentication Code (HMAC) - Secure Hash Algorithm (SHA)
- Use a privacy protocol
- Privacy protocol: Advanced Encryption Standard (AES)
- Privacy password: (empty)
- Confirm privacy password: (empty)
- Access type: Trap
- IP address or host name for traps: 192.168.70.231

## 4-7. IMM2 の SNMP Trap 送出に関する設定を行う

下図にて赤枠で囲まれているメニュー “IMM Management” / “Users” を選択してください。

タブ “User Accounts” をクリックして表示を切り替え、SNMPv3 Trap を送信する際に使用するユーザを作成または既存ユーザの設定を変更します。以下の例では既存ユーザ “USERID” の設定を変更する場合を示しています。

ユーザ名 “USERID” をクリックすると、下図のようにポップアップウィンドウ “USER Properties” が表示されます。タブ “SNMPv3” をクリックし、各項目を設定します。パスワードには適切な文字列を設定してください。入力終了後にボタン “OK” をクリックし、設定を保存してください。

- Authentication Protocol:  
Hash-based Message Authentication Code (HMAC) – Secure Hash Algorithm (SHA)
- Use a privacy protocol  
Advanced Encryption Standard (AES)
- Access Type:  
Get 以上の権限
- IP address or host name for traps:  
Zabbix サーバの IP アドレス

## 4-8. Zabbix Server 上の snmptrapd の設定を変更する

4-1 で追加した MIB 定義ファイル群を使用して、snmptrapd が OID からシンボル名に変換できるようにオプションを指定します。

```
/etc/sysconfig/snmptrapd
```

```
OPTIONS="-Lsd -p /var/run/snmptrapd.pid -m all"
```

次に、SNMP Trap を受信した際の動作を定義します。

```
/etc/snmp/snmptrapd.conf
```

```
authUser log,execute,net USERID
authCommunity log,execute,net public
traphandle default <trapハンドラへの full path>
createUser -e 80000450013440b5df0472 USERID SHA "xxxxxxxx" AES
createUser -e 80001F888056A0BF79AD414151 USERID SHA "xxxxxxxx" AES
```

authUser エントリの最後に、CMM, IMM2 で定義したユーザ名を指定します。

createUser エントリは次のフォーマットで、1 行で記述します。

```
createUser -e <EngineID> <ユーザ名> <authentication protocol> "<パスワード>"
<privacy protocol>
```

#### 4-9. [ケース 1] Zabbix のアイテムを用意する

ケース 1 (4-9, 4-10)では、各ホストに SNMP Trap 格納専用アイテムを用意する方法を説明します。trap ハンドラを、Zabbix 登録済ホスト毎に特定のアイテムへ格納するよう実装してください。

なお、このロジックは MIRACLE ZBX8000a, ZBX6000 では出荷状態で実装されています。

以下、新規テンプレート Template\_SNMP\_Traps にアイテム snmptraps およびトリガーを作成する方法を例示します。アイテム snmptraps の定義は次のとおりとしました。

- 名前 snmptraps
- タイプ Zabbixトラッパ
- キー snmptraps
- データ型 テキスト
- ヒストリの保存期間(日) 任意 (例では 90 日)
- アプリケーション 任意 (例では SNMP Traps)

CMM および IMM2 からの SNMP Trap は 255 文字に収まらないため、データ型にはテキストを選択する必要があります。

The screenshot shows the Zabbix web interface for configuring a new item. The breadcrumb trail is: トラガーの設定 > テンプレートの設定 > アイテムの設定 > トリガーの設定 > アイテムの設定. The current page is titled 'アイテムの設定' (Item Configuration). The breadcrumb trail below the title is: < テンプレートリスト | テンプレート: Template\_SNMP\_Traps | アプリケーション (1) | アイテム (1) | トリガー (1) | グラフ (0) | スクリーン (0) | ディスカバリールール (0). The main form is titled 'アイテム' (Item) and contains the following fields:

- ホスト: Template\_SNMP\_Traps
- 名前: snmptraps
- タイプ: Zabbixトラッパ (dropdown menu)
- キー: snmptraps (with a '選択' button)
- データ型: テキスト (dropdown menu)
- ヒストリの保存期間(日): 90
- 許可されたホスト: (empty text field)
- アプリケーションの作成: (empty text field)
- アプリケーション: -なし- (dropdown menu with 'SNMP Traps' selected)
- ホストイベントフィールドの自動設定: -なし- (dropdown menu)
- 説明: (empty text area)
- ステータス: 有効 (dropdown menu)

At the bottom of the form are buttons for '保存' (Save), '複製' (Copy), '削除' (Delete), and 'キャンセル' (Cancel). The footer of the page reads: Zabbix 2.0.4 Copyright 2001-2012 by Zabbix SIA / Powered by MIRACLE LINUX CORPORATION | ユーザー 'Admin' でログイン

## 4-10. [ケース 1] Zabbix にトリガーを設定する

4-9 で作成したアイテムに対し、トリガーを追加します。何らかの SNMP Trap を受信した際に、当該トリガーが発報される構成となります。障害内容については、SNMP Trap のメッセージを参照して判断します。

- 名前 任意 (例では Caught a SNMP Trap)
- 条件式 `{Template_SNMP_Traps:snmptraps.regex(.*)}>0`
- 障害イベントを継続して生成  
      チェック有
- 説明 任意
- URL 任意
- 深刻度 任意 (例では軽度の障害)

The screenshot shows the Zabbix web interface for configuring a trigger. The breadcrumb trail is: テンプレートの設定 > アイテムの設定 > トリガーの設定 > アイテムの設定 > トリガーの設定. The current page is titled 'トリガーの設定' (Trigger Configuration). The configuration details are as follows:

- 名前 (Name):** Caught a SNMP Trap
- 条件式 (Condition):** `{Template_SNMP_Traps:snmptraps.regex(.*)}>0`
- 障害イベントを継続して生成 (Continue to generate events):**
- 説明 (Description):** (Empty text area)
- URL:** (Empty text field)
- 深刻度 (Severity):** 未分類 | 情報 | 警告 | **軽度の障害** | 重度の障害 | 致命的な障害
- 有効 (Enabled):**

Buttons at the bottom include: 保存 (Save), 複製 (Copy), 削除 (Delete), and キャンセル (Cancel). The footer indicates 'Zabbix 2.0.4 Copyright 2001-2012 by Zabbix SIA / Powered by MIRACLE LINUX CORPORATION' and the user 'Admin' is logged in.

#### 4-11. [ケース 2] Zabbix のアイテムを用意する

ケース 2 (4-11, 4-12)では、各ホストに MIB 定義\_シンボル名のアイテムを用意する方法を説明します。trap ハンドラを、Zabbix 登録済みホスト毎に、SNMP Trap の内容に応じて「MIB 定義名\_シンボル名」のキーを持つアイテムに格納するよう実装してください。

このロジックは MIRACLE ZBX Cisco スイッチ用監視テンプレートほか、MIRACLE LINUX 製各種ハードウェア監視用テンプレートに実装済です。

以下、新規テンプレート Template\_IBM\_BLADESPPALT\_Traps に OID .1.3.6.1.4.1.2.6.158.3.0.176 を格納するためのアイテムを作成する方法を例示します。

最初に、アイテム名を決定します。

```
$ export MIBS=ALL
$ snmptranslate .1.3.6.1.4.1.2.6.158.3.0.176 2> /dev/null
BLADESPPALT-MIB::mmTrapBladeS
```

OID .1.3.6.1.4.1.2.6.158.3.0.176 は BLADESPPALT-MIB::mmTrapBladeS として名前解決されることが分かります。この「::」を「\_」に置換した文字列をアイテムのキーとして定義します。

- 名前 System Alert: Blade
- タイプ Zabbixトラッパー
- キー BLADESPPALT-MIB\_mmTrapBladeS
- データ型 テキスト
- ヒストリの保存期間(日) 任意 (例では 90 日)
- アプリケーション 任意 (例では TRAP\_BLADESPPALT-MIB)

The screenshot shows the Zabbix web interface for configuring a new item. The breadcrumb trail is: ホーム | サポート | プリント | プロファイル | ログアウト. The navigation menu includes: 監視データ | インベントリ | レポート | 設定 | 管理. The main menu includes: ホストグループ | テンプレート | アイテム | メンテナンス | ウェブ | アクション | スクリーン | スライドショー | マップ | ディスカバリ | ITサービス. The current page is 'アイテムの設定' (Item Configuration). The breadcrumb trail is: ヒストリ: トリガーの設定 >> アイテムの設定 >> トリガーの設定 >> テンプレートの設定 >> アイテムの設定. The page title is 'アイテムの設定'. The breadcrumb trail is: < テンプレートリスト | テンプレート: Template\_IBM\_BLADESPPALT\_Traps | アプリケーション (1) | アイテム (49) | トリガー (85) | グラフ (0) | スクリーン (0) | ディスカバリールール (0). The item configuration form includes:
 

- ホスト: Template\_IBM\_BLADESPPALT\_Traps
- 名前: System Alert: Blade
- タイプ: Zabbixトラッパー
- キー: BLADESPPALT-MIB\_mmTrapBladeS
- データ型: テキスト
- ヒストリの保存期間(日): 90
- 許可されたホスト: (empty)
- アプリケーションの作成: (empty)
- アプリケーション: TRAP\_BLADESPPALT-MIB
- ホスト-インベントリフィールドの自動設定: -なし-
- 説明: (empty text area)
- ステータス: 有効

 At the bottom, there are buttons for 保存 (Save), 複製 (Duplicate), 削除 (Delete), and キャンセル (Cancel). The footer contains: Zabbix 2.0.4 Copyright 2001-2012 by Zabbix SIA / Powered by MIRACLE LINUX CORPORATION and ユーザー 'Admin' でログイン.

また、定義済アイテムに合致しない SNMP Trap を格納するためのアイテムも同時に作成します。ここではテンプレート Template\_SNMP\_TRAPS\_OTHER にアイテム other-snmptaps を用意したものとして例示します。

- 名前                                   other-snmptaps
- タイプ                                Zabbixトラッパー
- キー                                   other-snmptaps
- データ型                             テキスト
- ヒストリの保存期間(日)           任意 (例では 90 日)
- アプリケーション                  任意 (例では「なし」)

The screenshot shows the Zabbix web interface for configuring a new item. The breadcrumb trail is: テンプレートの設定 >> アイテムの設定 >> ホストの設定 >> テンプレートの設定 >> アイテムの設定. The current page is titled 'アイテムの設定' (Item Configuration). The breadcrumb trail below the title is: << テンプレートリスト | テンプレート: Template\_SNMP\_TRAPS\_OTHER | アプリケーション (0) | アイテム (1) | トリガー (0) | グラフ (0) | スクリーン (0) | ディスカバリールール (0). The main form is titled 'アイテム' (Item) and contains the following fields:

- ホスト: Template\_SNMP\_TRAPS\_OTHER
- 名前: other-snmptaps
- タイプ: Zabbixトラッパー (dropdown)
- キー: other-snmptaps (with a '選択' button)
- データ型: テキスト (dropdown)
- ヒストリの保存期間(日): 90
- 許可されたホスト: (empty text field)
- アプリケーションの作成: (highlighted green bar)
- アプリケーション: -なし- (dropdown)
- ホスト-インベントリフィールドの自動設定: -なし- (dropdown)
- 説明: (empty text area)
- ステータス: 有効 (dropdown)

At the bottom of the form are buttons for '保存' (Save), '複製' (Copy), '削除' (Delete), and 'キャンセル' (Cancel). The footer of the page reads: Zabbix 2.0.4 Copyright 2001-2012 by Zabbix SIA / Powered by MIRACLE LINUX CORPORATION | ユーザー 'Admin' でログイン

## 4-12. [ケース 2] Zabbix にトリガーを設定する

4-11 で作成したアイテムに対し、トリガーを追加します。以下はアイテム System Alert: Blade に対するトリガーです。

- 名前 任意 (例では Caught a System Alert: Blade)
- 条件式

```
{Template_IBM_BLADESPPALT_Traps:BLADESPPALT-MIB_mmTrapBladeS.regexp(.*)}>0
```

- 障害イベントを継続して生成
- チェック有
- 説明 任意
- URL 任意
- 深刻度 任意 (例では軽度の障害)

The screenshot shows the Zabbix web interface for configuring a trigger. The breadcrumb trail is: トリガーの設定 > アイテムの設定 > テンプレートの設定 > ホストの設定 > アイテムの設定. The current page is titled 'トリガーの設定' (Trigger Configuration). The breadcrumb trail for the trigger is: < テンプレートリスト | テンプレート: Template\_IBM\_BLADESPPALT\_Traps | アプリケーション (1) | アイテム (49) | トリガー (85) | グラフ (0) | スクリーン (0) | ディスカバリールール (0). The trigger configuration form includes the following fields:

- 名前:** Caught a System Alert: Blade
- 条件式:** {Template\_IBM\_BLADESPPALT\_Traps:BLADESPPALT-MIB\_mmTrapBladeS.regexp(.\*)}>0
- 条件式ビルダー:** 条件式ビルダー
- 障害イベントを継続して生成:**
- 説明:** (Empty text area)
- URL:** (Empty text field)
- 深刻度:** 未分類 | 情報 | 警告 | **軽度の障害** | 重度の障害 | 致命的な障害
- 有効:**

Buttons at the bottom of the form are: 保存, 複製, 削除, キャンセル. The footer of the page reads: Zabbix 2.0.4 Copyright 2001-2012 by Zabbix SIA / Powered by MIRACLE LINUX CORPORATION | ユーザー 'Admin' でログイン



以下はアイテム other-snmptests に対するトリガーです。

- 名前 任意 (例では Caught a undefined SNMP Trap)
- 条件式 {Template\_SNMP\_TRAPS\_OTHER:other-snmptests.regex(.\*)}>0
- 障害イベントを継続して生成  
チェック有
- 説明 任意
- URL 任意
- 深刻度 任意 (例では警告)

The screenshot shows the Zabbix web interface for configuring a trigger. The breadcrumb trail is: 監視データ > イベントリポート > 設定 > 管理 > ホストグループ > テンプレート > 設定 > メンテナンス > ウェブ > アクション > スクリーン > スライドショー > マップ > ディスカバリ > ITサービス > 検索. The current page is titled 'トリガーの設定' (Trigger Configuration). The breadcrumb trail for the current page is: << テンプレートリスト >> テンプレート: Template\_SNMP\_TRAPS\_OTHER >> アプリケーション (0) >> アイテム (1) >> トリガー (1) >> グラフ (0) >> スクリーン (0) >> ディスカバリーール (0). The configuration form includes:
 

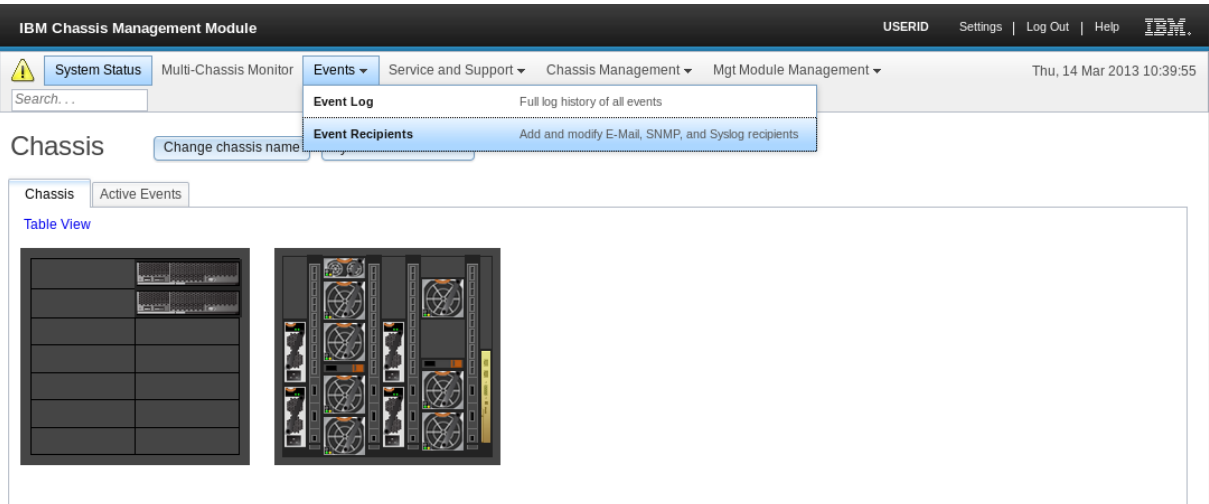
- 名前: Caught a undefined SNMP Trap
- 条件式: {Template\_SNMP\_TRAPS\_OTHER:other-snmptests.regex(.\*)}>0
- 条件式ビルダー: 条件式ビルダー
- 障害イベントを継続して生成:
- 説明: (empty text area)
- URL: (empty text field)
- 深刻度: 未分類, 情報, 警告 (selected), 軽度の障害, 重度の障害, 致命的な障害
- 有効:

 At the bottom of the form are buttons for 保存 (Save), 複製 (Copy), 削除 (Delete), and キャンセル (Cancel). The footer of the page reads: Zabbix 2.0.4 Copyright 2001-2012 by Zabbix SIA / Powered by MIRACLE LINUX CORPORATION | ユーザー 'Admin' でログイン

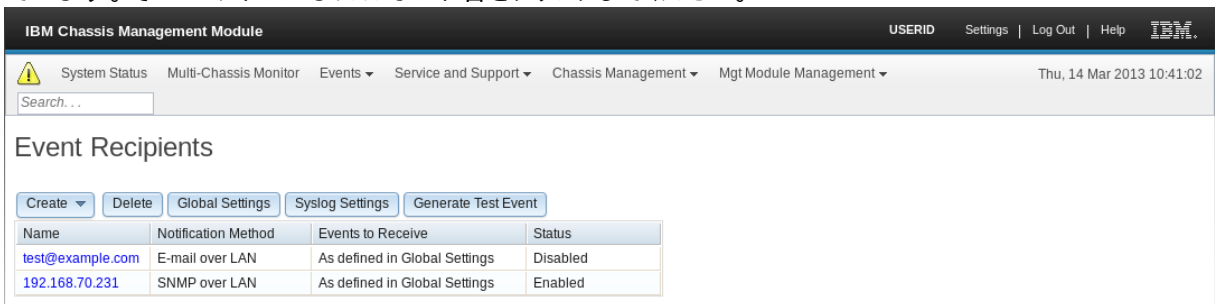
## 5.動作確認

### 5-1.試験用 SNMP Trap 送信

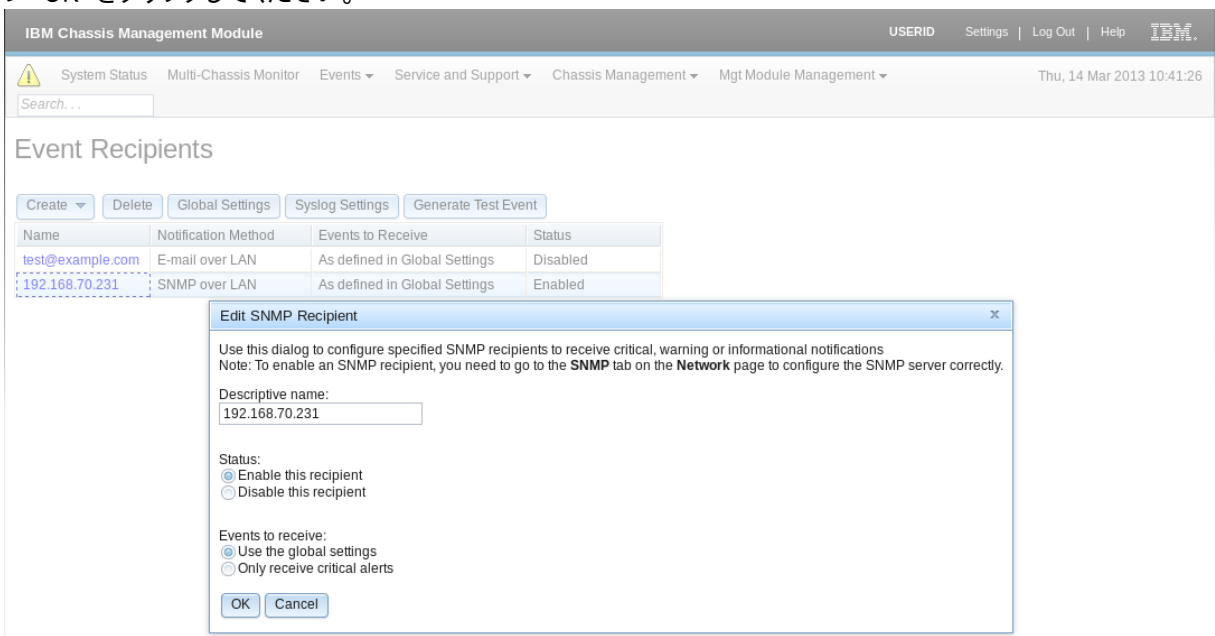
CMM にはテスト用の SNMP Trap を送出する機能が実装されています。この機能を利用して、SNMPv3 Trap を正常に受信できることを確認します。メニュー “Events” / “Event Recipients” を選択してください。



4-6 で設定したユーザの “IP address or hostname for traps” の値が “SNMP over LAN” の行に表示されています。その IP アドレスまたはホスト名をクリックしてください。



ポップアップウィンドウ “Edit SNMP Recipient” が表示されます。変更の必要がない限り、そのままボタン “OK” をクリックしてください。



ポップアップウィンドウ”Choose event type”が表示されます。ラジオボタン”Event Log”にフォーカスを合わせ、ボタン”OK”をクリックしてください。

The screenshot shows the IBM Chassis Management Module interface. At the top, there's a navigation bar with 'System Status', 'Multi-Chassis Monitor', 'Events', 'Service and Support', 'Chassis Management', and 'Mgt Module Management'. Below this is a search bar and the title 'Event Recipients'. There are buttons for 'Create', 'Delete', 'Global Settings', 'Syslog Settings', and 'Generate Test Event'. A table lists two recipients:

Name	Notification Method	Events to Receive	Status
test@example.com	E-mail over LAN	As defined in Global Settings	Disabled
192.168.70.231	SNMP over LAN	As defined in Global Settings	Enabled

A dialog box titled 'Choose event type' is open, showing 'Generated test event type:' with two radio buttons: 'Syslog' (unselected) and 'Event Log' (selected). There are 'OK' and 'Cancel' buttons at the bottom of the dialog.

Zabbix サーバで正常に受信できれば SNMPv3 Trap の内容がアイテム”other-smnptraps”に格納され、トリガー”Caught a undefined SNMP Trap”が発報されます。

The screenshot shows the Zabbix web interface. At the top, there's a navigation bar with '監視データ', 'インベントリ', 'レポート', '設定', and '管理'. Below this is a search bar and the title 'トリガーのステータス [2013/04/03 18:02:56]'. There are buttons for 'ヘルプ', 'サポート', 'プリント', 'プロフィール', and 'ログアウト'. A table lists one triggered event:

深刻度	ステータス	情報	最新の変更	経過時間	障害対応済	ホスト	名前	コメント
警告	障害		2013/04/03 18:02:53	3s	障害対応コスト (1)	IBM-FLEX	Caught a undefined SNMP Trap	追加

At the bottom of the table, there are buttons for '障害対応コストの一括処理' and '実行 (0)'. The footer shows 'Zabbix 2.0.4 Copyright 2001-2012 by Zabbix SIA / Powered by MIRACLE LINUX CORPORATION' and 'ユーザー'Admin'でログイン'.

## 5-2.実際の障害に伴う SNMP Trap 送信

Flex System に搭載された稼働中のブレード x240 から、HDD を抜いて実際の SNMPv3 Trap を送出するテストを行いました。HDD 挿抜の通知は BLADESPALM-MIB::mmTrapBladeS として送出されますので、アイテム "BLADESPALM-MIB\_mmTrapBladeS" に格納され、トリガー "Caught a System Alert: Blade" が発報されます。

The screenshot shows the Zabbix 2.0.4 web interface. The top navigation bar includes '監視データ', 'インベントリ', 'レポート', '設定', and '管理'. The main content area displays a list of events under the 'トリガー' (Triggers) section. The selected trigger is 'Caught a System Alert: Blade'. Below the trigger name, there is a table of events:

選択	ステータス	情報	最新の変更	経過時間	障害対応済	ホスト	名前	コメント
<input type="checkbox"/>	経度の障害		2013/04/03 18:09:56	57s	障害対応済み (1)	IBM-FLEX	Caught a System Alert: Blade	追加
<input type="checkbox"/>	警告		2013/04/03 18:02:53	8m	障害対応済み (1)	IBM-FLEX	Caught a undefined SNMP Trap	追加

At the bottom of the interface, there is a footer: 'Zabbix 2.0.4 Copyright 2001-2012 by Zabbix SIA / Powered by MIRACLE LINUX CORPORATION' and a user login field for 'Admin'.

なお、上記のように CMM から SNMPv3 Trap が送出されるとともに、ブレード x240 の IMM2 から SNMPv3 Trap が送出されます。IMM2 の IP アドレスを持つホストを Zabbix に登録し、アイテム "IMMALERT-MIB\_ibmSpTrapHdC" を作成すれば Trap の内容が格納されます。

CMM から送出される Trap のみを利用するケースでは、障害発生ポイントとなったブレードの特定にはメッセージの内容を確認する必要があります。しかし、IMM2 から送出される Trap も受信するように追加の設定を加えることで、障害発生ポイントの特定を更に容易に行うことが可能となります。

### 【参考情報】

MIRACLE ZBX 1.8 (1.8.5-2 以降) では、下図のように Trap の内容を Web 上で確認することが可能です。

The screenshot shows the Zabbix 1.8.10 web interface. The top navigation bar includes '監視データ', 'インベントリ', 'レポート', '設定', and '管理'. The main content area displays a list of events under the 'イベント' (Events) section. The selected event is 'Caught a System Alert: Blade'. Below the event name, there is a table of event log entries:

時間	説明	ステータス	選択	経過時間	コメント	アクション	ヒストリログ
2013.05.11 13:57:47	Caught a System Alert: Blade	障害	<input type="checkbox"/>	38m 44s	LU.S	-	BLADESPALM-MIB::mmTrapBladeS BLADESPALM-MIB::spTrapDate YYYY-MM-DDTh:mm:ss+2013-04-11T13:57:47Z BLADESPALM-MIB::spTrapAppId IBM Flex Chassis Management Module BLADESPALM-MIB::

At the bottom of the interface, there is a footer: 'Zabbix 1.8.10 Copyright 2001-2011 by ZIA Zabbix / Powered by MIRACLE LINUX CORPORATION' and a user login field for 'Admin'.

## 参考: SNMP Trap を格納するためのアイテムへ、複数トリガーを設定する監視設定について

トリガー関数 `str()` または `regexp()` を使用して検出することで特定の文字列が含まれていることを確認し、それらを別個のトリガーとして定義することで実現することは可能です。しかし、この設定は以下の2点の理由から推奨できません。

- トリガー間の依存性を維持することが難しい
- SNMP Trap 受信 1 件ごとの処理負荷が高まる

IBM Flex System に搭載されたブレード”Node\_01”から、HDD が挿抜されたことを検出するためのトリガーを例に説明します。

この事象は OID .1.3.6.1.4.1.2.6.158.3.0.176 (シンボル名 `BLADESPPALT-MIB::mmTrapBladeS`) の SNMP Trap として Zabbix サーバへ通知されます。よって、アイテム `BLADESPPALT-MIB_mmTrapBladeS` に対するトリガーを追加します。

### 【HDD が引きぬかれた際のトリガー】

- 名前 `Caught a System Alert: Blade (Hard drive removed from Node 01)`
- 条件式  

```
{Template_IBM_BLADESPPALT_Traps:BLADESPPALT-MIB_mmTrapBladeS.regexp(
BLADESPPALT-MIB::spTrapMsgText.*Hard drive .* removed.)}>0 &
{Template_IBM_BLADESPPALT_Traps:BLADESPPALT-MIB_mmTrapBladeS.regexp(
BLADESPPALT-MIB::spTrapSourceId.*\"Node_01\")}>0
```
- 障害イベントを継続して生成  
チェック有
- 深刻度 軽度の障害

### 【HDD が挿された際のトリガー】

- 名前 `Caught a System Alert: Blade (Hard drive installed into Node 01)`
- 条件式  

```
{Template_IBM_BLADESPPALT_Traps:BLADESPPALT-MIB_mmTrapBladeS.regexp(
BLADESPPALT-MIB::spTrapMsgText.*Hard drive .* installed.)}>0 &
{Template_IBM_BLADESPPALT_Traps:BLADESPPALT-MIB_mmTrapBladeS.regexp(
BLADESPPALT-MIB::spTrapSourceId.*\"Node_01\")}>0
```
- 障害イベントを継続して生成  
チェック有
- 深刻度 情報

同様に、Node\_02~14 の合計 28 個を作成する必要があります。加えて、OID .1.3.6.1.4.1.2.6.158.3.0.176 で通知される SNMP Trap は HDD 挿抜以外にも多数存在します。そのため、トリガー `Caught a System Alert: Blade` には、上に示したトリガー(少なくとも 28 件)への依存関係を設定する必要があります(次ページ参考図参照)。

また、現在の Zabbix の制約により、(フォールバック側の)依存する側のトリガーは、依存される側のトリガーよりも大きな `triggerid` が割り振られる必要があります。監視開始後に上記のような特定文字列を対象としたトリガーを追加した場合には、トリガー `Caught a System Alert: Blade` を再作成し、全ての依存先トリガーを設定する必要があります。

加えて、トリガーが増える毎に SNMP Trap の受信 1 件ごとに比較判定する処理の負荷が高まります。SNMP Trap がアイテムに格納されると、当該アイテムに設定されている各トリガーに合致するか、個別に判定を行う構造となっています。そのため、状況によっては SNMP Trap 受信後の処理遅延のみならず、SNMP Trap の取りこぼしが発生する可能性があります。

そのため、Zabbix への SNMP Trap の格納は OID ごとの分割程度にとどめ、具体的な通知内容についてはアクションで通知するメッセージを閲覧して判断する監視実装が望ましいと判断します。

依存関係

名前	アクション
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 01)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 02)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 03)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 04)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 05)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 06)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 07)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 08)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 09)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 10)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 11)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 12)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 13)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive installed into Node 14)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 01)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 02)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 03)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 04)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 05)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 06)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 07)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 08)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 09)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 10)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 11)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 12)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 13)	<a href="#">削除</a>
Template_IBM_BLADESPPAL_Traps: Caught a System Alert: Blade (Hard drive removed from Node 14)	<a href="#">削除</a>

[追加](#)

参考図: トリガー Caught a System Alert: Blade の依存関係定義(例)