BOM for Windows Ver.6.0
Lenovo 社製品連携ホワイトペーパー
(SNMP v3 対応版)

2016 年 9 月

セイ・テクノロジーズ株式会社

免責事項

本稿に記載された内容は、予告無しに変更される場合があります。
セイ・テクノロジーズ株式会社は、本稿に関していかなる種類の保証（商用性および特定の目的への適合性の黙示の保証を含みますが、これに限定されません）もいたしません。
セイ・テクノロジーズ株式会社は、本稿に含まれた誤謬に関しての責任や、本稿の提供、履行および使用に関して偶発的または間接的に起こる損害に対して、責任を負わないものとします。
本稿の内容は 2016 年 8 月時点で行った検証にそれぞれ基づいており、お客様にこの文章をご利用いただく際には、最新情報をご確認ください。

目次

1. はじめに

本書は BOM for Windows(以降 BOM と記)と Lenovo 社製品とを BOM の SNMP トラップ受信機能拡張モジュールを使用して連携する仕組みを解説したホワイトペーパーです。SNMP トラップ受信機能そのものの解説とそれを使用した Lenovo 社製品との連携方法を記載しています。BOM 本体の操作方法および解説については、本書では省略しています。BOM 付属の各種マニュアルをご参照ください。

※本書は「BOM for Windows Ver.6.0 SR2 向け SNMP トラップ受信機能（V3 対応） 拡張モジュール」を対象としています。

2. SNMP トラップ受信機能拡張モジュールの概要

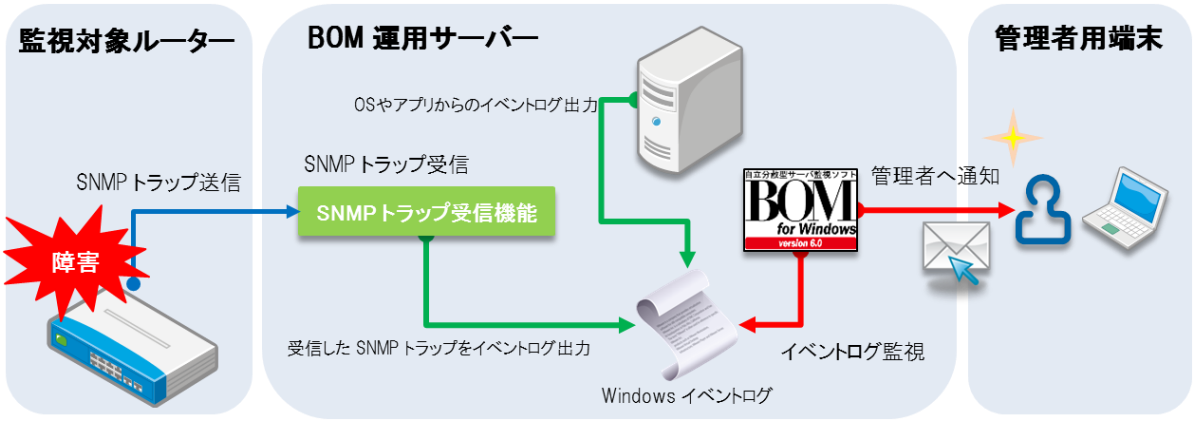
システムの安定稼働には、各種サーバー機器・ネットワーク機器・ストレージなどが正常に期待通りの動作を継続しているかを管理・監視をする必要があります。
これを実現するために BOM をはじめ様々な「監視・運用管理ソフト」と呼ばれるソフトウェアが開発・提供されています。
BOM はこの中において、サーバー機の OS 並びにその上で運用されている各種サービスやアプリケーションを監視すると言う分野に特化し、最少 1 台からの運用が可能で、別途マネージャー用サーバーもデータベースサーバーも必須ではありません。 BOM 単体で監視・通知・リカバリーをカバーします。
そんなシンプルさを追求した「サーバー監視ソフト」である BOM は他の「監視・運用管理ソフト」との連携は欠かせないものとなっております。

本書では他の「監視・運用管理ソフト」との連携を大幅に広げる新たな一歩となる SNMP トラップ受信機能拡張モジュール(以降 SNMP トラップ受信機能と記)についての、位置付けや運用例などを交えてご紹介する事を目的としています。

2.1. 特徴

サーバー機器のハードウェア状況、ネットワーク機器、ストレージなどは Windows などの標準的な OS の管理下ではない事が多いのが現状です。そのような場合には機器に搭載しているファームウェアにより SNMP トラップを送信することにより機器の異常を管理者へ通知するファーストステップとする運用が増えてきました。しかしこの SNMP トラップパケットを BOM の基本機能では受信・検知する事ができませんでした。

そこで今回ご紹介する SNMP トラップ受信機能を BOM 運用下に新たに導入する事により、この SNMP トラップのパケットを受信し、Windows OS のイベントログにこれを出力し、これを OS 上のサービスやアプリケーションが出力する各種イベントログと統合し、BOM の基本機能であるイベントログ監視機能により統合監視する運用が可能となります。



SNMP トラップ受信機能の運用イメージ

※ SNMP トラップ受信機能が動作するサーバー上で、他の SNMP マネージャー等 SNMP トラップ受信を行うアプリケーションやサービスを同時に起動することはできません。(別の SNMP マネージャーやサービスでの使用するポートを既定の 162 から変更する事により共存可能となります。)

3. SNMP に関する基本事項

SNMP は「Simple Network Management Protocol」の略で、ネットワークにおける標準的な監視・管理用のプロトコルです。残念ながら現在ではその名の通りのシンプルでわかり易いものではなくなってしまっています。出発点こそシンプルだったのですが、その後の様々な拡張により複雑になっていった仕様、管理情報である MIB(Management Information Base)、異なるバージョンやその成立経緯など難解な状況になってしまっています。

本章では SNMP の基本事項に絞って簡単なご紹介をしていきます。

3.1. エージェントとマネージャー

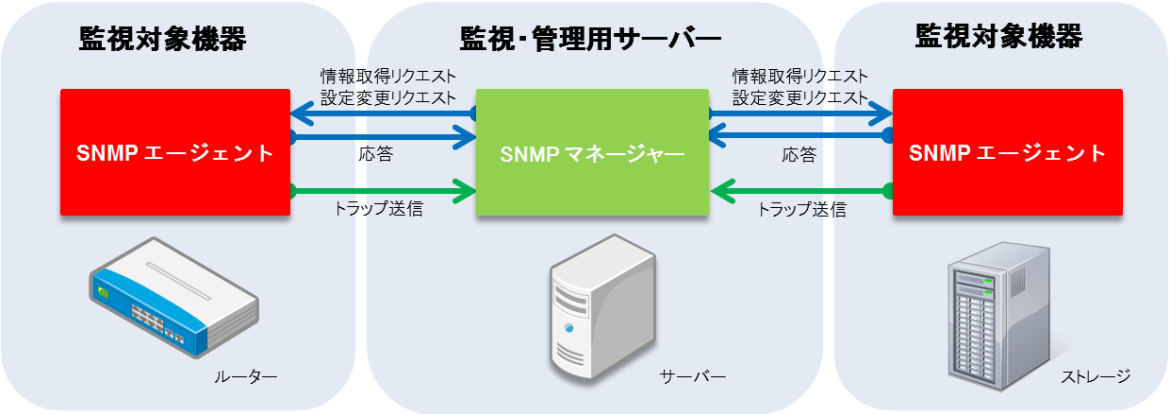
SNMP は監視対象となる機器で動作するエージェントと監視・管理ソフトウェア側であるマネージャーとの間で使用されるプロトコルになります。

エージェントとマネージャーの間で通信される情報を分類すると、大まかには以下の 3 種類となります。

－対象機器からの情報取得リクエスト(GetRequest)
マネージャーからエージェントに対して情報の提供を要求します。エージェントはそれに対して要求に応じた情報を返します。この情報取得リクエストは一定の間隔をおいて定期的にマネージャーより行われる事が一般的です。

－対象機器への設定変更リクエスト(SetRequest)
マネージャーからエージェントに対して対象機器の設定変更を要求します。エージェントはそれに対して設定変更を実行した上で、その結果を返します。

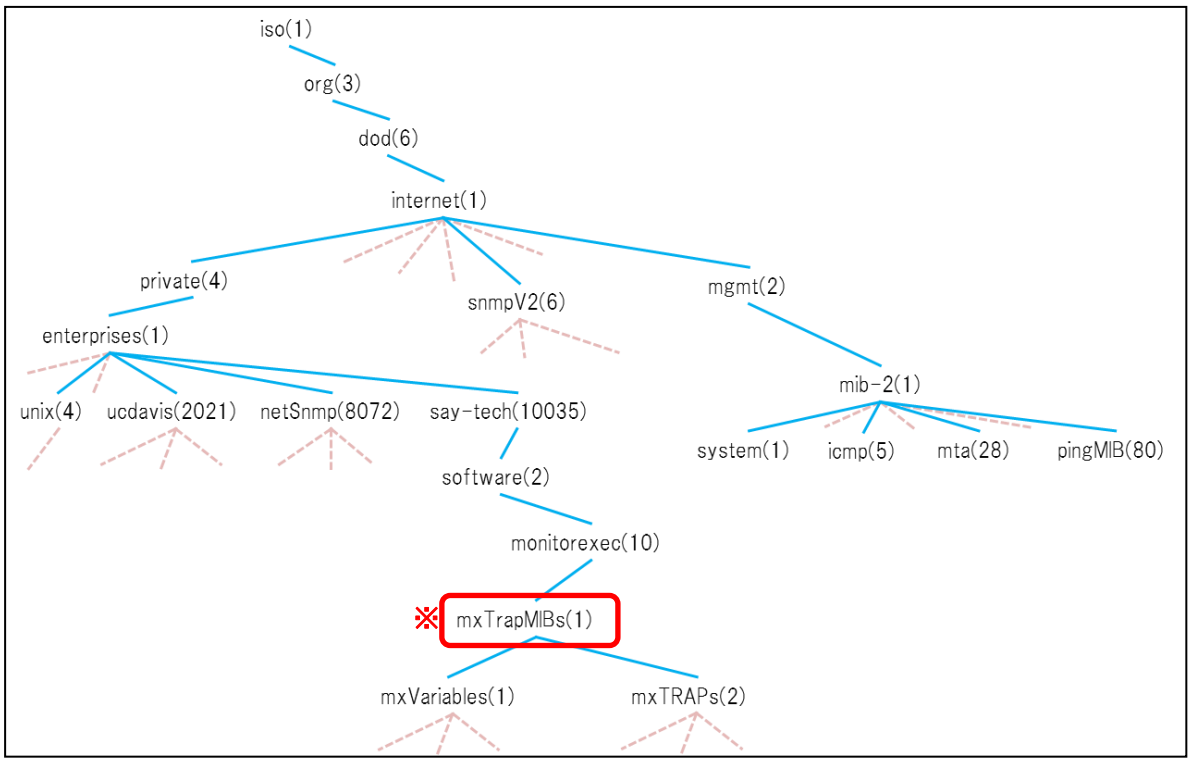
－対象機器からの状態変化の通知(Trap)
対象機器のエージェントが検知した各種イベントをマネージャーに通知するために使用されます。ただし応答確認のシーケンスが無いのでマネージャーに確実に届く保証はありません。この通知を SNMP トラップと呼びます。



SNMP におけるエージェントとマネージャー

3.2. MIB とは

SNMP に対応した各種機器はそれぞれの管理情報についてのデータベースを持っています。このデータベースには機器の状態や固有の情報などが管理されています。エージェントは、この管理情報データベースから必要な情報を引き出し、マネージャーに対して応答をします。マネージャーはこの管理情報を元にしてエージェントへ要求を出したり、エージェントからの情報を解析して異常個所の特定や判断をしたりします。この管理情報データベースを MIB(Management Information Base)と呼んでいます。
MIB は SMI(Structure of Management Information)と呼ばれる定義によって構成されており、個々の管理情報をツリー構造で管理しています。



MIB ツリー

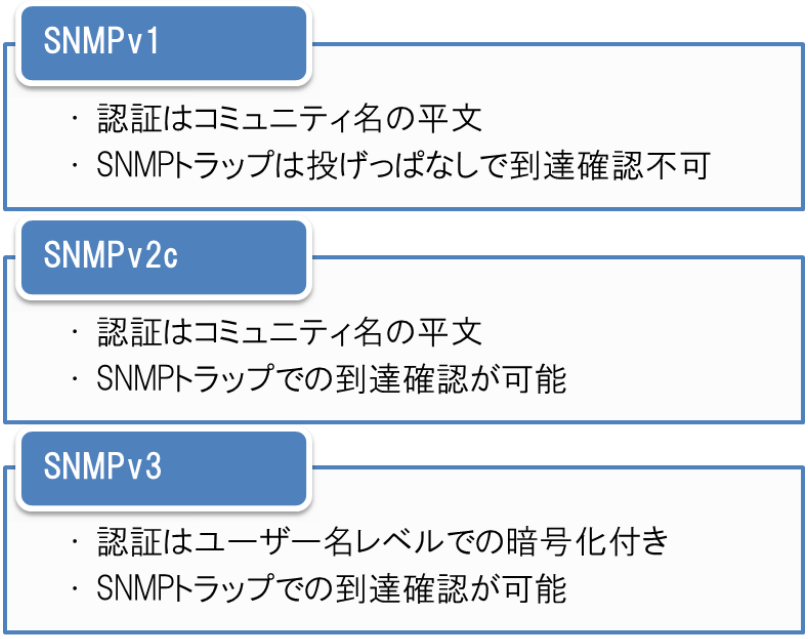
つまり SNMP とは MIB に規定されている情報を、エージェントが機器や OS から取得し、それをマネージャーへ送付するプロトコルとも言えます。

3.3. OID とは

MIB によって管理されている個々の情報をオブジェクト(Object)と呼びます。そのひとつひとつのオブジェクトを区別するために振られた識別子を OID(Object IDentifier)と呼んでいます。
OID は 1.3.6.1.・・・の様に、ピリオドで区切られた数字で表記されます。ピリオドで区切られた個々の数値は MIB のツリー構造の各階層に対応しています。
BOM での通知アクション機能の１つである SNMP トラップアクションは OID 1.3.6.1.4.1.10035.2.10.1 以下(「3.2 章 MIB とは」の図※印部分)に基づいた情報を送信している事になります。

3.4. SNMP のバージョン

SNMP には、大きく「SNMPv1」、「SNMPv2c」、「SNMPv3」の 3 つのバージョンが存在します。
それぞれのバージョンにおける差異は認証・暗号化と SNMP トラップになります。



SNMP バージョンの差異

① SNMPv1
1990 年に標準化されたバージョンで現在も広く採用されています。
GetRequest、GetNextRequest、GetResponse、SetRequest、Trap の５種の PDU(Protocol Data Unit)が定義されています。

※ PDU とはプロトコルが扱うデータの単位で、TCP/IP であれば「パケット」、Ethernet であれば「フレーム」になります。

② SNMPv2c
セキュリティ機能強化を目指したが、その多くは標準化に至りませんでした。ただトラップの再送確認などは盛り込まれました。
SNMPv1 の PDU から GetBulkRequest、InformRequest が加えられています。

③ SNMPv3
前バージョンの失敗を元に、セキュリティ強化をはかったバージョンで 2002 年に標準となりました。
コミュニティ単位ではなくユーザー単位でのパスワード認証やそのパスワードや PDU 全体への暗号化対応などがサポートされるようになりました。

※ SNMP トラップ受信機能が対応している 上記 SNMP のバージョンすべてに対応しています。

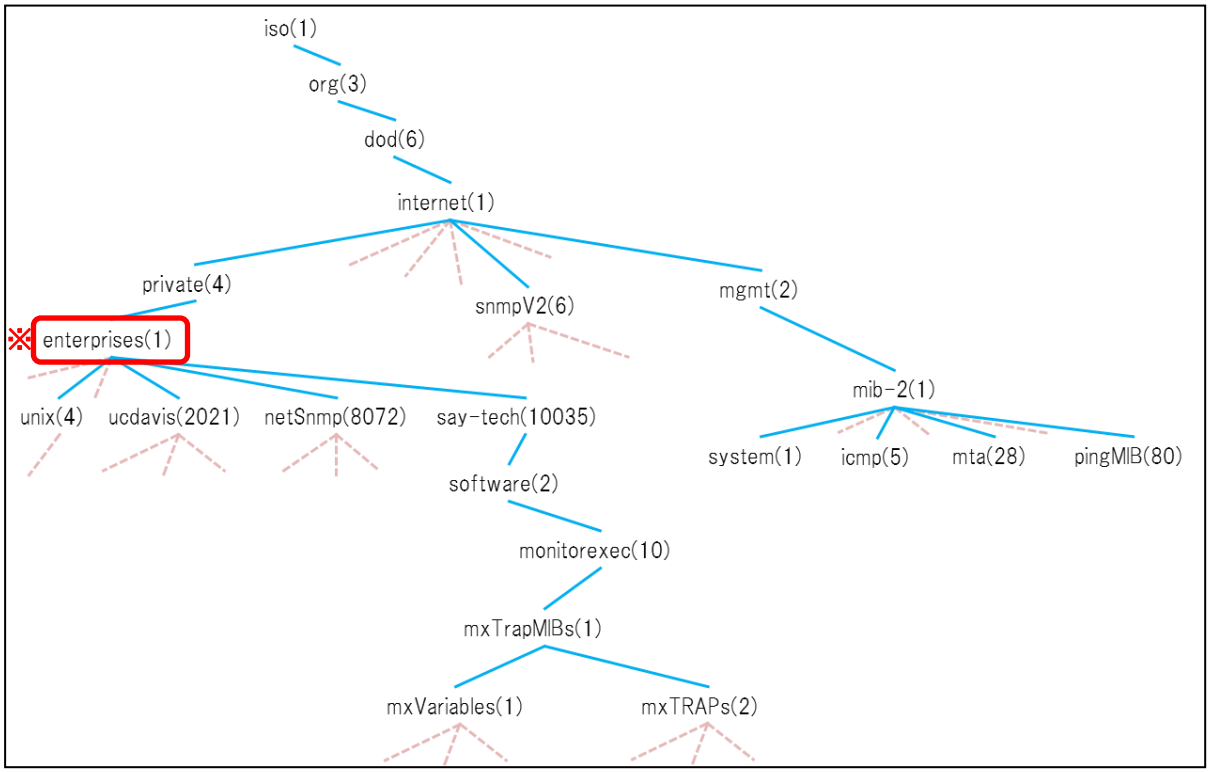
4. MIB ファイル徹底活用術

前章で MIB について簡単にご紹介しましたが、MIB の存在の意義などは今一歩と見えてこないと思います。また実際に MIB を活用するとは何をする事なのか？それはどうすれば良いのか？
本章では実際の MIB の運用方法に絞ってご紹介をしていきます。

4.1. 情報の受け手側にも MIB 情報を

情報の受け手側とは、一般的な SNMP の運用環境では SNMP マネージャーです。本書におけるその役割は BOM SNMP トラップ受信機能です。BOM SNMP トラップ受信機能であれ、SNMP マネージャーであれ、ある程度一般的な MIB に関してはあらかじめ情報を保持しています。ただし、各メーカー各機器の MIB に関しては必ずしも持ち合わせている訳ではありません。
ではそれらの MIB 情報はどうやって入手すれば良いのでしょうか。
実は機器ごとの MIB はメーカーがファイルとして公開している事が多いです。それを入手して情報の受け手側の環境に設定する事により、受け手側にも MIB に沿った運用が可能となるのです。

ここで書いた一般的な MIB とは“標準 MIB”と呼ばれています。それに対してメーカー・機器ごとの MIB については“プライベート MIB”、“独自 MIB”と呼ばれています。
以下の図での OID iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). (※部分)以下がメーカー独自に定義・作成できる部分になります。



MIB ツリー

メーカーの製品には多種多様なものがあり、MIB もそれに応じて複数種類存在します。本書では以下の連携をご説明します。

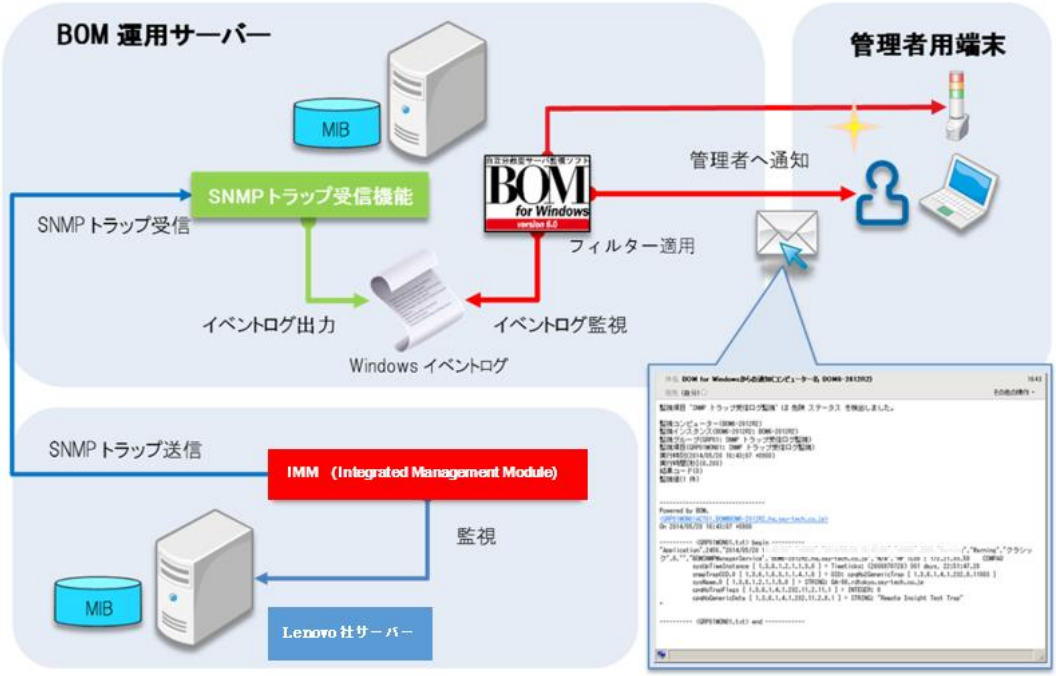
① Lenovo System x サーバーの MIB の設定と BOM との連携（5 章）
② Flex System x エンタープライズ・シャーシとの連携（6 章）
③ Lenovo Networking スイッチ関連との連携（7 章）
④ IBM Storwize との連携（8 章）

本書で対象となる Lenovo 製品は以下の通りです。

製品	対象 MIB
Lenovo System x サーバー	IMM / IMM2
Flex System x	CMM / CMM2
Lenovo Networking スイッチ	Lenovo RackSwitch G8052
IBM Storwize	IBM Storwize V7.6.0

5. Lenovo System x サーバーとの連携

本章では実際の Lenovo System x サーバー搭載の IMM / IMM2 と言う専用管理ツールによる監視・管理機能との連携パターンをご紹介していきます。
この IMM / IMM2 はサーバー本体のシステムとは完全に独立しており、専用の LAN ポートも兼ね備えていますので、サーバー本体のトラブル時にでも利用する事が可能です。



Lenovo 社サーバー搭載 IMM / IMM2 との連携パターン

5.1. Lenovo System x サーバーとの連携環境の構築手順

今回連携環境を構築する Lenovo 社製サーバー機は x3650 M5 で、当該機に Integrated Management Module(IMM) 2 が搭載されています。 (IMM 自体の持つ NIC の IP アドレスは 192.168.124.42)。また BOM 運用サーバーの OS には Windows Server 2012 R2 Datacenter エディションを入れています(こちらの IP アドレスは 192.168.124.100)。

手順は簡単には以下の通りになります。

① BOM の運用サーバーに BOM の本体並びに SNMP トラップ受信機能をインストール
② BOM サーバーに IMM2 の MIB ファイルを追加
③ SNMP トラップ受信サービスに IMM2 からのトラップを受信するように設定
④ BOM の監視サービスで受信トラップを出力したイベントログを検知する監視項目設定(テンプレート)
⑤ IMM2 の SNMP トラップ送信先として BOM サーバーの IP アドレス、コミュニティ名などを設定

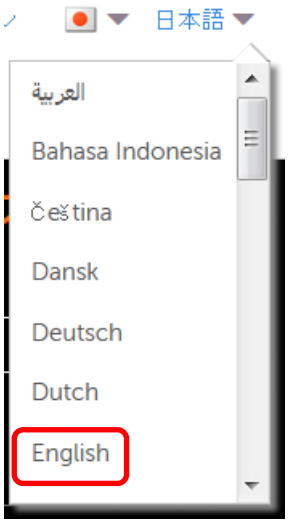
この手順のうち、②の IMM2 の MIB ファイル設定と⑤の IMM2 側でのトラップ送信先設定の 2 つに関しては、もう少し具体的に次章より補足したいと思います。

5.2. IMM / IMM2 関連 MIB ファイルの導入の内容

Lenovo System x サーバー製品用の MIB ファイルは自社サーバー用管理監視ソフト向けに提供されている Integrated Management Module 2（IMM2） のファームウェアを展開して入手した MIB ファイルを利用します。

① 以下のページにアクセスします。
Lenovo Support
http://support.lenovo.com/jp/ja/

② 右上の言語選択から[English]を選択します。

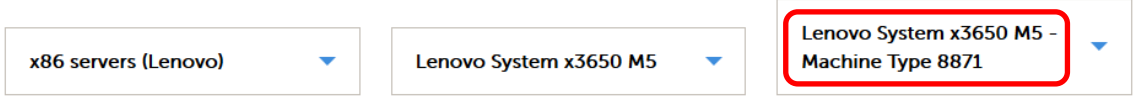


http://support.lenovo.com/jp/en/

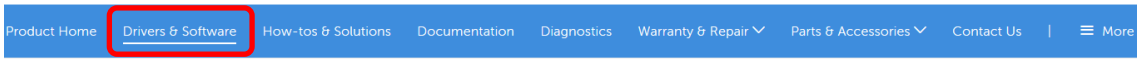
③ [Servers]をクリックします。
Select Series から[x86 servers (Lenovo)]を選択します。

④ Select Sub-Series から該当するマシン・シリーズを選択します。
例）Lenovo System x3650 M5

⑤ Select Machine Type から該当するマシン・タイプを選択します。
例）Lenovo System x3650 M5 – Machine Type 8871



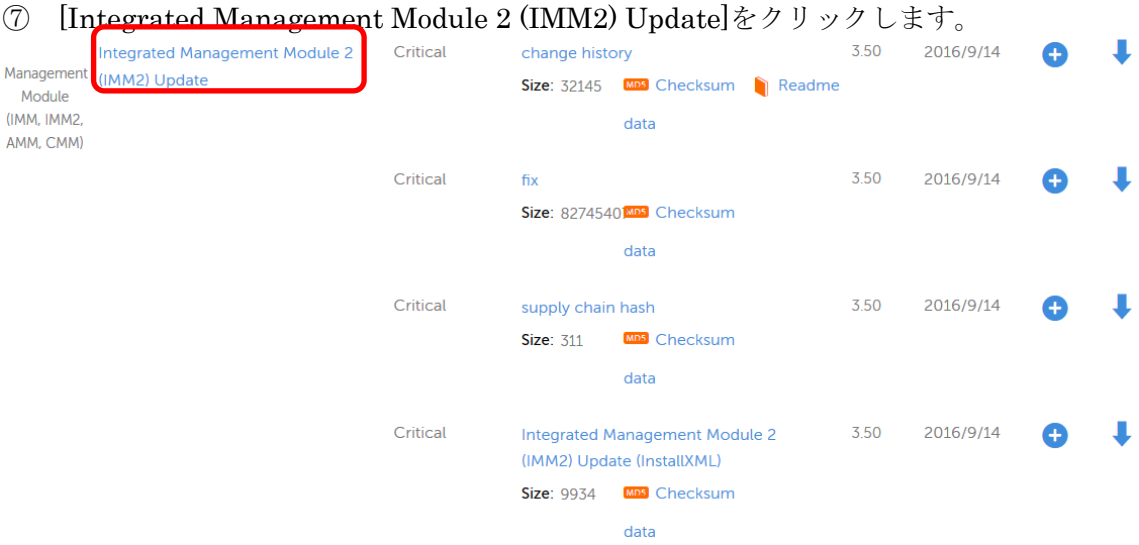
① [Drivers & Software]をクリックします。



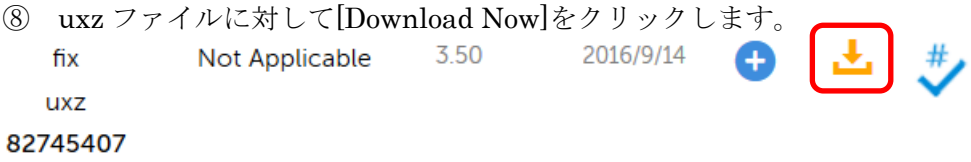
⑥ Component から[Management Module (IMM, IMM2, AMM, CMM)]を選択します。

Operating System から[Pick an OS]を選択します。

⑦ [Integrated Management Module 2 (IMM2) Update]をクリックします。



⑧ uxz ファイルに対して[Download Now]をクリックします。



⑨ Lenovo 社製 IMM2 のファームウェアをダウンロードし、ファームウェアの拡張子を uxz 形式から zip 形式に名前変更します。zip ファイルを展開することで、最新の MIB ファイルである imm.mib と immalert.mib を入手します。

5.3. MIB ファイルの設定

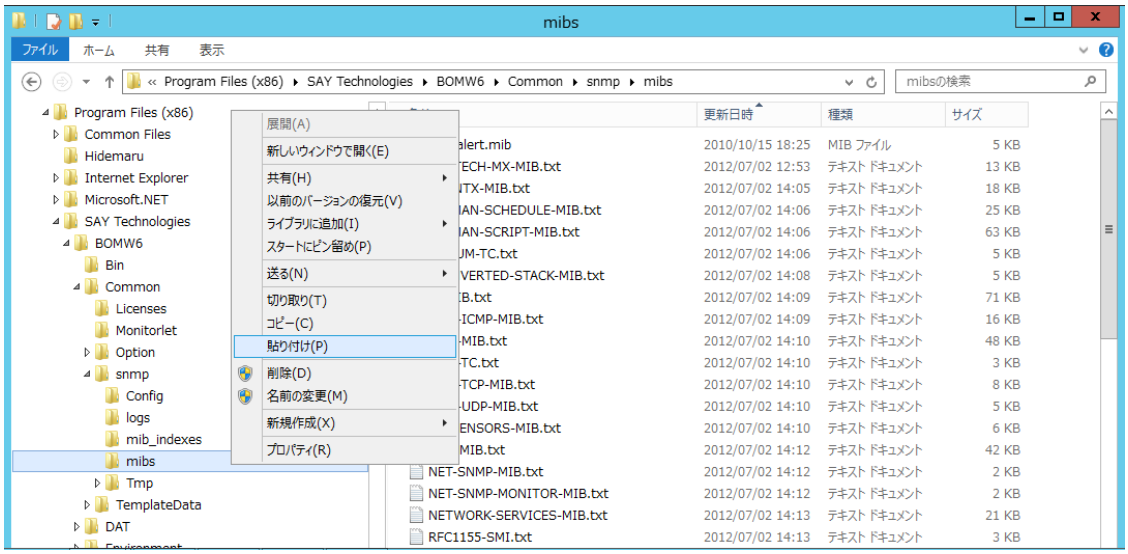
取得した MIB ファイル群を BOM の既定のフォルダーに保存します。そして保存したファイルを BOM SNMP トラップ受信機能に反映させるためには、BOM SNMP トラップ受信サービスの再起動を行います。

以下流れに沿って簡単にご案内します。

① BOM 指定のフォルダーへ保存するため、コピーをします。

MIB ファイルのコピー

② 貼り付けをします。



MIB ファイルの貼り付け

③ BOM SNMP トラップ受信サービスを再起動します。

BOM 6.0 コントロールパネル(停止前)

BOM 6.0 コントロールパネル(開始前)

これで Lenovo System x サーバーの MIB ファイル（IMM / IMM2 の MIB ファイル）が BOM SNMP トラップ受信サービスに反映されました。実際にこれらのファイルを BOM サーバーに導入し、SNMP トラップ受信サービスを再起動すると BOM サーバーでの設定は終了です。

5.4. IMM / IMM2 のコンソール

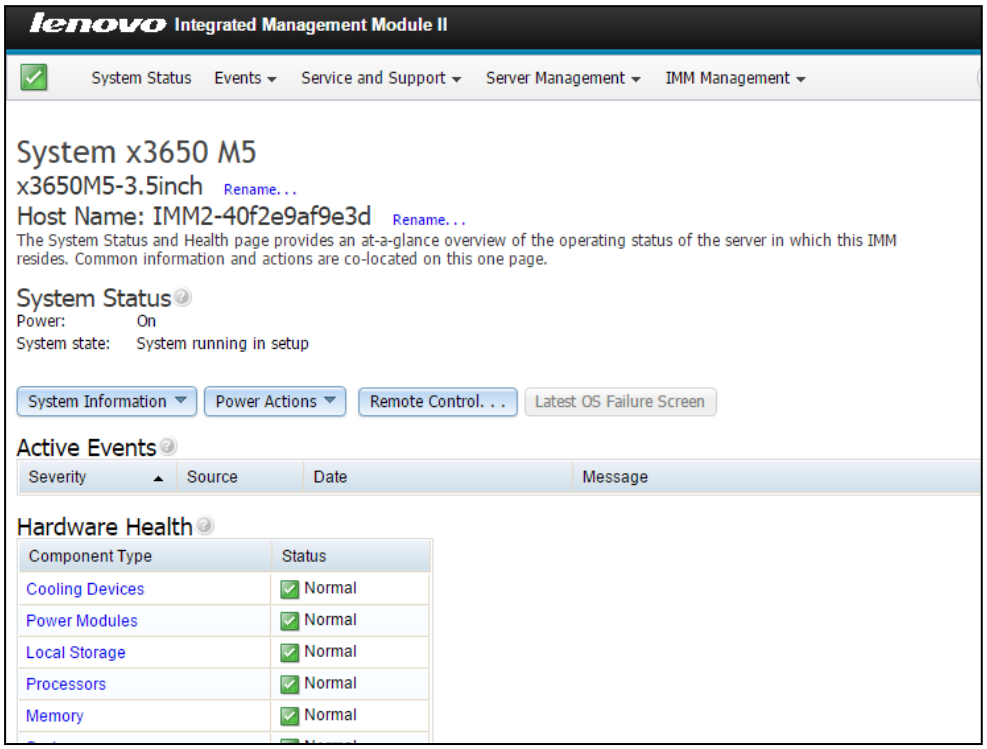
BOM と IMM / IMM2 を連携するには、IMM / IMM2 での設定が必要です。まずは IMM / IMM2 に接続して設定を行います。IMM / IMM2 は Web 経由でアクセスをしますので、コンソールは Web ブラウザーになります。

ユーザー名とパスワードを入力してログインします。

IMM / IMM2 コンソールのログイン画面

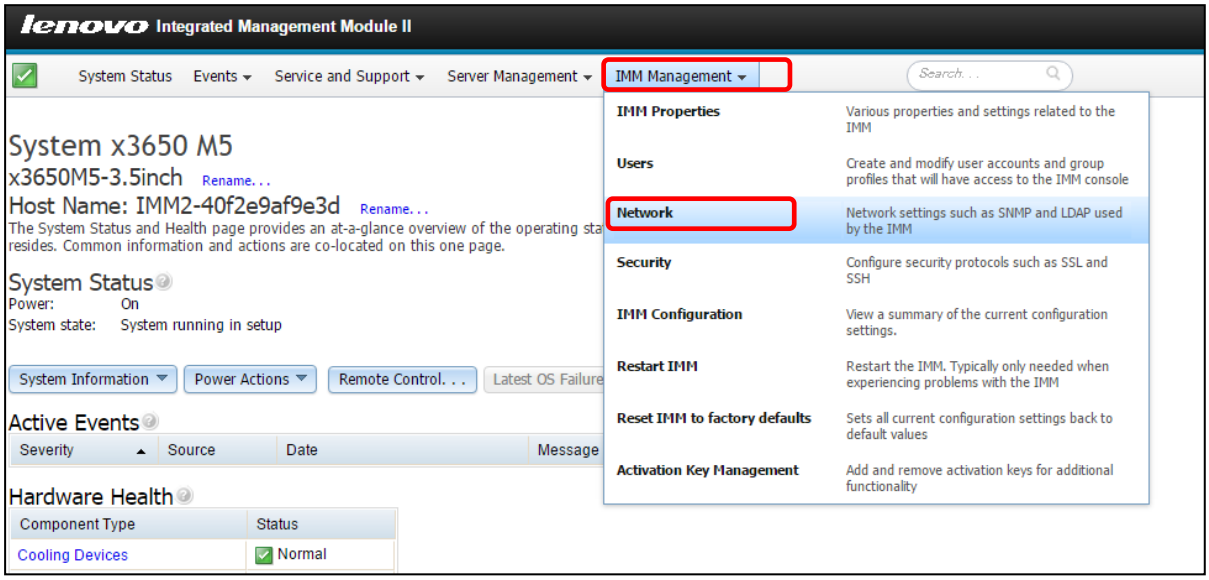
5.5. IMM / IMM2 での SNMP トラップ送信指定

① IMM / IMM2 のコンソールにログインをすると以下の様な画面へ移ります。ここでは Lenovo 製サーバー機の製品名、IMM / IMM2 で管理できるシステム状況が視認可能となっています。



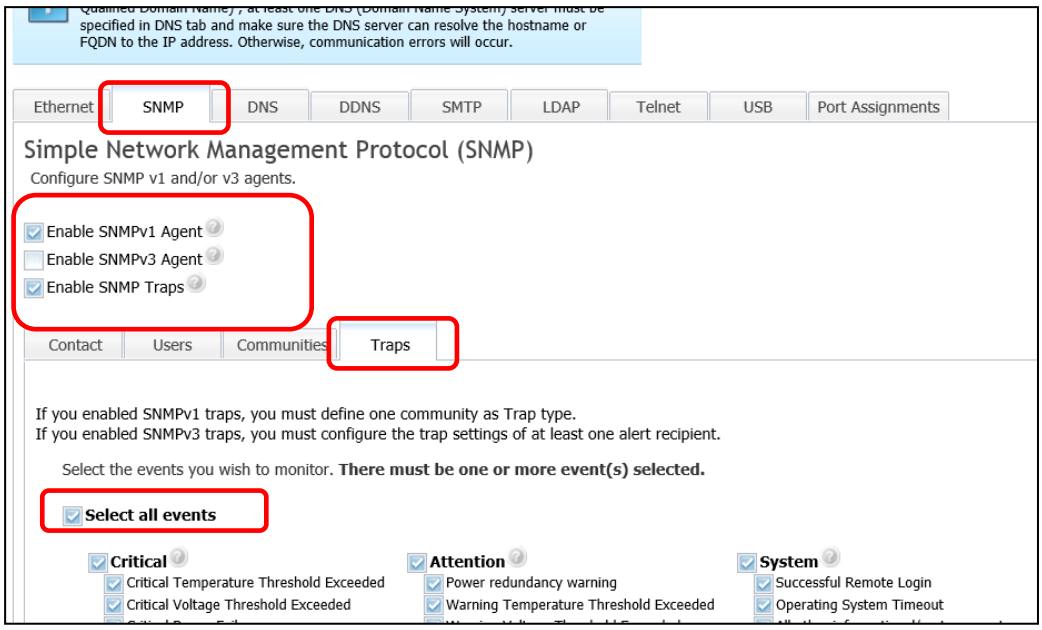
IMM / IMM2 ログイン直後のコンソール画面(システム状況を確認できます)

② SNMP トラップ送信設定をする場合には上部メニューの赤く囲った部分である [IMM Management]-[Network] をクリックします。



SNMP 関連の設定画面の選択

③　SNMP 関連のネットワークの設定を行います。[SNMP]タブをクリックし、赤く囲った部分を設定します。

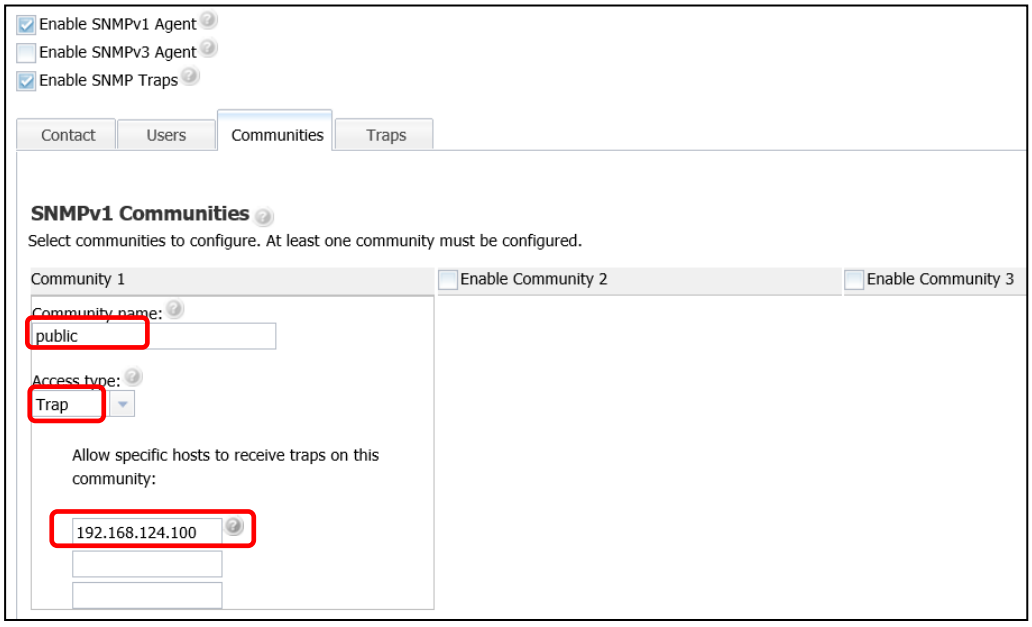


SNMP Trap 送信内容の設定

④　[Enable SNMPv1 Agent] と [Enable SNMP Traps] をクリックします。

⑤　何をトリガーに Trap 送信するかを[Traps]タブ 内でチェックします。本例では、すべてのイベントを Trap 送信するよう設定しています。

⑥　SNMPv1 の Trap 設定をします。[Comuunities]タブを開きます。



SNMPv1 のコミュニティ設定

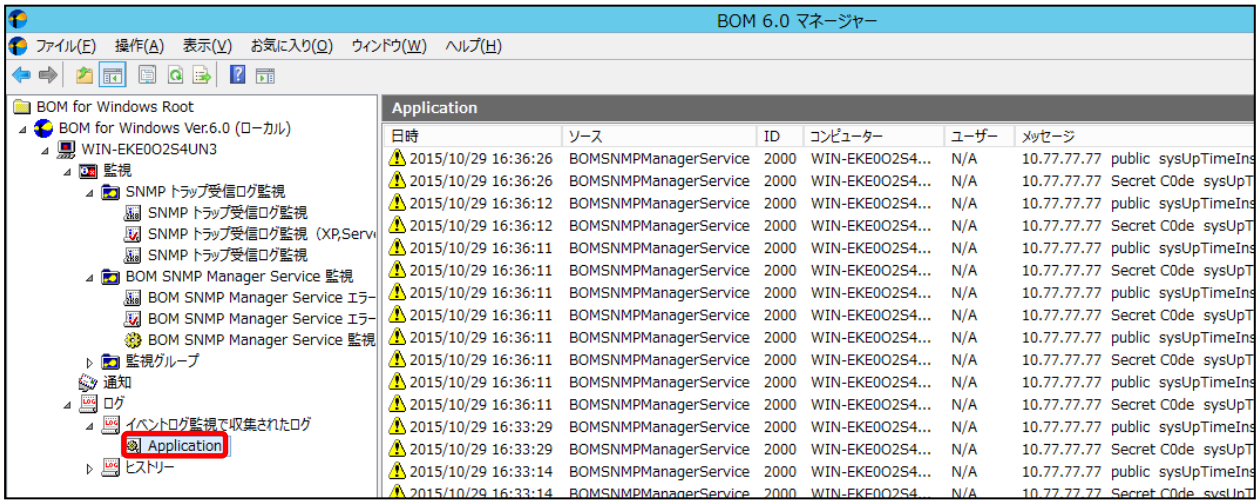
⑦　BOM サーバーで設定したコミュニティ名を[Community name]に設定します。本例では「public」になっています。

⑧　Access Type を「Trap」に設定します。

⑨　Trap 送信先(BOM サーバーの IP アドレス)を設定します。本例では、192.168.124.100 です。

5.6. トラップを受信、検知、メールを送信

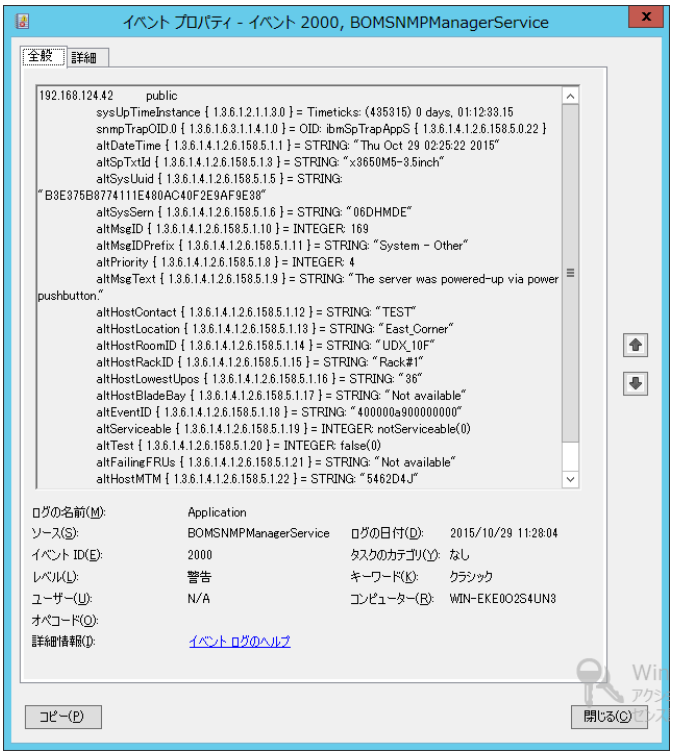
5.6 までの操作で SNMP トラップ受信機能が受信し Windows イベントログに出力をします。そして BOM の基本機能であるイベントログ監視によってこれを検知します。検知したログは BOM 6.0 マネージャーのイベントログ監視で収集されたログの配下の Application ノードを表示する事によって確認ができます。



日時	ソース	ID	コンピューター	ユーザー	メッセージ
⚠ 2015/10/29 16:36:26	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:26	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:12	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:12	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:33:29	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:33:29	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:33:14	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:33:14	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT

BOM 6.0 マネージャーにて収集された SNMP トラップを受信、出力されたイベントログ

その内の 1 つを詳しく見てみましょう。リザルトペイン(画面右側)よりレコードを 1 つ選びそのプロパティを開きます。

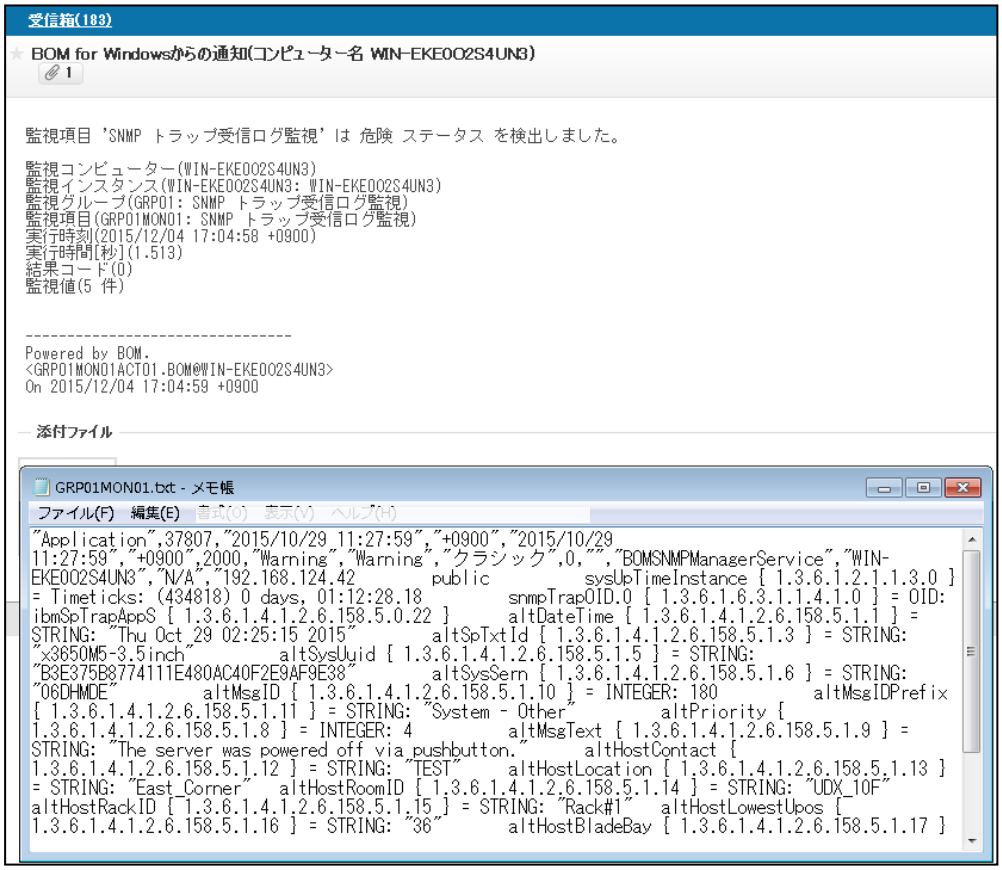


検知収集されたイベントログの詳細

SNMP トラップ受信機能からのイベントログ出力時のログの名前はアプリケーション、ソースは「BOMSNMPManagerService」、イベント ID は 2000、レベルは「警告」、ユーザーは N/A のそれぞれ固定となります。

トラップ発信元の IMM / IMM2 などの情報は説明欄であるログ本文に書かれています。

次に BOM から検知収集したこのイベントログをメールで送信します。
わかり易いように検知したイベントログをメール本文に添付ファイルとして送信をします。そしてそれをメールソフトにて受信した図が以下になります。

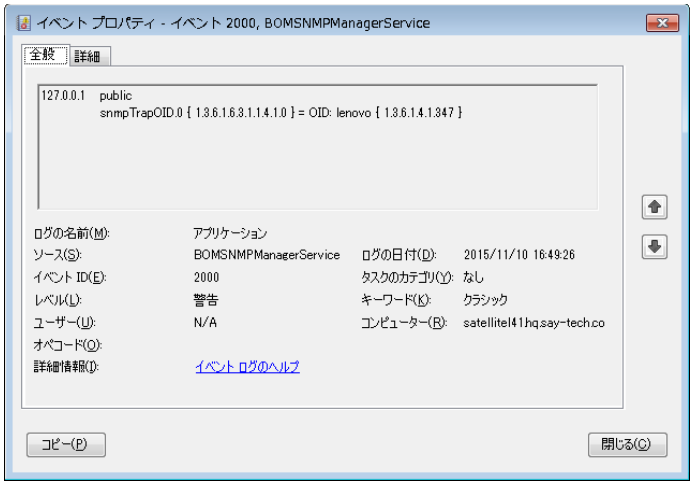


BOM からの通知メール(下部が添付されたイベントログのテキストファイル)

5.7. MIB ファイルで何が変わった？

前章にて MIB ファイルの適用方法などをご紹介しましたが、実際にはどのように変わるのでしょうか？ MIB ファイルが無いと BOM の SMMP トラップ受信機能ではトラップは受信不可能なのでしょうか？
そんな事はありません。BOM の SMMP トラップ受信機能では受信するトラップに応じた MIB ファイルの設定がされていなくても、受信自体は何の問題もなく行われます。もちろんイベントログへの出力も実行されます。
それでは受信トラップに応じた MIB ファイルの有無で何が変わるのでしょうか？実際に比較するのが一番わかり易いと思いますので以下をご参照ください。

これは BOM で検知収集したある Lenovo 用 MIB ファイル設定時のイベントログの詳細画面の抜粋です。



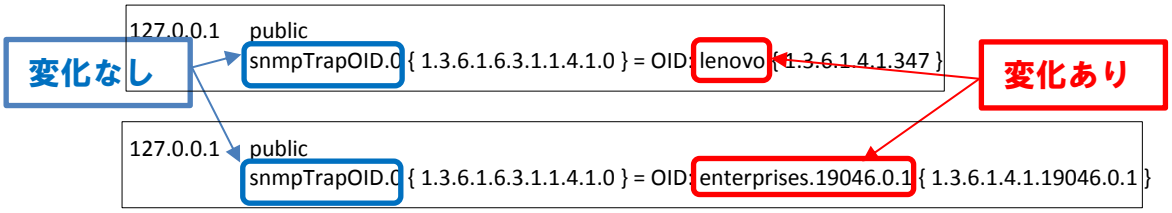
MIB ファイル設定時の画面

これに比べて Lenovo 用 MIB ファイルを未設定の場合は以下の様になります。

MIB ファイル未設定時の画面

どこが違うのでしょうか？何が違うかをわかり易く拡大したものが以下になります。

MIB ファイル設定



MIB ファイル未設定

赤い囲みが MIB ファイル設定の有無によって変わる部分になります。MIB ファイルによって定義される Lenovo 社製固有の部分が、設定済みの方は文字列が具体的に表示されていますが、MIB ファイル未設定の方は一部未定義部分が OID のまま表示されていることがわかります。標準 MIB で定義されている enterprises までが表示さており、そこから先が OID の数字のままになっています。
それとは対照的に青い囲みの部分は双方に違いがありません。この部分は標準 MIB で定義されている部分にあたるので違いが見られない訳です。

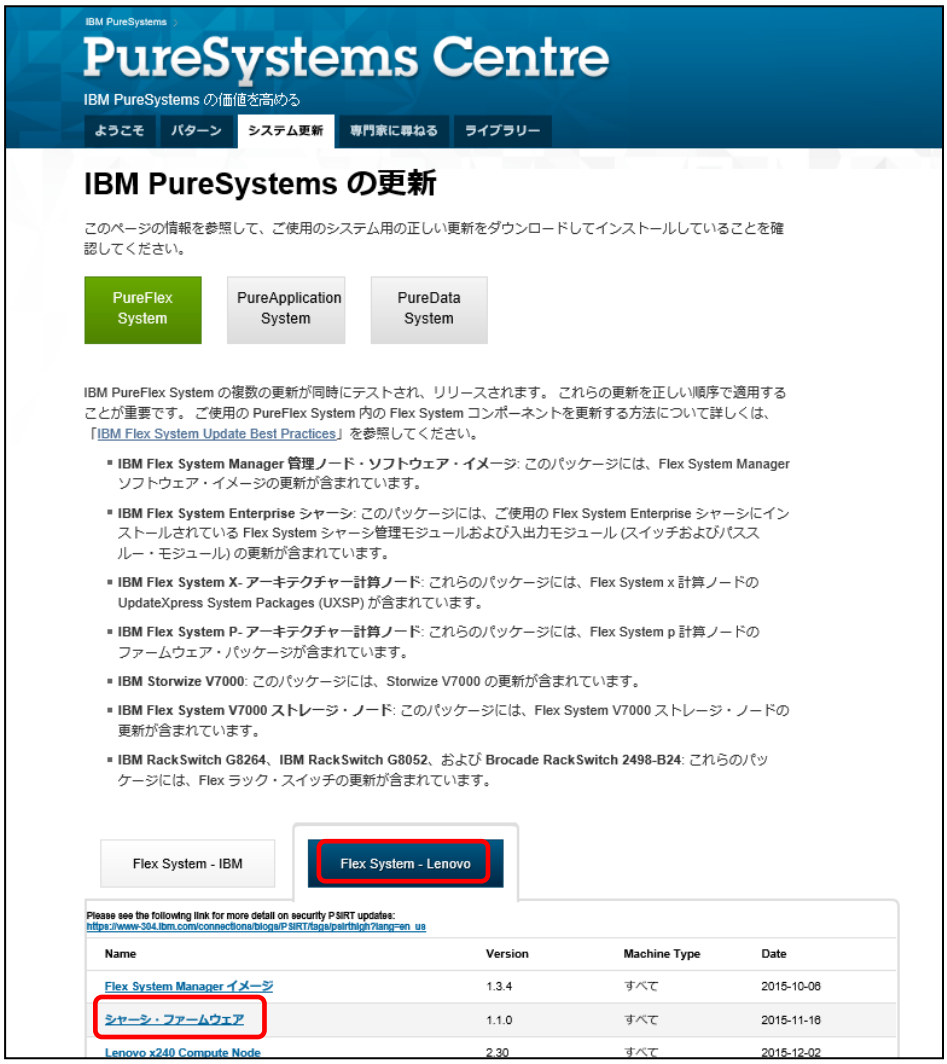
6. Flex System x エンタープライズ・シャーシとの連携

6.1. CMM / CMM2 の MIB 入手方法

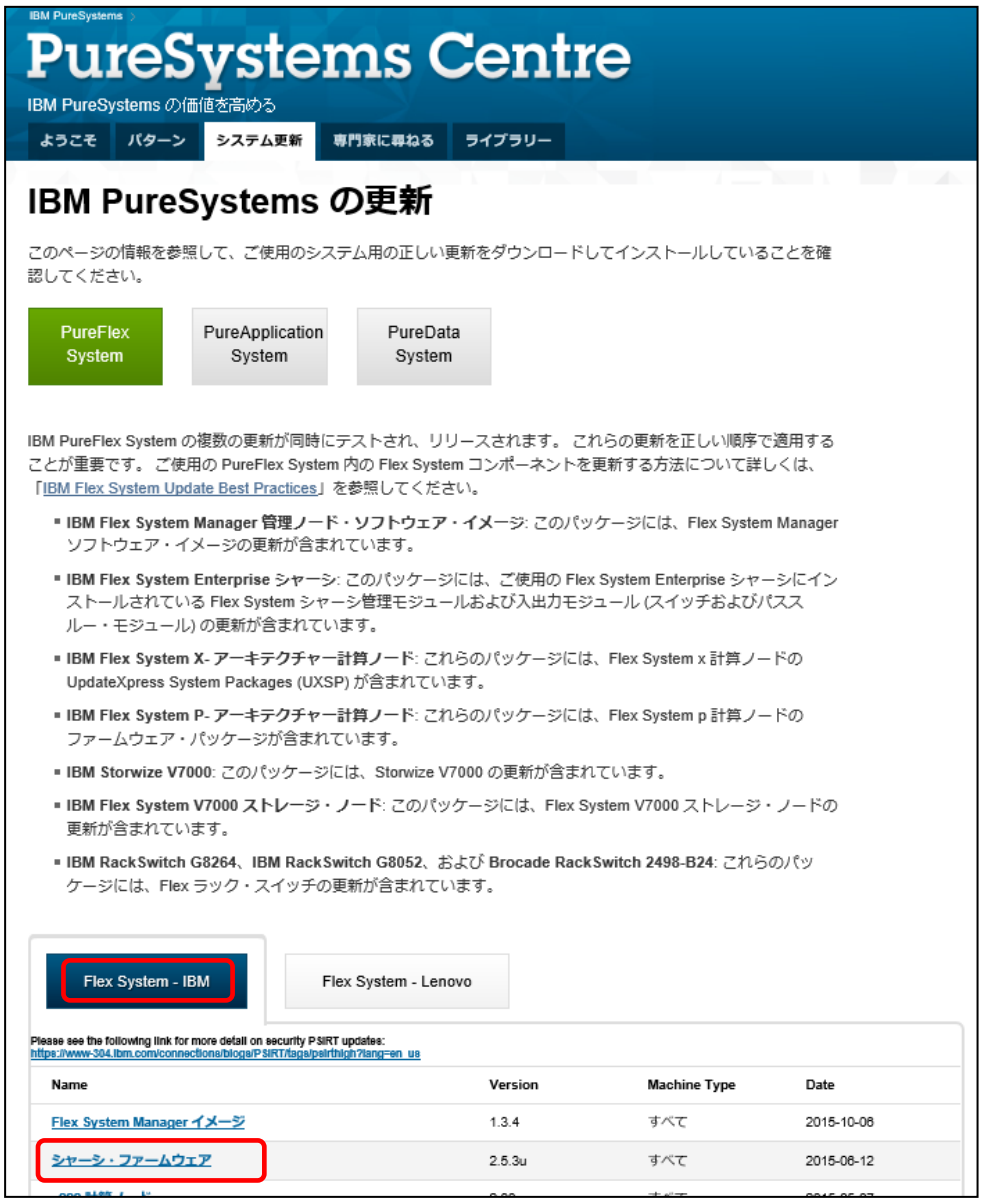
CMM / CMM2 の MIB ファイルは、CMM / CMM2 のファームウェア更新パッケージ(zip ファイル)に同梱されています。SNMP トラップ用の MIB ファイル名は「mmalert.mib」です。
CMM / CMM2 ファームウェア更新パッケージのダウンロードページは、Flex System 更新スタック掲載サイトにリンクが掲載されています。

① 以下ページにアクセスします。（IBM ID が必要です）
PureSystems Updates
https://www.ibm.com/software/brandcatalog/puresystems/centre/update

② CMM2
“Flex System ～ Lenovo”タブを選択し、”シャーシ・ファームウェア” をクリックして、リンク先の FixCentral web サイトからダウンロードします。



③ CMM
“Flex System ～ IBM”タブを選択し、”シャーシ・ファームウェア” をクリックして、リンク先の FixCentral web サイトからダウンロードします。



④　CMM / CMM2 共通
マシン・コードのアップデートが指定され、インストールされるマシン (各「ターゲット・マシン」) のシリアル番号を入力してからダウンロードしてください。

⑤　MIB ファイルの設定につきましては「5.3 章 MIB ファイルの設定」をご参照ください。

6.2. CMM / CMM2 の SNMP トラップ送信指定

CMM / CMM2 で検知したイベントを SNMP トラップとして BOM に通知するには、CMM Web UI で以下を設定します。

① イベント通知先の作成
② 通知するイベントの指定・フィルタリング
③ SNMP トラップの設定
　トラップの有効化
　Community 名の指定
　トラップ通知先 SNMP マネージャー（BOM サーバー）の IP アドレスの指定

詳しい手順は下記資料をご参照ください。

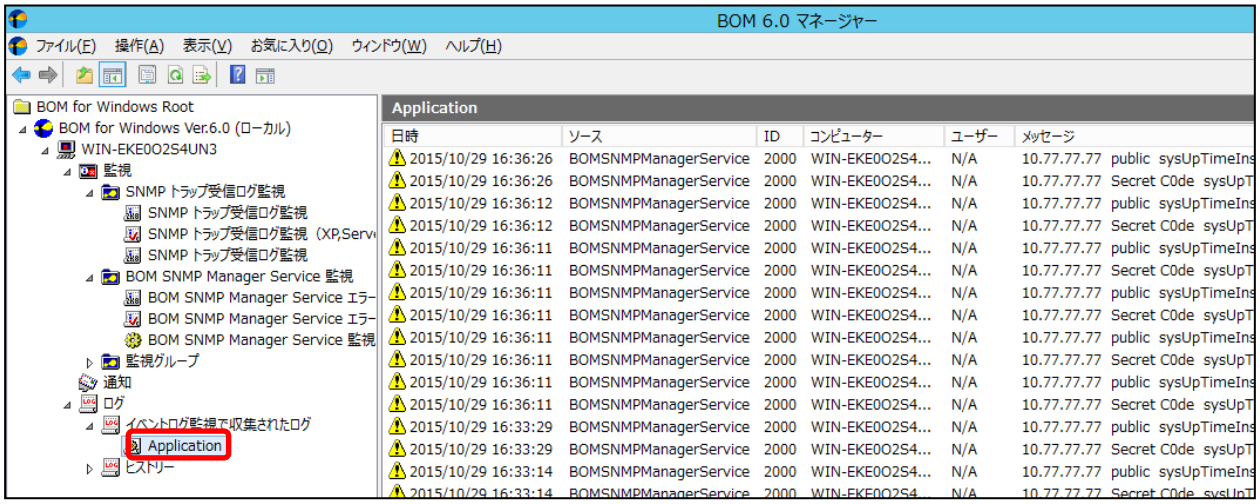
Flex System シャーシ・マネジメント・モジュールを使用したハードウェア監視 (2015 年 5 月 15 日)
p14-p16
http://www.lenovojp-cms.com/cmscontents/gdfiles.php?md=167

なお BOM が対応する SNMP v1 でトラップを送信するためには、CMM / CMM2 のセキュリティ・ポリシーが“Legacy”で設定されている必要があります。デフォルトではよりセキュアな“Secure”が設定されています。変更手順は以下をご参照ください。
Flex System InfoCenter > CMM2 > Using the Web interface > Web interface options > CMM management options
http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.lenovo.acc.cmm.doc/cmm_ui_mgt_module_management.html
Flex System InfoCenter > CMM > Using the Web interface > Web interface options > CMM management options
http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.cmm.doc/cmm_ui_mgt_module_management.html

各セキュリティ・ポリシーの詳細は以下をご参照ください。
Flex System InfoCenter > CMM 2 > Configuring the CMM > CMM security > Security policies
http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.lenovo.acc.cmm.doc/cmm_security_policies.html
Flex System InfoCenter > CMM > Configuring the CMM > CMM security > Security policies
http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.cmm.doc/cmm_security_policies.html

6.3. トラップを受信、検知

CMM / CMM2 からトラップが送信されると SNMP トラップ受信機能が受信し Windows イベントログに出力をします。そして BOM の基本機能であるイベントログ監視によってこれを検知します。検知したログは BOM 6.0 マネージャーのイベントログ監視で収集されたログの配下の Application ノードを表示する事によって確認ができます。



日時	ソース	ID	コンピューター	ユーザー	メッセージ
⚠ 2015/10/29 16:36:26	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:26	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:12	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:12	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:33:29	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:33:29	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
⚠ 2015/10/29 16:33:14	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
⚠ 2015/10/29 16:33:14	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT

BOM 6.0 マネージャーにて収集された SNMP トラップを受信、出力されたイベントログ

その内の 1 つを詳しく見てみましょう。リザルトペイン(画面右側)よりレコードを 1 つ選びそのプロパティを開きます。

```
192.168.70.100        public
          sysUpTimeInstance { 1.3.6.1.2.1.1.3.0 } = Timeticks: (7238131) 0 days, 20:06:21.31
          snmpTrapOID.0 { 1.3.6.1.6.3.1.1.4.1.0 } = OID: mmTrapAppS { 1.3.6.1.4.1.2.6.158.3.0.22 }
          spTrapDateTime { 1.3.6.1.4.1.2.6.158.3.1.1.1 } = STRING: "YYYY-MM-DDThh:mm:ssZZZ=
2015-10-29T06:04:27GMT"
          spTrapAppId { 1.3.6.1.4.1.2.6.158.3.1.1.2 } = STRING: "Lenovo Flex Chassis Management
Module"
```

ログの名前(M): Application
ソース(S): BOMSNMPManagerService
ログの日付(D): 2015/10/29 15:04:51
イベント ID(E): 2000
タスクのカテゴリ(Y): なし
レベル(L): 警告
キーワード(K): クラシック
ユーザー(U): N/A
コンピューター(R): WIN-EKE0O2S4UN3
オペコード(O):
詳細情報(I): イベント ログのヘルプ

検知収集されたイベントログの詳細

SNMP トラップ受信機能からのイベントログ出力時のログの名前はアプリケーション、ソースは「BOMSNMPManagerService」、イベント ID は 2000、レベルは「警告」、ユーザーは N/A のそれぞれ固定となります。

トラップ発信元の CMM / CMM2 などの情報は説明欄であるログ本文に書かれています。

イベントログのメール送信につきましては「5.6 章トラップを受信、検知、メールを送信」、MIB ファイルの適用で変更した内容につきましては「5.7 章ファイルで何が変わった？」をご参照ください。

7. Lenovo Networking スイッチ関連との連携

7.1. Lenovo Networking スイッチ関連 MIB ファイルの導入

Lenovo Networking スイッチ製品用の MIB ファイルは、Lenovo Networking スイッチのファームウェア更新パッケージ（zip ファイルもしくは tgz ファイル）に同梱されています。

① 以下ページにアクセスします。
Fix Central（IBM 社製 MIB ファイルを含んだ MIB Kit のダウンロードサイト）
https://www-933.ibm.com/support/fixcentral/

② 製品グループから「Lenovo RackSwitches and Storage devices」を選択し、機種名、ソフトウェア・バージョンを選択後、「次へ進む」を選択します。

③ 該当のフィックスパックをダウンロードします。

④　ダウンロード方式を選択して「次へ進む」を選択します。

⑤　「今すぐダウンロード」を選択します。

⑥　zip ファイルもしくは tgz ファイルを展開し、最新の MIB ファイルを入手します。

⑦　MIB ファイルの設定につきましては「5.3 章 MIB ファイルの設定」をご参照ください。

7.2. SNMP の設定方法

Lenovo Networking スイッチのコマンド・ライン・インターフェース
BOM と Lenovo Networking スイッチを連携するには、コマンド・ライン・インターフェース（CLI）での設定が必要です。今回は、Tera Term(http://www.forest.impress.co.jp/library/software/utf8teraterm/) を用い、Lenovo RackSwitch G8052 の IP インターフェースに Telnet 接続して設定する方法を記載いたします。
G8052 スイッチを管理実行するための IP インターフェース 1 の設定ですが、工場出荷時の設定値は以下になります。

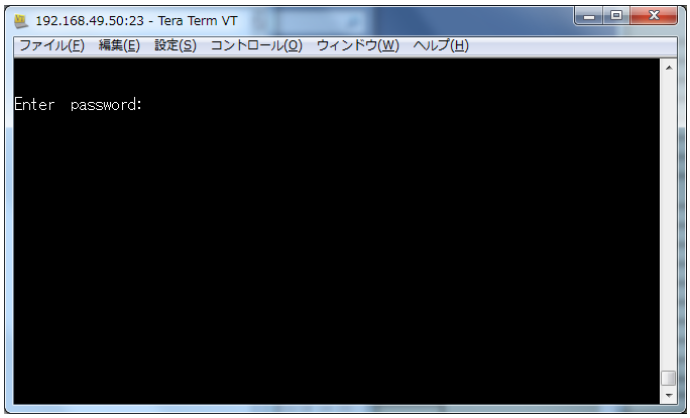
- IP アドレス: 192.168.49.50
- サブネットマスク: 255.255.255.0
- DHCP : Enabled

設定の詳細については、以下サイトに記載の各製品の初期設定ガイドをご参照ください。

Lenovo Networking はじめての導入セットアップ・ガイド
http://www.lenovojp.com/server/technical/gd-networking.shtml

① Tera Term で以下の通り入力しログインします。

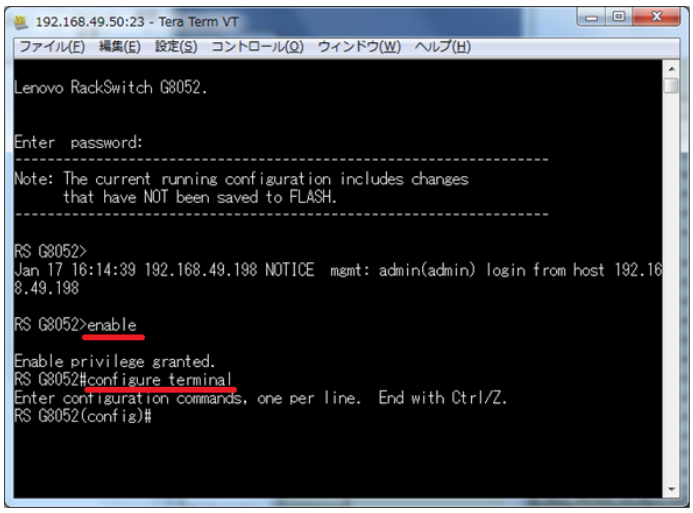
② ログインパスワードを入力します。（デフォルト値は admin です）



Lenovo Networking スイッチでの SNMP トラップ送信指定

コマンド・ライン・インターフェースにログインをすると以下の様な画面へ移ります。

③　「enable」と入力後、「configure terminal」と入力し、グローバル・コンフィギュレーション・モードに入ります。



④　IP アドレスの変更が必要な場合、以下を実行します（本例では、IP アドレスを 192.168.124.10、サブネットマスクを 255.255.255.0 に変更します）。設定反映後、Tera Term との接続が一旦切れた場合、再度新 IP アドレスでご接続下さい。
RS G8052(config)#interface ip 1
RS G8052(config-ip-if)#ip address 192.168.124.10 255.255.255.0 enable

⑤　SNMPv1 の Trap 設定をします。まず、BOM サーバーで設定したコミュニティ名を指定します。（本例では「public」です。こちらは当機器のデフォルト値の為必ずしも設定を行う必要はありません）
RS G8052(config)#snmp-server read-community public

⑥　トラップ送信元のインターフェース番号を指定します。本例では「1」です。
RS G8052(config)#snmp-server trap-source 1

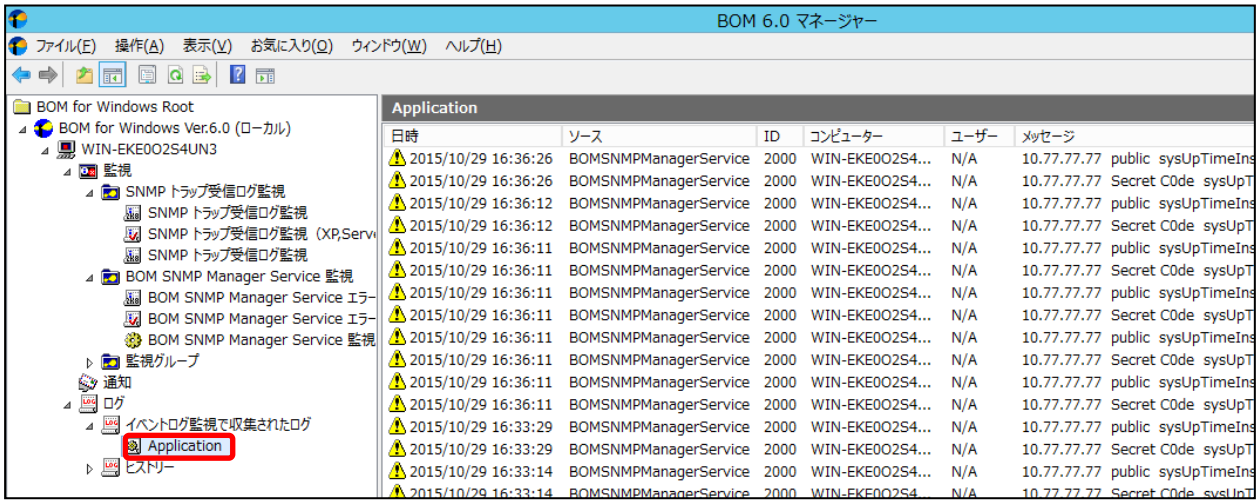
⑦　Trap 送信先(BOM サーバーの IP アドレス)を設定します。本例では、192.168.124.100 です。
RS G8052(config)#snmp-server host 192.168.124.100 public

⑧　設定内容を確認する際は、「show running-config」および「show snmp-server」を実行します。

⑨　再起動後も設定を維持したい場合は、「write」と入力し設定を保存して下さい。

7.3. トラップを受信、検知

Lenovo Networking スイッチからトラップが送信されると SNMP トラップ受信機能が受信し Windows イベントログに出力をします。そして BOM の基本機能であるイベントログ監視によってこれを検知します。検知したログは BOM 6.0 マネージャーのイベントログ監視で収集されたログの配下の Application ノードを表示する事によって確認ができます。



日時	ソース	ID	コンピューター	ユーザー	メッセージ
2015/10/29 16:36:26	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:26	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:12	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:12	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:33:29	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:33:29	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:33:14	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:33:14	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT

BOM 6.0 マネージャーにて収集された SNMP トラップを受信、出力されたイベントログ

その内の 1 つを詳しく見てみましょう。リザルトペイン(画面右側)よりレコードを 1 つ選びそのプロパティを開きます。

```
192.168.49.50        public
           sysUpTimeInstance { 1.3.6.1.2.1.1.3.0 } = Timeticks: (51732000) 5 days, 23:42:00.00
           snmpTrapOID.0 { 1.3.6.1.6.3.1.1.4.1.0 } = OID: linkUp { 1.3.6.1.2.1.11.0.3 }
           ifIndex.129 { 1.3.6.1.2.1.2.2.1.1.129 } = INTEGER: 129
           ifAdminStatus.129 { 1.3.6.1.2.1.2.2.1.7.129 } = INTEGER: up(1)
           ifOperStatus.129 { 1.3.6.1.2.1.2.2.1.8.129 } = INTEGER: up(1)
           ifDescr.129 { 1.3.6.1.2.1.2.2.1.2.129 } = STRING: Ethernet1
```

ログの名前(M):	Application		
ソース(S):	BOMSNMPManagerService	ログの日付(D):	2015/10/29 16:06:17
イベント ID(E):	2000	タスクのカテゴリ(Y):	なし
レベル(L):	警告	キーワード(K):	クラシック
ユーザー(U):	N/A	コンピューター(R):	WIN-EKE0O2S4UN3
オペコード(O):			
詳細情報(I):	イベント ログのヘルプ		

検知収集されたイベントログの詳細

SNMP トラップ受信機能からのイベントログ出力時のログの名前はアプリケーション、ソースは「BOMSNMPManagerService」、イベント ID は 2000、レベルは「警告」、ユーザーは N/A のそれぞれ固定となります。

トラップ発信元の Lenovo Networking スイッチ などの情報は説明欄であるログ本文に書かれています。

イベントログのメール送信につきましては「5.6 章トラップを受信、検知、メールを送信」、MIB ファイルの適用で変更した内容につきましては「5.7 章ファイルで何が変わった？」をご参照ください。

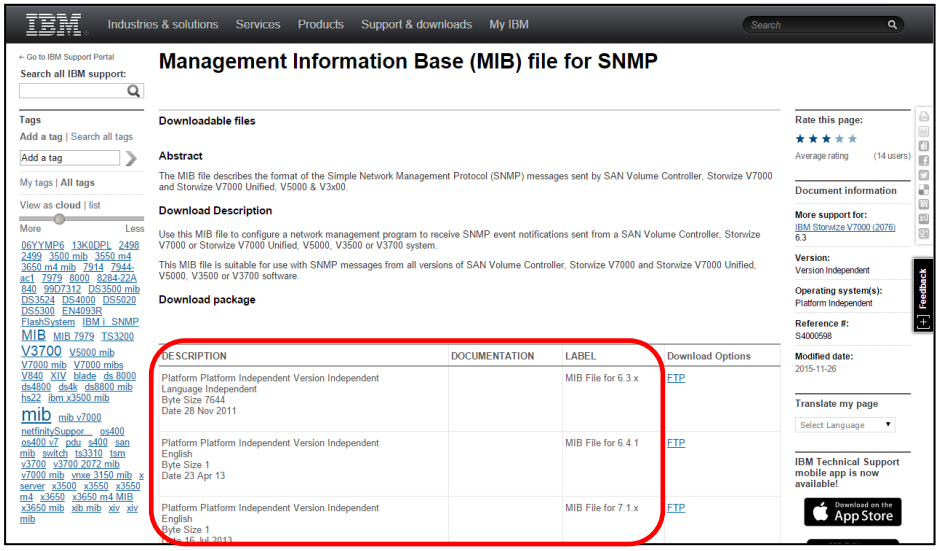
8. IBM Storwize との連携

8.1. IBM Storwize の MIB ダウンロード

MIB ファイルは、IBM Storwize V3700, V5000, V7000 で共通です。
MIB ファイルは、以下のサイトからダウンロードできます。
Management Information Base (MIB) file for SNMP

① 以下ページにアクセスして、対象 MIB ファイルをダウンロードします。
http://www-01.ibm.com/support/docview.wss?uid=ssg1S4000598

MIB ファイル名の例
V7.6.0 の場合は、SVC_MIB_7.6.0.MIB

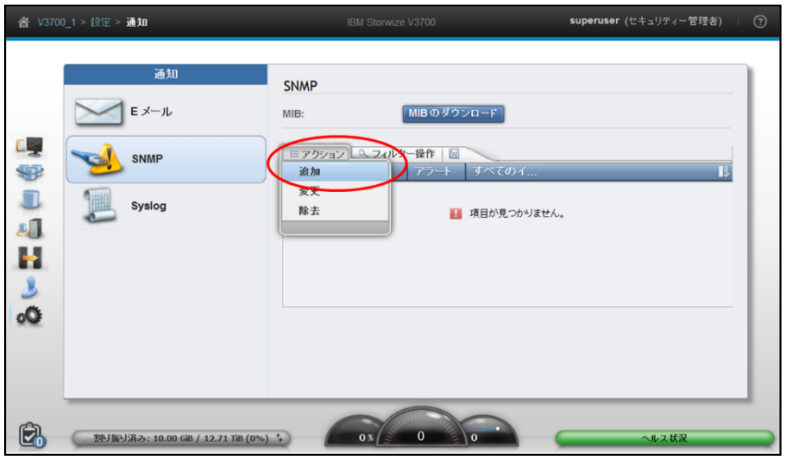


② MIB ファイルの設定につきましては「5.3 章 MIB ファイルの設定」をご参照ください。

8.2. SNMP サーバーの設定

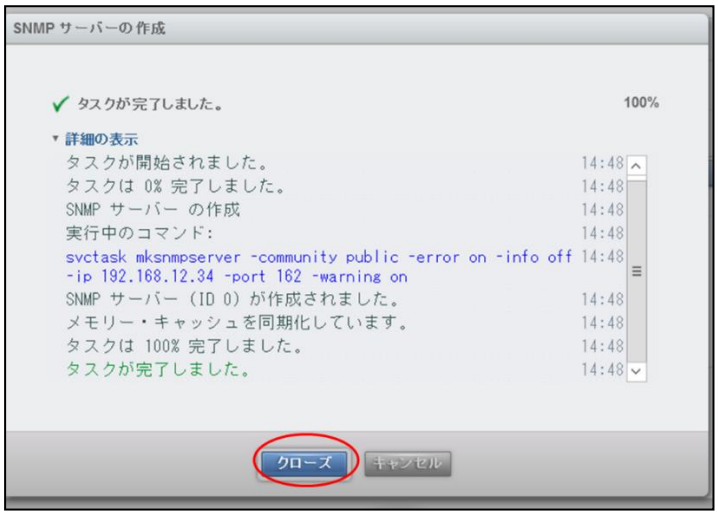
① 「設定」→「通知」→「SNMP」を選択します。

② 「アクション」→「追加」を選択します。

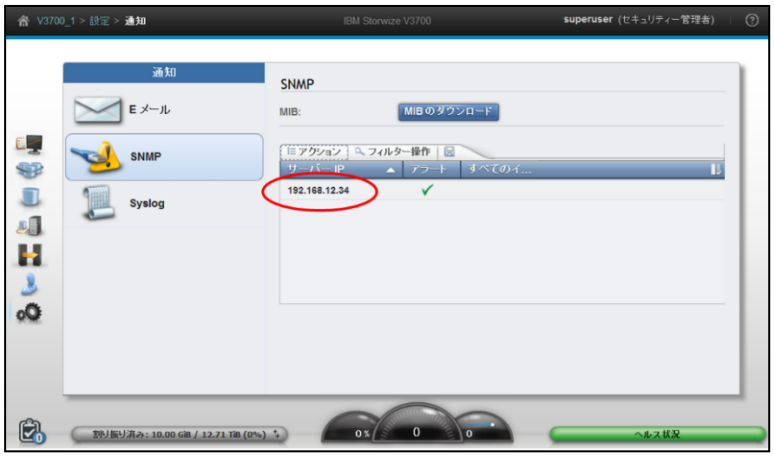


③ サーバー名、ポート、コミュニティ、イベントを適宜設定し、「追加」をクリックします。

④　SNMP サーバーが作成されたら、「クローズ」をクリックします。

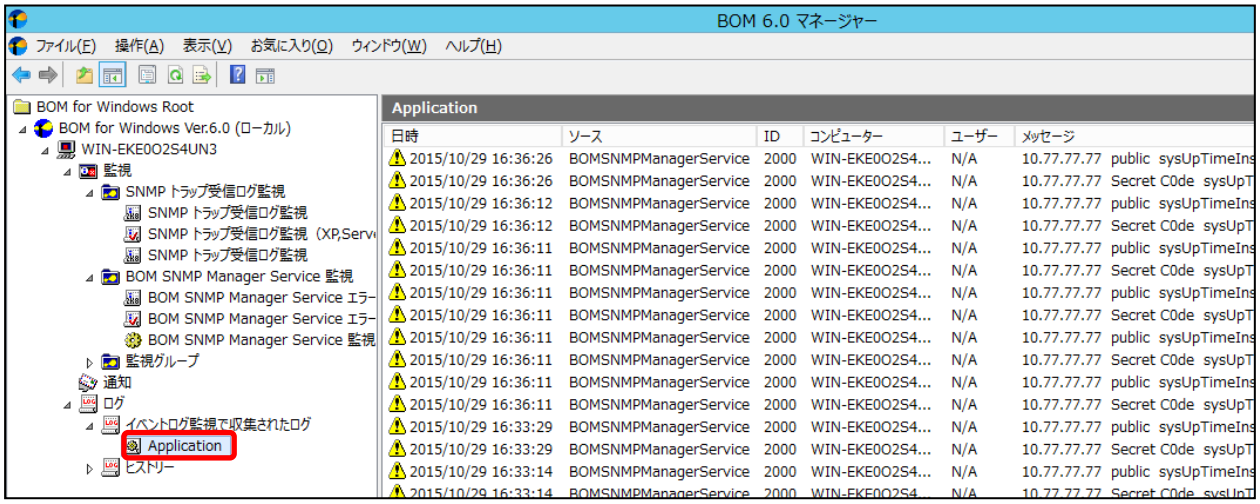


⑤　サーバーIP が追加されたことを確認します。



8.3. トラップを受信、検知

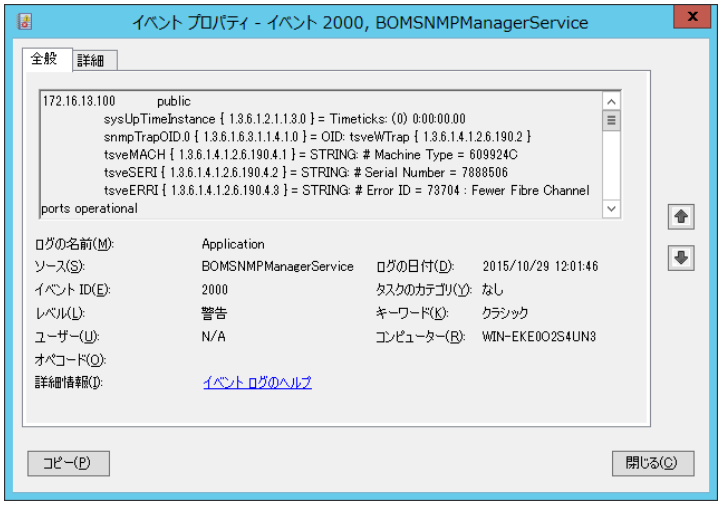
IBM Storwize からトラップが送信されると SNMP トラップ受信機能が受信し Windows イベントログに出力をします。そして BOM の基本機能であるイベントログ監視によってこれを検知します。検知したログは BOM 6.0 マネージャーのイベントログ監視で収集されたログの配下の Application ノードを表示する事によって確認ができます。



日時	ソース	ID	コンピューター	ユーザー	メッセージ
2015/10/29 16:36:26	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:26	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:12	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:12	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:36:11	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:33:29	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:33:29	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT
2015/10/29 16:33:14	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 public sysUpTimeIns
2015/10/29 16:33:14	BOMSNMPManagerService	2000	WIN-EKE0O2S4...	N/A	10.77.77.77 Secret C0de sysUpT

BOM 6.0 マネージャーにて収集された SNMP トラップを受信、出力されたイベントログ

その内の 1 つを詳しく見てみましょう。リザルトペイン(画面右側)よりレコードを 1 つ選びそのプロパティを開きます。



```
172.16.13.100          public
          sysUpTimeInstance { 1.3.6.1.2.1.1.3.0 } = Timeticks: (0) 0:00:00.00
          snmpTrapOID.0 { 1.3.6.1.6.3.1.1.4.1.0 } = OID: tsveWTrap { 1.3.6.1.4.1.2.6.190.2 }
          tsveMACH { 1.3.6.1.4.1.2.6.190.4.1 } = STRING: # Machine Type = 609924C
          tsveSERI { 1.3.6.1.4.1.2.6.190.4.2 } = STRING: # Serial Number = 7888506
          tsveERRI { 1.3.6.1.4.1.2.6.190.4.3 } = STRING: # Error ID = 73704 : Fewer Fibre Channel
ports operational
```

ログの名前(M): Application
ソース(S): BOMSNMPManagerService
ログの日付(D): 2015/10/29 12:01:46
イベント ID(E): 2000
タスクのカテゴリ(Y): なし
レベル(L): 警告
キーワード(K): クラシック
ユーザー(U): N/A
コンピューター(R): WIN-EKE0O2S4UN3
オペコード(O):
詳細情報(I): イベント ログのヘルプ

検知収集されたイベントログの詳細

SNMP トラップ受信機能からのイベントログ出力時のログの名前はアプリケーション、ソースは「BOMSNMPManagerService」、イベント ID は 2000、レベルは「警告」、ユーザーは N/A のそれぞれ固定となります。

トラップ発信元の IBM Storwize などの情報は説明欄であるログ本文に書かれています。

イベントログのメール送信につきましては「5.6 章トラップを受信、検知、メールを送信」、MIB ファイルの適用で変更した内容につきましては「5.7 章ファイルで何が変わった？」をご参照ください。

9. SNMP Trap v3 の受信

5 章から 8 章でご紹介した Lenovo 製品の SNMP トラップ送信は v1 あるいは v2c でした。v3 のトラップ受信をするためには、v3 受信のための設定が必要になります。v3 はトラップ送信元と送信先でユーザー認証方式と暗号化を指定し、セキュアなトラップ通信を可能にするものです。

トラップ送信元の Lenovo 製品の SNMP トラップ v3 設定については、各 Lenovo 製品の設定をご確認ください。受信設定方法の詳細はマニュアルをご参照ください。

SNMP Trap v3 の受信に必要な、SNMP v3 トラップ対象のエンジン ID、認証方式、暗号化方式の設定を以下のファイルで指定します。対象 SNMP 機器 1 台につき 1 行で指定します。エンジン ID については送信元 SNMPv3 の特有の ID になります。送信元の Lenovo 製品をご確認ください。

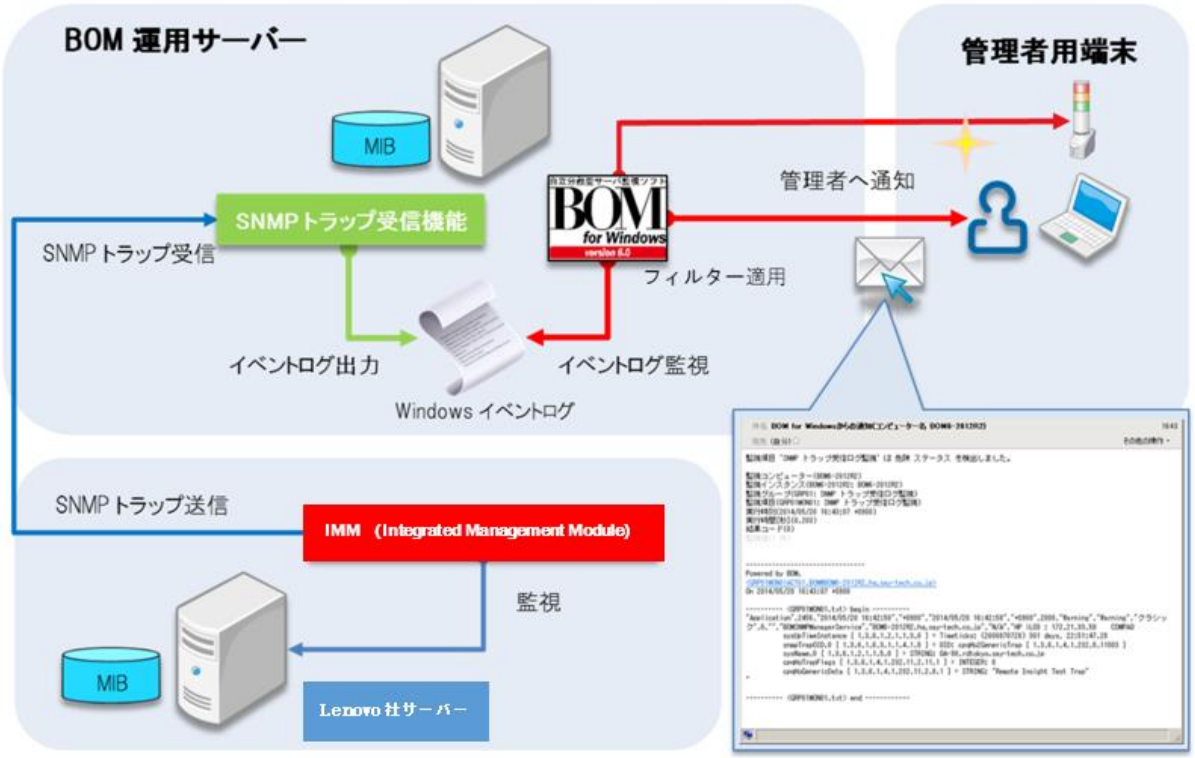
また、SNMP GetRequest により、エンジン ID を取得することも可能です。SNMP GetRequest については、「12.SNMP トラップ受信サービスの起動時の動作」をご参照ください。

10. SNMP Trap のフィルタリング

5 章から 8 章で Lenovo 製品の SNMP トラップの送信と、BOM SNMP マネージャーサービスによるトラップ受信を説明しました。
ここでは、IMM / IMM2 を例として、さらに実践的な運用パターンとして、以下のシナリオで、実際に受信した SNMP トラップのフィルタリング、分析、重要なメッセージの分類と、イベントログ監視のキーワードによるフィルター設定をご説明します。他の製品についても同様にフィルタリングすることは可能です。

【フィルタリングのシナリオ】

① SNMP トラップのフィルタリングとイベントログレベル変更の設定
② SNMP トラップ受信機能でイベントログへ書き出し、BOM でログの収集
③ 項番②を一定期間運用し、SNMP トラップ受信により書き出されたログを蓄積する
④ SNMP トラップのログを精査、重要度の高いログに特徴的なメッセージを拾い出す
⑤ 特徴的なメッセージをイベントログ監視のキーワードに設定した監視項目を作成



以下にご紹介する内容は本章の為に準備した環境下での検証結果に基づいており、広く一般的な運用方法の保証している訳ではございません。実際には、それぞれの環境に沿った情報の収集や動作の確認を行った上での運用をお願い致します。

10.1.SNMP トラップ受信機能でのトラップフィルタリングとイベント種類指定

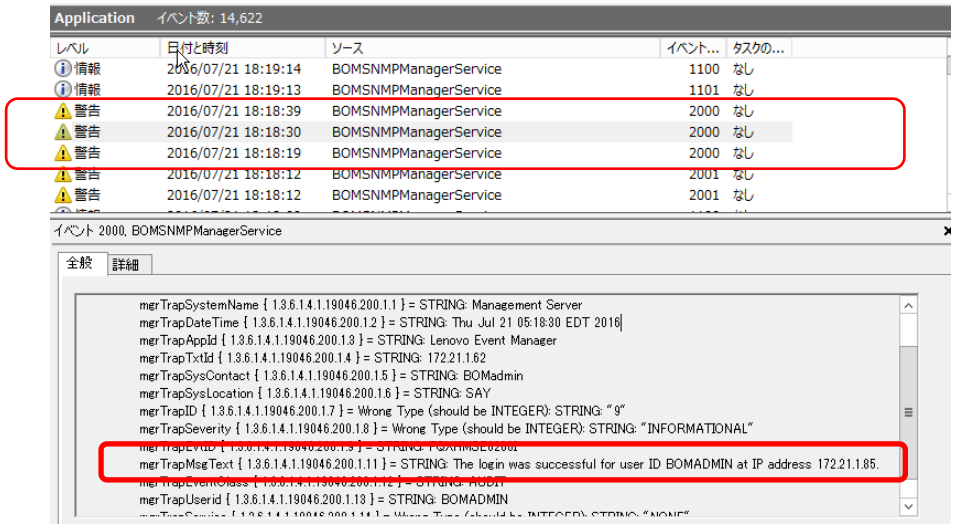
SNMP トラップ受信機能により受信した内容をフィルタリングして Windows イベントログに出力をすることが可能です。また、Windows イベントログに書き込むイベント種類（情報、警告、エラー）を指定できます。

本項では、SNMP トラップのフィルタリング方法とイベント種類の指定方法について例を挙げて説明します。

10.1.1. SNMP トラップフィルタリング

1. 指定トラップ内容を除外する

例えば、次のような SNMP トラップ内容があるとします。



ログイン成功の SNMP トラップです。これを除去するには、以下の設定ファイルを編集します。

<BOM インストールディレクトリ> ¥BOMW6¥Common¥snmp¥Config¥FilterBlack.txt
デフォルトでは：C:¥Program Files (x86)¥SAY Technologies¥BOMW6¥Common¥snmp¥Config¥FilterBlack.txt

以下の内容で設定します。

¥ssuccessful

※「¥s」は正規表現で「空白」です。「successful」という文字列を特定するため、「successful」文字列の前は空白であることを指定しています。
※設定変更を反映するには、SNMP マネージャーサービスを再起動する必要があります。

10.1.2. イベントレベル変更

1. 重要な SNMP トラップのイベントレベルを「エラー」に変更する

mib 情報で OID とアラート情報から、アラートレベルがわかっている場合、そのレベルに応じてイベントレベルを変更することが可能です。

一例として CPU 温度が危険状態になった場合の SNMP トラップ情報のイベントレベルを「エラー」レベルに指定します。IMM の mmcalert.mib ファイルの中で、該当する項目は mmTrapTempC で以下のようになっています。

```
mmTrapTempC            TRAP-TYPE
                    ENTERPRISE    mmRemoteSupTrapMIB
                    VARIABLES
                      {
                      spTrapDateTime,
                      spTrapAppId,
                      spTrapSpTxtId,
                      spTrapSysUuid,
                      spTrapSysSern,
                      spTrapAppType,
                      spTrapPriority,
                      spTrapMsgText,
                      spTrapHostContact,
                      spTrapHostLocation,
                      spTrapBladeName,
                      spTrapBladeSern,
                      spTrapBladeUuid,
                      spTrapEvtName,
                      spTrapSourceId,
                      spTrapCallHomeFlag,
                      spTrapSysIPAddress,
                      spTrapSysMachineModel,
                      spTrapBladeMachineModel
                      }
                      DESCRIPTION
                        "Critical Alert: Temperature threshold exceeded.
                        Note: This mib object will be replaced in a future release."
                      ::= 0
```

本 SNMP トラップを Windows イベントログに書き込むレベルを「エラー」にします。Windows イベントログへ書き込めるレベルは「情報」、「警告」、「エラー」の 3 レベルです。

イベント種類を設定するファイル：
<BOM インストールディレクトリ>¥BOMW6¥Common¥snmp¥Config¥EventLevel.txt

設定例：(EventLevel.txt)

```
3, mmTrapTempC
```

(”mmTrapTempC”文字列があるトラップを「エラー」イベントとしてイベントログに書き込みます)

EventLeve.txt の条件パラメータは以下の通りです。

<イベントレベル>,<正規表現>

<イベントレベル>

1： 情報(Information)

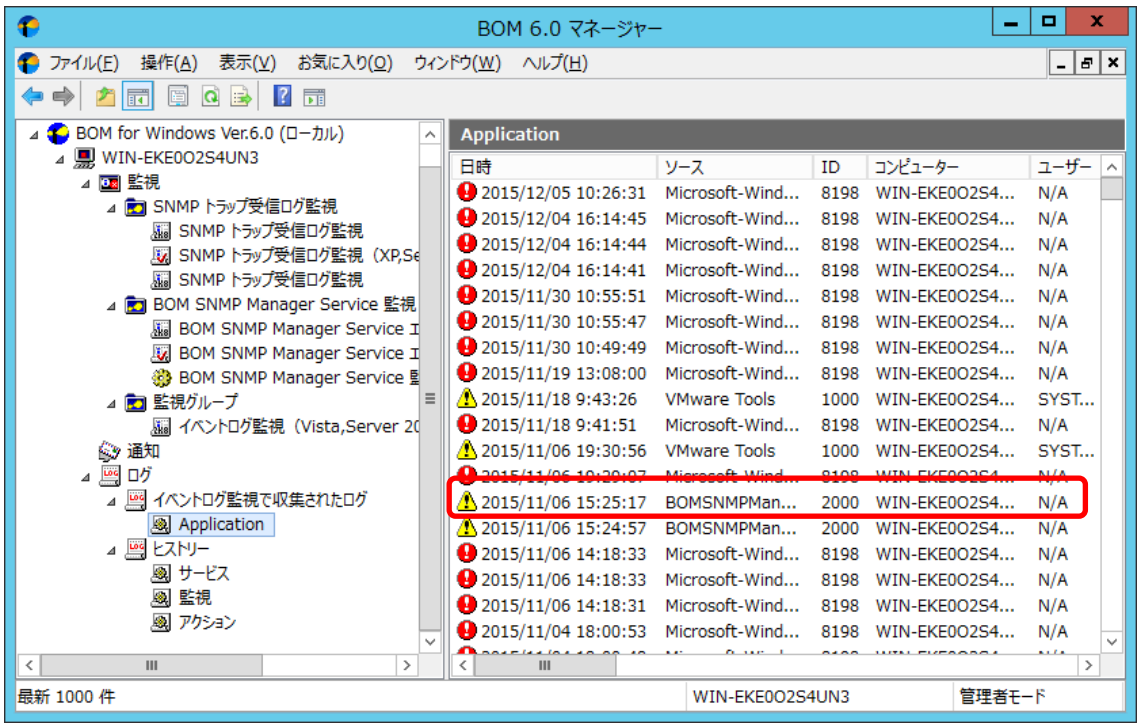
2： 警告(Warning)

3： エラー（Error）

※上記以外は警告になります。

10.2.IMM / IMM2 からのトラップ受信とデータの収集

前項までの操作で、フィルタリングされたトラップがイベントログに書き込まれます。IMM / IMM2 からの SNMP トラップ送信と、BOM を使用しての SNMP トラップ受信と連携は正常に動作し、BOM 6.0 マネージャーのログノードには検知したログが下の様に蓄積されているはずです。



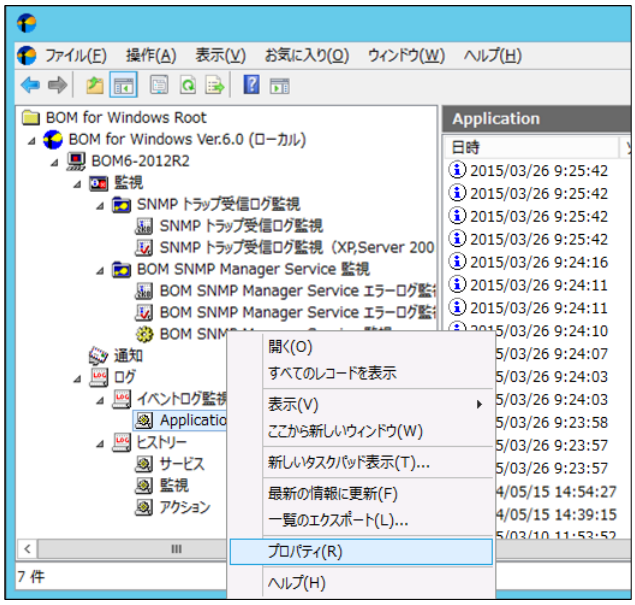
実際の環境では、送信元サーバーの状態と機能や役割によってトラップに含まれるメッセージは多様なものとなります。また、SNMP トラップのログ以外にも、BOM により検知したイベントログが蓄積されているため、そのままでは重要な内容を含むトラップが見逃され、重大なトラブルとなる可能性があります。

この様な環境のログ監視では、一定期間すべてのログを収集しその中から重要なログに含まれる特徴的なメッセージを特定し、イベントログ監視で監視対象キーワードとして設定することが有効です。

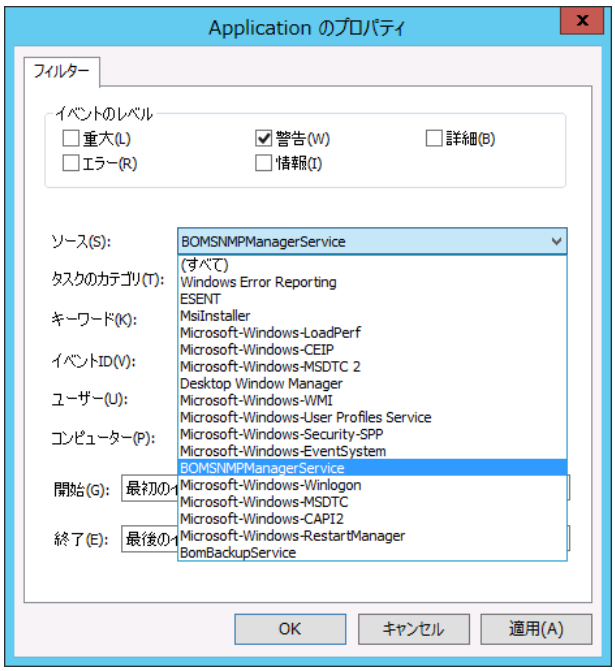
次の章では具体的な設定方法をご説明します。

10.3.重要度の高いログに特徴的なメッセージを拾い出す

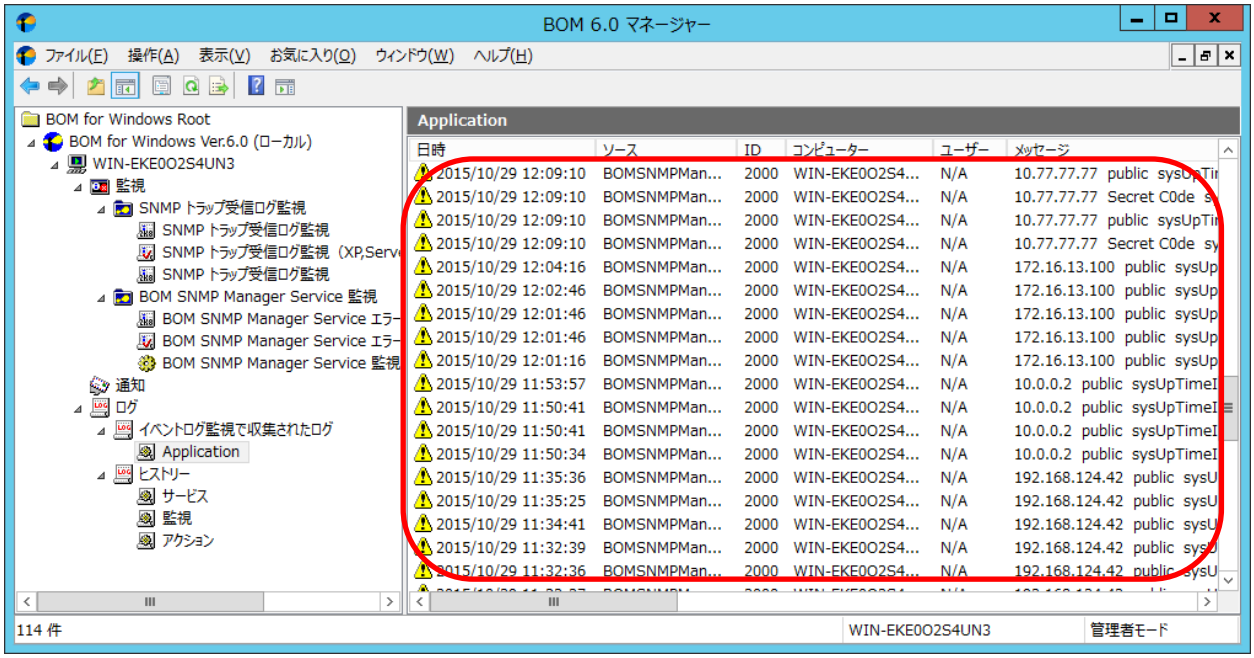
① 先ずは BOM 6.0 マネージャー上で、イベントログ監視により検知され取集された SNMP トラップのログのみを表示するために、ログノード内の[イベントログ監視で収集されたログ¥Application]を右クリックし「プロパティ」を選択します。



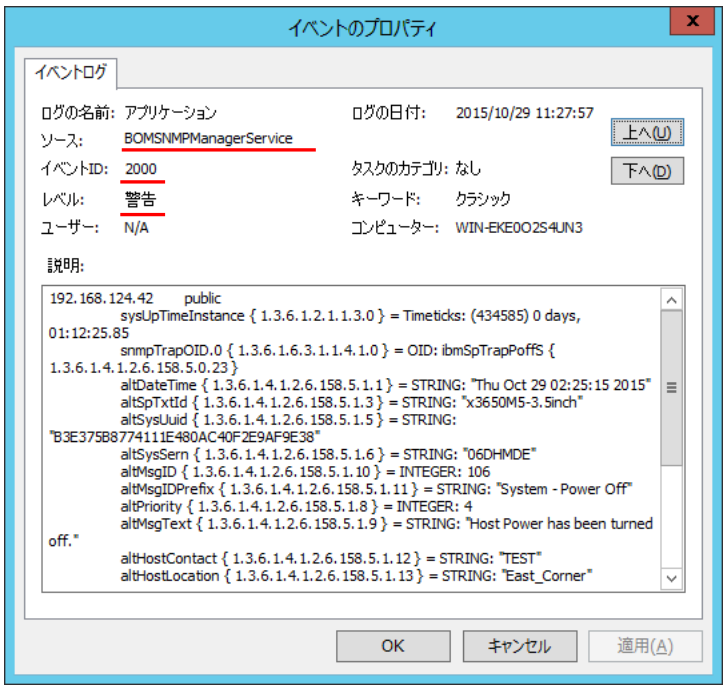
② 開いたプロパティシートでは、収集したイベントログに対して表示フィルターを設定します。BOM SNMP マネージャーサービスにより受信し書き込まれたログは、ソースが「BOMSNMPManagerService」となりますので、このシートでは「ソース」として「BOMSNMPManagerService」を指定します。イベントのレベルは、10.1.2 で指定したイベントレベルに応じて書き込まれています。例として「警告」を設定し OK をクリックします。



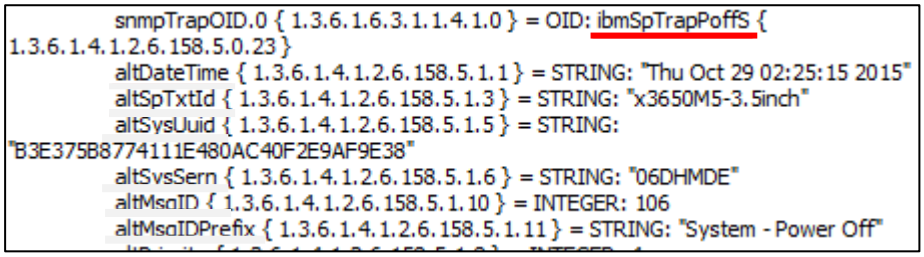
③　前項での設定に基づき、BOMSNMPMnanagerService をソースとする警告のログのみが表示されます。



④　BOM 6.0 マネージャーのログノード蓄積したログをダブルクリックし、プロパティを表示してください。
SNMP トラップ受信機能により受信された SNMP トラップのイベントソースは「BOMSNMPManagerService」となり、イベント ID 及びレベルは、それぞれ「2000」「警告」で固定値を使用しイベントログへ出力されるため、フィルターの条件には使用できません。



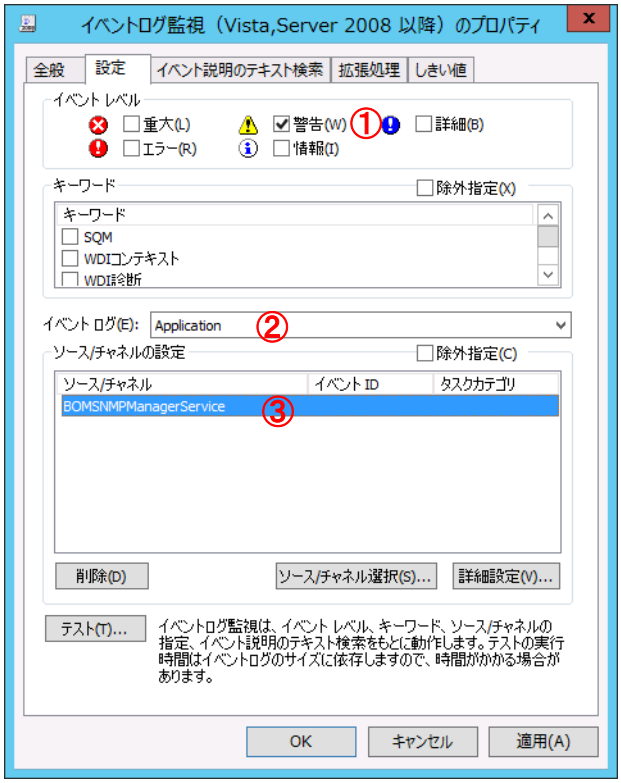
⑤ MIB が正しく導入された環境で受信した SNMP トラップでは、「説明」フィールドに表示されるメッセージが MIB の内容に従ってメッセージがデコードされているはずなので、その中からキーワードとして使用する文字列を選択してください。
ここで示しているログは、本書の「5.5 章 IMM での SNMP トラップ送信指定」で行ったテスト実行の結果であり、MIB ファイルも正しく適用されている環境です。したがってメッセージはデコードされており、下図の様に赤線部分が特徴的な文字列となっています。



10.4.BOM イベントログ監視のフィルタリング設定

フィルターのキーワードとして、「9.2 章 重要度の高いログに特徴的なメッセージを拾い出す」で確認した文字列の中から、「ibmSpTrapPoffS」の文字列を同時に含むレコードのみを検知するよう、BOM のイベントログ監視へ条件を設定します。
イベントログ監視の詳細な設定方法につきましては、BOM for Windows のユーザーガイドをご参照いただくとして、ここでは受信した SNMP トラップのログをフィルタリングする方法に焦点を当ててご説明します。
イベントログ監視（Vista,Server 2008 以降）を新規作成し、全般タブで監視間隔や監視項目名を設定後、下記の図の通り設定タブへ移動します。
このタブでは、以下を設定します。

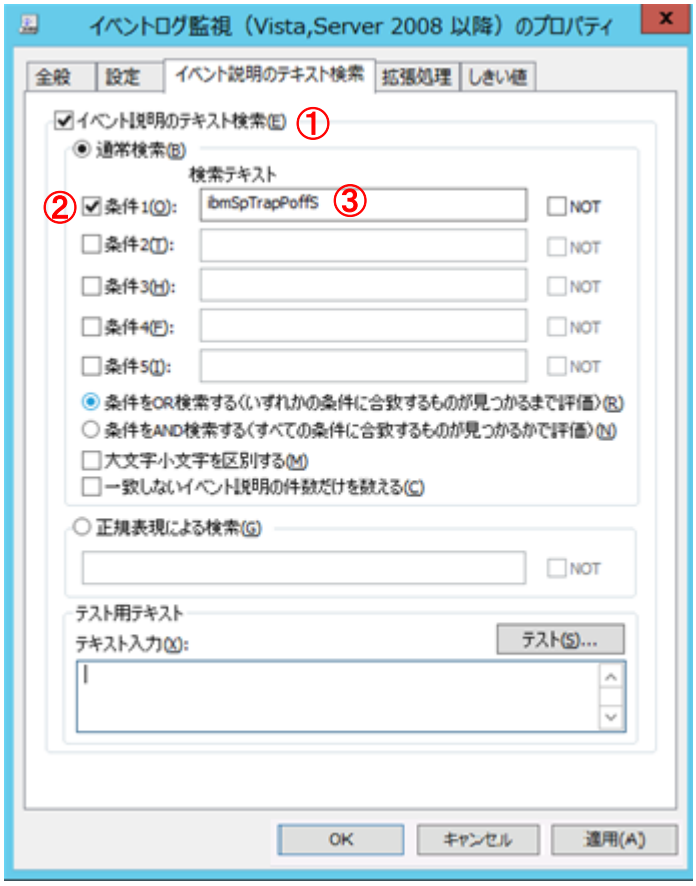
① イベントレベル：警告
② イベントログ：Application
③ ソースチャネル：BOMSNMPManagerService



イベントログ監視の設定

次に下記の図の通りイベント説明のテキスト検索タブへ移動し、フィルターに使用する文字列の設定を行います。
文字列は「9.2 章　重要度の高いログに特徴的なメッセージを拾い出す」で特定した文字列「ibmSpTrapPoffS」を使い検索を行う設定とします。

① 「イベント説明のテキスト検索」を有効にします
② 「条件 1」を有効にします
③ 条件 1 の検索テキストとして「ibmSpTrapPoffS」を入力します



イベント説明のテキスト検索の設定

「拡張処理」「しきい値」の各タブの設定については、BOM for Windows Ver.6.0 ユーザーズマニュアル等を参照し、要件に合った設定を行ってください。
ここまでの設定で、BOM SNMP マネージャーサービスにより書き込まれたイベントログの中から、特定の文字列をキーワードとして選択して、それを含むイベントログのみを検知する設定が出来ました。実際に監視インスタンスを開始し、目的のログのみが検知されることを確認してください。
この様にイベントログの説明文内にある特定の文字列をキーワード設定し監視を行うことで、目的のイベントログ以外をフィルターしてイベントログ監視を行うことができます。

イベントログの設定にはここでの説明以外にも多様な設定方法やオプションがあります。詳細については下記の情報をご参照ください。

イベントログ監視の設定につきまして、以下の情報をご参照ください。
【BOM for Windows Ver.6.0 ユーザーズマニュアル】
5 .9 .13 章 イベントログ監視（Vista,Server 2008 以降）

【イベントログ監視(Vista, Server 2008 以降)の除外指定について】
http://www.say-tech.co.jp/support/bom-for-windows/vista-server-2008/

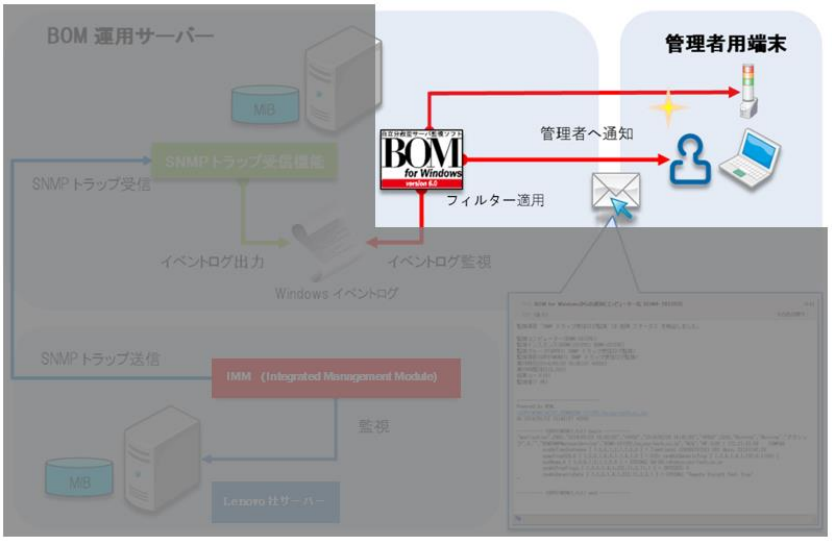
【正規表現を使用したキーワード 6 個以上の文字列検索方法】
http://www.say-tech.co.jp/support/bom-for-windows/6/

11. SNMP トラップ検知後の通知

BOM には、監視ステータスをトリガーとしたアクション/通知を実行する機能が実装されています。

通知項目 監視インスタンス全体で共通の通知を設定したい場合に便利です	メール送信	**アクション項目** 監視項目ごとに個別の通知やリカバリー動作を追加する場合に設定します	メール送信
	SNMP トラップ送信		SNMP トラップ送信
	イベントログ書込み		イベントログ書込み
	カスタム通知		カスタムアクション
			サービスコントロール
			監視有効/無効
			シャットダウン

5 章から 9 章で説明している運用パターンで検知した SNMP トラップのログや、その他の監視項目により発生する監視ステータスで管理者に各種通知を実行することができます。
一般的に管理者へ通知を行う場合、E メールでの通知を設定することが多いかと思いますが、「カスタム通知」や「カスタムアクション」を利用しパトライト等の信号灯を制御することも可能ですので、要件に合った多様な通知方法を選択頂けます。



メール送信による通知につきましては、以下をご参照ください。
【BOM for Windows Ver.6.0 ユーザーズ マニュアル】
6.7.8 章 メール送信アクション
7.7.5 章 メール送信アクション（通知項目）

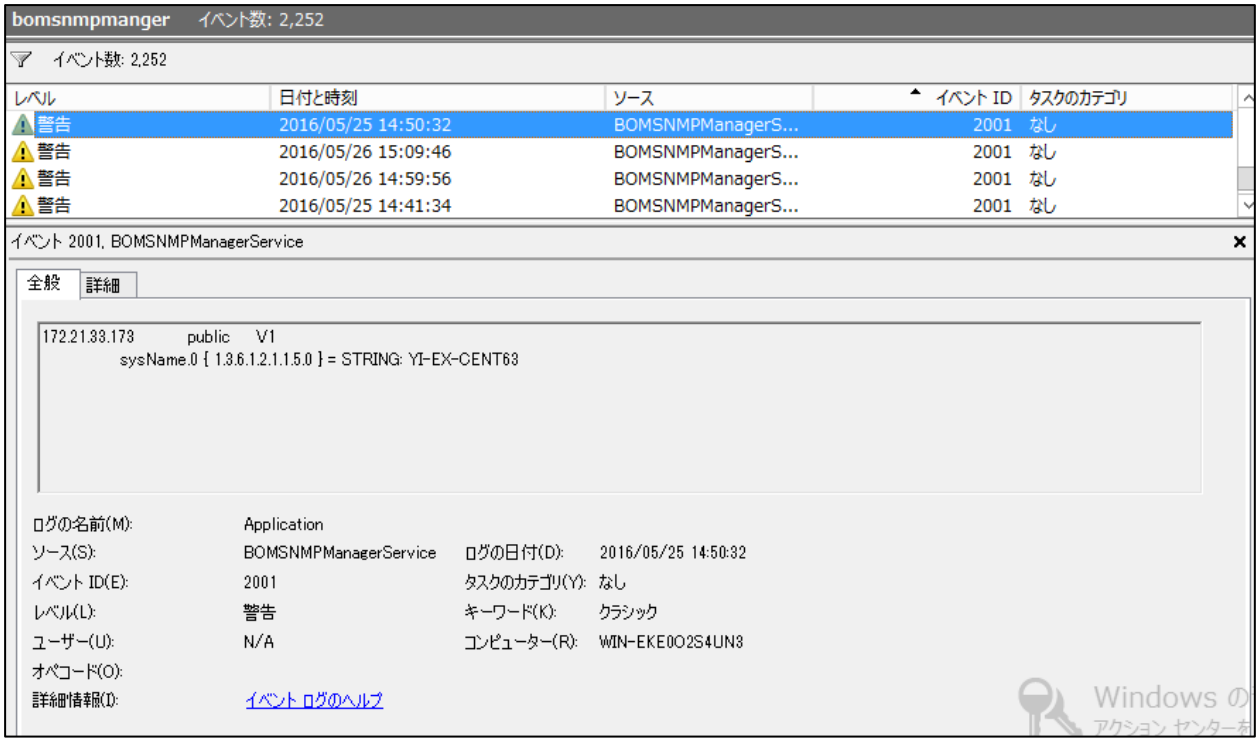
警告灯による通知設定につきましては、以下のサポート技術情報をご参照ください。
[サポート情報番号]：000198:BOM からパトライト社の信号灯を点灯させる
www.say-tech.co.jp/support/bom-for-windows/bom-7/

[サポート情報番号]：000223：BOM からアイエスエイ社の警告灯(警子ちゃん)を点灯させる
http://www.say-tech.co.jp/support/bom-for-windows/bom-5061/

12. SNMP トラップ受信サービスの起動時の動作

SNMP トラップ受信サービスのサービス起動直後に指定した OID の情報を取得します。機器のメンテナンス等で SNMP トラップ受信サービスが停止後、サービス起動時に各機器の状態を SNMP GetRequest で取得します。この機能により、SNMP トラップ受信サービス起動時に各機器の SNMP レベルでの生死確認が可能です。

SNMP トラップ受信サービス開始直後に生死確認したい機器の SNMP バージョン、IP アドレス、OID、等の設定を以下のファイルで指定します。対象 OID1 つにつき 1 行で指定します。GetRequest で取得した OID の情報はイベントログにイベント ID2001 として書き込まれます。SNMPv3 で必要なエンジン ID も取得可能です。



設定ファイル：<BOM インストールディレクトリ>¥BOMW6¥Common¥snmp¥Config¥GetOIDList.txt

設定例：(GetOIDList.txt ファイル)
・v1 の場合（ホスト名を取得する）
-v:1 -c:public -agent:192.168.1.100 -oid: 1.3.6.1.2.1.1.5.0

・V3 で必要なエンジン ID を取得する
-v:1 -c:public –agent:192.168.1.105 -oid:SNMP-FRAMEWORK-MIB::snmpEngineID.0

BOM for Windows Ver.6.0 Lenovo 社製品連携ホワイトペーパー

2016 年 10 月 12 日　　第六版

著者　　セイ・テクノロジーズ株式会社
発行者　　セイ・テクノロジーズ株式会社
発行　　セイ・テクノロジーズ株式会社