BOM for Windows Ver.6.0
SNMP トラップ受信機能拡張モジュール
ホワイトペーパー

2015 年 5 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 2015 年 4 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. SNMP トラップ受信機能拡張モジュールの概要

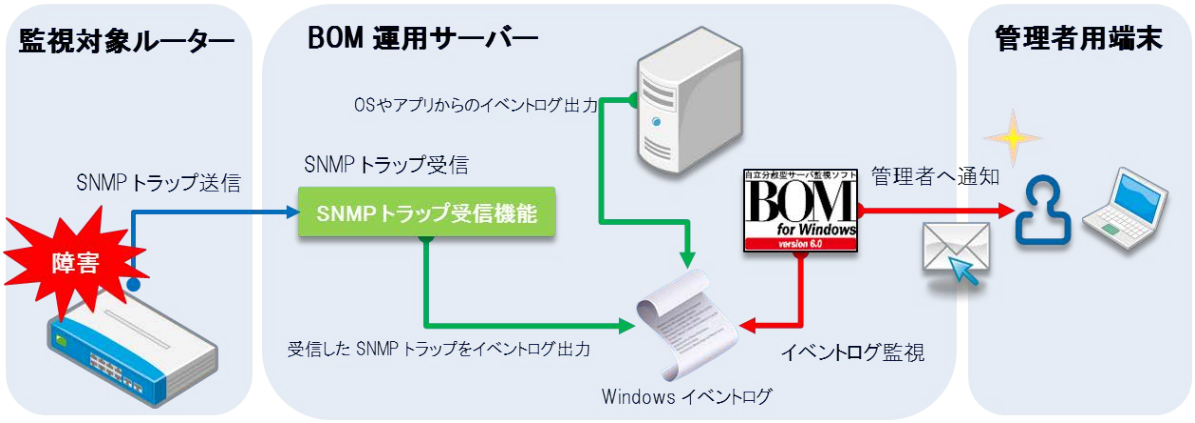
システムの安定稼働には、各種サーバー機器・ネットワーク機器・ストレージなどが正常に期待通りの動作を継続しているかを管理・監視をする必要があります。
これを実現するために BOM for Windows(以降 BOM と記)をはじめ様々な「監視・運用管理ソフト」と呼ばれるソフトウェアが開発・提供されています。
BOM はこの中において、サーバー機の OS 並びにその上で運用されている各種サービスやアプリケーションを監視すると言う分野に特化し、最少1台からの運用が可能で、別途マネージャー用サーバーもデータベースサーバーも必須ではありません。 BOM 単体で監視・通知・リカバリーをカバーします。
そ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

本稿では他の「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。

1.1. 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。)

2. 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。

本項では SNMP の基本事項に絞って簡単なご紹介をしていきます。

2.1. エージェントとマネージャー

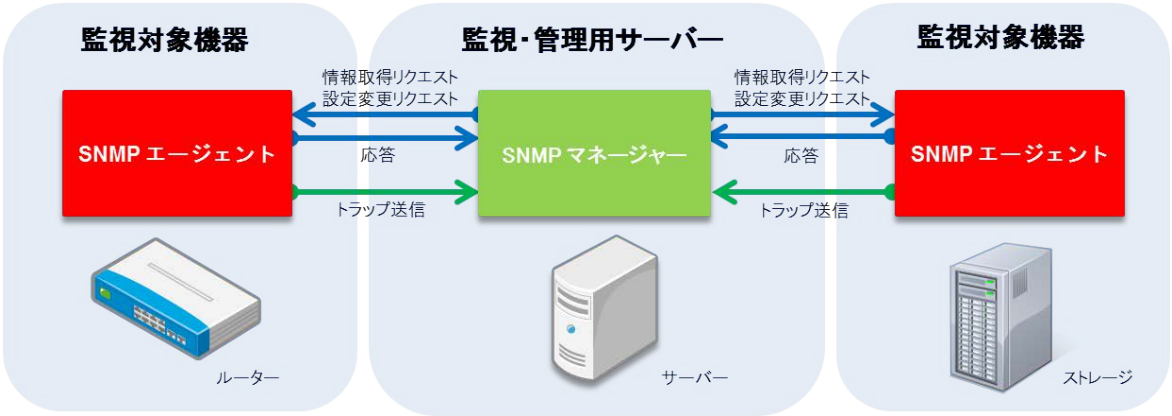
SNMP は監視対象となる機器で動作するエージェントと監視・管理ソフトウェア側であるマネージャーとの間で使用されるプロトコルになります。

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。

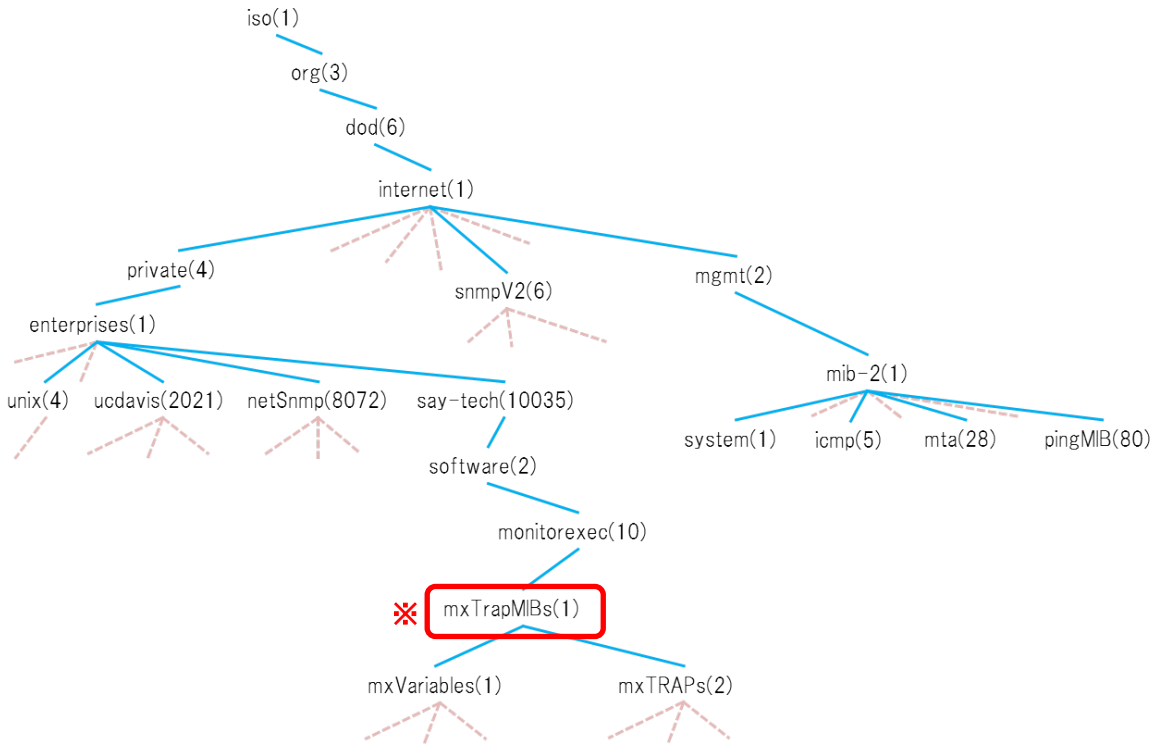


SNMP におけるエージェントとマネージャー

2.2. 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。

2.3. OID とは

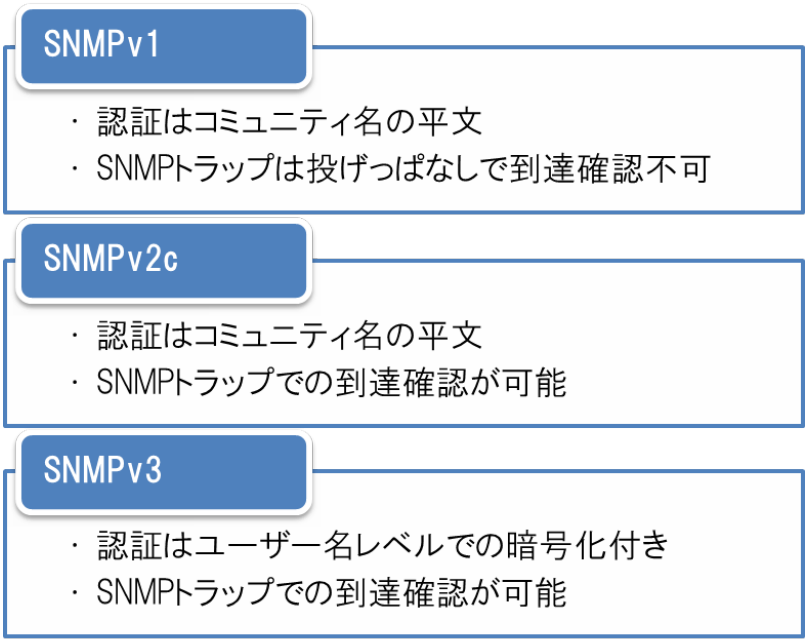
MIB によって管理されている個々の情報をオブジェクト(Object)と呼びます。そのひとつひとつのオブジェクトを区別するために振られた識別子を OID(Object IDentifier)と呼んでいます。

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(2.2.項の図※印部分)に基づいた情報を送信している事になります。

2.4. 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 SNMP のバージョンは SNMPv1 と SNMPv2c となります。

3. MIB ファイル徹底活用術

前項で 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？

本項では実際の MIB の運用方法に絞ってご紹介をしていきます。

3.1. 情報の受け手側にも MIB 情報を

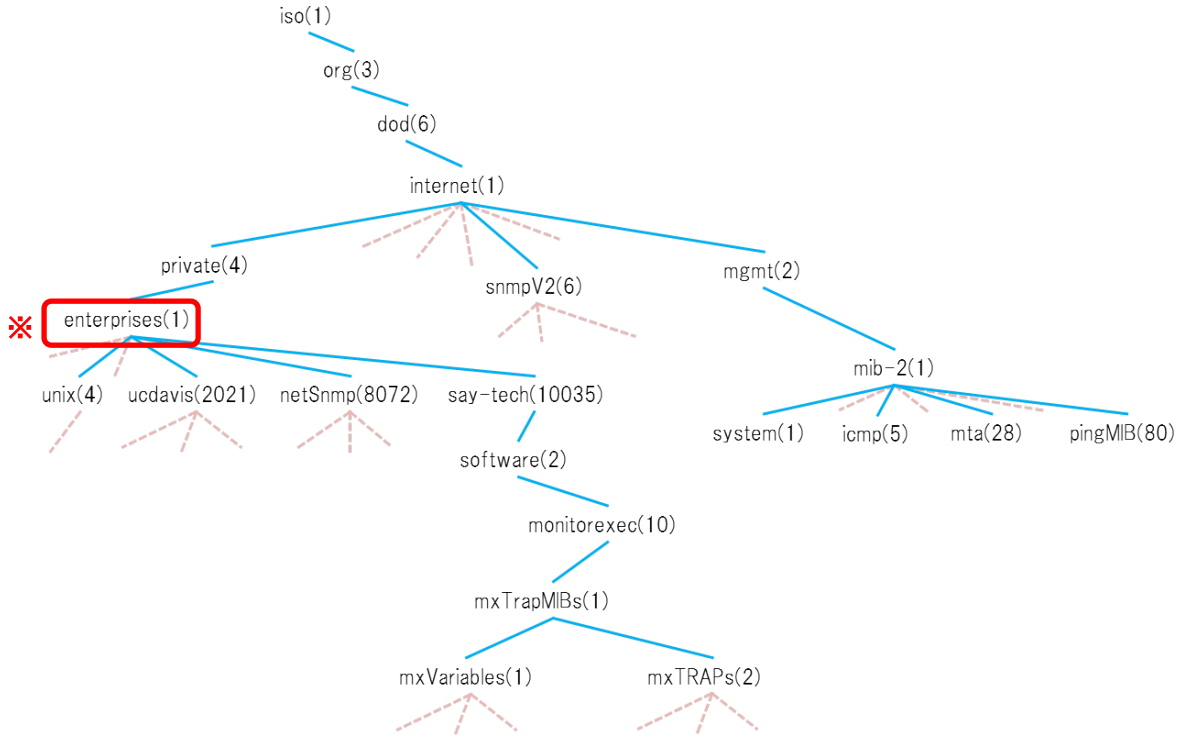
情報の受け手側とは、一般的な SNMP の運用環境では SNMP マネージャーです。本稿におけるその役割は BOM SNMP トラップ受信機能です。BOM SNMP トラップ受信機能であれ、SNMP マネージャーであれ、ある程度一般的な MIB に関してはあらかじめ情報を保持しています。ただし、各メーカー各機器の MIB に関しては必ずしも持ち合わせている訳ではありません。

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。定評のある国内通信機器メーカーである YAMAHA 製ルーターを例に上げて、実際の MIB の設定を行ってみることにします。

3.2. MIB ファイルの入手方法

YAMAHA 製品用の MIB ファイルは YAMAHA 社の Web サイトのトップページより“MIB”で検索をするとすぐ到達できます。2014 年 5 月現在では“http://www.rtpro.yamaha.co.jp/RT/docs/mib/” となっています。YAMAHA 製品用の MIB ファイル自体は複数存在しますが、そのまとめたものが ZIP 形式と tar.gz 形式の2種あります。Widows OS で使うのであれば ZIP 形式の方をダウンロードします。

以下に流れにそって簡単にご案内します。

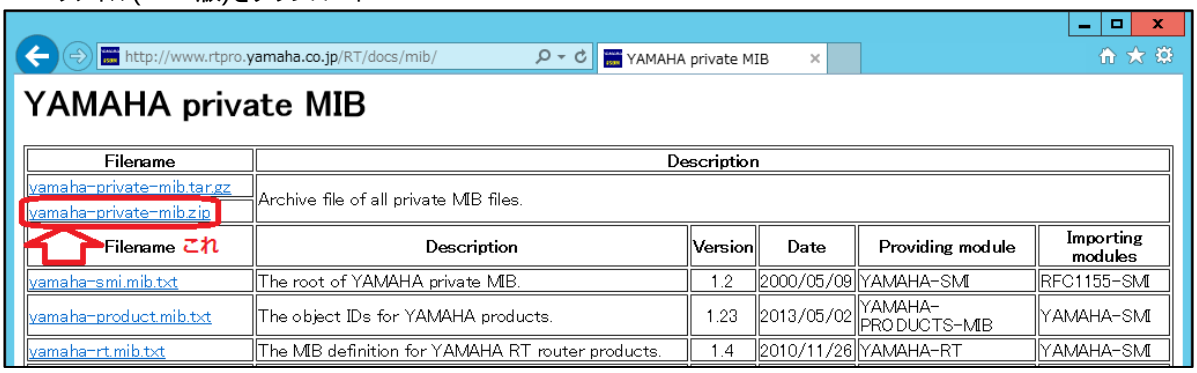
① YAHAMA の Web サイトにアクセスし“MIB”で検索をかける

YAMAHA 社 Web サイトのトップページ

② MIB ファイル群のページへ

検索ワード“MIB”の結果表示ページ

③ MIB ファイル(ZIP 版)をダウンロード



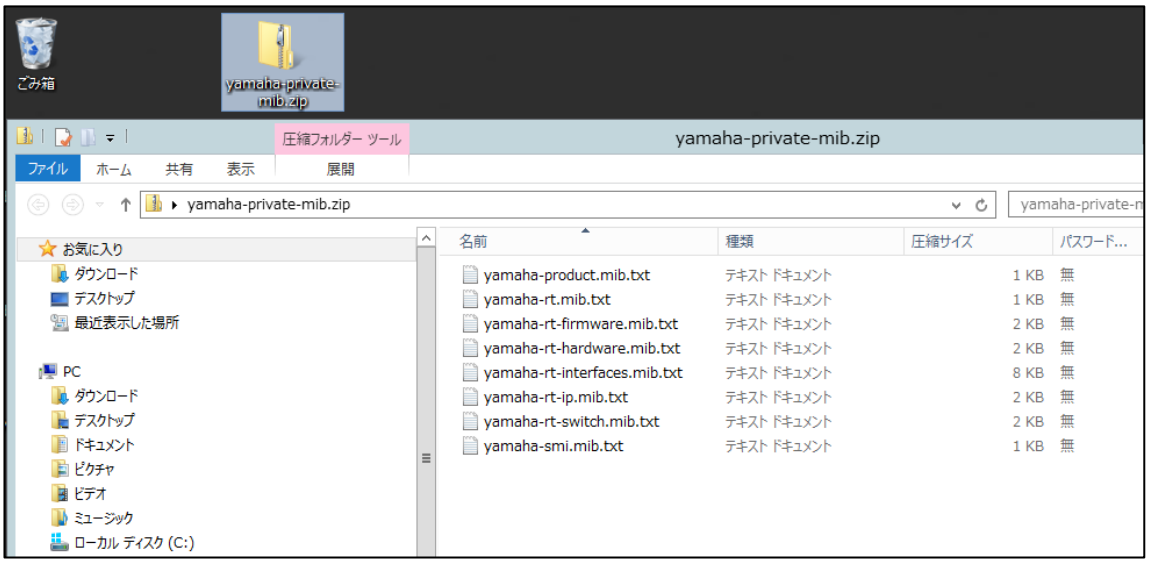
MIB 関連のダウンロードページ

3.3. MIB ファイルを設定しよう

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。

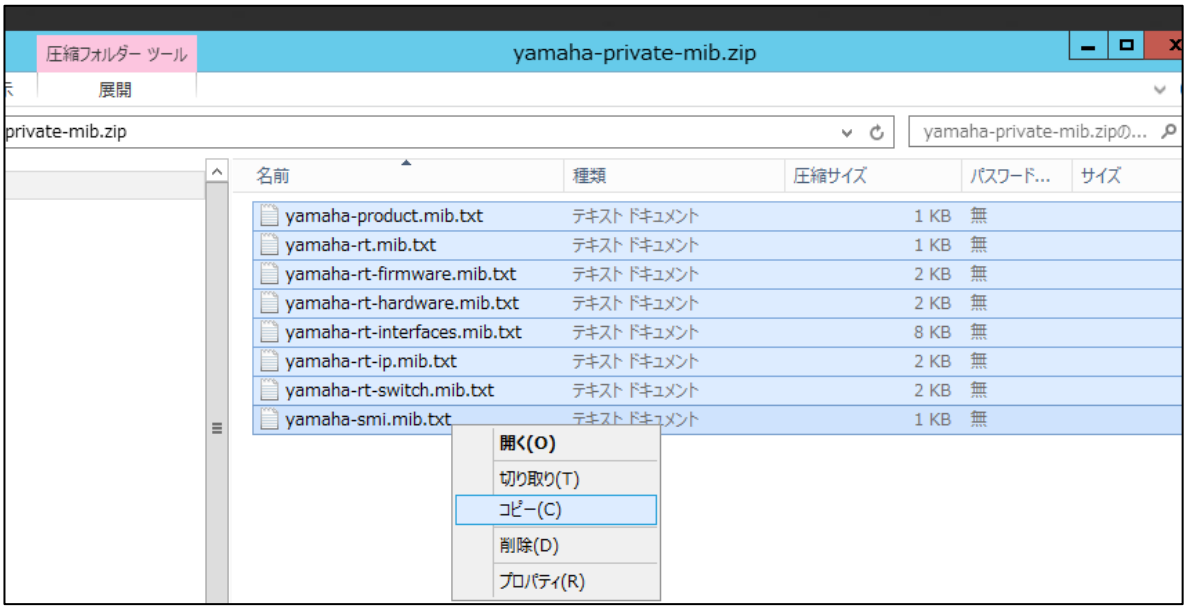
以下に流れにそって簡単にご案内します。

① ZIP ファイルを展開します



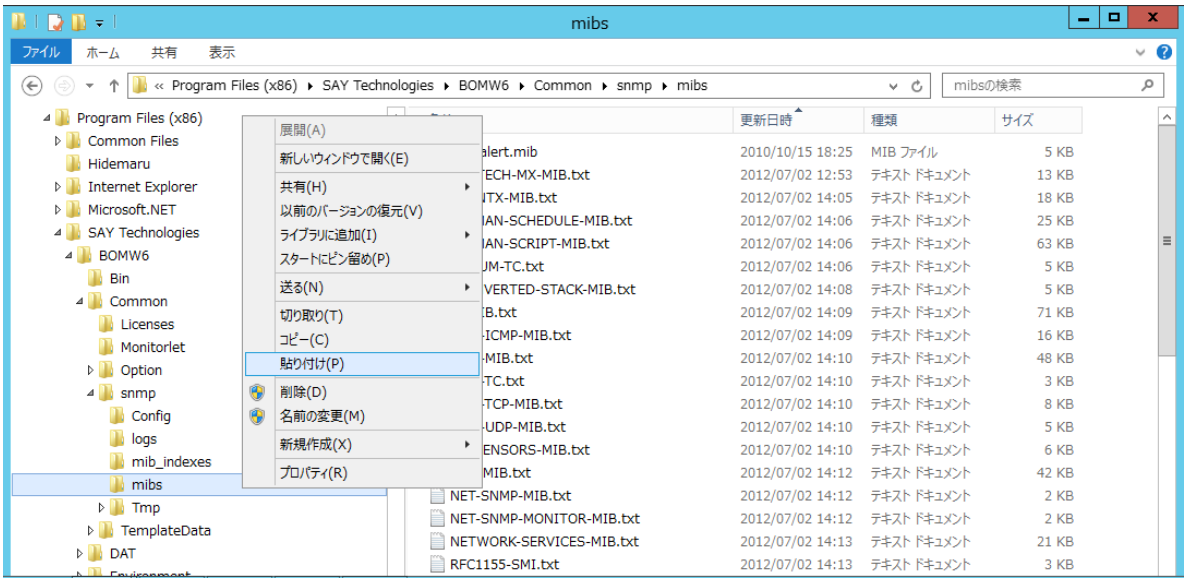
ZIP ファイルから MIB ファイルの展開

② BOM 指定のフォルダーへの保存



MIB ファイルのコピー

“コピー” & “貼り付け” です。



MIB ファイルの貼り付け

③ BOM SNMP トラップ受信サービスの再起動

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 YAMAHA 製機器の 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。

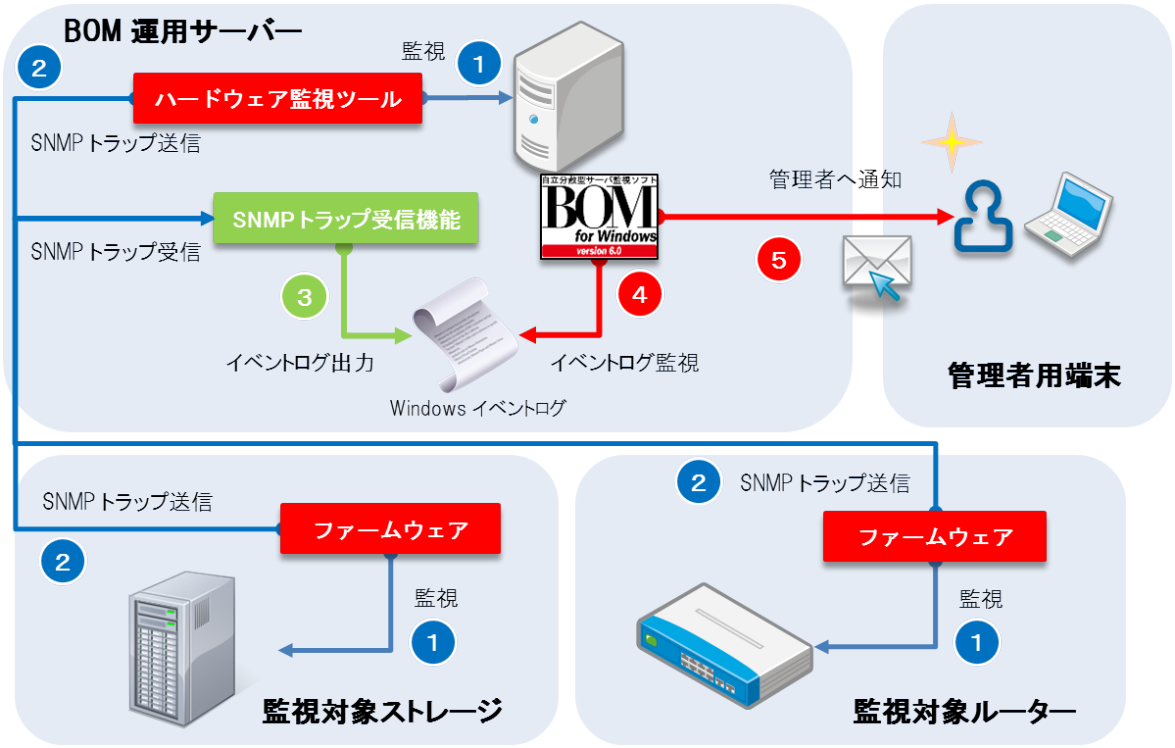
4. 運用パターン基礎編

SNMP トラップ受信機能を BOM 運用サーバーにインストールすると、SNMP トラップ受信機能自体は SNMP トラップパケットを受信しイベントログに出力を行う Windows サービスとして登録されます。これにより SNMP トラップ送信元より BOM 運用サーバーを送信先として指定することにより SNMP トラップを活用した監視をスタートすることが可能となります。

次の図では BOM 並びに SNMP トラップ受信機能を使った運用のイメージになっています。実際の運用の流れに沿って説明をしていきます。

① ファームウェアや SNMP 対応のツールによる対象機器の監視
② 異常を検知した場合や状態を示す数値があらかじめ設定された閾値を超えた場合に SNMP トラップを送信
③ BOM の SNMP トラップ受信機能によりトラップ受信し Windows のイベントログに出力
④ BOM の基本機能であるイベントログ監視により出力したイベントログを検知
⑤ 管理者へメールなどの手段にてアラートを通知

これにより BOM をインストール済みの Windows サーバー、ルーター、ストレージを一元的に監視運用が可能になります。

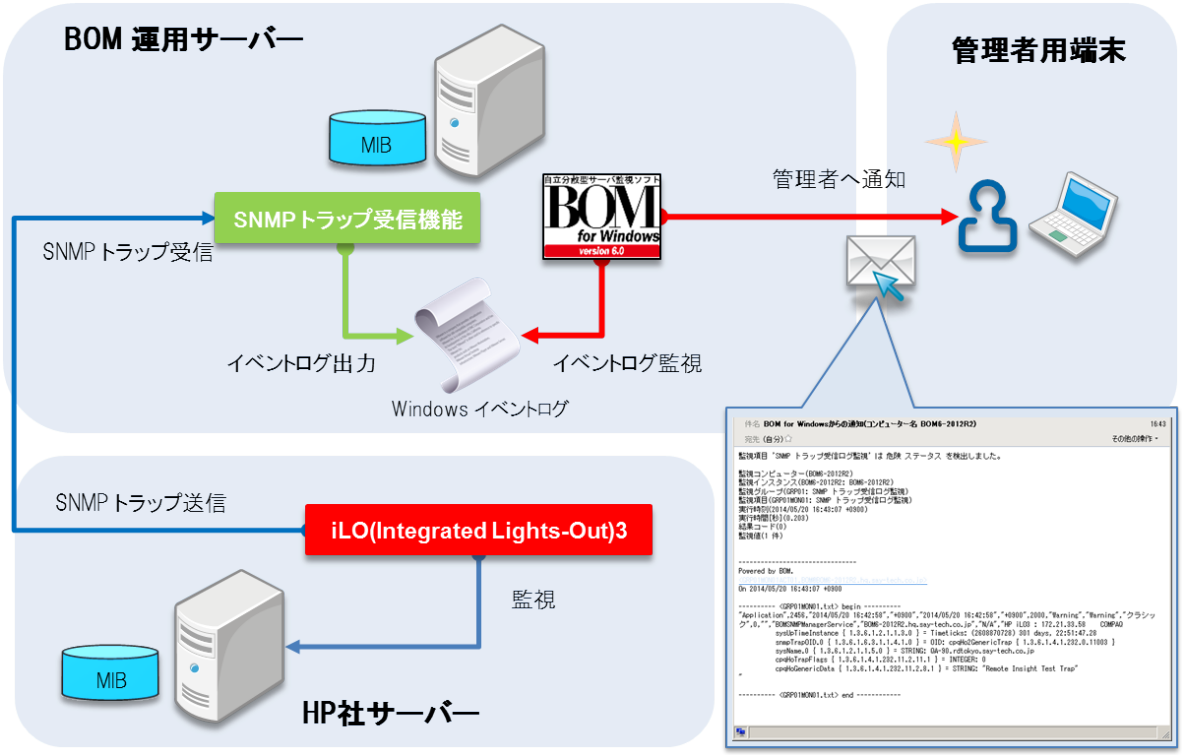


SNMP トラップ受信機能の基本運用パターン

5. 運用パターン実践編　ログの検知

本項では実際の HP 社製 ProLiant サーバー搭載の iLO(Integrated Lights-Out) と言う専用 LSI チップによる監視・管理機能との連携パターンをご紹介していきます。

この iLO 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。



HP 社サーバー搭載 iLO3 との連携パターン

5.1. HP iLO との連携環境の構築手順

今回連携環境を構築する HP 社製サーバー機は ProLiant ML110 G7 となり、当該機に搭載されている iLO は iLO3 になります(iLO 自体の持つ NIC の IP アドレスは 172.21.33.58)。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 172.21.1.74)。

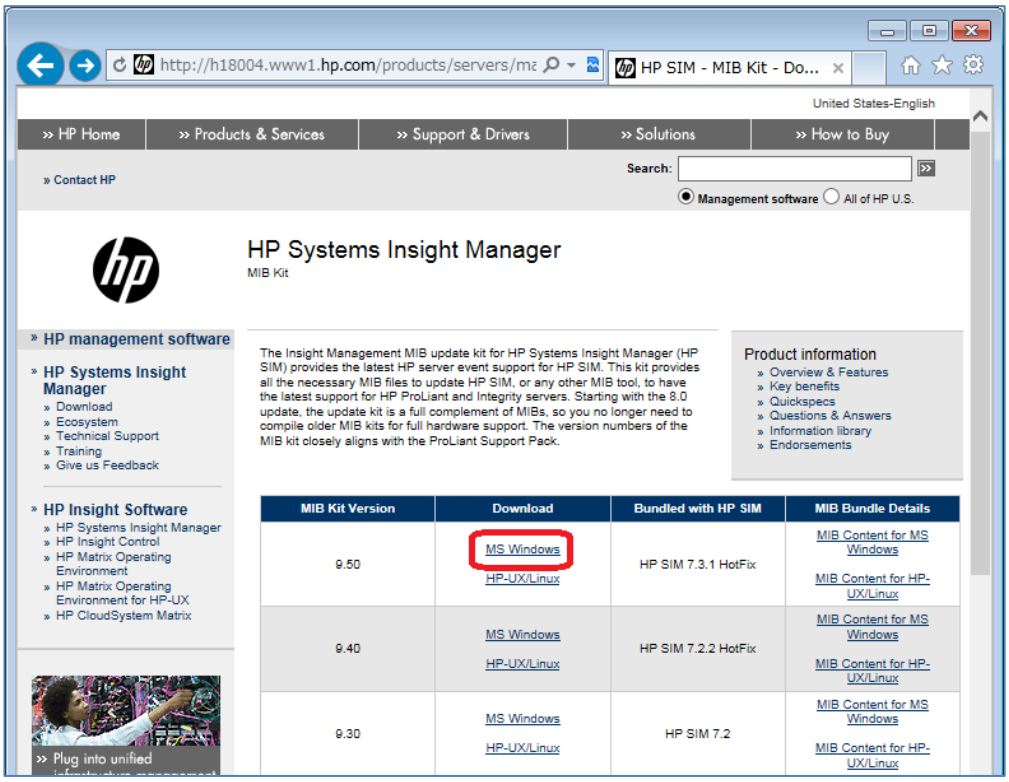
手順は簡単には以下の通りになります。

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 iLO の MIB ファイルを追加
③ SNMP トラップ受信サービスに iLO 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 iLO 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 iLO の MIB ファイル設定と⑤の iLO 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項より補足したいと思います。

5.2. iLO3 関連 MIB ファイルの導入

HP 社の製品用の MIB ファイルは Systems Insight Manager と呼ばれる自社サーバー用管理監視ソフト向けに提供されている MIB Kit を利用します。このキットは iLO をはじめとした HP 社製機器の MIB ファイルはもちろんの事、Systems Insight Manager の中の SNMP マネージャー機能内で使用するための他社製機器用の MIB ファイルも多く含んでいる膨大な MIB ファイル群となります。



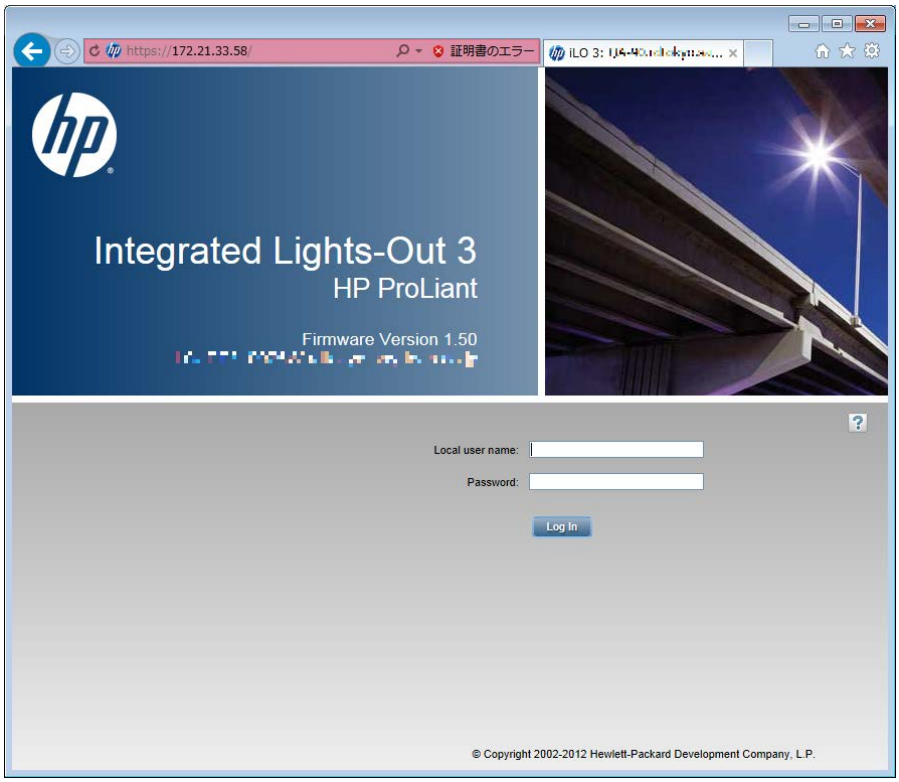
HP 社製 MIB ファイルを含んだ MIB Kit のダウンロードサイト(赤い囲みが Windows OS 用)

ここより最新の MIB Kit ファイルである upd950mib.zip を入手します。

この中で iLO 関連の MIB ファイルは HP 社の公開資料によると cpqida.mib , cpqhost.mib , cpqhlth.mib , cpqsm2.mib , cpqide.mib , cpqscsi.mib , cpqnic.mib の7つとなっています。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したところ MIB ファイルのエラーが発生しており、これを解消するにはさらに2つの cpqsinfo.mib , cpqstdeq.mib ファイルを導入が必要でした。よって今回は結果的に9つの MIB ファイルを BOM サーバーに導入をしたことになります。

5.3. iLO3 のコンソール

iLO3 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。

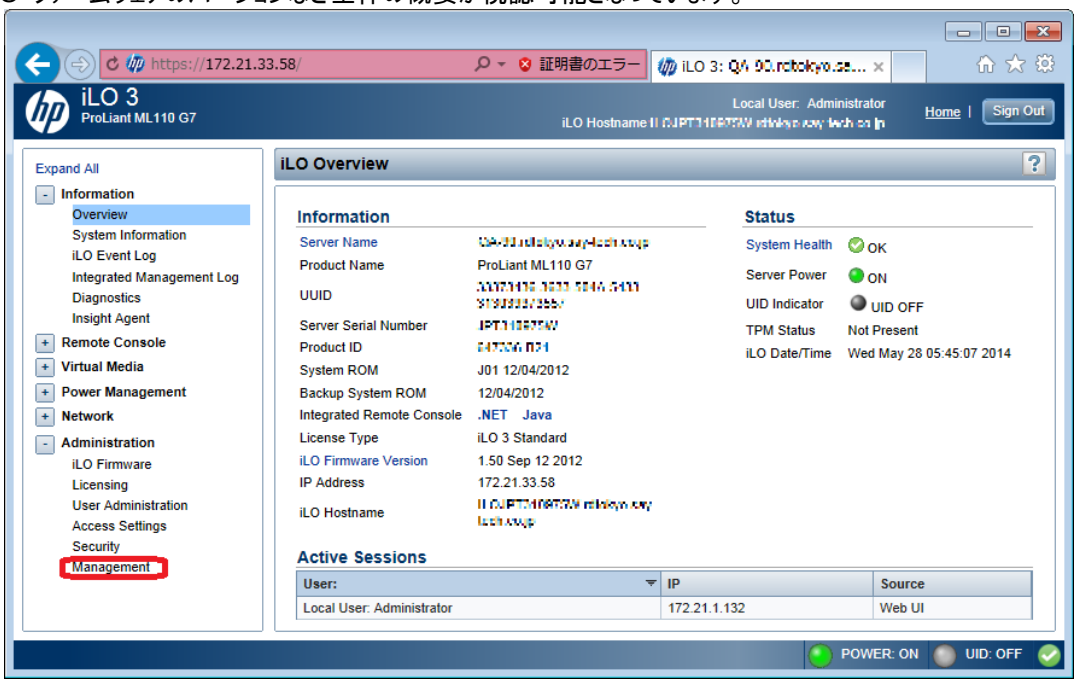


iLO3 コンソールのログイン画面(上部の証明書エラーは正式な認証局からの認証を受けていないため)

ここからユーザー名とパスワードを入力してログインします。

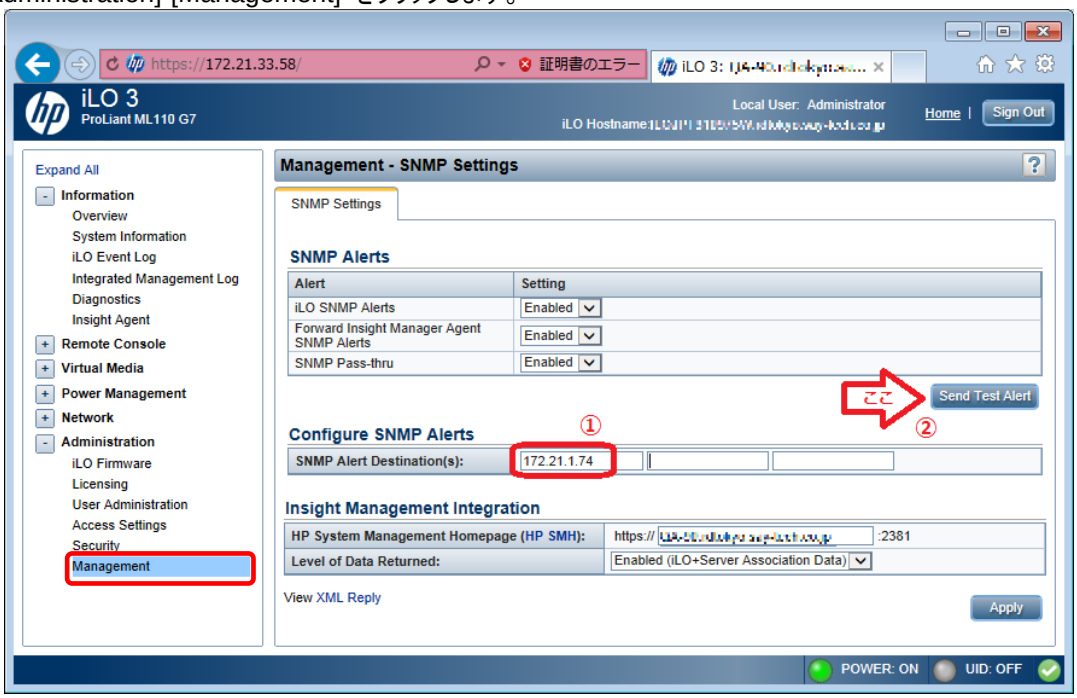
5.4. iLO3 での SNMP トラップ送信指定

iLO3 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 HP 製サーバー機のシリアル番号、iLO ファームウェアのバージョンなど全体の概要が視認可能となっています。



iLO3 ログイン直後のコンソール画面(ファームウェアのバージョンやライセンスなどの情報を確認できます。)

SNMP トラップ送信設定をする場合には左側のペインの赤く囲った部分である[Administration]-[Management] をクリックします。



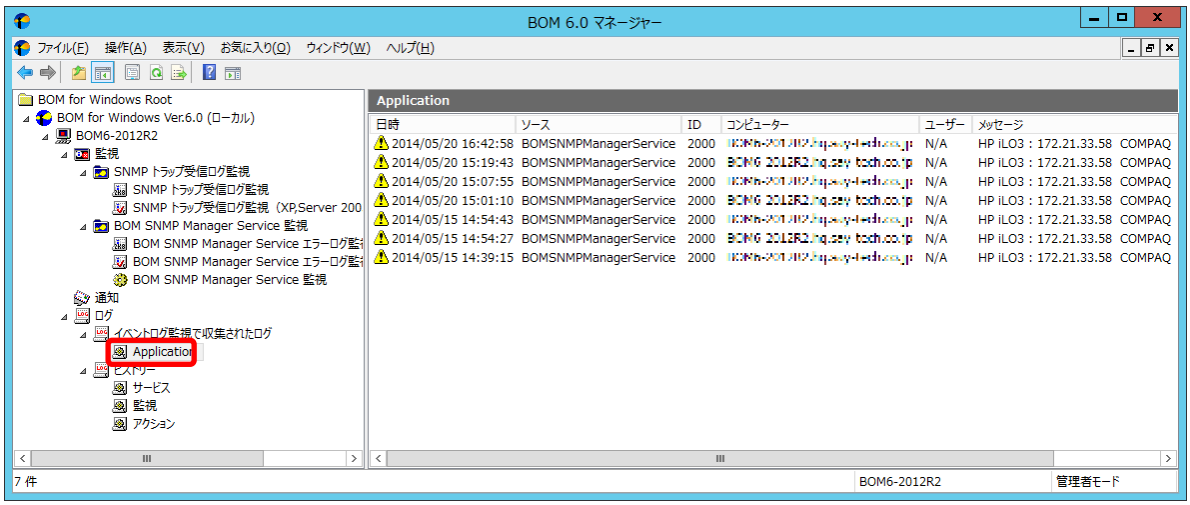
SNMP 関連の設定画面

① この画面での [Configure SNMP Alerts] の [SNMP Alerts Destination(s)] に送信先の IP アドレスを入力します。

② 右方 [Send Test Alert] ボタンを押すとテスト用の SNMP トラップが送信されます。

5.5. トラップを受信、検知、メールを送信

iLO3 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。



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

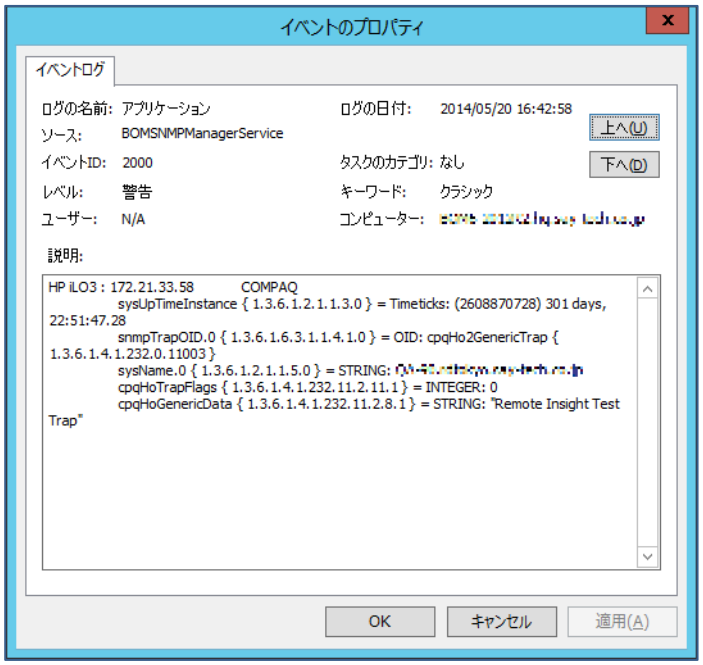
その内の1つを詳しく見てみましょう。リザルトペイン(画面右側)よりレコードを1つ選びそのプロパティを開きます。

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 iLO 機などの情報は説明欄であるログ本文に書かれています。

そのログ本文には HP 社と合併した COMPAQ 並びにその略と思われる cpq の文字が散見されます。

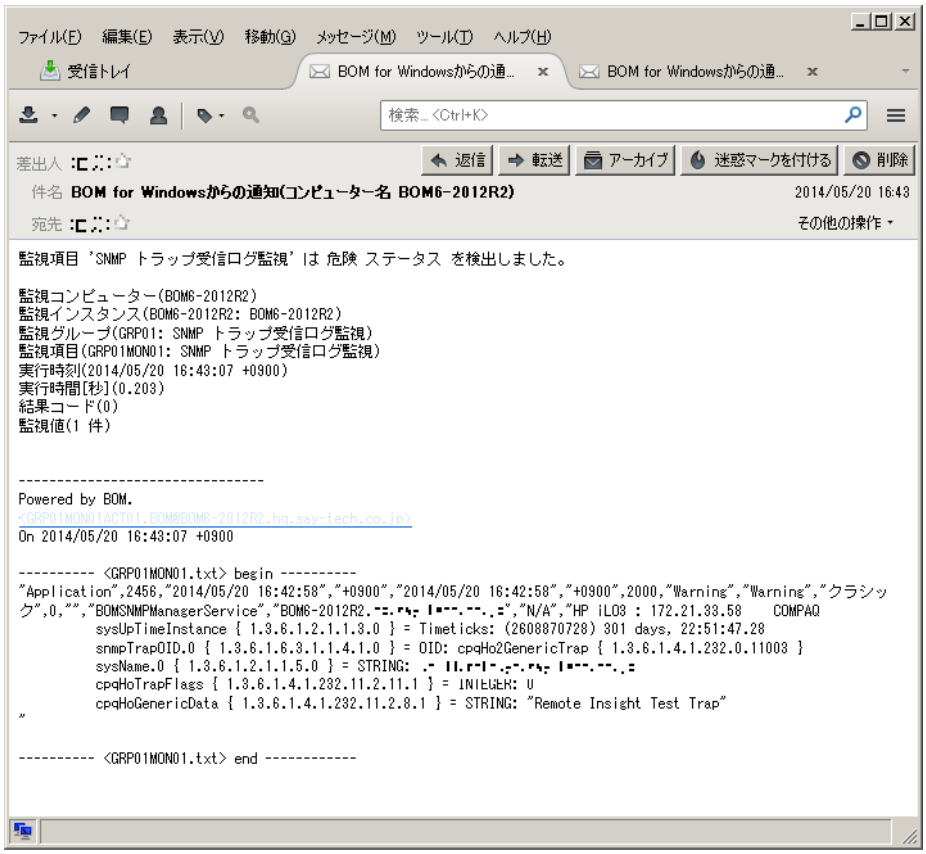
ちなみに本文の最後の部分に、このトラップはテスト送信のものであることが確認できます(Remote Insight Test Trap の語)。



検知収集されたイベントログの詳細

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埋め込み指定をした上で送信をします。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。



メールソフト Thunderbird にて受信した BOM からの通知メール(後半部が埋め込まれたイベントログ)

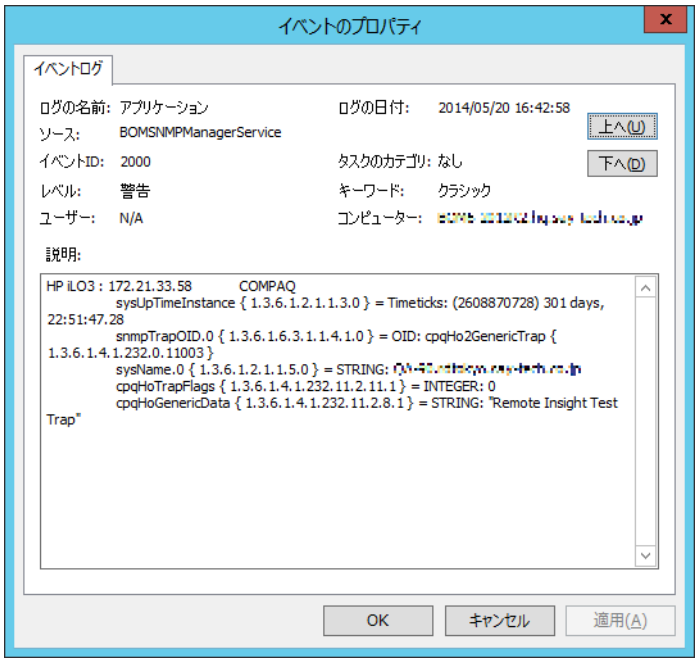
5.6. MIB ファイルで何が変わった？

4. 項にて 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。

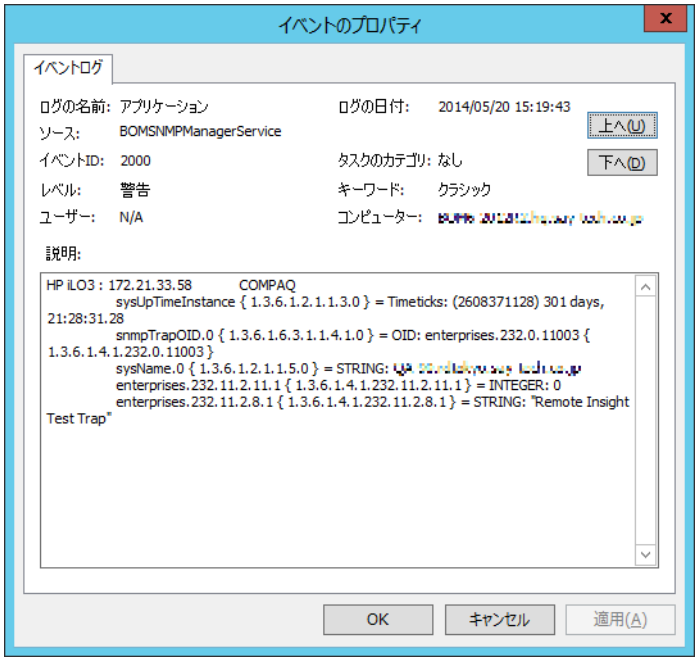
それでは受信トラップに応じた MIB ファイルの有無で何が変わるのでしょうか？実際に比較するのが一番わかり易いと思いますので以下をご参照ください。

これは BOM で検知収集した先ほどのイベントログの詳細画面になります。



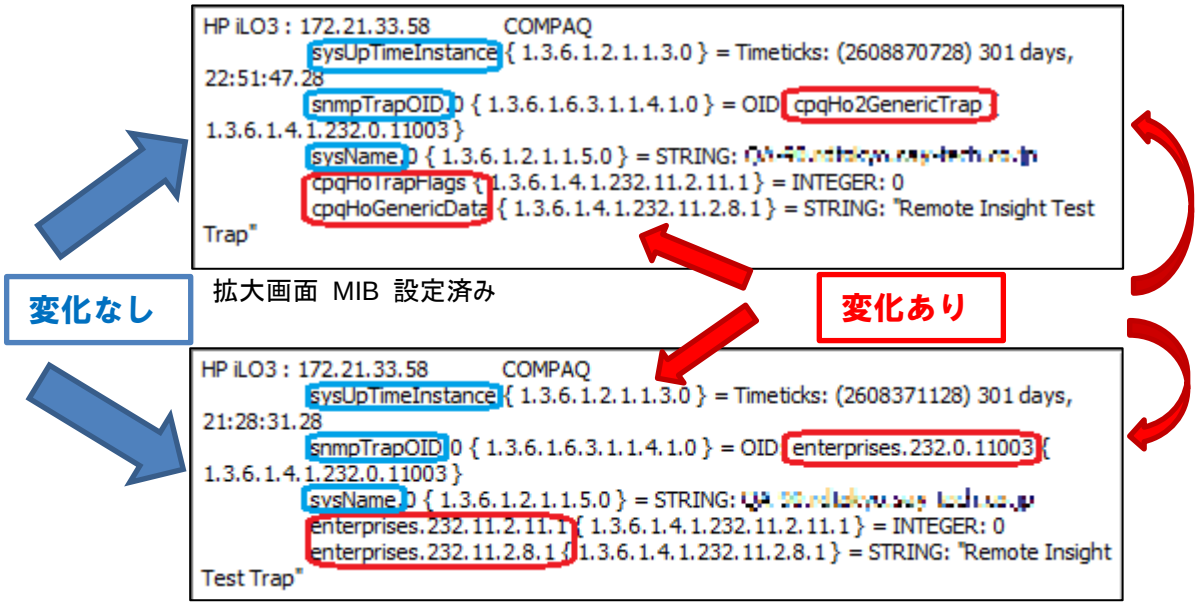
MIB ファイル設定時の画面

これに比べて iLO 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。



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 HP 社製固有の iLO 関連の部分が、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。

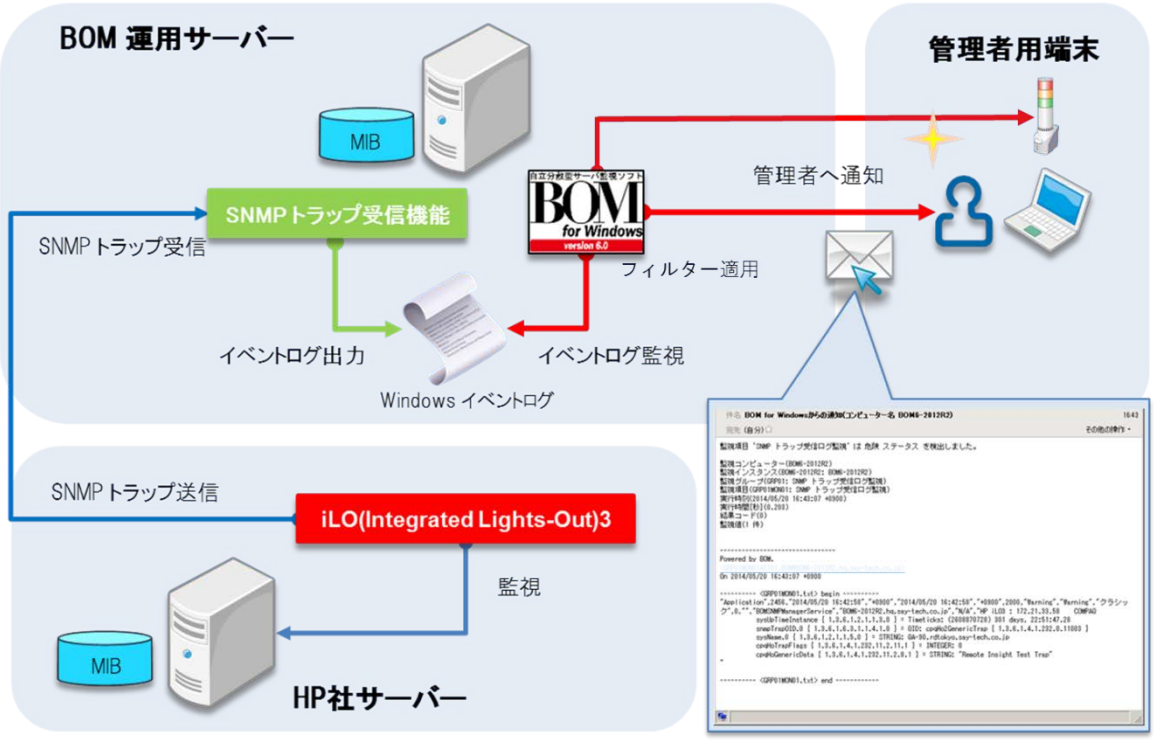
それとは対照的に青い囲みの部分は双方に違いがありません。この部分は標準 MIB で定義されている部分にあたるので違いが見られない訳です。

6. 運用パターン実践編 II　フィルタリング

前項でiLOからの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、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。

【フィルタリングのシナリオ】

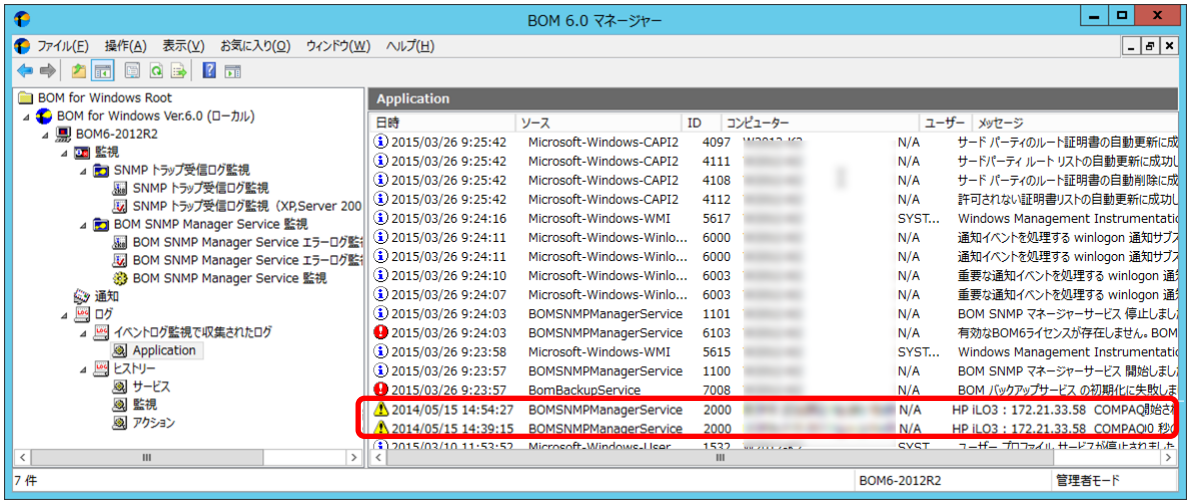
① SNMP トラップを受信、イベントログへ書き出し、BOM でログの収集
② 項番①を一定期間運用し、SNMP トラップ受信により書き出されたログを蓄積する
③ SNMP トラップのログを精査、重要度の高いログに特徴的なメッセージを拾い出す
④ 特徴的なメッセージをイベントログ監視のキーワードに設定した監視項目を作成



以下にご紹介する内容は本項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いたします。

6.1. iLO からのトラップ受信とデータの収集

前項までの操作で、iLO 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。



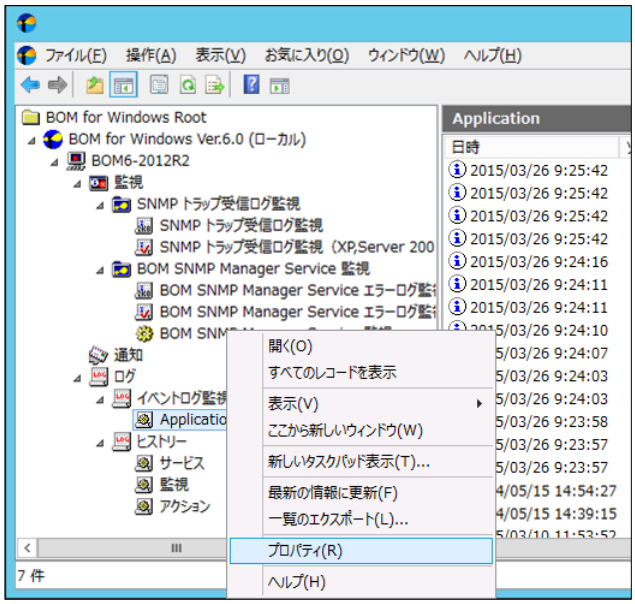
実際の環境では、送信元サーバーの状態と機能や役割によってトラップに含まれるメッセージは多様なものとなります。また、SNMP トラップのログ以外にも、BOM により検知したイベントログが蓄積されているため、そのままでは重要な内容を含むトラップが見逃され、重大なトラブルとなる可能性があります。

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。

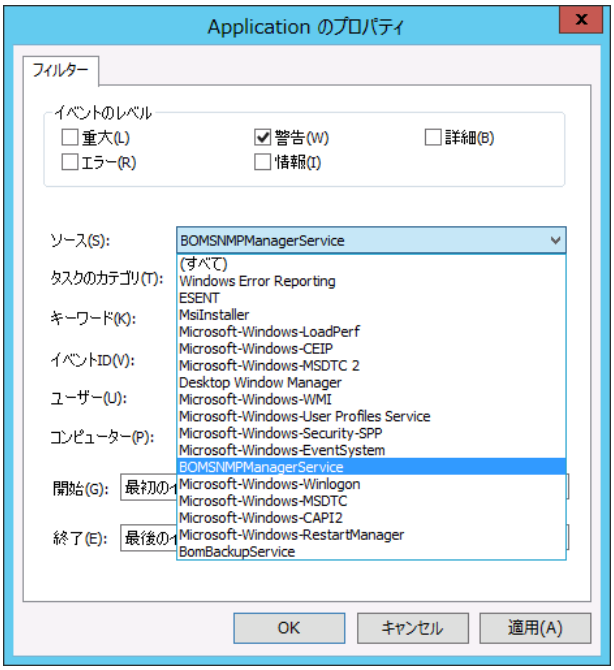
次の項では具体的な設定方法をご説明します。

6.2. 重要度の高いログに特徴的なメッセージを拾い出す

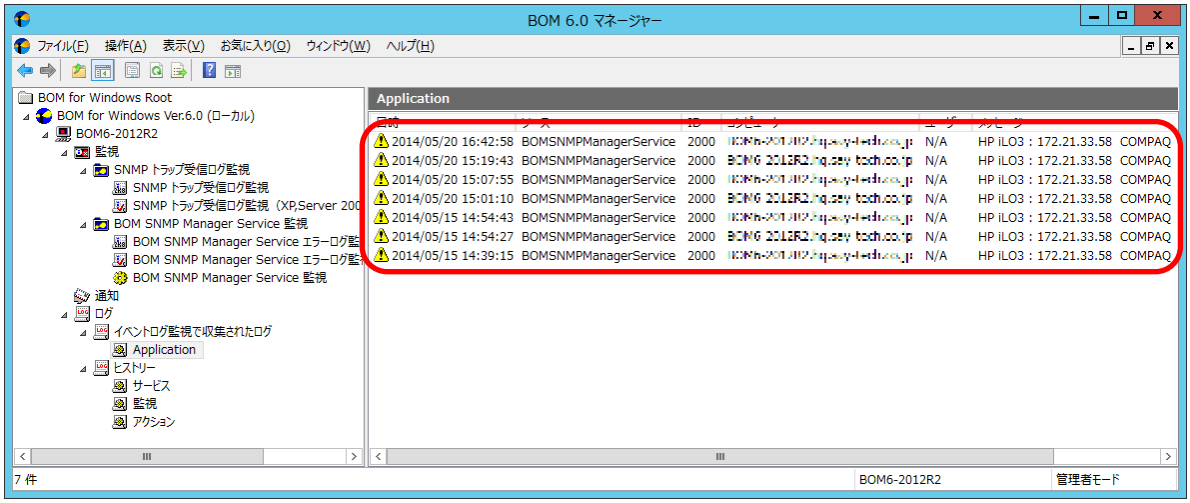
先ずは BOM 6.0 マネージャー上で、イベントログ監視により検知され取集された SNMP トラップのログのみを表示するために、ログノード内の[イベントログ監視で収集されたログ¥Application]を右クリックし「プロパティ」を選択します。



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。受信した SNMP トラップを書き出したログの場合、イベントのレベルはトラップの内容に関わらず「警告」に固定されていますので、イベントのレベルでは「警告」を設定し OK をクリックします。

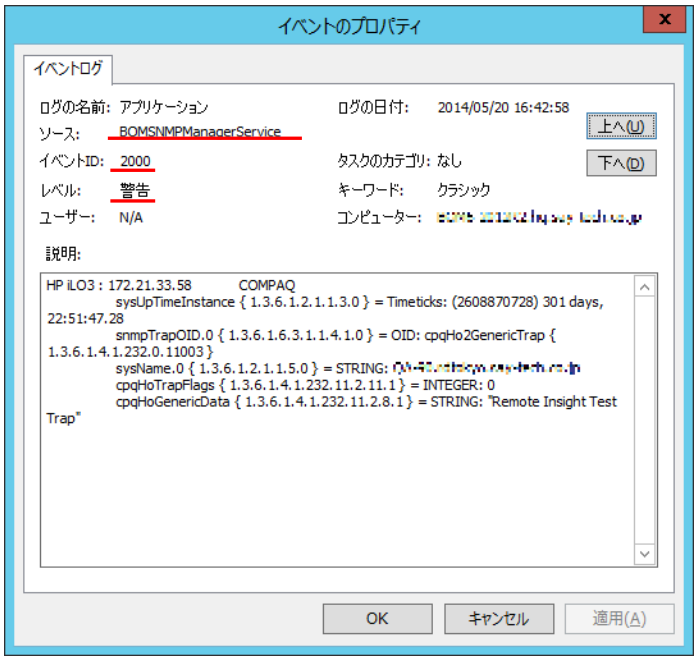


前項での設定に基づき、BOMSNMPMnanagerService をソースとする警告のログのみが表示されます。



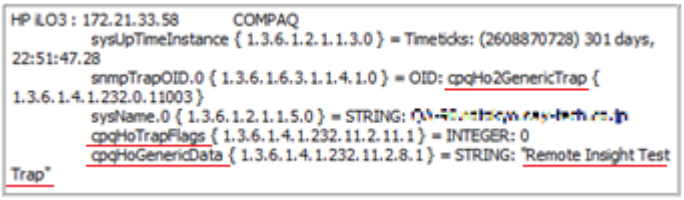
BOM 6.0 マネージャーのログノード蓄積したログをダブルクリックし、プロパティを表示してください。

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。



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「5.4 iLO3 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。



6.3. BOM イベントログ監視のフィルタリング設定

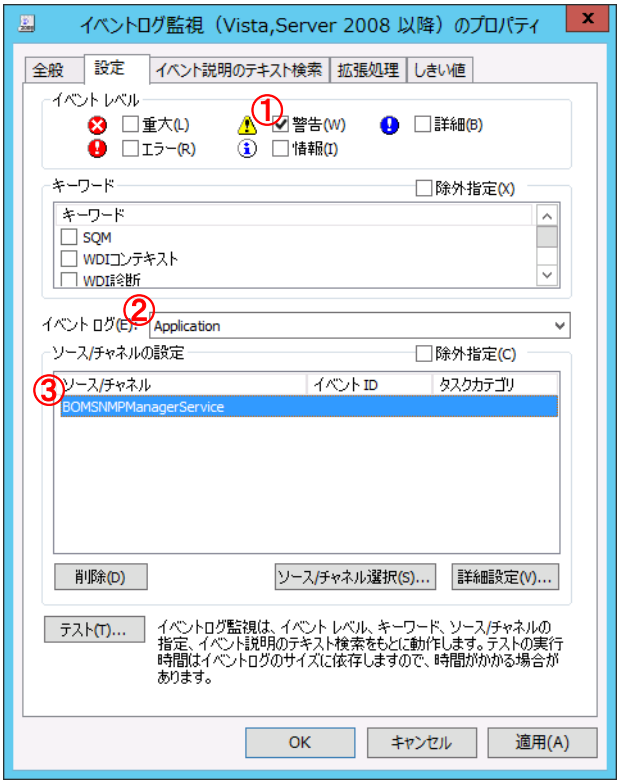
フィルターのキーワードとして、前章で確認した文字列の中から、「cpqHoTrapFlags」と「cpqHoGenericData」の 2 つの文字列を同時に含むレコードのみを検知するよう、BOM のイベントログ監視へ条件を設定します。

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あててご説明します。

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、上図の通り設定タブへ移動します。

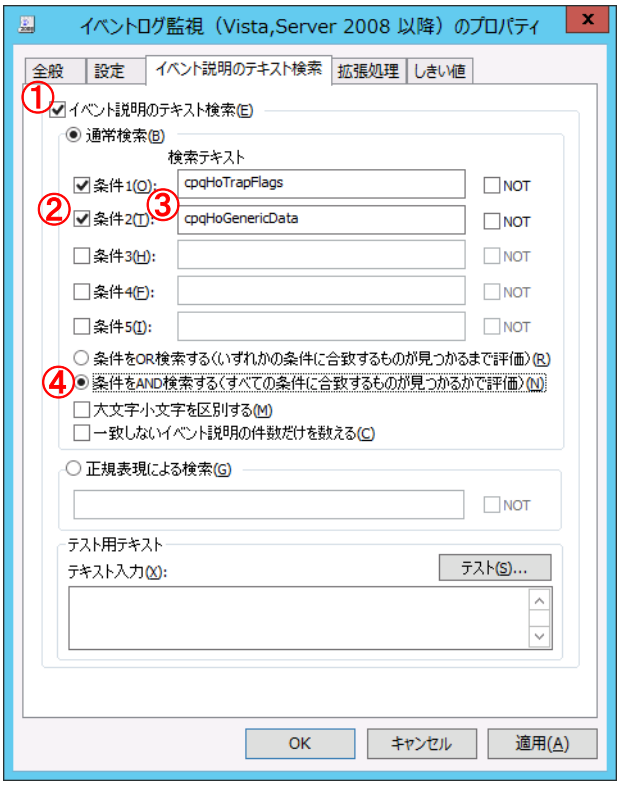
このタブでは、以下を設定します。

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



次に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 6.2 章で特定した 2 つの文字列「cpqHoTrapFlags」「cpqHoGenericData」使い、AND 条件（2 つの文字列が同時に説明文に含まれる）で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」「条件 2」を有効にします
③ 条件 1、条件 2 の検索テキストとして「cpqHoTrapFlags」「cpqHoGenericData」を入力します
④ 「条件を AND で検索する」を有効にします



「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の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のイベントログ監視をおこなうことができます。

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。詳細については下の情報をご参照下さい。

イベントログ監視の設定につきまして、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 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/

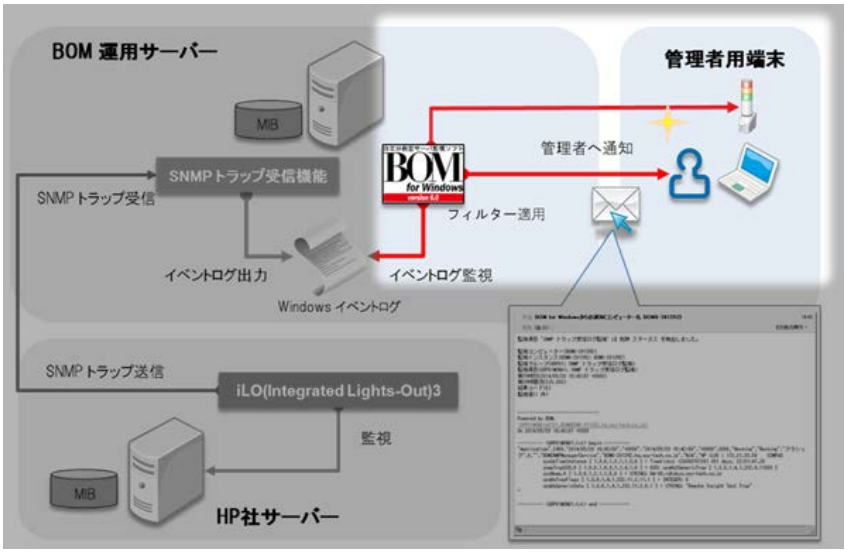
7. SNMP トラップ検知後の通知

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	メール送信	アクション項目	メール送信
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	SNMP トラップ送信	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	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 章や 6 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/

SNMP トラップ受信機能 拡張モジュール ホワイトペーパー

2014 年 6 月 9 日　初版
2015 年 5 月 11 日　第二版

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