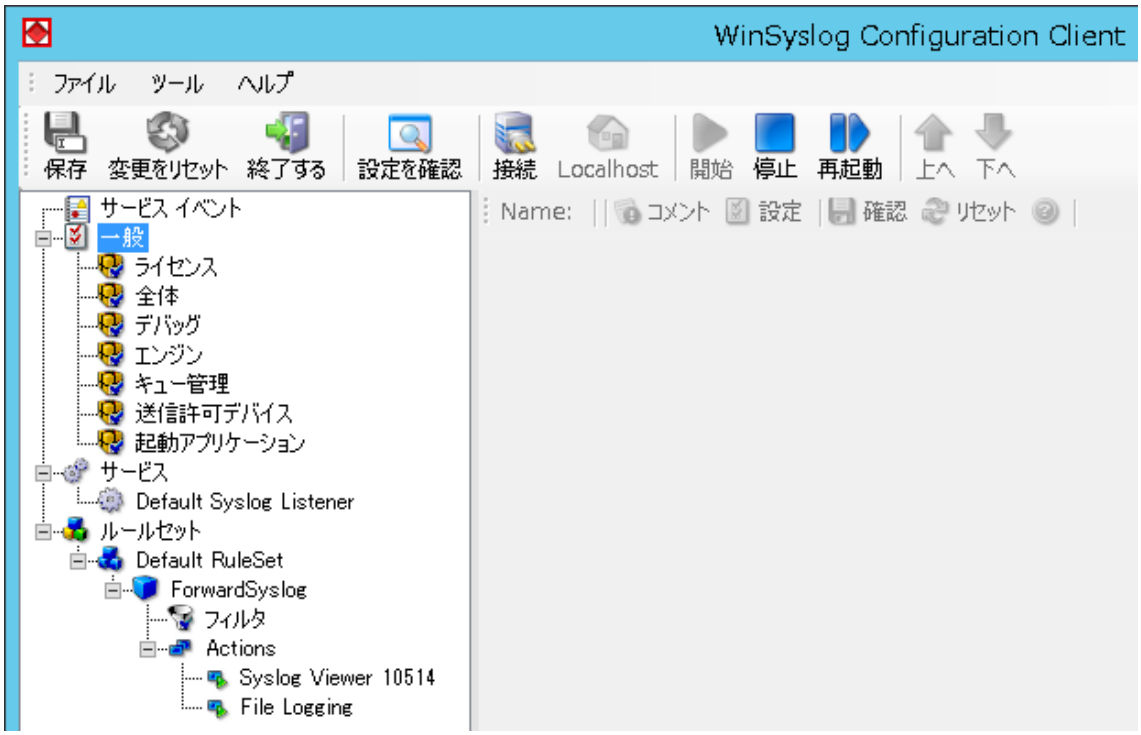
2017 年 7 月 3 日

SNMP トラップ受信と MIB 変換

SNMP トラップを受信し、メッセージ内の MIB 情報を変換する方法を説明します。

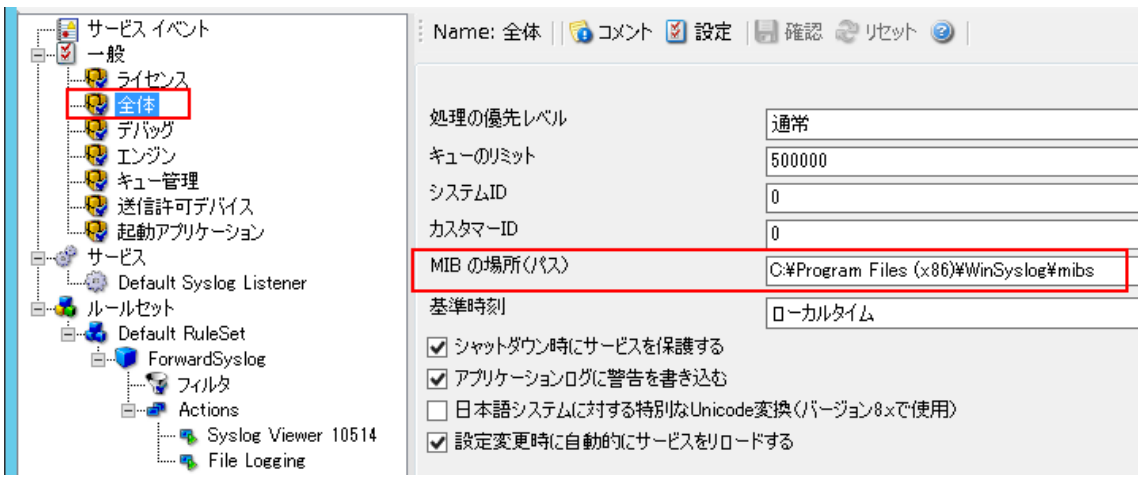
1　SNMP トラップ受信

1. WinSyslog Configuration Client を起動します。



デフォルトでは、左ペインのツリーには、上記のサービスとルールセットが設定されています。

2. ツリーから、「一般」>「全体」を選択します。ここで MIB データの場所を指定します。



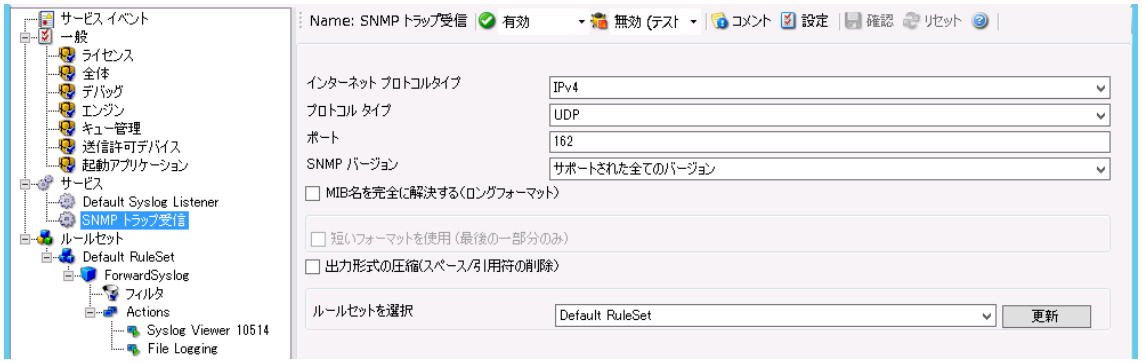
MIB の場所（パス）

MIB データの場所を指定します。「参照」ボタンを押下し、ブラウザより MIB ファイルを選択するか、MIB ファイルが入るフォルダを指定の場合は、パスを指定してください。

デフォルト値は、C:¥Program Files (x86)¥WinSyslog¥mibs です。

3. 左ペインの「サービス」上で右クリック、「サービスを作成」>「SNMP トラップ受信」>をクリックします。

以下のような右ペインが表示されます。



インターネット プロトコルタイプ

受信する SNMP トラップが IPv4 なのか IPv6 なのかを指定します。

IPv4 と IPv6 のデバイスが混在する場合、「SNMP トラップ受信」サービスを IPv4 用、IPv6 用として分けて作成･設定しなければなりません。

プロトコル タイプ

受信する SNMP トラップのプロトコルを指定します。UDP、TCP のどちらかを選択してください。

ポート

SNMP リスナーが使用するポートを指定します。

デフォルトポートは 162 です。

SNMP バージョン

ここでは、SNMP バージョンを限定します。

設定可能な値は、下記のとおりです。

・サポートされた全てのバージョン

・SNMP バージョン 1 のみ

・SNMP バージョン 2c のみ

□ Mib 名を完全に解決する（ロングフォーマット）

このオプションを有効にすると、「一般」>「全体」> MIB の場所（パス）で指定した MIB データを利用して、Mib 名が解決されます。

出力例：（網掛け表示は「短いフォーマット」ではカットされる部分）

community="private" version="Ver2" variables: snmp_var_1 = 'iso.org.dod.internet.mgmt.mib-2.system.sysUpTime: 'Timeticks: (1974003243) 228 days, 11:20:32.43" , snmp_var_2 = 'iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID: 'OID: CISCO-ERR-DISABLE-MIB::ciscoErrDisableMIB"

□ 短いフォーマットを使用（最後の一部分のみ）

完全な名前解決が長く読みづらい場合には、この機能を有効にしてください。

Mib 名の最後の部分だけになるようフォーマットが変更されます。こちらは新クライアントの機能です。

出力例：

community="private" version="Ver2" variables: snmp_var_1 = 'sysUpTime: 'Timeticks: (1973991754) 228 days, 11:18:37.54" , snmp_var_2 = 'snmpTrapOID: 'OID: CISCO-ERR-DISABLE-MIB::ciscoErrDisableMIB"

□ 出力形式の圧縮（スペース/引用符の削除）

メッセージプロパティの新しい圧縮出力形式が追加されました。

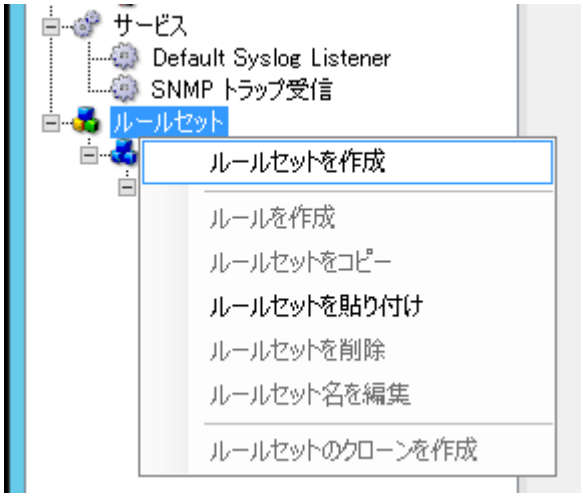
このオプションのチェックで、メッセージ中の “”(ダブルクオーテーション)の削除と、連続した空白の圧縮が有効になります。

□ ルールセットを選択（使用するルールセット）

このサービスのために使用されるルールセット名を選択します。本書では SNMP Trap 用ルールセット作成を次の手順で行い、その後、それを指定します。

4. SNMP Trap 用ルールセットを作成します。左ツリーで「ルールセット」上にカーソルを置き、

右クリック＞「ルールセットを作成」を選択します。



「Add RuleSet」のウィンドウが表示されます。

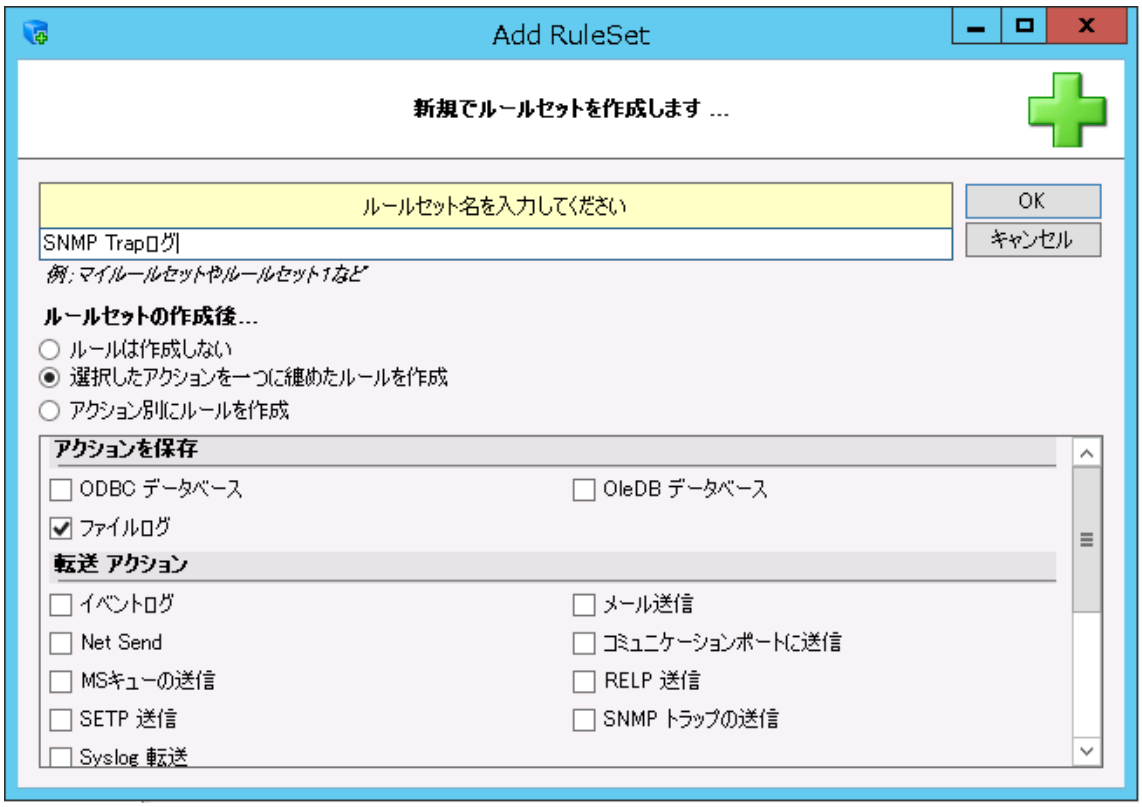
今回は、ルールセット名として、「SNMP Trap ログ」としますが適当な名称を付けてください。

ルールセットの作成後…で

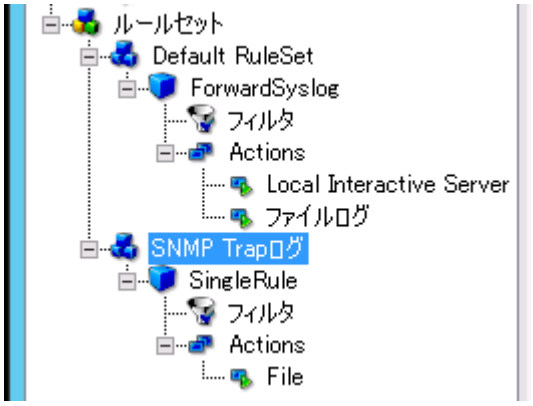
〇選択したアクションを一つに纏めたルールを作成

を選択し、

アクションを保存項目で、「ファイルログ」にチェックを入れて、「OK」を押下します。

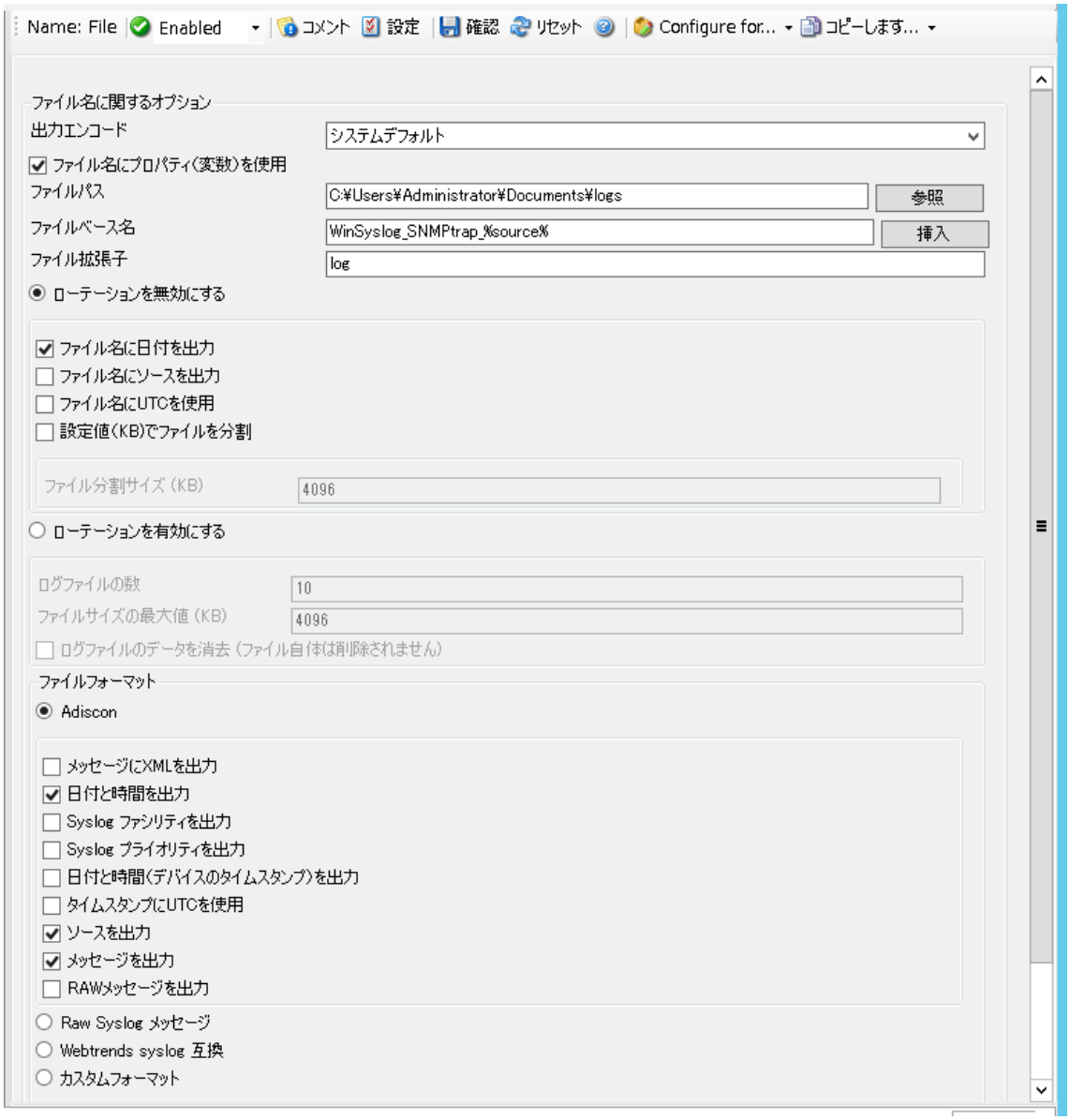


ルールセットとして「SNMP Trap ログ」が追加されますので、ツリーを開き、アクションが追加されていることを確認します。



5. 保存するファイル名を設定します。「SNMP Trap ログ」>「SingleRule」>「Actions」>「File」をクリックし、各パラメータを設定します。

設定の一例:

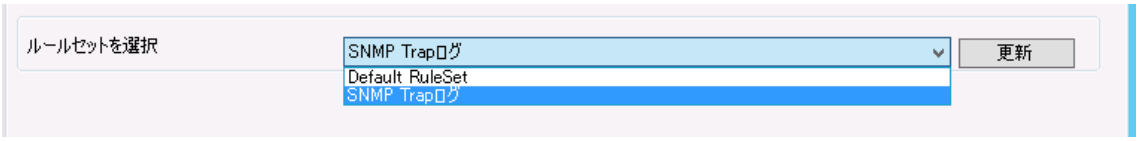


上の画面例では、

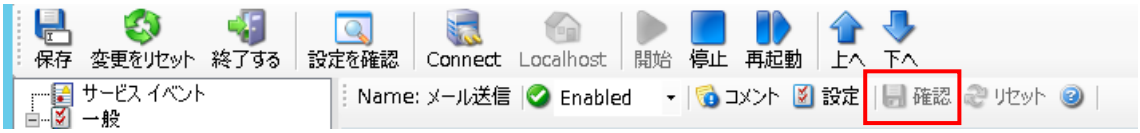
「ファイル名にプロパティ(変数)を使用」を有効とし、送信元(source)別にファイルが作成されるように設定しています。
ファイル名の例:WinSyslog_SNMPtrap_192.168.30.83-2016-06-29.log
また、ファイルへ出力される項目においても、不要な「Syslog ファシリティを出力」などを無効にしています。

アクション「ファイルログ」設定に関しては、『WinSyslog 標準ログサーバー設定』
http://www.jtc-i.co.jp/support/documents/etc/winsyslog_logserver_setting.pdf も参照してください。

6. 「サービス」>「SNMP Trap 受信」を選択し、「ルールセットを選択」のプルダウンから、先ほど作成した「SNMP Trap ログ」を選択し、「更新」ボタンをクリックします。

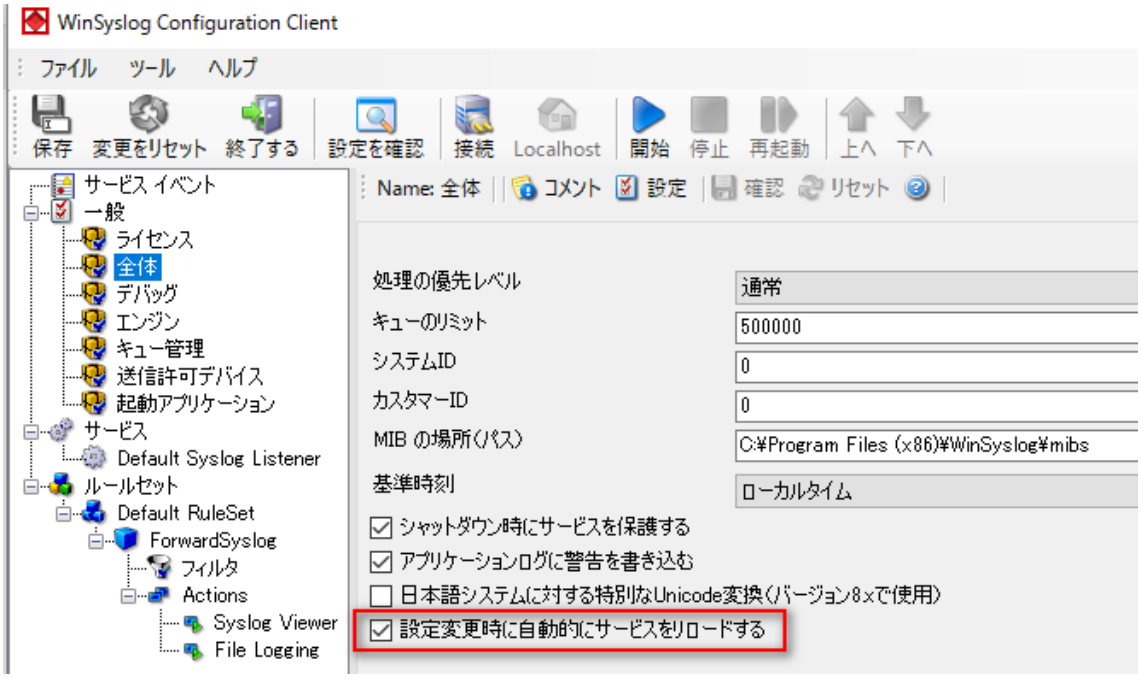


7. 設定した後は、問題がないか「確認」ボタンを押します。問題なければ、以下のようにグレーアウト表示になります。



次に、「保存」アイコンを押下し、設定を保存後、「再起動」アイコンをクリックして、サービスを再起動し、設定を反映させます。

※WinSyslog ver.14.1 以降、「設定変更時に自動的にサービスをリロードする」オプションが追加となりました。
このオプションはデフォルト設定では有効ですので、**設定変更後「保存」ボタンのみで変更が反映されます。**
この機能を無効にしたい場合は、チェックを外してください。



SNMP Trap 受信例:

SNMP Trap OID: 1.3.6.1.4.1.9.9.548 が送信された場合

この OID に関して詳細は↓を参照してください。

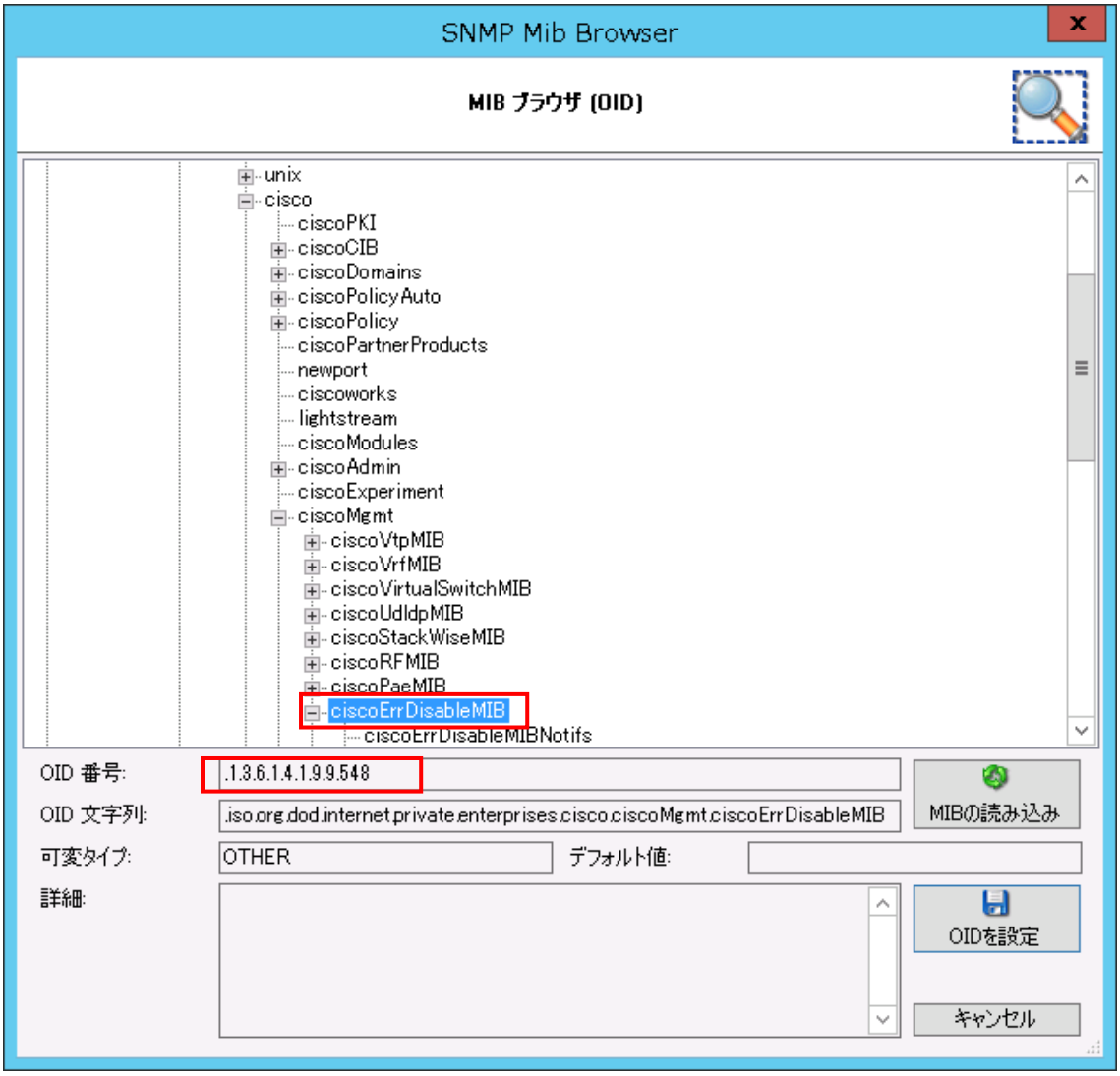
http://www.oidview.com/mibs/9/CISCO-ERR-DISABLE-MIB.html

WinSyslog 出力例(メッセージ部分):

community="private" version="Ver2" variables: snmp_var_1 = 'iso.org.dod.internet.mgmt.mib-2.system.sysUpTime: 'Timeticks: (1973372913) 228 days, 9:35:29.13" , snmp_var_2 = 'iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID: 'OID: CISCO-ERR-DISABLE-MIB::ciscoErrDisableMIB"

参考:SNMP Mib Browser MIB ブラウザ(OID) での「ciscoErrDisableMIB」の表示

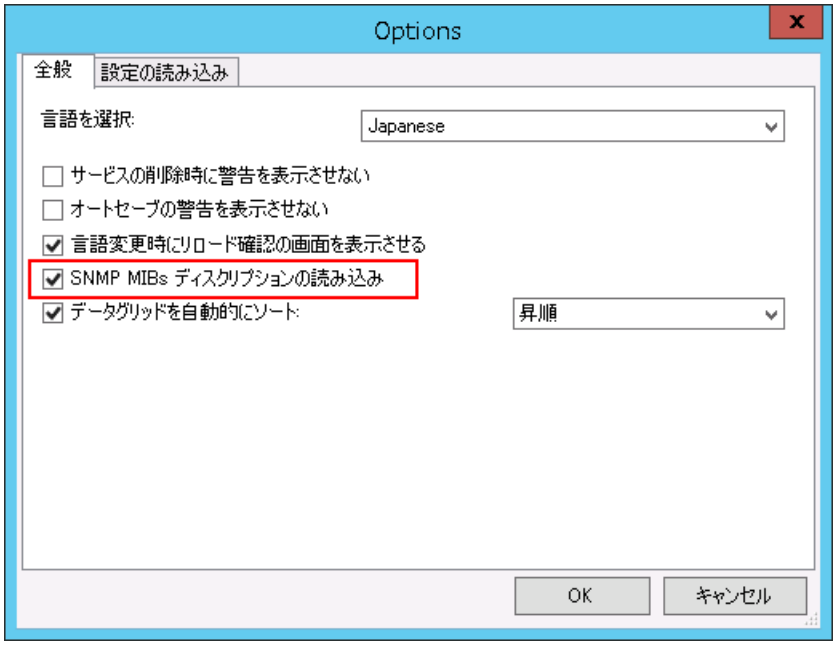
(「SNMP Mib Browser MIB ブラウザ(OID)」へのアクセス方法は、こちらをご参照ください。


SNMP Mib Browser
MIB ブラウザ (OID)
unix
cisco
ciscoPKI
ciscoCIB
ciscoDomains
ciscoPolicyAuto
ciscoPolicy
ciscoPartnerProducts
newport
ciscoworks
lightstream
ciscoModules
ciscoAdmin
ciscoExperiment
ciscoMgmt
ciscoVtpMIB
ciscoVrfMIB
ciscoVirtualSwitchMIB
ciscoUdldpMIB
ciscoStackWiseMIB
ciscoRFMIB
ciscoPaeMIB
ciscoErrDisableMIB
ciscoErrDisableMIBNotifs
OID 番号:
.1.3.6.1.4.1.9.9.548
OID 文字列:
.iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoErrDisableMIB
MIBの読み込み
可変タイプ:
OTHER
デフォルト値:
詳細:
OIDを設定
キャンセル

参考情報:

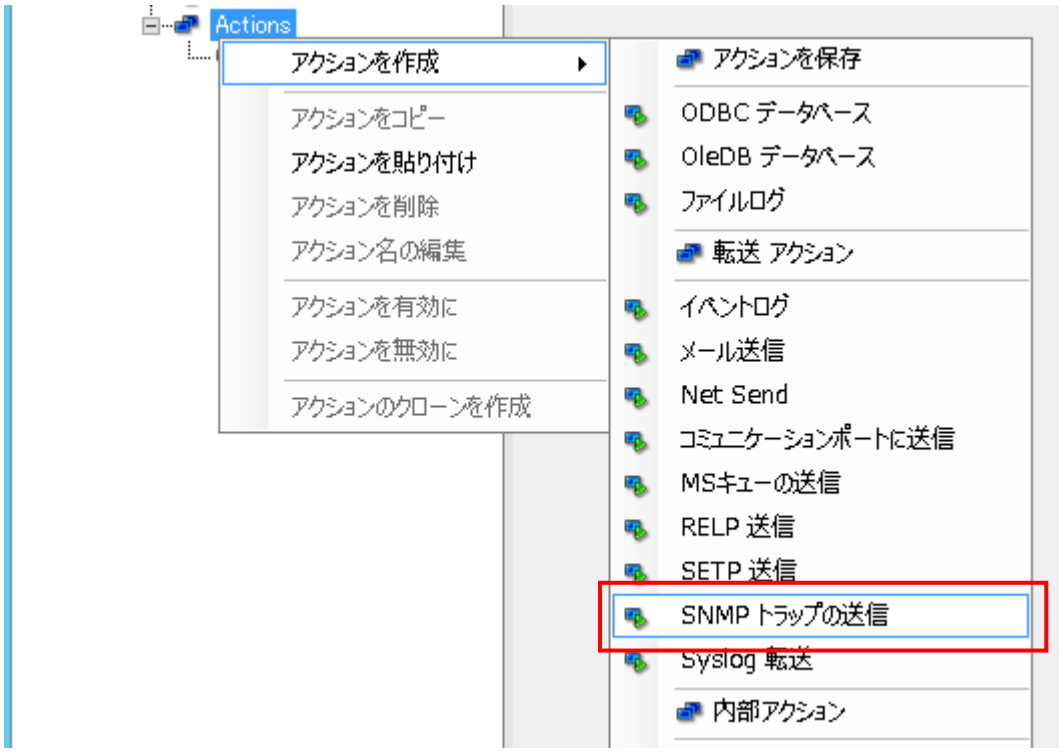
WinSyslog には、SNMP Mib Browser「MIB ブラウザ(OID)」があります。
アクセス方法を紹介します。

1. ファイル>オプションを選択し、「全般」タブで、
   ☐ SNMP Mibs ディスクリプションの読み込み
   にチェックします。



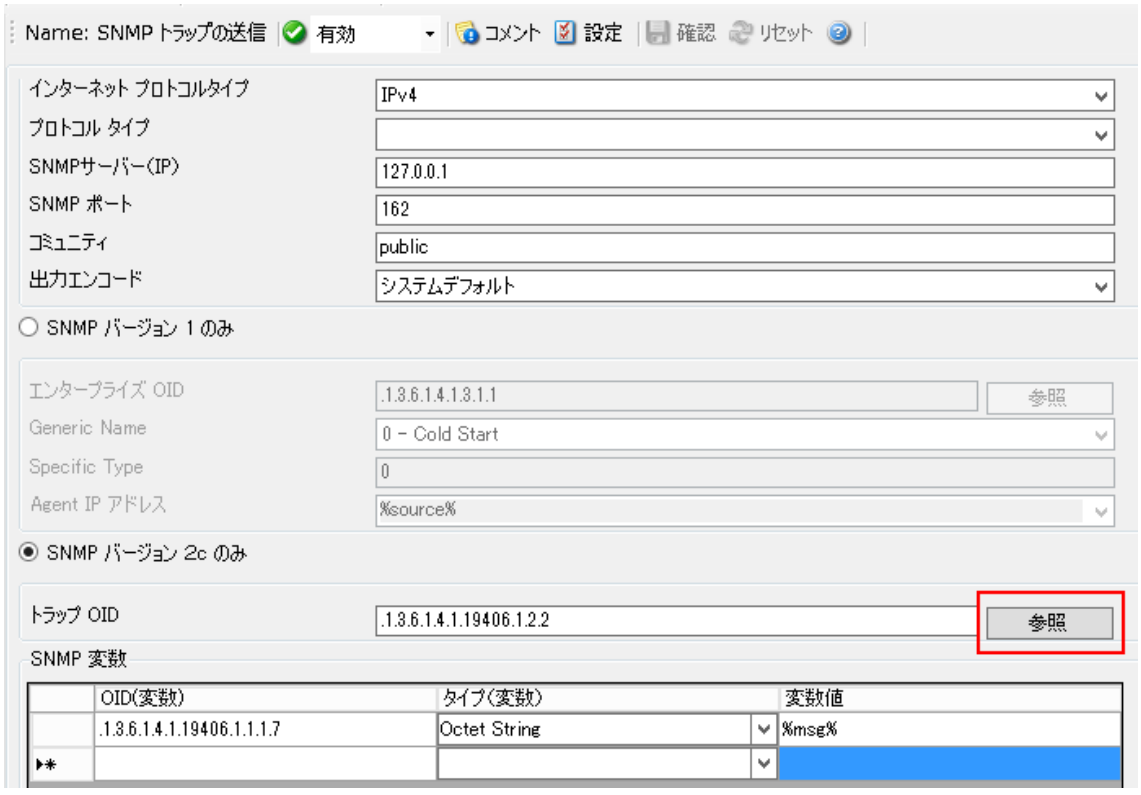
このオプションを有効にすると、クライアント(WinSyslog Configuration Client)を開いたとき MIB データが直ちにロードされます。
無効の場合、「MIB ブラウザ(OID)」を開く時に MIB データがロードされるため、遅延を感じることになります。

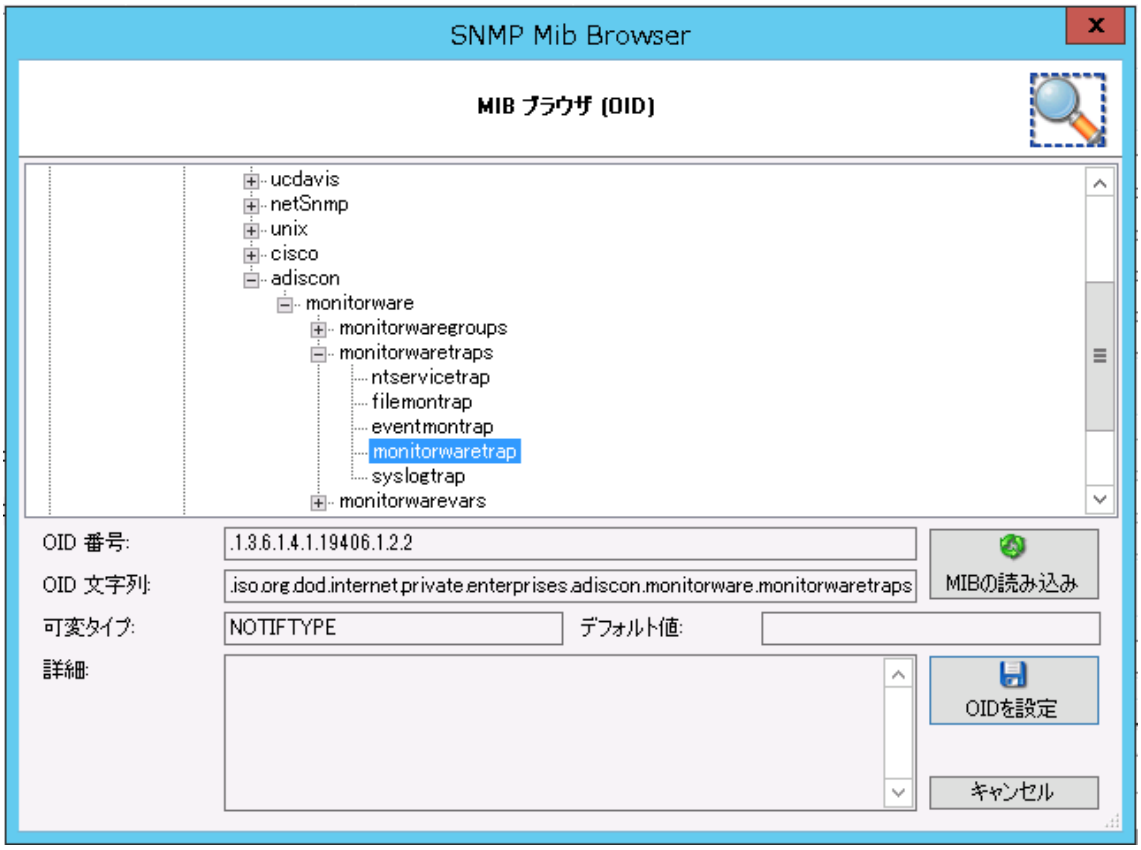
2. 「MIB ブラウザ(OID)」は、アクション「SNMP トラップの送信」の設定内からアクセスできます。
   ルールの Actions 上にカーソルを置き、右クリック>「アクションの追加」>「SNMP トラップの送信」を選択します。



アクション「SNMP トラップの送信」の右ペインは以下がデフォルト設定です。

「参照」ボタンのクリックで、SNMP Mib Browser「MIB ブラウザ(OID)」が開きます。




SNMP Mib Browser
MIB ブラウザ (OID)
ucdavis
netSnmp
unix
cisco
adiscon
monitorware
monitorwaregroups
monitorwaretraps
ntservicetrap
filemontrap
eventmontrap
monitorwaretrap
syslogtrap
monitorwarevars
OID 番号:
.1.3.6.1.4.1.19406.1.2.2
OID 文字列:
.iso.org.dod.internet.private.enterprises.adiscon.monitorware.monitorwaretraps
MIBの読み込み
可変タイプ:
NOTIFTYPE
デフォルト値:
詳細:
OIDを設定
キャンセル

以上