

株式会社エクストランス

X-MON3

X-MON 高度リファレンス

2017/11 版

まえがき

本書はX-MON3系列を用いてLinuxサーバを監視するリファレンスとなっております。
そのため、基本的なOSやGUIの一般的な操作、用語などについては知識をご理解の上でお読みください。

また、X-MONの操作画面はお使いのOSやブラウザによって異なる場合がございます。

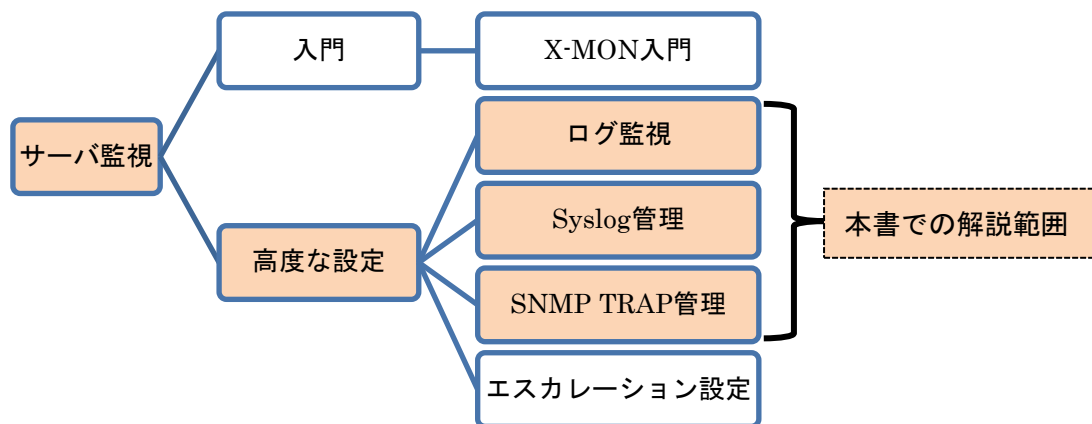
- ・ 本書における解説環境

X-MON ver 3.0.6

X-MON ver3.0.5 以前をご利用の方は ver3.0.5 用リファレンスをご利用ください。

また、SNMP TRAP 監視につきまして X-MON ver3.6.0 以上をご利用のお客様は別途「SNMPTRAP 監視設定マニュアル」をご利用ください。

X-MON の入門リファレンスや監視エージェント導入、Windows サーバの監視方法など本書以外のマニュアルについては X-MON サポートページにログインしてご確認ください。



X-MON サポートサイト

<https://x-mon.jp/support/>

2017 年 11 月

改定履歴
2013 年 02 月 初版
2013 年 06 月 二版
2017 年 11 月 三版

Copyright © 2004-2017 X-TRANS, Inc. All Rights Reserved.

目次

1	ログ監視	5
1.1	ログ監視	5
1.1.1	ログの閲覧権限について	6
1.1.2	監視設定例	7
1.1.3	試行回数の設定	7
1.1.4	volatile サービスの設定	8
1.1.5	設定項目一覧	9
1.2	NRPE 経由でのログ監視	10
1.2.1	ログの閲覧権限について	10
1.2.2	監視設定例	10
1.2.3	試行回数の設定	11
1.2.4	volatile サービスの設定	11
1.2.5	設定項目一覧	12
1.3	ログ監視のステータス情報について	13
1.4	ログ監視の正規表現について	13
1.4.1	ログで userXX からアクセスがあった場合に検知する	13
1.4.2	行に対する And 検索	14
2	syslog 管理	15
2.1	ログ転送の設定	15
2.1.1	X-MON サーバ（転送先）	15
2.1.2	監視ホスト（転送元）	16
2.1.3	注意点	16
2.1.4	ログ転送の確認	17
2.1.5	X-MON でのログ検出の範囲	17
2.2	syslog 管理画面	17
2.2.1	新規作成	18
2.2.2	プロパティベースフィルター	21
2.2.3	式ベースフィルター	22
2.3	監視設定例（プロパティベースフィルター）	23
2.3.1	基本的な設定例	23
2.3.2	「対象」の設定例	29
2.3.3	「条件否定」の設定例	30
2.3.4	「比較内容」の設定例	30
2.4	監視設定例（式ベースフィルター）	33

2.4.1	基本的な設定例.....	33
2.4.2	設定項目について	39
2.4.3	ファシリティ	39
2.4.4	プライオリティ.....	41
2.4.5	メッセージ.....	42
2.4.6	タグ	43
2.4.7	パネルを追加して複数の条件で検索する	44
2.4.8	注意点	52
2.5	共通の設定動作.....	53
2.5.1	通知条件を編集する	53
2.5.2	通知条件を削除する	57
2.5.3	複数の条件を一つの通知先に設定する	59
2.5.4	複数のホストで一つの通知先を設定する	61
2.5.5	自動復旧の条件.....	62
2.6	サービス設定からの設定について（共通）	63
2.6.1	通知先を編集する	63
2.6.2	ログを検知するたびに通知を行う（volatile サービスの設定）	68
2.6.3	アクティブチェックと試行回数の設定について.....	69
3	SNMP TRAP 監視.....	70
3.1	監視概要.....	70
3.1.1	監視について	71
3.1.2	MIB の依存関係について.....	71
3.1.3	監視ホストの設定について	72
3.2	TRAP する機器の確認.....	72
3.2.1	MIB ファイルの探し方	72
3.3	MIB ファイルの X-MON への登録	74
3.3.1	MIB ファイルを登録する	74
3.3.2	MIB ファイル登録時のエラーについて	77
3.3.3	SNMP TRAP 管理画面メニューについて	78
3.3.4	MIB の文字コード変更する	79
3.3.5	MIB ファイルの内容をプレビューする	79
3.3.6	MIB を削除する	80
3.4	TRAP 通知条件の設定.....	82
3.4.1	TRAP 通知条件の設定例.....	82
3.4.2	通知条件の確認する	87
3.4.3	通知条件の編集する	89

3.4.4	通知条件の削除する	91
3.4.5	Data Binding について	93
3.5	動作確認テスト	98
3.5.1	テストコマンドの発行	98
3.5.2	TRAP 履歴	99
3.5.3	監視の復旧方法	100
3.5.4	その他の機器でのテスト	102
3.6	任意の SNMP TRAP を設定する	103
3.6.1	設定画面	103
3.6.2	OID について	105
3.6.3	設定例(Linux サーバからの任意 TRAP 通知)	106
3.6.4	設定例 (Windows サーバからの任意 TRAP 通知)	108
3.6.5	通知条件の編集する	118
3.6.6	通知条件の削除する	121
3.7	不明な TRAP を通知する	124
3.7.1	設定画面	124
3.7.2	設定例	125
3.7.3	通知条件を編集する	127
3.7.4	通知条件を削除する	130
3.7.5	非監視 TRAP の運用使用例	131
3.8	サービス設定からの設定について (共通)	132
3.8.1	通知先を編集する	132
3.8.2	TRAP を受信するたびに通知を行う (volatile サービスの設定)	137
3.8.3	アクティブチェックと試行回数の設定について	138

1 ログ監視

ここでは X-MON を用いたログ監視について解説していきます。

X-MON ではログ監視を用いて、ログ（テキストファイル）内に指定の文字列が出現するかを監視し検知する事が出来ます。

ログ監視は 3 つ用意されています。

・ログ監視

X-MON サーバ自身のログを監視します。

どのログファイルを監視するか任意に指定が出来ます。

・NRPE 経由でのログ監視

監視対象ホストのログを NRPE を用いて監視します。

どのログファイルを監視するか任意に指定が出来ますので、

syslog 転送出来ないアプリケーションのログを監視する事が出来ます。

・syslog 管理

X-MON は syslog サーバとしても動作しますので、監視対象ホストの syslog を X-MON へ送り監視します。syslog のフォーマットが決まっていますので、プライオリティやファシリティ別のフィルターを使用する事が出来ます。

syslog の設定によりログが大きくなる可能性もありますので運用負荷は高くなります。

1.1 ログ監視

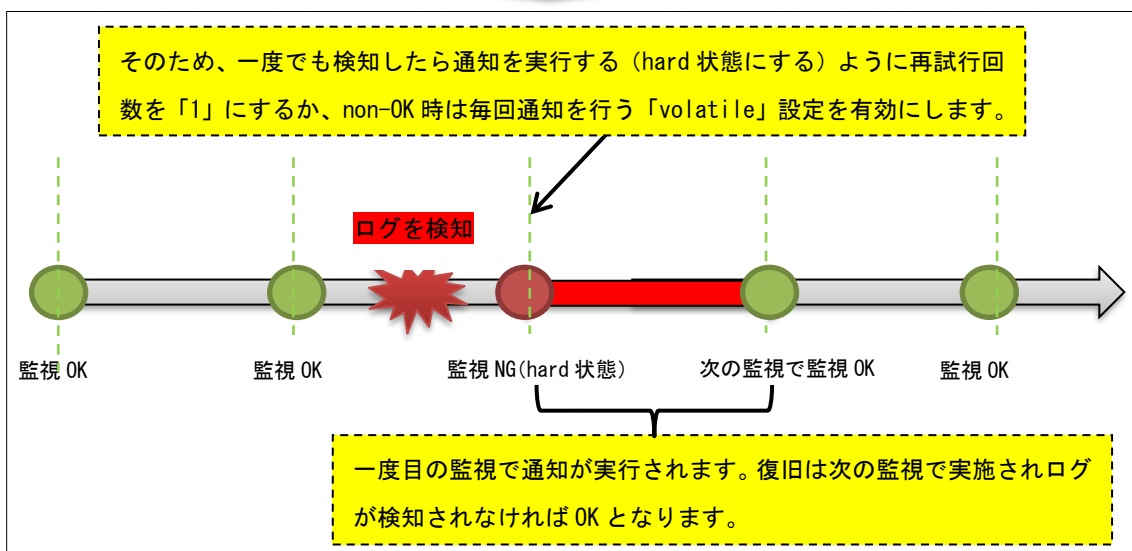
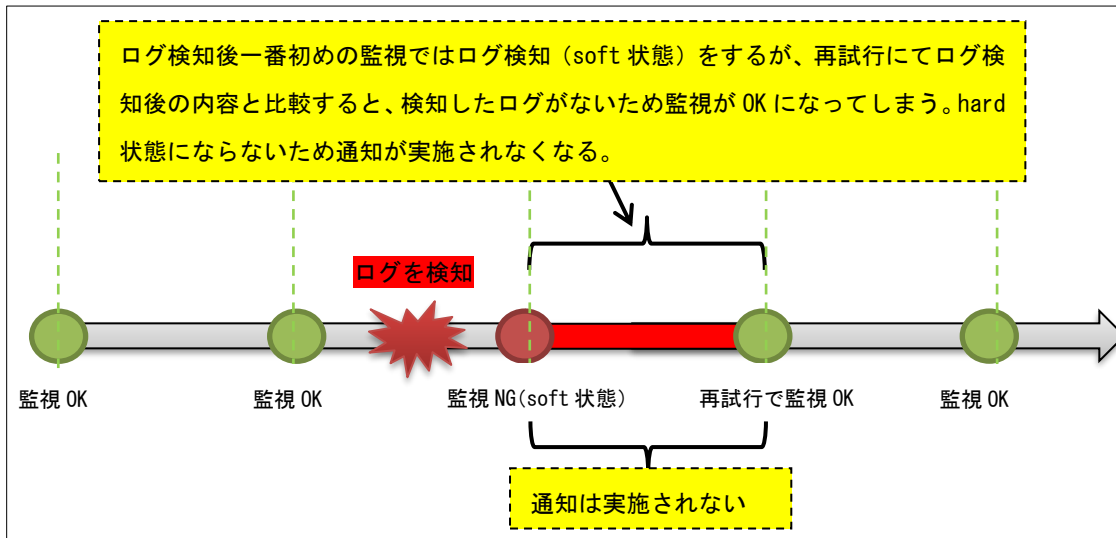
監視グループ	チェックコマンド
ログ監視	ログ監視

X-MON サーバ内のテキストファイルに指定した文字列が出現するかどうか監視を行います。

監視対象ファイルに指定した文字列が出現した場合、監視ステータスを CRITICAL にします。監視対象ファイルが存在しない場合、監視ステータスを UNKNOWN にします。

この監視を設定する際には、サービス設定画面の「高度な設定」タブ内の「volatile サービス」で「有効にする」を選択して、指定した文字列が出現する度に通知するように設定する必要があります。また、「監視の詳細設定」タブ内の「試行回数」で「1」を入力して、指定した文字列が 1 度出現したら通知するように設定する必要があります。

図 ログ監視の設定について



1.1.1 ログの閲覧権限について

指定したログが X-MON を実行する x-mon ユーザで読み取れる権限が必要となります。読み取り権限がない場合は読み取り権限を付与してください。

例として、/var/log/messages を監視する場合、デフォルトでは root のみ権限があります。

```
# ls -la /var/log/messages
-rw----- 1 root root 548037 12 月 12 16:03 /var/log/messages
```

所有者ごとに変更するとサーバ運用に問題が発生しやすいので、グループ設定を x-mon グループに変更します。

```
# chgrp x-mon /var/log/messages
# ls -la /var/log/messages
-rw----- 1 root x-mon 548227 12月 12 16:06 /var/log/messages
```

グループが x-mon になった事を確認して、グループ権限に読み取りを付与します。

```
# chmod g+r /var/log/messages
# ls -la /var/log/messages
-rw-r----- 1 root x-mon 548227 12月 12 16:06 /var/log/messages
```

これで x-mon グループに所属している x-mon ユーザでも読み取りが可能となります。

1.1.2 監視設定例

監視設定例として X-MON サーバの /var/log/messages を監視対象のログとします。ログを比較するための一時ファイルのパスを /tmp/kanshi_messages_old とします。

エラー文字列で検出する文字列を指定します。

入力は半角英数字で、大文字と小文字を区別しますので注意してください。

例では「sshd」を指定します。

図 監視設定例

サービス監視用コマンド	
ログ監視	▼
ログ監視	▼
対象ファイルパス	/var/log/messages
一時ファイルパス	/tmp/kanshi_messages_old
エラー文字列	sshd

ログ監視で 1 度でもエラー文字列を検知したら通知するように設定を行います。「**試行回数の設定**」か「**volatile サービスの設定**」のどちらかを設定してください。

1.1.3 試行回数の設定

下にある「監視の詳細設定」を開きます。ログ監視ではデフォルトで試行回数は「3」になっていますので、「1」に変更します。

図 試行回数

基本設定

監視の詳細設定

アクティブチェック
有効にする ▾

パッシブチェック
有効にする ▾

監視時間帯
24時間365日 ▾

試行回数
1

監視間隔(分)
5

再試行間隔(分)
1

通知の詳細設定

フラッピングの設定

高度な設定

1.1.4 volatile サービスの設定

下にある「高度な設定」を開きます。ログ監視ではデフォルトで「無効」になっていますので「有効」へ変更します。

図 volatile サービス

高度な設定

オブセスオーバー機能
無効にする ▾

volatileサービス
有効にする ▾

フレッシュネスチェック
無効にする ▾

フレッシュネスしきい値(秒)
0

パフォーマンスデータ処理
有効にする ▾

監視ステータス状態の保存
有効にする ▾

監視設定情報の保存
有効にする ▾

状態追跡オプション

- ☐ サービスのOKを追跡する
- ☐ サービスのWARNINGを追跡する
- ☐ サービスのUNKNOWNを追跡する
- ☐ サービスのCRITICALを追跡する

設定が完了したら作成を行い、X-MON を再起動してください。

ログ監視では比較する一時ファイルを作成するため、作成後一回目のチェックのみ「Log check data initialized」となります。

図 一回目の監視

正常(OK)	2012-12-12 16:17:02	0日と00時間 00分29秒	1/1	Log check data initialized...
--------	---------------------	-------------------	-----	-------------------------------

二回目のチェック以降は比較が実施されます。正常に監視が OK の場合は下記のように「Log check ok - 0 pattern matches found」が表示されます。

図 正常な場合

正常(OK)	2012-12-12 16:18:50	0日と00時間 12分24秒	1/1	Log check ok - 0 pattern matches found
--------	---------------------	-------------------	-----	--

異常を検知し CRITICAL となった場合は下記のように検知した文字列を表示します。
(セキュリティのため一部文字列を伏せております)

図 異常な場合

異常 (CRITICAL)	2012-12-12 16:18:01	0日と00時間 02分34秒	1/1	(1) < Dec 12 16:17:09 [redacted] sshd[22075]: Received disconnect from [redacted]: Bye Bye
------------------	---------------------	-------------------	-----	--

対象のファイルに読み取り権限がない場合は UNKNOWN を検知します。

図 権限がない場合

不明 (UNKNOWN)	2012-12-12 16:23:55	0日と00時間 00分05秒	1/1	Log check error: Log file /var/log/messages is not readable!
-----------------	---------------------	-------------------	-----	--

「[1.1.1 ログの閲覧権限について](#)」を参考に読み取り権限を付与してください。

1.1.5 設定項目一覧

対象ファイルパス	監視対象のテキストファイルのファイルパスを指定します。
一時ファイルパス	監視の際に生成する一時ファイルのファイルパスを指定します。
エラー文字列	監視ステータスを CRITICAL とする文字列を指定します。監視対象のテキストファイルに指定した文字列が出現した場合、監視ステータスを CRITICAL とします。

1.2 NRPE 経由でのログ監視

監視グループ	チェックコマンド
ログ監視	NRPE 経由でのログ監視

NRPE を利用して、監視対象ホストのテキストファイルに指定した文字列が出現するかどうか監視を行います。

監視対象ファイルに指定した文字列が出現した場合、監視ステータスを CRITICAL にします。監視対象ファイルが存在しない場合、監視ステータスを UNKNOWN にします。

この監視を設定する際には、サービス設定画面の「高度な設定」タブ内の「volatile サービス」で「有効にする」を選択して、指定した文字列が出現する度に通知するように設定する必要があります。また、「監視の詳細設定」タブ内の「試行回数」で「1」を入力して、指定した文字列が 1 度出現したら通知するように設定する必要があります。

1.2.1 ログの閲覧権限について

指定したログが NRPE を実行するユーザで読み取れる権限が必要となります。
設定については NRPE 導入手順をご参照ください。

1.2.2 監視設定例

監視設定例として監視対象ホストの/var/log/httpd/error_log 監視対象のログとします。
ログを比較するための一時ファイルのパスを/tmp/httpd_error とします。
エラー文字列で検出する文字列を指定します。
入力は半角英数字で、大文字と小文字を区別しますので注意してください。
例では「error」を指定します。

図 監視設定例

サービス監視用コマンド

ログ監視

NRPE経由でのログ監視

対象ファイルパス

/var/log/httpd/error_log

一時ファイルパス

/tmp/httpd_error

エラー文字列

error

NRPEタイムアウト
(秒)

15

ログ監視で 1 度でもエラー文字列を検知したら通知するように設定を行います。「**試行回数の設定**」か「**volatile サービスの設定**」のどちらかを設定してください。

1.2.3 試行回数の設定

下にある「監視の詳細設定」を開きます。ログ監視ではデフォルトで試行回数は「3」になっていますので、「1」に変更します。

図 試行回数

The screenshot shows the 'Monitoring Detailed Settings' (監視の詳細設定) tab. The 'Retry Count' (試行回数) field is highlighted with a red box and set to '1'. Other settings include 'Active Check' (アクティブチェック) set to 'Effective' (有効にする), 'Passive Check' (パッシブチェック) set to 'Effective' (有効にする), 'Monitoring Period' (監視時間帯) set to '24 hours 365 days' (24時間365日), 'Monitoring Interval (min)' (監視間隔(分)) set to '5', and 'Retry Interval (min)' (再試行間隔(分)) set to '1'.

1.2.4 volatile サービスの設定

下にある「高度な設定を開きます。ログ監視ではデフォルトで「無効」になっているので「有効」へ変更します。

図 volatile サービス

The screenshot shows the 'Advanced Settings' (高度な設定) tab. The 'volatile service' (volatileサービス) field is highlighted with a red box and set to 'Effective' (有効にする). Other settings include 'Obscure Function' (オブセスオーバー機能) set to 'Ineffective' (無効にする), 'Refreshness Check' (フレッシュネスチェック) set to 'Ineffective' (無効にする), 'Refreshness Threshold (sec)' (フレッシュネスしきい値(秒)) set to '0', 'Performance Data Processing' (パフォーマンスデータ処理) set to 'Effective' (有効にする), 'Monitoring Status State Saving' (監視ステータス状態の保存) set to 'Effective' (有効にする), 'Monitoring Setting Information Saving' (監視設定情報の保存) set to 'Effective' (有効にする), and 'Status Tracking Options' (状態追跡オプション) with checkboxes for 'OK', 'WARNING', 'UNKNOWN', and 'CRITICAL'.

設定が完了したら作成を行い、X-MON を再起動してください。

ログ監視では比較する一時ファイルを作成するため、作成後一回目のチェックのみ

「Log check data initialized」となります。

図 一回目の監視

正常(OК)	2012-12-12 16:17:02	0日と00時間 00分29秒	1/1	Log check data initialized...
--------	---------------------	-------------------	-----	-------------------------------

二回目のチェック以降は比較が実施されます。正常に監視が OK の場合は下記のように「Log check ok - 0 pattern matches found」が表示されます。

図 正常な場合

正常(OК)	2012-12-12 16:18:50	0日と00時間 12分24秒	1/1	Log check ok - 0 pattern matches found
--------	---------------------	-------------------	-----	--

異常を検知し CRITICAL となった場合は下記のように検知した文字列を表示します。

(セキュリティのため一部文字列を伏せております)

図 異常な場合

異常 (CRITICAL)	2012-12-13 15:54:55	0日と00時間 00分09秒	1/1	(3)<[Thu Dec 13 15:54:46 2012] [error] [client] client denied by server configuration: /var/www/html/moji2.html
------------------	---------------------	-------------------	-----	--

対象のファイルに読み取り権限がない場合は WARNING を検知します。

図 権限がない場合

警告 (WARNING)	2012-12-13 15:58:03	0日と00時間 00分37秒	1/1	NRPE: Unable to read output
-----------------	---------------------	-------------------	-----	-----------------------------

別途マニュアル「NRPE 導入手順」をご参照ください。

1.2.5 設定項目一覧

対象ファイルパス	監視対象のテキストファイルのファイルパスを指定します。
一時ファイルパス	監視の際に生成する一時ファイルのファイルパスを指定します。
エラー文字列	監視ステータスを CRITICAL とする文字列を指定します。監視対象のテキストファイルに指定した文字列が出現した場合、監視ステータスを CRITICAL とします。
NRPE タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

1.3 ログ監視のステータス情報について

ログ監視のステータス情報は複数の行が検知した場合、行の数を表示しますが、表示されるステータス情報の部分は 1 行しか表示されません。
そのため、ログ検知をした場合は行数を確認し、実際に監視ホストにてログを確認するような運用をお願いします。

図 1 行だけ検知している場合

異常 (CRITICAL)	2012-12-13 16:41:01	0日と00時間 00分08秒	1/1	(1) Dec 13 16:40:44 [redacted] nrpe[22834]: Error: Request contained illegal metachars!
------------------	---------------------	-------------------	-----	---

図 複数行検知している場合

異常 (CRITICAL)	2012-12-13 15:54:55	0日と00時間 00分09秒	1/1	(3) [Thu Dec 13 15:54:46 2012] [error] [client [redacted]] client denied by server configuration: /var/www/html/moji2.html
------------------	---------------------	-------------------	-----	--

また、下記のような Unknown が表示される事があります。

図 Unknown 表示

不明 (UNKNOWN)	2012-12-17 20:13:55	0日と00時間01 分11秒	2/3	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.
-----------------	---------------------	-------------------	-----	--

この場合は、検知文字列の入力にて使用出来ない文字列が入っており、監視ホストの NRPE プラグインでエラーが発生しています。

現状、X-MON の仕様により記号や漢字を入力しても入力エラーにならずに監視設定が出来てしまいます。そのため、入力の際は半角英数字での入力をお願いします。

1.4 ログ監視の正規表現について

ログ監視で検知する文字列を入力出来ますが、監視プラグインの仕様で正規表現が使用できます。

使用出来る正規表現は下記となります。

.(半角のドット)	任意の一文字
*(半角のアスタリスク)	0 回以上の繰り返し

1.4.1 ログで userXX からアクセスがあった場合に検知する

サーバへの sshd での接続や web サービスで特定のユーザからアクセスがあった場合に障害としたい例です。user01 や user35 など user の後に数字が入るとすると、検知文字列として「user*」とすることで検知出来ます。

「user3*」とすると「user300」など 3 桁の数字があった場合も検知されてしまいます。

1.4.2 行に対する And 検索

「.」と「*」を組み合わせる事でログの 1 行に対して and 検索が可能です。

例として下記のようなログがあるとします。

```
Dec 13 16:40:44 x-mon_manual xinetd[1085]: START: nrpe pid=22834 from>::ffff:192.168.19.201
Dec 13 16:40:44 x-mon_manual nrpe[22834]: Error: Request contained illegal metachars!
Dec 13 16:40:44 x-mon_manual nrpe[22834]: Client request was invalid, bailing out...
Dec 13 16:40:44 x-mon_manual xinetd[1085]: EXIT: nrpe status=0 pid=22834 duration=0(sec)
Dec 13 16:41:01 x-mon_manual xinetd[1085]: START: nrpe pid=22837 from>::ffff:192.168.19.201
```

このログの中から

```
Dec 13 16:40:44 x-mon_manual nrpe[22834]: Error: Request contained illegal metachars!
```

の行だけを検知させる場合は検知文字列として「**nrpe.*Error**」を指定します。

そうすると、「nrpe」の文字列を検知した行に対して、その行の **nrpe の文字列以降**に

「Error」の文字列もあるか検索し一致した場合は検知するという形となります。

注意として、検知したい順番があります。「Error.*nrpe」とした場合、Error を検知し、その行を検索しますが Error の文字列以降を検索しますので、上記例ログでは検知しない形となります。

2 syslog 管理

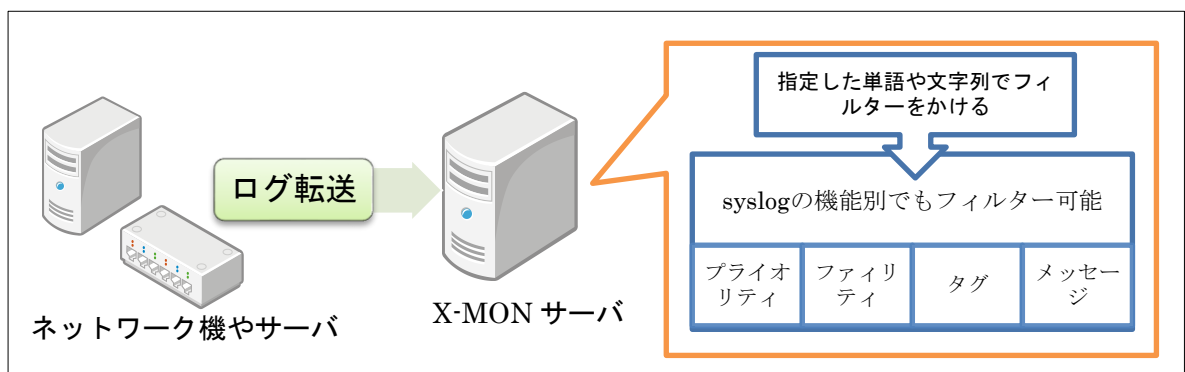
syslog 管理は X-MON をログサーバにして、監視ホストからログを転送させて指定した文字列がログに発生した場合検知して指定したステータスを通知します。

ログ監視との違いは正規表現が使用でき、複数条件を指定出来る事です。

また検知した際のステータスの種類も選択出来ます。

そのため、検知すれば CRITICAL という条件と検知すれば OK(復旧)を組み合わせる事で自動で監視復旧をさせる事も可能です。

図 ログ転送



フィルターは rsyslog が実施するので、X-MON の監視設定的にはパッシブチェックとなります。

X-MON サーバでは syslog 管理として rsyslog を使用しています。

本書では監視ホストの syslog 管理も多くのディストリビューションで使用されている rsyslog を例に取り上げます。ネットワーク機器のログ転送方法についてはそれぞれのマニュアルをご参照ください。

2.1 ログ転送の設定

2.1.1 X-MON サーバ（転送先）

X-MON では rsyslog を制御しています。

rsyslog は以前の syslog では UDP のみだったポートが TCP にも対応しております。

そのため X-MON サーバで iptables やファイアウォールでポート制限を実施している場合は下記ポートを許可するようにしてください。

TCP/UDP 514 番

2.1.2 監視ホスト（転送元）

rsyslog の設定で X-MON サーバへログを転送するようにします。

設定ファイルは/etc/rsyslog.conf、もしくは/etc/rsyslog.d/以下のファイルとなります。

下記は全てのログを X-MON サーバ(IP アドレスが 192.168.100.1 の場合) へ転送する設定です。(＃はコメント行です)

```
#to X-MON
*. * @192. 168. 100. 1
```

TCP を使って転送する場合は@を二つにしてください。また、明示的にポート番号を記載する場合は IP アドレスの後ろに「:」を付けてポート番号を記載してください。

(＃はコメント行です)

```
#to X-MON
*. * @@192. 168. 100. 1:514
```

特定のログを転送する場合はファシリティ、プライオリティを設定し記載してください。例として authpriv.info のみを転送する場合は下記のようになります。(＃はコメント行です)

```
#to X-MON
authpriv. info @192. 168. 100. 1
```

2.1.3 注意点

rsyslog では出力フォーマットをカスタマイズ出来ます。

カスタマイズした出力フォーマットのまま X-MON サーバへログを転送すると正常に検知しない場合がございます。

そのため、監視ホストでログの出力フォーマットをカスタマイズしている場合は X-MON サーバへ転送するログの出力フォーマットを rsyslog のデフォルトのフォーマットにするように指定してください。

フォーマットの種類は「**RSYSLOG_TraditionalFileFormat**」を指定し、X-MON サーバの IP アドレス、もしくはポート番号の後ろに「;」を付けて記載します。

例：すべてのログを 192.168.100.1 の X-MON サーバの TCP/514 番ポートへ **RSYSLOG_TraditionalFileFormat** を指定して転送する

```
#to X-MON
*. * @@192. 168. 100. 1:514;RSYSLOG_TraditionalFileFormat
```

2.1.4 ログ転送の確認

ログが正常に転送されているか確認してみましょう。

監視ホストで

```
# logger -i -t TEST -p user.warning "X-MON"
```

を発行し、監視ホストと X-MON サーバの/var/log/messages を確認します。

```
Dec 20 16:27:09 man-x64 TEST[1401]: X-MON
```

というログが両サーバにて記載されていれば正常にログが転送されています。

2.1.5 X-MON でのログ検出の範囲

ログ検出の範囲は、X-MON に転送されたログ全てが対象となります。

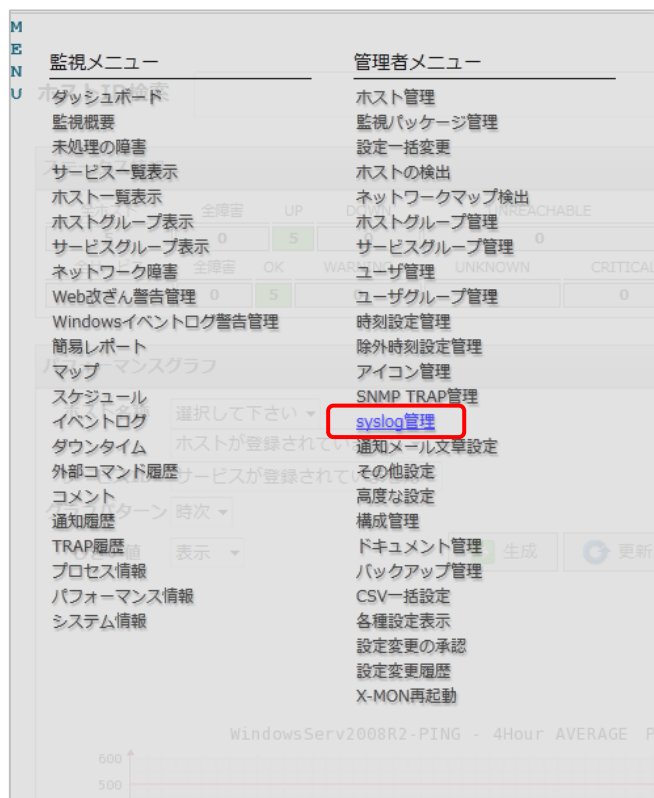
rsyslog でログに書き出される前に X-MON にて処理を実施しています。

X-MON サーバの rsyslog の設定ファイルは /etc/rsyslog.d/syslog.conf ですが、特別に別ファイルへ出力させたりする必要がある場合以外に設定ファイルは編集しないようにお願いします。(X-MON の動作関係の設定も記載されています)

2.2 syslog 管理画面

syslog 管理では通常の監視の追加方法とは異なり、syslog 管理という独立したメニューで行います。


図 MENU



また、ログを検知する方法はプロパティベースフィルター、式ベースフィルターの 2 種類があります。

2.2.1 新規作成


syslog 通知条件一覧が開きます。

 syslog 管理



何も設定していない場合は何も表示されません。

新規作成をクリックして、監視設定の作成を行います。検知するログの条件は、設定項目「フィルター」で設定します

 新規作成

登録ログ条件名			
<input type="text"/>			
フィルター			
プロパティベースフィルター ▼			
対象	条件否定	比較内容	詳細内容/正規表現
メッセージ ▼	なし ▼	部分一致 ▼	<input type="text"/>
対象ホスト			
<div> <div>↑</div> <div>↓</div> <div>↑(選択) ↓(外す)</div> <div>選択して下さい ▼</div> <div>↑</div> <div>↓</div> </div>			
通知先グループ			
<div> <div>↑</div> <div>↓</div> <div>↑(選択) ↓(外す)</div> <div>選択して下さい ▼</div> <div>↑</div> <div>↓</div> </div>			
<input type="checkbox"/> チェックで上書き登録/チェックなしで通知先を更新しない			
通知先サービス名			
<input type="text"/> LOG			
通知ステータス			
<input checked="" type="radio"/> OK <input type="radio"/> WARNING <input type="radio"/> CRITICAL <input type="radio"/> UNKNOWN			

登録ログ条件名	登録するログ通知条件コードの任意の ID を入力します。新規作成時のみ設定が可能であり、変更はできません。 入力制限：入力必須、半角英数字、アンダーバー、ドット、ハイフンのみ、重複する名称の登録不可。
フィルター	フィルターをプロパティベースフィルター、式ベースフィルターから選択します。フィルターによって入力項目が変わります。
対象ホスト	検索対象となるホストを選択します。選択したいホストの頭文字を選択し、表示された選択肢からホストを選択し、選択ボタンを押します。ホストを除外する場合は、任意のホストを選択後、外すボタンを押します。
通知先グループ	通知先グループを選択します。選択したい通知先グループの頭文字を選択し、表示された選択肢から通知先グループを選択し、「↑(選択)」をクリックします。通知先グループを除外する場合は、任意の通知先グループを選択後、「↓(外す)」ボ

	<p>タンをクリックします。</p> <p>通知先グループの登録はユーザグループ管理 - ユーザグループの作成、編集を参照して下さい。</p> <p>設定しない場合は、X-MON の管理画面のみでの通知となります。</p>
チェックで上書き登録/チェックなしで通知先を更新しない	<p>同じ通知先サービス名で複数の登録ログを設定する場合に通知先グループの設定を上書きするか更新しないかをチェック出来ます。同じ通知先サービス名で複数の登録ログを設定する際は注意してください。</p>
通知先サービス名	<p>ここで指定した名前で、対象ホストにサービスが登録されます。新規作成時のみ設定が可能であり、変更はできません。</p> <p>入力制限：入力必須、半角英数字,アンダーバー,ドット,ハイフンのみ。</p> <p>また、以下の通知先サービス名は設定できません。</p> <ul style="list-style-type: none"> ・「-VMPERF」で終わるサービス ID ・間に「-VMPERF-」を含むサービス ID ・間に「-VMWARE-」を含むサービス ID
通知ステータス	<p>通知する際に発行するステータスを選択します。</p>

登録ログ条件名は syslog 管理画面で表示する時の名前です。

X-MON のサービス一覧表示などで表示させた際には「通知先サービス名」が使用されます。別々の名前にするとわかりにくくなりますので、同じ名前にしておくと運用しやすくなります。

2.2.1.1 チェックで上書き登録/チェックなしで通知先を更新しないについて

こちらの項目は、現在サービスに設定している通知先グループの設定情報を上書きして設定するかどうか設定する項目となります。

例) ホスト「X-MON」のサービス「LOG」に通知先グループ「dev-team」が登録されている とき、以下の syslog 監視を設定する。

①

対象ホスト：X-MON

通知先サービス名：LOG

通知先グループ：op-team

チェックで上書き登録/チェックなしで通知先を更新しない：チェックを入れる

②

対象ホスト：X-MON

通知先サービス名：LOG

通知先グループ：op-team

チェックで上書き登録/チェックなしで通知先を更新しない：チェックを外す

①の場合ですと、ホスト「X-MON」のサービス「LOG」の通知先グループ「dev-team」が「op-team」に上書きされます。

②の場合ですと、上書き処理は発生せず、ホスト「X-MON」のサービス「LOG」の通知先グループは「dev-team」となります。

この処理では、対象ホストを追加/削除した場合も同様です。

そのため、同じ通知先サービス名で複数の対象ホストを登録している場合は全て同じ通知先グループへ通知されます。

対象ホストによって通知先グループを分けたい場合は、通知先サービス名をそれぞれ作成する必要があります。

2.2.2 プロパティベースフィルター

単純な文字列、指定するファシリティやプライオリティを検知する場合はプロパティベースフィルターをお勧めします。

ログは1行ずつのテキストとなっています。ログ管理にて検知するログは1行単位での範囲となります。

そのため、or 検索では、指定した単語が出た時点で検知します。

and 検索をする場合は、一つ目に指定した単語が出た時点で、その行に他の単語があるかを検索します。

図 プロパティベースフィルター

フィルター			
プロパティベースフィルター ▼			
対象	条件否定	比較内容	詳細内容/正規表現
メッセージ ▼	なし ▼	部分一致 ▼	

対象	検索する対象を選択します。 選択された対象に検索文字列が含まれていた場合、通知を行います。ファシリティ、プライオリティ、メッセージ、タグが選択出来ます。
条件否定	条件否定を行うか行わないかを設定します。条件否定を行わない場合、「なし」を選択します。

比較内容	指定した文字列の検索方法を選択します 部分一致、完全一致、前方一致、正規表現が選択出来ます。
詳細内容/正規表現	検索文字列を入力します。比較内容で正規表現を選択した場合、正規表現を入力します。

2.2.3 式ベースフィルター

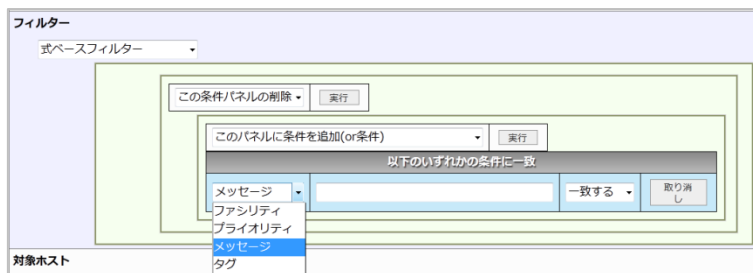
式ベースフィルターでは、複数の検索条件を設定することが可能です。いずれかの条件に一致した際に通知を行いたい場合は、同じパネル内に条件を追加していきます。全ての条件に一致した際に通知を行いたい場合は、別のパネル内に条件を追加します。

ログは 1 行ずつのテキストとなっています。ログ管理にて検知するログは 1 行単位での範囲となります。

式ベースの場合、設定により行全体での比較も可能です。

式フィルターで設定する条件の項目は、左端から、検索項目、検索内容、条件指示です。検索項目の説明は以下のとおりです。

図 式ベースフィルター



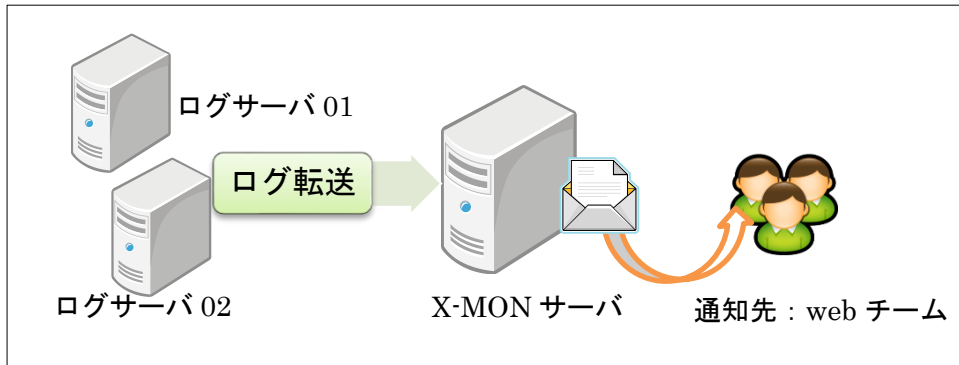
ファシリティ	ファシリティのステータスで条件を設定します。任意のステータスを選択し、そのステータスと一致するか一致しないかを選択します。
プライオリティ	プライオリティのステータスで条件を設定します。任意のステータスを選択し、そのステータスと一致するか一致しないかを選択します。
メッセージ	メッセージの内容で条件を設定します。入力文字列とメッセージが一致するかないかを選択します。
SYSLOG タグ	SYSLOG タグの内容で条件を設定します。SYSLOG タグが入力文字列と一致するかないかを選択します。

2.3 監視設定例（プロパティベースフィルター）

プロパティベースフィルター形式を例に交えながら解説を行います。

下記のサンプルネットワークをご確認頂きながらご参照ください。

図 サンプルネットワーク



2.3.1 基本的な設定例

2.3.1.1 新規作成

[MENU] の [syslog 管理] 内の [新規作成] を開き、条件を入力します。

図 MENU

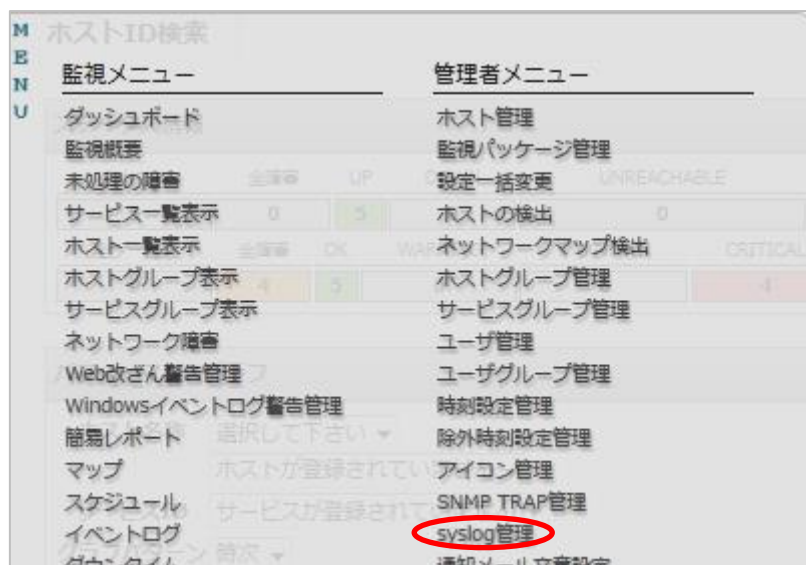


図 新規作成



下記の条件で設定してみます。

登録ログ条件名	LOG_X-MON-TEST01
対象	メッセージ
条件否定	なし
比較内容	完全一致
詳細内容/正規表現	X-MON-TEST
対象ホスト	ログサーバ01
通知先グループ	web チーム
通知先サービス名	LOG_X-MON-TEST01
通知ステータス	CRITICAL

図 入力例

The screenshot shows the X-MON configuration interface with the following fields and values, all highlighted with red boxes:

- 登録ログ条件名:** LOG_X-MON-TEST01
- フィルター:**
 - プロパティベースフィルター
 - 対象: メッセージ
 - 条件否定: なし
 - 比較内容: 完全一致
 - 詳細内容/正規表現: X-MON-TEST
- 対象ホスト:** ログサーバ01
- 通知先グループ:** Webチーム
- 通知先サービス名:** LOG_X-MON-TEST01
- 通知ステータス:** CRITICAL (selected)
- Buttons:** キャンセル and 作成と承認 (both highlighted with red circles)

Additional interface elements include a checkbox for "チェックで上書き登録/チェックなしで通知先を更新しない" and a list of notification destinations (W) under the "通知先グループ" section.

入力が完了したら一番下の[作成と承認]で反映後、X-MON を再起動します。

2.3.1.2 確認

設定出来たか確認してみましょう。

syslog 管理を開くと作成した LOG_X-MON-TEST01 があります。

図 syslog 管理



詳細表示を開くと設定が確認出来ます。

図 詳細表示



サービス一覧表示を見てみましょう。

図 サービス一覧

logsv01 (ログサーバー01)	LOG X-MON-TEST01	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
-----------------------	------------------	-----------------	-----	-----	-----	---------------------------------

監視が追加されています。

syslog 管理ではフィルターして検知するのを rsyslog が行い、結果を X-MON へ通知します。そのため監視はパッシブチェックとなります。そのため画像のように「このサービスはチェックするようにはスケジュールされていません。」となります。

2.3.1.3 検知テスト

それでは検知するかテストしてみましょう。

監視ホスト側で下記コマンドを発行します。

```
# logger -i -t TEST -p user.warning "X-MON-TEST"
```

発行後サービス一覧表示画面を開きます。下記画像のように CRITICAL を検知しました。

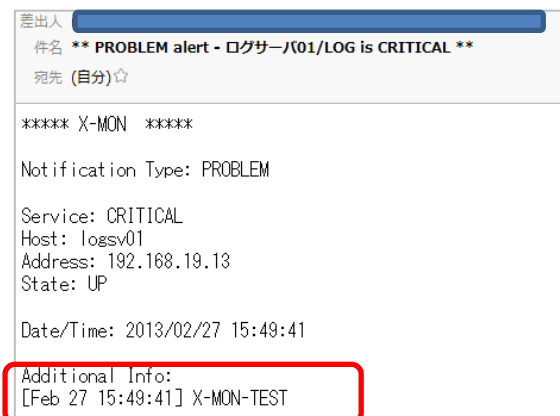
図 ログを検知

logsv01 (ログサーバー01)	LOG X-MON-TEST01	異常 (CRITICAL)	N/A	N/A	1/1	[Dec 28 22:06:47] X-MON-TEST
-----------------------	------------------	------------------	-----	-----	-----	------------------------------

例では通知先グループを設定していますので下記のようなメールが来ます。

デフォルトの通知内容の場合、メール本文の「Additional Info:」の部分にログの内容が記載されます。

図 通知メール



正常に検知出来ている事がわかりました。

2.3.1.4 監視を復旧させる

手動で監視を復旧させるにはパッシブの結果を送るという動作になります。

サービス一覧表示の監視名を開き、サービス情報画面の「サービス詳細」タブを開きます。

サービス詳細タブのメニューの中から「このサービスのパッシブチェックの結果を送信」を開きます。

図 サービス詳細タブ

サービス情報

logsv01(ログサーバ01)
サービスID: LOG_X-MON-TEST01
IPアドレス: 192.168.19.13

最終チェック時刻: N/A
次回チェック予定: 2012年12月28日 22時07分50秒

障害対応ガイド サービス詳細 ドキュメント 構成情報 イベントログ 通知履歴
外部コマンド履歴 コメント

サービス詳細タブのメニューの中から「このサービスのパッシブチェックの結果を送信」を開きます。

図 パッシブの結果を送信

このサービスの動作チェックを有効
このサービスの動作チェックを次回スケジュールに追加
このサービスのパッシブチェックの結果を送信
このサービスのパッシブチェックを停止
このサービスのObsessing Overを開始

下記のような画面となります。

図 パッシブチェック

外部コマンド

赤字の項目は必ず入力してください。入力していない場合エラーとなります。

リクエストしたコマンド: 指定したサービスのパッシブチェックの結果を登録する

ホストID: logsv01
サービスID: LOG_X-MON-TEST01
チェック結果: OK
チェック出力:
パフォーマンステータ:

発行 リセット

このコマンドは指定したサービスからのPassiveチェックの結果を送信します。これは作業が行われたり、作業を完了したり、セキュリティチェックなどに有効活用できます。

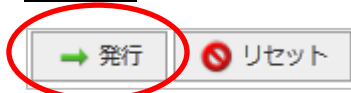
チェック結果を OK にします。(デフォルトで選択されています) チェック出力は必須入力となります。

例えば「ログ検知のテストのため OK」や実際の運用では「ログ確認、対応完了」などを記載するといいでしょう。

図 項目入力

入力出来たら発行を押します。

図 発行



コマンドを正常に受け付けた画面となります

図 発行後

復旧しているか確認しましょう。

サービス一覧表示にてステータス情報がパッシブの結果を送信の際に入力した「ログ検知のテストのため OK」というステータスとなり正常（OK）で復旧しています。

図 復旧後

logsv01 (ログサーバ01)	LOG X-MON-TEST01	正常 (OK)	2012-12-28 22:27:12	0日と00時間00分45秒	1/1	ログ検知のテストのためOK
----------------------	------------------	---------	---------------------	---------------	-----	---------------

また、通知先にも下記のような復旧のメールが届きます。

図 復旧通知メール

以上が基本的な設定例とテストとなります。

2.3.2 「対象」の設定例

「対象」について個別に設定例を記載します。

図 対象

対象は図のようにファシリティ、プライオリティ、メッセージ、タグの中から選択出来ます。

ファシリティの一覧は下記となります。

kern	user	mail	daemon	auth	syslog
lpr	news	uucp	cron	authpriv	ftp
ntp	audit	clock	alert	local0~7	

プライオリティの一覧は下記となります。

emerg	alert	crit	err (error)
warn (warning)	notice	info	debug

メッセージとタグは任意の文字列となります。

注意点としては、どの対象にしても、[詳細内容/正規表現]の欄に手動で入力します。そのためスペルの間違いに気を付けてください。

また、logger コマンドでのテスト時、監視ホスト上で発行する際にオプションでファシリティとプライオリティを指定しても X-MON サーバ上では違う値になる事があります。

例えば、監視ホストで下記コマンドを発行します。ファシリティに user プライオリティに warning を指定しています。

```
# logger -i -t TEST -p user.warning "X-MON-TEST"
```

監視ホスト側では下記のように出力されます。わかりやすいようにログ出力のフォーマットをカスタマイズしています。

```
Dec 29 21:49:32 man-x64 TEST[1370]: [user.warning]: X-MON-TEST
```

しかし、X-MON サーバでは下記のようにプライオリティが notice となります。

```
Dec 29 21:49:32 man-x64 TEST[1370]: [user.notice]: X-MON-TEST
```

そのため、サービスやアプリケーションでログを確認する際は X-MON サーバ上でどのようにログが転送されているかも確認するようにしてください。

2.3.3 「条件否定」の設定例

「条件否定」について個別に設定例を記載します。

図 条件否定

The screenshot shows the 'フィルター' (Filter) configuration window. At the top, there is a dropdown menu labeled 'プロパティベースフィルター' (Property-based Filter). Below it is a table with four columns: '対象' (Target), '条件否定' (Condition Negation), '比較内容' (Comparison Content), and '詳細内容/正規表現' (Detailed Content/Regular Expression). The '対象' column has a dropdown menu with 'ファシリティ' (Facility) selected. The '条件否定' column has a dropdown menu with 'なし' (None) selected. The '比較内容' column has a dropdown menu with '完全一致' (Exact Match) selected. The '詳細内容/正規表現' column is empty. Below the table, there is a section labeled '対象ホスト' (Target Host) with a text input field.

条件否定は[詳細内容/正規表現]の記述内容の否定を検知対象とします。イメージとしては、それ以外が対象となる形です。

注意点として、[対象]をメッセージにしている場合、記述内容の否定になってしまうため検知する内容が多くなってしまいます。

そのため、ファシリティ、プライオリティに対する否定で使用する事をお勧めします。

例：ファシリティが warning 以外を検知するようにする。

図 設定例

The screenshot shows the 'フィルター' (Filter) configuration window. At the top, there is a dropdown menu labeled 'プロパティベースフィルター' (Property-based Filter). Below it is a table with four columns: '対象' (Target), '条件否定' (Condition Negation), '比較内容' (Comparison Content), and '詳細内容/正規表現' (Detailed Content/Regular Expression). The '対象' column has a dropdown menu with 'ファシリティ' (Facility) selected. The '条件否定' column has a dropdown menu with '否定' (Negation) selected. The '比較内容' column has a dropdown menu with '完全一致' (Exact Match) selected. The '詳細内容/正規表現' column contains the text 'warning'. Below the table, there is a section labeled '対象ホスト' (Target Host) with a text input field.

2.3.4 「比較内容」の設定例

「比較内容」について個別に設定例を記載します。

図 比較内容

The screenshot shows the 'フィルター' (Filter) configuration window. At the top, there is a dropdown menu labeled 'プロパティベースフィルター' (Property-based Filter). Below it is a table with four columns: '対象' (Target), '条件否定' (Condition Negation), '比較内容' (Comparison Content), and '詳細内容/正規表現' (Detailed Content/Regular Expression). The '対象' column has a dropdown menu with 'メッセージ' (Message) selected. The '条件否定' column has a dropdown menu with 'なし' (None) selected. The '比較内容' column has a dropdown menu with '部分一致' (Partial Match) selected. The '詳細内容/正規表現' column is empty. Below the table, there is a section labeled '対象ホスト' (Target Host) with a text input field.

比較内容は下記 4 つを選択出来ます。

部分一致	完全一致	前方一致	正規表現
------	------	------	------

2.3.4.1 部分一致

指定した文字列を部分で検索し、検知します。

例えば、「X-MON-TEST」というメッセージを検知したい場合に「N-TES」と指定すれば検知する事が出来ます。

図 部分一致

フィルター			
プロパティベースフィルター ▼			
対象	条件否定	比較内容	詳細内容/正規表現
メッセージ ▼	なし ▼	部分一致 ▼	N-TES

2.3.4.2 完全一致

完全一致を検索し、検知します。

例えば、「X-MON-TEST」というメッセージを検知したい場合に「X-MON-TEST」と指定すれば検知する事が出来ます。

図 完全一致

フィルター			
プロパティベースフィルター ▼			
対象	条件否定	比較内容	詳細内容/正規表現
メッセージ ▼	なし ▼	完全一致 ▼	X-MON-TEST

完全一致のため、「X-MON-TEST-ERROR」というメッセージに対して「X-MON-TEST」を指定しても検知はされません。その場合は部分一致もしくは前方一致を使用します。

2.3.4.3 前方一致

指定した文字列の前方が合うか検索し検知します。

例えば、「X-MON-TEST」というメッセージを検知したい場合に「X-MON」と指定すれば検知する事が出来ます。

図 前方一致

フィルター			
プロパティベースフィルター ▼			
対象	条件否定	比較内容	詳細内容/正規表現
メッセージ ▼	なし ▼	前方一致 ▼	X-MON

2.3.4.4 正規表現

正規表現で検索し検知します。

一般的に多く用いられる「?」「*」「+」「.」、論理和である「|」も使用出来ます。

また、先頭を表す「^」や文末の「\$」も使用出来ます。

例：ファシリティが kern もしくは user の場合に検知する場合は「kern|user」とします。

図 正規表現

フィルター

プロパティベースフィルター ▼

対象	条件否定	比較内容	詳細内容/正規表現
ファシリティ ▼	なし ▼	正規表現 ▼	kern user

例：メッセージで「success」で終わる場合を検知するには「success\$」とします。

図 正規表現

フィルター

プロパティベースフィルター ▼

対象	条件否定	比較内容	詳細内容/正規表現
メッセージ ▼	なし ▼	正規表現 ▼	success\$

例：AND 検索（論理積）をしたい場合は正規表現で実現出来ます。

「 ^(?=.*文字列)(?=.*文字列).*\$ 」を使います。たとえば、X-MON と TEST で AND 検索したい場合は「 ^(?=.*X-MON)(?=.*TEST).*\$ 」とします。この場合はログの行に対して AND 検索する形となりますので、先に X-MON を検知し、その行で TEST があれば最終的に検知する、という形となります。

図 正規表現

フィルター

プロパティベースフィルター ▼

対象	条件否定	比較内容	詳細内容/正規表現
メッセージ ▼	なし ▼	正規表現 ▼	^(?=.*X-MON)(?=.*TEST).*\$

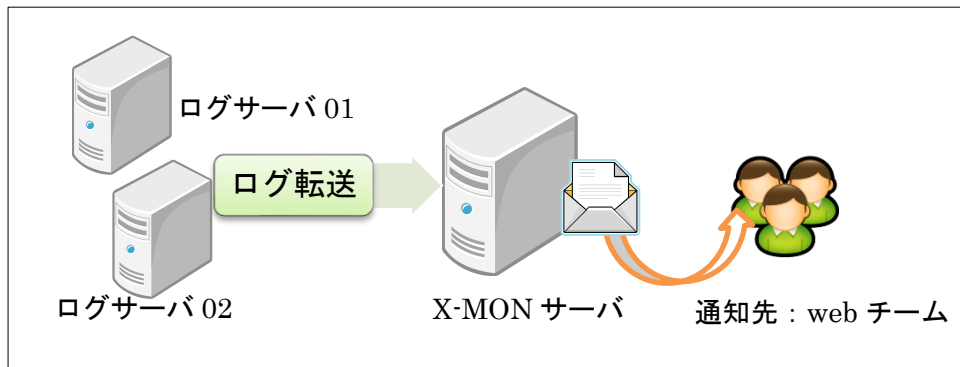
運用としては、ログを複数設定する場合や正規表現させる場合は一度監視環境にて検証を行い、正常に検知されるかを確認してから通常運用に入るようにお願いします。

2.4 監視設定例（式ベースフィルター）

式ベースフィルター形式を例に交えながら解説を行います。

下記のサンプルネットワークをご確認頂きながらご参照ください。

図 サンプルネットワーク



2.4.1 基本的な設定例

2.4.1.1 新規作成

[MENU]の[syslog 管理]内の[新規作成]を開き、条件を入力します。

図 MENU

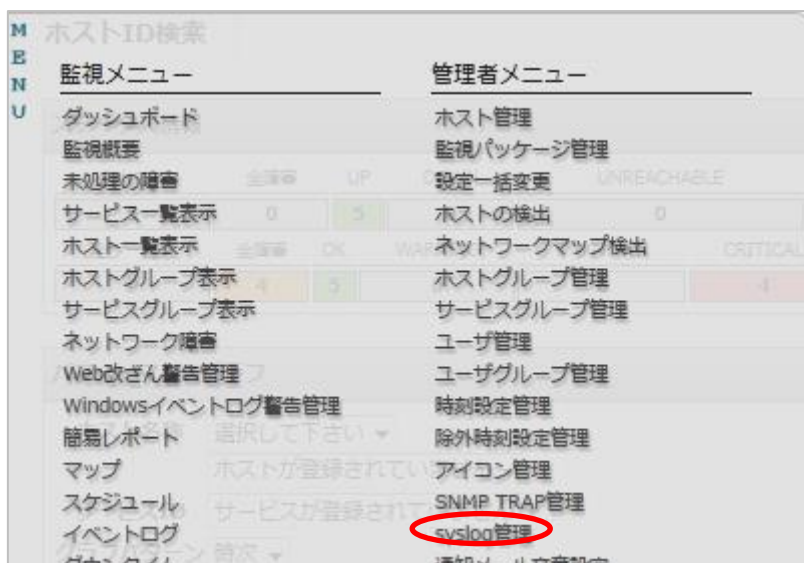


図 新規作成



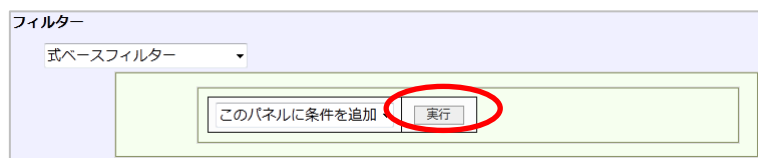
下記の条件で設定してみます。

登録ログ条件名	LOG_X-MON-TEST02
検索項目	メッセージ
検索内容	X-MON-TEST
条件指示	一致する
対象ホスト	ログサーバ 02
通知先グループ	web チーム
通知先サービス名	LOG_X-MON-TEST02
通知ステータス	CRITICAL

式ベースフィルターでは、パネルを使っていきます。

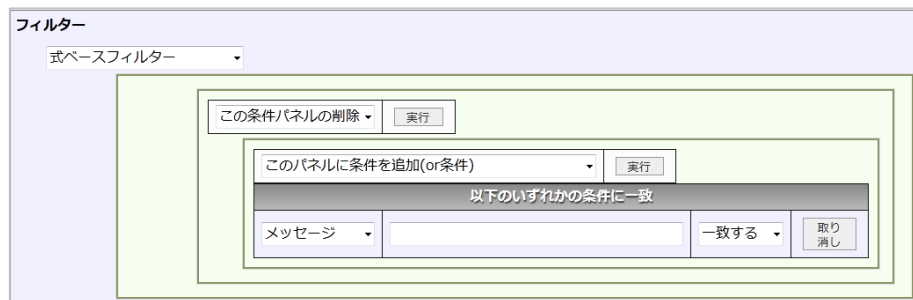
まずは、パネルに条件を追加します。「このパネルに条件を追加」を実行します。

図 追加



条件が追加されました。

図 追加後



パネル 1 つが 1 つの条件となります。例にそって入力します。

図 条件入力

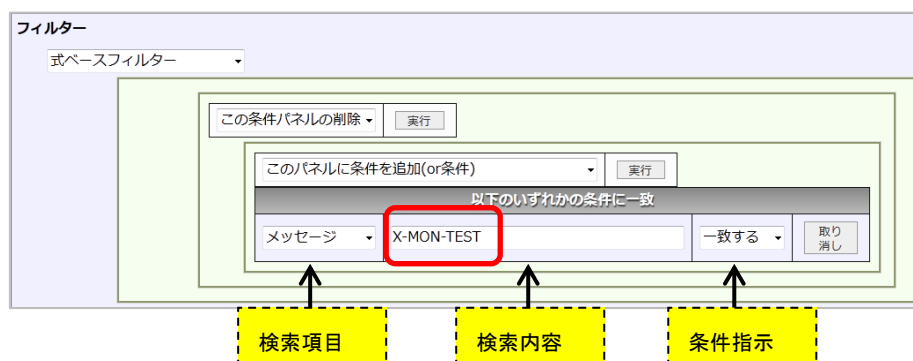


図 全体の入力例

登録ログ条件名
LOG_X-MON-TEST02

フィルター
データベースフィルター

この条件パネルの削除 ▼ 実行

このパネルに条件を追加(or条件) 実行

以下のいずれかの条件に一致

メッセージ X-MON-TEST 一致する 取り消し

対象ホスト
ログサーバー/02

↑(選択) ↓(外す)

--- □ ---

ログサーバー/01

通知先グループ
Webチーム

↑(選択) ↓(外す)

--- W ---

☐ チェックで上書き登録/チェックなしで通知先を更新しない

通知先サードパーティ
LOG_X-MON-TEST0

通知ステータス
☐ OK ☐ WARNING ☒ CRITICAL ☐ UNKNOWN

キャンセル 作成と承認

入力が完了したら一番下の「作成と承認」で反映後、X-MON を再起動します。

2.4.1.2 確認

設定出来たか確認してみましょう。

syslog 管理を開くと作成した LOG_X-MON-TEST02 があります。

図 syslog 管理

LOG_X-MON-TEST02	詳細表示
------------------	------

詳細表示を開くと設定が確認出来ます。

図 詳細表示

サービス一覧表示を見てみましょう。

図 サービス一覧

logsv02 (ログサーバ02)	LOG_X-MON-TEST02	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
--------------------------------------	----------------------------------	-----------------	-----	-----	-----	---------------------------------

監視が追加されています。

syslog 管理ではフィルターして検知するのを rsyslog が行い、結果を X-MON へ通知します。そのため監視はパッシブチェックとなります。そのため画像のように「このサービスはチェックするようにはスケジュールされていません。」となります。

2.4.1.3 検知テスト

それでは検知するかテストしてみましょう。

監視ホスト側で下記コマンドを発行します。

```
# logger -i -t TEST -p user.warning "X-MON-TEST"
```

発行後サービス一覧表示画面を開きます。下記画像のように CRITICAL を検知しました。

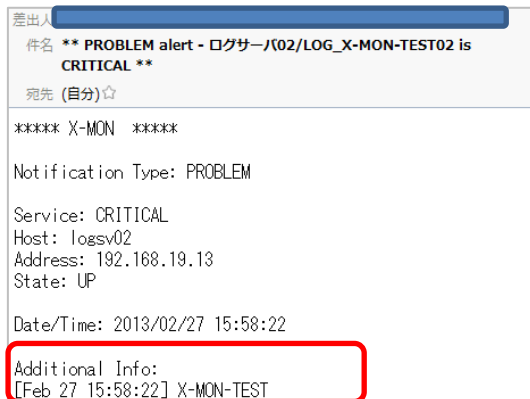
図 ログを検知

logsv02 (ログサーバ02)	LOG_X-MON-TEST02	異常 (CRITICAL)	N/A	N/A	1/1	[Dec 30 02:28:48] X-MON-TEST
--------------------------------------	----------------------------------	------------------	-----	-----	-----	------------------------------

例では通知先グループを設定していますので下記のようなメールが来ます。

デフォルトの通知内容の場合、メール本文の「Additional Info:」の部分にログの内容が記載されます。

図 通知メール



正常に検知出来ている事がわかりました。

2.4.1.4 監視を復旧させる

手動で監視を復旧させるにはパッシブの結果を送るという動作になります。

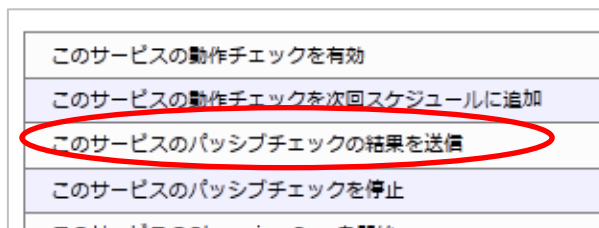
サービス一覧表示の監視名を開き、サービス情報画面の「サービス詳細」タブを開きます。サービス詳細タブのメニューの中から「このサービスのパッシブチェックの結果を送信」を開きます。

図 サービス詳細タブ



サービス詳細タブのメニューの中から「このサービスのパッシブチェックの結果を送信」を開きます。

図 パッシブの結果を送信



下記のような画面となります。

図 パッシブチェック

外部コマンド

赤字の項目は必ず入力してください。入力していない場合エラーとなります。

リクエストしたコマンド: 指定したサービスのパッシブチェックの結果を登録する

このコマンドは指定したサービスからのPassiveチェックの結果を送信します。これは作業が行われたり、作業を完了したり、セキュリティチェックなどに有効活用できます。

ホスト ID: logsv02

サービス ID: LOG_X-MON-TEST02

チェック結果: OK

チェック出力:

パスワード:

発行 リセット

チェック結果を OK にします。(デフォルトで選択されています) チェック出力は必須入力となります。

例えば「ログ検知のテストのため OK」や実際の運用では「ログ確認、対応完了」などを記載するといでしょう。

図 項目入力

チェック結果: OK

チェック出力: ログ検知のテストのためOK

入力出来たら発行を押します。

図 発行

発行 リセット

コマンドを正常に受け付けた画面となります

図 発行後

外部コマンド

コマンドを正常に受け付けました。
コマンドが実行されるまではしばらく時間がかかります。

了解

復旧しているか確認しましょう。

サービス一覧表示にてステータス情報がパッシブの結果を送信の際に入力した「ログ

検知のテストのため OK」というステータスとなり正常（OK）で復旧しています。

図 復旧後

logsv02 (ログサーバー02)	LOG_X- MON-TEST02	正常(O.K.)	2012-12-30 02:35:58	0日と00時間 00分03秒	1/1	ログ検知のテストのためOK
-----------------------	----------------------	----------	---------------------	-------------------	-----	---------------

また、通知先にも下記のような復旧のメールが届きます。

図 復旧通知メール

差出: [] ☆

件名 ** RECOVERY alert - ログサーバー02/LOG_X-MON-TEST02 is OK **

宛先 (自分) ☆

***** X-MON *****

Notification Type: RECOVERY

Service: OK
Host: logsv02
Address: 192.168.19.13
State: UP

Date/Time: 2012/12/30 02:35:58

Additional Info:
ログ検知のテストのためOK

以上が基本的な設定例とテストとなります。

2.4.2 設定項目について

式ベースフィルターでの検索項目は以下の4つとなります。

ファシリティ	プライオリティ	メッセージ	タグ
--------	---------	-------	----

図 検索項目

この条件パネルの削除 ▾ 実行

このパネルに条件を追加(or条件) ▾ 実行

以下のいずれかの条件に一致

メッセージ ▾		一致する ▾	取り消し
ファシリティ			
プライオリティ			
メッセージ			
タグ			

それぞれの検索項目について次項より解説します。

2.4.3 ファシリティ

検索項目でファシリティを選択すると条件欄が下記のようになります。

図 ファシリティ

検索内容が選択 BOX となります。検索内容は以下となります。

kern
user
mail
daemon
auth
syslog
lpr
news
uucp
cron
authpriv
ftp
ntp
audit
clock
alert
local0～7

上から順にレベルが高い順となっております。

条件指示は以下 4 つとなります。

一致する	以外	より大きい	より小さい
------	----	-------	-------

- ・ 一致する

選択したファシリティと一致する場合に検知します。

- ・ 以外

選択したファシリティと一致しない場合に検知します。

- ・ より大きい/より小さい

選択したファシリティより大きいレベルか小さいレベルの場合検知します。

(選択したものは含みません)

2.4.3.1 設定例

ファシリティを daemon より大きい、と設定する場合は下記のようになります。

図 設定例

The screenshot shows a configuration panel with a dropdown menu for 'Facility' (ファシリティ) set to 'daemon' and a comparison operator set to 'greater than' (より大きい). The panel also includes buttons for '実行' (Execute), 'この条件パネルの削除' (Delete this condition panel), and '取り消し' (Cancel).

この場合は daemon は含みませんので、上位の kern,user,mail のファシリティが検知対象となります。

2.4.4 プライオリティ

検索項目でファシリティを選択すると条件欄が下記のようになります。

図 プライオリティ

The screenshot shows a configuration panel with a dropdown menu for 'Priority' (プライオリティ) set to 'ERR' and a comparison operator set to 'match' (一致する). The panel also includes buttons for '実行' (Execute), 'このパネルに条件を追加(or条件)' (Add condition to this panel (or condition)), and '取り消し' (Cancel).

検索内容が選択 BOX となります。検索内容は以下となります。

emerg
alert
crit
err
warn
notice
info
debug

上から順にレベルが高い順となっております。

条件指示は以下 4 つとなります。

一致する	以外	より大きい	より小さい
------	----	-------	-------

- ・ 一致する

選択したプライオリティと一致する場合に検知します。

- ・ 以外

選択したプライオリティと一致しない場合に検知します。

- ・ より大きい/より小さい

選択したプライオリティより大きいレベルか小さいレベルかの場合検知します。

(選択したものは含みません)

2.4.4.1 設定例

プライオリティが CRIT に一致する、と設定する場合は下記のようになります。

図 設定例

2.4.5 メッセージ

検索項目でメッセージを選択すると条件欄が下記のようになります。

図 メッセージ

検索内容は記入欄となります。

条件指示は以下 4 つとなります。

一致する	一致しない	含める	含まない
------	-------	-----	------

- ・ 一致する

入力した文字列（単語ではなく、文字列）が一致するかどうかになります。

例えば、メッセージで"X-MON-TEST"とした場合、メッセージで"X-MON-TEST"と一致した場合のみ検知します。そのため、"X-MON-TEST WARNING"というメッセージの場合は検知しません。行そのものが一致するかどうか、と認識頂ければと思います。サービスによる複雑なメッセージであっても一致するかどうかを判別する事が出来ます。

- ・ 一致しない

入力した文字列（単語ではなく、文字列）が一致しない場合検知します。

- ・ 含める

入力した文字列が含まれるかとなります。

例えば、メッセージで

"X-MON-TEST"とした場合、メッセージが"X-MON-TEST"でも "X-MON-TEST WARNING"の場合でも検知します。

- ・ 含まない

入力した文字列が含まれない場合に検知する、となります。

2.4.5.1 設定例

メッセージで「X-MON-TEST」を含める場合検知するようにするには下記のように設定します。

図 設定例

The screenshot shows a configuration panel with a dropdown menu set to 'Message' (メッセージ) and a text input field containing 'X-MON-TEST'. The operator dropdown is set to 'Contains' (含める). A red box highlights the 'Message' dropdown, the text input, and the 'Contains' operator dropdown.

2.4.6 タグ

検索項目でタグを選択すると条件欄が下記のようにになります。

図 タグ

The screenshot shows a configuration panel with a dropdown menu set to 'Tag' (タグ) and an empty text input field. The operator dropdown is set to 'Match' (一致する). A red box highlights the 'Tag' dropdown, the text input, and the 'Match' operator dropdown.

検索内容は記入欄となります。

条件指示は以下 4 つとなります。

一致する	一致しない	含める	含まない
------	-------	-----	------

- ・ 一致する

入力した文字列（単語ではなく、文字列）が一致するかどうかになります。

例えば、タグで"sshd"とした場合タグで"sshd"と一致した場合のみ検知します。そのため、"ssh"というタグの場合は検知しません。

- ・ 一致しない

入力した文字列（単語ではなく、文字列）が一致しない場合検知します。

- ・ 含める

入力した文字列が含まれるかとなります。

例えば、タグで"ssh"とした場合、タグが"ssh"でも"sshd"の場合でも検知します。

- ・ 含まない

入力した文字列が含まれない場合に検知する、となります。

2.4.6.1 設定例

タグで「ssh」を含める場合検知するには下記のように設定します。

図 設定例

The screenshot shows a configuration window with a green header bar. Below the header, there is a section titled 'このパネルに条件を追加(or条件)' with a dropdown arrow and an '実行' button. Below this, a red box highlights a condition panel. The panel has a dropdown menu set to 'タグ', a text input field containing 'ssh', a dropdown menu set to '一致する', and a '取り消し' button. Above the panel, the text '以下のいずれかの条件に一致' is visible.

2.4.7 パネルを追加して複数の条件で検索する

条件を追加する（パネルを追加する）と and 条件と or 条件を設定出来ます

2.4.7.1 and 検索

例えば、メッセージで X-MON-TEST、ファシリティで user の場合は検知する場合を設定してみます。

まずは新規作成から、条件パネルを追加しメッセージの条件を入力します。

図 メッセージ

The screenshot shows a configuration window with a green header bar. Below the header, there is a section titled 'この条件パネルの削除' with a dropdown arrow and an '実行' button. Below this, there is a nested section titled 'このパネルに条件を追加(or条件)' with a dropdown arrow and an '実行' button. Below this nested section, a red box highlights a condition panel. The panel has a dropdown menu set to 'メッセージ', a text input field containing 'X-MON-TEST', a dropdown menu set to '一致する', and a '取り消し' button. Above the panel, the text '以下のいずれかの条件に一致' is visible.

そしてパネルの操作盤から「新しい条件パネルを横に追加(and 条件)」を選択し実行します。

図 操作盤

The screenshot shows a configuration window with a green header bar. Below the header, there is a section titled 'この条件パネルの削除' with a dropdown arrow and an '実行' button. Below this, there is a red oval highlighting a button labeled '新しい条件パネルを横に追加(and条件)'. To the right of the button is an '実行' button.

and 条件用の条件パネルが追加されました。

図 and 条件用のパネル

この条件パネルの削除 ▼ 実行

このパネルに条件を追加(or条件) ▼ 実行

以下のいずれかの条件に一致

メッセージ ▼ X-MON-TEST 一致する ▼ 取り消し

and

このパネルに条件を追加(or条件) ▼ 実行

まだ条件が追加されていないので、条件を追加するために「このパネルに条件を追加(or 条件)」を実行します。

図 条件の追加

このパネルに条件を追加(or条件) ▼ 実行

条件を入力する入力パネルが出ました

図 入力パネルの追加

この条件パネルの削除 ▼ 実行

このパネルに条件を追加(or条件) ▼ 実行

以下のいずれかの条件に一致

メッセージ ▼ X-MON-TEST 一致する ▼ 取り消し

and

このパネルに条件を追加(or条件) ▼ 実行

以下のいずれかの条件に一致

メッセージ ▼ 一致する ▼ 取り消し

2 つの条件パネルがあり真ん中に and と表示されます。これでこの 2 つが and 条件となることを意味しています。

入力パネルに条件を入力します。

図 設定例

The screenshot shows a configuration window with a light green background. At the top, there is a button labeled 'この条件パネルの削除' (Delete this condition panel) and an '実行' (Execute) button. Below this, there are two condition panels. The first panel has a dropdown menu labeled 'このパネルに条件を追加(or条件)' (Add condition to this panel (or condition)) and an '実行' (Execute) button. Below the dropdown is a section titled '以下のいずれかの条件に一致' (Match any of the following conditions). It contains a dropdown menu with 'メッセージ' (Message) selected, a text input field with 'X-MON-TEST', a dropdown menu with '一致する' (Match) selected, and a '取り消し' (Cancel) button. The second panel is identical but has 'ファシリティ' (Facility) selected in the dropdown menu and 'user' in the text input field. The two panels are connected by the word 'and'.

入力が完了すれば登録ログ条件名や通知先を設定しましょう。

以上で and 検索での設定は完了です。

2.4.7.2 or 検索

例えば、メッセージで X-MON-ERROR もしくはファシリティで daemon の場合は検知する場合を設定してみます。

まずは新規作成から、条件パネルを追加しメッセージの条件を入力します。

図 メッセージ

The screenshot shows the same configuration window as before, but with only one condition panel. The dropdown menu 'このパネルに条件を追加(or条件)' (Add condition to this panel (or condition)) is highlighted with a red rectangle. Below it, the section '以下のいずれかの条件に一致' (Match any of the following conditions) contains a dropdown menu with 'メッセージ' (Message) selected, a text input field with 'X-MON-ERROR', a dropdown menu with '一致する' (Match) selected, and a '取り消し' (Cancel) button.

そしてパネルの操作盤から「このパネルに条件を追加 (or 条件)」を選択し実行します。

図 操作盤

The screenshot shows a close-up of the operation disk for the condition panel. It features a dropdown menu labeled 'このパネルに条件を追加(or条件)' (Add condition to this panel (or condition)) and an '実行' (Execute) button. The dropdown menu is highlighted with a red oval.

or 条件用の条件入力パネルが追加されました。

図 or 条件用の入力パネル

以下のいずれかの条件に一致			
メッセージ	X-MON-ERROR	一致する	取り消し
メッセージ		一致する	取り消し

2 つの条件入力パネルが並んでおり、これでこの 2 つが or 条件となることを意味しています。入力パネルに条件を入力します。

図 設定例

以下のいずれかの条件に一致			
メッセージ	X-MON-ERROR	一致する	取り消し
ファシリティ	daemon	一致する	取り消し

入力が完了すれば登録ログ条件名や通知先を設定しましょう。

以上で or 検索での設定は完了です。

2.4.7.3 複雑な条件での検索

パネルを追加する事で複雑な条件での検索も可能となります。

例として

「プライオリティが ALERT、もしくはタグが X-MON がある場合にファシリティが user と一致、その場合にメッセージに ERROR の場合は検知する。」

少しわかりにくいですが、|| と && を使って式で表してみます。

```
((プライオリティ=ALLERT || タグ=X-MON)&&ファシリティ=user)&&メッセージ=ERROR
```

複雑な条件の場合は上記の式の内部の小さいものから設定していくのをイメージすればわかりやすくなります。

それでは、上記の例を実現するように設定をしていきます。

まずは、

プライオリティが alert もしくはタグが x-mon の場合を作成します

新規作成から条件パネルを追加します。1 行目にプライオリティの分を入力し、「このパネルに条件を追加 (or 条件)」を実行し、タグを入力する入力パネルを追加し、入力します。

図 or 条件

これで式の囲っている部分が出来ました。

((プライオリティ=ALLERT || タグ=X-MON)&&ファイリティ=user)&&メッセージ=ERROR

次はこの条件に対する and 条件ファシリティが user のパネルを追加します。

「新しい条件パネルを横に追加 (and 条件)」で条件パネルを追加し、「このパネルに条件を追加 (or 条件)」で入力パネルを追加します。追加出来たら、設定例を入力します。

図 and 条件

これで式の囲っている部分が出来ました。

((プライオリティ=ALLERT || タグ=X-MON)&&ファイリティ>user)&&メッセージ=ERROR

残りは、この大きい条件に対して、メッセージが ERROR の場合という and 条件となります。このままさらに条件パネルを追加すると、小さい条件に対する and 条件となります。

図 間違った and 条件の追加

この条件パネルの削除 ▼ 実行

このパネルに条件を追加(or条件) ▼ 実行

以下のいずれかの条件に一致

プライオリティ ▼	ALERT ▼	一致する ▼	取り消し
タグ ▼	X-MON	一致する ▼	取り消し

and

このパネルに条件を追加(or条件) ▼ 実行

以下のいずれかの条件に一致

ファシリティ ▼	user ▼	一致する ▼	取り消し
----------	--------	--------	------

and

このパネルに条件を追加(or条件) ▼ 実行

そのため、式でいう、かっこで纏めるようにイメージしてください。
この小さい条件をグループとしてまとめます。

操作盤にて「この条件と同じ階層のパネルを group 化する」を実行します。

図 グループ化

この条件パネルの削除 ▼ 実行

このパネルに条件を追加(or条件) ▼ 実行

以下のいずれかの条件に一致

プライオリティ ▼	ALERT ▼	一致する ▼	取り消し
タグ ▼	X-MON	一致する ▼	取り消し

and

このパネルに条件を追加(or条件) ▼ 実行

以下のいずれかの条件に一致

ファシリティ ▼	user ▼	一致する ▼	取り消し
----------	--------	--------	------

この条件と同じ階層をパネルにまとめる(group化)

これで group 化となります。

図 グループ化実施後

この条件パネルの削除 ▾ 実行

新しい条件パネルを横に追加(and条件) ▾ 実行

このパネルに条件を追加(or条件) ▾ 実行

以下のいずれかの条件に一致

プライオリティ ▾	ALERT ▾	一致する ▾	取り消し
タグ ▾	X-MON	一致する ▾	取り消し

and

このパネルに条件を追加(or条件) ▾ 実行

以下のいずれかの条件に一致

ファシリティ ▾	user ▾	一致する ▾	取り消し
----------	--------	--------	------

それではこのグループに and 条件のパネルを追加します。
グループ化した部分と and 条件になる事がわかります。

この条件パネルの削除 ▾ 実行

新しい条件パネルを横に追加(and条件) ▾ 実行

このパネルに条件を追加(or条件) ▾ 実行

以下のいずれかの条件に一致

プライオリティ ▾	ALERT ▾	一致する ▾	取り消し
タグ ▾	X-MON	一致する ▾	取り消し

and

このパネルに条件を追加(or条件) ▾ 実行

以下のいずれかの条件に一致

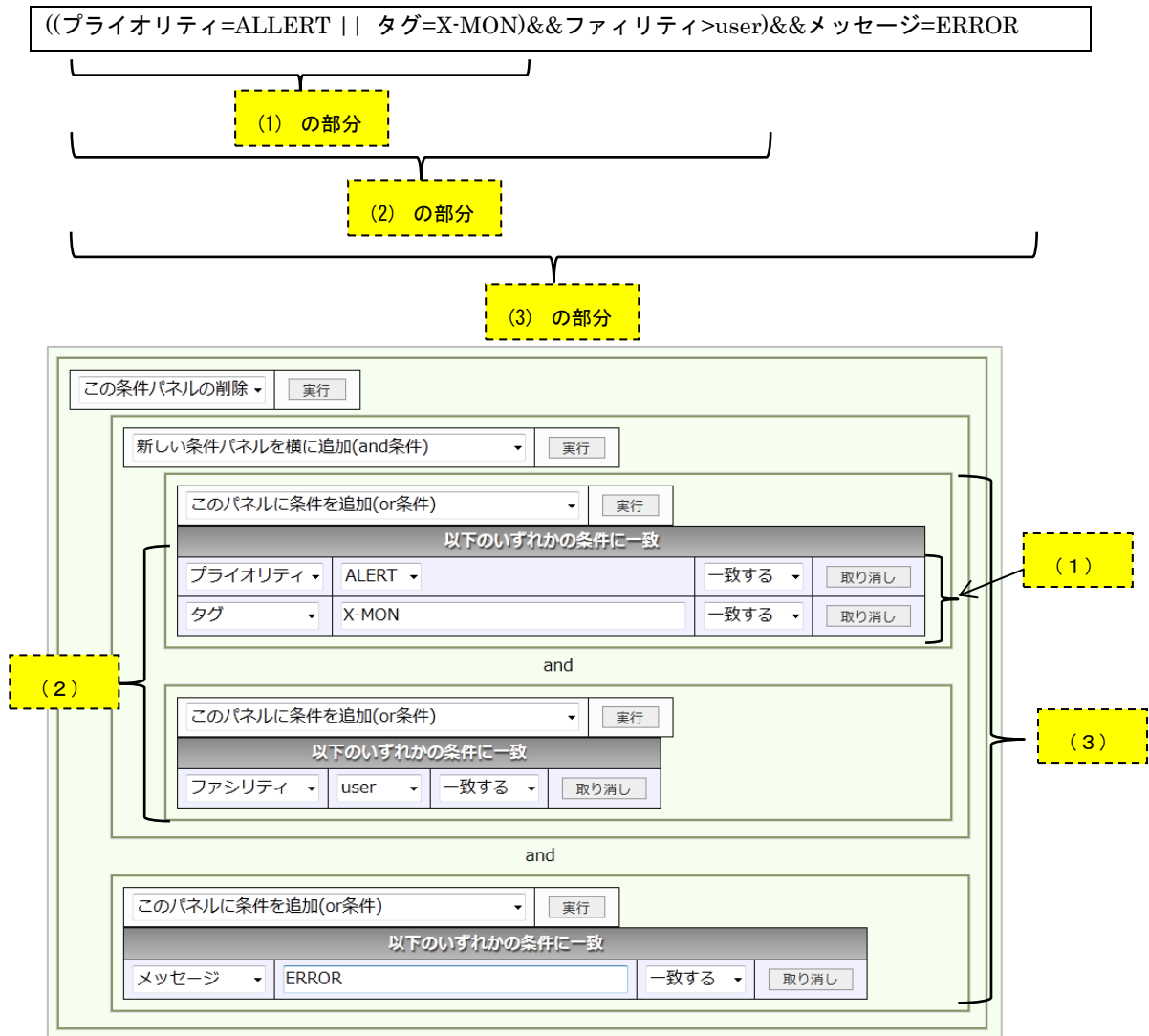
ファシリティ ▾	user ▾	一致する ▾	取り消し
----------	--------	--------	------

and

このパネルに条件を追加(or条件) ▾ 実行

これに and 条件用の入力パネルを追加し、入力しましょう。
これでグループと and 条件が完成し、設定例が完成しました。

図 設定例



このようにして、複雑な条件でも小さい部分から作成していく事によって実現する事が出来ます。

その他の作成方法として、大きい部分から作成する事も可能です。その場合は「この条件の下にパネルを追加」を実行します。

図 この条件の下にパネルを追加

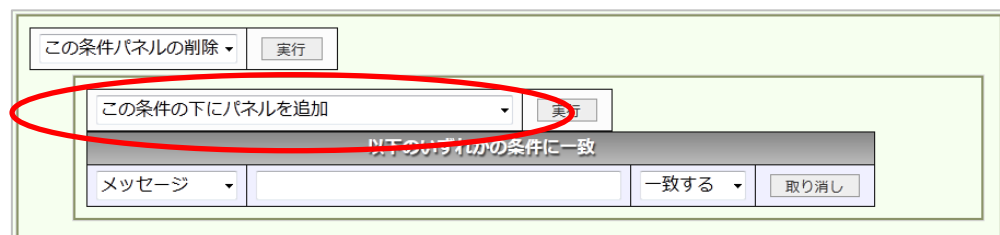


図 パネルを追加後

設定方法は大きくはかわりませんので、使いやすい方を使用してください。

2.4.8 注意点

式ベースフィルター形式を使用する上での注意点を纏めています。

2.4.8.1 パネルを間違えて追加した場合

間違ってパネルを追加してしまった場合、パネルを削除出来ます。

条件パネルの場合は選択 BOX から「この条件パネルの削除」を選んで実行します。

図 削除前

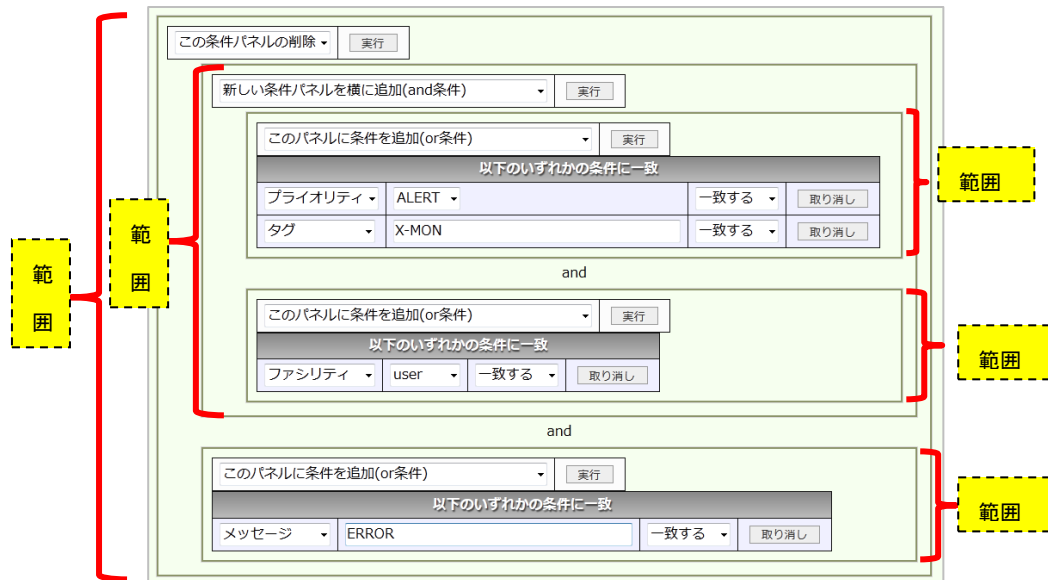
図 削除後

しかし、複雑な条件の場合に間違えて追加してしまった場合、そのパネルの境界がわかりにくいいため注意して実行してください。現在の X-MON のバージョンでは 1 つ前

の動作に戻る機能は搭載されておりません。

実行する操作盤を囲っている範囲が対象パネルとなります。下記画像では {} で囲っている範囲となります。

図 複雑な条件



運用としては、ログを複数設定する場合や正規表現させる場合は一度監視環境にて検証を行い、正常に検知されるかを確認してから通常運用に入るようにお願いします。

2.5 共通の設定動作

プロパティベースフィルター、式ベースフィルターで共通の設定動作を解説します。例や画像はプロパティベースフィルターが主になっていますが、式ベースフィルターでも共通です。(一部用語もプロパティベースフィルターに合わせていますが、ベースは同じです)

2.5.1 通知条件を編集する

一度設置した設定を編集する事が出来ます。

[MENU]の[syslog 管理]から対象の条件の「詳細表示」を開きます。

図 syslog 管理



設定の詳細が表示されますので、下のメニューの編集ボタンを開きます。

図 詳細



編集が可能となりますので、編集を実施します。

図 編集（プロパティベースフィルター）

登録ログ条件名
LOG_X-MON-TEST01

フィルター
プロパティベースフィルター

対象	条件否定	比較内容	詳細内容/正規表現
メッセージ	なし	完全一致	X-MON-TEST

対象ホスト
ログサーバー01

↑(選択) ↓(外す)
選択して下さい

通知先サービス名
LOG_X-MON-TEST01

通知ステータス
☐ OK ☐ WARNING ☒ CRITICAL ☐ UNKNOWN

キャンセル 作成と承認

ここだけの編集なら X-MON は再起動を必要としません。

図 編集（式ベースフィルター）

登録ログ条件名
LOG_X-MON-TEST02

フィルター
式ベースフィルター

この条件/ネルの削除 実行

この(ネル)に条件を追加(or条件) 実行

以下のいずれかの条件に一致

メッセージ	一致する
X-MON-TEST	一致する

取り消し

対象ホスト
ログサーバー02

↑(選択) ↓(外す)
選択して下さい

通知先サービス名
LOG_X-MON-TEST02

通知ステータス
☐ OK ☐ WARNING ☒ CRITICAL ☐ UNKNOWN

ここだけの編集なら X-MON は再起動を必要としません。

この際、フィルターの部分のみの編集ですと x-mon の再起動は必要ありませんので再起動を促す再起動ボタンは点滅しません。その他の項目を編集すると x-mon の再起動が必要となりますので、x-mon の再起動を実施してください。

2.5.1.1 編集できる項目について（サービス設定からの編集）

syslog 管理からは通知条件について編集を行います。再通知間隔やステータスによる通知の有無、また通知先グループについては[ホスト管理] の[サービス設定] から編集を行います。

図 サービス設定

登録サービス	エスカレーション設定数	操作	
<input type="checkbox"/> LOG_BATCH	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスカレーション設定
<input type="checkbox"/> LOG_ERR	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスカレーション設定
<input type="checkbox"/> LOG_X-MON-TEST01	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスカレーション設定

該当のサービスの[詳細表示] を開きます。一番下に[編集]がありますので開きます。

図 詳細表示

サービスの詳細

すべて開く

基本設定

ホストID(英数字)

logsv01

サービスID(英数字)

LOG_BATCH

サービス監視用コマンド

ダミープラグイン(ステータスを任意のものに更新)

通知先グループ

無し

イベントハンドラ

有効にする

イベントハンドラコマンド

無し

監視の詳細設定

通知の詳細設定

フラッシングの設定

高度な設定

戻る

編集

編集画面が開きますので、編集する項目を編集してください。

この際、「サービス監視用コマンド」の部分については syslog 管理部分にて動作をさせるための項目ですので編集しないようにお願いします。

編集が完了したら、[編集] もしくは[編集と承認]にて完了させ、X-MON を再起動させてください。

図 編集

サービスの編集

すべて閉く

基本設定

ホストID(英数字)
logsv01

サービスID(英数字)
LOG_BATCH

サービス監視用コマンド

DHCPサービス監視

ダミープラグイン(ステータスを任意のものに更新)

ステータス OK

メッセージ OK

通知先グループ

Webチーム

↑(選択) ↓(外す)

--- W ---

イベントハンドラ

有効にする

イベントハンドラコマンド

実行しない

監視の詳細設定

通知の詳細設定

フラッシングの設定

高度な設定

キャンセル 確認 確認と実行

2.5.2 通知条件を削除する

条件の削除は編集と同じく詳細表示から実施出来ます。

[MENU] の [syslog 管理] から対象の条件の「詳細表示」を開きます。

図 syslog 管理

syslog 通知条件一覧

新規作成

条件名	操作
LOG_X-MON-TEST01	→ 詳細表示

設定の詳細が表示されますので、下のメニューの削除ボタンを開きます。

図 詳細

登録ログ条件名
LOG_X-MON-TEST01

フィルター
プロパティベースフィルター

対象	条件否定	比較内容	詳細内容/正規表現
メッセージ	なし	完全一致	X-MON-TEST

対象ホスト
logsv01

通知先グループ

通知先サービス名
LOG_X-MON-TEST01

通知ステータス
CRITICAL

戻る 編集 削除

確認ウィンドウが出ますので、OK でしたら OK ボタンを押してください。

図 削除確認

ログ通知条件名「LOG_X-MON-TEST01」を削除しますがよろしいですか？

OK キャンセル

OK を押すと「設定を削除し反映しました。」と表示されます。

X-MON の再起動が必要となりますので、X-MON を再起動させて完了です。

図 削除実行

syslog 通知条件一覧

設定を削除し反映しました。

2.5.2.1 サービス設定から削除する

syslog 管理以外にも、[ホスト管理] の [サービス設定] から通知条件は削除出来ます。

どちらで削除を行っても動作への影響はありません。

該当のホストでサービス設定を開いて一覧を表示させます。

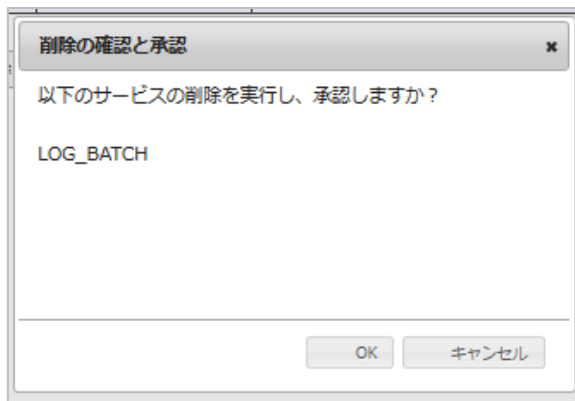
削除するサービスのチェックボックスにチェックを入れて [削除と承認] を押します。

図 サービス設定



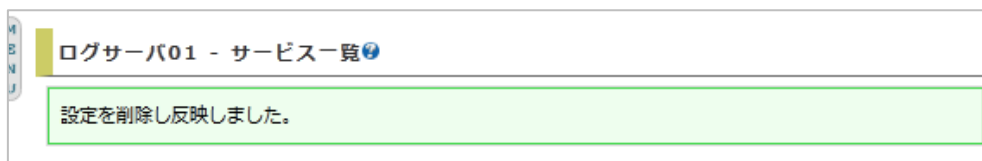
確認ウィンドウが出ますので、OK でしたら OK を押してください。

図 削除の確認



「設定を削除し反映しました。」と表示されますので X-MON を再起動させて完了してください。

図 削除



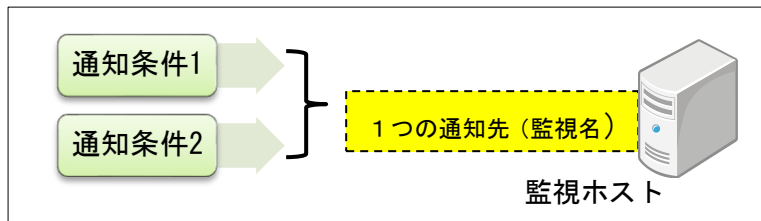
以上が通知条件の削除方法となります。

2.5.3 複数の条件を一つの通知先に設定する

複数の条件を 1 つの通知先（監視名）に設定する事が可能です。

例えば、LOG_ERR という監視名でメッセージが ERROR を検知した時とプライオリティで err を検知した際に通知する事が出来ます。

図 例



設定としては、通知条件を二つ作成します。

この例ですと、メッセージが ERROR を検知した時と、プライオリティで err を検知する条件です。登録ログ条件名を LOG_E01 と LOG_E02 とし、それぞれの「通知先サービス名」を LOG_ERR として作成します。

図 設定例



ログサーバ 01 に「LOG_ERR」は一つだけですが、検知する条件は LOG_E01 と LOG_E02 両方とも有効、という形になります。

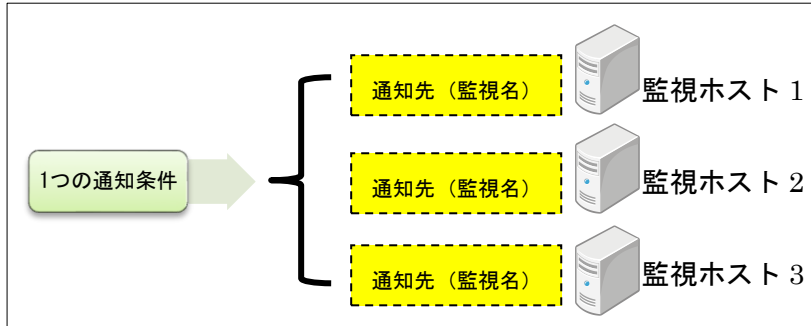
複数の監視を追加することなく、スマートな監視が可能となります

2.5.4 複数のホストで一つの通知先を設定する

複数のホストで1つの通知先を使用する形となります。

例えば、監視ホストが3つあり、それぞれメッセージで ERROR が出れば通知するような条件を設定したい場合に使用出来ます。

図 例



設定としては、対象ホストでホストを3つ選択するだけです。

例として、LOG_ERROR という通知条件を、sv01,sv02,sv03 の3つのホストに通知するように設定します。

図 作成時のホストの選択

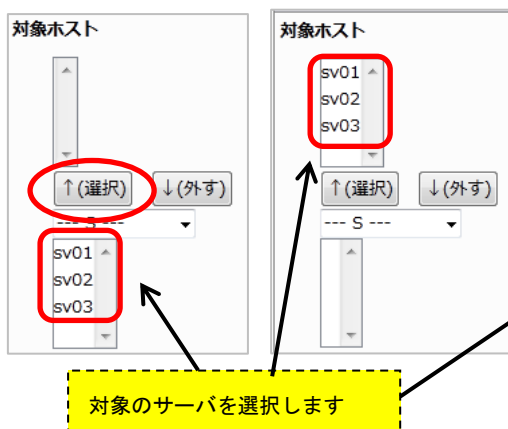


図 設定例

登録ログ条件名			
LOG_ERROR			
フィルター			
プロパティベースフィルター			
対象	条件否定	比較内容	詳細内容/正規表現
メッセージ	なし	完全一致	ERROR
対象ホスト			
sv01,sv02,sv03			
通知先グループ			
通知先サービス名			
LOG_ERROR			
通知ステータス			
CRITICAL			

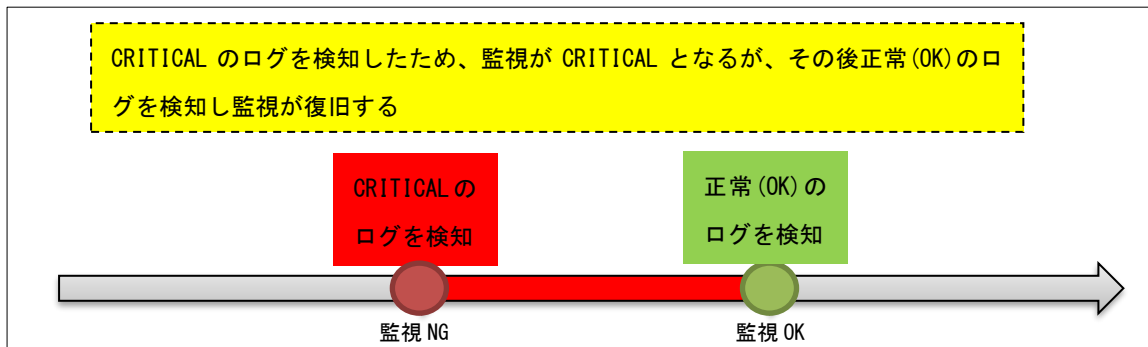
sv01 (sv01)	LOG_ERROR [P]	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
sv02 (sv02)	LOG_ERROR [P]	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
sv03 (sv03)	LOG_ERROR [P]	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。

それぞれのホストで同じ監視名で登録されます。

検索はそれぞれのホストで行われますが、通知条件を編集すると全てのホストへ影響が出ますので注意してください。

2.5.5 自動復旧の条件

条件を組み合わせる事により、監視の自動復旧も可能です、



例えば、メッセージで BATCH_ERROR が出た場合は CRITICAL、メッセージに BATCH_SUCCESS が出た場合は正常 (OK) にする条件を作成し、通知先サービス名を同じ名前 (同じ監視名) にします。ここでは通知条件名を LOG_BATCH01、LOG_BATCH02 とし、通知先サービス名を LOG_BATCH としています。

図 設定例



これで自動復旧の設定は完了です。

実際にテストをする場合は下記コマンド例で確認出来ます。

■ CRITICAL を検知

```
# logger -i -t TEST -p user.warning "BATCH_ERROR"
■OKを検知
# logger -i -t TEST -p user.warning "BATCH_SUCCESS"
```

図 自動復旧確認

logsv01 (ログサーバ01)	LOG_BATCH P	異常 (CRITICAL)	N/A	N/A	1/1	[Dec 30 02:00:03] BATCH_ERROR
↓						
logsv01 (ログサーバ01)	LOG_BATCH P	正常(OK)	N/A	N/A	1/1	[Dec 30 02:00:27] BATCH_SUCCESS

2.6 サービス設定からの設定について（共通）

syslog 管理で設定できる項目でも解説していますが、通知条件を作成し、ホストのサービス設定から設定する項目で重要な点について記載します。

2.6.1 通知先を編集する

メールの通知先については通知条件を新規作成する際に設定出来ますが、通知先を追加、削除する等編集したい場合はサービス設定から実施する必要があります。

図 編集

基本設定

ホストID(英数字)

logsv01

サービスID(英数字)

LOG_ERR

サービス監視用コマンド

DHCPサービス監視

ダミープラグイン(ステータスを任意のものに更新)

ステータス OK

メッセージ OK

通知先グループ

Webチーム

↑(選択) ↓(外す)

--- W ---

2.6.1.1 複数ホストを対象にしている場合

syslog の対象ホストを複数設定している場合、サービス設定で通知先を編集すると編集した該当のホストの通知先のみ編集されます。

例) LOG_SYSLOG_TEST をログサーバ 01,ログサーバ 02 を対象ホストとして設定。
通知先を web チームとする。

図 作成

登録ログ条件名
LOG_SYSLOG_TEST

フィルター
プロパティベースフィルター

対象	条件否定	比較内容	詳細内容/正規表現
メッセージ	なし	部分一致	test

対象ホスト

↑(選択) ↓(外す)

--- □ ---

ログサーバ01
ログサーバ02

通知先グループ

Webチーム

↑(選択) ↓(外す)

--- W ---

☐ チェックで上書き登録/チェックなしで通知先を更新しない



通知先サービス名
LOG_SYSLOG_TEST

通知ステータス
☐ OK ☐ WARNING ☒ CRITICAL ☐ UNKNOWN

キャンセル 作成と承認


この通知条件で設定するログサーバ 01,ログサーバ 02 に通知条件（監視設定）が作成されます。

図 通知条件設定

logsv01 (ログサーバ01)	LOG_SYSLOG_TEST 	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
logsv02 (ログサーバ02)	LOG_SYSLOG_TEST 	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。

ログサーバ01のサービス設定で通知先グループをDBチームに変更します。

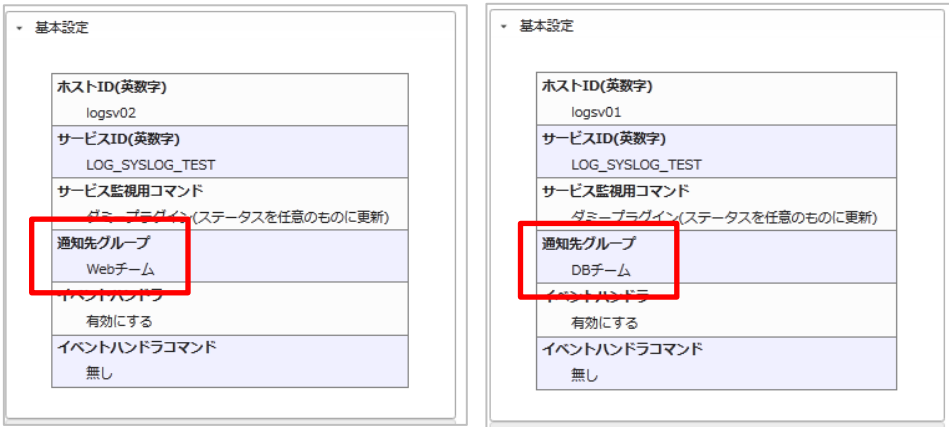
図 通知先グループの変更



こうする事で、ログサーバ01のLOG_SYSLOG_TESTの通知先グループはDBチームとなりますがログサーバ02のLOG_SYSLOG_TESTは通知先はwebチームのまま変更はされません。

これにより、同じsyslog通知条件でもホストによって通知先を変更する事が可能です。

図 同じsyslog設定で通知先グループが違う例



ただし、全ての通知先グループの変更が必要な場合は、設定されているサービス全てを変更する必要があります。

2.6.1.2 対象ホストを変更した際の挙動について

LOG_SYSLOG_TEST02 をログサーバ 01 に対象ホストとして設定。

通知先グループを web チームとする。

図 新規作成

登録ログ条件名
LOG_SYSLOG_TEST02

フィルター
プロパティベースフィルター

対象	条件否定	比較内容	詳細内容/正規表現
メッセージ	なし	部分一致	test

対象ホスト
ログサーバ(01)

通知先グループ
Webチーム

☐ チェックで上書き登録/チェックなしで通知先を更新しない

通知先サービス名
LOG_SYSLOG_TEST02

通知ステータス
☐ OK
 ☐ WARNING
 ☒ CRITICAL
 ☐ UNKNOWN

この通知条件で設定するログサーバ 01 に通知条件（監視設定）が作成されます。

図 作成後

logsv01 (ログサーバ01)	LOG_SYSLOG_TEST02	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
----------------------	-------------------	-----------------	-----	-----	-----	---------------------------------

syslog 管理より、通知条件を編集します。編集する内容は対象ホストにログサーバ 02 を追加します。これにより、ログサーバ 01、ログサーバ 02 に通知条件（監視設定）が設定されます。

図 編集

登録ログ条件名
LOG_SYSLOG_TEST02

フィルター
プロパティベースフィルター

対象	条件否定	比較内容	詳細内容/正規表現
メッセージ	なし	部分一致	test

対象ホスト

ログサーバ01
ログサーバ02

↑(選択) ↓(外す)

--- □ ---

通知先サービス名
LOG_SYSLOG_TEST02

通知ステータス
☐ OK
 ☐ WARNING
 ☒ CRITICAL
 ☐ UNKNOWN

図 作成後

logsv02 (ログサーバ02)	LOG_SYSLOG_TEST02	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
logsv01 (ログサーバ01)	LOG_SYSLOG_TEST02	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。

しかし、追加されたホスト（ログサーバ02）は通知先が設定されません。

図 追加したホストは通知先グループが設定されない（右側）

基本設定

ホストID(英数字)
logsv01

サービスID(英数字)
LOG_SYSLOG_TEST02

サービス監視用コマンド
ダミープラグイン(ステータスを任意のものに更新)

通知先グループ
Webチーム

イベントハンドラ
有効にする

イベントハンドラコマンド
無し

基本設定

ホストID(英数字)
logsv02

サービスID(英数字)
LOG_SYSLOG_TEST02

サービス監視用コマンド
ダミープラグイン(ステータスを任意のものに更新)

通知先グループ
無し

イベントハンドラ
有効にする

イベントハンドラコマンド
無し

そのため、サービス設定より通知先を編集する必要がありますので、対象ホストを追加した際はご注意ください。

2.6.2 ログを検知するたびに通知を行う（volatile サービスの設定）

X-MON の仕様により、一度ステータスが変わると、次にステータスが変わるか再通知間隔の時間が過ぎるまで通知は実施されません。

そのため、同じ通知サービス名で複数の通知条件を設定している場合に同じステータスのまま違う内容のログを受け取っても、ステータスが変わらないために通知が実施されません。

例）同じ通知先サービス名・ステータスを設定しているが、対象 TRAP が違う

登録ログ条件名	登録ログ条件名																
LOG_V_TEST01	LOG_V_TEST02																
フィルター プロパティベースフィルター <table border="1"> <thead> <tr> <th>対象</th> <th>条件否定</th> <th>比較内容</th> <th>詳細内容/正規表現</th> </tr> </thead> <tbody> <tr> <td>メッセージ</td> <td>なし</td> <td>部分一致</td> <td>test</td> </tr> </tbody> </table>	対象	条件否定	比較内容	詳細内容/正規表現	メッセージ	なし	部分一致	test	フィルター プロパティベースフィルター <table border="1"> <thead> <tr> <th>対象</th> <th>条件否定</th> <th>比較内容</th> <th>詳細内容/正規表現</th> </tr> </thead> <tbody> <tr> <td>メッセージ</td> <td>なし</td> <td>部分一致</td> <td>x-mon</td> </tr> </tbody> </table>	対象	条件否定	比較内容	詳細内容/正規表現	メッセージ	なし	部分一致	x-mon
対象	条件否定	比較内容	詳細内容/正規表現														
メッセージ	なし	部分一致	test														
対象	条件否定	比較内容	詳細内容/正規表現														
メッセージ	なし	部分一致	x-mon														
対象ホスト logsv01	対象ホスト logsv01																
通知先グループ	通知先グループ																
通知先サービス名 LOG_V_TEST01	通知先サービス名 LOG_V_TEST01																
通知ステータス CRITICAL	通知ステータス CRITICAL																

同じ通知先サービス名なので、作成される通知条件は 1 つです。

logsv01 (ログサービス01)	LOG_V_TEST01	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
-----------------------	--------------	-----------------	-----	-----	-----	---------------------------------

volatile サービスを設定する事により、同じステータスであっても別の内容のログを受信（厳密にはログ検知するたびに）すると通知を行います。デフォルトではこの機能は無効となっています。

サービス設定の[高度な設定] タブ内に「volatile サービス」がありますので有効にすれば設定は完了です。

図 volatile サービスの設定

高度な設定

オブセスオーバー機能
 無効にする

volatileサービス
 無効にする

フレッシュネスチェック
 無効にする

2.6.3 アクティブチェックと試行回数の設定について

syslog 通知条件では、パッシブチェックを利用し、syslog を受信したら通知を実施する設定となっています。

そのため、サービス設定のアクティブチェックは無効、試行回数は 1 の設定が通知条件を作成した際に設定されます。

設定項目	設定値	目的
アクティブチェック	無効にする	SYSLOG 監視は待ち受ける監視のため。
試行回数	1	条件に一致するログを 1 件受信したら即座にハードステータスとなり、メール等の通知が実施されます。

図 詳細

▼ 監視の詳細設定

アクティブチェック
無効にする ▼

パッシブチェック
有効にする ▼

監視時間帯
24時間365日 ▼

試行回数
1

監視間隔(分)
5

再試行間隔(分)
1

並びに、パッシブチェックも有効となっています。

syslog 管理を使用する際は上記内容は変更しないようにお願いします。

3 SNMP TRAP 監視

X-MON では、サーバやネットワーク機器からイベントが発生した際に状況を通知する SNMP TRAP に対応しています。

SNMP TRAP はサーバの管理ソフトやバックアップソフトで正常にジョブが終了した通知や、ネットワーク機器にてポートの状況が変化した場合などで使用されます。

SNMP TRAP は OID という数字列で構成され、その数字列が対応する MIB という各ベンダーが公開している管理項目と照らしあわせ、その TRAP が何を意味しているかを表示します。

X-MON では、各ベンダーの MIB をデフォルトで各種搭載しています。

また、各ベンダーが公開している MIB ファイルを X-MON に登録する事も可能です。

基本的な設定については 3.1～3.5、その他の使い方は 3.6 以降に掲載しております

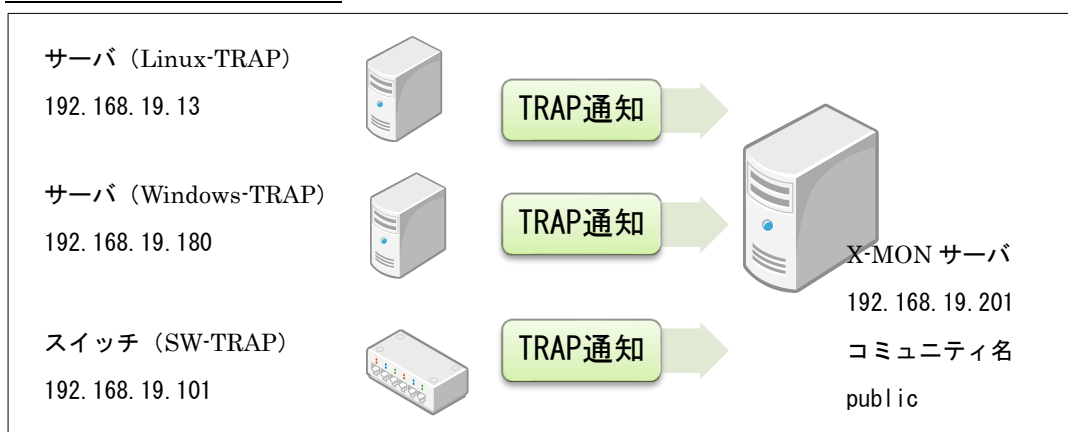
本章以降の SNMPTRAP 監視設定は X-MON ver3.0.6～3.5.0 までの設定方法となっております。X-MON3.6.0 以降をご利用のお客様は、別途「SNMPTRAP 監視設定マニュアル」をサポートサイトよりご利用ください。

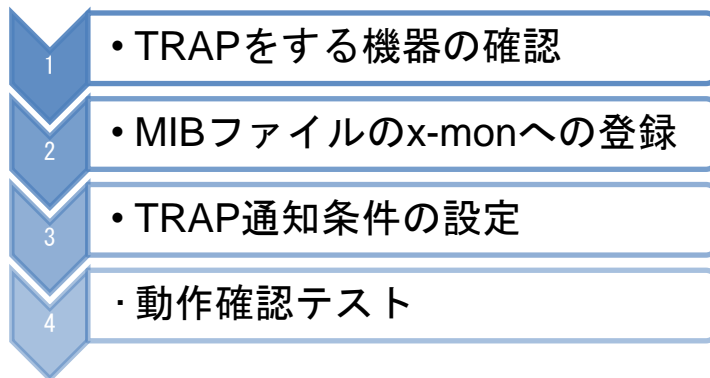
3.1 監視概要

SNMPTRAP の監視を設定するには以下のような手順を踏みます。

本リファレンスではサンプルネットワークを基に、手順について解説していきます。

図 サンプルネットワーク





3.1.1 監視について

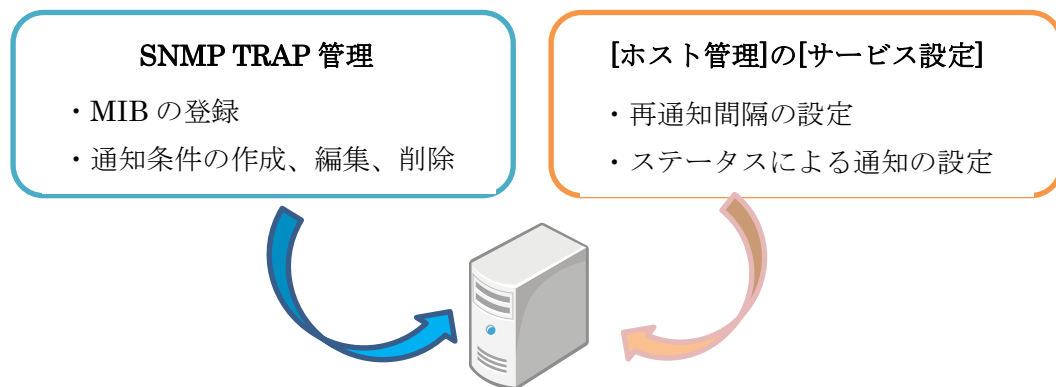
SNMP TRAP の監視は SNMP TRAP のデーモン (SNMPTT) で動作しています。

SNMPTT が TRAP を受信し X-MON へ通知する、という形です。

そのため、X-MON では SNMP TRAP の監視設定については「**通知条件の設定**」という名称で実施しております。そのため監視については**パッシブチェック**となります。

設定については、どのような SNMP TRAP を通知条件に設定するか、MIB を登録する、編集するについては SNMP TRAP 管理にて行います。

基本的には SNMP TRAP 管理のみで運用（新規作成、編集、削除）は可能ですがステータスによる通知の有無や再通知間隔など監視詳細（Nagios コアを使用する部分）については、SNMP TRAP 管理で新規作成後に[ホスト管理]の[サービス設定]から設定を行います。



3.1.2 MIB の依存関係について

MIB ファイルには依存関係が存在します。大きいカテゴリから小さいカテゴリがあり、小さいカテゴリの MIB ファイルを使用するには、大きいカテゴリの MIB ファイルが登録されていないといけません。ベンダーのサイトでも依存関係については表記があり、また X-MON では MIB 登録時に依存関係のチェックを実施します。

その際に、どの依存関係の MIB ファイルが必要かも表示されます。[\(3.3.2.3 依存関係の不足](#)を参照)

3.1.3 監視ホストの設定について

機器やソフトウェアの SNMP TRAP の設定は各マニュアルを確認してください。

Cisco スイッチではグローバルコンフィギュレーションモードにて

```
(config)# snmp-server enable traps  
(config)# snmp-server host [IP アドレス] version 2c [コミュニティ名]
```

で設定が可能です。X-MON ではデフォルトのコミュニティ名は public です。

ソフトウェアですと、TrendMicro 社の ServerProtect や Symantec 社の BackupExec など GUI の管理画面があるものは管理画面から設定出来るものもあります。また、Windows サーバも GUI より設定可能です。Windows に関しては

[3.6.4 設定例 \(Windows サーバからの任意 TRAP 通知\)](#) を参照ください。

次章より、サンプルネットワークに沿って設定方法を解説いたします。

3.2 TRAP する機器の確認

本リファレンスのサンプルでは Cisco スイッチで解説いたします。

スイッチは Cisco の catalyst2950 を例にします。

Cisco 機器の場合、以下の web サイトにてどのような trap があるか解説されています。

■ URL1

http://www.cisco.com/cisco/web/support/JP/100/1004/1004133_SNMPTTrapsInImages.html

各ベンダーにてスイッチの MIB は web サイトで公開されています。

Cisco 機器の場合は

■ URL2

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=ja>

の SNMP オブジェクトナビゲータというところから検索が可能です。

また、URL1 の SNMP TRAP の解説のページから URL2 へのオブジェクトナビゲータへのリンクもあります。

3.2.1 MIB ファイルの探し方

どのように MIB ファイルを探すか、例をします。

例えば、コンフィグファイルを新しく保存された際に TRAP の通知をしたい、とします。

URL1 のページで確認すると、config という項目があります。設定通知を送信する TRAP で、MIB ファイル名は「CISCO-CONFIG-MAN-MIB」でそれを示す OID は「1.3.6.1.4.1.9.9.43.2.0.1」、TRAP 名は「ciscoConfigManEvent」であることがわかり

ます。この MIB のリンクか、URL2 で「CISCO-CONFIG-MAN-MIB」を検索します。

■ URL3

<http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=ja&step=2&mibName=CISCO-CONFIG-MAN-MIB>

ここで必要な MIB の一覧が表示されます。

X-MON では SNMP バージョン 2 を推奨しますので、ダウンロードします

それ以外依存のあるものも必要となりますが、X-MON では基本的な MIB はすでに搭載しています。そのため、登録されていない物だけダウンロードしてください。

この例では、「CISCO-CONFIG-MAN-MIB」以外はすでに X-MON に登録されていますので、ダウンロードするのは「CISCO-CONFIG-MAN-MIB」のみとなります。

これで必要な MIB ファイルは準備出来ました。

3.2.1.1 その他の MIB ファイルの探し方

・ YAMAHA ルータの場合

<http://www.rtpro.yamaha.co.jp/RT/docs/mib/>

にて公開されています。全ての MIB が X-MON に初期登録済です

・ サーバソフトウェアの場合

サーバソフトウェアの場合でもスイッチと同じように各ベンダーの web サイトにて公開されております。

TrendMicro 社 ServerProtect では

<http://esupport.trendmicro.co.jp/Pages/JP-2080116.aspx>

<http://esupport.trendmicro.co.jp/Pages/JP-23681.aspx>

サポートページから検索できます。

<http://esupport.trendmicro.co.jp/corporate/sresult.aspx?q=MIB>

商品のディスクに付属している場合もあります。

Symantec 社の BackupExec では

<http://www.symantec.com/business/support/index?page=content&id=HOWTO73524>

このように商品の中にしかないものもありますので注意してください。

また、Windows サーバでは独自の MIB ファイルがありませんので手動で登録する形となります。(3.6.4 設定例 (Windows サーバからの任意 TRAP 通知) 参照)

必要な MIB ファイルが用意出来たら、X-MON へ MIB ファイルを登録しますので次章をご参照ください。

3.3 MIB ファイルの X-MON への登録

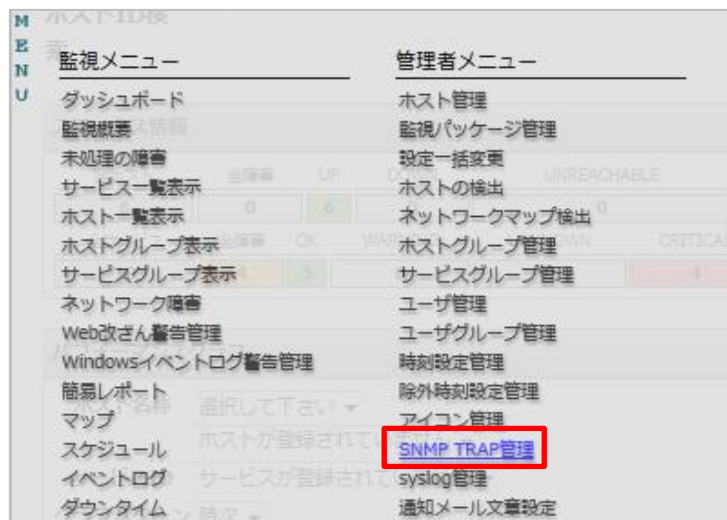
MIB ファイルが準備出来たら X-MON へ登録します。

サンプルでは Cisco catalyst2950 の CISCO-CONFIG-MAN-MIB を使用します。

3.3.1 MIB ファイルを登録する

X-MON の画面から SNMP TRAP 管理を選択します。

図 MENU



このような画面が表示されます。

図 SNMP TRAP 一覧

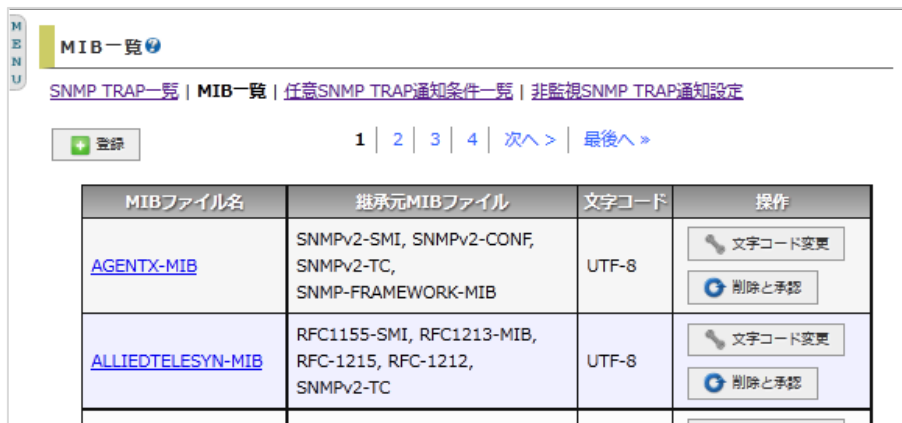
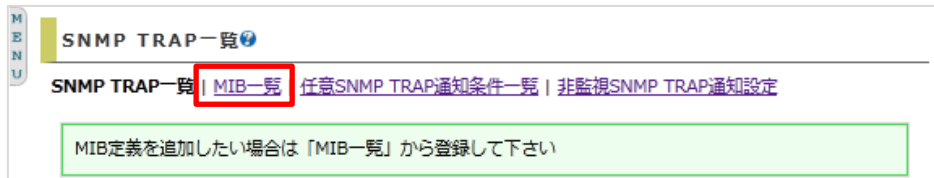
SNMP TRAP一覧			
SNMP TRAP一覧 MIB一覧 任意SNMP TRAP通知条件一覧 非監視SNMP TRAP通知設定			
MIB定義を追加したい場合は「MIB一覧」から登録して下さい			
1 2 次へ > 最後へ >>			
MIB定義	定義TRAP数	登録TRAP通知条件数	操作
ALLIEDTELESYN-MIB	28	0	→ 詳細表示
AT-C9000-MIB	23	0	→ 詳細表示
AT-FS900M-MIB	15	0	→ 詳細表示
AT-GS900M-MIB	27	0	→ 詳細表示
AT-IA800M-MIB	27	0	→ 詳細表示
AT-PAE-MIB	6	0	→ 詳細表示
AtiStackSwitch-MIB	22	0	→ 詳細表示

ここが SNMP TRAP の管理画面となります。管理画面の詳細は
[3.3.3 SNMP TRAP 管理画面メニューについて](#) に記載しております。

それでは MIB を X-MON に登録していきます。

MIB 一覧を選択して開いてください。

図 MIB 一覧



現在 X-MON に登録されている MIB ファイルの一覧が表示されます。表示はアルファベット順で 50 件ごとです。

左上に「登録」のボタンがありますので開きます。

図 登録



MIB ファイルの登録画面になります。



「参照」ボタンを押し、ファイルを選んでください。

文字コード欄は下記 3 つが選択出来ます。

・ UTF-8 ・ SJIS ・ EUC

ファイルの文字コードではなく、TRAP の文字コードとなります。

通常でしたら UTF-8 を選択してください。(デフォルト)

しかし、TRAP の送信元が Windows の場合は SJIS の場合がございます。

例：TrendMicro 社 ServerProtect Windows 版の場合

<http://esupport.trendmicro.co.jp/Pages/Jp-2078841.aspx?print=true>

送信元が sift-jis でエンコードされているとありますので、その場合は sjis を選択してください。

不明な場合は各ベンダーサポートへお問い合わせをお願いします。

(文字コードは登録後でも変更可能です)

選択が出来たら「登録と承認」を押します。

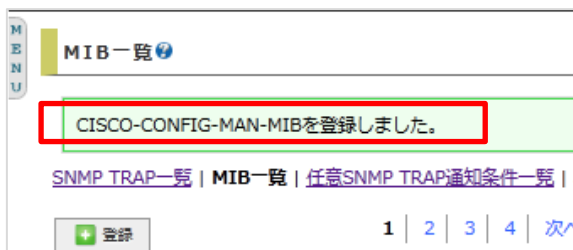
図 登録と承認



正常に登録できれば MIB 一覧の画面に戻ります。

「CISCO-CONFIG-MAN-MIB を登録しました。」と表示が出ます。

図 登録完了



MIB 一覧でも確認出来ます。

図 MIB 一覧

CISCO-CONFIG-MAN-MIB	SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, SNMP-FRAMEWORK-MIB, CISCO-TC, CISCO-SMI	UTF-8	文字コード変更 削除と承認
----------------------	---	-------	--

左から、MIB ファイル名、継承元 MIB ファイル、文字コード、操作となっています。

SNMP TRAP 一覧を見てみましょう。SNMP TRAP 一覧画面を開いてください。

ここにも「CISCO-CONFIG-MAN-MIB」が追加されています。

図 SNMP TRAP 一覧

CISCO-CONFIG-MAN-MIB	3	0	→ 詳細表示
----------------------	---	---	------------------------

左側から MIB 定義、定義 TRAP 数、登録 TRAP 通知条件数、操作となっています。
詳細表示を開いてください。

図 OID 一覧

CISCO-CONFIG-MAN-MIB SNMP TRAP OID一覧			
TRAP名	OID	登録TRAP通知条件数	操作
ciscoConfigManEvent	.1.3.6.1.4.1.9.9.43.2.0.1	0	→ 詳細表示
ccmCLIRunningConfigChanged	.1.3.6.1.4.1.9.9.43.2.0.2	0	→ 詳細表示
ccmCTIDRolledOver	.1.3.6.1.4.1.9.9.43.2.0.3	0	→ 詳細表示

[← 戻る](#)

この MIB から 3 つの TRAP が定義されました。

通知条件はここから設定します。

受信する OID によってステータスの変化や通知先を変更できます。

3.3.2 MIB ファイル登録時のエラーについて

3.3.2.1 二重登録の禁止

すでに登録されている MIB ファイルをもう一度登録しようとすると、すでに登録されていると表示され登録出来ません。

図 登録時のエラー

MIB ファイルの登録

このMIBファイルは既に登録されています。

MIBファイル
 [参照...](#)

文字コード
 UTF-8 ▼

[キャンセル](#) [登録と承認](#)

3.3.2.2 MIB ファイル以外の形式の禁止

MIB ファイルでないファイルを登録しようとした場合はエラーが表示され登録出来ません。

図 登録時のエラー

The screenshot shows the 'MIBファイルの登録' (MIB File Registration) screen. A red box highlights the error message: 'MIBファイルではないファイルがアップロードされています。' (A file that is not a MIB file has been uploaded.). Below the error message, there is a form with a 'MIBファイル' (MIB File) input field, a '参照...' (Reference...) button, a '文字コード' (Character Code) dropdown menu set to 'UTF-8', and two buttons at the bottom: 'キャンセル' (Cancel) and '登録と承認' (Register and Approve).

3.3.2.3 依存関係の不足

登録しようとしている MIB ファイルに継承元の必要な MIB が X-MON に登録されていない場合はエラーとなり登録出来ません。

図 登録時のエラー

The screenshot shows the 'MIBファイルの登録' (MIB File Registration) screen. A red box highlights the error message: 'このMIBファイルを登録するには以下のMIBファイルが必要です。SNMPv2-TC-v1' (To register this MIB file, the following MIB file is required: SNMPv2-TC-v1).

この場合は表示されている「SNMPv2-TC-v1」という MIB を先に X-MON に登録する必要があります。

3.3.3 SNMP TRAP 管理画面メニューについて

TRAP 管理画面メニューの項目一覧は下記となります。

SNMP trap 一覧	登録されている trap の一覧が表示されます。定義されている trap 数や通知条件数、または詳細が表示されます。監視設定もここから行います。
MIB 一覧	X-MON に MIB ファイルを登録します。MIB ファイルは一覧で表示され、MIB ファイルの内容をプレビューできます。TRAP 通知条件の設定を行うためには、設定する TRAP の OID が含まれている MIB ファイルを登録する必要があります
任意 SNMP TRAP 通知条件一覧	X-MON に MIB ファイルを登録せず、独自の TRAPOID を登録し通知条件の設定を行えます。
非監視 SNMP TRAP 通知設定	X-MON に登録していない条件の TRAP が送られてきた場合に通知するサービス、通知先を登録します。

3.3.4 MIB の文字コード変更する

登録した MIB の文字コードを変更する際は MIB 一覧から対象の MIB ファイル名の [文字コード変更] を開いてください。

図 文字コード変更

CISCO-CONFIG-MAN-MIB	SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, SNMP-FRAMEWORK-MIB, CISCO-TC, CISCO-SMI	UTF-8	<div>文字コード変更</div> <div>削除と承認</div>
--------------------------------------	---	-------	-------------------------------------

変更する文字コードを選択し、変更ボタンを押してください。

図 文字コード変更選択

MIBファイルの文字コード変更

MIBファイル名	文字コード
CISCO-CONFIG-MAN-MIB	UTF-8

キャンセル

変更

例では「CISCO-CONFIG-MAN-MIB」 SJIS へ変更してみます。

変更が完了すれば「CISCO-CONFIG-MAN-MIB の文字コードを SJIS に変更しました」と画面に表示されます。

図 文字コード変更完了

MIB一覧

CISCO-CONFIG-MAN-MIBの文字コードをSJISに変更しました

[SNMP TRAP一覧](#) | [MIB一覧](#) | [任意SNMP TRAP通知条件一覧](#) | [非監視SNMP TRAP通知設定](#)

MIB 一覧でも文字コードの部分が変更されているか確認してください。

図 文字コード変更確認

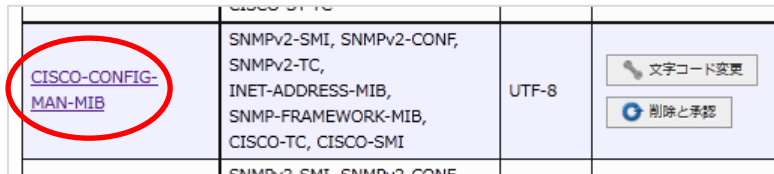
CISCO-CONFIG-MAN-MIB	SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, SNMP-FRAMEWORK-MIB, CISCO-TC, CISCO-SMI	<div>SJIS</div>	<div>文字コード変更</div> <div>削除と承認</div>
--------------------------------------	---	-----------------	-------------------------------------

3.3.5 MIB ファイルの内容をプレビューする

MIB ファイルの内容をプレビューで確認出来ます。

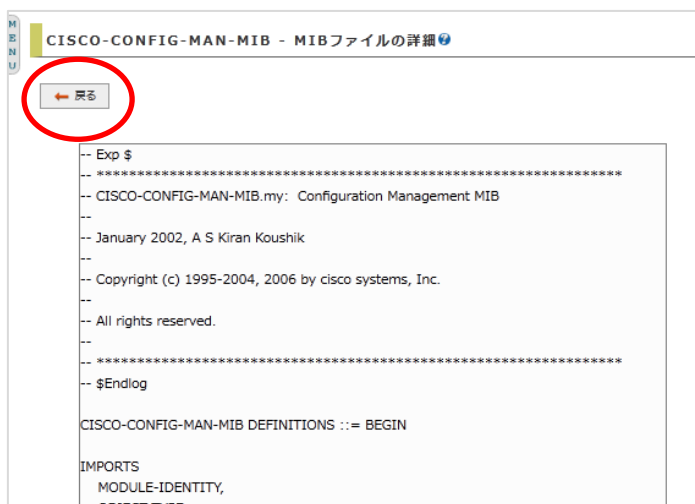
MIB 一覧からプレビューする該当の MIB の名前のリンクを開いてください。

図 MIB ファイル選択



リンクを開くと下記図のような画面となり MIB ファイルの内容を確認出来ます。

図 MIB ファイルプレビュー

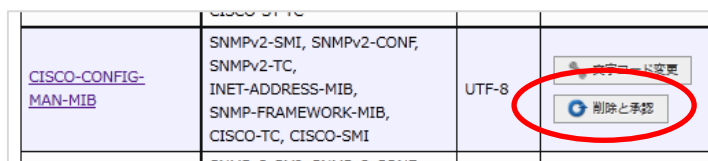


MIB ファイル一覧に戻るには[戻る]を押してください。

3.3.6 MIB を削除する

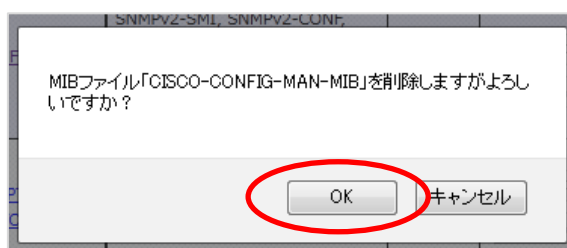
登録している MIB を削除するには、MIB 一覧から対象の MIB ファイル名の[削除と承認]を開いてください。

図 削除と承認



確認ウィンドウが出ますので、OK でしたら OK を押してください。

図 削除の確認



「CISCO-CONFIG-MAN-MIB を削除しました」の表示が出ます。
これで削除は完了です。



3.3.6.1 通知設定（監視）がされている場合

削除対象の MIB から TRAP の通知設定（監視）がされている場合は削除できません。

図 削除エラー



この場合は先に通知設定を削除してください。

（削除の方法については [3.4.4 通知条件の削除する](#) をご参照ください。）

3.4 TRAP 通知条件の設定

必要な MIB を X-MON へ登録できたので、通知条件の設定（監視設定）をしていきましょう。ここでは「CISCO-CONFIG-MAN-MIB」を例にします。

3.4.1 TRAP 通知条件の設定例

メニューから SNMP TRAP 管理を開き SNMP TRAP 一覧を表示します。

図 MENU

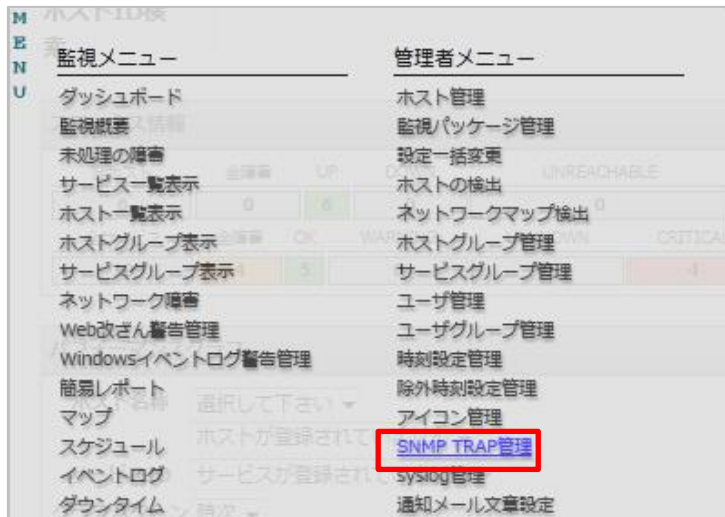


図 SNMP TRAP 一覧

MENU

SNMP TRAP一覧

SNMP TRAP一覧 | [MIB一覧](#) | [任意SNMP TRAP通知条件一覧](#) | [非監視SNMP TRAP通知設定](#)

MIB定義を追加したい場合は「MIB一覧」から登録して下さい

1 | 2 | [次へ >](#) | [最後へ >>](#)

MIB定義	定義TRAP数	登録TRAP通知条件数	操作
ALLIEDTELESYN-MIB	28	0	→ 詳細表示
AT-C9000-MIB	23	0	→ 詳細表示
AT-FS900M-MIB	15	0	→ 詳細表示
AT-GS900M-MIB	27	0	→ 詳細表示
AT-IA800M-MIB	27	0	→ 詳細表示
AT-PAE-MIB	6	0	→ 詳細表示
AtiStackSwitch-MIB	22	0	→ 詳細表示

「CISCO-CONFIG-MAN-MIB」の詳細表示を開いてください。
OID 一覧が表示され、3 つの TRAP が定義されています。

図 SNMP TRAP 一覧

CISCO-CONFIG-MAN-MIB	3	0	→ 詳細表示
----------------------	---	---	------------------------

図 OID 一覧

CISCO-CONFIG-MAN-MIB SNMP TRAP OID一覧			
TRAP名	OID	登録TRAP通知条件数	操作
ciscoConfigManEvent	1.3.6.1.4.1.9.9.43.2.0.1	0	→ 詳細表示
ccmCLIRunningConfigChanged	1.3.6.1.4.1.9.9.43.2.0.2	0	→ 詳細表示
ccmCTIDRolledOver	1.3.6.1.4.1.9.9.43.2.0.3	0	→ 詳細表示

[← 戻る](#)

「ciscoConfigManEvent」の TRAP を設定してみましょう。
詳細表示を開いてください。

図 通知条件一覧

ciscoConfigManEvent SNMP TRAP通知条件一覧

このOIDのTRAPを受信した際の挙動を登録して下さい。

[← 戻る](#) [+ 新規作成](#)

通知条件の一覧が表示されます。まだこの TRAP に対して通知条件は設定されておりませんので、「この OID の TRAP を受信した際の挙動を登録して下さい。」と画面に表示されます。

[新規作成]のボタンがありますので、開きましょう。
条件設定の画面となります。

図 通知条件の設定

それぞれの項目は下記となります。

条件名	登録する通知条件の名前を入力します。
DataBinding(上級者向け)	TRAP OID の中に含まれている変数バインドの情報を表示し条件を指定することが出来ます。TRAP の中には変数バインドを持たないものも含まれます。変数バインドを持っていない場合、「この TRAP は Data Binding を持っていないため設定できません」と表示されます。変数バインドをもっている場合、バインド名、条件入力フィールド、使用条件が表示されます。
バインド名	変数の名前を表示します。
条件入力フィールド	バインド名に対して自由に記述することが出来るテキストフィールドで、使用条件と組み合わせます。

使用条件	<p>「完全一致」「前方一致」「正規表現」が選択でき、その情報と条件入力フィールドの値と組み合わせて比較します。データバインディングの条件は、そのバインド名の項目が未入力だった場合はその項目は比較されません。このため特にそのバインドに対して条件を指定したくない場合は未記入で構いません。</p> <p>正規表現を選択している時は先頭と末尾にデリミタの「/」を必ず指定してください。例:) ^X-MON\$/</p> <p>また、全て未記入の場合エラーではなく対象 TRAP OID が送られてきた場合に通知します。(旧 X-MON2 系仕様)</p>
対象ホスト	<p>通知対象となるホストを選択します。選択したい「ホスト名称」の頭文字や「ホストグループ名称」を選択し、表示された選択肢からホストを選択し、「↑(選択)」をクリックします。また、ホストを除外する場合は、任意のホストを選択後、「↓(外す)」ボタンをクリックします。</p>
通知先グループ	<p>任意 SNMP TRAP 通知条件に反応した場合に通知する通知先グループを選択します。選択したい「ユーザグループ名称」の頭文字を選択し、表示された選択肢から通知先を選択し、「↑(選択)」をクリックします。また、通知先を除外する場合は、任意の通知先を選択後、「↓(外す)」ボタンをクリックします。</p> <p>通知先の登録は、ユーザグループ管理・ユーザグループの作成、編集を参照してください。</p> <p>通知先グループはサービス登録・編集時でも指定が可能な為、どちらの設定条件を優先すべきか選択できます。</p> <p>「チェックで上書き登録/チェックなしで通知先を更新しない」にチェックを付けた場合、通知先情報を上書きし登録します。</p>
通知先サービス名	<p>対象ホストに入力した通知先サービス名が登録されます。新規作成時のみ設定が可能であり、変更はできません。</p> <p>入力制限：入力必須、半角英数字,アンダーバー,ドット,ハイフンのみ。</p> <p>また、以下の通知先サービス名は設定できません。</p> <ul style="list-style-type: none"> ・「-VMPERF」で終わる ・間に「-VMPERF-」を含む ・間に「-VMWARE-」を含む

通知ステータス	対象 TRAP が通知条件と一致した場合に X-MON に投げるステータス情報を「OK」「WARNING」「CRITICAL」「UNKNOWN」から選択します。
---------	--

今回は data binding は入力せず、下記のような条件で設定します。

(Data Binding については [3.4.5 Data Binding について](#) をご参照ください)

対象 TRAP	CISCO-CONFIG-MAN-MIB - ciscoConfigManEvent
条件名	snmp-trap-test
対象ホスト	SW-TRAP
通知先グループ	web チーム
通知先サービス名	snmp-trap-test
通知ステータス	CRITICAL

条件名と通知先サービス名は別の名前を指定出来ますが、同じにしておくほうが管理しやすくなります。

図 条件入力

対象TRAP

CISCO-CONFIG-MAN-MIB - ciscoConfigManEvent

条件名

snmp-trap-test

Data Binding設定(上級者向け)

ccmHistoryEventCommandSource		完全一致 ▼
ccmHistoryEventConfigSource		完全一致 ▼
ccmHistoryEventConfigDestination		完全一致 ▼

対象ホスト

SW-TRAP

↑(選択) ↓(外す)

--- S ---

通知先グループ

Webチーム

↑(選択) ↓(外す)

--- W ---

☐ チェックで上書き登録/チェックなしで通知先を更新しない

通知先サービス名

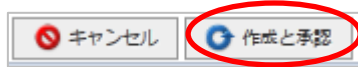
snmp-trap-test

通知ステータス

☐ OK
☐ WARNING
☒ CRITICAL
☐ UNKNOWN

入力出来たら作成と承認を押してください。

図 作成と承認



「snmp-trap-test を設定しました。」と表示されますので、X-MON の再起動を実施してください。



以上で通知条件の作成は完了です。

3.4.2 通知条件の確認する

登録出来ているか確認してみましょう。

SNMP TRAP 一覧の「CISCO-CONFIG-MAN-MIB」の部分に「登録 TRAP 通知条件数」が 1 となっています。

図 登録後

CISCO-CONFIG-MAN-MIB	3	1	→ 詳細表示
----------------------	---	---	--------

詳細表示を開いてください。

「ciscoConfigManEvent」の部分の「登録 TRAP 通知条件数」が 1 となっています。

図 登録後 OID 一覧

TRAP名	OID	登録TRAP通知条件数	操作
ciscoConfigManEvent	.1.3.6.1.4.1.9.9.43.2.0.1	1	→ 詳細表示
ccmCLIRunningConfigChanged	.1.3.6.1.4.1.9.9.43.2.0.2	0	→ 詳細表示
ccmCTIDRolledOver	.1.3.6.1.4.1.9.9.43.2.0.3	0	→ 詳細表示

さらに詳細表示を開くと設定した通知条件一覧が表示されますので、作成した snmp-trap-test が表示されます。

図 登録後通知条件一覧



設定した通知条件を確認するには[詳細表示]を開けば表示されます。

図 通知条件の詳細



サービス一覧を表示させてみましょう。

設定したホストに snmp-trap-test があります。

図 ホスト

ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
SW-TRAP (SW-TRAP)	snmp-trap-test	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするにはスケジュールされていません。

パッシブチェックとなるため、ステータス情報は「このサービスはチェックするにはスケジュールされていません。」と表示されます。

SNMPTT が TRAP を検知し、X-MON へ通知すると検知します。

以上で通知条件の設定と確認は完了です。

実際に検知するかテストは [3.5 動作確認テスト](#)にて行います。

3.4.3 通知条件の編集する

通知条件を編集するには、通知条件の詳細から行います。

該当の通知条件の詳細を表示させ、下の[編集] を開きます。

図 通知条件の詳細

SNMP TRAP通知条件の詳細

対象TRAP
CISCO-CONFIG-MAN-MIB - ciscoConfigManEvent

条件名
snmp-trap-test

Data Binding設定(上級者向け)

ccmHistoryEventCommandSource	指定なし
ccmHistoryEventConfigSource	指定なし
ccmHistoryEventConfigDestination	指定なし

対象ホスト
SW-TRAP

通知先サービス名
snmp-trap-test

通知ステータス
CRITICAL

戻る 編集 削除と承認

編集画面が開きますので、編集したい項目を編集してください。

編集が完了したら、[作成と承認] を押して完了後、X-MON を再起動させます。

図 通知条件の編集

対象TRAP
CISCO-CONFIG-MAN-MIB - ciscoConfigManEvent

条件名
snmp-trap-test

Data Binding設定(上級者向け)

ccmHistoryEventCommandSource		完全一致 ▼
ccmHistoryEventConfigSource		完全一致 ▼
ccmHistoryEventConfigDestination		完全一致 ▼

対象ホスト
SW-TRAP

通知先サービス名
snmp-trap-test

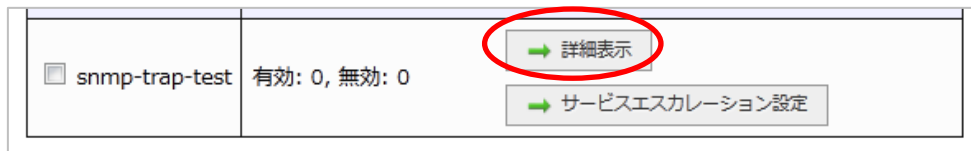
通知ステータス
☐ OK
 ☐ WARNING
 ☒ CRITICAL
 ☐ UNKNOWN

キャンセル 作成と承認

3.4.3.1 編集できる項目について（サービス設定からの編集）

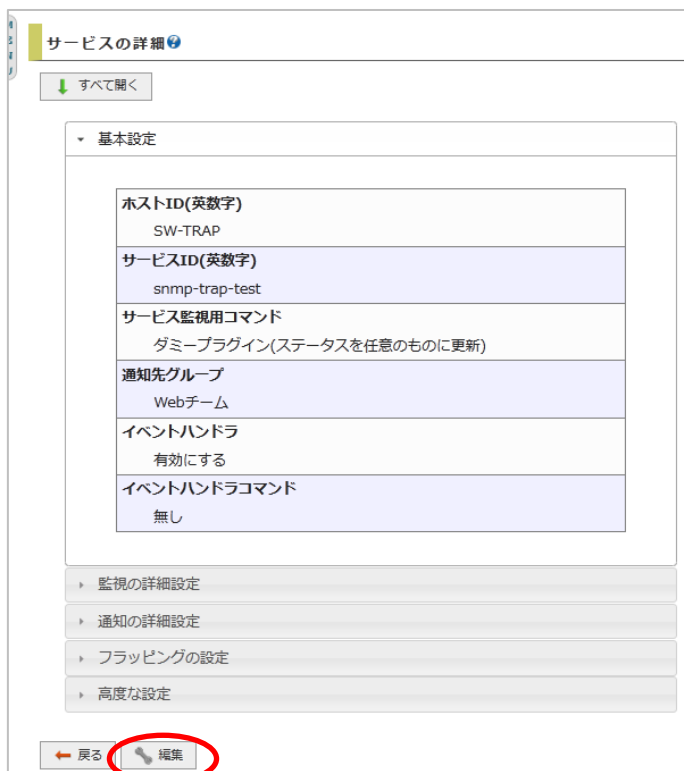
SNMP TRAP 管理からは通知条件について編集を行います。再通知間隔やステータスによる通知の有無、また通知先グループについては[ホスト管理] の[サービス設定] から編集を行います。

図 サービス設定



該当のサービスの[詳細表示] を開きます。一番下に[編集]がありますので開きます。

図 詳細表示



編集画面が開きますので、編集する項目を編集してください。

この際、「サービス監視用コマンド」の部分については SNMP TRAP 管理部分にて動作をさせるための項目ですので編集しないようにお願いします。

編集が完了したら、[編集] もしくは[編集と承認]にて完了させ、X-MON を再起動させてください。

図 編集

サービスの編集

すべて開く

基本設定

ホストID(英数字)
SW-TRAP

サービスID(英数字)
snmp-trap-test

サービス監視用コマンド

DHCPサービス監視

ダミープラグイン(ステータスを任意のものに更新)

ステータス OK

メッセージ OK

通知先グループ

Webチーム

↑(選択) ↓(外す)

選択して下さい

イベントハンドラ

有効にする

イベントハンドラコマンド

実行しない

監視の詳細設定

通知の詳細設定

フラッピングの設定

高度な設定

キャンセル 構築 構築と承認

3.4.4 通知条件の削除する

通知条件を削除するには、通知条件の詳細から行います。

該当の通知条件の詳細を表示させ、下の[削除と承認]を開きます。

図 通知条件の詳細

対象TRAP
CISCO-CONFIG-MAN-MIB - ciscoConfigManEvent

条件名
snmp-trap-test

Data Binding設定(上級者向け)

ccmHistoryEventCommandSource	指定なし
ccmHistoryEventConfigSource	指定なし
ccmHistoryEventConfigDestination	指定なし

対象ホスト
SW-TRAP

通知先サービス名
snmp-trap-test

通知ステータス
CRITICAL

戻る 編集 削除と承認

確認ウィンドウが出ますので、OK でしたら OK を押してください。

図 削除の確認

通知条件「snmp-trap-test」を削除しますがよろしいですか？

OK キャンセル

「設定を削除し反映しました」の表示が出ます。

X-MON を再起動させて完了です。

ciscoConfigManEvent SNMP TRAP通知条件一覧

設定を削除し反映しました。

3.4.4.1 サービス設定から削除する

SNMP TRAP 管理以外にも、[ホスト管理] の[サービス設定]からも通知条件は削除出来ます。どちらで削除を行っても動作への影響はありません。

該当のホストでサービス設定を開いて一覧を表示させます。

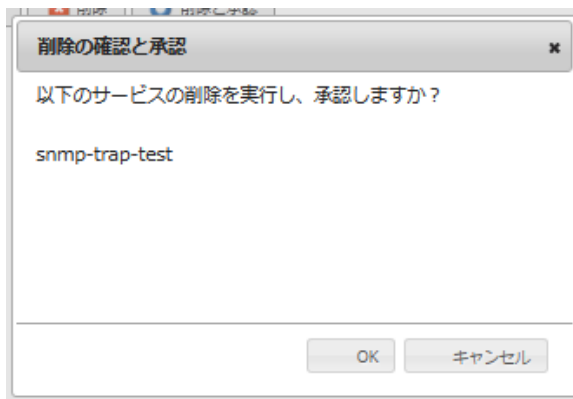
削除するサービスのチェックボックスにチェックを入れて[削除と承認] を押します。

図 サービス設定



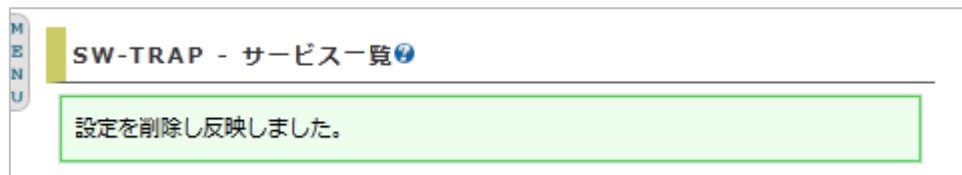
確認ウィンドウが出ますので、OK でしたら OK を押してください。

図 削除の確認



「設定を削除し反映しました。」と表示されますので X-MON を再起動させて完了してください。

図 削除



以上が通知条件の削除方法となります。

3.4.5 Data Binding について

通知条件にある「Data Binding」について解説します。

Data Binding とは変数バインド、不可データとも呼ばれ、SNMP TRAP に付与されるデータの事を指します。同じ OID であっても Data Binding の中の値によってさらに値を振り分ける（通知条件を絞り込む）事が可能となります。

例えば、監視対象ホストのインタフェースのリンクのアップ/ダウンを示す TRAP があります。

この TRAP は「IF-MIB」という名前で定義されており一般的にも広く使われている TRAP となっております。

図 TRAP 定義

IF-MIB	2	3	→ 詳細表示
--------	---	---	------------------------

リンクダウンを示す TRAP は「linkDown」という TRAP 名で定義されており、それ
を示す OID は「.1.3.6.1.6.3.1.1.5.3」です。

図 TRAP 一覧

IF-MIB SNMP TRAP OID一覧?			
TRAP名	OID	登録TRAP通知条件数	操作
linkDown	.1.3.6.1.6.3.1.1.5.3	3	→ 詳細表示
linkUp	.1.3.6.1.6.3.1.1.5.4	0	→ 詳細表示

[← 戻る](#)

この linkDown について Data Binding がどのようなになっているか通知条件の新規作成画面で確認してみます。

図 新規作成

対象TRAP	
IF-MIB - linkDown	
条件名	
<input type="text"/>	
Data Binding設定(上級者向け)	
ifIndex	<input type="text"/> 完全一致 ▾
ifAdminStatus	<input type="text"/> 完全一致 ▾
ifOperStatus	<input type="text"/> 完全一致 ▾

図の通り、「ifindex」「ifAdminStatus」「ifOperStatus」の3つの Data Binding がある事がわかります。

つまり、OID である.1.3.6.1.6.3.1.1.5.3 と共にこの3つのデータが TRAP に含まれるということになります。

「ifindex」はインタフェース番号、「ifAdminStatus」は管理上のステータス（機器としてインタフェースは正常に動作しているか）、「ifOperStatus」は運用上（インタフェ

ースが開いているか閉じているか) のステータスを意味します。

しかし、この Data Binding のデータについては、使用する機器やソフトウェアによってどのようなデータが含まれるか確認する必要があります。

それは機器によって仕様が違う、また拡張 MIB を使用している場合はベンダー固有の MIB となるためどのようなデータが含まれるかは受信してみないとわからないためです。

この DataBinding は X-MON 上では、その通知条件を検知するための条件の一部として考えて頂ければと思います。

例としてこの linkDown を検知する場合を想定してみます。

Data Binding を設定せずに通知条件を作成してみます。

詳細画面では画像のように表示されます。

図 確認

対象TRAP	
IF-MIB - linkDown	
条件名	
IF_test01	
Data Binding設定(上級者向け)	
ifIndex	指定なし
ifAdminStatus	指定なし
ifOperStatus	指定なし

この状態で、監視対象ホスト（設定しているのは switch 機器）の 7 番のインタフェースをダウンさせてみます。「1.3.6.1.6.3.1.1.5.3」の TRAP を検知しますので設定したステータスに変化します。また、ステータス情報を確認してみます。

障害対応ガイド	サービス詳細	ドキュメント	構成情報	イベントログ	通知履歴	外部コマンド履歴
コメント						
現在のステータスは、 異常(CRITICAL)						
<p>A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. 7 FastEthernet0/7 ethernetCsmacd administratively down</p>						
<div>関連付けられたドキュメント</div> <div>ホストドキュメント</div> <div>サービスドキュメント</div>						

画像のようにステータス情報を受信しています。

この時、文章の一番最後に

This other state is indicated by the included value of ifOperStatus. 7 FastEthernet0/7 ethernetCsmacd administratively down

というがあります。FastEthernet0/7 がダウンしたという意味となります。

このように、DataBinding を指定していない場合は DataBinding による振り分け（検知する条件の絞り込み）はされませんので監視対象ホストのどのインタフェースにも対応できる通知条件となる、という事になります。

次に、DataBinding を使用する事を考えてみます。

このステータス情報に「ifOperStatus. 7」という記載があります。この値を X-MON から snmpwalk コマンドで確認します。

```
# snmpwalk -v 2c -c public 192.168.19.101 ifOperStatus.7
IF-MIB::ifOperStatus.7 = INTEGER: down(2)
```

このような結果となります。down(2)に注目します。

DataBinding の設定項目にも ifOperStatus というのがありました。down を意味する数字は「2」である事を示しています。

それでは、この ifOperStatus. 7 が実際にどのインタフェースに関連づけされているか確認してみます。確認するには ifDescr の値を見ます。

```
# snmpwalk -v 2c -c public 192.168.19.101 ifDescr.7
IF-MIB::ifDescr.7 = STRING: FastEthernet0/7
```

Switch 機器の FastEthernet0/7 である事が確認されました。

これに関連付けされている ifIndex の値も確認してみましょう。

```
# snmpwalk -v 2c -c public 192.168.19.101 ifIndex.7
IF-MIB::ifIndex.7 = INTEGER: 7
```

ifIndex の値は 7 であることがわかりました。

それでは、もう一つの値である

```
# snmpwalk -v 2c -c public 192.168.19.101 ifAdminStatus.7
IF-MIB::ifAdminStatus.7 = INTEGER: up(1)
```

up している状態であり、示す数字は「1」である事がわかりました。

情報をここで纏めてみましょう。

FastEthernet0/7 で Data Binding を指定する場合、

ifindex でインタフェース番号を指定すれば、指定したインタフェース番号の linkdown の TRAP を検知します。

idAdminStatus で down の条件を指定する場合は 2 を、up の条件の場合は 1 を入力すれば検知します。

iDoperStatus で down の条件を指定する場合は 2 を、up の条件の場合は 1 を入力すれば検知します。

複数の組み合わせや、完全一致・正規表現も利用出来ます。

このように、DataBinding の値を指定すれば細かく通知条件を指定する事が出来ます。。

しかし、拡張 MIB を利用する場合、DataBinding の内容はベンダーによりさまざまです。さらに、例で示したのは数字を指定する形ですが、テキスト(データ型では String) の DataBinding もあります。さらにシチュエーションにより内容もかわってきます。


そのため、該当の TRAP がどのような DataBinding を付与するかの詳細については各ベンダーサポートにご確認をお願いします。

3.5 動作確認テスト

それでは検知するかテストしてみましょう。

今回登録した Cisco の「CISCO-CONFIG-MAN-MIB」の「ciscoConfigManEvent」は機器の設定ファイルを上書きしたら TRAP を通知します。

(その他の動作でも TRAP を通知しますが、例ではこちらの動作を記載します)

 **テスト前には設定のバックアップを取得するようにしてください**

3.5.1 テストコマンドの発行

今回の例では Cisco Catalyst2950 を使用しています。

まずは通知前のサービスの状態を確認しておきましょう。

図 通知前

ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
SW-TRAP (SW-TRAP)	snmp-trap-test	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。

スイッチでテストコマンドを発行します。

```
SW-TEST# copy run start
```

これでトラップが送信されます。サービス一覧を確認します。

図 通知後

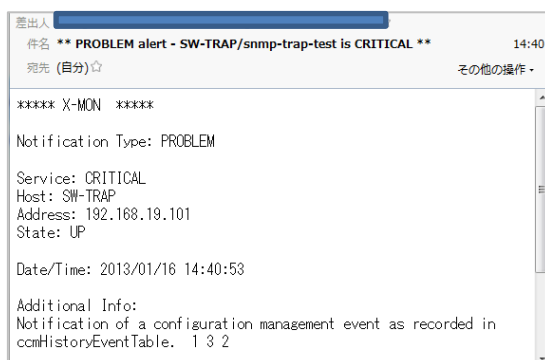
ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
SW-TRAP (SW-TRAP)	snmp-trap-test	異常 (CRITICAL)	2013-01-16 14:41:23	0日と00時間 02分57秒	1/1	Notification of a configuration management event as recorded in comHistoryEventTable. 1 3 4

該当のサービスが critical になっています。

さらにステータス情報には登録した MIB ファイルにひも付けられる情報 (MIB ファイル内に記載されているメッセージ) が表示されます。

また、例ではメール通知をしておりますのでメールも届きます。

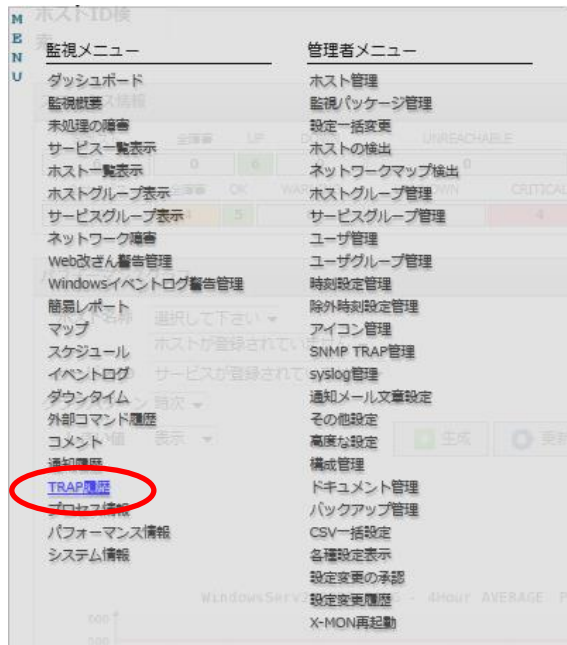
図 通知メール



3.5.2 TRAP 履歴

トラップについては、[メニュー] の[TRAP 履歴]からも確認出来ます。

図 TRAP 履歴



TRAP ログは、X-MON に通知条件の設定（監視の設定）がされているサービスのログの履歴が記録されています。不明 TRAP ログは、反対に通知条件の設定がされていない TRAP が記録されています。

セキュリティ上必要ない TRAP や TRAP のテストで OID を確認する場合はここを調べてください。また、特定の機器から不明な TRAP を受けると通知を行う事が「非監視 SNMP TRAP 通知設定」にて可能です。

こちらの設定方法は [3.7 不明な TRAP を通知する](#) をご参照ください。

図 TRAP ログ

The image shows the 'TRAP 履歴' (TRAP History) page in X-MON. The page title is 'TRAP履歴'. Below it, there is a red circle around the text 'TRAP ログ | 不明TRAPログ'. The main content is a table with the following structure:

受信日時	送信元ホスト
受け取ったOID	
受け取ったメッセージ	
2013年01月21日 10時44分18秒	192.168.19.101
.1.3.6.1.4.1.9.9.43.2.0.1	
Notification of a configuration management event as recorded in ccmHistoryEventTable. 1 3 4	
2013年01月21日 10時43分58秒	192.168.19.101
.1.3.6.1.4.1.9.9.43.2.0.1	

図 不明 TRAP ログ

受信日時	受け取ったOID	送信元ホスト
2013年01月21日 10時44分53秒	.1.3.6.1.4.1.9.0.1 [UNKNOWN TRAP] 5 synReceived 7333 114 2884	192.168.19.101
2013年01月21日 10時43分38秒	.1.3.6.1.4.1.9.0.1 [UNKNOWN TRAP] 5 synReceived 32398 80 2658	192.168.19.101

3.5.3 監視の復旧方法

通知された監視を知らせるにはパッシブの結果を送るという動作になります。

[サービス一覧表示]もから該当のホストのサービス情報画面の[サービス詳細]タブを開きます。今回の例では「SW-TRAP」ホストの「snmp-trap-test」になります。

図 サービス情報

SW-TRAP(SW-TRAP)
 サービスID: snmp-trap-test
 IPアドレス: 192.168.19.101

最終チェック時刻: 2013年01月16日 14時41分23秒
 次回チェック予定: 2013年01月16日 14時45分53秒

現在の状態: **異常(CRITICAL)**
 ステータス情報: Notification of a configuration management event as recorded in cmHistoryEventTable. 1 3 4

パフォーマンスデータ:
 現在の試行数: 1/1(ハード状態)

アクティブチェック: 無効
 パッシブチェック: 有効
 Obsessing: 無効
 通知/エスカレーション: 有効
 イベントハンドラ: 無効

[サービス詳細]タブのメニューの中から「このサービスのパッシブチェックの結果を送信」を開きます。

図 パッシブの結果を送信

このサービスの動作チェックを有効

このサービスの動作チェックを次回スケジュールに追加

このサービスのパッシブチェックの結果を送信

このサービスのパッシブチェックを停止

このサービスのObsessing Overを開始

この問題を認知済にする

このサービスの通知及びエスカレーションを無効

次のサービス通知及びエスカレーションを遅らせる

今すぐ通知及びエスカレーションを実行する

このサービスのダウンタイムをスケジュール

このサービスのイベントハンドラを無効

このサービスのフラップ検知を無効

項目の入力画面になります。

チェック結果を OK にします。(デフォルトで選択されています) チェック出力は必須入力となります。例えば「トラップ検知のテストのため OK」や実際の運用では「トラップ確認、対応完了」などを記載するといいでしょう。

図 パッシブ外部コマンド

入力出来たら[発行]を押します。

コマンドを正常に受け付けた画面となります

図 パッシブ外部コマンド発行

復旧しているか確認しましょう。

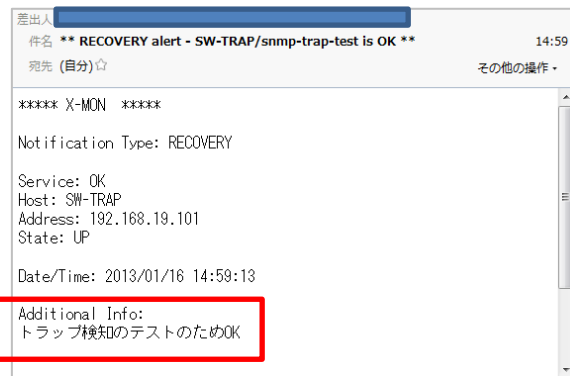
サービス一覧表示にてステータス情報がパッシブの結果を送信の際に入力した「ログ検知のテストのため OK」というステータスとなり正常 (OK) で復旧しています。

図 監視復旧

ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	実行回数	ステータス情報
SW-TRAP (SW-TRAP)	snmp-trap-test	正常(OK)	2013-01-16 14:58:13	0日と00時間00分56秒	1/1	トラップ検知のテストのためOK

また、通知先にも下記のような復旧のメールが届きます。

図 通知メール



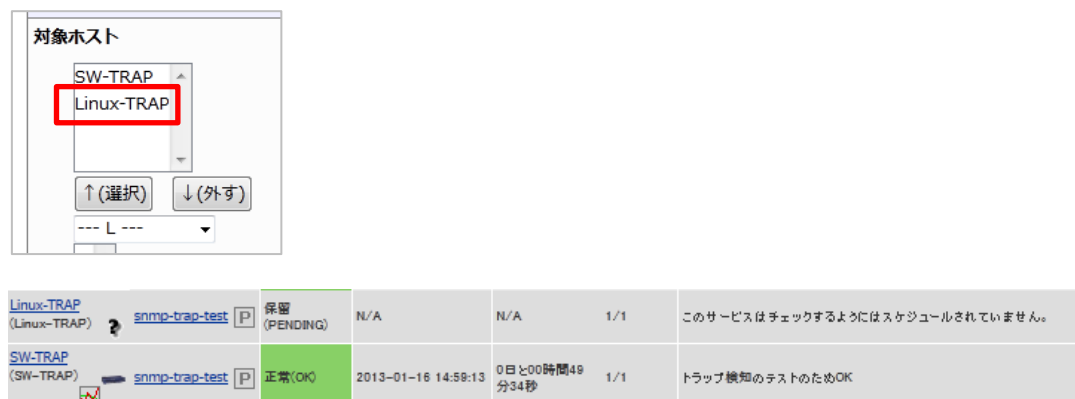
以上が基本的な設定例とテストとなります。

3.5.4 その他の機器でのテスト

サーバソフトウェアの中には GUI の画面からテストを実施する事が可能なものもあります (TrendMicro 社 ServerProtect など)。また、Windows サーバからもテストは可能です。

稼働中の機器のためテストが出来ない場合、linux からコマンドでテストする事も可能です。その場合は、テスト用の linux サーバをホスト登録し、通知条件でテストホストを追加してテストホストにも通知条件を設定してください。既にホスト登録しているサーバでテストを実施して頂いても結構です。

図 テストを行う Linux サーバを追加



今回の例では、OID は「.1.3.6.1.4.1.9.9.43.2.0.1」で X-MON サーバの IP アドレスが「192.168.19.201」ですので、Linux サーバにて発行するコマンドは

```
# snmptrap -v 2c -c public 192.168.19.201 '' .1.3.6.1.4.1.9.9.43.2.0.1
```

となります。

監視ホストにはコミュニティ名の設定はしておりませんが、TRAP は X-MON サーバ

で受け取りますので、デフォルトの public を指定します。

コマンドが発行出来たらサービス一覧を確認します。

図 テスト後

Linux-TRAP (Linux-TRAP)	snmp-trap-test	異常 (CRITICAL)	2013-01-16 15:50:03	0日と00時間00分05秒	1/1	Notification of a configuration management event as recorded in oomHistoryEventTable.
SW-TRAP (SW-TRAP)	snmp-trap-test	正常(OK)	2013-01-16 14:59:13	0日と00時間50分55秒	1/1	トラップ検知のテストのためOK

Linux-TRAP から発行しましたので、Linux-TRAP のみ、CRITICAL を検知しました。
この OID は正常に X-MON で監視出来る事が確認出来ました。

3.6 任意の SNMP TRAP を設定する

基本的な使い方以外に、MIB ファイルがない OID など任意の SNMP TRAP を設定する事が出来ます。

例えば、サーバでバッチスクリプトを定期動作させており、バッチスクリプト完了時に TRAP を送信する設定すれば X-MON にてバッチ処理の監視が可能です。

また、Windows サーバにてイベントトラップトランスレーターを使用する場合はエンタープライズ OID を使用しますので、こちらで登録します。

本セクションでは Linux からと Windows からと設定例を取り上げます。

3.6.1 設定画面

[メニュー]の[SNMP TRAP 管理]から[任意 SNMP TRAP 通知条件一覧]を開いてください。

図 任意 SNMP TRAP 通知条件一覧



何も登録されていない場合は「任意 OID の TRAP を受信した際の挙動を登録して下さい。」と表示されます。

[新規作成]を開いてください。条件を入力する画面が開きます。

図 任意 SNMP TRAP 通知条件の設定

任意SNMP TRAP通知条件の設定

TRAP名

OID

メッセージフォーマット(省略可)

文字コード
UTF-8

対象ホスト

↑(選択) ↓(外す)
選択して下さい

通知先グループ

↑(選択) ↓(外す)
選択して下さい

☐ チェックで書き登録/チェックなしで通知先を更新しない

通知先サービス名
TRAP

通知ステータス
☒ OK ☐ WARNING ☐ CRITICAL ☐ UNKNOWN

キャンセル 作成と承認

それぞれの項目は以下となります。

TRAP 名	登録する TRAP 名を定義します。 既に登録されている MIB ファイル名、TRAP オブジェクト名禁止。
OID	登録する任意 TRAP の OID を指定します
メッセージフォーマット(省略可)	登録した TRAP が送られてきた場合に、サービス一覧表示「ステータス情報」の欄に表示される情報を記述します
文字コード	送られてくるメッセージの文字コードを指定します
対象ホスト	通知対象となるホストを選択します。 選択したい「ホスト名称」の頭文字や「ホストグループ名称」を選択し、表示された選択肢からホストを選択し、「↑(選択)」をクリックします。
	また、ホストを除外する場合は、任意のホストを選択後、「↓(外す)」ボタンをクリックします。
通知先グループ	任意 SNMP TRAP 通知条件に反応した場合に通知する通知

	<p>先グループを選択します。選択したい「ユーザグループ名称」の頭文字を選択し、表示された選択肢から通知先を選択し、「↑(選択)」をクリックします。また、通知先を除外する場合は、任意の通知先を選択後、「↓(外す)」ボタンをクリックします。</p> <p>通知先の登録は、ユーザグループ管理・ユーザグループの作成、編集を参照してください。</p> <p>通知先グループはサービス登録・編集時でも指定が可能な為、どちらの設定条件を優先すべきか選択できます。</p> <p>「チェックで上書き登録/チェックなしで通知先を更新しない」にチェックを付けた場合、通知先情報を上書きし登録します。</p>
通知先サービス名	<p>対象ホストに入力した通知先サービス名が登録されます。新規作成時のみ設定が可能であり、変更はできません。</p> <p>入力制限：入力必須、半角英数字,アンダーバー,ドット,ハイフンのみ。</p> <p>また、以下の通知先サービス名は設定できません。</p> <ul style="list-style-type: none"> ・「-VMPERF」で終わる ・間に「-VMPERF-」を含む ・間に「-VMWARE-」を含む
通知ステータス	<p>対象 TRAP が通知条件と一致した場合に X-MON に投げるステータス情報を「OK」「WARNING」「CRITICAL」「UNKNOWN」から選択します。</p>

3.6.2 OID について

OID には標準 MIB と拡張 MIB（別名：エンタープライズ MIB）があります。

標準 MIB は多くのベンダーで共通で使用されている定義で、拡張 MIB がベンダー独自に定義している MIB となります。任意での OID を作成する場合、この拡張 MIB を指定する形となります。しかし、拡張 MIB は IANA(<http://www.iana.org/>)にて登録する必要があります。独自にする際の OID は

.1.3.6.1.4.1.

から始まるようにしてください。この.1.3.6.1.4.1.から始まる OID は拡張 MIB であることを意味しています。また、使用する際はプライベートネットワーク内でのみ使用するようにお願いします。（すでに登録されている IANA の拡張 MIB と被る可能性があるため）

3.6.3 設定例(Linux サーバからの任意 TRAP 通知)

設定例として、Linux サーバから

.1.3.6.1.4.1.3.3.3.4

という OID を受信したらメッセージ（ステータス情報で表示される）に「任意トラップテスト」と表示するようにしましょう。

設定項目は表の通りです。

TRAP 名	TRAP-ORI-TEST
OID	.1.3.6.1.4.1.3.3.3.4
メッセージフォーマット	任意トラップテスト
文字コード	UTF-8
対象ホスト	Linux-TRAP
通知先グループ	web チーム
通知先サービス名	TRAP-ORI-TEST
通知ステータス	CRITICAL

条件を設定した例は下記となります。

図 任意 SNMP TRAP 通知条件の設定

任意SNMP TRAP通知条件の設定

TRAP名
TRAP-ORI-TEST

OID
.1.3.6.1.4.1.3.3.3.4

メッセージフォーマット(省略可)
任意トラップテスト

文字コード
UTF-8

対象ホスト
Linux-TRAP

通知先グループ
Webチーム

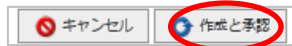
通知先サービス名
TRAP-ORI-TEST

通知ステータス
☐ OK
 ☐ WARNING
 ☒ CRITICAL
 ☐ UNKNOWN

条件名と通知先サービス名は別の名前を指定出来ますが、同じにしておくほうが管理しやすくなります。

記入が出来たら[作成と承認] ボタンを押して作成してください。

図 作成と承認



作成が出来ると、一覧の画面に戻り、「TRAP-ORI-TEST を設定しました」と表示されます。反映させるため、X-MON を再起動させてください。

図 設定完了



サービスの一覧で確認してみましょう。

図 正常時

ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
Linux-TRAP (Linux-TRAP)	TRAP-ORI-TEST	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。

正常に追加されています。

確認する際のコマンドは

```
# snmptrap -v 2c -c public 192.168.19.201 '' .1.3.6.1.4.1.3.3.3.4
```

となります。テストの準備が出来たらコマンドを発行してください。

3.6.3.1 テストの確認

図 TRAP 検知

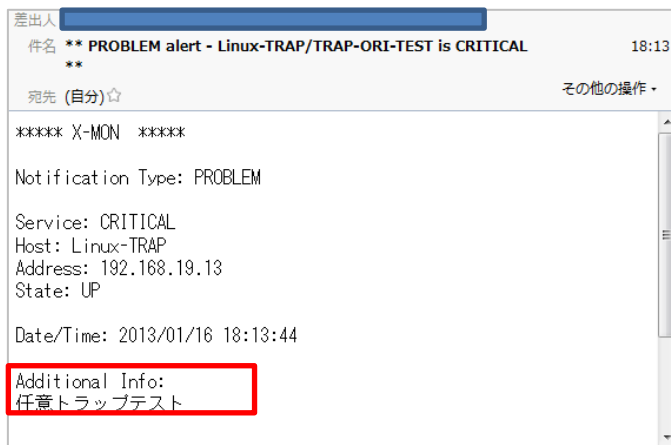
ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
Linux-TRAP (Linux-TRAP)	TRAP-ORI-TEST	異常 (CRITICAL)	2013-01-16 18:13:44	0日と00時間 00分14秒	1/1	任意トラップテスト

正常に任意 SNMPTRAP が検知したら画像のようになります。

ステータス情報にも「任意トラップテスト」と設定した文字列が表示されます。

またメールでも通知先を設定していますので、画像のようにメールが送信されます。

図 検知メール



監視を復旧させる際は基本操作と同じくパッシブから OK をして復旧させてください。

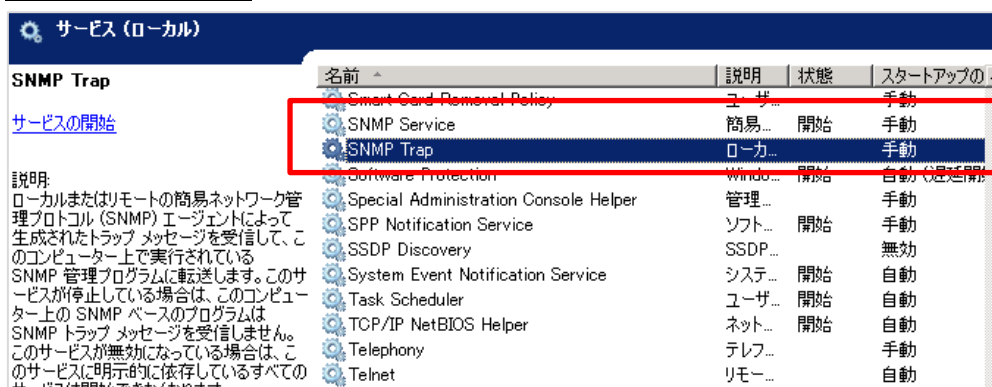
これで、任意の SNMPTRAP である、OID「.1.3.6.1.4.1.3.3.4」は正常に登録されており、検知可能であることがわかりました。

3.6.4 設定例（Windows サーバからの任意 TRAP 通知）

Windows サーバの SNMP TRAP は MIB ファイルがないため任意 SNMP TRAP 通知で設定します。

Windows サーバにはデフォルトで SNMP Trap サービスはインストールされていますが TRAP 通知の設定をするには SNMP サービスをインストールする必要があります。インストール手順は別途、SNMP 導入手順をご参照ください。

図 SNMP サービス

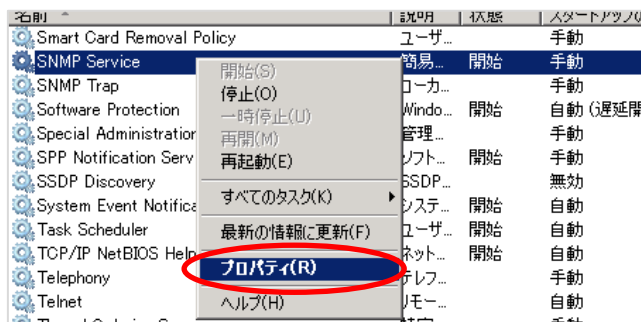


3.6.4.1 通知先の設定

Windows サーバの SNMP サービスから TRAP の通知先を設定します。

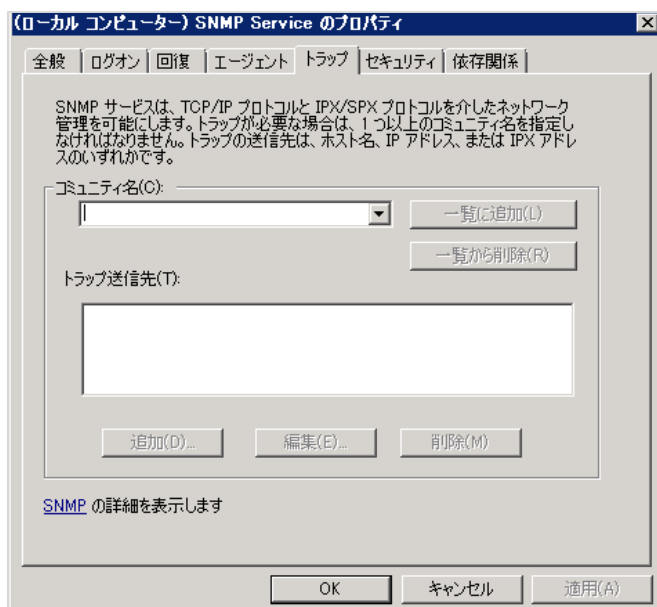
[サービス]から [SNMP Service] を右クリックし、[プロパティ]を開いてください。

図 プロパティ



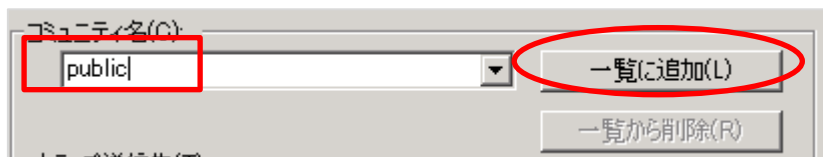
プロパティ画面が表示されますので、「トラップ」タブを開きます。

図 TRAP タブ



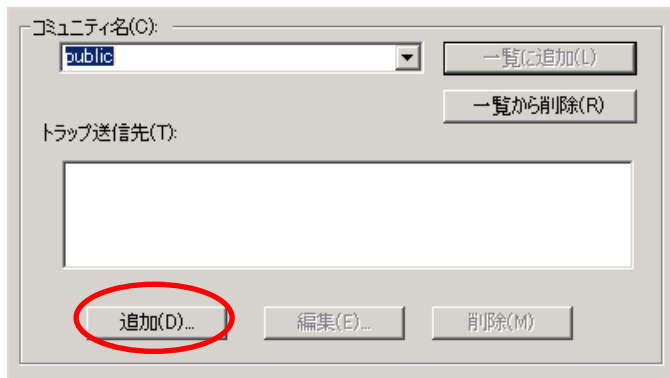
X-MON のデフォルトのコミュニティ名である「public」と入力し、「一覧に追加」ボタンを押してください。

図 コミュニティ名入力



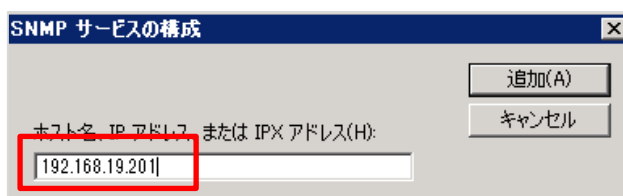
「一覧に追加」をすると、「トラップ送信先」に「追加」ボタンがアクティブになりますので、「追加」を押します。

図 トラップ送信先



IP アドレスを入力する画面が出ますので X-MON サーバの IP アドレスを入力します。

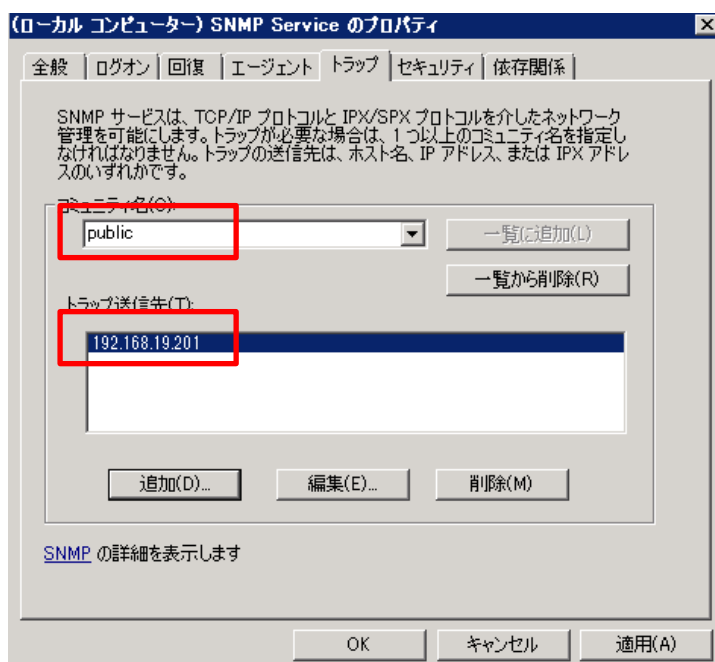
図 IP アドレスの入力



入力できたら[追加] を押してください。

これでコミュニティ名「public」でトラップ送信先が「192.168.19.201」が登録できました。[OK]ボタンを押してプロパティを閉じてください。

図 入力完了

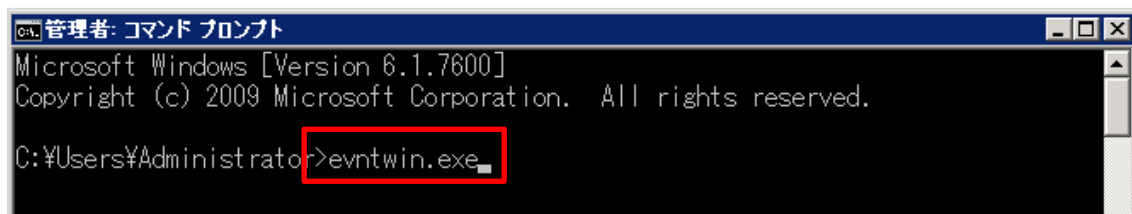


3.6.4.2 TRAP の送信

Windows サーバにて SNMP TRAP を送信するにはイベントトラップトランスレーターで設定します。

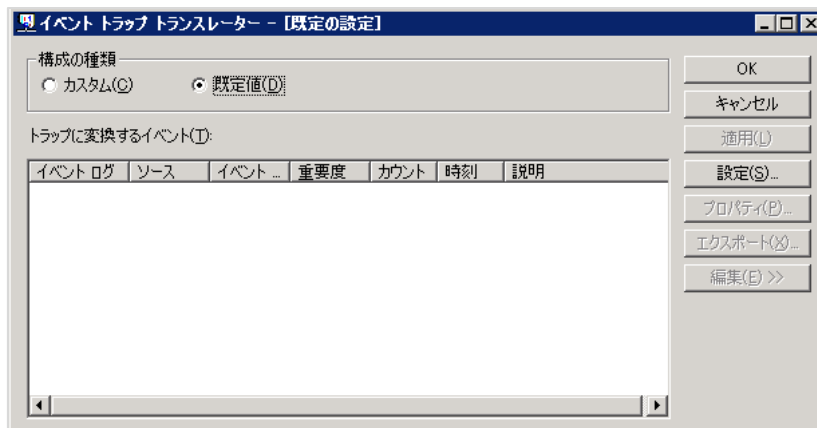
コマンドプロンプトにて、「eventwin.exe」を実行します。

図 コマンドプロンプト



イベントトラップトランスレーターが起動します。何も設定が入っていない場合は空欄となります。詳細はマイクロソフトのサポートマニュアルをご参照ください。

図 イベントトラップトランスレーター

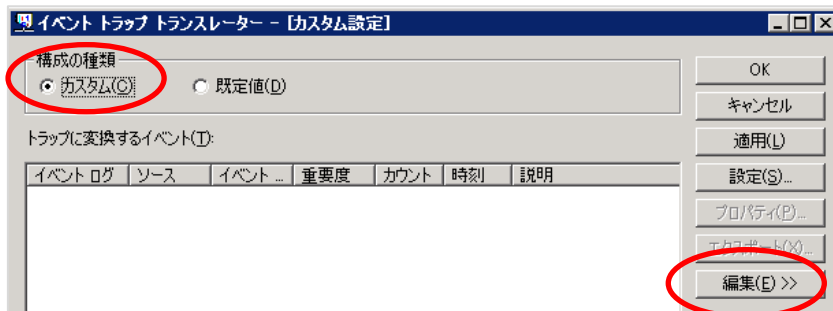


設定例では、DHCP クライアントサービスが停止すればトラップを送信する、という設定を行います。

[構成の種類] のラジオボタンを[カスタム] を選択します。

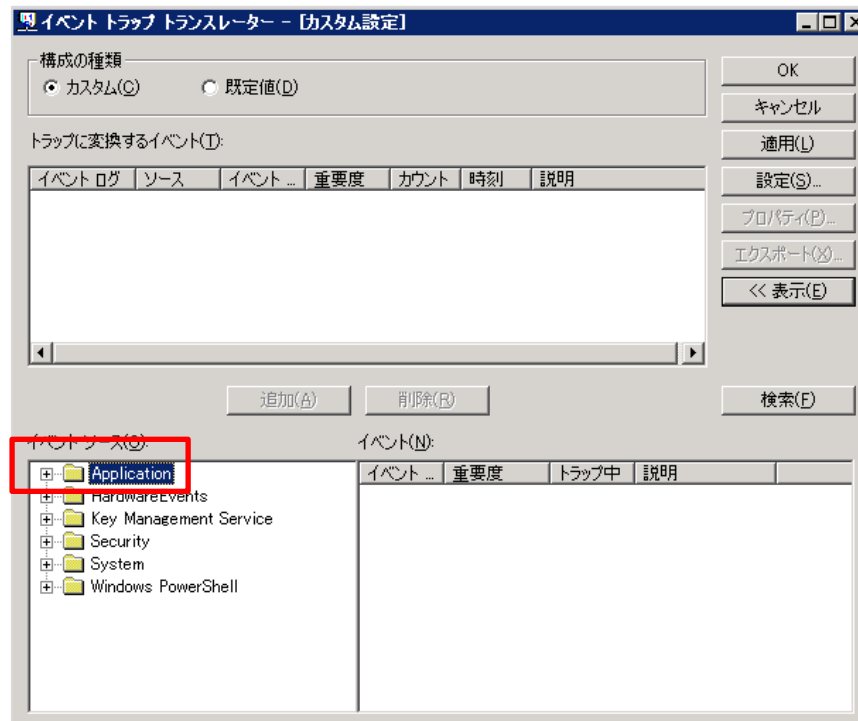
[編集] ボタンがアクティブになりますので開きます。

図 カスタム



ウィンドウの下部分にイベントソースなどが表示されます。

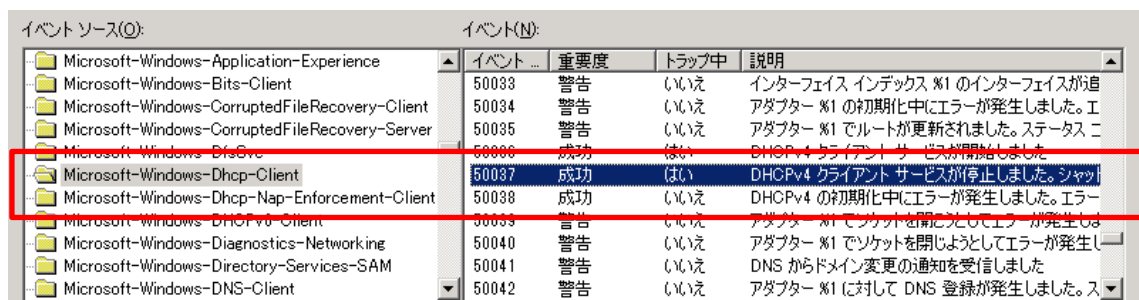
図 イベントソース



イベントソースの中の[System -> Microsoft-Windows-Dhcp-Client]ので、50037 番を選択します。

この 50037 番が Dhcp クライアントサービスが停止したイベントの番号です。

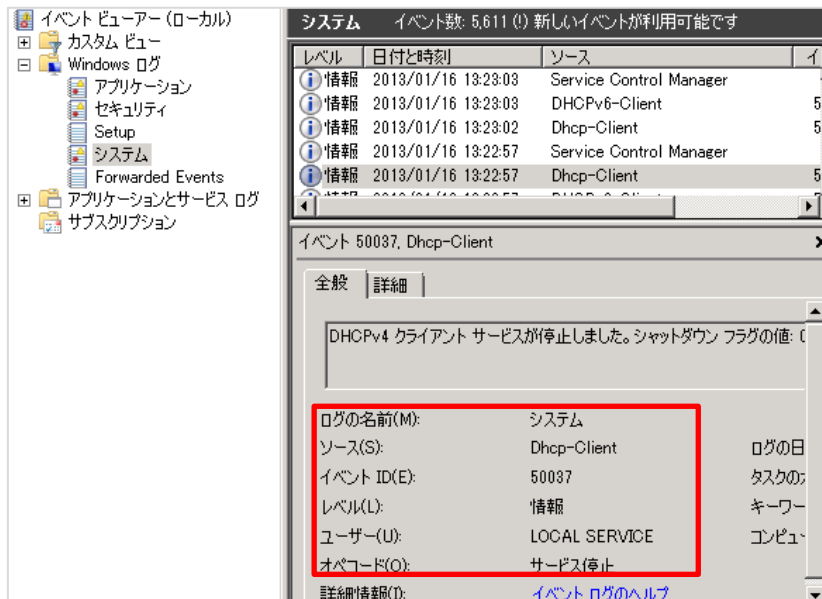
図 イベントソースを選択



この番号はイベントビューアーにて確認が出来ます。

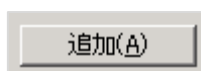
そのため他の任意のサービスやイベントにトラップを設定する際はイベントビューアーからイベント ID を検索してください。

図 イベントビューアー



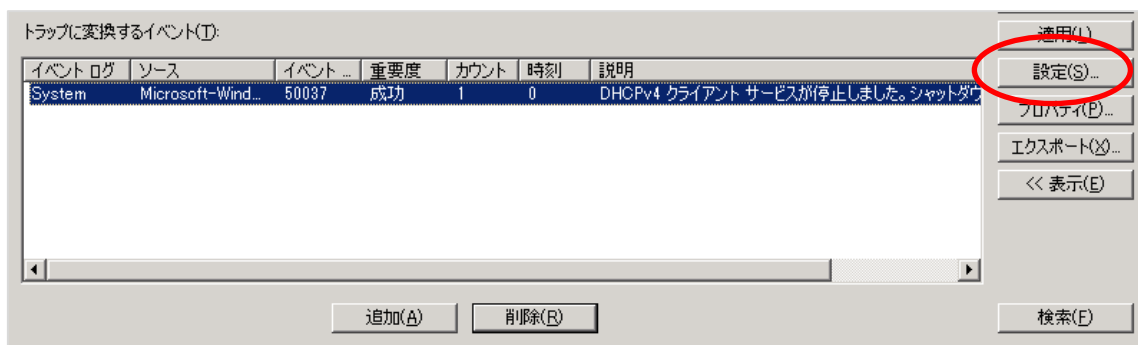
イベントの 50037 番を選択し、[追加]を押してください。

図 追加



追加されると、「トラップに変換するイベント」に追加されます。

図 追加後



OID を確認するには[設定]を開きます。

図 プロパティ

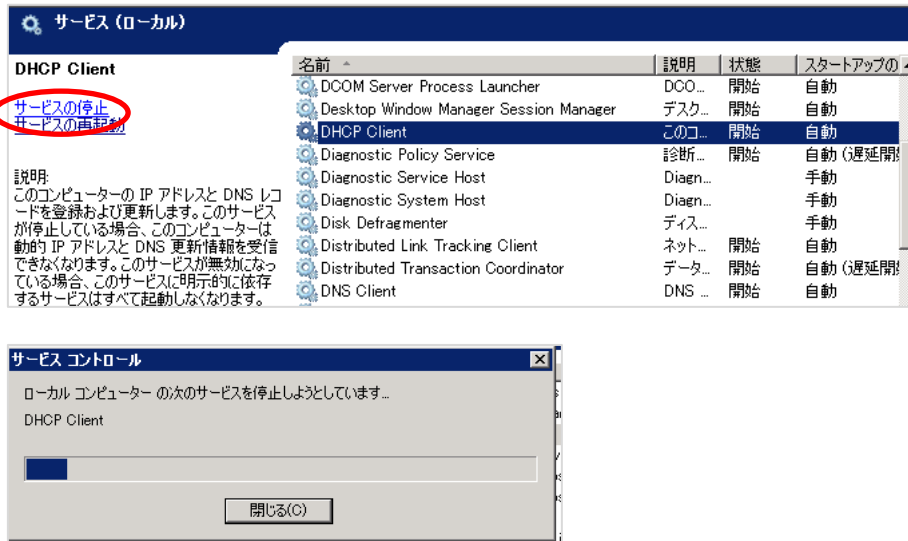
エンタープライズ OID とイベント固有の ID を足したものが OID となります。
 しかし、Windows サーバの場合、OID がとても長くなっています。
 そのため、X-MON 側では通知設定はまだせず、テストでトラップを送信し、SNMP
 TRAP 履歴の不明トラップの画面で OID を確認する方法をとります。
 [OK]で画面が戻ります。

画面が戻り、[適用]を押してください。これで設定は完了です。

図 適用

それでは、実際に TRAP を送信します。
 サービスの画面にて[DHCP Client]を停止させます。
 実際にサービスを停止して確認をする際は、サービス影響に問題がないか確認してから実施するようにしてください

図 サービスの停止



サービスが停止したのを確認して X-MON の TRAP 履歴の不明 TRAP ログを確認します。

図 不明 TRAP ログ

TRAPログ 不明TRAPログ	
受信日時	送信元ホスト
受け取ったOID	
受け取ったメッセージ	
2013年02月27日 16時25分44秒	192.168.19.180
.1.3.6.1.4.1.311.1.13.1.29.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.68.104.99.112.45.67.108.105.101.110.116.0.50037	
[UNKNOWN TRAP] DHCPv4 クライアント サービスが停止しました。シャットダウン フラグの値: 0 LOCAL SERVICE WIN-E7RDU5UA00S 4 4 0	

画像のように、送信元ホストが設定した Windows サーバ、受け取ったメッセージの部分に「DHCPv4 クライアント サービスが停止しました。」というメッセージが含まれていれば正常に TRAP が送信され、X-MON でも受信出来ている事が確認出来ました。受け取った OID の部分の OID を任意 SNMP TRAP 通知で設定します。

3.6.4.3 X-MON へ通知条件の設定

前章にて調べた（不明 TRAP ログにて確認した）OID を使用します。

設定項目は表の通りです。

TRAP 名	TRAP-Windows-TEST
OID	.1.3.6.1.4.1.311.1.13.1.29.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.68.104.99.112.45.67.108.105.101.110.116.0.50037
メッセージフォーマット	任意トラップ Windows テスト
文字コード	SJIS

対象ホスト	Windows-TRAP
通知先グループ	web チーム
通知先サービス名	TRAP-Windows-TEST
通知ステータス	CRITICAL

条件を設定した例は下記となります。

図 任意 SNMP TRAP 通知条件の設定

任意SNMP TRAP通知条件の設定

TRAP名
TRAP-Windows-TEST

OID
.1.3.6.1.4.1.311.1.13.1.29.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.4!

メッセージフォーマット(省略可)
任意トラップWindowsテスト

文字コード
SJIS

対象ホスト
Windows-TRAP
↑(選択) ↓(外す)
--- W ---

通知先グループ
Webチーム
↑(選択) ↓(外す)
--- W ---

☐ チェックで書き登録/チェックなしで通知先を更新しない

通知先サービス名
TRAP-Windows-TEST

通知ステータス
☐ OK ☐ WARNING ☒ CRITICAL ☐ UNKNOWN

キャンセル 作成と承認

条件名と通知先サービス名は別の名前を指定出来ますが、同じにしておくほうが管理しやすくなります。また、Windows 環境から送られてきますので文字コードを「SJIS」にしています。

記入が出来たら[作成と承認] ボタンを押して作成してください。

図 作成と承認

キャンセル 作成と承認

作成が出来ると、一覧の画面に戻り、「TRAP-Windows-TEST を設定しました」と表

示されます。反映させるため、X-MON を再起動させてください。

図 設定完了



サービスの一覧で確認してみましょう。

監視が追加されている事が確認出来ました。

図 確認

ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
Windows-TRAP (Windows-TRAP)	TRAP-Windows-TEST	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。

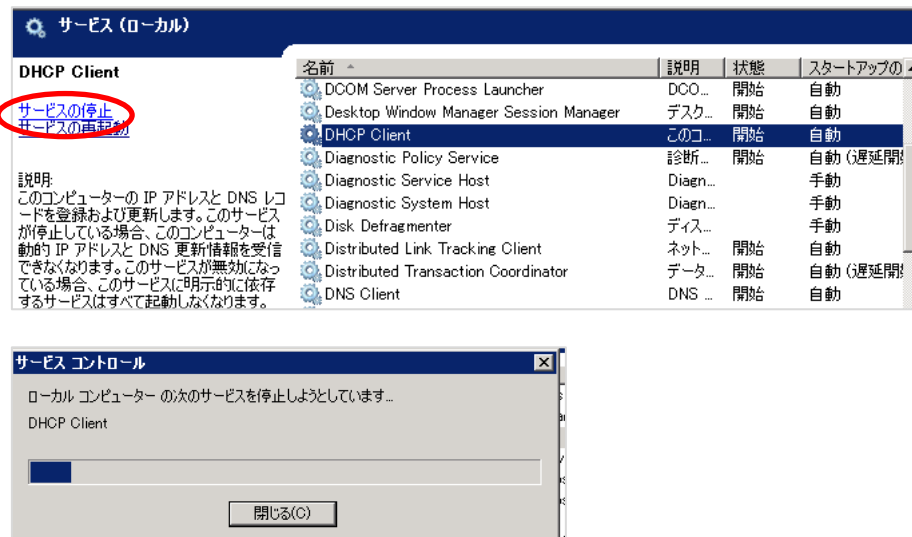
これで通知条件の設定は完了です。

3.6.4.4 テストの確認

それでは、[3.6.4.2 TRAP の送信](#) で実施したように、Windows 上で TRAP を発生させて X-MON で検知するかテストしてみましょう。

実際にサービスを停止して確認をする際は、サービス影響に問題がないか確認してから実施するようにしてください

図 サービスの停止



サービス一覧で確認してみましょう。

図 検知後

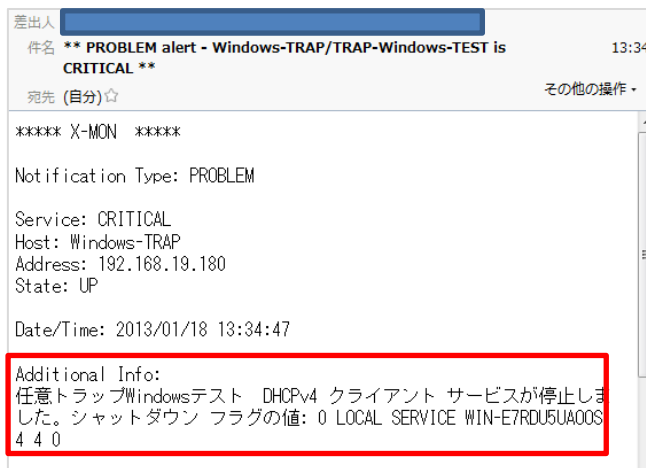
ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
Windows-TRAP (Windows-TRAP)	TRAP-Windows-TEST	異常 (CRITICAL)	2013-01-18 13:34:47	0日と00時間 00分09秒	1/1	任意トラップWindowsテスト DHCPv4 ク ライアント サービスが停止しました。 シャットダウン フラグの値: 0 LOCAL SERVICE WIN-E7RDU5UA00S 4 4 0

正常に検知しています。

ステータス情報の欄には、通知条件で設定した「任意トラップ Windows テスト」の後に TRAP に含まれるメッセージが表示されます。

メールの通知先には下記のようなメールが届きます。

こちらにもステータス情報が記載されています。



監視を復旧させる際は基本操作と同じくパッシブから OK をして復旧させてください。

これで、正常に登録されており、検知可能であることがわかりました。

3.6.5 通知条件の編集する

通知条件を編集するには、通知条件の詳細から行います。

任意 SNMP TRAP 通知条件一覧から該当の通知条件の詳細を表示させ、下の[編集]を開きます。

図 通知条件の詳細

任意SNMP TRAP通知条件の詳細

TRAP名	TRAP-ORI-TEST
OID	.1.3.6.1.4.1.3.3.3.4
メッセージフォーマット	任意トラップテスト
文字コード	UTF-8
対象ホスト	Linux-TRAP
通知先サービス名	TRAP-ORI-TEST
通知ステータス	CRITICAL

戻る 編集 削除と承認

編集画面が開きますので、編集したい項目を編集してください。

編集が完了したら、[作成と承認] を押して完了後、X-MON を再起動させます。

図 通知条件の編集

任意SNMP TRAP通知条件の設定

TRAP名	TRAP-ORI-TEST
OID	.1.3.6.1.4.1.3.3.3.4
メッセージフォーマット(省略可)	任意トラップテスト
文字コード	UTF-8
対象ホスト	Linux-TRAP
通知先サービス名	TRAP-ORI-TEST
通知ステータス	<input type="radio"/> OK <input type="radio"/> WARNING <input checked="" type="radio"/> CRITICAL <input type="radio"/> UNKNOWN

キャンセル 作成と承認

3.6.5.1 編集できる項目について（サービス設定からの編集）

SNMP TRAP 管理からは通知条件について編集を行います。再通知間隔やステータスによる通知の有無、また通知先グループについては[ホスト管理] の[サービス設定] から編集を行います。

図 サービス設定

登録サービス	エスカレーション設定数	操作	
<input type="checkbox"/> TRAP-ORI-TEST	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスカレーション設定

該当のサービスの[詳細表示] を開きます。一番下に[編集]がありますので開きます。

図 詳細表示

サービスの詳細

すべて開く

基本設定

ホストID(英数字)

Linux-TRAP

サービスID(英数字)

TRAP-ORI-TEST

サービス監視用コマンド

ダミープラグイン(ステータスを任意のものに更新)

通知先グループ

無し

イベントハンドラ

有効にする

イベントハンドラコマンド

無し

監視の詳細設定

通知の詳細設定

フラッピングの設定

高度な設定

戻る

編集

編集画面が開きますので、編集する項目を編集してください。

この際、「サービス監視用コマンド」の部分については SNMP TRAP 管理部分にて動作をさせるための項目ですので編集しないようにお願いします。

編集が完了したら、[編集] もしくは[編集と承認]にて完了させ、X-MON を再起動させてください。

図 編集

サービスの編集

すべて開く

基本設定

ホストID(英数字)
Linux-TRAP

サービスID(英数字)
TRAP-ORI-TEST

サービス監視用コマンド

DHCPサービス監視
ダミープラグイン(ステータスを任意のものに更新)
ステータス OK
メッセージ OK

通知先グループ

↑(選択) ↓(外す)
選択して下さい

イベントハンドラ
有効にする

イベントハンドラコマンド
実行しない

監視の詳細設定
通知の詳細設定
フラッピングの設定
高度な設定

キャンセル 編集 削除と承認

3.6.6 通知条件の削除する

通知条件を削除するには[任意 SNMP TRAP 通知条件一覧] から行います。

削除する該当の TRAP の[詳細表示] を開きます。

図 任意 SNMP TRAP 通知条件一覧

任意 SNMP TRAP 通知条件一覧

SNMP TRAP一覧 | MIB一覧 | 任意SNMP TRAP通知条件一覧 | 非監視SNMP TRAP通知設定

新規作成

TRAP名	OID	操作
TRAP-ORI-TEST	.1.3.6.1.4.1.3.3.3.4	→ 詳細表示

詳細が表示されますので、[削除と承認] ボタンを開きます。

図 詳細

TRAP名	TRAP-ORI-TEST
OID	.1.3.6.1.4.1.3.3.3.4
メッセージフォーマット	任意トラップテスト
文字コード	UTF-8
対象ホスト	Linux-TRAP
通知先サービス名	TRAP-ORI-TEST
通知ステータス	CRITICAL

戻る 編集 削除と承認

確認ウィンドウが出ますので、OK でしたら[OK]を押してください。

図 確認

任意OID条件「TRAP-ORI-TEST」を削除しますがよろしいですか？

OK キャンセル

削除が実施され、「設定を削除し反映しました」と表示されますので X-MON を再起動して完了してください。

図 削除後

設定を削除し反映しました。

[SNMP TRAP一覧](#) | [MIB一覧](#) | [任意SNMP TRAP通知条件一覧](#) | [非監視SNMP TRAP通知設定](#)

新規作成

任意OIDのTRAPを受信した際の挙動を登録して下さい。

登録している MIB ファイルを削除する場合は、監視設定がされている場合、削除ができませんが、任意 SNMP TRAP 通知の場合、登録した OID が監視設定されていても OID を監視が削除されます。

3.6.6.1 サービス設定から削除する

SNMP TRAP 管理以外にも、[ホスト管理] の[サービス設定]からも通知条件は削除出来ます。どちらで削除を行っても動作への影響はありません。

該当のホストでサービス設定を開いて一覧を表示させます。

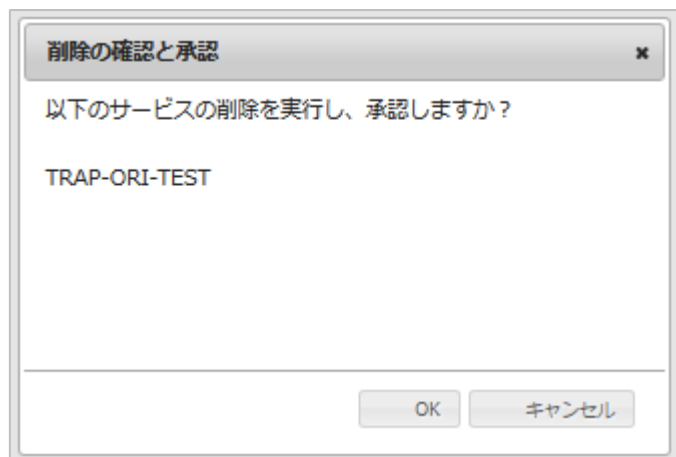
削除するサービスのチェックボックスにチェックを入れて[削除と承認] を押します。

図 サービス設定



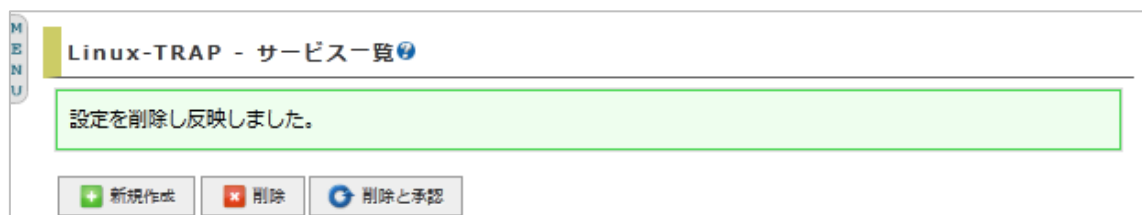
確認ウィンドウが出ますので、OK でしたら OK を押してください。

図 削除の確認



「設定を削除し反映しました。」と表示されますので X-MON を再起動させて完了してください。

図 削除



以上が通知条件の削除方法となります。

3.7 不明な TRAP を通知する

「非監視 SNMP TRAP 通知設定」を使用すると、対象ホストの通知条件を設定していない TRAP を受信したら X-MON へ通知します。MIB ファイルで定義されている TRAP も、定義されていない TRAP も全てが対象となります。

検知する TRAP は[MENU] の [TRAP 履歴] 内、[不明 TRAP ログ] の部分となります。

図 不明 TRAP ログ

TRAP 履歴		
TRAP ログ 不明 TRAP ログ		
受信日時	受け取ったOID	送信元ホスト
受け取ったメッセージ		
2013年02月27日 16時25分44秒		192.168.19.180
1.3.6.1.4.1.311.1.13.1.29.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.68.104.99.112.45.67.108.105.101.110.116.0.5003.7		
[UNKNOWN TRAP] DHCPv4 クライアント サービスが停止しました。シャットダウン フラグの値: 0 LOCAL SERVICE WIN-E7RDU5UA00S 4 4 0		
2013年02月27日 16時24分18秒		192.168.19.180
1.3.6.1.4.1.311.1.13.1.29.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.68.104.99.112.45.67.108.105.101.110.116.0.5003.6		
[UNKNOWN TRAP] DHCPv4 クライアント サービスが開始しました LOCAL SERVICE WIN-E7RDU5UA00S 4 4		

3.7.1 設定画面

[MENU] の [SNMP TRAP 管理] の [非監視 SNMP TRAP 設定] を開きます。

図 非監視 SNMP TRAP 設定

非監視 SNMP TRAP 通知設定
SNMP TRAP一覧 | MIB一覧 | 任意SNMP TRAP通知条件 | 非監視SNMP TRAP通知設定

対象TRAP
不明TRAP 条件不一致TRAP全て

対象ホスト
X-MON
↑(選択) ↓(外す)
選択して下さい

通知先グループ
↑ ↓
↑(選択) ↓(外す)
選択して下さい

☒ チェックで上書き登録/チェックなしで通知先を更新しない

通知先サービス名
DEFAULT-TRAP

通知ステータス
UNKNOWN

設定

それぞれの項目は以下となります。

対象 TRAP	<p>デフォルト TRAP の条件が表示されます。</p> <p>デフォルト TRAP は、X-MON で登録されていない TRAP や、条件に一致しなかった TRAP が対象となります</p> <p>この項目は固定で変更は出来ません。</p>
対象ホスト	<p>通知対象となるホストを選択します。</p> <p>選択したい「ホスト名称」の頭文字や「ホストグループ名称」を選択し、表示された選択肢からホストを選択し、「↑(選択)」をクリックします。また、ホストを除外する場合は、任意のホストを選択後、「↓(外す)」ボタンをクリックします。</p>
通知先グループ	<p>デフォルト TRAP が反応した場合に通知する通知先グループを選択します。選択したい「ユーザグループ名称」の頭文字を選択し、表示された選択肢から通知先を選択し、「↑(選択)」をクリックします。また、通知先を除外する場合は、任意の通知先を選択後、「↓(外す)」ボタンをクリックします。</p> <p>通知先の登録は、ユーザグループ管理・ユーザグループの作成、編集を参照してください。通知先グループはサービス登録・編集時でも指定が可能な為、どちらの設定条件を優先すべきか選択できます。</p> <p>「チェックで上書き登録/チェックなしで通知先を更新しない」にチェックを付けた場合、通知先情報を上書きし登録します。</p>
通知先サービス名	<p>対象ホストに登録する際のサービス名を表示します。</p> <p>「DEFAULT-TRAP」というサービス名で固定されます。</p>
通知ステータス	<p>対象サービスにステータス通知する際のステータスを表示します。「UNKNOWN」で固定されます。</p>

先にも記載しましたが、本設定は対象ホストの不明 TRAP となります。

「対象ホスト」で複数の通知対象のホストを選択（選択したホストに監視が追加されます）すると同じ「DEFAULT-TRAP」で対象ホストにサービスが追加されます。その場合、不明 TRAP を受信した際は送信元のホストと一致したホストのみが通知されます。

3.7.2 設定例

それでは設定してみましょう。

前章でも記載しましたが、全ての不明 TRAP を検知しますので、対象ホストは X-MON のみとし、通知先に Web チームを選択します。

図 設定例

対象TRAP
不明TRAP 条件不一致TRAP全て

対象ホスト
X-MON
↑(選択) ↓(外す)
選択して下さい

通知先グループ
Webチーム
↑(選択) ↓(外す)
--- W ---

☒ チェックで上書き登録/チェックなしで通知先を更新しない

通知先サービス名
DEFAULT-TRAP

通知ステータス
UNKNOWN

設定

入力が出来たら、[設定] ボタンを押してください。

図 設定ボタン



「設定を変更し反映しました」と画面に表示されますので、X-MON を再起動してください。

図 設定完了後



確認してみましょう。

サービス一覧の X-MON に「DEFAULT TRAP」が表示されます。

図 default trap

ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
X-MON (X-MON)	DEFAULT-TRAP	保留 (PENDING)	N/A	N/A	1/1	このサービスは チェックするようには スケジュールされて いません。
	PING	正常(OK)	2013-01-17 16:28:16	90日と23時 間05分56秒	1/3	PING OK - Packet loss = 0%, RTA = 0.05 ms

検知するかテストしてみましょう。

前章の任意 SNMP TRAP 通知で使用した「.1.3.6.1.4.1.3.3.3.4」ではなく
「.1.3.6.1.4.1.3.3.3.5」を Linux サーバから TRAP を送信してみます。

```
# snmptrap -v 2c -c public 192.168.19.201 '' .1.3.6.1.4.1.3.3.3.5
```

TRAP を受け取り、UNKnown 状態となります。

図 TRAP を受け取った

ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
X-MON (X-MON)	DEFAULT-TRAP	不明 (UNKNOWN)	2013-01-17 16:34:25	0日と00時間01分02 秒	1/1	(No output returned from plugin)
	PING	正常(OK)	2013-01-17 16:33:16	90日と23時間10分09 秒	1/3	PING OK - Packet loss = 0%, RTA = 0.05 ms

不明 TRAP ログも確認すると、履歴にも記載がされています。

図 不明 TRAP ログ

TRAP履歴?			
TRAPログ 不明TRAPログ			
番号	日付	時刻	
1	2013/01/17 (Thu)	16:34:25	.1.3.6.1.4.1.3.3.3.5

これで X-MON サーバに対して、不明な TRAP が通知されても、すぐに検知する事が
出来るようになります。

3.7.3 通知条件を編集する

[MENU] の [SNMP TRAP 管理] の [非監視 SNMP TRAP 設定] を開きます。

図 非監視 SNMP TRAP 設定

新規に作成するのと同じく、この画面が編集する画面となりますので編集する項目を入力し、[設定] を押して完了し、X-MON を再起動させてください。

3.7.3.1 編集できる項目について（サービス設定からの編集）

SNMP TRAP 管理からは通知条件について編集を行いますが、再通知間隔やステータスによる通知の有無、また通知先グループについては[ホスト管理] の[サービス設定] から編集を行います。

図 サービス設定

登録サービス	エスカレーション設定数	操作	
<input type="checkbox"/> DEFAULT-TRAP	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスカレーション設定

該当のサービスの[詳細表示] を開きます。一番下に[編集]がありますので開きます。

図 詳細表示

サービスの詳細

すべて開く

基本設定

ホストID(英数字)	X-MON
サービスID(英数字)	DEFAULT-TRAP
サービス監視用コマンド	ダミープラグイン(ステータスを任意のものに更新)
通知先グループ	Webチーム
イベントハンドラ	有効にする
イベントハンドラコマンド	無し

監視の詳細設定

通知の詳細設定

フラッピングの設定

高度な設定

戻る 編集

編集画面が開きますので、編集する項目を編集してください。

この際、「サービス監視用コマンド」の部分については SNMP TRAP 管理部分にて動作をさせるための項目ですので編集しないようにお願いします。

編集が完了したら、[編集] もしくは[編集と承認]にて完了させ、X-MON を再起動させてください。

図 編集

サービスの編集

すべて開く

基本設定

ホストID(英数字)
X-MON

サービスID(英数字)
DEFAULT-TRAP

サービス監視用コマンド
DHCPサービス監視
ダミープラグイン(ステータスを任意のものに更新)
ステータス: OK
メッセージ: OK

通知先グループ
Webチーム
↑(選択) ↓(外す)
選択して下さい

イベントハンドラ
有効にする
イベントハンドラコマンド
実行しない

監視の詳細設定
通知の詳細設定
フラッピングの設定
高度な設定

キャンセル 編集 削除と承認

3.7.4 通知条件を削除する

通知条件の削除は[ホスト管理] の[サービス設定]から行います。

該当のホストでサービス設定を開いて一覧を表示させます。

削除するサービスのチェックボックスにチェックを入れて[削除と承認] を押します。

図 サービス設定

X-MON - サービス一覧

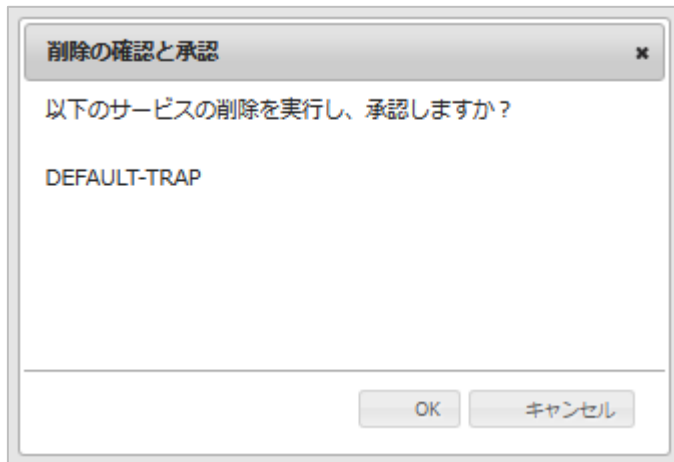
新規作成 削除 削除と承認

登録サービス	エスカレーション設定数	操作
<input checked="" type="checkbox"/> DEFAULT-TRAP	有効: 0, 無効: 0	詳細表示 サービスエスカレーション設定
<input type="checkbox"/> PING	有効: 0, 無効: 0	詳細表示 サービスエスカレーション設定
<input type="checkbox"/> log	有効: 0, 無効: 0	詳細表示 サービスエスカレーション設定

戻る 削除 削除と承認

確認ウィンドウが出ますので、OK でしたら OK を押してください。

図 削除の確認



「設定を削除し反映しました。」と表示されますので X-MON を再起動させて完了してください。

図 削除



以上が通知条件の削除方法となります。

3.7.5 非監視 TRAP の運用使用例

使用例として、下記画像のように「サービスがシャットダウンした」という TRAP が通知されてきたとします。

図 使用例

ホストID (ホスト名称)	サービスID	状態	最終チェック時刻	経過時間	試行回数	ステータス情報
X-MON (X-MON)	DEFAULT-TRAP	不明 (UNKNOWN)	2013-01-17 16:39:41	0日と00時間06分24秒	1/1	DHCPv4 クライアント サービスが停止しました。 シャットダウン フラグの値: 0 LOCAL SERVICE WIN-E7RDU5UADQS 4 4 0
	PING	正常(OK)	2013-01-17 16:38:16	90日と23時間15分31秒	1/3	PING OK - Packet loss = 0%, RTA = 0.05 ms

ステータス情報だけでは、どの IP アドレスが送信元なのかわからないため、[TRAP 履歴] の[不明トラップ]を確認します。

送信元 IP アドレスと、メッセージの内容が記載されていますので、障害や負荷に問題がないか確認し、すぐに対応する事が出来ます。

図 不明 TRAP

受信日時	送信元ホスト
受け取ったOID	
受け取ったメッセージ	
2013年02月27日 16時25分44秒	192.168.19.180
.1.3.6.1.4.1.311.1.13.1.29.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.68.104.99.112.45.67.108.105.101.110.116.0.50037	
[UNKNOWN TRAP] DHCPv4 クライアント サービスが停止しました。シャットダウン フラグの値: 0 LOCAL SERVICE WIN-E7RDU5UA00S 4 4 0	

利点としては MIB 毎に通知設定していなくても通知をしてくれます。
しかし全ての不明 TRAP を通知しますので環境に合わせて使用しましょう。

3.8 サービス設定からの設定について（共通）

SNMP TRAP 管理で設定できる各 TRAP の項目でも解説していますが、通知条件を作成し、ホストのサービス設定から設定する項目で重要な点について記載します。

3.8.1 通知先を編集する

メールの通知先については通知条件を新規作成する際に設定出来ますが、通知先を追加、削除する等編集したい場合はサービス設定から実施する必要があります。

図 編集

Host ID (Alphanumeric): SW-TRAP

Service ID (Alphanumeric): TRAP

Service Monitoring Command:

- DHCP Service Monitoring
- Fake Login (Update status to any of your choice)
- Status OK
- Message OK

Notification Group:

- Webチーム
- ↑(選択)
- ↓(外す)
- 選択して下さい

3.8.1.1 複数ホストを対象にしている場合

TRAP の対象ホストを複数設定している場合、サービス設定で通知先を編集すると編

集した該当のホストの通知先のみ編集されます。

例) snmp-trap-test を Linux-TRAP,SW-TRAP にホストを対象ホストとして設定。

通知先を web チームとする。

図 作成

この通知条件で設定する Linux-TRAP,SW-TRAP に通知条件（監視設定）が作成されます。

図 通知条件設定

SW-TRAP (SW-TRAP)	snmp-trap-test	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
Linux-TRAP (Linux-TRAP)	snmp-trap-test	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。

Linux-TRAP のサービス設定で snmp-trap-test の通知先グループを DB チームに変更します。

図 通知先グループの変更

こうすることで、Linux-TRAP の snmp-trap-test の通知先グループは DB チームとなりますが SW-TRAP の snmp-trap-test は通知先は web チームのまま変更はされません。これにより、同じトラップ通知条件でもホストによって通知先を変更する事が可能です。

図 同じ TRAP 設定で通知先グループが違う例

ただし、全ての通知先グループの変更が必要な場合は、設定されているサービス全てを変更する必要があります。

3.8.1.2 対象ホストを変更した際の挙動について

snmp-trap-test02 を Linux-TRAP を対象ホストとして設定。

通知先グループを web チームとする。

図 新規作成

この通知条件で設定する Linux-TRAP に通知条件（監視設定）が作成されます。

図 作成後

Linux-TRAP (Linux-TRAP)	snmp-trap-test02	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするにはスケジュー ルされていません。
----------------------------	------------------	-----------------	-----	-----	-----	-----------------------------------

SNMP TRAP 管理より、通知条件を編集します。編集する内容は対象ホストに SW-TRAP を追加します。これにより、Linux-TRAP,SW-TRAP に通知条件（監視設定）が設定されます。

図 編集

対象TRAP
CISCO-CONFIG-MAN-MIB - ciscoConfigManEvent

条件名
snmp-trap-test02

Data Binding設定(上級者向け)

ccmHistoryEventCommandSource		完全一致 ▼
ccmHistoryEventConfigSource		完全一致 ▼
ccmHistoryEventConfigDestination		完全一致 ▼

対象ホスト

Linux-TRAP
SW-TRAP

↑(選択) ↓(外す)

--- S ---

snmp-win

通知先サービス名
snmp-trap-test02

通知ステータス
☐ OK ☐ WARNING ☒ CRITICAL ☐ UNKNOWN

キャンセル 作成と承認

図 作成後

SW-TRAP (SW-TRAP)	snmp-trap-test02	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするにはスケジュールされていません。
Linux-TRAP (Linux-TRAP)	snmp-trap-test02	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするにはスケジュールされていません。

しかし、追加されたホスト（SW-TRAP）は通知先が設定されません。

図 追加したホストは通知先グループが設定されない（右側）

基本設定

ホストID(英数字)
Linux-TRAP

サービスID(英数字)
snmp-trap-test02

サービス監視用コマンド
タミープラグイン(ステータスを任意のものに更新)

通知先グループ
Webチーム

イベントハンドラ
有効にする

イベントハンドラコマンド
無し

基本設定

ホストID(英数字)
SW-TRAP

サービスID(英数字)
snmp-trap-test02

サービス監視用コマンド
タミープラグイン(ステータスを任意のものに更新)

通知先グループ
無し

イベントハンドラ
有効にする

イベントハンドラコマンド
無し

そのため、サービス設定より通知先を編集する必要がありますので、対象ホストを追加の際はご注意ください。

3.8.2 TRAP を受信するたびに通知を行う (volatile サービスの設定)

X-MON の仕様により、一度ステータスが変化すると、次にステータス変化するか再通知間隔の時間が過ぎるまで通知は実施されません。

そのため、同じ TRAP 名で複数の通知条件を設定している場合に同じステータスのまま違う内容の TRAP を受け取っても、ステータス変化しないために通知が実施されません。

例) 同じ通知先サービス名・ステータスを設定しているが、対象 TRAP が違う

対象TRAP CISCO-CRYPTO-ACCELERATOR-MIB - ciscoCryAccelInserted 条件名 SNMP-v-test Data Binding設定(上級者向け) ccaAccelSlot 指定なし 対象ホスト Linux-TRAP 通知先サービス名 SNMP-v-test 通知ステータス CRITICAL	対象TRAP CISCO-CRYPTO-ACCELERATOR-MIB - ciscoCryAccelRemoved 条件名 SNMP-v-test Data Binding設定(上級者向け) ccaAccelSlot 指定なし 対象ホスト Linux-TRAP 通知先サービス名 SNMP-v-test 通知ステータス CRITICAL
---	--

同じ通知先サービス名なので、作成される通知条件は1つです。

Linux-TRAP (Linux-TRAP) ?	SNMP-v-test P	保留 (PENDING)	N/A	N/A	1/1	このサービスはチェックするようにはスケジュールされていません。
------------------------------	---------------	-----------------	-----	-----	-----	---------------------------------

volatile サービスを設定する事により、同じステータスであっても別の内容の TRAP を受信 (厳密には TRAP を受信するたびに) すると通知を行います。デフォルトではこの機能は無効となっています。

サービス設定の[高度な設定]タブ内に「volatile サービス」がありますので有効にすれば設定は完了です。

図 volatile サービスの設定

▼ 高度な設定

オブセスオーバー機能
 無効にする ▼

volatileサービス
 無効にする ▼

フレッシュネスチェック
 無効にする ▼

3.8.3 アクティブチェックと試行回数の設定について

SNMP TRAP の通知条件では、パッシブチェックを利用し、TRAP を受信したら通知を実施する設定となっています。

そのため、サービス設定のアクティブチェックは無効、試行回数は 1 の設定が通知条件を作成した際に設定されます。

設定項目	設定値	目的
アクティブチェック	無効にする	SNMP TRAP 監視は待ち受ける監視のため。
試行回数	1	TRAP を 1 件受信したら即座にハードステータスとなり、メール等の通知が実施されます。

図 詳細

▼ 監視の詳細設定

アクティブチェック
無効にする ▼

パッシブチェック
有効にする ▼

監視時間帯
24時間365日 ▼

試行回数
1

監視間隔(分)
5

再試行間隔(分)
1

並びに、パッシブチェックも有効となっています。

SNMP TRAP を受信する際は上記内容は変更しないようにお願いします。