WinSyslog v.15
ユーザーマニュアル

Rev.1.2

2018.10.05

ジュピターテクノロジー

目次

Adiscon WinSyslog は以下のサードパーティツールを使用しています。

Openssl-1.0.2k:	http://www.adiscon.org/3rdparty/openssl-1.0.2k.tar.gz
Net-SNMP-5.7.3:	http://www.adiscon.org/3rdparty/net-snmp-5.7.3.tar.gz
Liblogging:	http://www.adiscon.org/3rdparty/liblogging.zip
VB6 NeoCaption:	http://www.adiscon.org/3rdparty/VB6_NeoCaption_Full_Source.zip
Librelp-1.2.11:	http://download.rsyslog.com/librelp/librelp-1.2.11.tar.gz
Openssl-1.0.2k:	http://www.adiscon.org/3rdparty/openssl-1.0.2k.tar.gz

更新履歴

このドキュメントの更新履歴は以下の通りです。

版	発行日	更新内容
第 1.0 版	2018/07/06	新規作成（Ver.15）
第 1.1 版	2018/09/13	改訂
第 1.2 版	2018/10/05	改訂（Ver.15.1 対応）

この資料について

- この資料は WinSyslog マニュアル（Adiscon GmbH 社）を日本語翻訳したものですが、オリジナルの内容を一部省略・変更しています。
- v14.1 より、弊社ソフトウェアダウンロードページからダウンロードしていただける WinSyslog プログラムは日本国内ユーザー向けの初期設定となりました。この資料では日本仕様の WinSyslog について説明します。
- 設定クライアントに関する説明には、v13.1 で実装された新しいユーザーインターフェイス（表示言語は「日本語」を選択）を使用します。
- WinSyslog を単独で利用する場合は使用しない機能（EventReporter や MonitorWare など Adiscon 社の別製品と連携利用する場合のみ有効な機能）についての説明も含まれます。

1. WinSyslog とは

1.1. 概要

WinSyslog は、Windows 上で稼動する Syslog サーバーです。
（Unix の Syslog デーモンと同じ役目を果たします。）

ネットワーク管理において WinSyslog をご使用頂けば、継続的にシステムを監視することができます。さらに、重要なイベントが発生した場合には、即座に通知を受け取るようにも設定できます。

Syslog は、システムイベントの集中レポート作成のための標準プロトコルです。そのルーツは UNIX 環境にありますが、例えば、Cisco ルーターなどのデバイスも Syslog プロトコルを使用しています。これらのデバイスは、重要なイベントや動作パラメーター、デバッグメッセージでさえ Syslog でレポートします。残念ながら Microsoft Windows は Syslog サーバーを含んでいません。（Syslog サーバーは「Syslog デーモン」や「Syslogd」などとも呼ばれます。）

Adiscon の WinSyslog はこのギャップを埋めるものです。バージョン 3.0 以前、WinSyslog は「NTSLog」の名で知られていました。WinSyslog は Windows プラットフォームで利用可能になった最初のオリジナル Syslog サーバーです。最初のバージョンは、Cisco ルーターのステータスメッセージを受け取るために 1996 年に作成されました。製品は、これまで継続的に開発されています。この製品は、バージョン 3 で飛躍的に機能性が高まりました。それがバージョン 3 で製品名を変えるきっかけとなりました。

また WinSyslog は、Adiscon 製品の MonitorWare エージェント、EventReporter、ActiveLogger とともに、Windows のイベントログをトータルに集中監視するツールとして使うこともできます。（弊社では WinSyslog と EventReporter の販売とサポートサービスを提供しております。その他の Adiscon 製品については https://www.adiscon.com/products/（英語）で詳細を確認できます。）

ほとんどのユーザーは Syslog 有効デバイス（例： ルーター、スイッチ、ファイアーウォールやプリンターなど）から発生したイベントログを集め、それらを持続的に Windows のシステムに保存することなどに WinSyslog を利用しています。WinSyslog は、インタラクティブにスクリーン上で Syslog メッセージを表示することができるだけでなく、さらに収集した Syslog メッセージをフラットな ASCII ファイル、ODBC データベース、または Windows イベントログに保存することもできます。この製品は、はじめに設定を行えば、信頼できるバックグラウンドサービスとして動作し、オペレーターの操作は必要ありません。サービスは、Windows の起動時に自動的に起動することができます。

バージョン 4 で改良されたサービス、ルールによって、WinSyslog の設定はより融通性の高いものになりました。WinSyslog は、受信メッセージ内の文字列照合などで状態を発見したり、それに従って能動的に動作を行ったりすることが可能です。例えば、優先順位の高いメッセージを発見した場合に、E メールメッセージを送信す

るなどが可能です。複数の Syslog サーバーはそれぞれ異なるポートをリスンすることで同時に動作することができます。

1.2. 特長と機能

ここでは WinSyslog の特長と主な機能を紹介します。

ログの集中管理

これは WinSyslog のキーとなる機能です。WinSyslog は、それぞれのソース（送信元）から送られた全ての Syslog メッセージをまとめて、ローカルの Windows システムに保存します。デバイスが Syslog に対応していれば、WinSyslog でそれらを処理できます。今日においては、事実上、すべてのデバイスで Syslog を使うことができます。顕著な実例として、Cisco ルーターが挙げられます。

使い易さ

WinSyslog 設定クライアントにより、セットアップやカスタマイズが容易に行えます。さらに、大規模な環境で利用できる GUI を利用しないインストール方法もサポートされます。

効果的なアクション

受信した各メッセージは、WinSyslog の効果的で柔軟性の高いルールエンジンによって処理されます。各ルールでは、メッセージがルールの「フィルタの条件」に一致したときに、どのアクションが実行されるのかを設定します（例えば、E メールでメッセージを送信するのか、データベースに保存するのかなど）。「フィルタの条件」では、メッセージ内の文字列や Syslog ファシリティ、プライオリティなど、お客様のニーズに合わせた条件設定が可能となっており、不要なメッセージの絞込みが容易に行えます。なお、ルールで利用できるフィルタの条件とアクションの数には制限がありません。

インタラクティブ Syslog ビューア

受信したメッセージをインタラクティブに表示したい場合は、インタラクティブ Syslog ビューア（インタラクティブ Syslog サーバーの後継ツール）を使用します。日本語メッセージも処理できます。メッセージバッファサイズは変更可能です。

Syslog テストメッセージの送信

WinSyslog 設定クライアントには、「Syslog テストメッセージを送信」機能が実装されています（ツールメニュー内にあります）。このオプションにより、ルールセットの設定を確認したり、インタラクティブ Syslog ビューアへ送信テストを行なったりすることができます。ただし、このオプションによるメッセージ送信に利用できるプロトコルは、UDP のみです。（RFC 3195、TCP 送信には対応していません。）

トライアル版とフリー版

WinSyslog とインタラクティブ Syslog ビューアは、セットアップ後 30 日間は試用モードとして全ての機能を送信元デバイス数の制限なく、ご利用になれます。

30 日間の試用期間が終了すると、WinSyslog は以下のようになります:

- **v13.3（日本仕様 BasicFree 版）以降のバージョンの場合**

  WInSyslog: フリー版（送信元 IP 最大 3 台、Basic 機能に制限）に移行します。
  インタラクティブ Syslog ビューア: 送信元 IP 最大 3 台まで表示可能

- **v13.2 以前のバージョンの場合:**

  WInSyslog: サービスが開始できなくなります。
  インタラクティブ Syslog ビューア: 閲覧開始 5 分後に停止するようになります。

Syslog サーバーサービスやその他の拡張機能を送信元 IP 4 台以上でご利用になりたい場合は、ライセンスをご購入頂く必要があります。ライセンスを適用すると正規版として動作します（ソフトウェアの再インストールは必要ありません）。

標準の互換性

WinSyslog は、Syslog RFC3164、RFC5424 に対応しています。送信者（デバイス）やサーバーや中継マシン（リレーサーバー）として稼動します。全ての仕様のオペレーションモードがサポートされます。
RFC に対応していない部分は、ローカルの環境に合うように管理者が設定することが可能です。（例えば、デバイス時計が信頼できない場合に、報告しているデバイスの代わりにローカルシステムからタイムスタンプを取り出すことができます。）

Syslog 階層

WinSyslog は大きな組織で必要となるカスケードされた設定をサポートします。カスケード設定には、重要なイベントを本部の中心となる WinSyslog に報告する、部やサイトレベルで動作するローカルの WinSyslog が例としてあげられます。カスケードされたシステムには、レベル数に対する制限はありません。

E メールでの通知

ユーザーが設定したルールセットに基づいて、受信した Syslog メッセージを E メールで送ることができます。この E メールによる通知は、どんな E メールアドレスにも送る事ができます（携帯電話でも受信できます）。
また、E メールの件名は完全にカスタマイズすることができます。オリジナルのメッセージを本文内に含むように設定する事もできます。従って、携帯電話であっても十分に情報を受信する事ができます。

継続的メッセージの保存

WinSyslog の Syslog サーバーは、継続して全てのメッセージを保存することができます。したがって、後の監査や重要なシステムイベントの再調査などを容易に行うことができます。メッセージは、フラットな ASCII ファイル、ODBC データソース、Windows イベントログなどに書くことができます。

複数のインスタンス

WinSyslog は、同じマシン上で複数の Syslog サーバーサービスを稼動させることができます。それぞれが異なる Syslog ポートを使用し、TCP または UDP を選択できます。そして、異なるルールセットを作成できます。同じ設定内容（ポート・プロトコル）の Syslog サーバーサービスを複数稼動させることはできません。

完全なログ収集

WinSyslog は、受信した Syslog メッセージに加え、送信側システムの IP アドレスや日付だけでなく、そのプライオリティやファシリティコードをも記録します。さらに正常にフォーマットされていないパッケージ（無効なプライオリティ/ファシリティがある、またはそれら自体ない）を記録することができるので、メッセージは消失しません。

安定性

WinSyslog は、正常でない環境のもとでも実行できるように作成されています。その信頼性は、1996 年以降、顧客サイトで証明されています。

最小限のリソース使用

WinSyslog には、システムリソースへの顕著な影響がありません。それは、最小限のリソース使用ということを念頭において、作成されたからです。これは、負荷の大きなサーバーに対してもインストールできるということを保証しています。

ファイアーウォールサポート

セキュリティポリシーなどにより、標準でない Syslog ポートを使う必要にせまられた場合でも、WinSyslog は、Syslog メッセージに対して、いかなる TCP/IP ポートでも使用できるように設定できます。

Windows サービス

WinSyslog サービスは、マルチスレッドな Windows サービスとして実行されます。それは、コントロールパネルやコンピューターの管理 MMC (Windows 2000)で制御できます。

IPv6

ネットワークに関連のある全てのサービスやアクションで IPv6 を利用できます。IPv6 のアドレスが有効ならば、DNS 名前解決も可能です。「Syslog サーバー」サービスなど、IP アドレスを設定する項目では、IPv4 または IPv6 を選択することができます。

IPv4 と IPv6 が混在する環境では、その IP タイプ別にサービスを設定する必要があります。(RELP サービスだけは、IP タイプが自動検知されますので、サービスを分けて設定する必要はありません。)

Windows 2000, 2003, 2008, 2012, 2016, XP, Vista, 7, 8, 8.1, 10 完全対応

WinSyslog は、Windows 2000、2003、2008、2012、2016、XP、Vista、7、8、8.1、10 に完全対応しています(R2 含む)。

多言語対応クライアント

WinSyslog クライアントは、多言語に対応しています。新クライアント(v13.1 以降)は、英語、ドイツ語、日本語を選択できます。言語は、すぐに切り替えることができ、ユーザー自身が自由に選択できます。

分かりやすく使いやすいユーザーインターフェイス

クローンの機能が追加されました。クリックするだけで、ルールセット、ルール、アクション、サービスそれぞれのクローンを作成できます。

「上へ」、「下へ」の機能がアクションで使用できるようになりました。ドラッグ &ドロップでの移動もできます。また、アクション、サービス、ルールセット作成のウィザードが改良されました。

低メモリ(メモリ不足)への対応

WinSyslog は、起動時に非常用のメモリを割り当てます。システムのメモリ制限に達した場合、非常用のメモリが解除され、キューはロックされます。これにより、それ以上どんな項目もキューに入れられなくなります。結果として、サービスの停止(crash)を防ぐことができるようになります。

注記:
Windows 2000 と他の EOL オペレーティングシステムは、一部のみ有効です。最小限のサービスインストールに限り可能です。

1.3. 構成要素（コンポーネント）

ここでは、WinSyslog の構成要素（コンポーネント）について説明します。

1.3.1. 中核要素（コアコンポーネント）

WinSyslog 設定クライアント

WinSyslog 設定クライアント（「クライアント」と呼ばれます）は、WinSyslog サービスの全ての要素と機能の設定に使用されます。また、多数のマシンで同じ設定で WinSyslog を使用したい場合など、ベースシステム上のクライアントで設定ファイルを作成、エクスポートし、対象システムに組み込むこともできます。

WinSyslog サービス

WinSyslog サービス（「サービス」と呼ばれます）は、Windows サービスとして稼動し、実際の処理を実行します。

WinSyslog を動作させるためには、サービスがインストールされていなければなりません。WinSyslog サービスは、製品の「エンジン」と呼ばれています。したがって、サービスのみインストールされたシステムを「エンジンだけの」インストールと呼びます。

サービスは、ユーザーの操作の必要なしにバックグラウンドで動作します。これは、コントロールパネルやコンピューターの管理-MMC（Windows 2000 または XP）で制御できます。クライアントからもサービスを制御することができます。

x64 対応バージョンの組み込み

インストーラーは 32bit および 64bit 版で利用できます。セットアップ時にお使いのオペレーティングシステムに合うバージョンが自動的に決定されてインストールされます。x64 プラットフォーム用の主な互換性に関する変更点は、サービスコアの部分です。詳しくは以下のとおりです：

- **「ODBC データベース」アクションが x64 システム上で動作するようになりました。**
  但し、各データベースの ODBC 接続 32bit 版ドライバーのインストールが必要です。
- **設定情報（レジストリ）の保存に関して、DWORD 値が QWORD 値としてレジストリに保存されるようになりました。**
  但し、設定クライアントと Win32 バージョンのサービスではこれらのデータタイプを処理でき、必要に応じて自動的に値が DWORD 値に変換されます。設定クライアントは win32 アプリケーションのままです。サービスのみが x64 プラットフォーム対応になりました。

WinSyslog win32 版から x64 版へのクロスアップデートについての注意事項

通常のセットアップ更新手順で直接 32bit 版 OS から 64bit 版 OS へアップグレードできません。この問題はマイナーアップグレードにより、必要なすべての x64 コンポーネントがインストールされないことです。クロスアップデートのためには、フルインストールの実施が必要です。以下の手順に従ってください:

1. レジストリまたは xml ファイルとして設定ファイルをバックアップします。(設定クライアントのコンピュータメニューをご確認ください)
2. WinSyslog をアンインストールします。
3. WinSyslog をインストールします。
4. レジストリまたは xml ファイルから旧設定をインポートします。

1.3.2. アドオン構成要素

インタラクティブ Syslog ビューア

インタラクティブ Syslog ビューアは、Syslog イベントを受信し、リアルタイムに表示する Windows GUI アプリケーションです。一般的には WinSyslog や EventReporter とともに使用されます。しかし、独立した Syslog サーバーとしても使用することができます。インタラクティブ Syslog ビューアは、インタラクティブ Syslog サーバーの後継ツールです。

インタラクティブ Syslog ビューアでは、日本語文字列を含むメッセージの処理も可能です。また、WinSyslog や EventReporter で作成したデータベースの内容を読み込み、確認することもできます。但し、各データベースの ODBC 接続 32bit 版 Driver のインストールが必要です。

> **注記:**
> インタラクティブ Syslog ビューアは WinSyslog で受信した Syslog をリアルタイムに閲覧することはできますが、保存された大量のログメッセージを閲覧する目的で開発されたものではありません(ログ受信確認用の簡易(補助)ツールです)。本番稼働環境での大量ログデータを閲覧、検索するためには、別の検索・閲覧用ツールをご利用いただくことをお勧めいたします。

Adiscon LogAnalyzer (旧 PhPLogCon)

Adiscon LogAnalyzer は、収集されたメッセージを Web 上に表示できる便利な機能を持っています。このツールは、たいていのブラウザに対応しています。

Adiscon LogAnalyzer は、Syslog メッセージ、Windows イベントログデータ、その他のネットワークイベントを簡単に Web で閲覧することができます。このツールを使用することにより、システム管理者は、迅速かつ容易にログをチェックすることが可能となります。

Adiscon LogAnalyzer は、WinSyslog のインストールフォルダに含まれています。詳細については、http://loganalyzer.adiscon.com/doc/または「(プログラムインストールフォルダ)¥loganalyzer¥doc」フォルダ配下の英語マニュアルをご参照下さい。

> **注記:**
> LogAnalyzer はサポート対象外のフリーツールです(無償でご利用いただけますが、サポートはありません)。ご利用いただく場合は、ご自身の責任においてご利用ください。別途 IIS や Apache などの WebServer、PHP、データベースを構築する必要があります。

MonitorWare コンソール

MonitorWare コンソールは、ネットワークから役に立つ情報を容易に集めることができ、また、その集めた情報に対して、セキュリティ違反を含む無数の問題を調査することが可能です。MonitorWare コンソールの表示、レポートモジュールを使用することで、能率的に問題を含む範囲をネットワーク上で検出することができます。

> **メモ**: MonitorWare は Adiscon 社の製品ですが弊社での取り扱いはありません。

1.3.3. これらの構成要素を共に動作させるには

ここでは、上述の構成要素(コンポーネント)がどのように動作するかについて説明します。

これらの構成要素を共に動作させるには

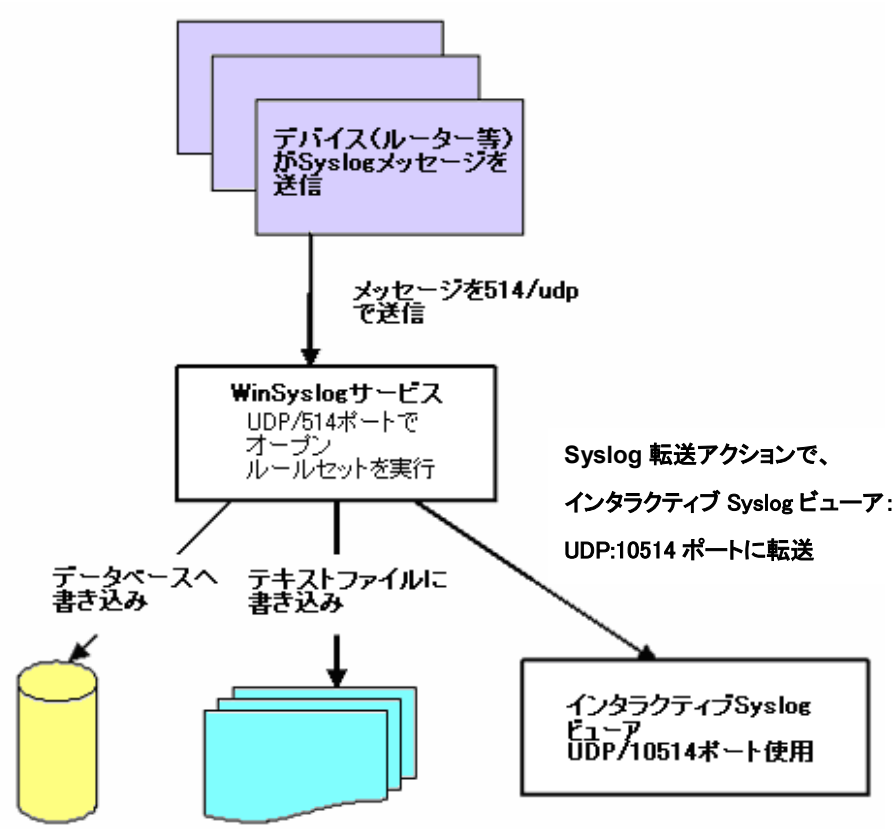
WinSyslog サービス、設定クライアント、インタラクティブ Syslog ビューア、Adiscon LogAnalyzer の 4 つの構成要素は、共に密接に動作します。中核は WinSyslog サービスです。これは継続的にバックグラウンドで動作しています。WinSyslog 設定クライアントはサービスの設定を行うために使用し、WinSyslog の設定完了後は、継続して起動させておく必要はありません。

一度サービスの設定を行えば、サービスはバックグラウンドで動作し、設定のとおり実行されます。最も重要な処理として、Syslog メッセージの受信や、ルールベースによるそれらのメッセージの処理、それらをデータベースやテキストファイルに保存すること、アラートを出すことなどがあります。

WinSyslog サービス自体には、インタラクティブな(収集したログメッセージを表示する)構成要素はありません。Syslog メッセージを Windows GUI で表示するには、インタラクティブ Syslog ビューアが必要となります。インタラクティブ Syslog ビューアは軽量な Syslog サーバーとして実装されています。それ自体は機能が制限された完全な Syslog サーバーですが、メッセージをインタラクティブに表示することができます。

インタラクティブ Syslog ビューアは、起動時のみ処理を実行します。WinSyslog で受信した Syslog メッセージをインタラクティブ Syslog ビューアで表示させるために、WinSyslog サービスはメッセージをインタラクティブ Syslog ビューアへ転送します。デフォルトでは、標準ポートでない UDP 10514 ポートで処理されます。従って、WinSyslog サービス、およびインタラクティブ Syslog サーバーは、ポートの衝突なしに同一のマシン上で稼動します。

メッセージの流れについては、下図を参照して下さい:



典型的な設定では、ルーターやスイッチなどの Syslog デバイスは、WinSyslog サービスへ 514 ポートを使用して Syslog メッセージを送信します。サービスは、メッセージを受信し、ルールセットでの設定に基づき、それらを処理します。上図の例では、受信した全てのメッセージに対して、データベースへの書き込み、テキストファイルへの書き込み、インタラクティブ Syslog ビューアへの転送の 3 つのアクションが設定されています。

デフォルトでは、メッセージは 10514 ポートを使用して、ローカル(127.0.0.1)のインタラクティブ Syslog ビューアへ転送されます。インタラクティブ Syslog ビューアは、ポートを開き、サーバーから転送された Syslog メッセージを受け取ります。

UNIX-用語では、WinSyslog Service は Syslog リレーと同様に受信機としての機能を果たします。一方、インタラクティブ Syslog ビューアは、ただの受信機としての機能のみで、中継の機能はありません。

実際はカスケードされた Syslog サーバーの設定がここではなされています。インタラクティブ Syslog ビューアは、その機能を可能にする Syslog プロトコルに対して共通の機能拡張が守られるので、メッセージソースとして、オリジナルのメッセージアドレスを表示することが可能です。

WinSyslog 設定クライアントは、サービスの設定を行う際にだけ必要とされます。一旦その設定がなされると、クライアントは使用する必要がなく、メッセージの処理には必要ありません。

Adiscon LogAnalyzer は Web を介して Syslog メッセージにアクセスする必要がある場合にのみ必要です。主要なブラウザはすべてサポートされています。LogAnalyzer は WinSyslog のインストールセットに含まれておりマシンにコピーされますが、インストールはされません。
詳しくは、http://loganalyzer.adiscon.com/doc/manual.html をご参照ください。

> **注記：** LogAnalyzer は無償で使用できますが、サポートの対象外です。

上図の設定は、WinSyslog 構成要素がどのように相互に機能するかを示すためのものであり、あくまでサンプルです。WinSyslog にはこれら以外にも多数の設定が可能です。

1.4. システム要件

ここでは WinSyslog の最小システム要件について説明します。実際の最小システム要件はインストールタイプによって異なります。設定クライアントをインストールする場合は必要な要件が高くなります。サービスの要件は最小限であるため、多種多様なマシン上で実行することができます。

> **注記：** 以下のシステム要件はメーカーのマニュアル通りの記述ですが、弊社 JTC としては CPU4 コア、メモリ 8GB 以上を備えたサーバーPC での運用を推奨いたします。

WinSyslog 設定クライアント/インタラクティブ Syslog ビューア

WinSyslog 設定クライアントは、以下の環境でご利用いただけます：

OS	Windows 2000 SP3 以降のシステム （Windows XP, Windows Server 2003/2008/2012/2016, Windows Vista, Windows 7/8/8.1/10（R2 含む）） ワークステーション、サーバーを問わず 32 ビット版、64 ビット版の両方に対応
メモリ	OS の最少要件に加えて 8MB RAM
ハードディスク	およそ 10MB の空き容量
必要ソフトウェア	IE 5.5 以降のバージョン（クライアントは XML を使用します。） .NET Framework 3.5 SP1（インストール時に要求されます。） （.NET Framework 4.x では動作しません。）
その他	Intel ベースシステム

WinSyslog サービス

WinSyslog サービスの動作要件はより小さいです。最も重要な違いは、サービスはシステム上に IE を必要としないということです。

WinSyslog サービスは、以下の環境で動作します:

OS	Windows 2000 SP3 以降のシステム （Windows XP, Windows Server 2003/2008/2012/2016, Windows Vista, Windows 7/8/8.1/10（R2 含む）） ワークステーション、サーバーを問わず 32 ビット版、64 ビット版の両方に対応
メモリ	5MB（使用環境により 64MB のメモリ追加を推奨（*1）
ハードディスク	およそ 5MB の空き容量 *1

(*1)使用される実際のリソースは、主に設定されるサービスに左右されます。

サービスが受信するメッセージが 1 秒間に数件である場合は、パフォーマンスへの影響は顕著ではありません。もし 1 秒間に数百件のメッセージを WinSyslog サービスが受信するならば、より大きなリソースを必要とします。それでも、実際の負荷は実行されるアクションに左右されます。テキストファイルにメッセージを保存する方が、データベーステーブルにそれらを書き込むより(データベースエンジンが同じマシン上に存在するは特に)パフォーマンスへの影響がかなり少なくすみます。ハードウェアサイジングのためのガイドラインはありません。予想される作業負荷に合わせる必要があります。詳しくは「performance optimization for syslog server operations」記事(英語)をお読みください。

しかし、このサービスはメッセージバースト(Syslog 経由など)などの高スループットを処理するために特別に最適化されています。大量のバーストが予想される場合や時間のかかるアクション(例:データベース書き込み)を実行する場合は、マシンにメモリを追加することをお勧めします。典型的な Syslog メッセージ(オーバーヘッドを含む)はおよそ 4～8 KB 使用します。最大 100,000～200,000 のメッセージを 1,024 MB でバッファできます。WinSyslog は、マシンのメッセージ処理が遅い場合でも、このようなバーストを一時的にメモリに格納することができます。

Adiscon LogAnalyzer

Adiscon LogAnalyzer でログを閲覧するには、Microsoft Internet Information Server (IIS) バージョン 4 以降、または Apache、PHP、データベース(MySQL 等)が必要です。Adiscon LogAnalyzer のインストールは必須ではありません。WAMP に含まれているような PHP5 と Apache の組み合わせで使用することをお勧めします。

> 注記: LogAnalyzer は無償で使用できますが、サポートの対象外です。

2. インストールと初期設定

ここでは WinSyslog のインストールおよび初期設定について説明します。

2.1. ソフトウェアの入手

WinSyslog のインストーラーは弊社ソフトウェアダウンロードページからダウンロードしていただけます。

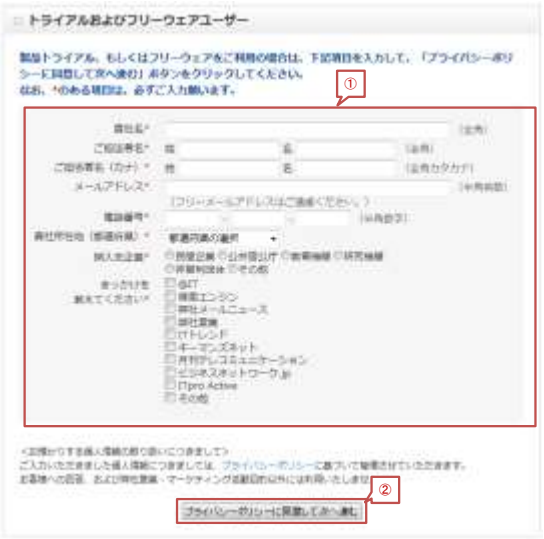
ソフトウェアダウロードページ：https://www.jtc-i.co.jp/support/download/

管理番号をお持ちの場合：

有効な管理番号をお持ちの場合（商用ライセンスをご購入いただきライセンスがサポート有効期限内である場合）は、「ライセンスユーザー」セクションで**「管理番号」**を入力し**「ダウンロードページへ進む」**をクリックしてください（①→②）。

管理番号をお持ちでない場合：

有効な管理番号をお持ちでない場合（購入前の評価利用またはフリー版利用の場合）は、**「トライアルおよびフリーウェアユーザー」**セクションで必要な情報を入力し**「プライバシーポリシーに同意して次に進む」**をクリックしてください（①→②）。



ソフトウェアのダウンロード

ソフトウェアの一覧で「Adiscon WinSyslog」を選択します。

「**Adiscon WinSyslog**」グループから
使用したいインストーラーのダウンロードアイコンを
クリックします。

ファイルを任意の場所に保存します。

2.2. インストール

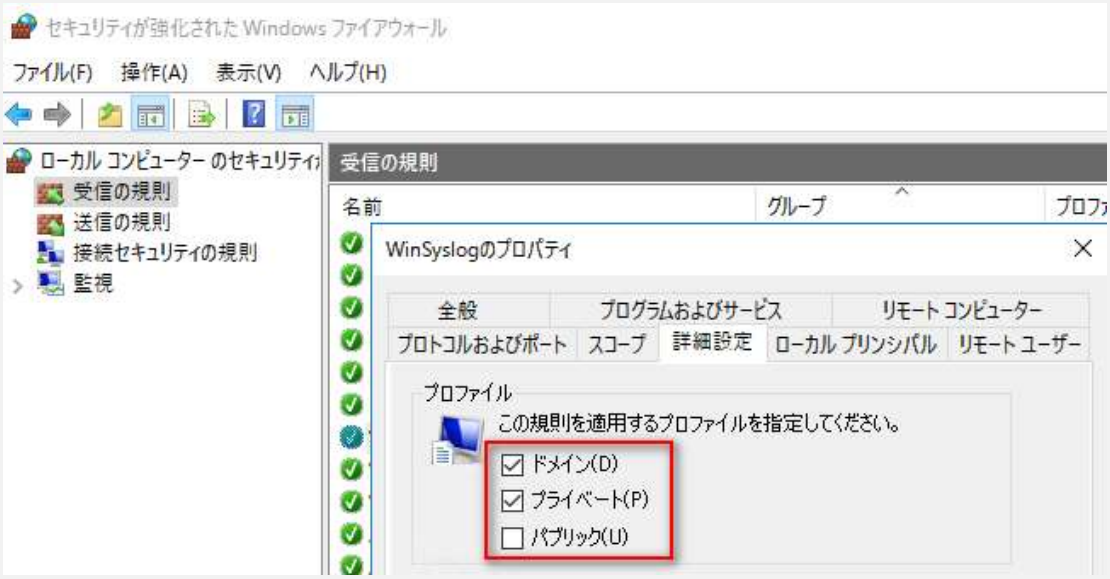
WinSyslog のインストールは単純で簡単です。

「2.1 ソフトウェアの入手」の手順でダウンロードしたインストールセット（zip ファイル）には、wnsyslogjp.exe が含まれています。任意の場所で展開した後、「wnsyslogjp.exe」をダブルクリックし、画面上の指示に従って進んでください。インストールおよびライセンス登録手順の詳細については、別紙「WinSyslog インストールとライセンス登録」ガイドをご参照ください。

注記：

ファイアーウォール設定について

インストールによって Windows ファイアーウォールに受信ルールが追加されます。Syslog メッセージを受信できないときは、受信ルールを適用するプロファイルをご確認ください。

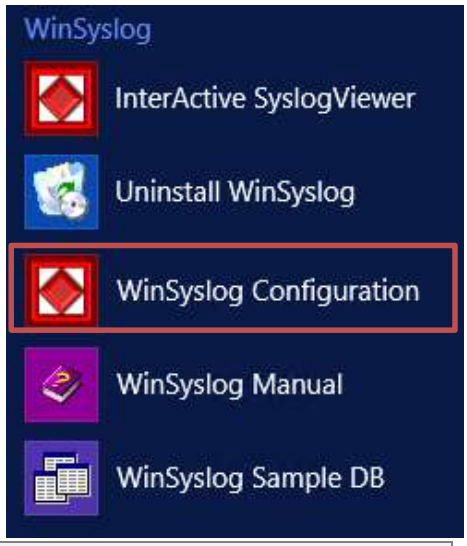


Adiscon LogAnalyzer について

Adiscon LogAnalyzer は無償でご利用いただけますが、弊社のサポート対象外です。、自己の責任の下でご利用ください。

2.3. 設定クライアントの起動

WinSyslog 設定クライアントを起動するには、アプリケーション一覧より「**WinSyslog Configuration**」をダブルクリックします。



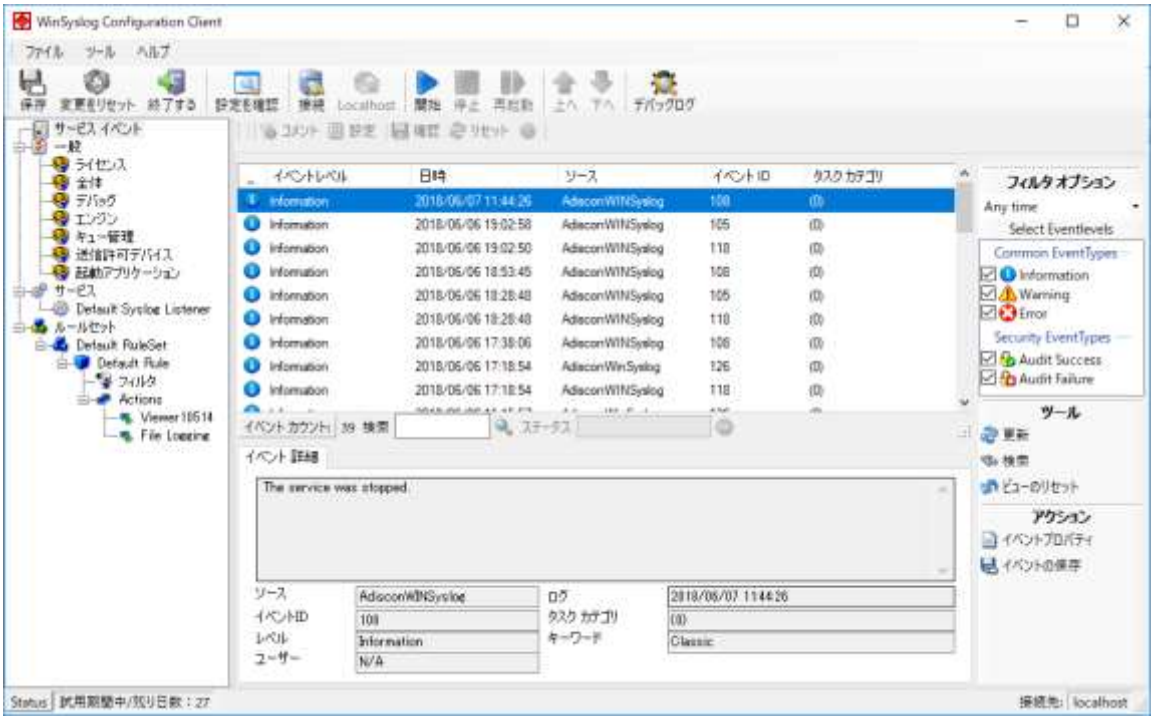
メモ:
「**WinSyslog Configuration**」（設定クライアント）と「**InterActive SyslogViewer**」（インタラクティブ Syslog ビューア）のデスクトップショートカットを作成しておくと便利です。

2.4. 設定クライアントの表示言語の変更

ここでは、WinSyslog 設定クライアントの表示言語を日本語に切り替える手順を説明します。

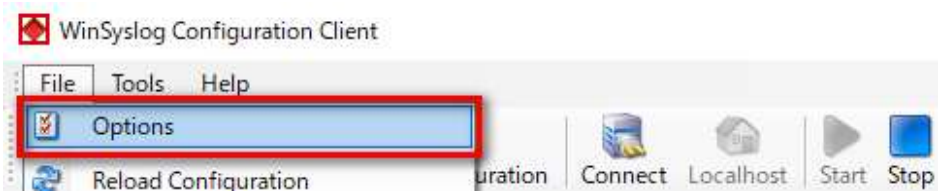
注記:
この資料は、表示言語に日本語が選択されていることを前提としています。初回起動時に表示言語を「**Japanese**」（日本語）に変更してください。

WinSyslog 設定クライアントを初めて起動すると、ユーザーインターフェイスが英語で表示されます。

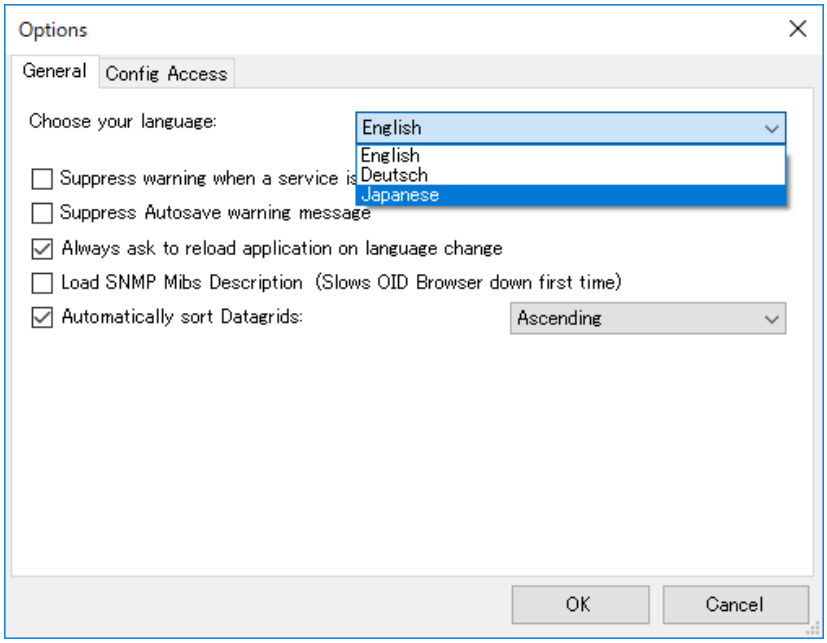


表示言語の変更手順は以下のとおりです:

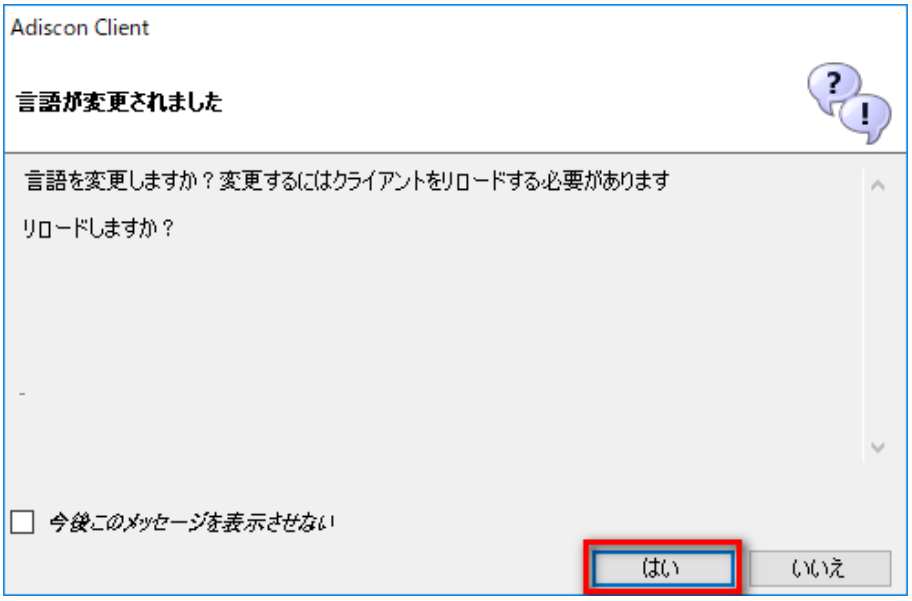
1. 「**File > Options**」を選択します。



2. 「**General**」タブの「**Choose your language:**」で「**Japanese**」を選択し、「**OK**」をクリックします。



3. 「**はい**」をクリックすると、クライアントが再起動されます。



4. 設定クライアントが日本語で表示されます。

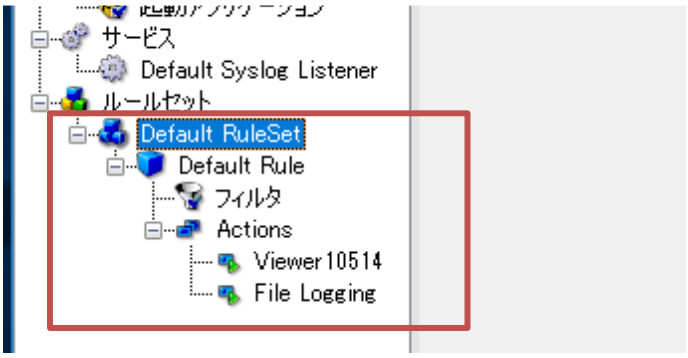
2.5. 初期設定

WinSyslog のインストール後は、動作設定を行う必要があります。
ここでは WinSyslog の初期設定について説明します。

> **注記:**
> v14.1 から日本国内ユーザー向けの初期設定となりました。この資料では v14.1 以降の日本仕様 WinSyslog について説明します。

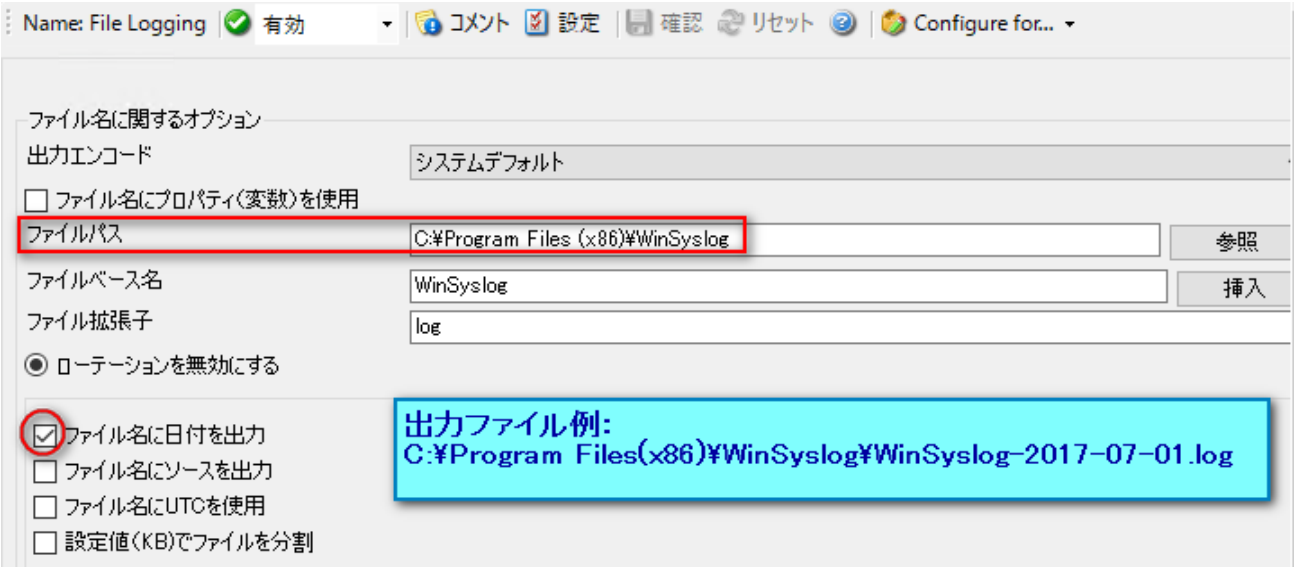
2.5.1. ルールセット - Default RuleSet の確認

インストール時に「**Default RuleSet**」という名前でデフォルトのルールセットが作成されます。



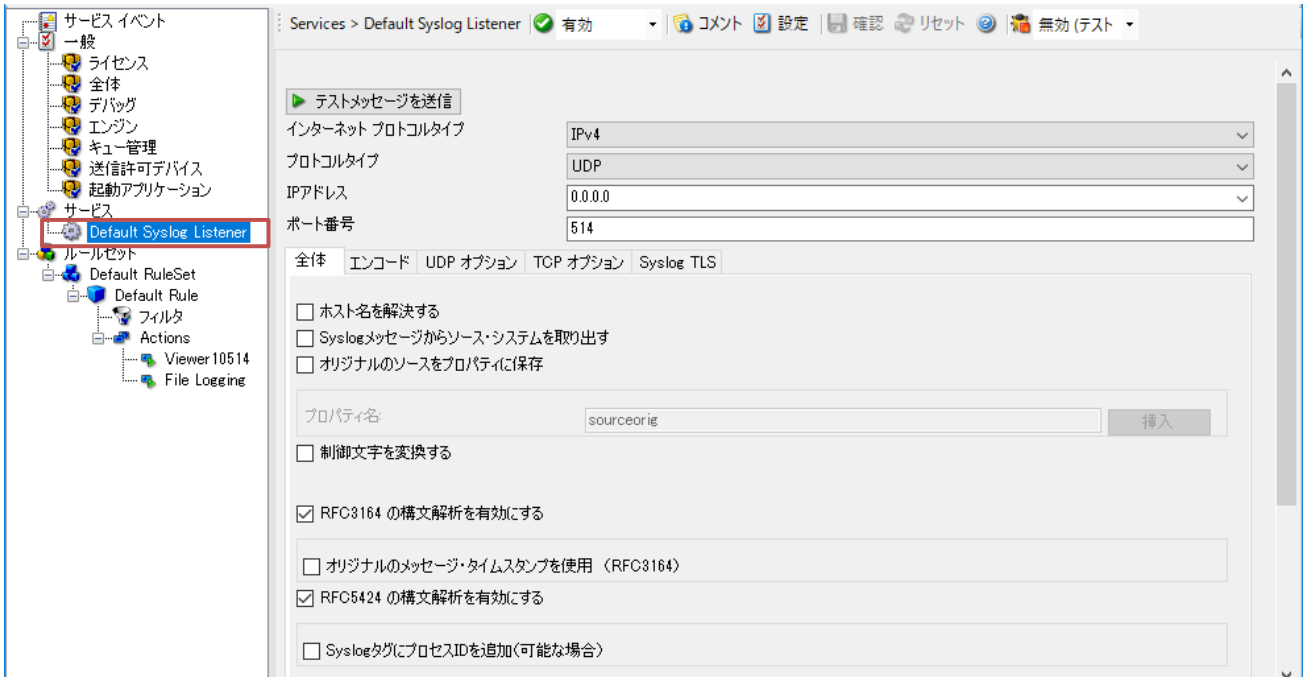
配下の「**Default Rule**」(デフォルトルール)には、フィルタの条件が設定されていません。これは、メッセージを絞り込まずに、WinSyslog で受信した全てのメッセージを処理することを意味します。「**Actions**」には「**Viewer 10514**」と「**FileLogging**」(ファイルログ)が設定されています。このデフォルト設定により、WinSyslog は、UDP 514 で受信したすべての Syslog を 10514 ポートでインタラクティブ Syslog ビューアへ転送した後、プログラムインストールフォルダ下のログファイルに書き込みます。作成されるログファイルの末尾には日付が付与される設定となっているため、1 日ごとに 1 ログファイルが作成されます。デフォルトのログファイルパスは以下のとおりです: C:¥Program Files (x86)¥WinSyslog¥WinSyslog-*YYYY-MM-dd*.log

> **注記:**
> ログの保存先は「**ファイルパス**」で指定できます。十分な空き容量があるドライブのフォルダに変更することをお勧めします。



2.5.2. サービス – Default Syslog Listener の確認

インストール時に「**Default Syslog Listener**」という名前でデフォルトの Syslog サーバーサービスが作成されます。



このデフォルトの Syslog サーバーサービスは、UDP 514 ポートで Syslog を受信するように設定されています。UDP 514 で Syslog を受信する場合は、新しく Syslog サービスを追加する必要はありませんが、異なるプロトコルやポート番号で Syslog を受信したい場合は Syslog サーバーサービスを追加するかまたは「**Default Syslog Listener**」の設定を変更する必要があります。

2.5.3. WinSyslog サービスの起動

WinSyslog はインストールが完了すると、すぐに UDP 514 ポートで Syslog を受信し、インタラクティブ Syslog ビューアへの転送とログファイルへの書込みを開始します（サービスは自動で起動します）。

デフォルト設定を変更した場合は、設定を保存しサービスを再起動してください。

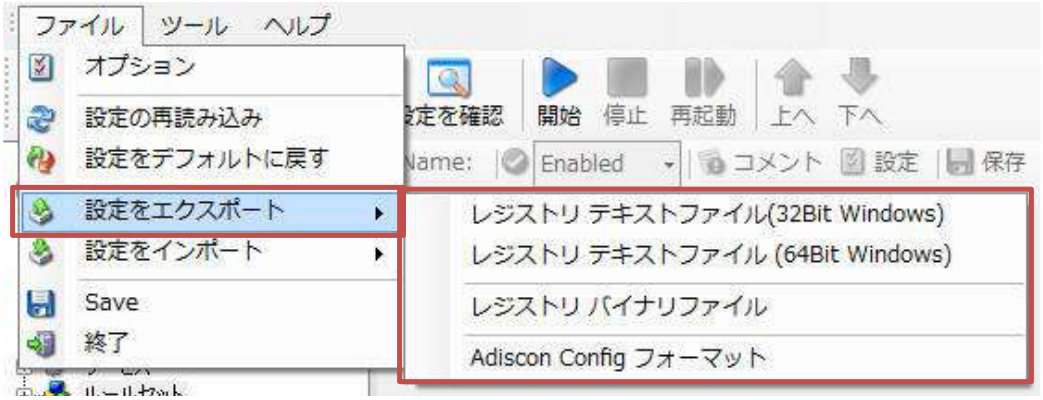
> **メモ:**
>
> 「**一般**」>「**全体**」>「**設定変更時に自動的にサービスをリロードする**」チェックボックスがオンの場合、ツールバー上の「**保存**」ボタンをクリックすると、自動的にサービスが再起動されます。
>
> 標準的なログサーバーの設定手順については、別紙「標準ログサーバー設定」をご参照ください。

3. 設定情報のエクスポート

弊社カスタマーポータル宛にお問い合わせ頂いた際、その内容によっては、お客様の設定内容を確認させて頂く場合があります。設定情報は、「**ファイル**」>「**設定をエクスポート**」メニューからエクスポートできます。

> **メモ**:
>
> 設定情報のエクスポート手順については、別紙「設定のエクスポートとインポート」をご参照下さい。
>
> 技術サポートで提供を依頼する設定ファイルは、通常「**Adiscon Config フォーマット**」を選択して保存したファイル(.cfg ファイル)です。

設定情報のエクスポートは、サポートの場合だけでなく、設定のバックアップを行いたい場合や、複数のマシンで同じ設定をご利用になりたい場合など、様々な状況で役立ちます。



レジストリ テキストファイル(32Bit Windows)

32bit 版 OS で WinSyslog をご利用の場合で、設定をレジストリファイルにエクスポートしたい場合に使用します。

レジストリ テキストファイル(64Bit Windows)

64bit 版 OS で WinSyslog をご利用の場合で、設定をレジストリファイルにエクスポートしたい場合に使用します。

> **注記**:
> レジストリテキストファイルをインポートするためのオプションはありません。「**レジストリ テキストファイル**」の設定を読込みたい場合は、エクスポートしたレジストリファイルをダブルクリックしてください。ダブルクリックすると、「**…内の情報をレジストリに追加しますか？**」という確認画面で、「**はい**」を選択して下さい。

レジストリバイナリファイル

レジストリバイナリファイルとして出力することができます。

> **メモ:**
> WinSyslog の設定情報は、下記のレジストリキーに保存されています:
> - 32bit 版: HKEY_LOCAL_MACHINE¥SOFTWARE¥Adiscon¥WinSyslog
> - 64bit 版: HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Adiscon¥WinSyslog
>
> レジストリエディタからエクスポートすることもできます。

Adiscon Config フォーマット

「**Adiscon Config フォーマット**」は、v13.0 で追加されました。設定情報を出力する場合は、このオプションをご利用ください。拡張子は、.cfg です。

4. InterActive SyslogViewer（インタラクティブ Syslog ビューア）

ここでは、InterActive SyslogViewer（以降、「インタラクティブ Syslog ビューア」と表記）について説明します。詳しい使用方法については、別紙「InterActive SyslogViewer ユーザーマニュアル」をご参照ください。

4.1. インタラクティブ Syslog ビューアとは

インタラクティブ Syslog ビューアは、受信した Syslog をリアルタイムに表示することができます。WinSyslog のアドオンコンポーネントとして提供されます。

しかし、インタラクティブ Syslog ビューアは、リアルタイムのトラブルシューティングに重点を置いたユーティリティプログラム（Syslog の受信確認などデバッグ目的での利用を想定した補助ツール）であることに注意してください。これはシステムを継続的に監視するためのものではありません（現在の Syslog トラフィックを表示することはできますが、受信したログをログファイルに保存するなど他の手段でログを保存してください）。

WinSyslog にはローカルマシンのインタラクティブ Syslog ビューアへ 10514 ポートで Syslog メッセージを転送するアクションがデフォルトで設定されています（「**Viewer 10514**」アクション）。インタラクティブ Syslog ビューア側もデフォルトで 10514 ポートが設定されています。このため、WinSyslog のインストール後、インタラクティブ Syslog ビューアで受信した Syslog メッセージを確認することができます。

> **注記：**
> インタラクティブ Syslog ビューアには検索機能やフィルタ機能がないため、過去に受信し保存済みの大量のログデータの中から、特定の Syslog メッセージを見つけ出すのは困難です。このような目的のためには、閲覧・検索のために別ツールをご利用いただくことをお勧めします。

4.1.1. 機能

ここではインタラクティブ Syslog ビューアの機能について説明します。

早くて簡単な Syslog 表示

Syslog メッセージの表示・確認が簡単に行えます。従って、監視システムで起こっている問題をより早く発見し、対処することも可能となります。

選択したデータのエクスポート

受信したデータのうち必要なものだけを選択し、エクスポートすることができます。データは、テキストファイル、または CSV ファイルとして保存できます。

データベースの読み込み

ODBC（32bit）経由で指定したデータベースのログエントリを直接確認することができます。列のハイライトとフィルタ機能を使用できます。それにより、テキストを指定して対象データのみハイライト表示させたり、ファシリティやプライオリティを指定して、対象データのみを表示させたりすることができます。

注記： インタラクティブ Syslog ビューアは、リアルタイムのトラブルシューティングに重点を置いたユーティリティプログラムです。本番運用のサイズの大きいデータベースを継続的に閲覧する場合は、別のアプリケーションをご利用いただくことを推奨します。

> **注記：**
> インタラクティブ Syslog ビューアは、リアルタイムのトラブルシューティングに重点を置いたユーティリティプログラムです。本番運用のサイズの大きいデータベースを継続的に閲覧する場合は、別のアプリケーションをご利用いただくことを推奨します。

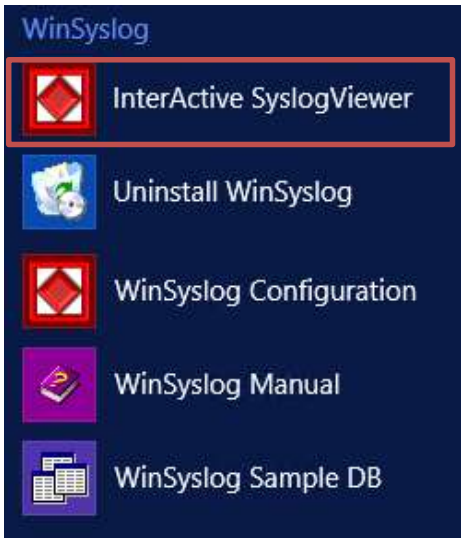
4.1.2. システム要件

インタラクティブ Syslog ビューアの最小システム要件は以下のとおりです：

OS	Windows ベースのオペレーティングシステム （Windows XP, Vista, 7,8, 10, 2003, 2008, 2012, 2016 など）
メモリ	32MB RAM 以上
必要ソフトウェア	.NET Framework 2.0 またはそれ以降のバージョン

4.2. インタラクティブ Syslog ビューアの起動

インタラクティブ Syslog ビューアを起動するには、スタートメニューから「**WinSyslog**」＞「**InterActive SyslogViewer**」をクリックします。



> **メモ**： デスクトップショートカットを作成しておくと便利です。

コマンドプロンプトから起動することもできます。

コマンドプロンプトからの起動手順は以下のとおりです：

1. コマンドプロンプトを起動します。
2. WinSyslog がインストールされているドライブディレクトリに変更します。
3. InteractiveSyslogViewer.exe と入力し「Enter」キーを押します。

利用可能なコマンドラインパラメーターは以下のとおりです：

パラメーター	説明
/?	オプションを表示します。
/autolisten	自動的に Syslog ビューアを起動します。
/port=10514	設定ポートを上書きします。
/windowpos 0,0,512,800	デフォルトのウィンドウポジションを設定します。

4.3. オプションと設定

インタラクティブ Syslog ビューアのオプションおよび設定については、別紙「InterActive SyslogViewer ユーザーマニュアル」をご参照ください。

5. WinSyslog の設定

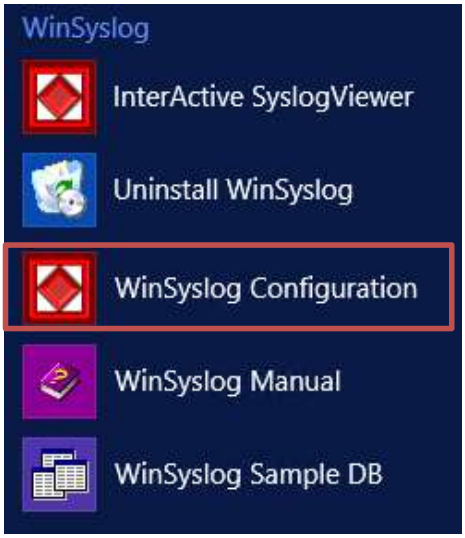
WinSyslog は簡単に操作でき、効果的な製品です。

この章では、WinSyslog の設定方法について説明します。

WinSyslog の最も重要な部分であるサービスは、一旦設定されるとバックグラウンドで動作します。そして、それ以降はユーザーの操作は必要ありません。従って、この章では、WinSyslog 設定クライアントに焦点を当てて説明します。WinSyslog 設定クライアントは、サービスの設定を行うために使用されます。

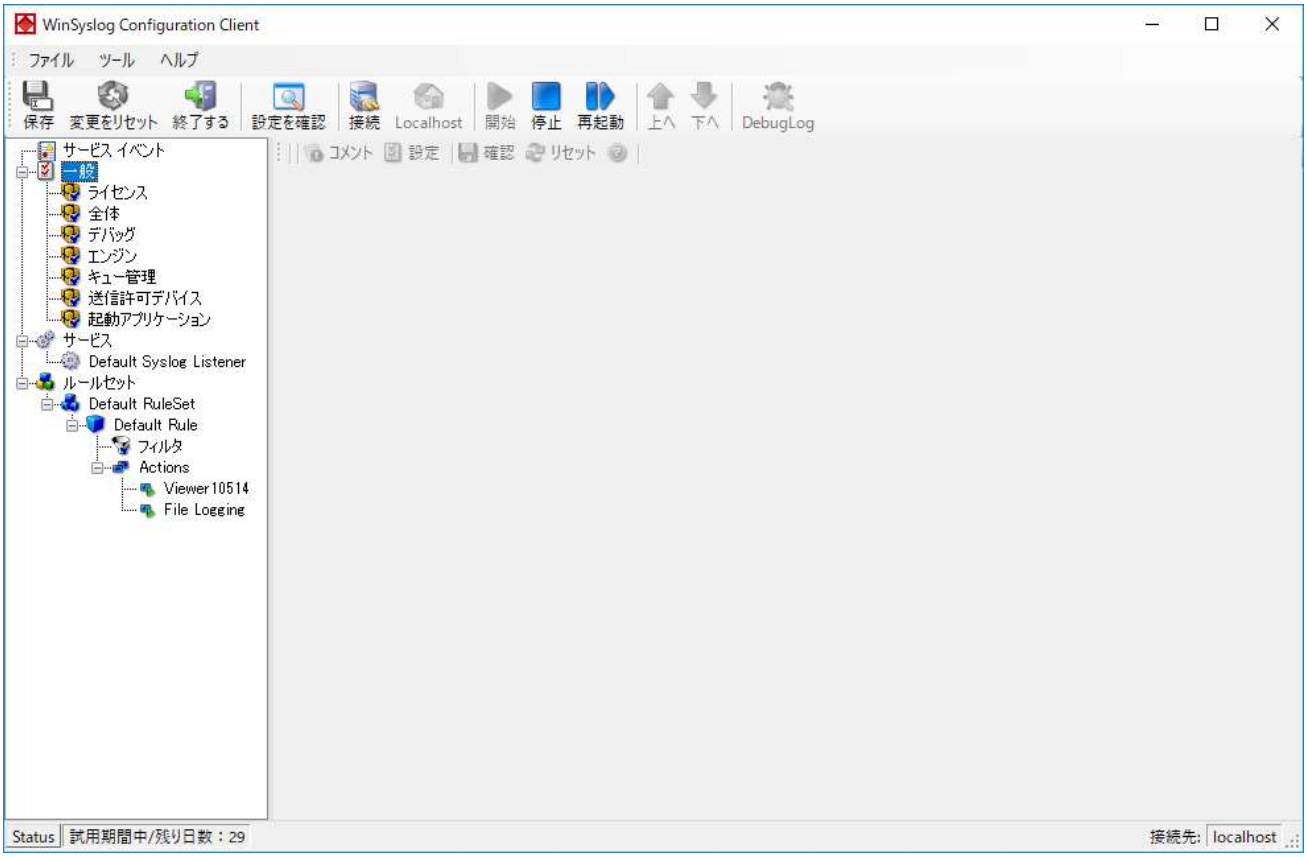
> **注記:**
> WinSyslog では、v13.1 で実装された現在のクライアントとそれ以前のバージョンで使用されていた旧クライアント(レガシークライアント)が利用できます。この資料では、現在の設定クライアントについて説明します。

WinSyslog 設定クライアントを起動するには、スタートメニューまたは、アプリケーション一覧より「**WinSyslog Configuration**」をダブルクリックして、設定クライアント(**WinSyslog Configuration Client**)を起動します(C:¥Program Files (x86)¥ WINSyslogClient.exe)。



すると、下図のようなウィンドウが現れます。

> **メモ:**
> この文書は、日本語ユーザーインターフェイスの利用を前提としています。表示言語の変更手順については「2.4 設定クライアントの表示言語の変更」をご参照ください。



設定クライアントには、2つの要素があります。
左側には、WinSyslog システムのそれぞれの要素を選択するツリー表示があります。
右側には、ツリー表示で選択されたパラメーターが表示されます。

ツリー表示には、「**一般**」、「**サービス**」、「**ルールセット**」の3つのトップレベル項目があります。

一般

「**一般**」では、基本的な操作パラメーターと、アクションとサービスのデフォルトが定義されています。この設定自体は何も起動しませんが、ここでのパラメーターは、実際のサービスまたはアクションが設定パラメーターを必要とする時に使用されます。特定のインスタンスは定義されていません。最も一般的なパラメーターをデフォルトにすることを強く推奨します。これにより、特定の要素のデータ入力量が大幅に削減されます。**各デフォルトは、特定のサービスまたはアクションで上書きされます**。詳しくは「5.3 一般オプション」をお読みください。

サービス

「**サービス**」のツリー表示には、設定されたサービスとそのパラメーターがあります。1サービスエントリにつき1つのサービスを作成します。**サービスの作成数に制限はありませんが、同じ設定内容のサービスは、複数稼動させることはできません**。同じ種類のサービスを複数作成する場合には、ポートの衝突を避けるように設定を行って下さい。Syslog サーバーサービスならば、同じポート（例： 514）を使用しているが

プロトコルタイプが違うもの、違うポート（例： 515）を使用しているものを設定すれば、同じ種類のサービスを同一システム上で3つ作成し、稼動させることも可能です。同じポートで同じプロトコルを設定した Syslog サービスが存在する場合は、複数の Syslog サービスのインスタンスが実行されているという内容のエラーが Windows のイベントログに記録されます。

以下のようなイベントログが記録されます。

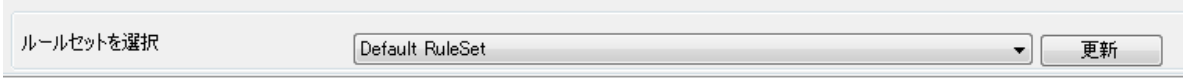
イベントの種類	警告
イベント ソース	AdisconWinSyslog
イベント カテゴリ	なし
イベント ID	1001
説明	A configured syslog server service can not be started. Most often, this happens when more than one syslog server service is configured to use the same port and protocol, e.g. 514/UDP. Please make sure that only a single syslog server is defined to listen on the same port and protocol. If you would like to do multiple actions, this can be done within a single rule set that is bound to a single syslog server service. The socket subsystem reported the following reason: "Can't bind to socket - will keep retrying..." Additional help might be available at http://www.adiscon.com/EventHelp.asp （設定した Syslog サーバーサービスは、実行できません。これは、同じポートやプロトコルを使用するよう（例：514/UDP）設定された Syslog サーバーサービスが複数存在する場合に、起こりえます。もし、複数のアクションを実行したい場合には、1つのルールセットを1つのサービスに関連付けるように設定を行ってください ･･･）

理論的には、数百ほどのサービスを追加できますが、オペレーティングシステムのリソースや取り扱いについての観点から、最大でも 20 から 30 までのサービスに数を制限することをお勧めします。もちろん、この制限より多くのサービスが有効である場合もあります。WinSyslog 自体は、サービスの作成数に制限はありません。数多くのサービスを必要とし、ハードウェアがその処理に耐えうる場合は、数の制限は必要ありません。

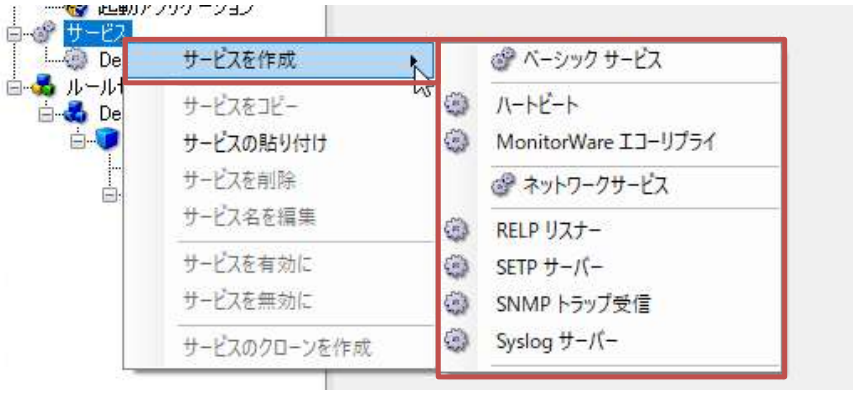
実際のパラメーターは、サービスの種類に左右されます。

サービスの「**有効**」「**無効**」は全てのサービスに共通です。「**有効**」なサービスは機能します。「**無効**」のサービスは設定されていても実行されません。これにより、サービス定義を削除しなくても簡単にサービスを一時的に使用不能にすることができます。

同様に、右側の設定ダイアログの最下部にある「**使用するルールセット**」も、サービスの種類に関係なく共通のものです。どのサービスに対して、どのルールセットを実行するのかをここで指定します。



新しくサービスを作成する場合には、「**サービス**」を右クリックして下さい。それから、「**サービスの追加**」を選択し、さらにポップアップメニューからサービスの種類を選択します。



サービスを削除したい場合は、その対象のサービスを右クリックし、「**サービスの削除**」を選択します。

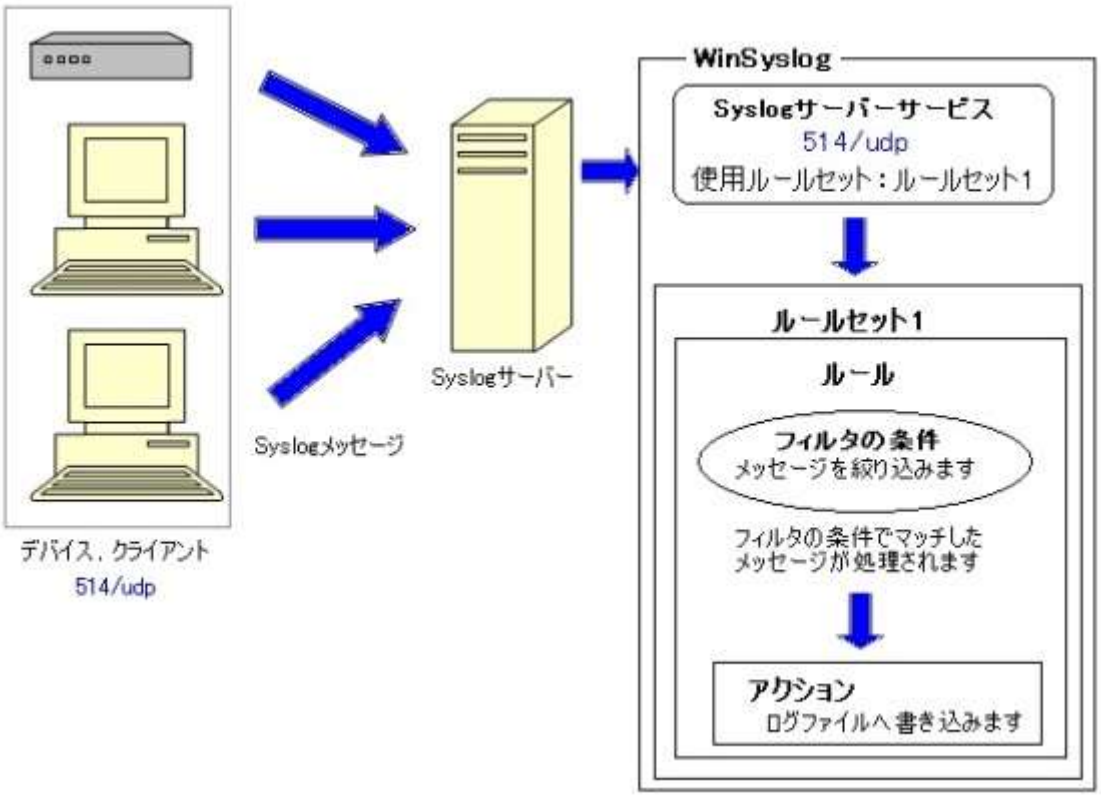
一時的に削除したい場合には、「**無効**」を選択してください。またはサービスを右クリックして「**サービスを無効に**」を選択することでも無効にすることができます。

それぞれのサービスについては「5.4 サービスオプション」をお読みください。

ルールセット

ツリー表示の最後の項目は「**ルールセット**」です。
ここで全てのルールセットの設定を行います。それぞれのルールセットは、完全にお互いから独立しています。ルールセットは、サービスと組み合わせて使用します。ルールセットの配下には、ルールを作成します。さらに、ルールの下には、それに関連するフィルタとアクションの条件があります。別途ご説明しますが、ルールは非常に重要な機能です。
ルールは上から順に実行されます。ルールを上や下に移動するには、移動したいルールをクリックして「**上へ** 」や「**下へ** 」のボタンをクリックするか、ドラッグ＆ドロップで移動します。

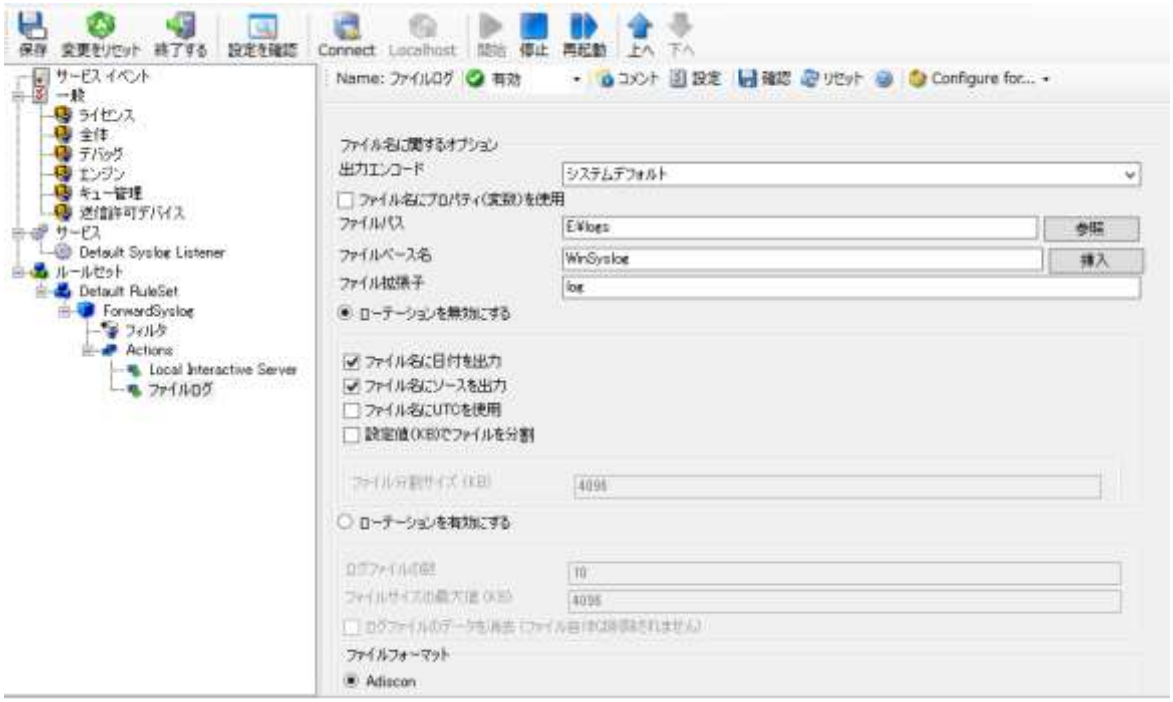
下図を例に、WinSyslog で Syslog メッセージがどのように処理されるかについて概要を説明します:



例として、WinSyslog で受信した Syslog メッセージをログファイルに書き込む場合、Syslog メッセージは下記のように処理されます:

1. Syslog サーバーサービスで Syslog メッセージを受信します。
   （Syslog メッセージ送信側と受信側で通信の設定を合わせてください）
2. 1 のサービスの「**使用するルールセット**」で指定されたルールセットへメッセージが渡されます。
3. 2 のルールセットのルール（複数ある場合には上から順に）に渡されます。
4. 3 のルール内のフィルタの条件が適用されます。
   （設定されていない場合には、全てのメッセージでアクションが実行されます。）

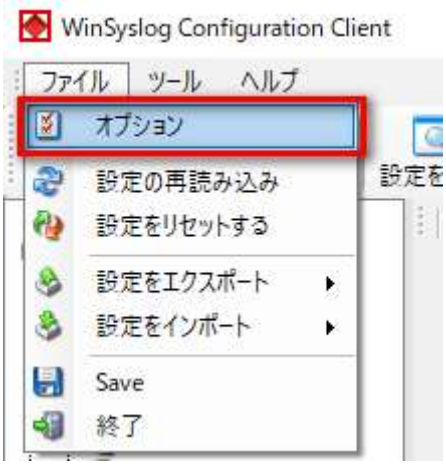
5. 4 のフィルタ条件に合致したメッセージに対して、その配下にあるアクション（上図の場合「ファイルログ」アクション）が実行されます。



上のスクリーンショットは、前頁のサンプルの設定画面です。

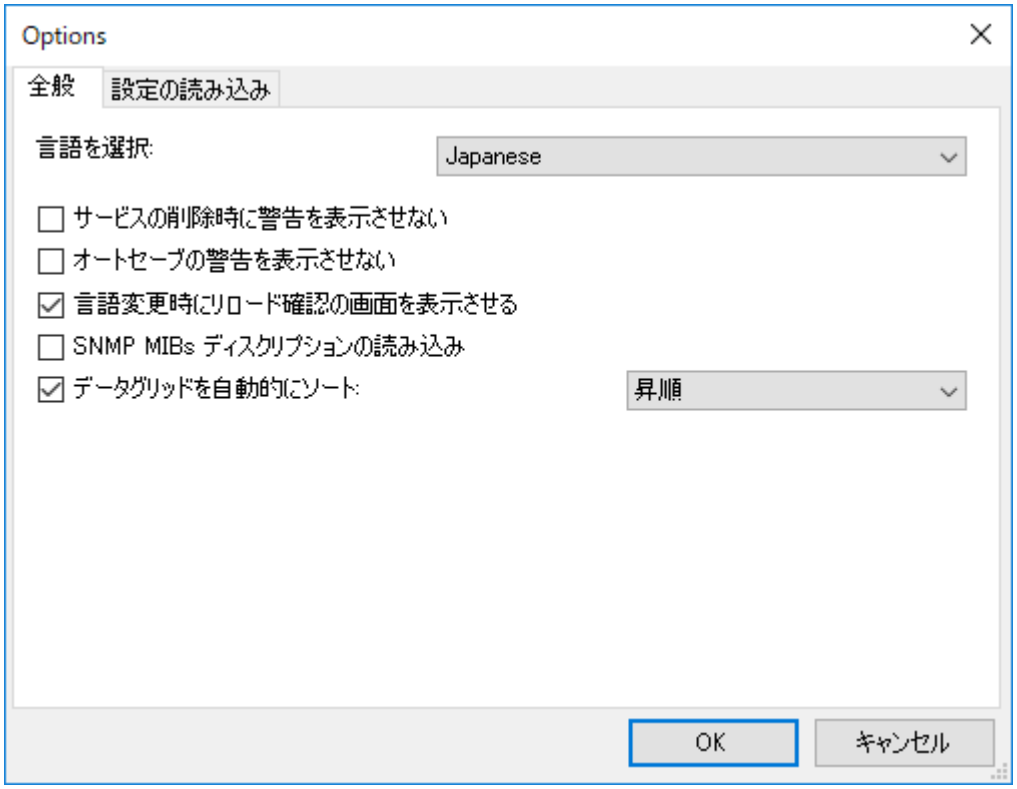
5.1. 設定クライアントオプション

ここでは、設定クライアントの「**ファイル**」>「**オプション**」で使用できる設定項目について説明します。



「全般」タブ

「**全般**」タブを選択すると、以下の画面が表示されます：



言語を選択

設定クライアントの表示言語を指定します。

サービスの削除時に警告を表示させない

サービスを削除する際の確認メッセージを表示させたくない場合には、このチェックボックスをオンにしてください。オフの場合は、削除時に「サービスを削除してもよろしいでしょうか？」という確認メッセージが表示されます。

オートセーブの警告を表示させない

設定変更後、保存せずに別の設定に移るときに表示される確認メッセージを表示させたくない場合には、このチェックボックスをオンにします。

言語変更時にリロード確認の画面を表示させる

設定クライアントの表示言語変更時の確認画面を表示させたくない場合には、このチェックボックスをオフにしてください。

SNMP MIBs ディスクリプションの読み込み

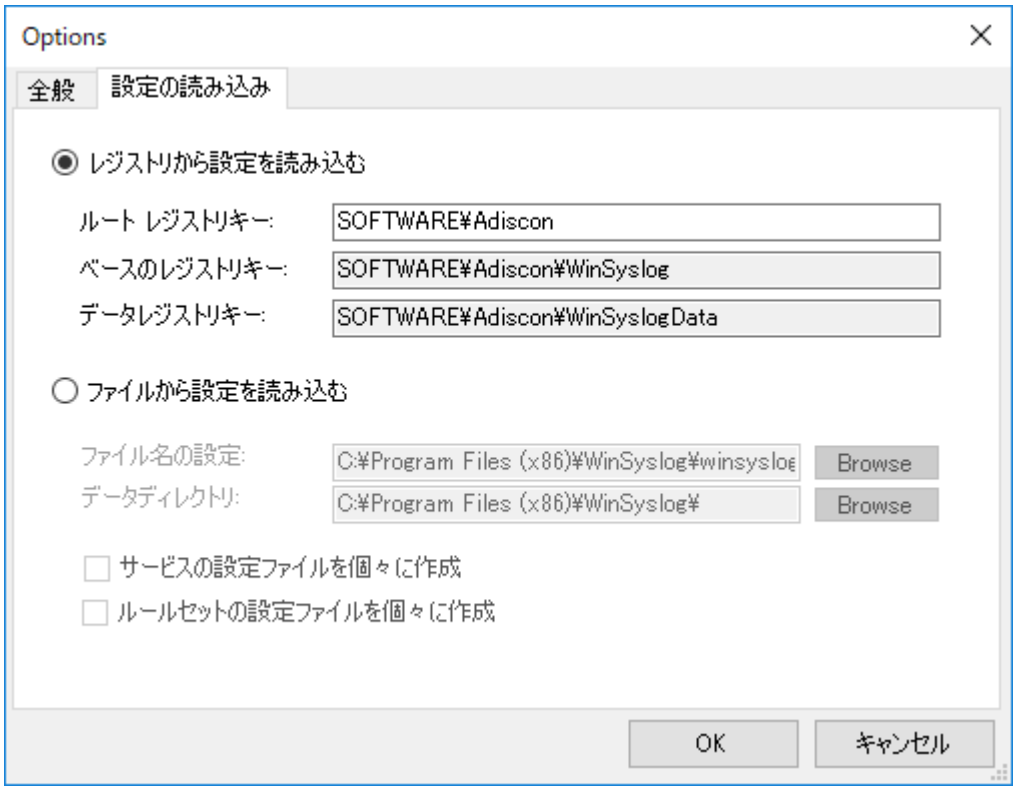
このチェックボックスをオンにすると、MIB 定義ファイルを設定クライアントの起動時に読み込みます。MIB 定義ファイルは、「一般」>「全体」>「MIB の場所（パス）」で指定した場所においてください。

データグリッドを自動的にソート

このチェックボックスをオンにすると、データグリッド（表）で表示される画面で行項目が昇順または降順でソート表示されます。v14.3 で追加された DebugLog のビューアでこの設定が反映されます。

「設定の読み込み」タブ

「**設定の読み込み**」タブを選択すると、以下の画面が表示されます：



レジストリから設定を読み込む

オンにすると、ここで指定したレジストリキーから設定を読み込みます。

ファイルから設定を読み込む

オンにすると、ここで指定したファイル（.cfg ファイル）から設定が読みこまれます。

- **サービスの設定ファイルを個々に作成**

「**ファイルから設定を読み込む**」がオンの場合のみ使用できます。オンにすると、設定クライアントは、設定されたサービスごとに個別の設定ファイルを作成します。メインの設定ファイルは includeconfig 文でパターンを使用してこれらの設定ファイルをすべてインクルードします。サービスを削除すると、その設定ファイルも削除されます。

- **ルールセットの設定ファイルを個々に作成**

  「**ファイルから設定を読み込む**」がオンの場合のみ使用できます。オンにすると、設定クライアントは、設定された各ルールセットに対して個別の設定ファイルを作成します。メインの設定ファイルは includeconfig 文でパターンを使用してこれらの設定ファイルをすべてインクルードします。ルールセットを削除すると、その設定ファイルも削除されます。

5.2. ファイルベース設定の使い方

ここでは、「**ファイル**」>「**オプション**」>「**設定の読み込み**」タブで「**ファイルから設定を読み込む**」を選択した場合の設定について説明します。

ファイルベース設定（「**ファイルから設定を読み込む**」がオン）は、レジストリアクセスを最小限に抑えたい場合や、設定クライアントを毎回使用せずに手動で設定を編集したい場合に使用します。

Adiscon Config フォーマットは大変シンプルです。以下にすべての設定オプション詳細について説明します。

Adiscon Config フォーマット

Adiscon 設定フォーマットは JSON 形式と XML 形式を合わせた、非常にシンプルな形式です。

変数

すべての変数はドル（$）で始まります。変数の名前と値は、最初の空白文字で区切られます。最初のスペースの後にくるものはすべて Value（値）とみなされます。改行で値を終了します。設定値に改行が含まれている場合は、¥¥n または¥¥r¥¥n で置換する必要があります。中括弧（{ と }）をエスケープするには、バックスラッシュを 1 つ使用してください。

コメント

シャープ(#)で始まるすべての行は無視されます。

ファイルインクルード

サンプル: includeconfig my-subconfigfiles-*.cfg

includeconfig ステートメントはファイル名パターンに基づき、単一または複数のファイルを含みます。上記の例の場合は、”my-subconfigfiles-“で開始し、”.cfg”で終了するすべてのファイルが設定に含まれます。include を使用すれば、独自のカスタムファイル構造を作成することができます。設定クライアントはカスタムファイル構造をロードして表示することができますが、それを維持(保存)することはできません。includeconfig ステートメントを使用する場合、最大 10 レベルのインクルード深度をサポートします。

「一般」オプション

サンプル:

```
general(name="[name]") {
   $nOption 1
   ...
}
```

角括弧内のすべてのオプションは、変数として一般設定オブジェクトにロードされます。name 属性フィールドは一般設定ブロック名を指定します。オブジェクトブロックは括弧で開始し、括弧で終了します。

サービス

サンプル:

```
input(type="[ID]" name="[name]") {
   $var1 Value1
   $var2 Value2
   ...
}
```

サービスブロックは括弧で開始し、括弧で終了します。括弧内のすべての変数はサービス設定にロードされます。name 属性はサービス表示名を指定します。type 属性はサービスタイプ ID を含みます。以下のいずれかを指定できます:

1 = Syslog
2 = Heartbeat
3 = EventLog Monitor V1 (Win 2000 / XP / 2003)
4 = SNMP Trap Listener
5 = File Monitor
8 = Ping Probe
9 = Port Probe

10 = NTService Monitor
11 = Diskspace Monitor
12 = Database Monitor
13 = Serialport Monitor
14 = CPU Monitor
16 = MonitorWare Echo Request
17 = SMTP Probe
18 = FTP Probe
19 = POP3 Probe
20 = IMAP Probe
21 = IMAP Probe
22 = NNTP Probe
23 = EventLog Monitor V2 (Win VISTA/7/2008 or higher)
24 = SMTP Listener
25 = SNMP Monitor
26 = RELP Listener
27 = Passive Syslog Listener
1999998= MonitorWare Echo Reply
1999999= SETP Listener

ルールセット

サンプル:

```
ruleset(name="[name]" expanded="[on/off]") {
  rule(name="[name]" expanded="[on/off]" actionexpanded="[on/off]"
ThreatNotFoundFilters="[on/off]" GlobalCondProperty="[on/off]" GlobalCondPropertyString=""
ProcessRuleMode="[0/1/2]" ProcessRuleDate="[uxtimestamp") {

        action(type="[ID]" name="[name]") {
                $var1 Value1
                $var2 Value2
                ...
        }
        filter(nTabSelection="0") {
                $nOperationType AND
                $PropertyType NOTNEEDED
                $PropertyValueType NOTNEEDED
                $CompareOperation EQUAL
                $nOptionalValue 0
                $nSaveIntoProperty 0
```

```
                    $szSaveIntoPropertyName FilterMatch
                }
        }
    }
```

ルールセットブロックは括弧で開始し、括弧で終了します。ルールセットの属性は自己説明可能です。ルールセット内にルールを設定することができます。ルールの属性も自己説明可能であり、部分的にフィルタダイアログに表示されるオプションと同じグローバル設定です。ルール内では、1つのベースフィルタを持つことができます。ベースフィルタは子フィルタを持つことができ、これらの子フィルタはさらに子フィルタを持つことができます。すべての"expanded"設定は任意であり、クライアントのツリービューでのみ重要です。ルール内には、アクションを持つことができます。アクションブロックは括弧で開始し、括弧で終了します。括弧内のアクションブロックのすべての変数は、アクション設定にロードされます。name 属性はサービスの表示名を指定します。type 属性にはアクションのタイプ ID が含まれます。次のいずれかのタイプを指定できます。

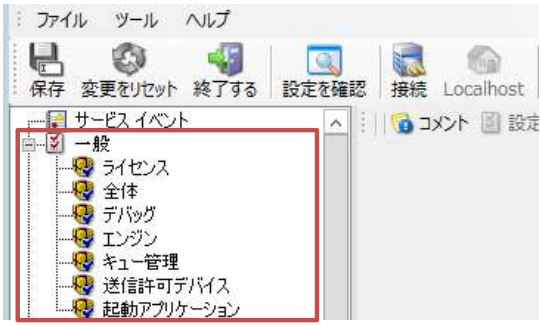
1000 = ODBC Database
1001 = Send Syslog
1008 = Net Send
1009 = Start Program
1011 = Send SETP
1012 = Set Property
1013 = Set Status
1014 = Call RuleSet
1015 = Post Process
1016 = Play Sound
1017 = Send to Communication Port
1021 = Send SNMP
1022 = Control NT Service
1023 = Compute Status Variable
1024 = HTTP Request
1025 = OleDB Database
1026 = Resolve Hostname
1027 = Send RELP
1028 = Send MS Queue
1029 = Normalize Event
1030 = Syslog Queue

ファイルベース設定の有効化手順

ファイルベースの設定に変更するには、設定クライアントを起動して「**ファイル**」>「**オプション**」>「**設定の読み込み**」タブを選択し、「**レジストリから設定を読み込む**」から「**ファイルから設定を読み込む**」に切り替えます。「**OK**」をクリックすると、現在ロードされている設定をファイルに保存するかどうかを尋ねられます。ファイルに保存したい場合は「**はい**」を、保存しない（既存の設定ファイルがある）場合は「**いいえ**」を選択します。設定クライアントが自動的にリロードします。

5.3. 一般オプション

ここでは、設定クライアントのツリービューにある「**一般**」オプションについて説明します。



5.3.1. ライセンス

ここでは、「**ライセンス**」オプションで使用できる機能について説明します。この機能は、ご購入いただいたライセンスを製品に適用する際に使用します。

注記:

WinSyslog はインストールすると、30日評価版（無償で30日間、すべての機能を使用可能）として動作します。30日の試用期間が終了すると、フリー版に切り替わります。製品版としてご利用いただくためには、有効なライセンスを登録していただく必要があります。

ライセンス適用後は WinSyslog サービスを再起動してください。

以下は、弊社からお送りするライセンスファイル（ライセンス情報）のサンプルです：

Product: WinSyslog Professional

Version: 15

Licensee Name: "XXX Corp." (without the quotes)

License Key(s): 11111-22222-333333-444444-555555

Licensed Copies: 1

Licensed Clients: 100

ユーザー登録名

ライセンス情報の「**Licensee Name**」の文字列部分（前後のダブルクォーテーションは除く）をクリップボードへコピーし、貼り付けてください。

> **注記：**
>
> ご注文時に「エンドユーザーライセンス申請フォーム」に記載していただきましたユーザー情報の「会社名（英語）」です。
>
> ライセンス発行後は、登録名の変更はできませんのでご注意ください。
>
> 大文字小文字が区別されます。ライセンスファイルの「**Licensee Name**」の内容を正確に入力してください。

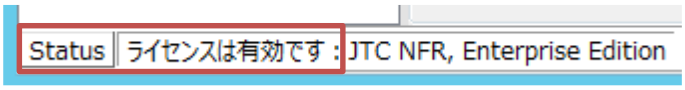
ユーザー登録番号

ライセンス情報の「**Licence Key**」の文字列部分（数字とハイフン含む）をクリップボードへコピーし、「**クリップボードから貼り付け**」を選択してください。数字部分がそれぞれの Key 欄に貼り付けられます。

> **注記：**
>
> この番号は、ご注文後 Adiscon 社によって発行されます。（ユーザー登録名に対して、固有のユーザー登録番号が発行されます。）
>
> 「**ユーザー登録名**」と「**ユーザー登録番号**」がライセンスキーとなり、これらを設定クライアントでご登録いただくことで、製品版として動作するようになります。
>
> 登録番号を正確に入力してください。登録内容に間違いがある場合には、製品版として登録されません。

「**ライセンスを確認**」をクリックし、「**有効なライセンスです**」と表示されれば、ライセンス情報が正しく入力されています。「**OK**」をクリックして画面を閉じます。

画面下部の「**Status**」エリアにも「**ライセンスは有効です**」と表示されます。



> **注記：**
> 「**ライセンスを確認**」をクリックすると、有効なライセンスの場合は「**Status**」エリアにも「**ライセンスは有効です**」メッセージが表示されますが、ライセンスはまだ適用されていません。

有効なライセンスであることを確認したら、ツールバー上の「**保存**」をクリックして設定を保存します（インストール後、一度も「**再起動**」を行ったことがない場合は、「**再起動**」もクリックしてください）。

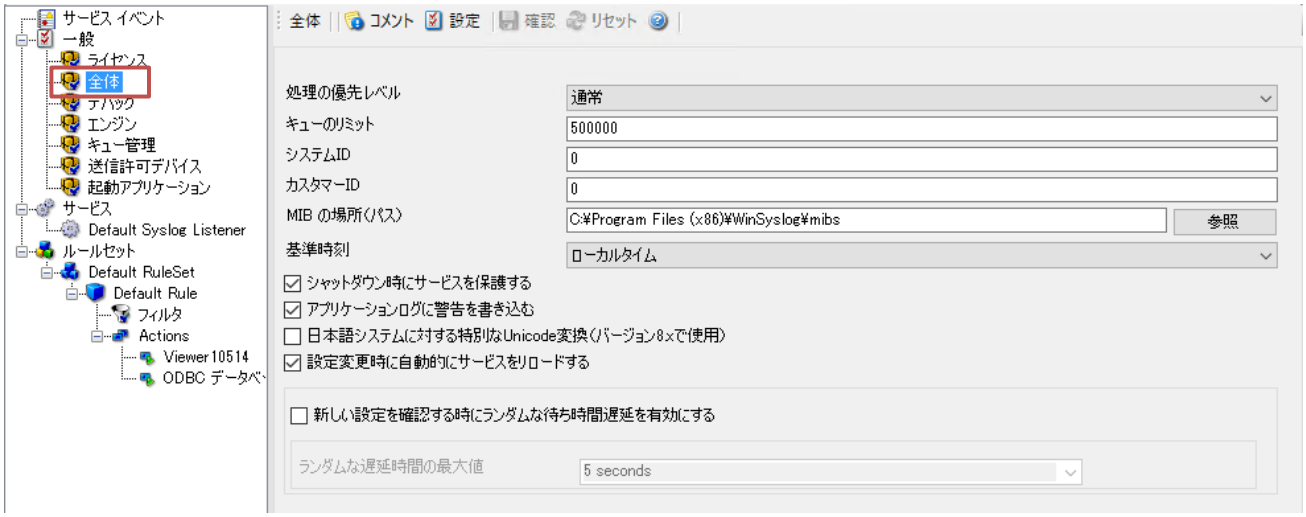
> **メモ：**
> 「**一般**」＞「**全体**」＞「**設定変更時に自動的にサービスをリロードする**」チェックボックスがオンの場合、「**保存**」をクリックすると、WinSyslog サービスが自動的に再起動されます。
> このチェックボックスをオフにしている場合は、「**保存**」をクリックした後で「**再起動**」を選択し、WinSyslog サービスを手動で再起動してください。

> **注記：**
> インストール後、一度も「**再起動**」をクリックしたことがない場合は、「**保存**」後に「**再起動**」をクリックしてください。「**一般**」＞「**全体**」＞「**設定変更時に自動的にサービスをリロードする**」はデフォルトでオンですが、この機能を有効にするには、一度「**再起動**」を実行する必要があります。

ライセンスの適用が完了すると、アプリケーションログにもイベントが出力されます。（例： イベント ID=118、レベル=情報、ソース=AdisconWINSyslog、イベントデータ=WinSyslog Professional (14.X.XXX) is running in registered mode.）

5.3.2. 全体

ここでは「**全体**」オプションで使用できる項目について説明します。



以下の項目を設定できます:

処理の優先レベル

ここでは、WinSyslog の処理の優先レベルを設定できます。選択肢は、アイドルクラス、低、通常、高があります。

キューのリミット

WinSyslog の処理時におけるキューの最大値を設定します。
0 を設定すると、無制限になります。

アプリケーションは、受信したがまだ処理されていないイベントが格納されているメモリ内バッファを保持します。これにより、製品は大きなメッセージバーストを処理できます。このようなバーストの間、イベントは受信され、メモリ内のキューに入れられます。（ルールセットを介した）キューの処理自体は、受信プロセスから分離されています。トラフィックバースト中はキューサイズが増加し、追加のメモリが割り当てられます。バーストが終了すると、キューのサイズが小さくなり、メモリが再び解放されます。

上限に達すると、それ以上キューに追加することはできません。この場合、古いイベントを最初に処理する必要があります。このような場合、受信イベントが失われる可能性があります（受信レートによって異なります）。メッセージ損失のリスクがあるため、キューサイズの上限値は高く設定することをお勧めします。値に 0 を設定すると無制限となり、キューサイズは利用可能な仮想メモリによってのみ制限されますが、使用可能なすべてのシステムメモリを使い切る可能性があり、システム障害を引き起こす可能性があるため推奨されません。

システム ID

システム ID を変更したい場合は、整数値を入力します。

カスタマーID

カスタマーID を変更したい場合は、整数値を入力します。

例えば、顧客のサーバーを監視する際に、会社ごとに違う ID を設定することが可能です。サーバーA と B を監視しているとして、5 台あるサーバーA はカスタマーID を 1、2 台あるサーバーB のカスタマーID を 2 といった具合で設定することが可能です。サーバーA と B のサーバー名が同じ場合でも、カスタマーID を設定すれば別の定義を行うことが可能です。

MIB の場所（パス）

MIB ファイルの場所を指定します。パスを指定するか、または「**参照**」ボタンから指定してください。

基準時刻

ファイルログやデータベースログ、E メール送信など、WinSyslog 全体で使用するタイムスタンプを設定します。UTC またはローカルタイムの指定を行えない設定項目に対しても、ここで選択したタイムスタンプが設定されます。ただし、プロパティ値（%timegenerated% や %timereported%）の基準時刻には、この設定値は反映されません。

シャットダウン時にサービスを保護する

このチェックボックスをオンにすると、サービスは未処理のイベントをインメモリキューに保存します。

サービスが停止すると、このインメモリキューは空になります。この場合、未処理イベントは消失してしまいます。このチェックボックスをオンにすると、サービスの停止前に全てのイベントが確実に処理されます。ただし、その処理中はサービスがハングアップしたかのような状態になります。このオプションは、大きなインメモリキューがある場合には有効です。

アプリケーションログに警告を書き込む

このチェックボックスをオンにすると、Windows アプリケーションイベントログへ警告を記録できるようになります。

日本語システムに対する特別な Unicode 変換（バージョン 8.x で使用）

日本語のシステムにおいては、文字の処理方法が異なります。WinSyslog 8 をご利用の場合には、このチェックボックスをオンにしてください。それ以外のバージョンではオフのままご利用ください。

設定変更時に自動的にサービスをリロードする

デフォルトでオンのこのチェックボックスをオンにすると、サービスは設定の変更を検出し、コアを自動的に再読み込みします。この機能は、（レガシークライアントアプリケーションではなく）新しいクライアントアプリケーションが使用されている場合にのみ機能します。また、ファイルベースの設定方法を使用して設定ファイルを更新する場合にも機能します。コンソールに入力を送らない限り、コンソールモードでサービスを使用している場合は機能しません。

> **注記：** この機能を有効にするには、インストール後に一度「**再起動**」を実行する必要があります。

新しい設定を確認する時に、ランダムな待ち時間遅延を有効にする

このチェックボックスをオンにすると、新しい設定チェックの間に指定したランダムな遅延時間が追加されます。このランダム遅延の最大値は 24 時間です。ランダム遅延はサービス制御に影響を及ぼしません。

- **ランダムな遅延時間の最大値**

  「**新しい設定を確認するときに、ランダムな待ち時間遅延を有効にする**」がオンの場合のみ、使用できます。待ち時間の最大値を指定します。

5.3.3. デバッグ

ここでは「**デバッグ**」オプションで使用できる項目について説明します。

ここでは、ルールベースのデバッグを行うことが可能です。複雑なルールベースの場合は特に、その処理が実行されている間、WinSyslog が内部で何を行っているかを知る必要があります。デバッグのログにより WinSyslog の内部での働きを知る事ができます。

ルールベースのテストとは別に、このデバッグのログは技術的な問い合わせの際に役に立ちます。問題解決のために、デバッグログの提出を依頼される場合があります。この場合は依頼されたレベルでデバッグログを取得してご提供ください。

> **重要:**
> デバッグ出力は、かなりのシステムリソースを必要とします。ログ出力が多ければ多いほど、より大きなリソースが必要となります。ログ出力が少なくともサービスの処理はかなり遅くなります。このため、通常は(必要な時以外は)このオプションは使用しないでください。

以下の項目を設定できます:

デバッグ出力を有効にする(必要時のみ)

このチェックボックスをオンにすると、デバッグログが有効となりサービスが稼動する際にログがファイルに書き込まれます。オフの場合は、デバッグログは書き込まれません。パフォーマンスの観点から、普段は選択なし(オフのまま)にしてください。

ファイルパス

「**デバッグ出力を有効にする（必要時のみ）**」がオンの場合のみ使用できます。
書き込みを行うログファイルの完全な名前を設定します。ドライブレターを含む完全なパス名を指定してください。ファイルまたはパス名だけを入力した場合、ローカルのサービスのデフォルトディレクトリが参照されます。これは多くのパラメーターに依存するため、実際のログファイルを見つけるのが難しくなります。整合性を考慮して、ドライブを含む完全なファイル名を指定してください。

> **注記:**
> 指定したディレクトリが見つからない場合、アプリケーションによってフォルダが自動的に作成されます。

デバッグレベル

「**デバッグ出力を有効にする（必要時のみ）**」がオンの場合のみ使用できます。
このセクションのチェックボックスでファイルへ書き込むデバッグ情報量を制御します。サポートサービスからの依頼がない限り、「**エラー警告を出力**」または「**最少デバッグ出力**」のいずれかを使用するようにしてください。

- **エラー警告を出力**

  このチェックボックスをオンにすると、エラーと警告がデバッグログへ出力されます。

- **最少デバッグ出力**

  このチェックボックスをオンにすると、最小のデバッグログが出力されます。

- **情報デバッグ出力**

  このチェックボックスをオンにすると、情報のデバッグログが出力されます。

- **Ultra Verbose デバッグ出力**

  このチェックボックスをオンにすると、詳細なデバッグログが出力されます。

- **ルールフィルタを出力**

  このチェックボックスをオンにすると、ルールとフィルタエンジンがデバッグログへ出力されます。

循環ログを使用

「**デバッグ出力を有効にする(必要時のみ)**」がオンの場合のみ使用できます。
このチェックボックスをオンにすると、指定したファイル数およびファイルサイズでログファイルを循環させることができます。これによりハードディスクの予期しないオーバーロードを回避することができます。

- **ログファイル数**

  「**循環ログを使用**」がオンの場合のみ使用できます。
  最大のログファイル数を指定します。

- **最大のファイルサイズ(KB)**

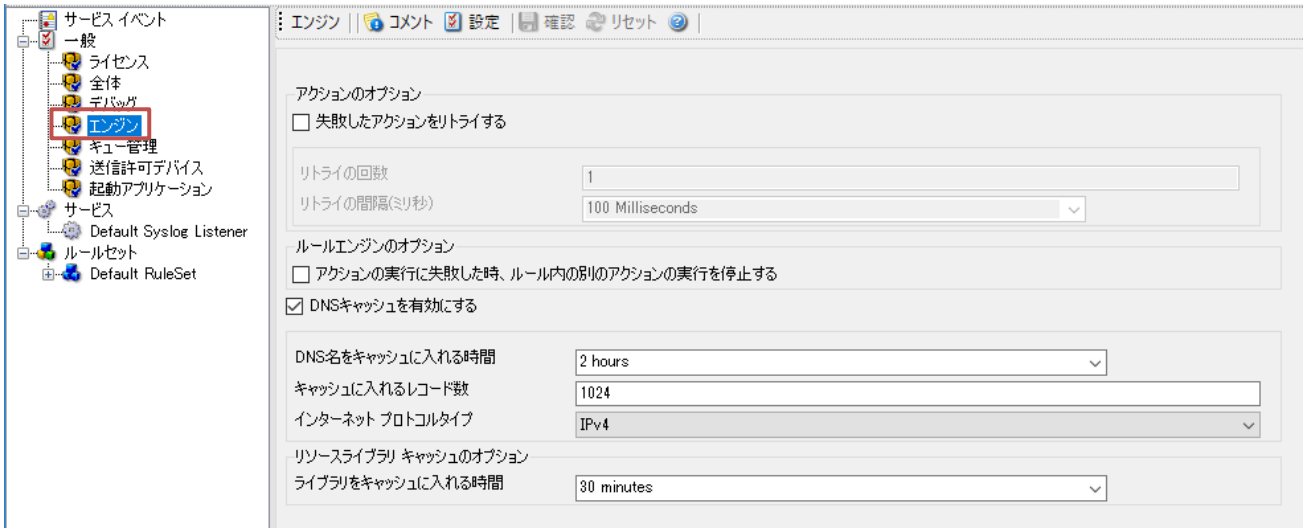
  「**循環ログを使用**」がオンの場合のみ使用できます。
  ファイルの最大サイズ(KB)を指定します。

クラッシュレポート - Adiscon サポートに問題報告を自動的に送信する

このチェックボックスをオンにすると、障害レポートが自動的に Adiscon 社(http://crashdump.adiscon.com)へアップロードされます。障害レポートはサービスが何らかの原因で内部的に停止した場合に生成されます。このレポートは問題を発見し修正するために役立つ小さいダンプファイルで、個人情報は含まれません。また、このダンプファイルは非常に小さく 256Kbyte を超えることはありません。大抵の場合は 32Kbyte です。

5.3.4. エンジン

ここでは「**エンジン**」オプションで使用できる項目について説明します。



以下の項目を設定できます:

アクションのオプション

失敗したアクションをリトライする

このチェックボックスをオンにすると、サービスは「**リトライの回数**」の設定値に達するまで、失敗したアクションを実行します。エラーイベント（ID=114）は最後のリトライが失敗した場合のみ記録されることにご注意ください。それ以前のエラーは、デバッグログ（エラーファシリティ）に記録されます。「**リトライの回数**」と「**リトライの間隔（ミリ秒）**」をカスタマイズできます。

- **リトライの回数**

  リトライの回数を指定します。

- **リトライの間隔（ミリ秒）**

  次のリトライを実行するまでの待ち時間を指定します。

ルールエンジンのオプション

アクションの実行に失敗した時、ルール内の別のアクションの実行を停止する

このチェックボックスをオンにすると、ルールに定義されているアクションのうちの１つが失敗した場合に、そのルールの実行を中止します。オフの場合は、ルール内に複数あるアクションのうち１つが失敗してもルールは停止せず、次のアクションが実行されます。

DNS キャッシュオプション

DNS キャッシュを有効にする

このチェックボックスをオンにすると、DNS キャッシュが使用されます。

DNS キャッシュは、逆引き DNS の検索に使用します。逆引き検索は、IP アドレスをコンピューター名に変換するために使用され、これは「ホスト名の解決」アクションで実行されます。検索のたびに、DNS が照会されるため、（パフォーマンスの観点で）システムへの負荷が比較的大きくなってしまいます。このため、検索結果がキャッシュされます。検索のたびに、システムはまずローカルキャッシュに検索結果が存在するかどうかをチェックします。検索結果がない場合にのみ DNS クエリが実行され、その結果がキャッシュに保存されます。これにより、ホスト名の解決速度が格段に上がります。

しかし、コンピューター名や IP アドレスは変更される場合があります。その場合、変更を反映するために DNS は更新されます。もし、検索結果を永久にキャッシュされると、（結果がキャッシュに存在し DNS クエリが行われないため）新しい情報を得ることができません。この問題を軽減するために、キャッシュレコードの有効期限を指定できます。有効期限が切れたレコードはキャッシュ内に存在していないと認識され、新しく検索されます。

また、キャッシュレコードは、システムメモリを使います。非常に多数の送信元を名前解決したい場合は、より多くのメモリをキャッシュに割り当てる必要が出てくるでしょう。これを解決するために、キャッシュに入れる DNS レコード数の上限を指定することができます。この設定値に達すると、新しいキャッシュレコードは割り当てられず、直近に使用されたレコードが新しいリクエスト結果で上書きされます。

このチェックボックスがオンの場合のみ、以下のオプションを使用できます。

- **DNS 名をキャッシュに入れる時間**

  DNS 名をキャッシュに入れる有効期限を設定します。長い期間を設定すると、名前変更時に問題が生じる可能性があります。短すぎると、DNS 検索が頻繁に発生します。経験則として、IP とホスト名の構成が固定である場合、有効期限を長くすることができます。ただし、24～48 時間を超えるタイムアウトは使用しないことをお勧めします。

- **キャッシュに入れるレコード数**

  キャッシュするレコードの最大数を指定します。デフォルトは、1024 です。システムは必要なレコードの分だけメモリを割当てます。このため、ここで大きな値を設定しても、名前解決を行うホストの数が少ない場合は、キャッシュは大きくなりません。しかし、名前解決を行うホスト数が非常に多い場合は、キャッシュサイズに上限を設定すると便利です。しかしこの場合、引き換えに DNS クエリが頻繁に行われます。1 つのキャッシュレコードにつきおよそ 1～2KB として計算できます。

- **インターネットプロトコルタイプ**

  名前解決の際に IPv4 と IPv6 アドレスのどちらを優先するかを指定します。これは IPv4 と IPv6 の両方の名前を返す場合にのみ影響します。

リソース ライブラリキャッシュオプション

ライブラリをキャッシュに入れる時間

このオプションは、EventReporter のイベントログの監視機能において特に役立つ機能です。同じイベントが何度も処理される状況では、このオプションを使用することでパフォーマンスが大幅に向上します。また、キャッシュはリモートシステムライブラリ（管理用のデフォルト共有が必要）で動作します。デフォルトは 30 分（30 minutes）です。

5.3.5. キュー管理

ここでは「**キュー管理**」オプションで使用できる項目について説明します。

以下の項目を設定できます:

ディスクキャッシュのキュー管理を有効にする

このチェックボックスをオンにすると、アイテムをディスク上の内部キュー（指定したデータファイル）にキャッシュすることができます。

> **警告:**
> この機能は本当に必要な場合のみ使用してください。
> ご利用のマシンのハードディスク速度によっては、アクションの処理速度が低下する場合があります。最悪の場合には、マシンが IO 負荷を処理できなくなり、キューがいっぱいになってしまいます。ディクスキャッシュは、受信したがまだ処理されていない Syslog メッセージを確実に処理したいユーザー向けの追加機能です。

ディスクキャッシュは EventReporter の「イベントログ監視」などアクションが成功している場合のみ継続して動作する種類のサービスからはインフォメーションユニットをキャッシュしません。Syslog サーバーのような他のすべての情報ソースは、このファイルにメッセージをキャッシュします。何らかの理由でサービスまたはサーバーがクラッシュした場合、次回のエージェントの起動時にキューが自動的にロードされるため、キューに入っていたメッセージは失われません。クラッシュ時に処理されていたメッセージのみ失われます。

このチェックボックスがオンの場合のみ、以下のオプションを使用できます。

- **ファイルパス**

  キューファイルの保存場所を指定します。

- **キューファイルサイズ（静的）**

  キューのサイズを指定します。システムメモリより大きいサイズは設定しないでください。システムメモリの合計よりも小さいサイズでご利用になることをお勧めします。最大値は 2048MB です。

  キューファイルのサイズを変更すると、次回のサービス起動時に新たにキューファイルが作成されます。それまで作成されていたキューファイルの内容は新しいファイルに移行されませんので、サイズ変更後はそれまでのキューがきちんと処理されたかどうかを確認してください。また、一般的にサービスを停止した際にも同様にそれまでのキューが処理されます。

  > **注記：**
  > 「**ディスクキャッシュのキュー管理を有効する**」がオンの場合、「**一般**」>「**全体**」>「**キューのリミット**」の設定が重要になります。「**キューファイルサイズ**」を大きくても、キューに保存されるアイテムの最大数は「キューのリミット」の設定値です。

- **処理ポインタ**

  処理ポインタ（ディスクキャッシュのどの位置にポインタが来るか）を指定します。

- **保存ポインタ**

  このポインタは、前回どこの位置で項目が保存されたかを表します。

ワーカースレッドの数

WinSyslog がキューの処理に使用するワーカーバックグラウンドスレッド数を指定します。

5.3.6. 送信許可デバイス

ここでは「**送信許可デバイス**」オプションで使用できる項目について説明します。

注記:

WinSyslog はインストールすると、評価版として動作します。評価版は送信元デバイス数に制限なく(送信元デバイス数は無制限)、30日間無償で全機能を試用できます。送信許可リストの設定は必要ありません。

- 評価期間の30日が経過すると、自動的にフリー(Basic)版へ移行し、Syslog 送信元が最大3台(IP 3つ)に制限されます。**評価期間終了後に、WinSyslog をフリー(Basic)版として使用するには、この画面で送信元デバイスの IP アドレスを設定する必要があります。**WinSyslog Basic フリー版については、別紙「WinSyslog Basic フリー版について」をご参照ください。
- エディション別の機能比較はこちらをご参照ください。

以下の項目を設定できます:

送信許可リストを有効にする

このチェックボックスをオンにすると、すべてのネットワーク関連サービスが、設定された IP アドレスからのメッセージのみを受信するように制限されます。このリストはライセンスの上限にも制限されることにもご注意ください。例えば、フリー版の場合(送信元最大3台)、最初に設定した3台(3 IP)のみが許可されます。このリストへの入力に制限はありませんが、例えば送信元 10IP 制限のライセンスを所有の場合、設定送信許可リスト中の最初の 10 台のみ受け付けられます。

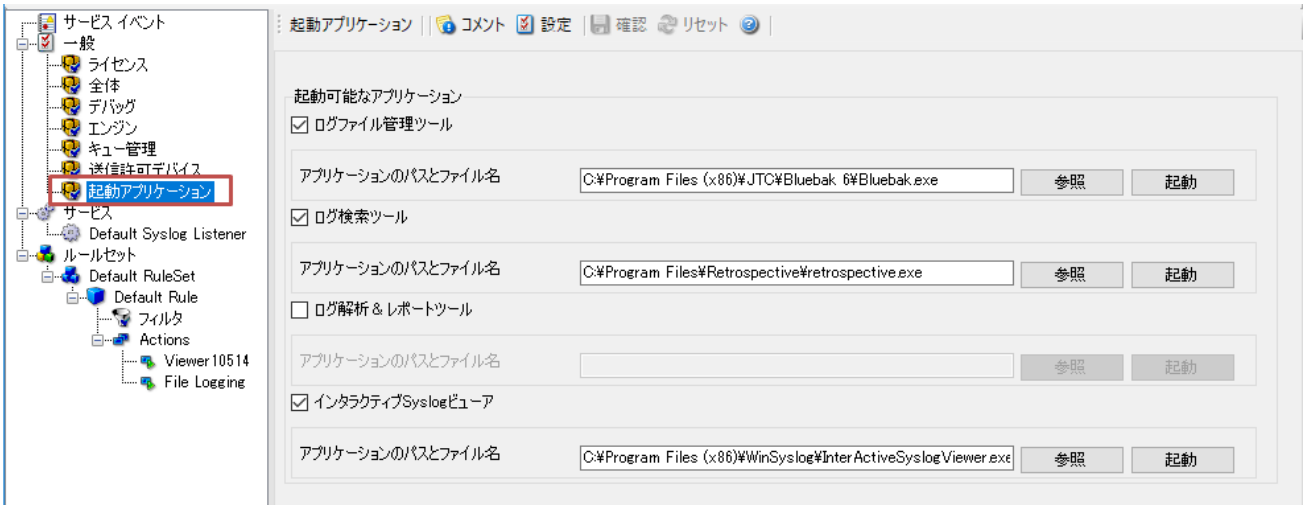
- **次の IP アドレスからの Syslog メッセージのみ受信**

  「**送信許可リストを有効にする**」がオンの場合のみ使用できます。
  このリストに含まれる IP アドレスからの Syslog メッセージのみを受信します。IPv4 または IPv6 アドレスを指定することができます。

5.3.7. 起動アプリケーション

ここでは「**起動アプリケーション**」オプションで使用できる項目について説明します。

この画面では、アプリケーションのランチャー（起動ツール）を設定することができます。



それぞれのアプリケーションの「**起動**」ボタンをクリックすることで、指定したアプリケーションを WinSyslog 設定クライアントから起動することができます。

ログファイル管理ツール

デフォルトでは、バックアップツールが指定されています。必要に応じて変更してください。

ログ検索ツール

デフォルトでは、ログファイル閲覧・検索ツールが指定されています。必要に応じて変更してください。

ログ解析&レポートツール

必要に応じて設定してください。

インタラクティブ Syslog ビューア

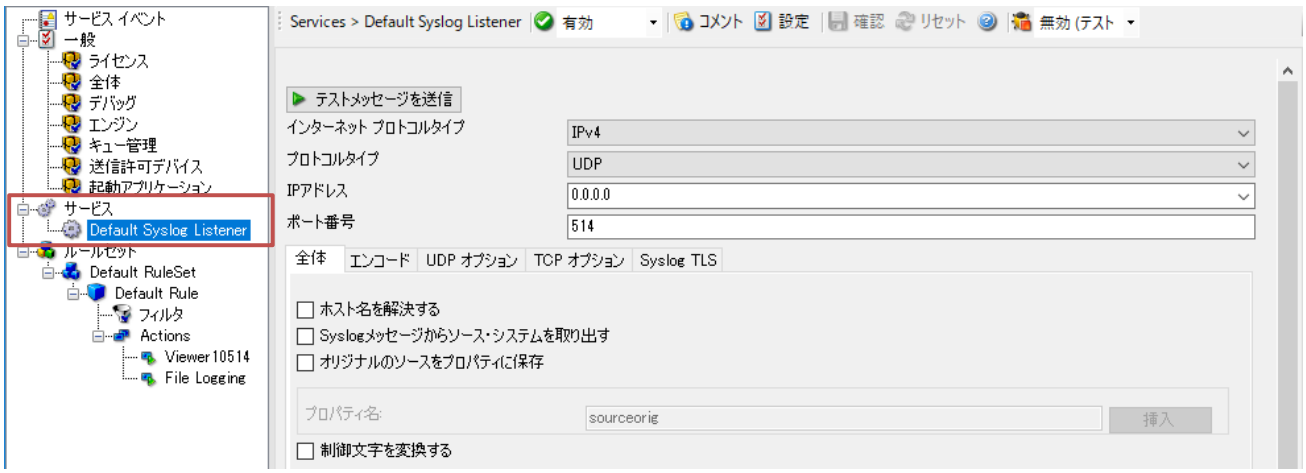
デフォルトではインタラクティブ Syslog ビューアが指定されています。

5.4. サービスオプション

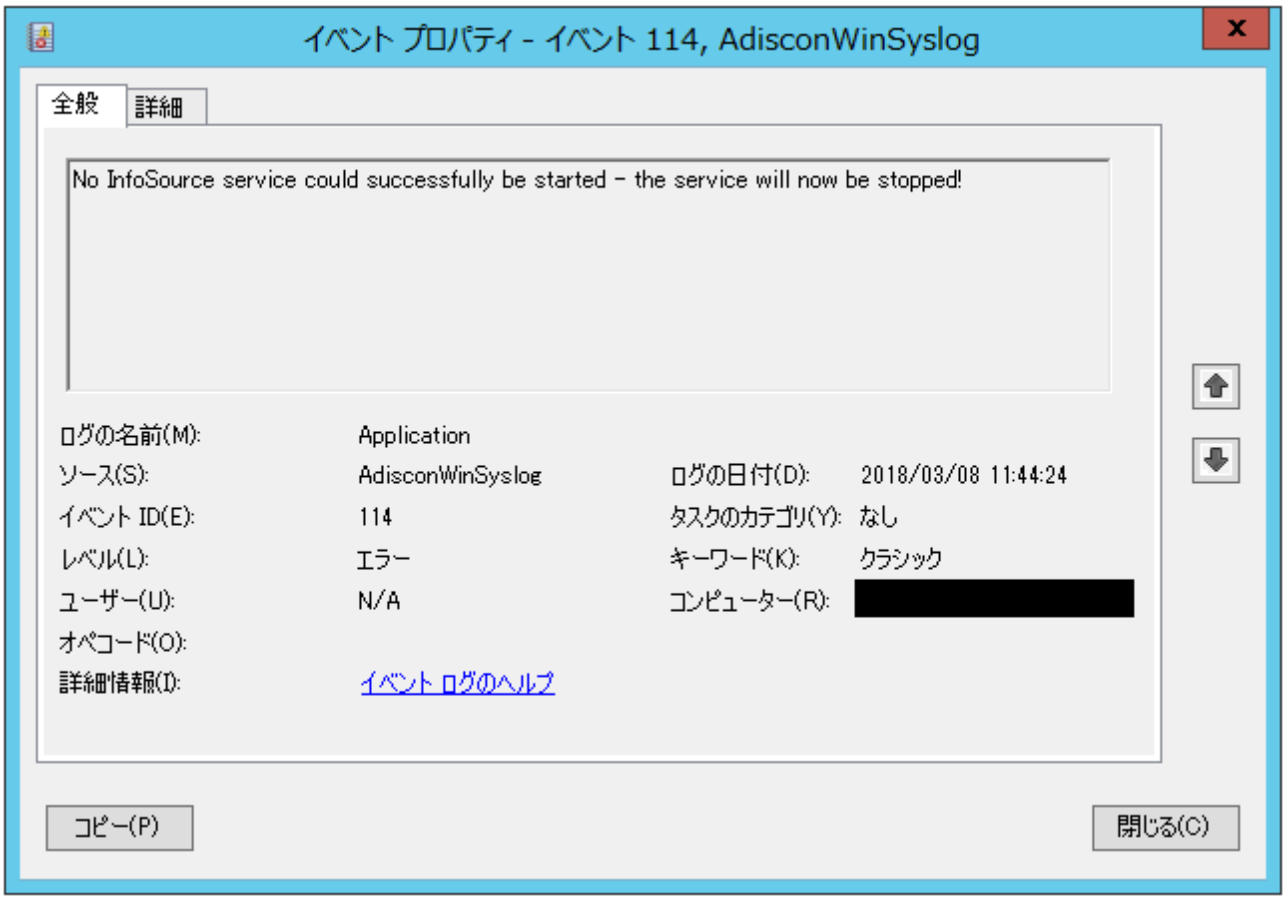
ここでは、設定クライアントのツリービューにある「**サービス**」オプションについて説明します。

5.4.1. サービスとは

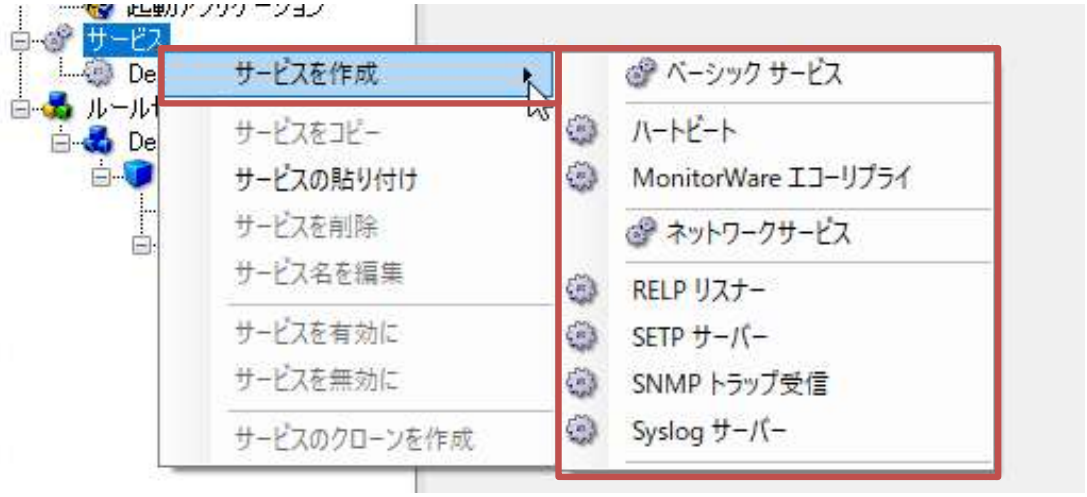
サービスはイベントデータを収集します。例えば、Syslog サーバーサービスは、受信した Syslog メッセージを受け入れます。サービス数に制限はありませんが、同じ設定内容（使用ポートとプロトコル）のサービスを複数稼動させることはできません（その場合、正常に動作しません）。異なる設定内容であれば、同じタイプのサービスを複数稼動させることが可能です。



サービスは少なくとも1つ定義しなければなりません。そうしないと、WinSyslog はイベントデータを収集しないため、全く役に立ちません。有効なサービスが1つも存在しない場合、以下のようなメッセージがイベントログに記録されます。

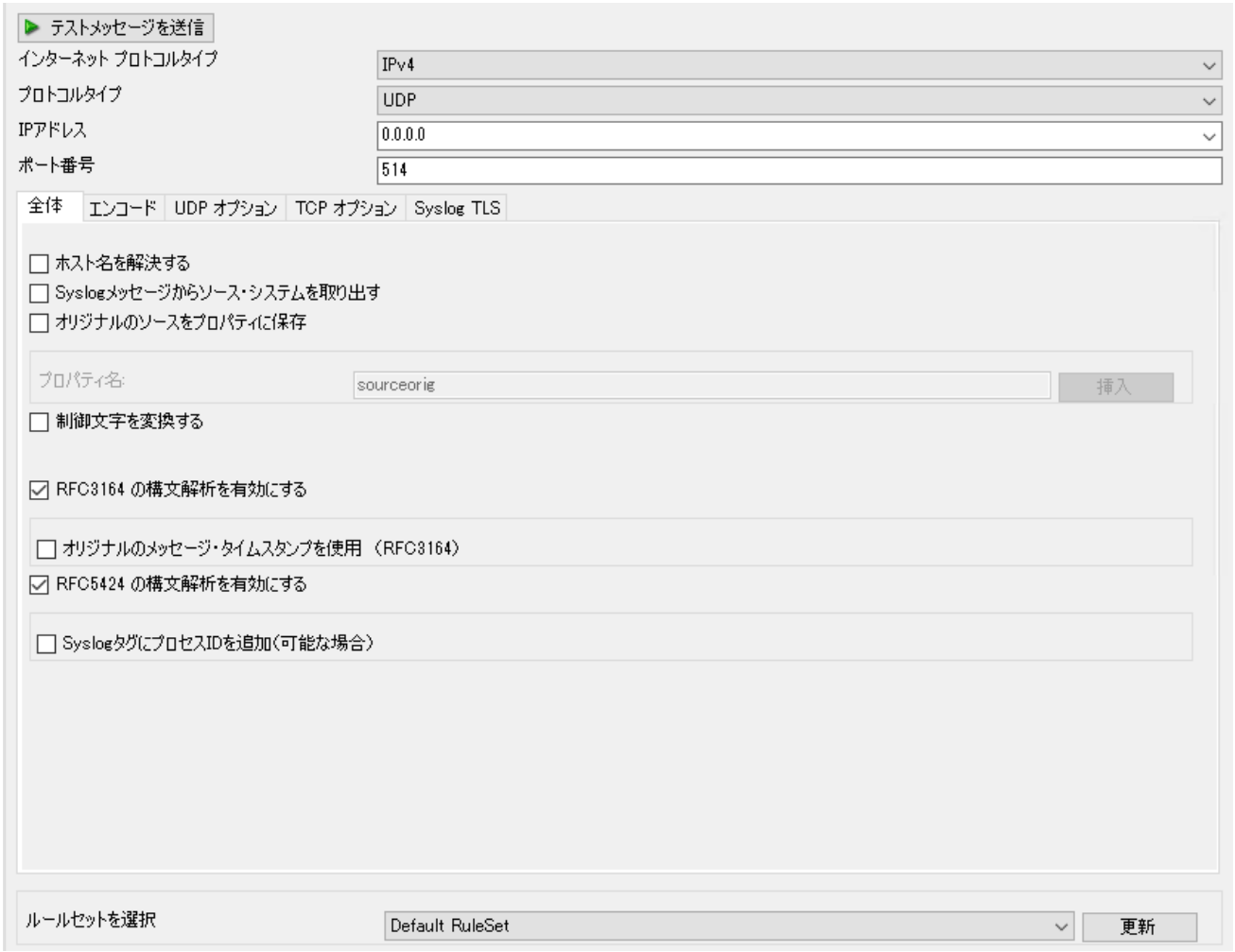


新しいサービスは、ツリービュー上の「**サービス**」を右クリックして「**サービスを作成**」を選択し、希望のサービスタイプを選択することで追加できます。



5.4.2. Syslog サーバー

ここでは Syslog サーバーサービスについて説明します。Syslog サーバーサービスを使用すると、任意の有効なポートで Syslog メッセージをリスンすることができます。UDP と TCP 通信の両方がサポートされます。



以下の項目を設定できます:

インターネット プロトコルタイプ

使用したいプロトコルタイプを選択します。IPv4 と IPv6 を利用できます。IPv6 プロトコルを使用する場合は、適切にインストールする必要があります。1つのサービスでは IPv4 または IPv6 のどちらか1つしか扱えないため、両方のプロトコルを使用する場合(IPv4 と IPv6 が混在する環境の場合)は、サービスを IPv4 用と IPv6 用の2つ作成する必要があります。

プロトコルタイプ

Syslog メッセージは、UDP、TCP、RFC3195 RAW で受信できます。1つのサービスは1つのプロトコルを使用できます。一般的に、Syslog メッセージは UDP プロトコルを介して受信されるため、デフォルトは UDP に設定されています。Syslog サーバーは、UDP 以外にも TCP や RFC3195 RAW に準拠した TCP で送信された Syslog メッセージを受信することも可能です。

> **注記:**
> TCP、RFC3195 は、Professional 版と Enterprise 版でのみ利用できます。フリー版および Basic 版では利用できません。

IP アドレス

Syslog サーバーサービスを特定の IP アドレスにバインドできます。IPv4、IPv6 アドレス、または IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを使用できます。この機能は、異なる IP アドレスで異なる Syslog サーバーを実行するマルチホーム環境で役立ちます。デフォルトは「0.0.0.0」です。「0.0.0.0」はすべて（ANY）の IP アドレスを意味します。

ポート番号

Syslog サーバーが使用するポート番号を指定します。標準のポート番号は 514 です。変更しなければいけない理由が明確である場合のみ、変更を行って下さい。そのような必要性は、概してセキュリティに対する懸念から生じます。ポートの変更を行った場合は、すべてのレポートデバイス（ルーター、プリンタなど）も非標準ポートを使用するように設定する必要があります。

全体タブ

ここでは、「**全体**」タブの設定項目について説明します。

ホスト名を解決する

このチェックボックスをオンにすると、DNS を介してソースシステム（Syslog 送信元）のホスト名が取得されます。オフの場合は、IP アドレス自体が名前として使用されます。

> **注記：**
> 「Syslog メッセージからソースシステムを取り出す」がオンの場合は、この設定は機能しませんので、ご注意ください。この場合は、ホスト名は常に Syslog メッセージ自体から取り出されます。

Syslog メッセージからソースシステムを取り出す

このチェックボックスをオンにすると、ソースシステムの名前または IP アドレスは（RFC 3164 による）Syslog メッセージから抽出されます。オフの場合は、メッセージを受信したアドレスに基づいて生成されます。

オリジナルのソースをプロパティに保存

このチェックボックスをオンにすると、オリジナル（元）のネットワークソースがカスタム定義されたプロパティ（デフォルトでは%sourceorig%）に保存されるようになります。この場合、オリジナルのネットワークソースをもとにフィルタリングすることができます。

- **プロパティ**

  「**オリジナルのソースをプロパティに保存**」がオンの場合にのみ使用できます。オリジナルのソースを保存するプロパティを指定します。

制御文字を変換する

制御文字は特殊文字です。これらは例えばビープ音やその他の非印刷用途に使用されます。通常、Syslog メッセージには制御文字を含めるべきではありません。もし含む場合、制御文字が最終的にロギングに影響を及ぼす可能性があります。ただし、制御文字が必要な場合もあります。

このチェックボックスをオンにすると、制御文字が ASCII 文字 ID の 5 バイトシーケンスに置換されます。例えば、ビープ音は ASCCII BEL 文字です。BEL には数字コード 7 が割当てられているため、このチェックボックスをオンにすると、Syslog メッセージの中で<007>に変換されます。オフの場合は、変換は行われません。

いずれにせよ、ASCII NUL はログファイルのセキュリティ問題を防ぐために <000>に変換されます。

> **注記：**
> 日本語など2バイト文字セットを使用している場合は、制御文字をエスケープするとメッセージが壊れてしまう可能性が高いので、この機能は使用しないようにして下さい。

RFC3164 の構文解析を有効にする

このチェックボックスをオンにすると、RFC3164 準拠のメッセージ解析が有効になります。オフにすると従来の Adiscon メッセージ解析が使用されます。送信元のホスト名やタイムスタンプが正常に処理されない場合は、オフにすることをお勧めします。既存の多くのデバイスが RFC3164 に完全に準拠していないため、これらの問題が引き起こされる可能性があります。RFC3164 に準拠しない Syslog メッセージを受信する場合は、オフにしてください。

- **オリジナルのメッセージ・タイムスタンプを使用 (RFC3164)**

  「**RFC3164 の構文解析を有効にする**」がオンの場合のみ使用できます。
  このチェックボックスをオンにすると、WinSyslog はメッセージ受信時刻の代わりに、(RFC3164 に基づいて)Syslog メッセージからタイムスタンプを抽出します。オフの場合は、タイムスタンプはローカルのシステム時刻に基づいて生成されます。Syslog メッセージのタイムスタンプには、タイムゾーン情報が含まれていません。このため、複数のタイムゾーンにあるデバイスからメッセージを受信する場合は、オフにすることを強くお勧めします。

RFC5424 の構文解析を有効にする

このチェックボックスをオンにすると、Syslog RFC5424 ヘッダーの検出と復号で RFC5424 に準拠したメッセージの解析が可能になります。また、新しい Syslog プロパティも含まれます。

オフの場合は、従来の Adiscon メッセージ解析が選択されます。送信元のホスト名やタイムスタンプが正常に処理されない場合は、このチェックボックスをオフにすることをお勧めします。既存の多くのデバイスが RFC5424 に完全に準拠していないため、これらの問題が引き起こされる可能性があります。RFC5424 に準拠しない Syslog メッセージを受信する場合は、オフにしてください。

- **Syslog タグにプロセス ID を追加(可能な場合)**

  「**RFC5424 の構文解析を有効にする**」がオンの場合にのみ使用できます。
  このチェックボックスをオンにすると、Syslog タグに、プロセス名だけでなくプロセス ID(pid)も追加されるようになります。

「エンコード」タブ

ここでは、「**エンコード**」タブの設定項目について説明します。

メッセージのエンコードを自動検出する (UTF-8, SHIFT_JIS, EUC-JP)

このチェックボックスをオンにすると、異なるエンコーディングのメッセージがチェックされます。日本語などマルチバイト文字を含む Syslog メッセージを処理する場合には、このチェックボックスをオンにしてください。エンコーディングが検出されると、自動的に UTF16 に変換されます。

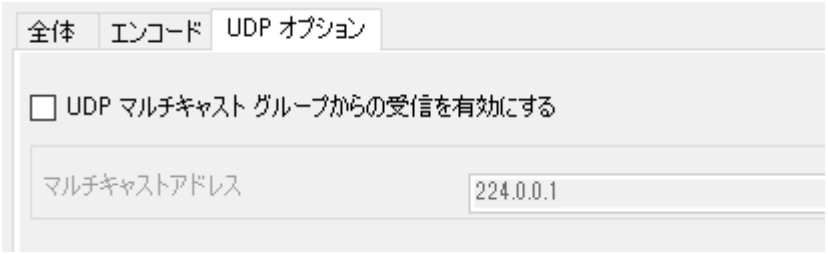
- **メッセージの文字コードを全て UTF-8 として処理する**

  このチェックボックスをオンにすると、すべての受信メッセージの UTF8 デコーディングを強制します。この機能は、UTF8 でエンコードされた BOM なしの Syslog メッセージの処理に役立ちます。BOM を含まない UTF-8 の Syslog メッセージを受信する際は、このチェックボックスをオンにしてください。

> **注記:**
> すべてのメッセージが UTF-8 として扱われるため、他の文字コードで送信されてきた Syslog メッセージは正しく処理されない可能性があります。

UDP オプションタブ

ここでは、「**UDP オプション**」タブの設定項目について説明します。



UDP マルチキャスト グループからの受信を有効にする

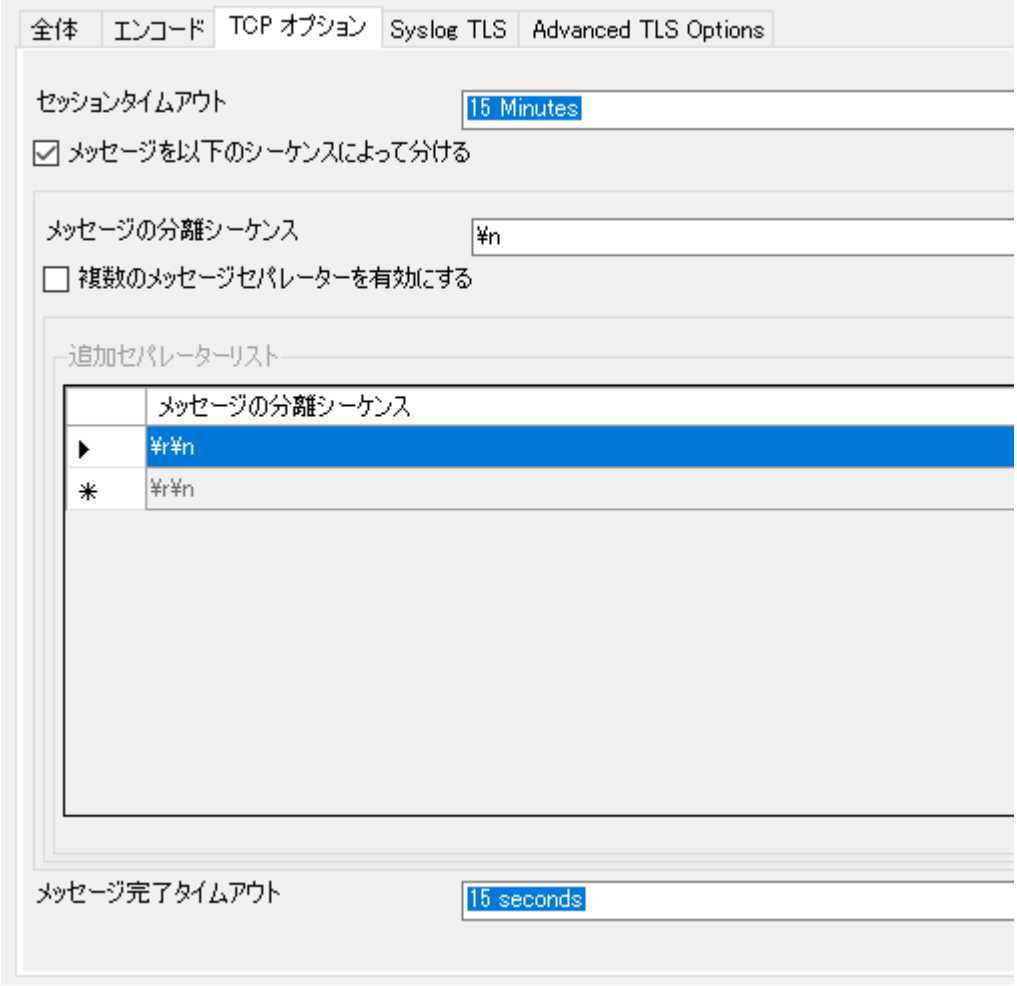
このチェックボックスをオンにすると、マルチキャスト IP アドレス（例： 224.0.0.1）からの Syslog メッセージを受信することができます。

- **マルチキャストアドレス**

  「**UDP マルチキャスト グループからの受信を有効にする**」がオンの場合にのみ使用できます。
  例えば 224.0.0.1 などのマルチキャストアドレスを使用して Syslog メッセージを受信するときに指定します。

TCP オプションタブ

ここでは、「**TCP オプション**」タブの設定項目について説明します。



セッションタイムアウト

TCP 固有のオプションの 1 つが、セッションタイムアウトです。ここでは、データの最後のパッケージが送信された後、TCP セッションを開いたままにする期間を設定します。プルダウンメニューから値を選択するか、「Custom」を選択して任意の値（ミリ秒）を指定できます（最大は 2147483646）。セッションタイムアウトを無効にする場合は、「Custom」を選択して「0」と入力します。。

メッセージを以下のシーケンスによって分ける

このチェックボックスをオンにすると、複数のメッセージを使用することができます。また、以下のオプションを使用できるようになります。

- **メッセージ分離のシーケンス**:

  メッセージをどのように分離するかを指定します。ほとんどの場合、メッセージは改行（キャリッジリターンと（または）ラインフィード）で終了します。しかし、ここで独自の分離シーケンスを設定することができます。

- **複数のメッセージセパレーターを有効にする**

  複数のメッセージセパレーターを設定する場合は、このチェックボックスをオンにし、「**追加セパレーターリスト**」に追加します。

  - **追加セパレーターリスト**

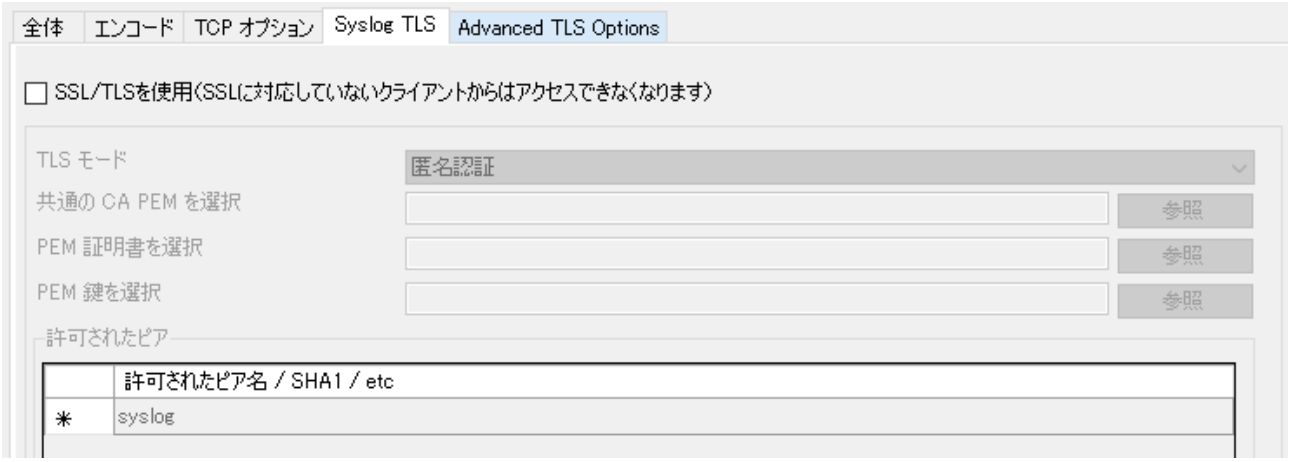
    リストには、デフォルトで「¥r¥n」（改行コード CR+LF）が設定されています。

メッセージ完了タイムアウト

ここではメッセージを完了させる時間を設定します。ここで設定した時間内に処理されなかったメッセージは、次の（新しい）メッセージとして分けて処理されます。カウンタは毎回リセットされ、新しいメッセージが開始されます。プルダウンメニューから値を選択するか、「Custom」を選択して任意の値（ミリ秒）を入力します（最大 2147483646）。「0」を入力すると、無効になります。

Syslog TLS タブ

ここでは、「**Syslog TLS**」タブの設定項目について説明します。

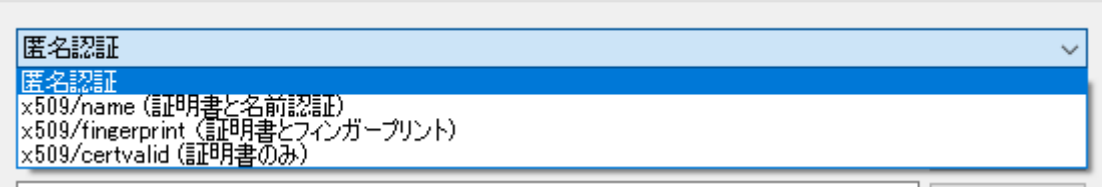


SSL/TLS を使用（SSL に対応していないクライアントからはアクセスできなくなります）

このチェックボックスをオンにすると、Syslog サーバーの SSL/TLS 暗号化が有効になります。SSL/TLS に対応していないデバイス（クライアント）からのメッセージを受信できなくなります。
オンにした場合は、以下のオプションを使用できます。

- **TLS モード**

  認証モードを次のモードから選択します。



- **匿名認証**
  デフォルトで選択されています。どんな証明書でも(証明書がない場合でも)受信できます。
- **x509/name(証明書と名前認証)**
  「**許可されたピア**」リストのクライアント証明書の subject がチェックされます。それによりセキュリティで保護された接続のみ許可されるようになります。
- **x509/fingerprint(証明書とフィンガープリント)**
  受信したクライアント証明書から SHA1 フィンガープリントを作成し、「**許可されたピア**」リストのフィンガープリントと比較します。デバッグログを使用して、許可されなかったクライアント証明書のフィンガープリントを確認することができます。
- **x509/certvalid(証明書のみ)**
  クライアント証明書が有効でありさえすれば接続が許可されます。

- **共通の CA PEM を選択**

  CA(Certificate Authority:認証局)からの証明書を選択します。Syslog の送信側と受信側で同じ CA を使用しなければなりません。

- **PEM 証明書を選択**

  クライアント証明書(PEM フォーマット)を選択します。

- **PEM 鍵を選択**

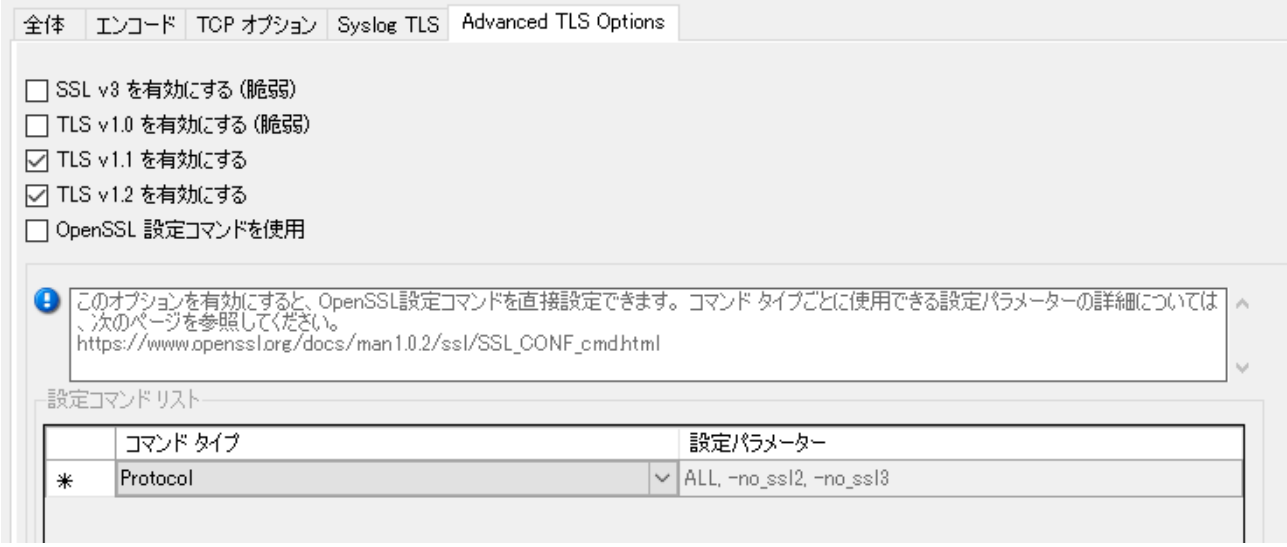
  クライアント証明書の鍵ファイル(PEM フォーマット)を選択します。

- **許可されたピア**

  このリストには、許可されているすべてのピアが含まれます。「**x509/name**」が使用されている場合は、クライアント証明書の subject の一部を含むことができます。例えば、証明書の subject に CN = secure.syslog.msg が含まれている場合、secure.syslog.msg を許可されたピアとして追加できます。「**x509/fingerprint**」が使用されている場合は、許可された SHA1 フィンガープリントのリストを保持できます。フィンガープリントは、OpenSSL ツールで生成することもできますが、デバッグログファイルから取得することもできます。形式は RFC542 で記述されています。
  例: SHA1:2C:CA:F9:19:B8:F5:6C:37:BF:30:59:64:D5:9A:8A:B2:79:9D:77:A0

Advanced TLS Options タブ

ここでは、「**Advanced TLS Options**」タブの設定項目について説明します。



暗号化方式を選択します。

暗号化方式を選択します。以下の 4 つの項目をそれぞれチェックボックスで設定できます。

- ・SSL v3 を有効にする（脆弱）
- ・TLS v1.0 を有効にする（脆弱）
- ・TLS v1.1 を有効にする
- ・TLS v1.2 を有効にする

OpenSSL 設定コマンドを使用する。

このオプションを有効にすると、OpenSSL 設定コマンドを直接設定できます。 コマンド・タイプごとに使用可能な構成パラメーターの詳細については、以下のリンクを参照してください。
https://www.openssl.org/docs/man1.0.2/ssl/SSL_CONF_cmd.html

ルールセットを選択

このサービスで使用するルールセットの名前を選択します。ルールセット名は有効なルールセットでなければなりません。

5.4.3. SETP サーバー

ここでは SETP サーバーサービスについて説明します。

> **注記：** SETP サーバーサービスは Enterprise 版でのみ利用できます。

SETP サーバーは、他のシステムからイベントを確実に受信するために MonitorWare 製品ライン内で使用されます。SETP は送信元からオリジナルのメッセージを受け取り、送信元が設定した正確な設定を使用するため、設定オプションはごくわずかです。SETP サーバー側では変更は発生しません。したがってメッセージフォーマットのために設定する値はありません。

以下の項目を設定できます:

インターネット プロトコルタイプ

使用したいプロトコルタイプを選択します。IPv4 と IPv6 を利用できます。IPv6 プロトコルを使用する場合は、適切にインストールする必要があります。1つのサービスでは IPv4 または IPv6 のどちらか1つしか扱えないため、両方のプロトコルを使用する場合(IPv4 と IPv6 が混在する環境の場合)は、サービスを IPv4 用と IPv6 用の 2 つ作成する必要があります。

リスナー ポート

SETP サーバーが使用するポート番号を指定します。デフォルトは、5432 です。変更しなければいけない理由が明確である場合のみ、変更を行って下さい。そのような必要性は、概してセキュリティに対する懸念から生じます。SETP には TCP が使用されます。ポートの変更を行った場合は、送信側の設定も変更してください。

リスナーIP アドレス

SETP サーバーサービスを特定の IP アドレスにバインドできます。IPv4、IPv6 アドレス、または IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを使用できます。この機能は、異なる IP アドレスで異なる SETP サーバーを実行するマルチホーム環境で役立ちます。デフォルトは「0.0.0.0」です。「0.0.0.0」はすべて(ANY)の IP アドレスを意味します。

セッションタイムアウト

サーバー側のセッションをオープン状態とする時間を指定します。

SSL/TSL を使用（SSL に対応していないクライアントはアクセスできなくなります）

このチェックボックスをオンにすると、アクションが SSL/TLS SETP サーバーに接続します。

> **注記：**
> このチェックボックスをオンにすると、SSL に対応していない SETP サーバーへ接続できなくなります。

データの圧縮に zLib 圧縮を使用する

このチェックボックスをオンにすると、SETP 送信元によって送信された zLib 圧縮データを解凍します。オンにしても、通常のデータも受信できます。zLib 圧縮は、WAN 環境において通信量を減少させることに役立ちます。

ルールのエラーを送信者に通知する

このオプションをオンにすると、アクションの結果を SETP メッセージの送信元へ通知します。

この通信は受信側で実行されたアクションのステータスをイベントの送信側に戻します。本質的には、送信側システムはアクションがリモートマシン上で失敗したか、成功したかを知ることができます。ローカルマシン上で実行されたアクションとまったく同じように動作します。障害状態の正確な処理はイベントソースにより異なります。

例： EventReporter でイベントログを監視し、SETP を介してこれらのイベントを送信、一方で受信イベントをデータベースに書き込むよう設定しているとします。もしデータベースがオフラインになりイベントを書き込めない場合、（このチェックボックスがオンであれば）SETP サーバーはアクションが失敗した最後のメッセージを返し、ID 1005 のエラーイベントを生成します（その後、このアクションが成功した場合には、ID 1012 のイベントを生成します）。送信側はその後、イベントを停止して再試行します。これは、SETP が TCP と同様にデータ転送を保証するように構築されているためですが、次のアクションが成功した場合には送信側にステータスを返すことができます。

これは、「イベントログの監視」サービスが再起動可能なイベントソースであるために発生します。アクションの結果を使用して、同じソースの別の実行でアクションが再試行されるかどうかを判断します。他のイベントソースは、異なる動作をします。例えば、「Syslog サーバー」サービスは、失敗したアクションを再試行しません。これは、Syslog メッセージは消失する可能性があるという性質によるものです。

> **注記：**
> このチェックボックスをオンにすると、WinSyslog v7.2 および EventReporter v8.2 以前のバージョンは、ルールの例外が発生したときに SETP でデータを送信する際に問題が発生する可能性があります。この機能を使用する場合は、WinSyslog v7.3.x および EventReporter v8.3.x 以上であることを確認してください。

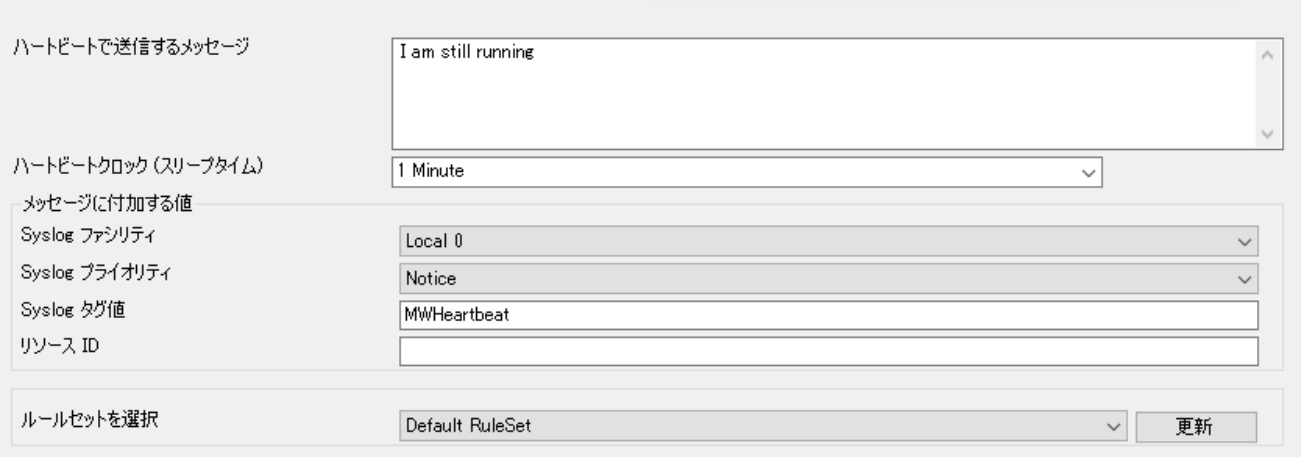
ルールセットを選択

このサービスで使用するルールセットの名前を選択します。ルールセット名は有効なルールセットでなければなりません。

5.4.4. ハートビート

ここではハートビートサービスについて説明します。

ハートビートサービスを使用することで、WinSyslog サービスが稼動しているかどうかを継続的に確認することができます。指定した時間間隔ごとにインフォメーションユニットを生成します。このインフォメーションユニットは別のシステムに転送することができます。指定した時間間隔内で追加のパケットを受信しない場合、送信側に問題が発生しているかすでに実行が停止している可能性が疑われます。



以下の項目を設定できます:

ハートビートで送信するメッセージ

インフォメーションユニット内のテキストとして使用されるメッセージです。入力する内容は、どんなものでも構いません。このメッセージテキストには特別な意味はありません。適当と考える値を入力してください。

ハートビートクロック(スリープタイム)

ハートビートサービスがインフォメーションユニットを生成する間隔(ミリ秒)を指定します。受信側は寛大であるべきということにご注意ください。ここで指定された間隔はパケット間の最小時間です。高負荷環境においては、生成間隔が設定より少し長くなる場合があります。システムでサービスヘルスの監視により、サービスが疑わしいとみなされる前に、この間隔を 2 倍にすることをお勧めします。

メッセージに付加する値

Syslog ファシリティ

ハートビートサービスによって作成されるイベントに割り当てられる Syslog ファシリティを指定します。メッセージを Syslog サーバーに転送する際に役立ちます。

Syslog プライオリティ

ハートビートプロセスによって作成されるイベントに割り当てられる Syslog プライオリティ（Severity）です。メッセージを Syslog サーバーに転送する際に役立ちます。

Syslog タグ値

ハートビートプロセスによって作成されるイベントに割り当てられる Syslog タグ値です。メッセージを Syslog サーバーに転送する際に役立ちます。

リソース ID

ハートビートプロセスによって作成されるイベントに割り当てられるリソース ID です。メッセージを Syslog サーバーに転送する際に役立ちます。

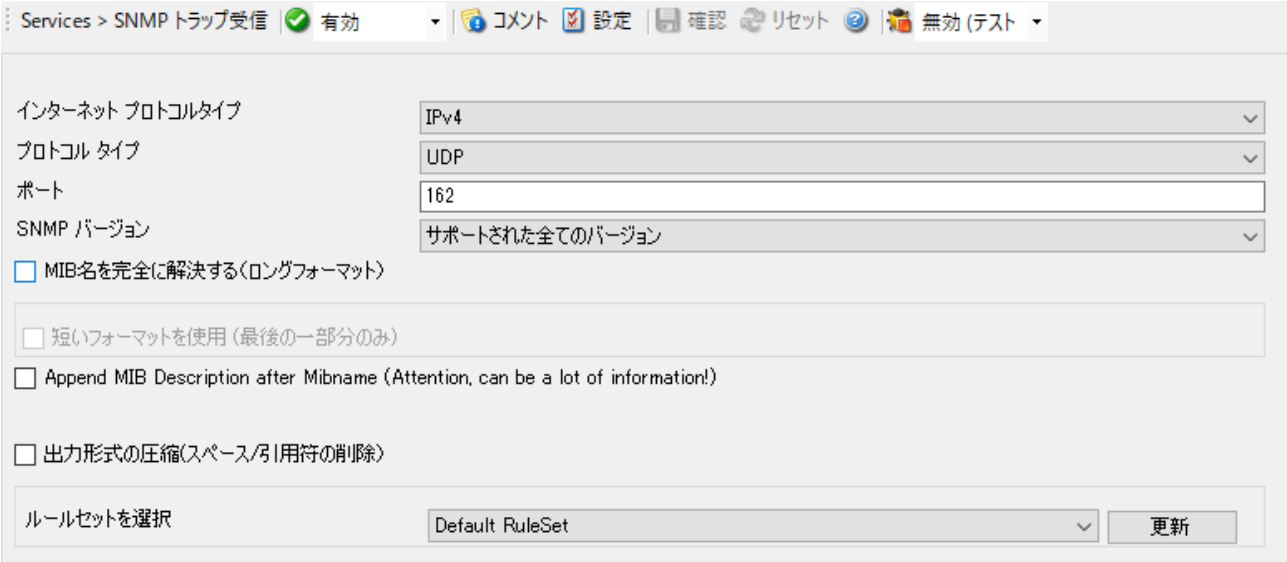
ルールセットを選択

このサービスで使用するルールセットの名前を選択します。ルールセット名は有効なルールセットでなければなりません。

5.4.5. SNMP トラップ受信

ここでは SNMP トラップ受信サービスについて説明します。

SNMP トラップ受信サービスによって、SNMP メッセージを受信することができます。トラップは、別のプロトコル（SNMP）を使う Syslog メッセージのようなものです。トラップはデバイスが送信すべき情報があると感じたときに生成され、デバイスが送信すべきであると感じる情報を含みます。その情報には、バージョンやコミュニティなどいくつかの標準項目が含まれます。



以下の項目を設定できます:

インターネット プロトコルタイプ

使用したいプロトコルタイプを選択します。IPv4 と IPv6 を利用できます。IPv6 プロトコルを使用する場合は、適切にインストールする必要があります。1つのサービスでは IPv4 または IPv6 のどちらか1つしか扱えないため、両方のプロトコルを使用する場合(IPv4 と IPv6 が混在する環境の場合)は、サービスを IPv4 用と IPv6 用の 2 つ作成する必要があります。

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 トラップ受信サーバーが使用するポート番号を指定します。よくわからない場合は、デフォルトの 162 のままにしてください。162 は標準ポートです。

SNMP バージョン

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 と SNMP バージョン 2c のみ。
- **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）

このチェックボックスをオンにすると、クライアント MIB ブラウザアプリケーションのように MIB 名を解決します。

- **短いフォーマットを使用（最後の一部分のみ）**

  「**MIB 名を完全に解決する（ロングフォーマット）**」がオンの場合にのみ使用できます。
  完全に名前解決された MIB 名は長く読みづらくなる場合があります。このチェックボックスをオンにすると、MIB 名の最後の部分だけになるよう短縮します。

Append MIB Descripttion after Mibname (Attention, can be a lot of information!)

このチェックボックスをオンにすると、出力に SNMP OID 記述を含めることができます。

出力形式の圧縮（スペース/引用符の削除）

このチェックボックスをオンにすると、出力フォーマットはスペースや引用符が削除され、縮小されて、コンマで区切られます。
出力例:

source=127.0.0.1, community=public, version=Ver2,
iso.3.6.1.2.1.1.3.0=Timeticks: (3493305159) 404 days, 7:37:31.59,
iso.3.6.1.6.3.1.1.4.1.0=OID: iso.3.6.1.4.1.19406.1.2.2,
iso.3.6.1.4.1.19406.1.1.1.7=This is a SyslogTest

ルールセットを選択

このサービスで使用するルールセットの名前を選択します。ルールセット名は有効なルールセットでなければなりません。

注記:

受信トラップの管理は、例えば Syslog サーバーと同じように動作します。受信トラップは対応するルールセットに転送され、ルールに従って処理されます。"Community", "Version", "Value"などの一般的な情報をフィルタリングすることができます。最後にアクションによって処理されます。SNMP エージェントは Windows SNMP エージェントと共存でき、その機能を妨げません。Windows SNMP エージェントは 161 ポートを使用しますが、WinSyslog は 162 ポートを使用します。

内部処理では、受信した SNMP メッセージの変数が新しいプロパティに追加されます。これらのプロパティ名は%snmp_var_x%で、x の値は 1 から開始します。これらのカスタムプロパティは、フィルタリングやプロパティの使用や印刷が可能なあらゆる場所で使用できます。例えば「メール送信」アクションを作成することができます。ここでメッセージ内容を自由に指定することができます。

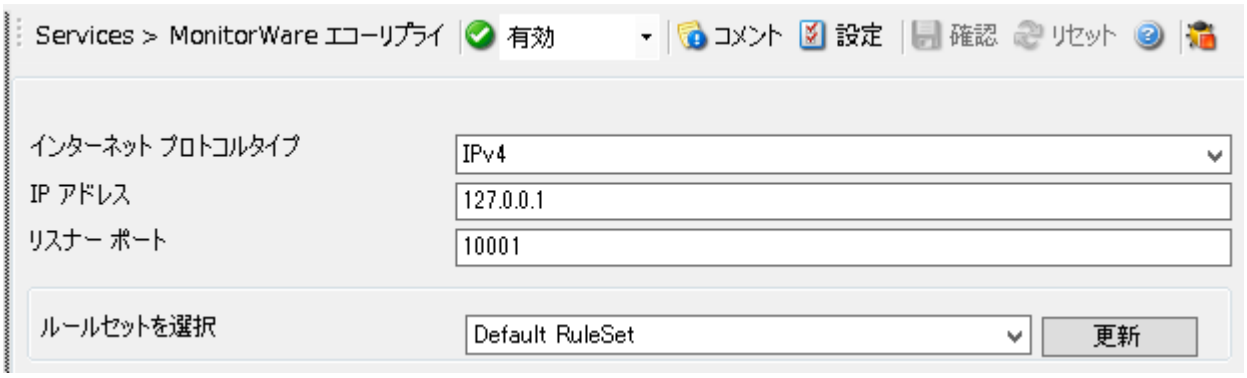
例: 下図の場合、SNMP トラップの 5 番目のプロパティがメッセージに挿入されます。

5.4.6. MonitorWare エコーリプライ

ここでは MonitorWare エコーリプライサービスについて説明します。

メモ: この機能は、MonitorWare エージェントに関連するものです。MonitorWare は Adiscon 社の製品ですが弊社での取り扱いはありません。

MonitorWare エコーリプライサービスは、インストールされた各 WinSyslog で使用されます。MonitorWare エージェントを実行している中央エージェントがエコー要求を使用しており、他の各 WinSyslog サービスをポーリングするように指示しています。要求が正常に実行されない場合、アラートが生成されます。MonitorWare エコープロトコルは、リモートの WinSyslog サービスの新しいプローブが常に実行されていることを確認します。



以下の項目を設定できます:

インターネット プロトコルタイプ

使用したいプロトコルタイプを選択します。IPv4 と IPv6 を利用できます。IPv6 プロトコルを使用する場合

は、適切にインストールする必要があります。1つのサービスでは IPv4 または IPv6 のどちらか1つしか扱えないため、両方のプロトコルを使用する場合（IPv4 と IPv6 が混在する環境の場合）は、サービスを IPv4 用と IPv6 用の 2 つ作成する必要があります。

IP アドレス

MonitorWare エコーリプライサービスは、特定の IP アドレスにバインドできます。IPv4、IPv6 アドレス、または IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを使用できます。この機能は、異なる IP アドレスで異なる MonitorWare エコーリプライサービスを実行するマルチホーム環境で役立ちます。デフォルトは「127.0.0.1」です。「0.0.0.0」はすべて（ANY）の IP アドレスを意味します。

リスナーポート

MonitorWare エコーリプライサービスが使用するポート番号を指定します。

ルールセットを選択

このサービスで使用するルールセットの名前を選択します。ルールセット名は有効なルールセットでなければなりません。

5.4.7. RELP リスナー

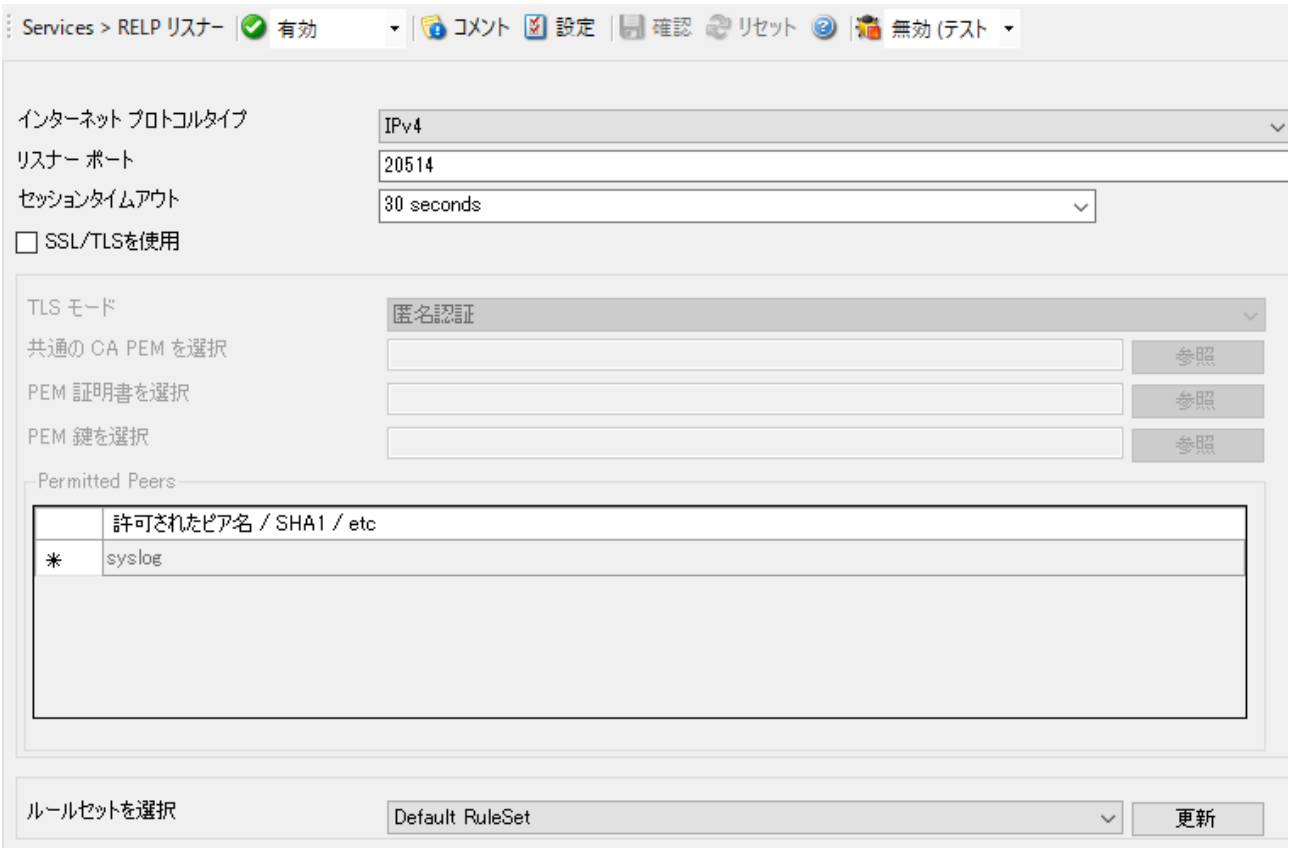
ここでは RELP リスナーサービスについて説明します。

> **注記：** RELP リスナーサービスは Enterprise 版でのみ利用できます。

RELP リスナーサービスは、新しいプロトコルである RELP（Reliable Event Logging Protocol）に対応しています。このプロトコルを使用することで、従来の TCP Syslog プロトコルより確実な転送が可能となります。

> **メモ：**
> RELP（Reliable Event Logging Protocol）は、転送中のメッセージがロストしないよう設計されたプロトコルです。現行バージョンの RELP プロトコルは、接続が切れた場合でもメッセージを複製できる可能性があります。

このサービスは、RELP に対応した送信元からのメッセージを受信します。RELP プロトコルを使用すること以外は、機能的には Syslog サーバーサービスと同じような働きをします。



以下の項目を設定できます:

インターネット プロトコルタイプ

使用したいプロトコルタイプを選択します。IPv4 と IPv6 を利用できます。IPv6 プロトコルを使用する場合は、適切にインストールする必要があります。1つのサービスでは IPv4 または IPv6 のどちらか1つしか扱えないため、両方のプロトコルを使用する場合(IPv4 と IPv6 が混在する環境の場合)は、サービスを IPv4 用と IPv6 用の 2 つ作成する必要があります。

リスナーポート

RELP リスナーサービスで使用するポート番号をここで指定します。デフォルトは、20514 です。この値は変更できますが、その際は、メッセージを送信している機器のポートも合わせて変更するようにしてください。

セッションタイムアウト

ここでは、サーバー側のセッションを開いたままにする期間を設定します。プルダウンメニューから値を選択するか、「**Custom**」を選択して任意の値(ミリ秒)を指定できます(最大は 2147483646)。セッションタイムアウトを無効にする場合は、「**Custom**」を選択して「0」と入力します。

SSL/TLS を使用

このチェックボックスをオンにすると、Syslog サーバーの SSL/TLS 暗号化が有効になります。SSL/TLS に対応していないデバイス（クライアント）からのメッセージを受信できなくなります。
チェックをオンにした時の詳細設定項目は「Syslog TLS」をご参照ください。

ルールセットを選択

このサービスで使用するルールセットの名前を選択します。ルールセット名は有効なルールセットでなければなりません。

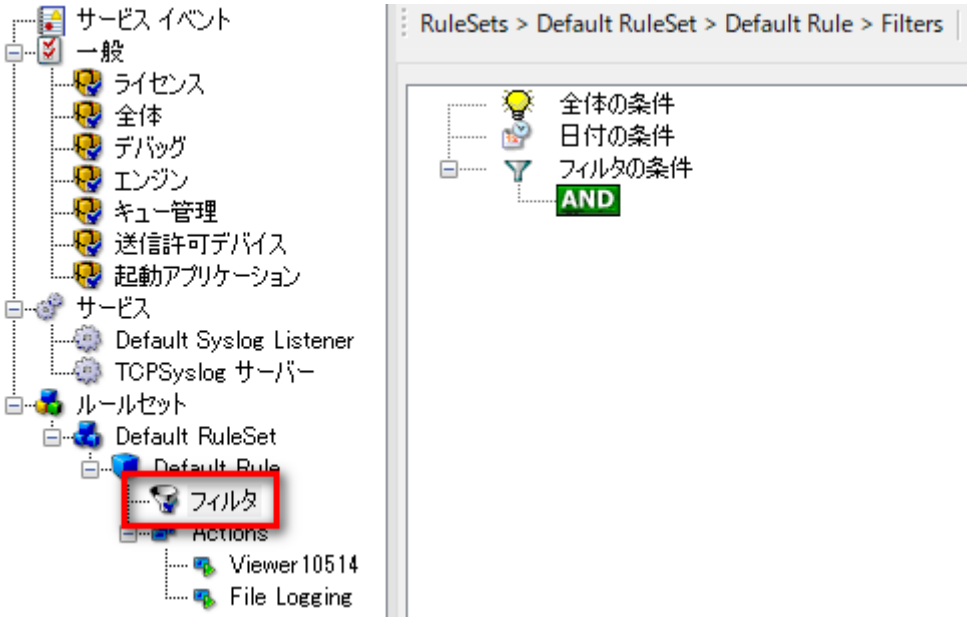
5.5. フィルタ条件

ここでは、フィルタ条件について説明します。

5.5.1. フィルタとは

フィルタ条件はルールをいつ適用するかを指定します。フィルタ条件が真であると評価された場合、これらの条件を含むルールが一致とみなされ、そのルールで指定されたアクションが実行されます。

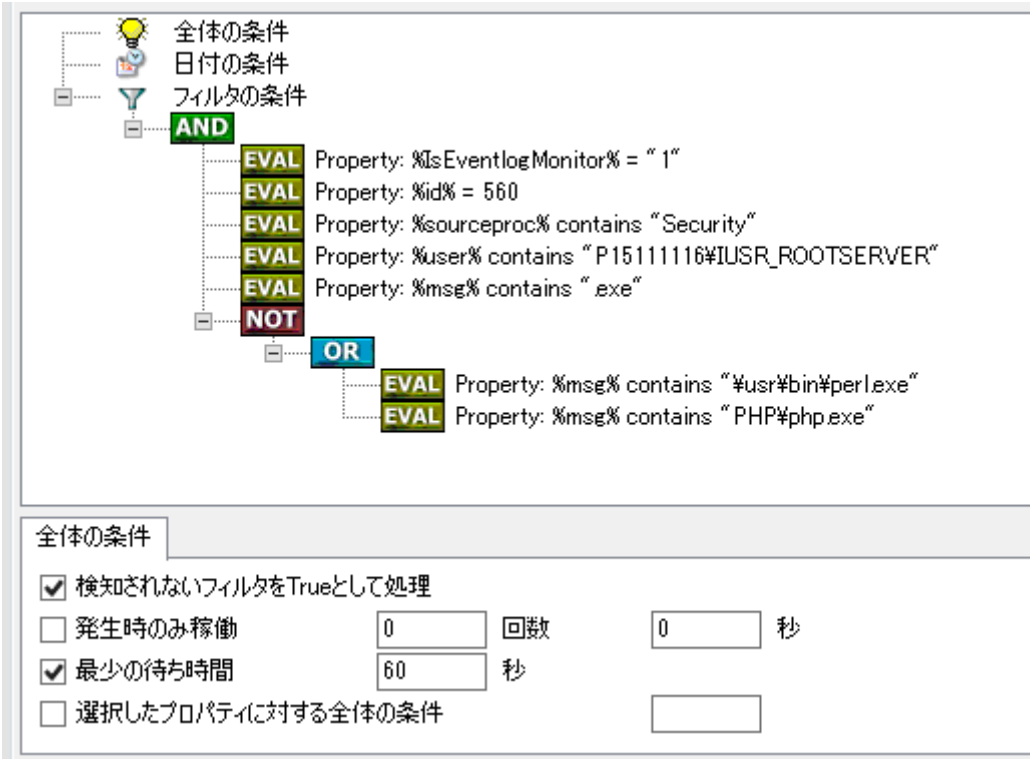
フィルタ条件は必要に応じて複雑にすることができます。ブール演算と条件のネストがサポートされています。デフォルトでは、フィルタ条件は空です。それぞれのツリーには、フィルタを簡単に追加できるようにするため、トップレベルに「AND」が１つだけ含まれています（トップレベルで使用されるノードは通常「AND」なので、デフォルトで設定されています）。この「AND」のみを含むフィルタ条件は常に真と評価されます。



デフォルトのフィルタ条件（「AND」のみを含むフィルタ条件）の場合、受信されたすべてのメッセージに対してこのルールに関連付けられたアクションが実行されます。これは、例えば、受信したすべてのインフォメーションユ

ニットをデータベースやテキストファイルに書き込みたい場合などによく使用されます。

一方、特定の条件において（メッセージを絞り込んで）アクションを実行させたい場合には、フィルタ条件を指定する必要があります。これは、複数階層のブール演算を含む複雑なフィルタ条件が必要になる場合もあります。下図はこのような場合のサンプルです：



このフィルタ条件は、侵入検知ルールセットの一部です。ここでは、Windows ファイルシステム監査を使用して、Internet Information Server (IIS)を介して潜在的に成功した侵入を検出します。これはすべての実行可能ファイルで監査を有効にすることで実行されます。Internet Information Server は、IUSR_<machinename>アカウント下でこれらのアカウントにアクセスします（この例の場合は、「P15111116¥IUSR_ROOTSERVER」です）。このユーザーが予期しない実行ファイル（exe ファイル）を実行した場合、誰かが IIS 経由でコンピューターに侵入した可能性があります。Perl と PHP スクリプトが Perl および PHP エンジンを実行する必要があることに注意してください。これは、perl.exe と php.exe が実行されているかどうかを確認することで反映されます。もしそうであれば、アラートはトリガされません。

具体的には、上記のサンプルは以下のように動作します：
まず、メッセージに perl.exe または php.exe へのフルパス名が含まれている場合、メッセージの内容がチェックされます。これは、下部の「OR」ブランチで行われます。フィルタ条件が「真（True）」と評価されたときにアクションが実行されることにご注意ください。perl.exe と php.exe の場合、希望するものの逆です（この場合はアクションを実行したくありません）。アクションは他のファイルが実行されたときに実行する必要があります。このため、「OR」の結果を否定（ブール演算「NOT」）します。「NOT」オペレーションの結果が「AND」を介して他の必要なプロパティと結合されます。

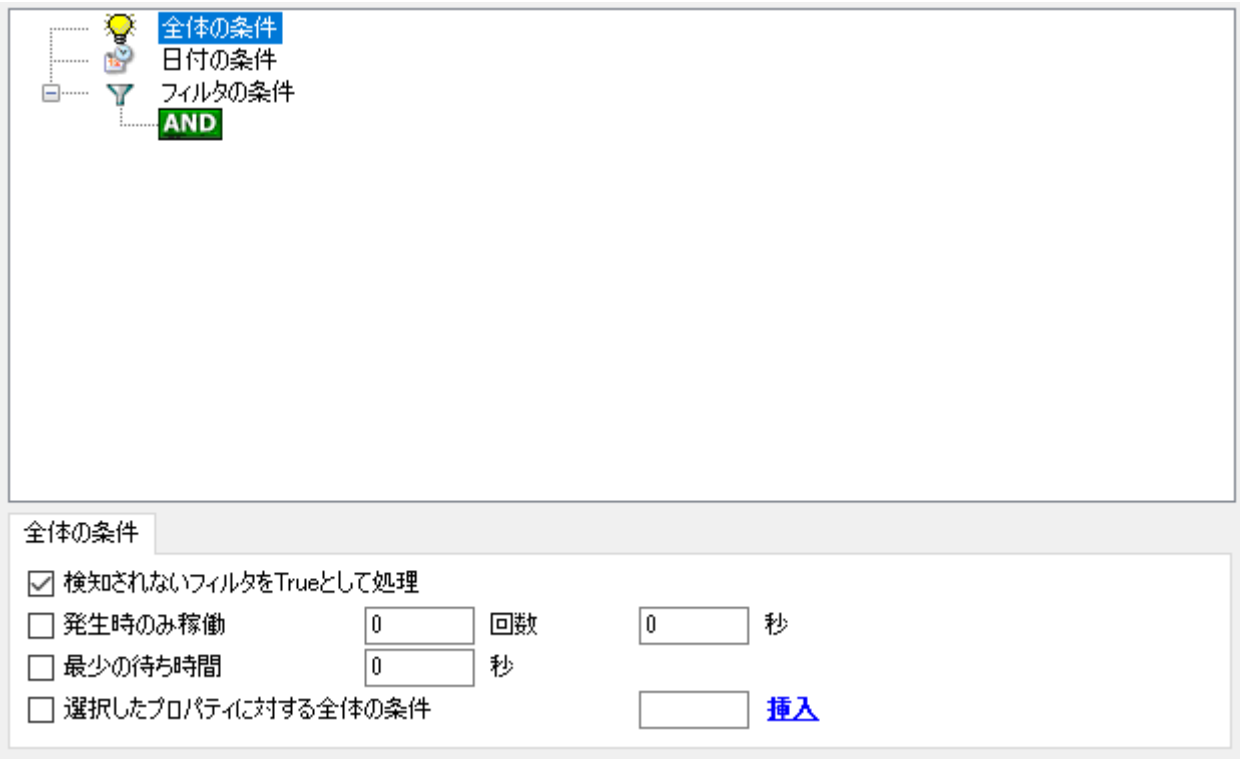
まず、特定のイベントが実際に発生したかどうかを確認します。このためには「イベントログの監視」のインフォメーションユニットを処理する必要があります。次に、これらのインフォメーションユニットはイベントソース（Security）とイベント ID（ID=560）で識別されます。また、イベントユーザー（P15111116¥IUSR_ROOTSERVER）も確認します。最後に、メッセージに「.exe」という文字列が含まれているかどうかを確認します。

さらに、上のサンプルでは、頻繁にアラートが発生しないように、「最少の待ち時間」を 60 秒に指定しています。したがって、全ての条件が真であっても、フィルタの条件は 60 秒ごとに「真（True）」と評価し、アクションを実行します。

> **注記：**
> フィルタ条件の文字列比較では大文字と小文字が区別されます。例えば、「ws01」という名前のソースシステムに対してフィルタ条件に「WS01」と定義した場合、このフィルタ条件は決して「真（True）」であると評価されません。

5.5.2. 全体の条件

「**全体の条件**」は、ルール全体に適用されます。それらは、自動的にフィルタツリーの条件と論理的な「AND」と組み合わされます。



以下の項目を設定できます：

検知されないフィルタを True として処理

「**フィルタの条件**」で照会されたプロパティがイベントに存在しない場合、それぞれの条件は通常「偽

（False）」を返します。ただし、ルールエンジンがこれを代わりに「真（True）」と評価する方が望ましい場合もあります。このオプションを使用すると、意図した動作を選択できます。これをチェックすると、イベントに見つからないプロパティを持つ条件が「真（True）」と評価されます。

発生時のみ稼働

これは、「**最少の待ち時間**」と正反対の機能と言えます。このチェックボックスがオンの場合、イベントが指定した回数発生するとルールが起動します。指定期間内に同じイベントが指定回数発生するまで待機します。指定回数に達すると、フィルタ条件が一致しルールが起動されます。

最少の待ち時間

このチェックボックスをオンにすると、ルールが頻繁に起動するのを防ぐことができます。ルールが指定した時間間隔で起動するようになります。例えば「60」と入力すると、60 秒以内にイベントが複数回発生した場合は2回目以降のルール（アクション）は実行されませんが、60 秒後に発生したイベントに対してはルール（アクション）が実行されます。

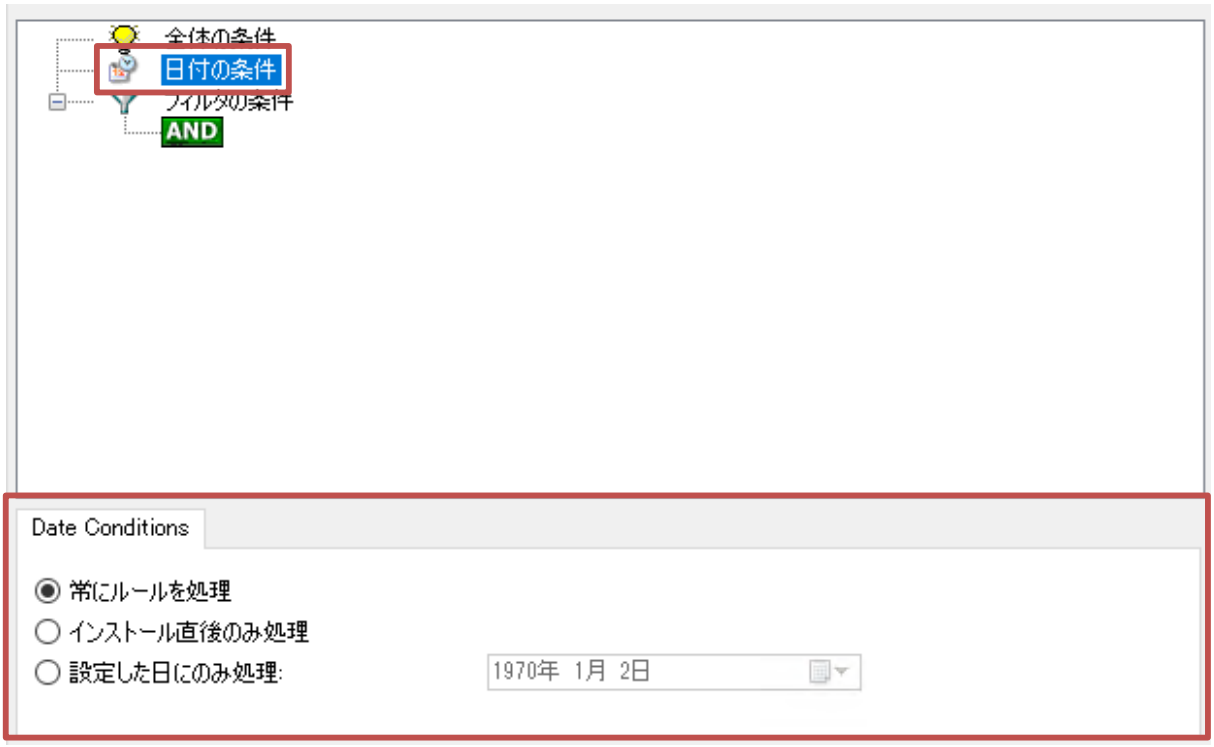
選択したプロパティに対する全体の条件

このチェックボックスをオンにすると、指定したプロパティに基づいて「**全体の条件**」を制御することができます。例えば %source% を指定した場合、Syslog メッセージのソース（送信元）ごとに条件が適用されます。

5.5.3. 日付の条件

ここでは、「**日付の条件**」について説明します。

ルール処理を特定の日付またはインストール直後のみに処理することができます。デフォルトの場合、ルールは常に処理されます。



以下の項目を設定できます:

常にルールを処理

オンの場合、条件はなく、常にルールが実行されます。

インストール直後のみ処理

オンの場合、メッセージがアプリケーションのインストール日以降に生成、受信された場合にのみルールが処理されます。。

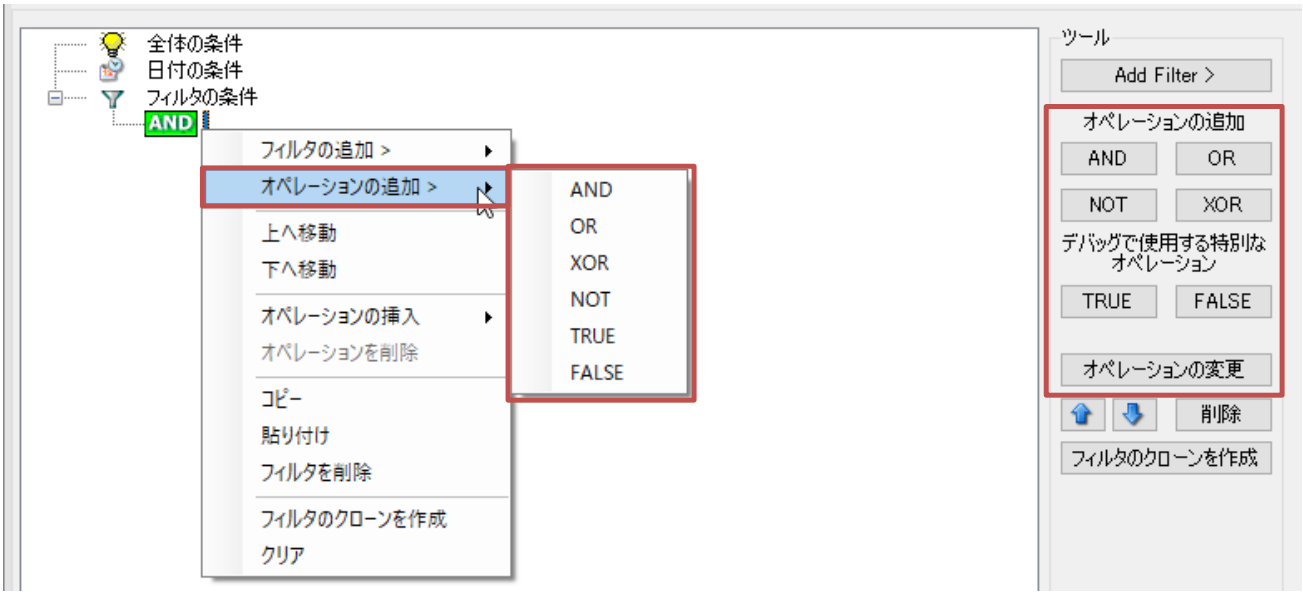
設定した日にのみ処理（正しくは「設定日以降のみ処理」）

オンの場合、設定した日付以降に生成、受信された場合にのみルールが処理されます。

5.5.4. オペレーション

ここでは、「**オペレーション**」について説明します。
オペレーションは、フィルタの条件がどのようにリンクするかを設定します。

オペレーションは、「AND」を選択して右クリックし「**オペレーションの追加 >**」のカスケードメニューから追加、または画面右側の「**ツール**」から追加、変更することができます。


全体の条件
日付の条件
フィルタの条件
AND
フィルタの追加 >
オペレーションの追加 >
上へ移動
下へ移動
オペレーションの挿入
オペレーションを削除
コピー
貼り付け
フィルタを削除
フィルタのクローンを作成
クリア
AND
OR
XOR
NOT
TRUE
FALSE
ツール
Add Filter >
オペレーションの追加
AND
OR
NOT
XOR
デバッグで使用する特別な
オペレーション
TRUE
FALSE
オペレーションの変更
削除
フィルタのクローンを作成

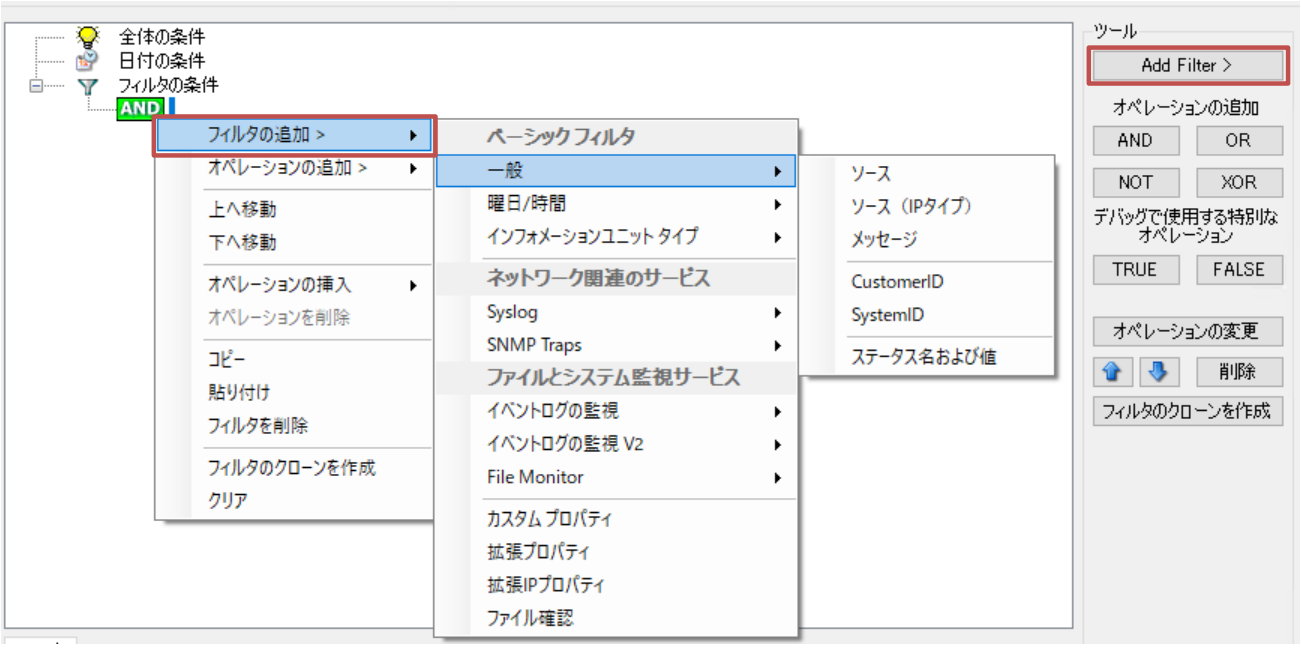
以下のオペレーションを使用することができます。

オペレーション	説明
AND	配下にある全てのフィルタが一致した場合のみ、結果が「真（True）」になります。 例：「AND」配下にフィルタ a、 b、 c を設定した場合 a、b、c のすべての条件を満たす場合に「真（True）」となり、アクションが実行されます。
OR	配下にあるフィルタのうち、ひとつでも一致すれば、結果が「真（True）」となります。 例：「OR」配下にフィルタ a、 b、 c を設定した場合 a、b、c のどれか1つでも条件を満たせば、「真（True）」となり、アクションが実行されます。
NOT	配下には1つのフィルタしか配置できません。フィルタが一致した場合、 「偽（False）」となります。 例： 配下にフィルタ a を設定した場合 a の条件を満たす場合（逆に「偽（False）」となり）、アクションは実行されません。
XOR	2つのフィルタのうち1つが一致した場合のみ、「真（True）」となります。 例： フィルタ a、 b を設定した場合 a と b のどちらか一方の条件のみを満たす場合に「真（True）」となり、アクションが実行されます。a と b の両方の条件を満たす、または両方の条件を満たさない場合は、「偽（False）」となり、アクションは実行されません。
TRUE	デバッグを行う際に役立ちます。結果は「真（True）」となります。
FAULSE	デバッグを行う際に役立ちます。結果は「偽（False）」となります。

5.5.5. フィルタの条件

ここでは、「**フィルタの条件**」について説明します。

フィルタの条件は、各オペレーションノードの下に追加することができます。オペレーションノードを右クリックし「**フィルタの追加 >**」のカスケードメニュー、または画面右側の「**Add Filter >**」から追加します。

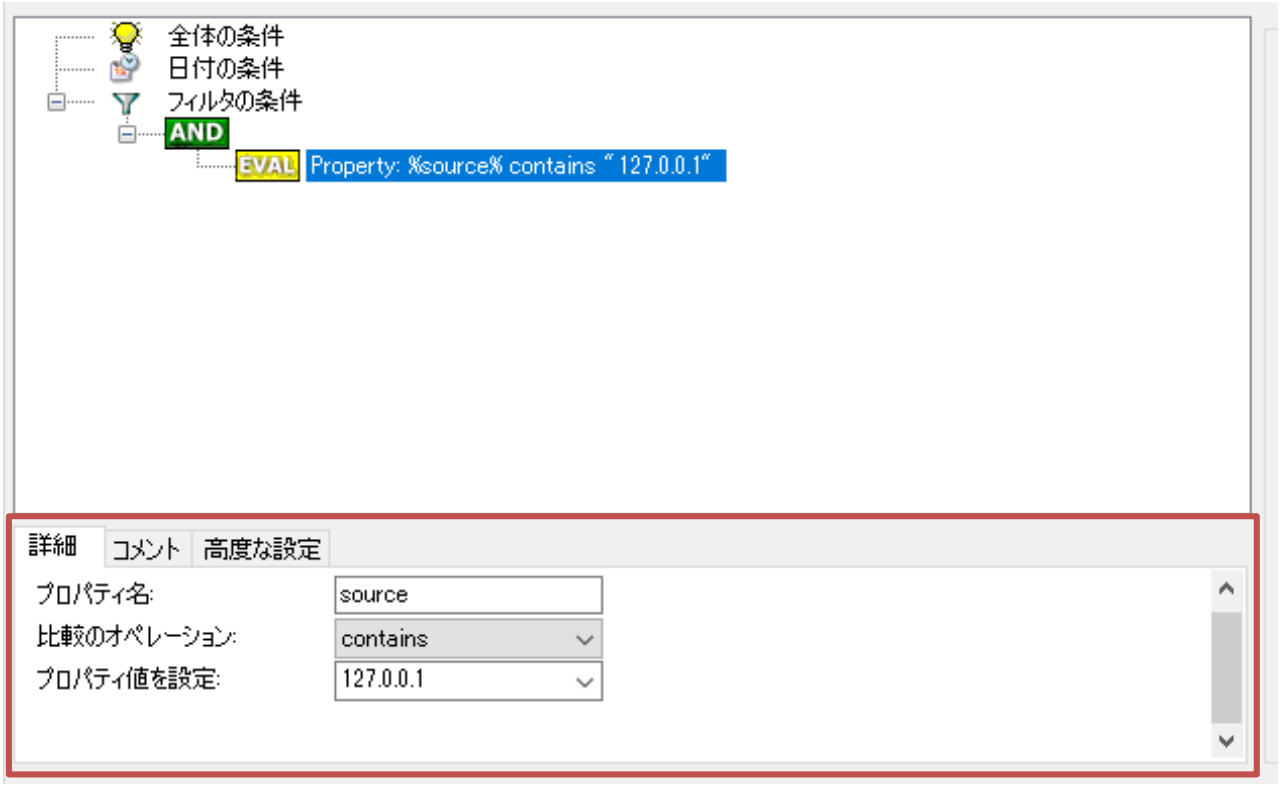


フィルタには全てのサービスで使用できる共通のフィルタ（ベーシックフィルタ）と、特定のインフォメーションユニットでのみ使用できるフィルタがあります。

インフォメーションユニットで一致しない全てのフィルタは、フィルタリング処理で無視されます。インフォメーションユニットのタイプに特化したしたフィルタを作成したい場合は、必ず「**インフォメーションユニットタイプ**」フィルタを追加してください。

> **注記：**
> 評価されたインフォメーションユニットに適用されないフィルタが使用されている場合は無視されます。これにより、いくつかのタイプのインフォメーションユニットに対して１つのフィルタセットを構築することができます。

フィルタの条件は画面下部の「**詳細**」タブエリアで指定します。フィルタを選択すると、「**詳細**」タブにフィルタ条件が表示されます。「**比較のオペレーション**」で比較する方法、「**プロパティ値を設定**」で比較する値を指定します。



フィルタの条件で使用できるプロパティごとにタイプ（型）が異なります。このため、比較に使用できるオペレーションもプロパティのタイプ（型）により異なります。

タイプ（型）の種類と使用できる比較のオペレーションは以下のとおりです：

タイプ	使用できる比較のオペレーション
文字列（String）	「contains（包含する）」、「does not contain（包含しない）」、「contains within range（範囲内に含む）」、「is equal（等しい）」、「is not equal（等しくない）」、「mach regex（正規表現一致）」で別の文字列と比較できます。
番号（Number）	「＝」、「Not ＝」、「<」、「>」で別の番号と比較できます。
ブール演算子（Boolean）	「＝」、「Not ＝」で比較できます。
時間（Time）	「＝」、「<」、「>」で別の時間と比較できます。

比較のオペレーションについてはこちらをお読みください。

5.5.5.1 REGEX の比較動作

このプロパティは、正規表現に対して評価されます。正規表現の構文で知られているすべてを使用して、一致するパターンを定義することができます。

以下は正規表現のサンプルです：

サンプル	説明
[0-9]{4,4}-[0-9]{1,2}-[0-9]{1,2}[0-9]{1,2}:[0-9]{1,2}:[0-9]{1,2}	典型的な日付と一致します。 例： 2015-11-20 12:11:01
¥n[0-9]{4,4}	改行と 4 桁の数字に一致します。
(;|:)	セミコロンまたはコロンに一致します。

正規表現構文について詳しくは、以下をご参照ください：
https://msdn.microsoft.com/ja-jp/library/bb982727(v=vs.90).aspx

5.5.5.2 比較のオペレーション

使用できる「比較のオペレーション」は以下のとおりです：

オペレーション	タイプ	真（True）と評価される条件
contains	文字列（String）	指定したプロパティ値に「プロパティ値を設定」に入力した文字列が含まれる
does not contain	文字列（String）	指定したプロパティ値に「プロパティ値を設定」に入力した文字列が含まれない
contains within range	文字列（String）	指定したプロパティ値の指定範囲内（開始、終了を指定）に「プロパティ値を設定」に入力した文字列が含まれる
is equal	文字列（String）	指定したプロパティ値が「プロパティ値を設定」に入力した文字列と全く同じ内容である
is not equal	文字列（String）	指定したプロパティ値が「プロパティ値を設定」に入力した文字列と異なる
=	番号（Number） ブール演算子（Boolean） 時間（Time）	指定したプロパティ値が「プロパティ値を設定」に入力した値と同じである
Not ＝	番号（Number） ブール演算子（Boolean）	指定したプロパティ値が「プロパティ値を設定」に入力した値と異なる
<	番号（Number） 時間（Time）	指定したプロパティ値が「プロパティ値を設定」に入力した値より小さい
>	番号（Number） 時間（Time）	指定したプロパティ値が「プロパティ値を設定」に入力した値より大きい

5.5.6. 一般

ここでは、「**一般**」フィルタについて説明します。

以下のフィルタを使用できます：

ソース

このフィルタの条件は、インフォメーションユニットを生成したシステムをチェックします。例えば、Syslog サーバーの場合、これは Syslog メッセージを送信する Syslog デバイスです。
このフィルタのタイプは、文字列（String）です。ソースシステム名または IP アドレスを含む必要があります。

ソース（IP タイプ）

IP のフィルタは基本的にどのプロパティ上でも機能しますが、通常は有効な IP アドレスまたはホスト名が含まれていることを確認できるので、%source%プロパティでのみ使用することをお勧めします。

このフィルタは、IP アドレスとホスト名に対してフィルタをかけることができます。ホスト名は（パフォーマンス上の理由から）内部の DNS キャッシュを使用して自動的に解決されます。
このフィルタのタイプは、拡張 IP（Extended IP）です。ソースシステム名または IP アドレスを含む必要があります。詳しくは、「拡張 IP プロパティ」をお読みください。

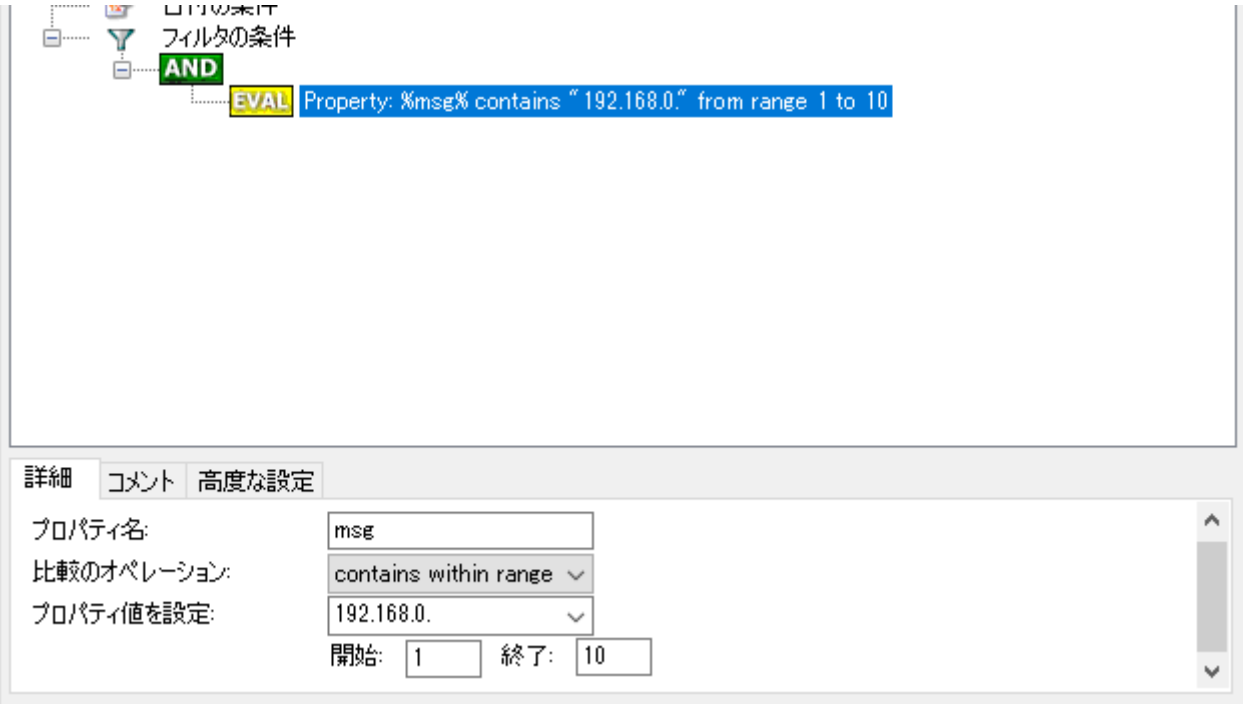
メッセージ

このフィルタは、処理されるイベントのメッセージに含まれる文字列をもとにフィルタリングしたい場合に使

用します。指定した文字列がメッセージ内のどこにあっても「真（True）」と評価されます。暗黙のうちにワイルドカード処理されるため、ワイルドカードを追加する必要はありません。

検索範囲をメッセージ内の特定の領域に限定することもできます。これを行うには、「**比較のオペレーション**」で「**contains within range**」を選択し、「**開始**」と「**終了**」を指定します。
メッセージ文字列の先頭から検索したい場合には、「**開始**」は「**1**」と指定します。

下図は「**プロパティ名**」で設定した「**メッセージ**」中の「**開始**」で設定した「**1**」と「**終了**」で設定した「**10**」の間の文字列から「**プロパティ値を設定**」で設定した「**192.168.0.**」を検索した例です。



このように設定することで、192.168.0.x（192.168.0.0 から 192.168.0.254 まで）のデバイスで作成されるログを検出することもできます。上記の設定で、「**プロパティ値**」を「**192.168.0**」（最後のドットを含まない設定）としてしまうと、例えば「192.168.010」なども検出されてしまうので、ご注意下さい。
このフィルタのタイプは、文字列（String）です。

CustomerID

CustomerID はユーザーが利便性を向上させるために使用できる数値です。CustomerID をもとにフィルタリングしたい場合に使用します。
このフィルタのタイプは、番号（Number）です。

注記：
CustomerID は EventReporter の全体設定「一般」-「全般」-「カスタマーID」で設定することができます。

SystemID

SystemID はユーザーが利便性を向上させるために使用できる数値です。SystemID をもとにフィルタリングしたい場合に使用します。

このフィルタのタイプは、番号（Number）です。

注記:

SystemID は EventReporter の全体設定「一般」-「全般」-「システム ID」で設定することができます。

ステータス名および値

このフィルタタイプは、「ステータスの設定」アクションに対応しています。

このフィルタのタイプは、文字列（String）です。

5.5.7. 曜日/時間

ここでは、「**曜日/時間**」フィルタについて説明します。

このフィルタの条件は、イベントが発生した時間枠および/または曜日をチェックするために使用されます。

以下のフィルタを使用できます：

時間

このフィルタの条件は、イベントが発生した時間を確認するために使用されます。例えば、Cisco ルーター

からダイヤルアップしたことを示す Syslog メッセージが営業時間内に発生したのであれば正常ですが、夜間に発生した場合は警告すべきことなので管理者はこのイベントの通知を受信するといったことができます（逆に破棄することもできます）。これは、時間設定で行うことができます。
このフィルタのタイプは、時間（Time）です。

また、タイムモードを指定することもできます。以下から選択できます：

- **デフォルト タイムモード - 受信時間**
- **デフォルト タイムモード - デバイスの報告時間**
- **ローカルタイム - 受信時間**
- **ローカルタイム - デバイスの報告時間**
- **UTC - 受信時間**
- **UTC - デバイスの報告時間**

曜日

このフィルタの条件は、上記の時間のフィルタとよく似ていますが、こちらは1日単位で適用されます。例えば、週末に発生したイベントを検出し、そのイベントの処理方法を変更することができます。

次のフィルタを使用することができます：

- **月曜日に実行**
- **火曜日に実行**
- **水曜日に実行**
- **木曜日に実行**
- **金曜日に実行**
- **土曜日に実行**
- **日曜日に実行**

このフィルタのタイプは、ブール演算子（Boolean）です。

5.5.8. インフォメーション ユニット タイプ

ここでは、「**インフォメーションユニットタイプ**」フィルタについて説明します。

このフィルタは一部のインフォメーションユニットタイプに対してルールを処理させたい場合に使用します。これ

は、特定のタイプに標準でない処理が必要な場合に特に役立ちます。利用可能なインフォメーションユニットタイプには、事前定義済みのフィルタがあります。

次のフィルタを使用することができます:

- **Syslog**
- **ハートビート**
- **SNMP トラップ**
- **イベントログの監視**
- **イベントログの監視 V2**
- **ファイル モニタ**
- **RELP リスナー**

このフィルタのタイプは、ブール演算子(Boolean)です。

> **メモ**:「イベントログの監視」および「イベントログの監視 V2」フィルタは EventReporter から、「ファイル モニタ」フィルタは MonitorWare から SETP を介して送信されたメッセージをフィルタリングする際に使用します。

5.5.9. Syslog

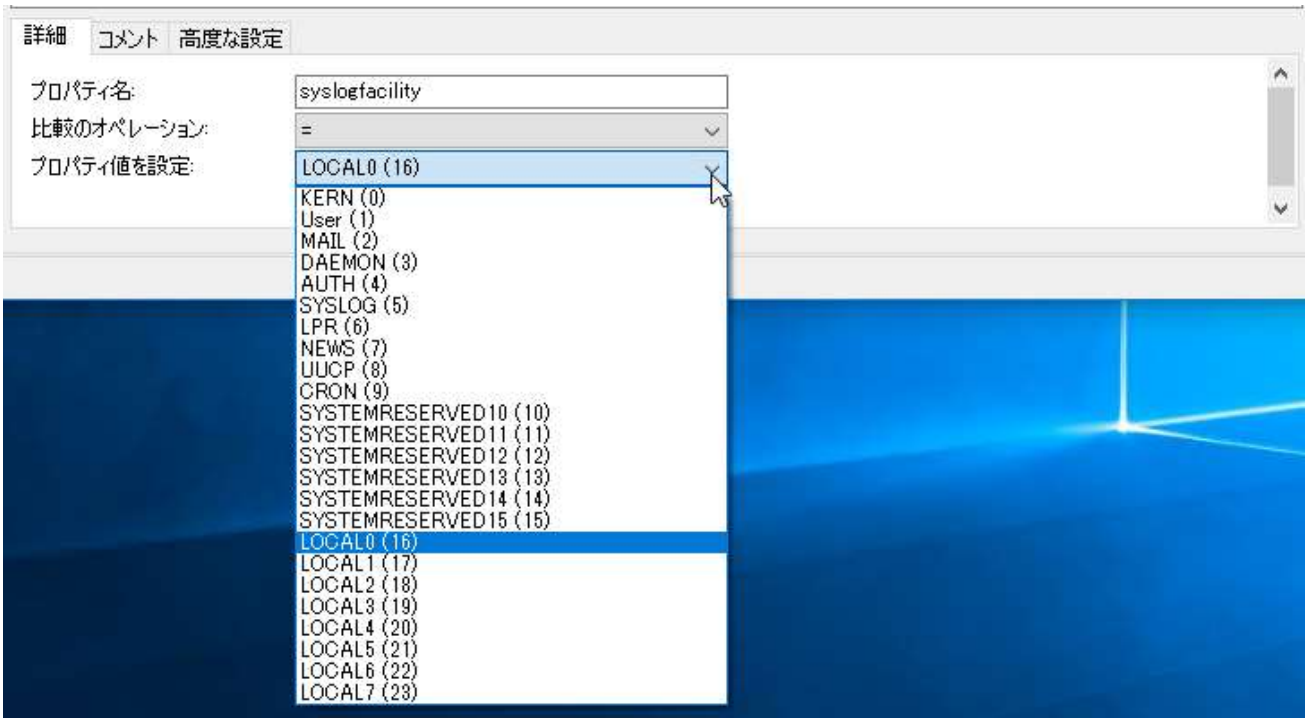
ここでは、「Syslog」フィルタについて説明します。

Syslog 関連のフィルタがグループ化されています。インフォメーションユニットごとに Syslog プライオリティとファシリティが割当てられるため、これらのフィルタはすべてのインフォメーションユニットで使用できます。

次のフィルタを使用することができます：

ファシリティ

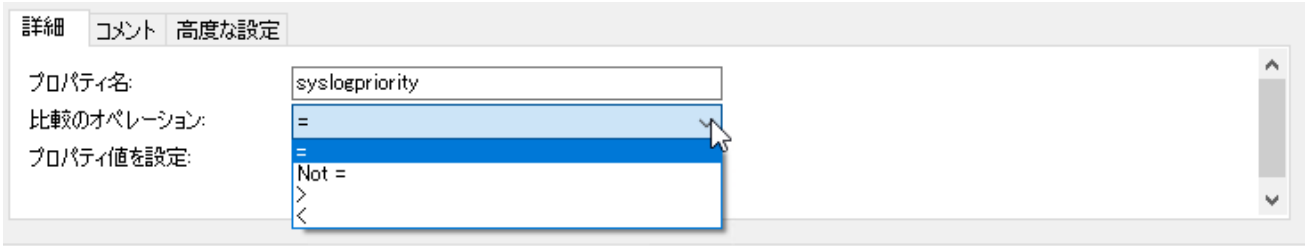
Syslog ファシリティによりフィルタリングを行う場合に設定します。インフォメーションユニットに指定された Syslog ファシリティ値が必要です。Syslog タイプのインフォメーションユニットの場合は、実際の Syslog ファシリティコードです。その他のインフォメーションユニットの場合は、ベストエフォート方式でマッピングされた値となります。
このフィルタのタイプは、番号（Number）です。ファシリティ値はリストから選択することができます：



プライオリティ

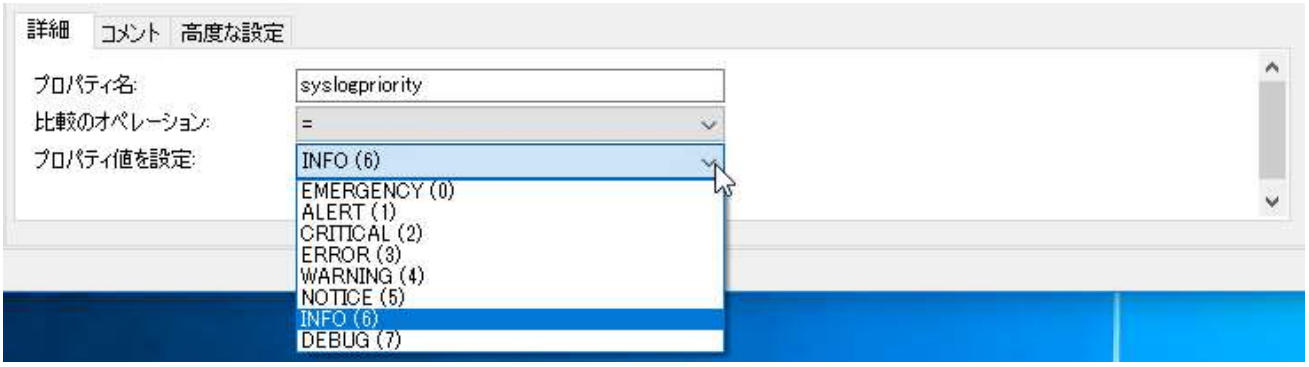
Syslog プライオリティ(Severity)によりフィルタリングを行う場合に設定します。インフォメーションユニットに指定された Syslog プライオリティ値が必要です。Syslog タイプのインフォメーションユニットの場合は、実際の Syslog プライオリティ(Severity)コードです。その他のインフォメーションユニットの場合は、ベストエフォート方式でマッピングされた値となります。

プライオリティ値は数値が小さいほど重要度(Level)が高いメッセージとなります。「**比較のオペレーション**」では、一致モードを選択することができます。



等しい(=)、異なる(Not =)、より大きい(>)、より小さい(<)からオペレーションを選択できます。例えば、「<」を選択した場合、「**プロパティ値を設定**」で指定したプライオリティ値より小さいものすべてが一致する(「真(True)」と評価される)ことを意味します。この場合、指定したプライオリティ値は含まれないことにご注意ください(「<」は「より小さい」なので、指定したプライオリティ値は含まれません)。この値を含めたい場合は、その次の値(この場合は 1 つ大きい値)を指定してください。

プライオリティ値はリストから選択することができます:



このフィルタのタイプは、番号（Number）です。

Syslog タグ

Syslog タグ（メッセージを生成したプログラムまたはプロセスの名前）によりフィルタリングしたい場合に設定します。
このフィルタのタイプは、文字列（String）です。

メモ:
その他、**Syslog バージョン**、**Syslog Appname**、**Syslog ProcID**、**Syslog MSGID**、**Syslog Structdata** は、RFC5424（新しい規格）に対応したフィルタです。

5.5.10. SNMP Traps

ここでは、「**SNMP Traps**」フィルタについて説明します。

SNMP トラップを使用することで、WinSyslog は、コンピューター、ルーター、配線ハブなどを含むいろいろな装置を管理したり、監視したりすることができます。SNMP トラップはデバイスが送信すべき情報がある場合に生成されます。

「SNMP Traps」には SNMP トラップ関連のフィルタがグループ化されています。

次のフィルタを使用することができます：

Version

それぞれの SNMP エンティティに対応します。
このフィルタのタイプは、文字列（String）です。

Uptime

それぞれの SNMP エンティティに対応します。
このフィルタのタイプは、文字列（String）です。

SNMP V1 Filters

Community

それぞれの SNMP エンティティに対応します。
このフィルタのタイプは、文字列（String）です。

Enterprise

それぞれの SNMP エンティティに対応します。
このフィルタのタイプは、文字列（String）です。

Generic Name

それぞれの SNMP エンティティに対応します。
このフィルタのタイプは、文字列（String）です。

Specific Type

それぞれの SNMP エンティティに対応します。
このフィルタのタイプは、文字列（String）です。

AgentIP

それぞれの SNMP エンティティに対応します。
このフィルタのタイプは、拡張 IP（EXTPROPIP）です。

5.5.11. イベントログの監視

ここでは、「**イベントログの監視**」フィルタについて説明します。

EventReporter（Windows イベントログ監視ソフトウェア）から SETP 通信で送信されたイベントログメッセージをフィルタリングする際に使用します。

> **メモ**:
>
> WinSyslog を単体でご利用いただいている場合は、このフィルタグループは使用しません。
>
> 「イベントログの監視」フィルタグループは、Windows 2000, 2003, XP のイベントログ監視で使用します。
> WIndows Vista 以降のイベントログ監視については「イベントログの監視 V2」を使用してください。

「イベントログの監視」にはイベントログ監視関連のフィルタがグループ化されています。

次のフィルタを使用することができます：

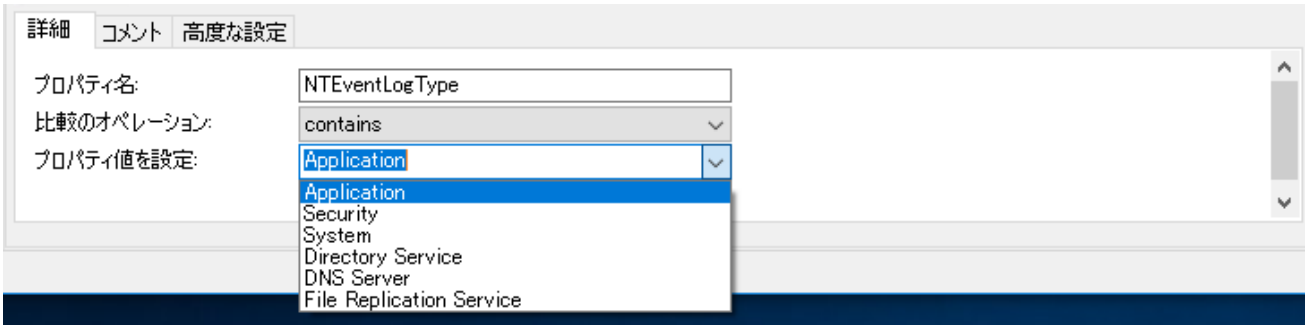
イベント ID

Windows イベントログ ID によりフィルタリングしたい場合に設定します。
このフィルタのタイプは、番号（Number）です。デフォルトは、id プロパティ値が 0 と一致する（=）場合に「真（True）」と評価されます。

イベント タイプ

Windows イベントログタイプによりフィルタリングしたい場合に設定します。

プロパティ値はリストから選択することができます。



このフィルタ条件には、イベントログインフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性がありま

す。
このフィルタのタイプは、文字列（String）です。

イベント ソース

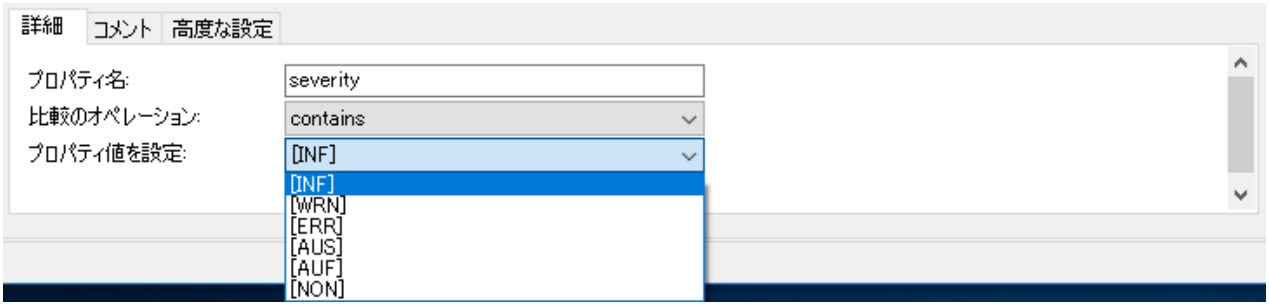
Windows イベントログソースによりフィルタリングしたい場合に設定します。プロパティ値は大文字と小文字が区別されます。

このフィルタ条件には、「イベントログの監視」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント 重要度

Windows イベントログ重要度によりフィルタリングしたい場合に設定します。

プロパティ値はリストから選択することができます。



このフィルタ条件には、「イベントログの監視」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント カテゴリ

Windows イベントログカテゴリによりフィルタリングしたい場合に設定します。

このフィルタ条件には、「イベントログの監視」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、番号（Number）です。

イベント カテゴリ名

Windows イベントログカテゴリ文字列によりフィルタリングしたい場合に設定します。解決可能な場合、この値にはカテゴリ値が文字列として格納されます。解決できない場合は、カテゴリ番号が含まれます。

このフィルタ条件には、「イベントログの監視」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント レコード ナンバー

内部のイベントレコード番号によりフィルタリングしたい場合に設定します。イベントログが以前切り捨てられた場合、0 または 1 で始まらず、より大きな番号である可能性があることにご注意ください。

このフィルタ条件には、「イベントログの監視」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、番号（Number）です。

イベント ユーザー

Windows イベントログユーザーによりフィルタリングしたい場合に設定します。大文字小文字が区別されることにご注意ください。

このフィルタ条件には、「イベントログの監視」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

5.5.12. イベントログの監視 V2

ここでは、「**イベントログの監視 V2**」フィルタについて説明します。

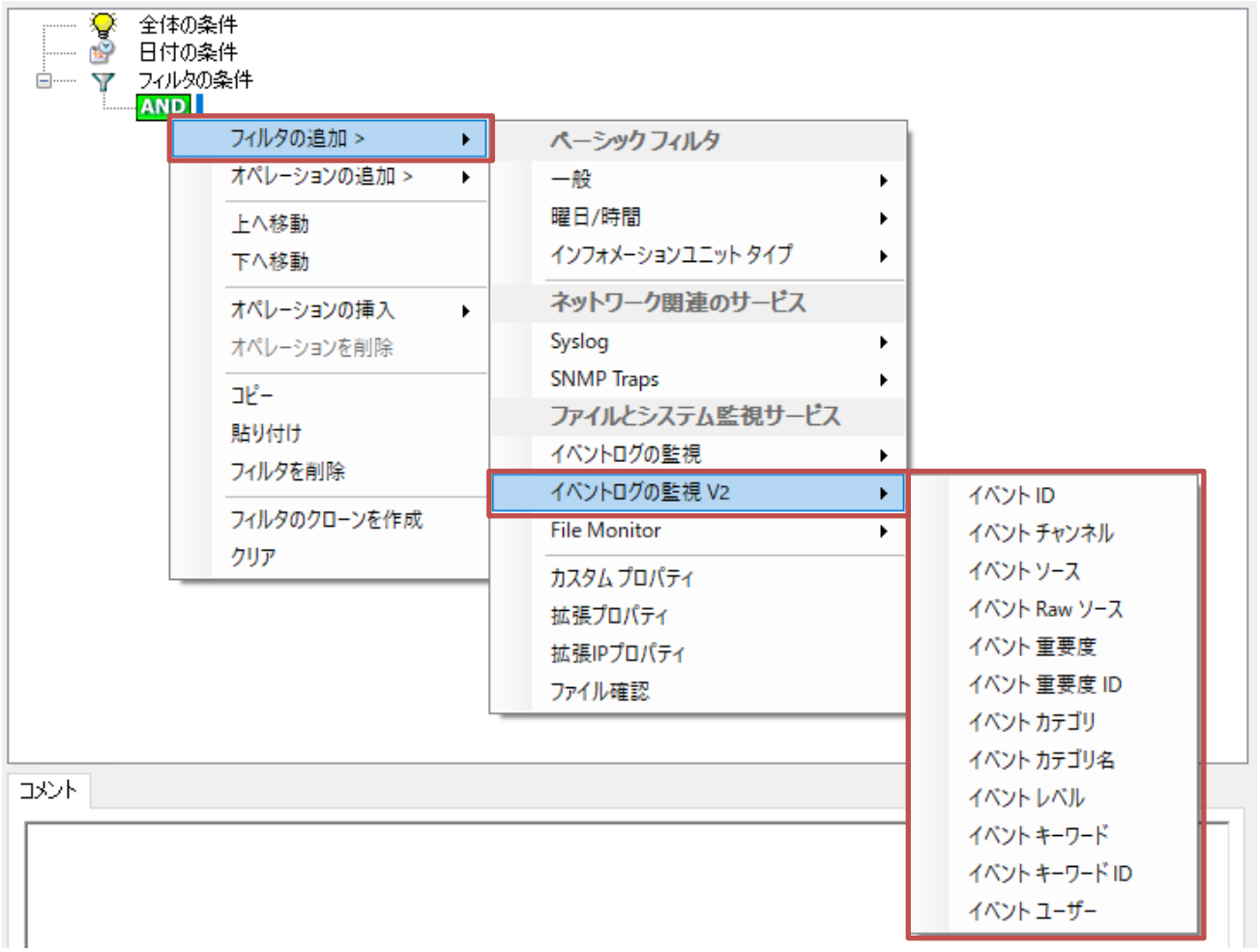
EventReporter（Windows イベントログ監視ソフトウェア）から SETP 通信で送信されたイベントログメッセージをフィルタリングする際に使用します。

メモ:

WinSyslog を単体でご利用いただいている場合は、このフィルタグループは使用しません。

「イベントログの監視 V2」フィルタグループは、Windows Vista 以降（Windows Vista,7,8,8.1,10, Windows 2008, 2012, 2016（R2 含む））のイベントログ監視で使用します。Windows 2000, 2003, XP のイベントログ監視については「イベントログの監視」を使用してください。

「イベントログの監視 V2」にはイベントログ監視関連のフィルタがグループ化されています。



次のフィルタを使用することができます:

イベント ID

Windows イベントログ ID によりフィルタリングしたい場合に設定します。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、番号（Number）です。

イベント チャンネル

Windows イベントログチャンネルによりフィルタリングしたい場合に設定します。プロパティ値は大文字と小文字が区別されます。正確に記入してください。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント ソース

Windows イベントログソースによりフィルタリングしたい場合に設定します。プロパティ値は大文字と小文字が区別されます。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント Raw ソース

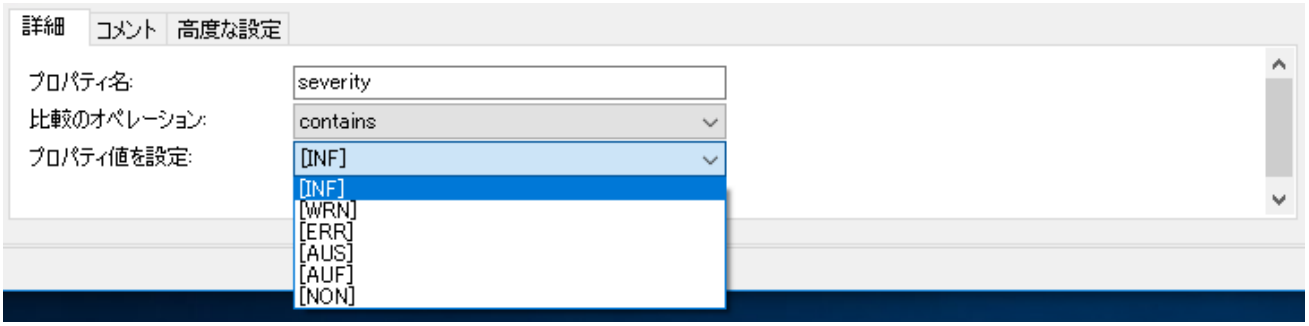
Raw ソースには、イベントソースの完全な内部名が含まれています。Windows イベントログの完全なイベントソース名によりフィルタリングしたい場合に設定します。プロパティ値は大文字と小文字が区別されます。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント 重要度

Windows イベントログ重要度によりフィルタリングしたい場合に設定します。

プロパティ値はリストから選択することができます。



このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント 重要度 ID

Windows イベントログレベルの内部 ID によりフィルタリングしたい場合に設定します。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、番号（Number）です。

イベント カテゴリ

Windows イベントログカテゴリによりフィルタリングしたい場合に設定します。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、番号（Number）です。

イベント カテゴリ名

Windows イベントログカテゴリ文字列によりフィルタリングしたい場合に設定します。解決可能な場合、この値にはカテゴリ値が文字列として格納されます。解決できない場合は、カテゴリ番号が含まれます。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント レベル

Windows イベントログレベル名によりフィルタリングしたい場合に設定します（ログレベルの数値は severityid プロパティに保存されます）。このプロパティはシステムで自動的にローカライズされます。大文字と小文字が区別されます。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント キーワード

Windows イベントログキーワード名によりフィルタリングしたい場合に設定します。大文字と小文字が区別されます。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント キーワード ID

これは内部的なキーワード ID です。Windows イベントログキーワード ID によりフィルタリングしたい場合に設定します。

このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

イベント ユーザー

Windows イベントログユーザーによりフィルタリングしたい場合に設定します。大文字小文字が区別されることにご注意ください。

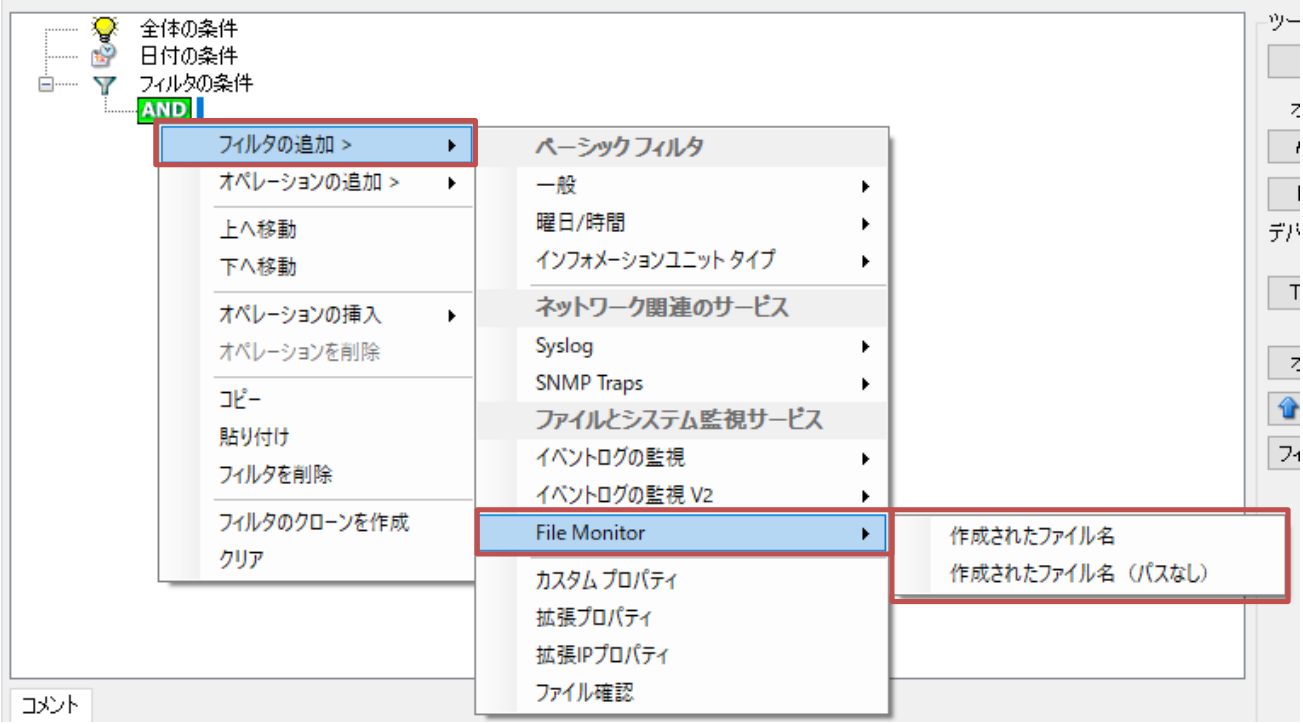
このフィルタ条件には、「イベントログ監視 V2」インフォメーションユニットのみを使用してください。他のものと一緒に一緒に使用する場合、マップされた値が使用されますが、実際の値が正しく反映されない可能性があります。
このフィルタのタイプは、文字列（String）です。

5.5.13. File Monitor

ここでは、「**File Monitor**」フィルタについて説明します。

MonitorWare エージェントから SETP 通信で送信されたファイル監視をフィルタリングする際に使用します。

> **メモ**: MonitorWare は Adiscon 社の製品ですが弊社での取り扱いはありません。WinSyslog を単体でご利用いただいている場合は、このフィルタグループは使用しません。



次のフィルタを使用することができます:

作成されたファイル名

生成されたファイル名によりフィルタリングしたい場合に設定します。プロパティ値は大文字と小文字が区別されます。正確に記入してください。
このフィルタのタイプは、文字列(String)です。

作成されたファイル名(パスなし)

生成されたファイル名(パスなし)によりフィルタリングしたい場合に設定します。プロパティ値は大文字と小文字が区別されます。正確に記入してください。
このフィルタのタイプは、文字列(String)です。

5.5.14. カスタムプロパティ

ここでは、「**カスタムプロパティ**」フィルタについて説明します。

次のフィルタを使用することができます：

カスタムプロパティ

WinSyslog の内部では、すべての値がプロパティに保存されています。例えば、メインのメッセージは「msg」というプロパティに保存されています。このフィルタを使用すると、（SNMP Trap v2 プロトコルを使用している場合と同じく）動的なプロパティにアクセスすることができます。
このフィルタのタイプは、文字列（String）です。

5.5.15. 拡張プロパティ（Extened Number Property）

ここでは、「**拡張プロパティ**」フィルタについて説明します。

このフィルタのタイプは、EXTPROPINT です。

5.5.16. 拡張 IP プロパティ

ここでは、「**拡張 IP プロパティ**」フィルタについて説明します。

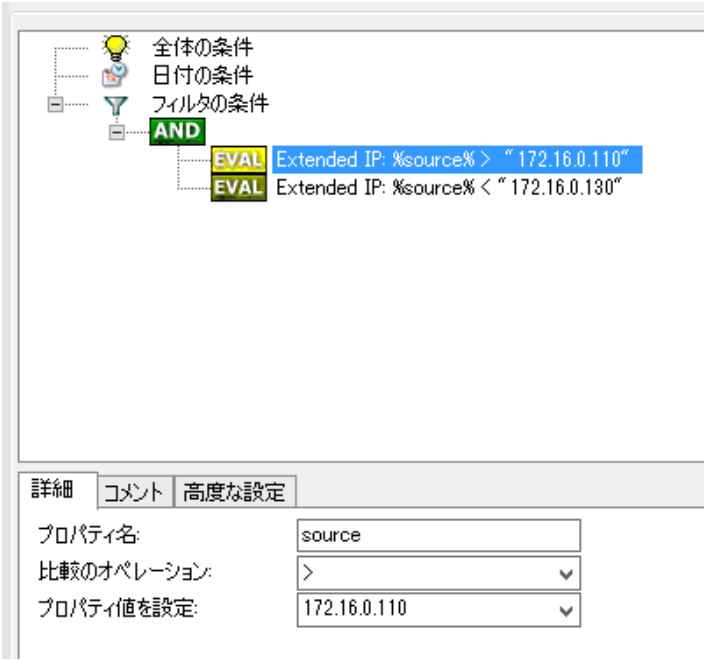
ホスト名や IP アドレスでフィルタリングしたい場合に使用します。この IP フィルタは基本的にはどんなプロパティでも動作しますが、通常は有効な IP アドレスまたはホスト名が含まれていることを確認できるため %source% でのみ使用することをお勧めします。IP フィルタはホスト名と IP アドレスに対してフィルタリングすることができます。ホスト名は(パフォーマンス上の理由から)DNS キャッシュを使用して自動的に解決されます。別のプロパティまたはカスタムプロパティを使用する場合は、プロパティのデータが有効な IP アドレスであることを確認してください。

比較のオペレーション結果は以下のとおりです:

比較のオペレーション	結果
=	プロパティ値に入力した IP アドレスに一致すると「真(True)」になります。
Not =	プロパティ値に入力した IP アドレス以外であれば「真(True)」になります。
>	プロパティ値に入力した IP アドレスより大きければ「真(True)」になります。
<	プロパティ値に入力した IP アドレスより小さければ「真(True)」になります。

「>」または「<」については、192.168.0.10, 192.168.0, 192.168, 192 などの IP アドレスフォーマットを使用できます。これはどの IP 範囲をフィルタしたいかによります。

IP 範囲をフィルタリングする場合は、範囲を定義するフィルタを 2 つ(1 つは「>」比較、もう 1 つは「<」比較)作成することをお勧めします。



上の例の場合、172.16.0.110 と 172.16.0.130 の間にあるすべての IP を受け入れます(「172.16.0.110 より大きい」かつ(AND)「172.16.0.130 より小さい」)。つまり、これら2つの条件に一致するすべての IP に対して、フィルタ全体が「真(True)」と評価され、メッセージが処理されます。フィルタが「真(True)」と評価されない場合は、ツールは中止され、メッセージは次のルールへ送信されます。
このフィルタのタイプは、EXTPROPIP です。

5.5.17. ファイル確認

ここでは、「**ファイル確認**」フィルタについて説明します。

次のフィルタを使用することができます:

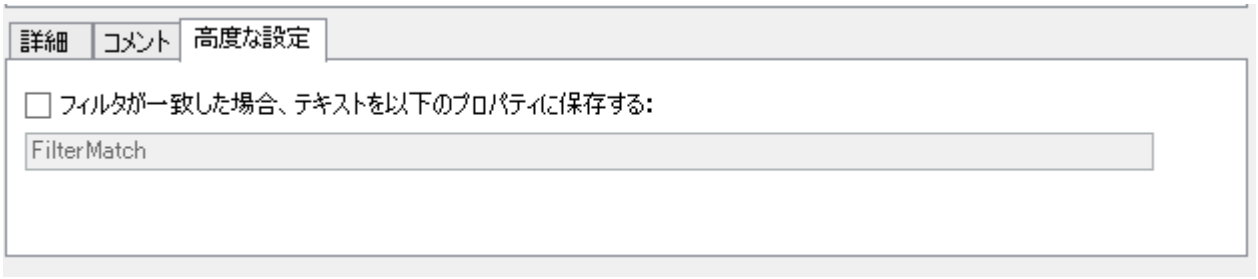
ファイル確認

このフィルタを使用するとファイルが存在するかどうかを簡単に確認することができます。ファイルとその場所を直接入力するか、「**参照**」ボタンを使用してファイルを指定することができます。
このフィルタのタイプは、FILEEXISTS です。

5.5.18. フィルタ結果の保存

ここでは、フィルタ結果の保存方法について説明します。

フィルタの結果は、それぞれのフィルタを選択したときに画面下部に表示される「**高度な設定**」タブで保存するかどうかを指定できます。



フィルタが一致した場合、テキストを以下のプロパティに保存する:

フィルタが一致した場合、その結果をカスタムプロパティに保存することができます。そのカスタムプロパティは、後のアクションで使用することができます。

5.6. アクション

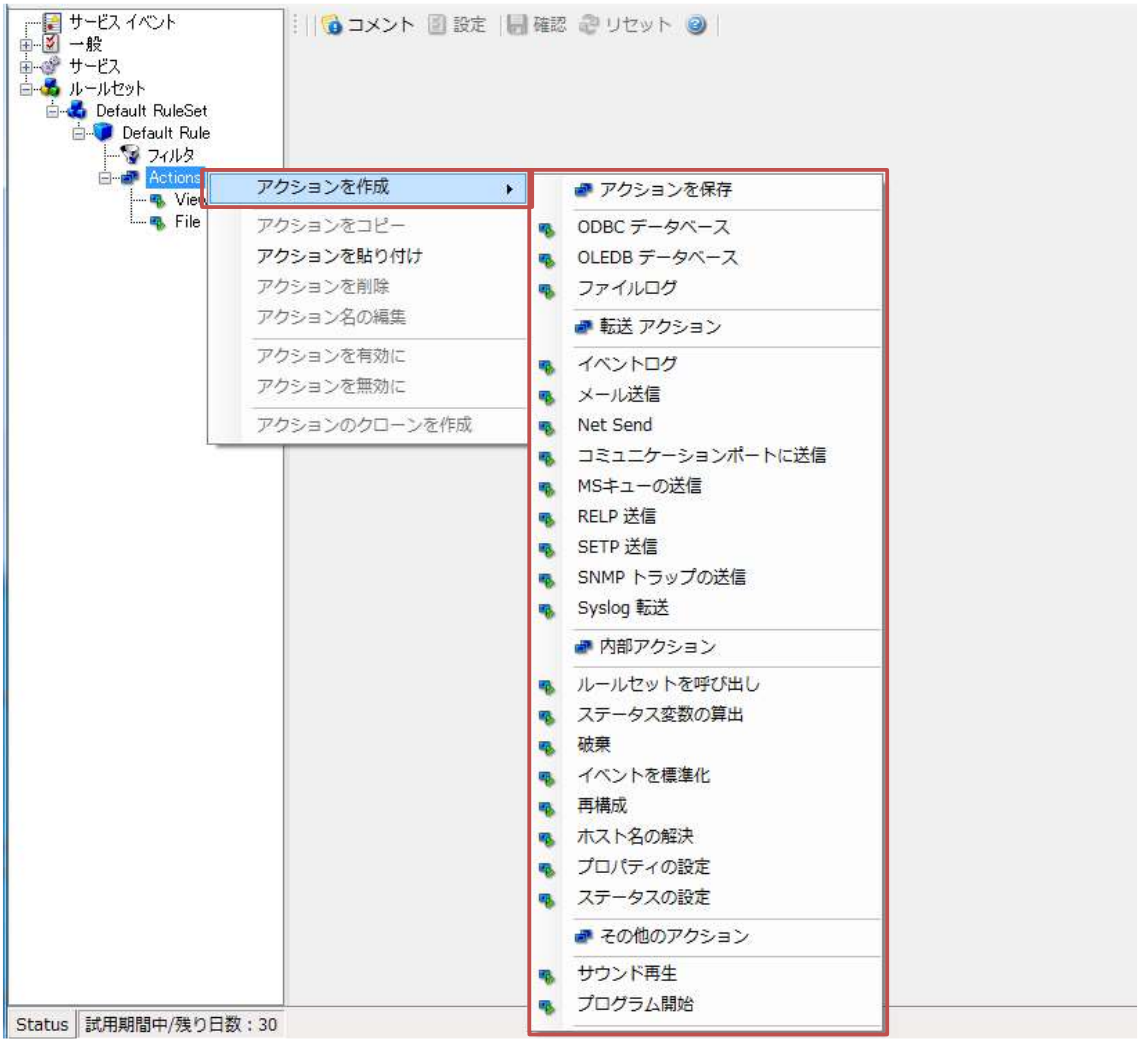
ここでは、アクションについて説明します。

5.6.1. アクションとは

アクションは、特定のイベントに対して何をすべきかをアプリケーションに指示します。アクションを使用すると、イベントを E メールで送信する、Syslog サーバーへ転送する、ファイルまたはデータベースに格納するなど多くのことを行うことができます。

> **メモ**:
> 日本国内ユーザー向け仕様のインストーラーで WinSyslog をインストールした場合、デフォルトとして「Viewer10514」と「File Logging」アクションが設定されています（「Default RuleSet」>「Default Rule」>「Actions」下）。

アクションは、画面左のツリービューの任意のルール配下にある「**Actions**」ノードの下に追加することができます。「**Actions**」ノードを右クリックし「**アクションを作成 >**」のカスケードメニューから追加します。



各ルールには複数のアクションを作成することができます。ルール内にアクションが複数存在する場合、上から順番に処理されます。アクションの表示順序はツールバー上の「**上へ**」「**下へ**」ボタンまたはドラッグアンドドロップ操作で変更することができます。

アクションは3つのグループに分かれています:

- 保存アクション
- 転送アクション
- 内部アクション

5.6.2. 保存アクション

ここでは、「保存アクション」(画面上は「アクションを保存」と表示されています)グループに属するアクションについて説明します。
以下のアクションを含みます:

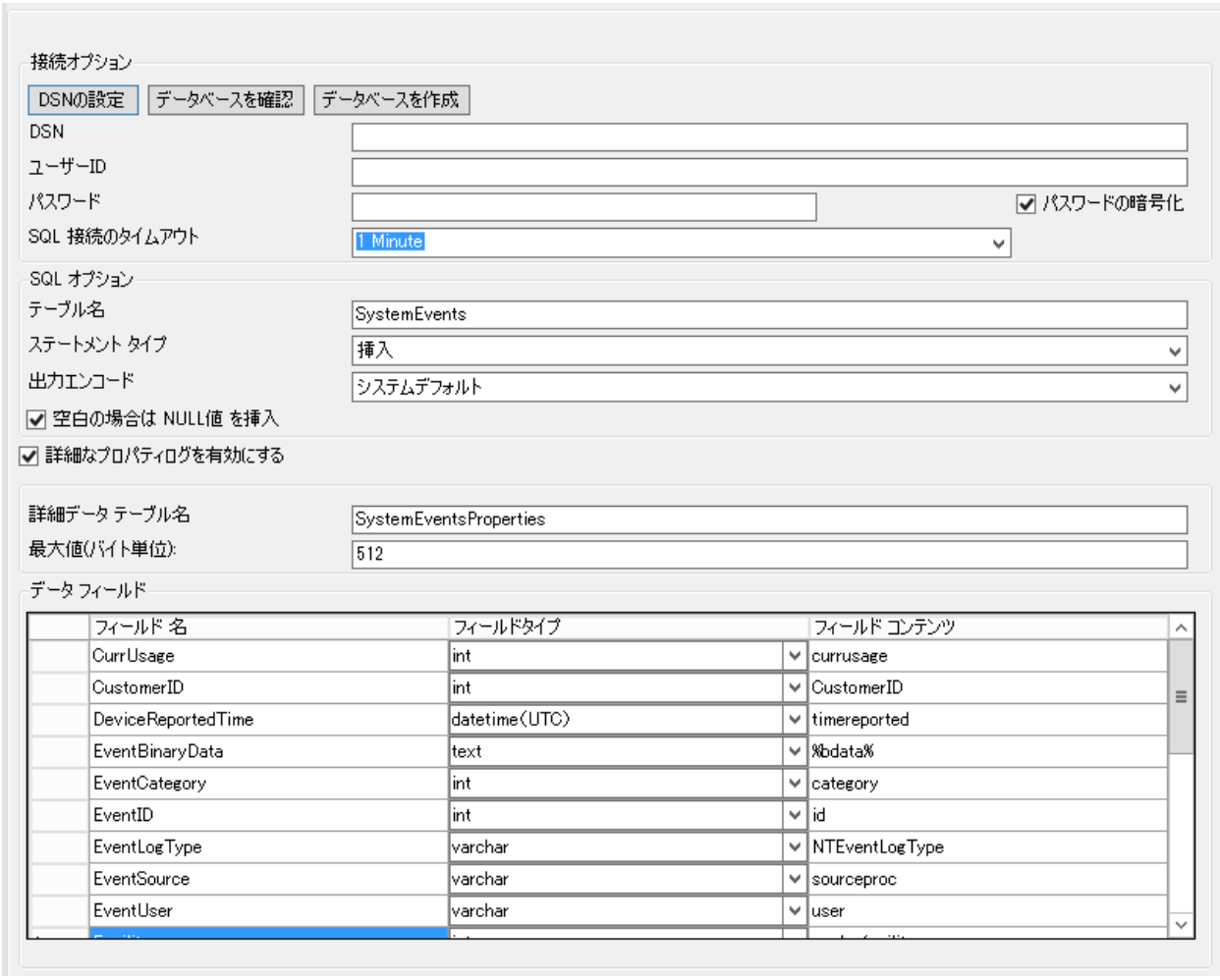
- ODBC データベース
- OLEDB データベース
- ファイルログ

5.6.2.1 ODBC データベース

このアクションは、受信したメッセージを ODBC 準拠のデータベースへ直接書き込むことができます(Windows オペレーティングシステムで現在利用可能なほとんどすべてのデータベースシステムが ODBC をサポートしています)。(Microsoft Access で使用される)Microsoft JET データベース、Microsoft SQL サーバー、MySQL がサポートされます(「データベースを作成」機能でテーブルを作成することができます)。Oracle、Sybase、およびその他のさまざまなシステムで正常に稼動している例もあります。

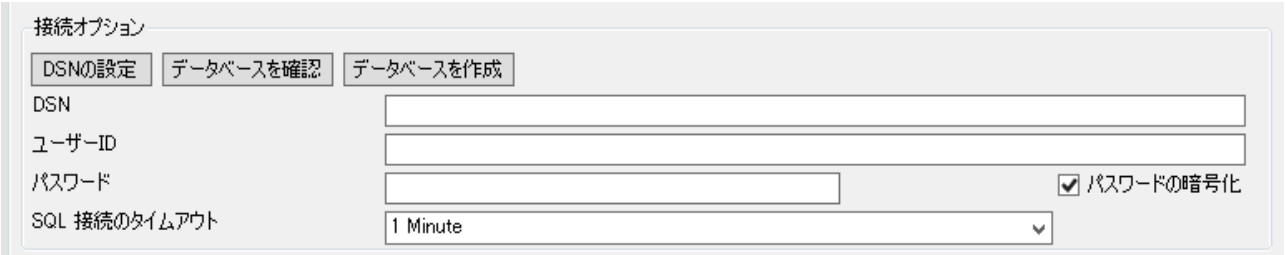
データがデータベースに格納されると、さまざまメッセージビューアやカスタムアプリケーションから簡単に参照することができます。

データベース形式は微調整することができます。これはデータベースで追加の分析を行いたい場合に便利です。また、データ量が多い環境では、フィールドをチューニングすることで性能の向上が期待できます。



接続オプション

ここでは「接続オプション」セクションについて説明します。



DSN の設定

このボタンをクリックすると「**ODBC データソース アドミニストレーター**」ダイアログが表示されます。ここでデータソースを追加、編集、削除することができます。

> **メモ:** 事前に任意の名前でデータベースを作成してください。

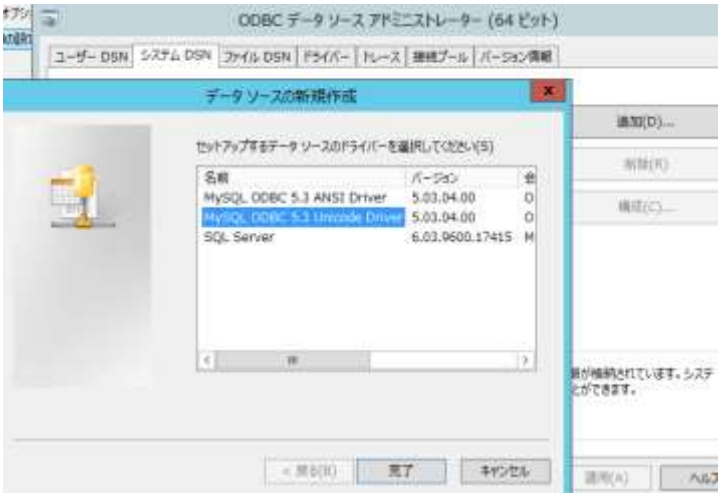
注記:

WinSyslog で使用するデータソースは「**システム DSN**」(「**システム DSN**」タブ画面で追加)でなければなりません。

64bit システムで、Adiscon のサービスを 64bit アプリケーションとして稼動させるために必要なドライバーがあります。

「**ODBC データソース アドミニストレーター**」ダイアログの「**システム DSN**」タブで「**追加**」をクリックすると、「**データ ソースの新規作成**」ダイアログが表示され選択可能なドライバーが表示されます。

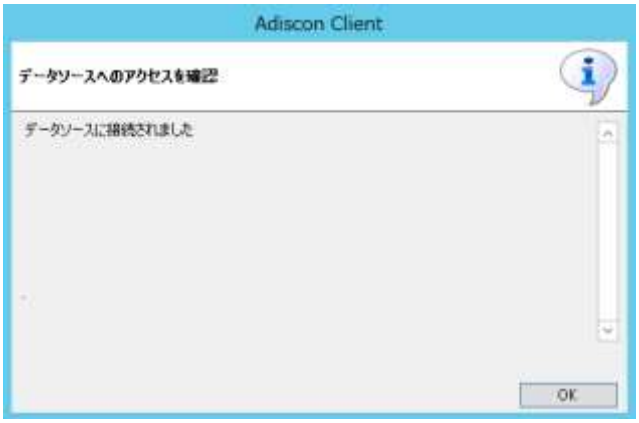
例: MySQL ODBC 5.3 Unicode Driver ver.5.3.4 (64bit)ドライバーを選択:



データソースの設定が完了したら、「**OK**」をクリックして「**ODBC データソース アドミニストレーター**」ダイアログを閉じます。

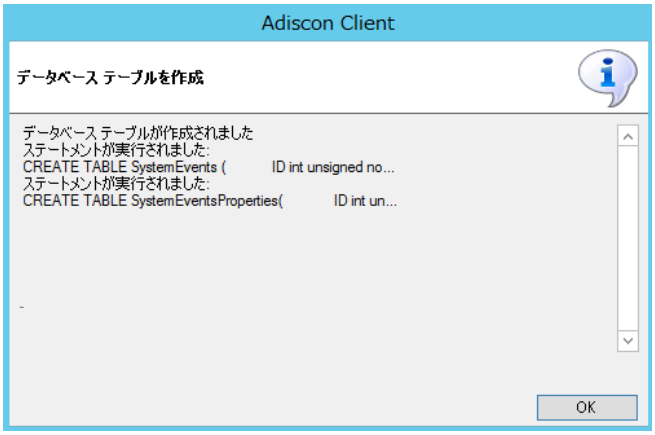
データベースを確認

このボタンをクリックすると、データソースへの接続を確認することができます。



データベースを作成

このボタンをクリックすると、DSN で指定したデータベースに SystemEvents と SystemEventsProperties の2つのデータベーステーブルが自動的に作成されます。



DSN

データベースに接続するときに使用されるシステムデータソース(DSN:データソース名)の名前です。これは「**ODBC データ ソース アドミニストレーター**」で作成します(「**DSN の設定**」ボタンまたは「**Windows コントロールパネル**」>「**管理ツール**」>「**データ ソース (ODBC)**」から作成できます)。

> **注記:**
> DSN は、「**システム DSN**」でなければなりません(「ユーザーDSN」または「ファイル DSN」ではありません)。DSN は正しい接続パラメーター(データベース種類、名前、サーバー名、認証モードなど)で構成してください。

ユーザーID

データベースに接続する際に利用するユーザーID を入力します。ユーザーID の設定が必要か否かは、使用するデータベースシステムに依存します。(例えば、Microsoft Access には必要ありませんが、Microsoft SQL Server には必要です。)不明な場合は、データベース管理者にご確認ください。

パスワード

データベースに接続する際に利用するパスワードを入力します。「**ユーザーID**」で指定したアカウントのパ

スワードでなければなりません。「**ユーザーID**」と同様に、パスワードが必要かどうかは、データベースシステムに依存します。パスワードは、暗号化されていてもされていなくてもどちらでも保存できます。暗号化して保存することを強くお勧めします。

パスワードの暗号化

このチェックボックスをオンにすると、ODBC のパスワードを暗号化して保存します。チェックされていない場合、パスワードは暗号化されずに保存されます。

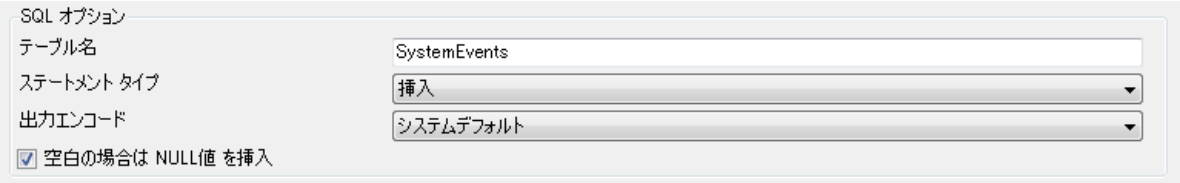
何らかの理由で、暗号化せずにパスワードを保存する場合は、セキュリティに気を付けてください。この場合、アクセス権の制限されたアカウントを使用することをお勧めします。暗号化されている場合でも、限定された特権アカウントを使用することをお勧めします。ここでは、強力な暗号を適用されません。

SQL 接続のタイムアウト

接続のタイムアウトを設定します。

SQL オプション

ここでは「SQL オプション」セクションについて説明します。



テーブル名

ログを記録するテーブルの名前です。この名前は、SQL の insert（挿入）ステートメントを作成するために使用されるので、データベース定義と一致していなければなりません。デフォルトは、「SystemEvents」です。

> **注記：**
> デフォルトのテーブル名は、MonitorWare ファミリーの他のメンバー（Web インターフェイスや MonitorWare コンソールなど）がデータベースで動作する必要がある場合に使用しなければならないことにご注意ください。これは他のソフトウェアまたはカスタムソフトウェアを使用するユーザー向けのカスタマイズオプションです。

ステートメントタイプ

「**挿入**」または「**CALL（MSSQL ストアドプロシージャ）**」（Microsoft 固有のストアドプロシージャ呼び出し）のいずれかを選択できます。このタイプの SQL ステートメントは、MSSQL がデータベースとして使用され

ている場合にのみ機能します。「**CALL（MSSQL ストアドプロシージャ）**」を選択した場合、「**テーブル名**」フィールドが自動的にプロシージャ名として使用されます。

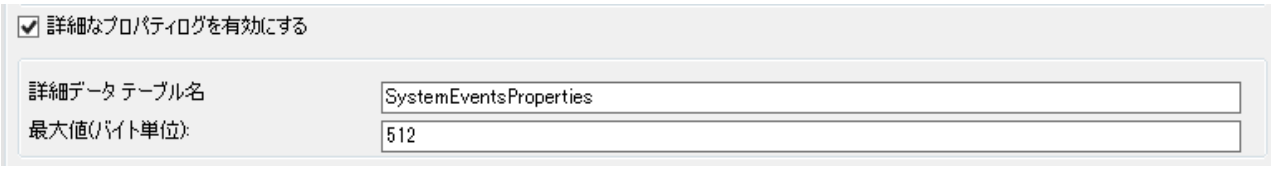
出力エンコード

出力エンコードを「**システムデフォルト**」、「**Unicode (UTF-8)**」、「**SHIFT-JIS**」、「**JIS(ISO-2022JP)**」、「**EUC－JP**」のいずれかから選択できます。

この設定はアジア言語で最も重要です。別のエンコーディングが必要であることが明確でない場合、「**システムデフォルト**」のままにしておくことをお勧めします。「**システムデフォルト**」は、アジア言語（例えば、日本語）の Windows バージョンであっても、ほとんどの場合問題なく機能します。

空白の場合は NULL 値を挿入

このチェックボックスをチェックすると、プロパティが空の場合 NULL 値が挿入されます。



詳細なプロパティログを有効にする

このオプションは、標準プロパティ以外のイベントプロパティを「**詳細データ テーブル名**」に設定したテーブル（デフォルト：SystemEventProperties テーブル）を記録します。1 つのイベントに複数のプロパティがある可能性があるので、このオプションを選択すると複数の書き込みが発生する可能性があります。しかし、Syslog データの場合、追加のプロパティはあまり存在しません。これは「再構成（Post Processing）」アクションを使用して独自のプロパティを定義しているときに最も頻繁に発生します。追加のプロパティは、通常、「イベントログの監視」、「File Monitor」、（およびその他の監視）からの SETP 受信データにあります。

例えば、SETP でイベントログデータを受信すると、これらのプロパティには実際の Windows イベントプロパティとイベントデータが含まれます。これは、Syslog で受信したイベントログメッセージはネイティブイベントではなく Syslog データであるため適用されません。

このチェックボックスをオンにする前に、実際にこれが必要かどうかを確認してください。一部の MonitorWare コンソールレポートには詳細ログが必要となる場合があります。

- **詳細データ テーブル名**

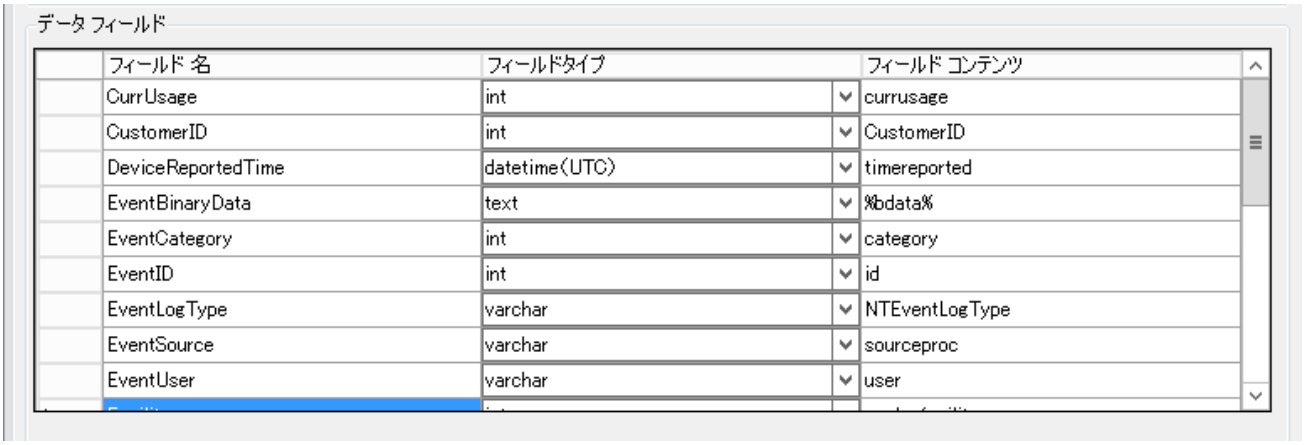
  「**詳細なプロパティログを有効にする**」がオンの場合のみ使用できます。
  詳細データを記録するためのテーブル名です。

- **最大値（バイト単位）**

  「**詳細なプロパティログを有効にする**」がオンの場合のみ使用できます。
  詳細データを記録するためのテーブルの最大値をバイト単位で設定します。

データ フィールド

ここでは「データ フィールド」セクションについて説明します。



「**ODBC データベース**」アクションで最も重要な部分は、データフィールドリストです。デフォルトでは、イベントプロパティの一般的な割り当てがデータベース列へ反映されます。この割り当ては、自由に変更することができます。ただし、（MonitorWare Console などの）Adiscon 分析製品には、指定されたデータベース内容が必要であることに留意してください。データベースの割り当てを変更してからこれらのツールを使用すると、誤動作が発生する可能性があります。

データフィールドには、「**フィールド名**」、「**フィールドタイプ**」、「**フィールドコンテンツ**」が含まれます：

フィールド名

データベースの列名です。テーブル内に任意のフィールドを作成することができます。予め設定されたフィールド名は、Adiscon のスキーマが使用するものです。必要であれば、追加することができます。

フィールドタイプ

データベース列のデータ型です。これは、データベースで選択される列の型を反映しなければなりません。また、格納される実際のプロパティと一致していなければなりません。例えば、syslogpriority のような整数（Integer）型のプロパティは、varchar 列に格納できますが、syslogtag のような文字列（String）型は、整数（Integer）列に格納することはできません。

フィールドコンテンツ

イベントプロパティです。サポートされているプロパティの一覧については、「WinSyslog プロパティリスト」をご参照ください。

文字列（String）型の場合は、プロパティの置換機能を使用できます。例えば、メッセージの最初の 200 文字だけを保存したい場合には、「**フィールドコンテンツ**」欄に"%msg:1:200%"と指定します。

フィールドを追加したい場合は、テーブルの一番下の空白行に入力して「**Enter**」を押します。既存のフィールドを編集したい場合は、行を選択してテキストフィールドを変更します。既存のフィールドを削除したい場合は、行を選択して「**DEL**」を押します。

5.6.2.2 OLEDB データベース

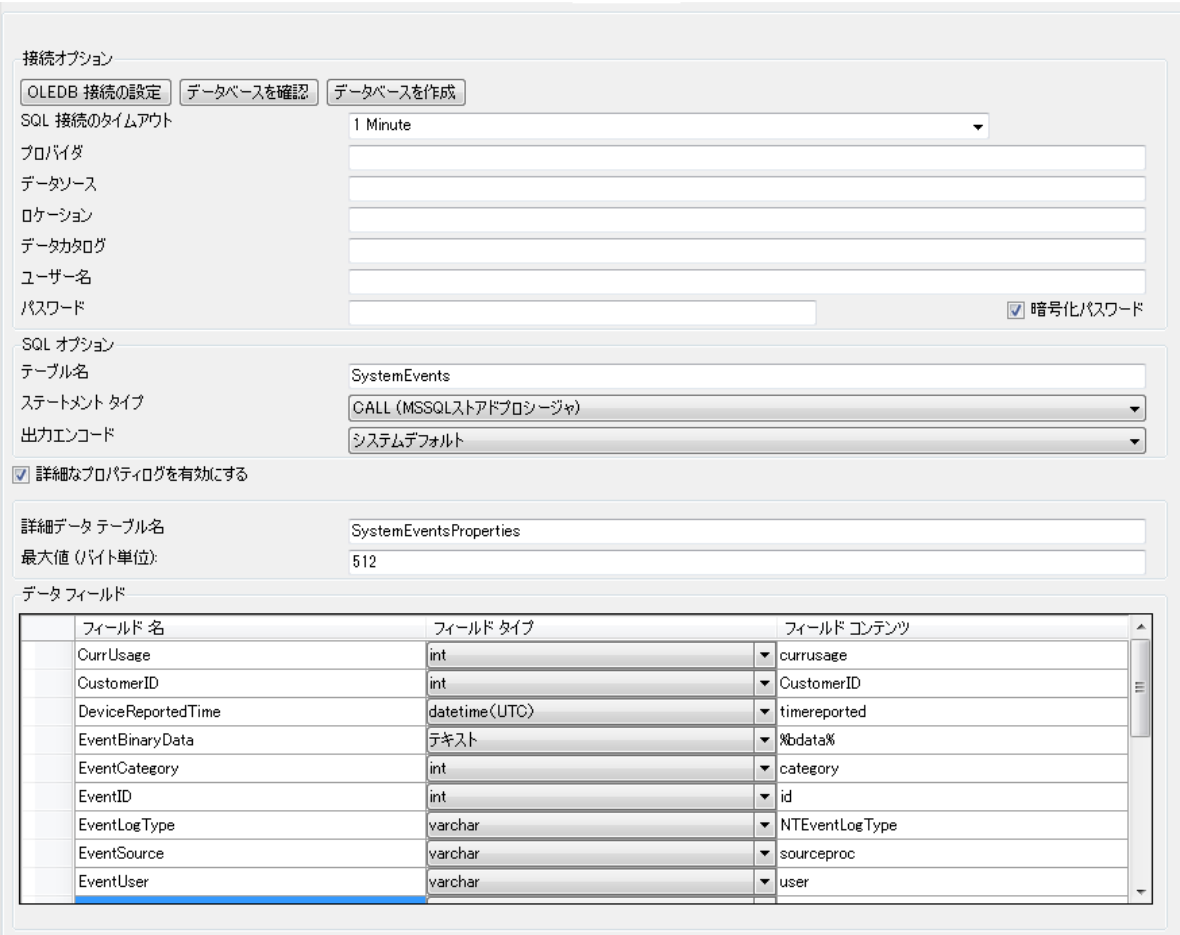
x64 への変更により、Microsoft から OLEDB という新しいデータベースレイヤのサポートも重要になりました。

このアクションは、「ODBC データベース」アクションと同様に、いくつかの構成ポイントから機能します。Win32 環境では、MS SQL OLEDB プロバイダと JET4.0 OLEDB プロバイダは問題なく動作することが確認できておりますが、残念ながら、JET4.0 OLEDB プロバイダはまだ x64 プラットフォームに移植されていません。Adiscon 社での内部パフォーマンステストでは、ODBC に比べて最大 30%向上しました。このため、大量の受信データをデータベースに書き込みたい方にとっては興味があるかもしれません。

このアクションにより、受信したイベントを OLEDB 準拠のデータベースに直接書き込むことができます。

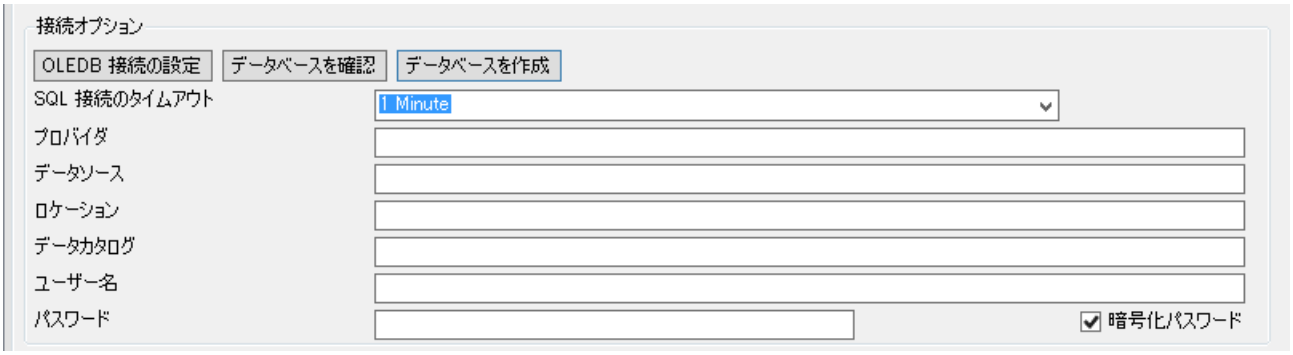
データがデータベースに格納されると、さまざまなメッセージビューアやカスタムアプリケーションから簡単に参照することができます。デフォルト設定は、Adiscon MonitorWare Console 製品および Web インターフェイスに適しています。

データベース形式は微調整することができます。これはデータベースで追加の分析を行いたい場合に便利です。また、データ量が多い環境では、フィールドをチューニングすることで性能の向上が期待できます。



接続オプション

ここでは「接続オプション」セクションについて説明します。



OLEDB 接続の設定

このボタンをクリックすると、「**データ リンク プロパティ**」ダイアログが表示されます。ここでデータソースを追加、編集、削除することができます。

> **メモ:** 事前に任意の名前でデータベースを作成してください。

データベースを確認

このボタンをクリックすると、データソースへの接続を確認することができます。

データベースを作成

このボタンをクリックすると、DSN で指定したデータベースに SystemEvents と SystemEventsProperties の 2 つのデータベーステーブルが自動的に作成されます。

SQL 接続のタイムアウト

接続のタイムアウトを設定します。

プロバイダ

接続する OLE DB プロバイダを指定します。

データソース

データベースに接続するときに使用されるデータソースの名前を指定します。

ロケーション

ロケーションを指定します。

データカタログ

接続に使用するカタログを指定します。

ユーザーID

データベースに接続する際に利用するユーザーID を入力します。

パスワード

データベースに接続する際に利用するパスワードを入力します。

暗号化パスワード

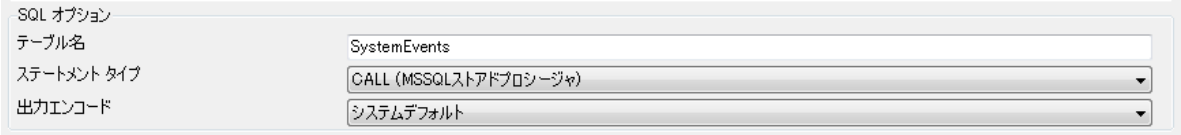
このチェックボックスにチェックをつけると、OLEDB のパスワードを暗号化して保存します。チェックされていない場合、パスワードは暗号化されずに保存されます。この

何らかの理由で、暗号化せずにパスワードを保存する場合は、セキュリティに気を付けてください。この場合、アクセス権の制限されたアカウントを使用することをお勧めします。暗号化されている場合でも、限定

された特権アカウントを使用することをお勧めします。ここでは、強力な暗号を適用されません。

SQL オプション

ここでは「SQL オプション」セクションについて説明します。



テーブル名

ログを記録するテーブルの名前です。この名前は、SQL の insert（挿入）ステートメントを作成するために使用されるので、データベース定義と一致していなければなりません。デフォルトは、「SystemEvents」です。

> **注記：**
> デフォルトのテーブル名は、MonitorWare ファミリーの他のメンバー（Web インターフェイスや MonitorWare コンソールなど）がデータベースで動作する必要がある場合に使用しなければならないことにご注意ください。これは他のソフトウェアまたはカスタムソフトウェアを使用するユーザー向けのカスタマイズオプションです。

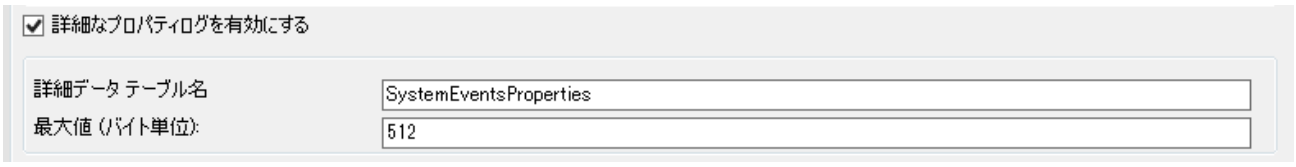
ステートメントタイプ

「**挿入**」または「**CALL（MSSQL ストアドプロシージャ）**」（Microsoft 固有のストアドプロシージャ呼び出し）のいずれかを選択できます。このタイプの SQL ステートメントは、MSSQL がデータベースとして使用されている場合にのみ機能します。「**CALL（MSSQL ストアドプロシージャ）**」を選択した場合、「**テーブル名**」フィールドが自動的にプロシージャ名として使用されます。

出力エンコード

出力エンコードを「システムデフォルト」、「Unicode (UTF-8)」、「SHIFT-JIS」、「JIS(ISO-2022JP)」、「EUC－JP」のいずれかから選択できます。

この設定はアジア言語で最も重要です。別のエンコーディングが必要であることが明確でない場合、「システムデフォルト」のままにしておくことをお勧めします。「システムデフォルト」は、アジア言語（例えば、日本語）の Windows バージョンであっても、ほとんどの場合問題なく機能します。



詳細なプロパティログを有効にする

このオプションは、標準プロパティ以外のイベントプロパティを「**詳細データ テーブル名**」に設定したテーブル（デフォルト：SystemEventProperties テーブル）を記録します。1つのイベントに複数のプロパティがある可能性があるので、このオプションを選択すると複数の書き込みが発生する可能性があります。しかし、Syslog データの場合、追加のプロパティはあまり存在しません。これは「再構成（Post Processing）」アクションを使用して独自のプロパティを定義しているときに最も頻繁に発生します。追加のプロパティは、通常、「イベントログの監視」、「File Monitor」、（およびその他の監視）からの SETP 受信データにあります。

例えば、SETP でイベントログデータを受信すると、これらのプロパティには実際の Windows イベントプロパティとイベントデータが含まれます。これは、Syslog で受信したイベントログメッセージはネイティブイベントではなく Syslog データであるため適用されません。

このチェックボックスをオンにする前に、実際にこれが必要かどうかを確認してください。一部の MonitorWare コンソールレポートには詳細ログが必要となる場合があります。

- **詳細データ テーブル名**

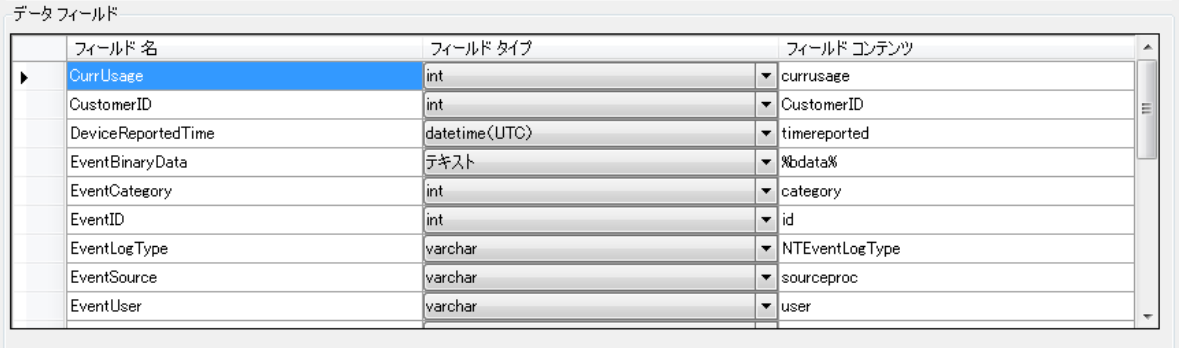
  「**詳細なプロパティログを有効にする**」がチェックされている場合に、詳細データを記録するためのテーブル名です。

- **最大値（バイト単位）**

  「**詳細なプロパティログを有効にする**」がチェックされている場合に、詳細データを記録するためのテーブルの最大値をバイト単位で設定します。

データ フィールド

ここでは「データ フィールド」セクションについて説明します。



「**OLEDB データベース**」アクションで最も重要な部分は、データフィールドリストです。デフォルトでは、イベントプロパティの一般的な割り当てがデータベース列へ反映されます。この割り当ては、自由に変更することができます。ただし、（MonitorWare Console などの）Adiscon 分析製品には、指定されたデータベース内容が必要であることに留意してください。データベースの割り当てを変更してからこれらのツールを使用すると、誤動作が発

生する可能性があります。

データフィールドには、「**フィールド名**」、「**フィールドタイプ**」、「**フィールドコンテンツ**」が含まれます:

フィールド名

データベースの列名です。テーブル内に任意のフィールドを作成することができます。予め設定されたフィールド名は、Adiscon のスキーマが使用するものです。必要であれば、追加することができます。

フィールドタイプ

データベース列のデータ型です。これは、データベースで選択される列の型を反映しなければなりません。また、格納される実際のプロパティと一致していなければなりません。例えば、syslogpriority のような整数(Integer)型のプロパティは、varchar 列に格納できますが、syslogtag のような文字列(String)型は、整数(Integer)列に格納することはできません。

フィールドコンテンツ

イベントプロパティです。サポートされているプロパティの一覧については、「WinSyslog プロパティリスト」をご参照ください。

文字列(String)型の場合は、プロパティの置換機能を使用できます。例えば、メッセージの最初の 200 文字だけを保存したい場合には、「**フィールドコンテンツ**」欄に"%msg:1:200%"と指定します。

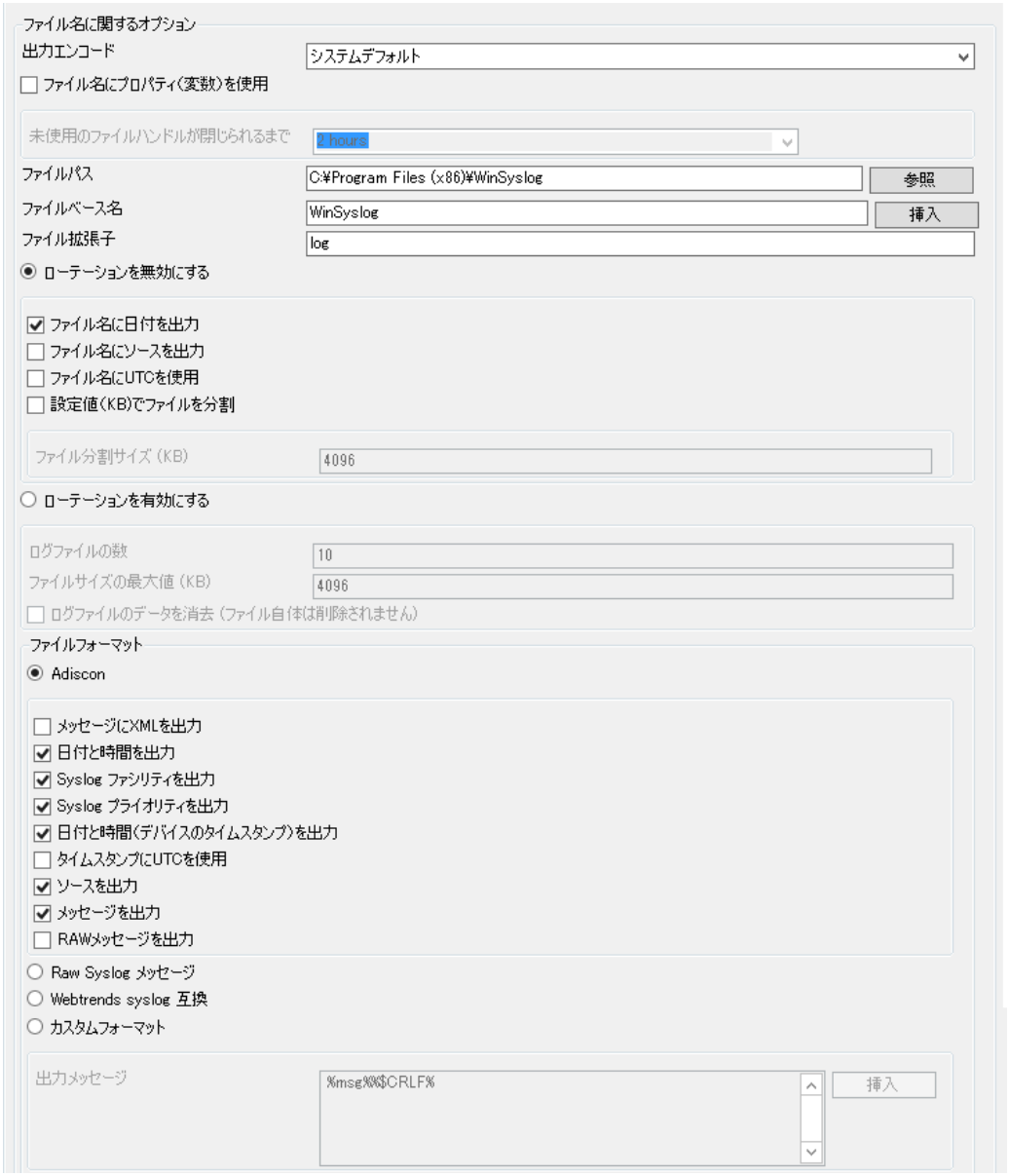
フィールドを追加したい場合は、テーブルの一番下の空白行に入力して「**Enter**」を押します。既存のフィールドを編集したい場合は、行を選択してテキストフィールドを変更します。既存のフィールドを削除したい場合は、行を選択して「**DEL**」を押します。

5.6.2.3 ファイルログ

このアクションは、受信したメッセージをテキストファイルに書き込むために使用します。デフォルト設定の場合、1日1ファイルが書き込まれます。新しいエントリはファイルの末尾に追加されます。

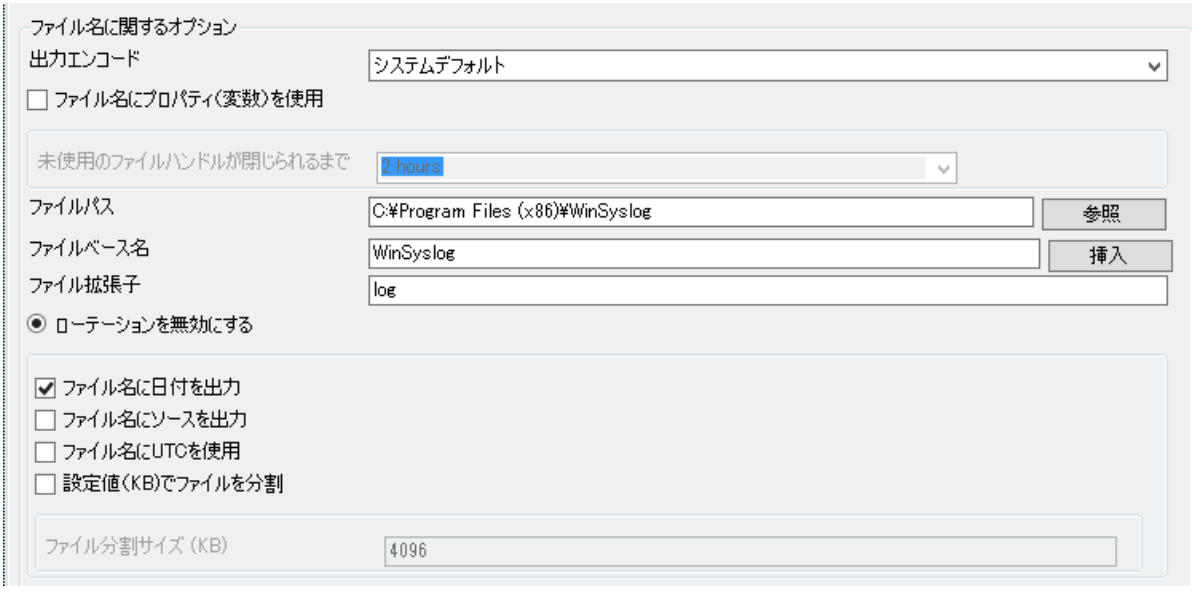
ファイルのロックはデータが書き込まれていないときに解除されます。そのため、他のアプリケーションは、WinSyslog サービスの実行中もファイルにアクセスすることができます。しかし、他のアプリケーションがファイルをロック状態で開かないように注意してください。他のアプリケーションがファイルをロックしている場合、WinSyslog サービスはメッセージを記録することができません(ERROR_SHARING_VIOLATION エラーイベントが Windows イベントログに書き込まれます)。WinSyslog サービスの稼働中に書き込み中のファイルにアクセスする場合は、ファイルをコピーするか、開いたファイルをロックしないメモ帳(notepad.exe)などを使用ください。
ファイル名は以下のとおりです(括弧内(<>)はオプション名です。自由に設定することができます):

<ファイルパス><ファイルルベース名>-年-月-日.<ファイル拡張子>



ファイル名に関するオプション

ここでは「ファイル名に関するオプション」セクションについて説明します。



出力エンコード

受信したメッセージをファイルに書き込む際の出力エンコードを「システムデフォルト」、「Unicode (UTF-8)」、「Unicode (UTF-16)」、「SHIFT-JIS」、「JIS(ISO-2022JP)」、「EUC－JP」のいずれかから選択できます。

ファイル名にプロパティ(変数)を使用

このチェックボックスをオンにすると、%source%などのプロパティを「ファイルパス」や「ファイルベース名」で使用できます。
オフの時の保存先及びファイル名は「C:¥temp¥MonitorWare-年-月-日.log」です。

例えば、以下のように指定した場合、

「**ファイルパス名**」: F:¥syslogs¥%source%
「**ファイルベース名**」: IIS-%source%

ソースが「10.0.0.1」の場合、ファイル名は「F:¥syslogs¥10.0.0.1¥IIS-10.0.0.1.log」となります。
”F:¥syslogs¥10.0.0.1”というパスが生成されたのは、「**ファイルパス名**」に%source%プロパティが使用されたためです。

> **注記:**
> 「ファイルパス」と「ファイルベース名」には、その他にも様々なプロパティを指定することができます。
> 詳しくは、別紙「WinSyslog プロパティリスト」および「標準ログサーバー設定」をご参照ください。

- **未使用のファイルハンドルが閉じられるまで**

  「**ファイル名にプロパティ(変数)を使用**」がオンの場合にのみ使用できます。

  動的なファイル名が使用されると、大量のファイルのオープン/クローズ操作を避けるために、ファイルハンドルが内部的にキャッシュされます。ここでは、使用されなくなったときにファイルハンドルを最後に閉じなければならないタイムアウト時間を指定します。ファイルへの書き込みごとに、現在のファイルハンドルのタイムアウトカウンタがリセットされます。

ファイルパス

ファイルを保存するフォルダのパス(ディレクトリ)を指定します。テキストボックスに直接入力するか、「**参照**」ボタンから保存先のフォルダを選択します。

「**ファイル名にプロパティ(変数)を使用**」がオンの場合、パス名に%source%などのプロパティを入力することができます(例:F:¥syslogs¥%source%)。プロパティについて詳しくは、別紙「WinSyslog プロパティリスト」をご参照ください。

ファイルベース名

ファイルのベース名を入力します。デフォルトは WinSyslog です。

「**ファイル名にプロパティ(変数)を使用**」がオンの場合は、「**挿入**」ボタンをクリックすることで、ファイル名に%source%などのプロパティを入力することができます(例:IIS-%source%)。プロパティについて詳しくは、別紙「WinSyslog プロパティリスト」をご参照ください。

ファイル拡張子

ファイルの拡張子を指定します。デフォルトは log です。

ローテーションを無効にする

オンの場合、ファイルはローテーションされません。

- **ファイル名に日付を出力**

  このチェックボックスをオンにすると、ファイル名に日付が含まれるようになります(例:WinSyslog-2017-06-30.log)。つまり毎日新しいファイルが作成されます。

  オフの場合は、ファイル名に日付は含まれません。このため、「**ファイルベース名**」で指定したファイルに出力され続けることになります。ファイル名を参照するカスタムスクリプトを持つユーザーの中には、この設定を使用する方もいます。

- **ファイル名にソースを出力**

  このチェックボックスをオンにすると、Syslog メッセージのソース（送信元）が自動的にファイル名に追加されます（ファイル名にソースのデバイス情報が含まれます）。

  この機能は、デバイスごとに別のファイルを作成する場合に使用します。これは複数のルールを作成することで実現できますが、このチェックボックスを使う方がずっと簡単です。

- **ファイル名に UTC を使用**

  これは、「**ファイル名に日付を出力**」設定とともに機能します。

  このチェックボックスをオンにすると、ファイル名は「協定世界時（UTC）」に基づいて生成されます。オフの場合は、「ローカルタイム」に基づいて生成されます。

  UTC は、以前は「GMT」と呼ばれ、タイムゾーンシステムの基礎となっています。日本の場合、「ローカルタイム」は「UTC」より 9 時間進んでいます。「UTC」で正午であれば、日本は午後 9 時です。

  ログファイルの作成に関しては、日付は「UTC」で計算されることを意味しています。同じ例を考えてみると、このチェックボックスがオンの場合、ファイル名は日本時間の午前 9 時に次の日付にロールオーバーされます。オフの場合は、日本時間の午前 0 時（UTC の午後 3 時）にロールオーバーされます。

  ログファイルが異なるタイムゾーンに書き込まれ、後でそれらを統合しなければならない場合は、「UTC」を使用するとすべてのログファイルで一貫した時刻表記となるため役立ちます。時差の問題に無関係の場合には、このチェックボックスはオフとし、「ローカルタイム」を基準にしてください。

  > **注記：**
  > この設定はファイル名の作成のみに影響します。ファイル内に記録される日付は、別の設定で制御します。

- **設定値（KB）でファイルを分割**

  このチェックボックスをオンにすると、「**ファイル分割サイズ（KB）**」で指定したサイズに達するとファイルが分割されます。ファイル名には連続した番号（_1 から _n）が付加されます。
  例：
  WinSyslog-2017-04-26_1.log
  WinSyslog-2017-04-26_2.log
  WinSyslog-2017-04-26_3.log

- **ファイル分割サイズ（KB）**

  「**設定値（KB）でファイルを分割**」がオンの場合にのみ使用できます。
  ファイルの上限サイズを指定します。

ローテーションを有効にする

ここでは「ローテーションを有効にする」セクションについて説明します。

ローテーションを有効にする

有効の場合、下の 3 つの条件でファイルがローテーション（循環）されます。

- **ログファイルの数**

  ここで指定した最後のログファイルに達すると、ローテーション（循環）され、最初のファイルに書き込まれます。

- **ファイルサイズの最大値（KB）**

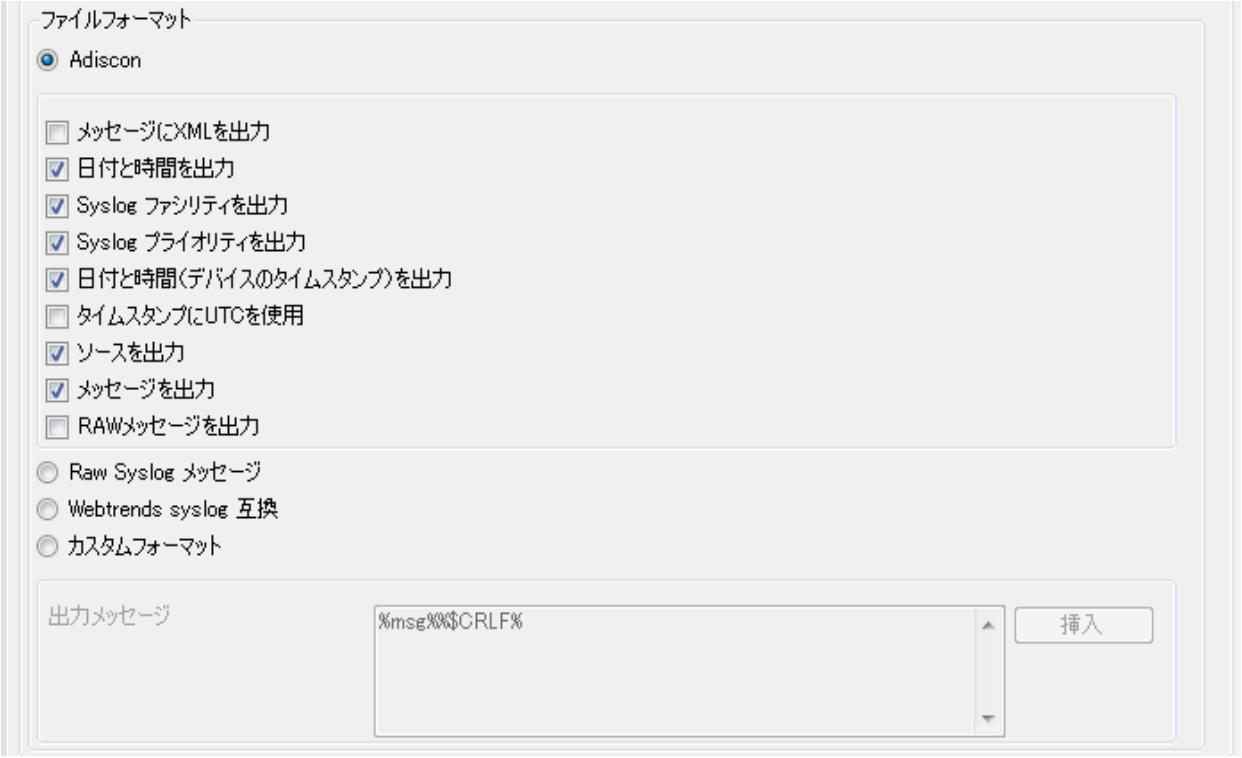
  ここで指定したファイルサイズに達すると、新しいログファイルが作成されます。

- **ログファイルのデータを消去（ファイル自体は削除されません）**

  このチェックボックスをオンにすると、ファイルローテーションの際に、元のファイルを削除して新しくファイル再作成するのではなく、元のファイルの中身（データ）だけが消去されるようになります。
  WinSyslog のログファイルを別のアプリケーションで監視している場合などに有効です。

ファイルフォーマット

ここでは「ファイルフォーマット」セクションについて説明します。



ここでは、ログファイルに書き込むフォーマットを設定します。デフォルトは「Adiscon」です。他の形式を使用することで、他のアプリケーションとの互換性を高めることもできます。

Adiscon

Adiscon フォーマットを選択した場合には、以下にある様々な出力オプションを選択することができます。

- **メッセージに XML を出力**

  このチェックボックスをオンにすると、メッセージ部分に完全な XML フォーマットの情報レコードが含まれます。XML フォーマットでメッセージを出力することで、タイムスタンプ、Syslog ファシリティ、プライオリティなどの追加情報を解析しやすくなります。このオプションを選択した場合、XML ストリームにすべての情報が含まれているため、他のすべてのチェックボックスをオフにすることもできます。しかし、これは必要条件ではありません。

以下の「XXXX を出力」チェックボックスは、ログファイルに書き込むフィールドを指定するために使用します。メッセージ部分（%msg%）以外のすべてのフィールドはオプション（任意）です。以下のチェックボックスでオンのフィールドはログファイルに書き込まれますが、オフの場合は書き込まれません。フィールドはカンマ区切りで書き込まれます。

- **日付と時間を出力**

  このチェックボックスをオンにすると、WinSyslog がメッセージを受信した日時が出力されます。

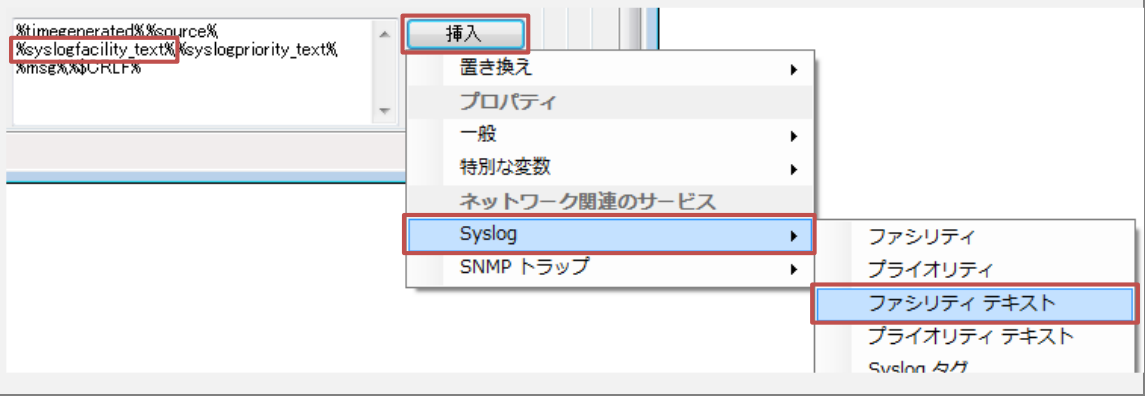
注記:
「日付と時間(デバイスのタイムスタンプを使用)」との違いに注意してください。両方ともタイムスタンプですが、この「日付と時間」は WinSyslog がメッセージを受信した時刻です。「**タイムスタンプに UTC を使用**」チェックボックスがチェックされている場合は UTC 時間、チェックされていない場合はローカルタイムが書き込まれます。

- **Syslog ファシリティを出力**

このチェックボックスをオンにすると、Syslog ファシリティが数字で出力されます。

例: User ファシリティは 01 として出力されます。
2017-07-04,10:44:30,192.168.30.12,01,03,This is a test message.

注記:
Syslog ファシリティを数字ではなくテキストで出力したい場合は、「**カスタムフォーマット**」を選択し、「**出力メッセージ**」フィールドに「**ファシリティ テキスト**」(%syslogfacility_text%)を挿入(「**挿入**」>「**Syslog**」>「**ファシリティ テキスト**」を選択)します。



例: 「カスタムフォーマット」で「ファシリティ テキスト」を選択した場合
2017-07-04 10:57:30,192.168.30.12,User,Error,This is a test message.

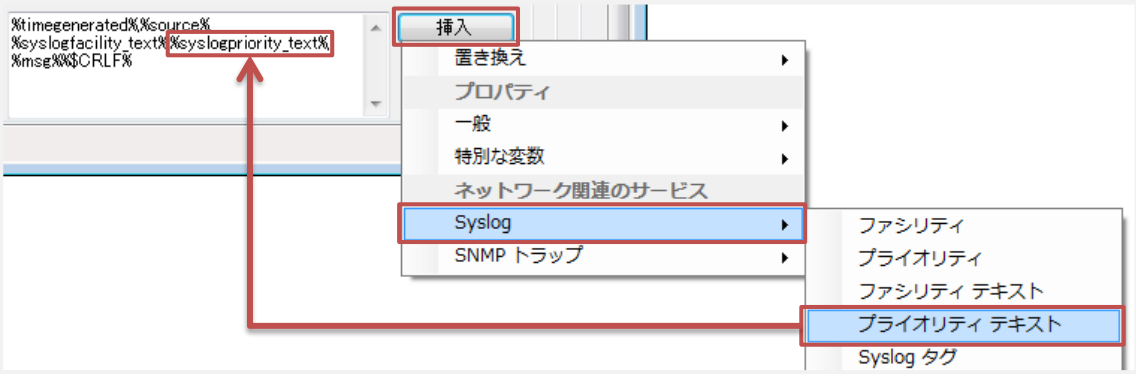
- **Syslog プライオリティを出力**

このチェックボックスをオンにすると、Syslog プライオリティ(Severity)が数字で出力されます。

例: Error プライオリティ(Severity)は 03 として出力されます。
2017-07-04,10:44:30,192.168.30.12,01,03,This is a test message.

注記:

Syslog プライオリティ(Severity)を数字ではなくテキストで出力したい場合は、「**カスタムフォーマット**」を選択し、「**出力メッセージ**」フィールドに「**プライオリティ テキスト**」(%syslogpriority_text%)を挿入(「**挿入**」>「**Syslog**」>「**プライオリティ テキスト**」を選択)します。



例:「カスタムフォーマット」で「プライオリティ テキスト」を選択した場合

2017-07-04 10:57:30,192.168.30.12,User,Error,This is a test message.

- **日付と時間(デバイスのタイムスタンプ)を出力**

このチェックボックスをオンにすると、実際のメッセージから取り出されたタイムスタンプが出力されます。

注記:

「日付と時間」との違い注意してください。両方ともタイムスタンプですが、この「**日付と時間(デバイスのタイムスタンプ)を出力**」は受信したメッセージから取り出したタイムスタンプです。このため、デバイスのクロックに依存しますが、オフになっている場合もあります。また、Syslog メッセージの場合、デバイスが報告するタイムスタンプにタイムゾーン情報はありません。このため、複数のタイムゾーンにデバイスが存在する場合、タイムスタンプ情報はばらばらになってしまいます。これは、RFC 3164 の Syslog の仕様によるものです。この場合、Syslog サーバーは RFC を無視し、一貫したタイムスタンプを提供するように設定することができます。ただし、ログファイルライターの観点からは、このオプションは「日付と時間」と同程度信用できない場合があります。そうではあっても、「日付と時間」よりは有効かもしれないため、両方のタイムスタンプを選択できるようになっています。

- **タイムスタンプに UTC を使用**

  このチェックボックスをオンにすると、すべてのタイムスタンプが UTC で書き込まれます。オフの場合は、ローカルタイムで書き込まれます。UTC は複数のタイムゾーンで書き込まれたログを統合したい場合に、便利です。

- **ソースを出力**

  このチェックボックスをオンにすると、Syslog のソース（送信元）が出力されます。

  > **注記：**
  > このアクションが属するルールセットが関連付けられた Syslog サービスの「**Syslog メッセージからソースシステムを取り出す**」チェックボックスがチェックされている場合は、（RFC 3164 による）Syslog メッセージからソースシステムの名前または IP アドレスが抽出されます。チェックされていない場合は、Syslog メッセージの送信元が出力されます。

- **メッセージを出力**

  このチェックボックスをオンにすると、「メッセージ」として解析された Syslog メッセージの一部が出力されます。「メッセージ」部分は、Syslog メッセージからタグ値（PRI 部）やホスト情報など（HEADER 部）が除外されています。

  > **注記：**
  > 「**メッセージを出力**」と「**RAW メッセージを出力**」のどちらか1つを選択することをお勧めします。これら両方を選択した場合は、2つのメッセージフィールドが書き込まれます（メッセージ内容が重複します）。両方を選択しない場合は、メッセージは全く書き込まれません。両方とも選択する、両方とも選択しない、どちらの設定もサポートされることにご注意ください。これは正当な理由があるかもしれないためです。

- **RAW メッセージを出力**

  このチェックボックスをオンにすると、受信したメッセージそのものが出力されます（変更されません）。これは、他のアプリケーションで RAW Syslog（未処理の Syslog）メッセージが必要とされている場合に便利です。

注記:
「**メッセージを出力**」と「**RAW メッセージを出力**」のどちらか1つを選択することをお勧めします。これら両方を選択した場合は、2つのメッセージフィールドが書き込まれます（メッセージ内容が重複します）。両方を選択しない場合は、メッセージは全く書き込まれません。両方とも選択する、両方とも選択しない、どちらの設定もサポートされることにご注意ください。これは正当な理由があるかもしれないためです。

Raw Syslog メッセージ

このフォーマットを選択すると、Raw Syslog 形式（送信元デバイスが送信したメッセージそのもの、「生ログ」と呼ばれることもあります）がログファイルに書き込まれます。つまり、ログファイルには RFC3164 の Syslog メッセージが1行ごとに書き込まれます。特定のフィールド処理や情報の追加は行われません。他の（互換性を持たせたい）アプリケーションの中にはこの形式が必要なものもあります。

webtrends syslog 互換

このフォーマットを選択すると、webtrends アプリケーションが期待するフォーマットを模倣します。このフォーマットは、ログファイルのフォーマットを模倣しただけに過ぎないということに注意してください。正確な webtrends WELE フォーマットを生成するのは、レポートするデバイス側の仕事です。

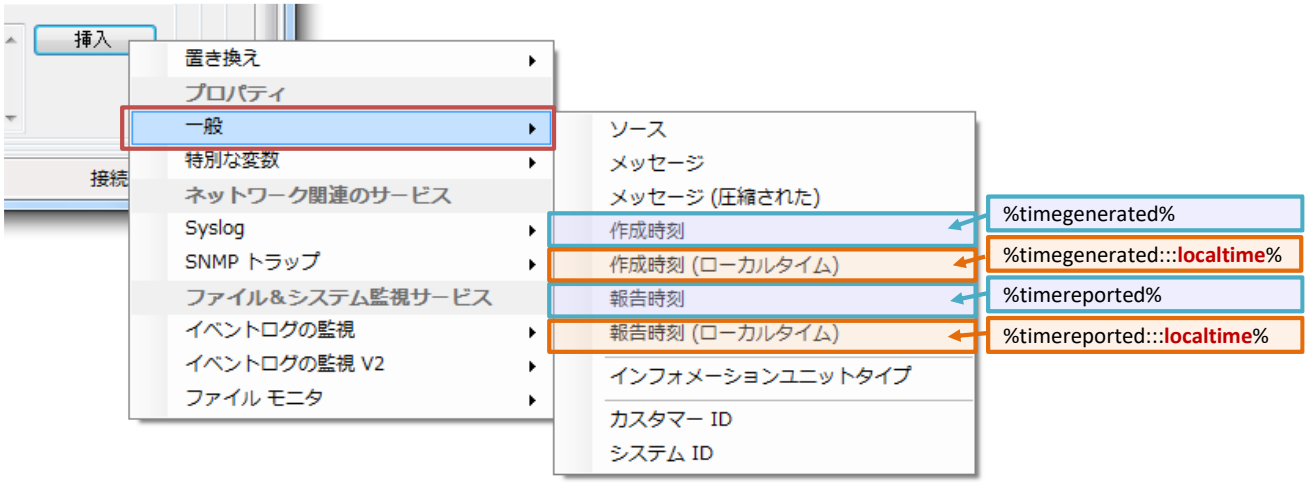
カスタムフォーマット

このフォーマットを選択すると、出力フォーマットを完全にカスタマイズすることができます。これにより、他のアプリケーションとの互換性を高めることができます。

- **出力メッセージ**

  「**カスタムフォーマット**」が選択されている場合に、出力フォーマットをここで指定します。「**挿入**」ボタンをクリックすることでプロパティを挿入することができます。デフォルト値は、「%msg%%$CRLF%」（"%msg%"はメッセージ、"%$CRLF%"は改行コード）です。

時刻についての注意事項:
「**作成時刻**」（%timegenerated%）または「**報告時刻**」（%timereported%）プロパティを使用すると、協定世界時（UTC）を基準として時刻が記録されます。日本標準時（JST）は、協定世界時（UTC）より9時間進んでいるため、ログファイルに記録される時刻は、日本時間（ローカルタイム）-9時間の時刻となります。このため、日本時間（ローカルタイム）で時刻をファイルに記録したい場合は、「**作成時刻（ローカルタイム）**」、「**報告時刻（ローカルタイム）**」を使用してください。「（ローカルタイム）」付きの時刻プロパティには「:::localtime」が付与されます。



出力メッセージに使用できるプロパティについては、別紙「WinSyslog プロパティリスト」をご参照ください。

5.6.3. 転送アクション

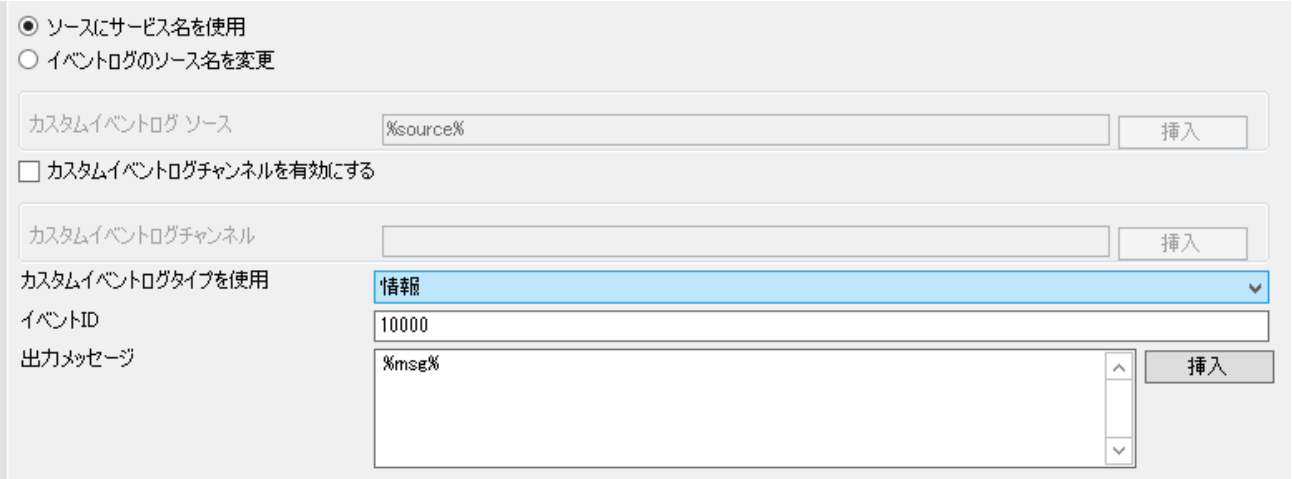
ここでは、「転送アクション」グループに属するアクションについて説明します。

以下のアクションを含みます:

- イベントログ
- メール送信
- Net Send
- コミュニケーションポートに送信
- MS キューの送信
- RELP 送信
- SETP 送信
- SNMP トラップの送信
- Syslog 転送

5.6.3.1 イベントログ

このアクションは、Syslog メッセージをイベントログに記録するために使用します。



ソースにサービス名を使用

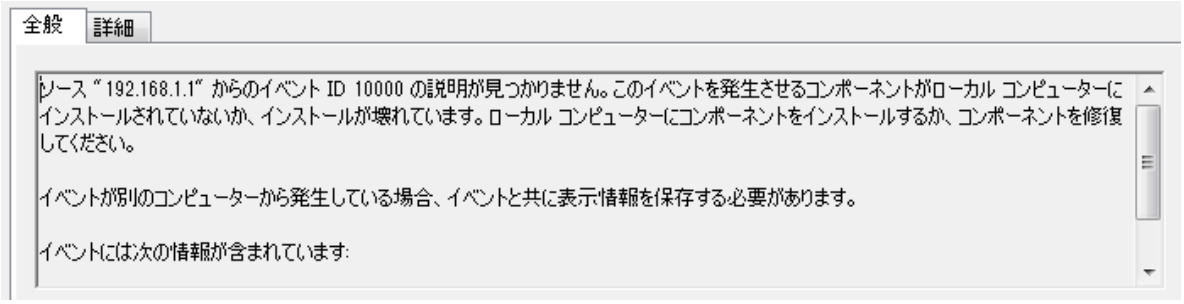
オンにすると、ログエントリのログソースとしてサービス名（AdisconWinSyslog）が使用されます。

イベントログのソース名を変更

オンにすると、下の「**カスタムイベントログ ソース**」フィールドに入力したプロパティ値がイベントログソースとして設定されます。このモードは、Windows イベントビューアでシステムステータスに関する情報をすばやく収集したい場合に役立ちます。

> **注記：**
> このモードには欠点があります。このオプションをオンにすると、無効なイベントソース情報をイベントログに書き込むことになります。これ自体は他のアプリケーションに影響を与えませんが、Windows イベントビューアは一致するメッセージライブラリを見つけることができないことをユーザーに警告します。（警告は表示されますが）ログメッセージは問題なく表示されます。このオプションをオンにする前に、利用環境でのマッピングメカニズムの影響を十分理解してください。

警告メッセージ例：



- **カスタムイベントログ ソース**

  「**イベントログのソース名を変更**」がオンの場合のみ使用できます。
  イベントログのソースとして使用したいプロパティを指定します。「**挿入**」ボタンをクリックすることでプロパティを挿入することができます。

  挿入できるプロパティについては、別紙「WinSyslog プロパティリスト」をご参照ください。

カスタムイベントログチャンネルを有効にする

このチェックボックスをオンにすると、イベントログチャンネルをカスタマイズすることができます。

- **カスタムイベントログチャンネル**

  「**カスタムイベントログチャンネルを有効にする**」がオンの場合に、イベントログチャンネルとして使用したいプロパティを指定します。

カスタムイベントログタイプを使用

このログエントリのタイプまたはレベルを指定します。使用可能な Windows システム値（成功、エラー、警告、情報、成功の監査、失敗の監査）から選択します。

イベント ID

イベントログに書き込むイベント ID を指定します。他のプロセスに特定のメッセージに対して整合性のあるインターフェイスを与えるために、異なる ID を使用することができます。

> **注記：**
>
> WinSyslog は使用できる ID を制限しませんが、オペレーティングシステムに登録されていない ID が書き込まれた場合、Windows イベントビューアは実際のメッセージテキストの前に ID が登録されていないことを指摘するエラーメッセージを表示します。このエラーを避けるために、イベント ID 10,000 から 10,100 が OS に登録されています。カスタマイズした全てのメッセージにはこれらの ID を使用することを強くお勧めします。
>
> 10,000 未満の ID は、WinSyslog 自体が生成するイベントと衝突する可能性があるため、使用しないでください。

出力メッセージ

Windows イベントログに書き込むメッセージを指定します。

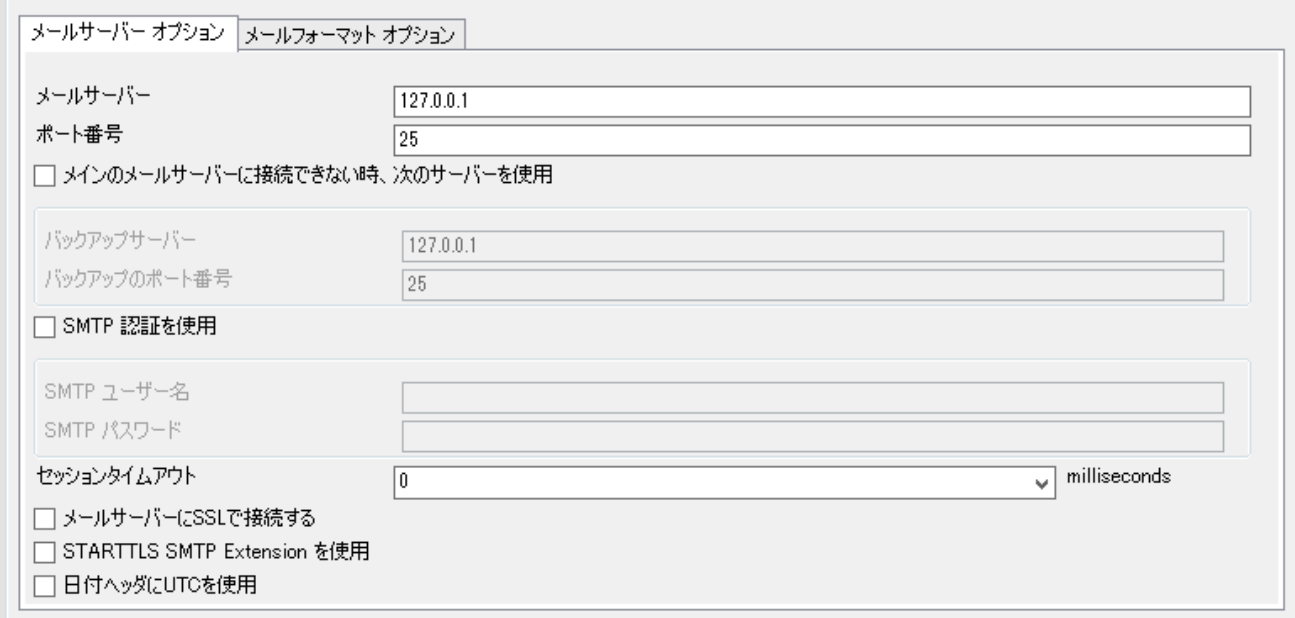
「**挿入**」ボタンからメッセージに出力したいプロパティを選択することができます。挿入できるプロパティにつ

いては、別紙「WinSyslog プロパティリスト」をご参照ください。

5.6.3.2 メール送信

このアクションは、WinSyslog で受信したメッセージを E メール送信する場合に使用します。

デフォルト設定の場合、1つの受信メッセージにつき1通 E メールが送信されます。このアクションは、緊急の通知を行うための機能です。E メールレポートを提供するための機能ではありません。



メールサーバー オプション

ここでは、「メールサーバーオプション」タブについて説明します。
メール送信に使用するメール（SMTP）サーバーの情報を正しく設定する必要があります。

メールサーバー

メッセージの転送に使用するメールサーバーの名前または IP アドレスを指定します。IPv4 アドレス、IPv6 アドレス、IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを使用できます。

> **注記：**
>
> 受信者がこのサーバーでホストされていない場合、メッセージがリレーされる可能性があります。不明な場合はメールサーバーの管理者に問い合わせてください。
>
> このアクションは標準の SMTP メールサーバーと通信することを想定しています。最終宛先へのメッセージリレーは許可されていなければなりません。

ポート番号

メールサーバーに接続するためのポート番号を指定します。

> **注記:**
> 通常は 25 番ポートが使用されますが、別のポートが使用されている場合もあります。不明な場合はメールサーバーの管理者に問い合わせてください。

メインのメールサーバーに接続できない時、次のサーバーを使用

このチェックボックスをオンにすると、通常のメールサーバーが利用不能またはアクセス不能な場合に使用するセカンダリ(2 番目)のメールサーバーを構成することができます。。

> **注記:**
> 下の「**バックアップサーバー**」で指定したメールサーバーへの接続にも失敗した場合にのみ、エラーが生成されます。

- **バックアップサーバー**

  「**メールサーバー**」フィールドで指定したメールサーバーへの接続が確立できない場合に使用するバックアップのメールサーバーを指定します。

  > **注記:**
  > どれくらいのメールがバックアップサーバーで処理されるかは、セッションがクローズされるまでに実行されたメールアクションの数に依存します。このセッションがクローズされると、その後は、再びメインのサーバーへの接続が試みられます。接続が確立できない場合には、再度バックアップのサーバーが使用されます。

- **バックアップのポート番号**

  メールサーバーに接続するためのポート番号を指定します。

  > **注記:**
  > 通常は 25 番ポートが使用されますが、別のポートが使用されている場合もあります。不明な場合はメールサーバーの管理者に問い合わせてください。

SMTP 認証を使用

サーバーが SMTP 認証を要求する(またはサポートしている)場合、このチェックボックスをオンにして下の「**SMTP ユーザー名**」と「**SMTP パスワード**」を入力します。多くのサーバー管理者は、SPAM 対策のた

めに認証されたユーザーに対してのみリレーを許可しています。サーバーが匿名の投稿（anonymous posting）を許可しないように再設定されると、既存のアカウントが使用できなくなる可能性もあります。

> **注記：**
>
> メールサーバーが認証をサポートしていない場合は、オフにしてください。
>
> メールサーバーが認証をサポートしている場合は、オンにすることをお勧めします。現在のサーバー構成で認証されていないリレーが許可されている場合であっても、将来（SPAM の問題が拡大すると）変更される可能性があります。すでに認証を使用している場合は、そのようなサーバー構成の変更による影響はありません。認証を使用していない場合は、サーバー構成の変更によりメールサービスが止まってしまう恐れがあります。

- **SMTP ユーザー名**

  認証に使用するユーザーID を入力します。

  > **注記：**
  > 正確な値を入力してください。不明な場合はメールサーバー管理者に問い合わせてください。

- **SMTP パスワード**

  認証に使用するパスワードを入力します。

  > **注記：**
  > 正確な値を入力してください。不明な場合はメールサーバー管理者に問い合わせてください。

セッションタイムアウト

このオプションは、短い間隔で受信する複数のメッセージを1つの E メールメッセージに統合かどうかを制御します。サーバーとの SMTP セッションは、指示されたタイムアウトに達するまで開いたままになります。タイムアウト期間は、プルダウンから選択するか「Custom」を選択して値を直接入力してミリ秒で指定します。2つのメッセージがどんなに高速に発生しようが関係なく、それぞれのイベントが別々のメッセージで送信されます。

指定されたタイムアウト期間内に新しいイベントを受信した場合は、そのイベントは前のイベントと同じ E メールメッセージに含まれます。その後、タイムアウトが再開されます。このように、タイムアウト期間内に受信したイベントは、単一のメールにまとめられます。

このオプションは、メッセージの大量なバーストが予想され、これらを少数の E メールメッセージにまとめた

い場合に最適です。そうしない場合、管理者のメールボックスは大量のメールによりオーバーフローしてしまう可能性があります。

> **注記:**
> 4000 より大きな値は、SMTP サーバーのパフォーマンスに影響を与え、予測できない結果につながる可能性があるためサポートされません。

メールサーバーに SSL で接続する

このチェックボックスをオンにすると、SSL で保護されたトラフィックをメールサーバーに送信できます。

> **注記:**
>
> 受信メールサーバーが SSL で保護された E メール送信をサポートしている場合にのみ機能します。
>
> この機能を利用する場合は、465 番ポートを使用してください。
>
> このチェックボックスをオンにした状態で、SSL 非対応の SMTP サーバーへメール送信を行うと、アクションは失敗します(メールは届きません)。

STARTTLS SMTP Extension を使用

このチェックボックスをオンにすると、STARTTLS SMTP 拡張機能(暗号化)が有効になります。

日付ヘッダに UTC を使用

このチェックボックスをオンにすると、WinSyslog が送信するメールの日付ヘッダに UTC 時刻を使用します。

> **注記:**
> UTC 時刻に対応していないメールソフトをご利用の場合は無効にしてください。

メールフォーマット オプション

ここでは「メールフォーマット オプション」タブについて説明します。

メール送信元

送信者のメールアドレスを指定します。SMTP サーバーが受信できる、有効なアドレスを指定して下さい。

メール送信先

受信者のメールアドレスを指定します。複数の受信者へメッセージを送信したい場合は、それぞれの E メールアドレスをスペース、セミコロン、コンマのいずれかで区切ってすべての E メールアドレスを入力します（例： "receiver1@example.com, receiver2@example.com"）。または、メールソフトウェアで配信リストを定義しこのフィールドには単一の E メールアドレスを指定することもできます。受信者が頻繁に変更されたり、受信者の数が多かったりする場合は配信リストの方が便利です。

メールタイトル（subject）にレガシーの変数を使用

このチェックボックスをオンにすると、1 文字の置換シーケンスを使用する旧式の処理が適用されます。オフの場合は、より強力なイベントプロパティベースの方式が使用されます。

レガシーモード（このチェックボックスがオンの場合）は、件名の中で次の置換文字が認識されます：

置換文字	説明
%s	メッセージを送信したソースシステムの IP アドレスまたはホスト名（「ホスト名の解決」の設定に左右されます）
%f	受信したメッセージのファシリティコード（数値）
%p	受信したメッセージのプライオリティコード（数値）
%m	メッセージそのもの **注記**：これは完全なメッセージテキストであり、かなり長くなる場合があります。こ

	のため、255 文字を超えた場合は以降が切り捨てられます。この場合、%m 置換文字の後にある他のすべての情報も切り捨てられます。このため、%m 置換文字は件名の最後で使用することを強くお勧めします。
%%	単一の %記号を表します。

例えば、このチェックボックスをオンにすると、「**メールタイトル**」フィールドに「Syslog from %s:%m」と指定している場合に“172.16.0.1”から“This is a test”というメッセージを受信すると、
「Syslog from 172.16.0.1: This is a test」という件名の E メールが送信されます。

非レガシーモード（このチェックボックスをオフにした場合）では、プロパティの置換を使用できます。これを使用すると、イベントメッセージの任意のプロパティを含めることができます。詳しくは、別紙「WinSyslog プロパティリスト」をご参照ください。

例えば、（デフォルトのまま）このチェックボックスをオフにしたまま、「メールタイトル」フィールドに「Mesg: '%msg:1:15%' From: %fromhost%」と指定している場合に“172.16.0.1”から“This is a lengthy test message”というメッセージを受信すると、「Mesg: 'This is a lengt' From: 172.16.0.1」という件名の E メールが送信されます。（%msg:1:15% と指定することで）メッセージテキストから最初の 15 文字（1 文字目から 15 文字目まで）のみが抽出されたため、16 文字目以降のメッセージ（「hy」の 2 文字）が切り捨てられます。

メールタイトル

送信メールの件名を指定します。この件名は送信されるメッセージごとに使用されます。イベントの詳細を表示するために、置換文字またはプロパティを含めることができます。これは、件名のみでメッセージの内容が判断できるので、携帯電話などのモバイル機で E メールを受信する際に特に役立ちます。件名の最大文字数は、（置換シーケンスの拡張後）255 文字です。255 文字を超える場合は、切り捨てられます。

> **注記：**
> 多くの E メールシステムでは、より厳密な制限が設定され、255 文字よりも少ない文字数で切り捨てられる可能性があります。件名の長さは、80 文字以下に設定することをお奨めします。「**メールの本文**」には、文字数の制限はありません。

「**挿入**」ボタンからプロパティを挿入することができます。挿入可能なプロパティについては、別紙「WinSyslog プロパティリスト」をご参照ください。

メールの優先度

送信するメールの優先度を設定します。「Low Priority」（低）、「Normal Priority」（中）、「High Priority」（高）のいずれかを選択できます。

メール本文

送信するメール本文の内容を指定します。ソースシステム、ファシリティ、プライオリティ、実際のメッセージテキスト、このイベントに付随するその他の情報を含めることができます。メッセージ本文にはサイズの制限がないため、受信した完全なメッセージを含めることができます。

「挿入」ボタンをクリックすることで、プロパティを含めることができます。挿入可能なプロパティについては、「WinSyslog プロパティリスト」をご参照ください。出力エンコード

メール送信を行う際に使用する文字コードを設定します。「システムデフォルト」、「Unicode(UTF-8)」、「SHIFT-JIS」、「JIS (ISO-2022JP)」、「EUC-JP」のいずれかから選択できます。

メッセージに XML を出力

このチェックボックスをオンにすると、受信したイベントは XML フォーマットでメールに含まれます。その場合、オリジナルのタイムスタンプ、ファシリティ、プライオリティなどの全ての情報が含まれます。メールがメッセージを解析する自動システムに送信される場合に特に便利です。チェックされていない場合は、プレーンテキストメッセージがメールに含まれます。

5.6.3.3 Net Send

このアクションは、Windows の「net send」機能を使用して短い警告メッセージを送信します。

これらのメッセージはベストエフォート方式で配信されます。受信者に届くと、受信者のマシンのメッセージボックスにポップアップ表示されます。受信者に届かない場合は、単に破棄されます。バッファリングは行われません。従って、ルールエンジンはメッセージが配信されたかどうかをチェックしません。「net send」でのレポート配信の問題によってアクションがエラーになることはありません。

ターゲット

受信者の Windows ユーザー名、NETBIOS マシン名、IPv4 アドレス、IPv6 アドレス、IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを指定します。

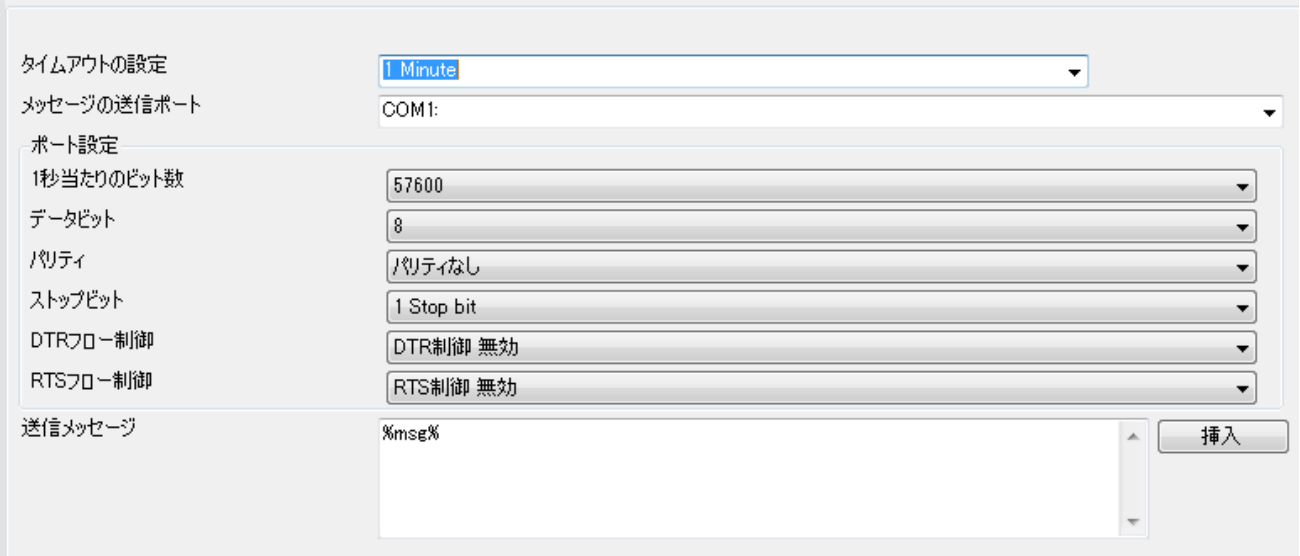
送信メッセージ

設定した「**ターゲット**」に対して送信するメッセージを指定します。「**挿入**」ボタンをクリックすることでプロパ

ティを使用することができます。

5.6.3.4 コミュニケーションポートに送信

このアクションは、接続された通信デバイスに文字列を送信します。つまり、シリアルポート（COM（通信）ポート）経由でメッセージを送信します。



タイムアウトの設定

デバイスがメッセージを受け入れるために許容される最大待ち時間を指定します。ここで設定した時間内にメッセージを送信できなかった場合、アクションは中止されます。デバイスによっては、不安定な状態になることがあります。

メッセージの送信ポート

デバイスが接続されているポートを指定します。通常、COMx: ポートの 1 つです。リストボックスには、ローカルマシンで検出されたすべてのポートが表示されます。リモートマシンを構成している場合は、この値を別の値に調整する必要があります。

ポート設定

ここでは「ポート設定」セクションについて説明します。

デバイスのポート設定に合わせて設定してください。不明な場合は、デバイスのマニュアルを参照してください。

1 秒当たりのビット数

110 から 256000 までの値を設定できます。

データビット

COM（通信）ポートに送受信するビット数を指定します。

パリティ

使用するパリティスキームを指定します。「パリティなし」、「奇数パリティ」、「偶数パリティ」、「マークパリティ」、「スペースパリティ」のいずれかから選択できます。

ストップビット

使用するストップビット（終了ビット）を指定します。「1 Stop bit」、「1.5 Stop bit」、「2 Stop bits」のいずれかから選択できます。

DTR フロー制御

DTR（Data Terminal Ready： データ端末レディー）フロー制御を指定します。以下のいずれかを選択します。

DTR フロー制御	説明
DTR 制御 無効	デバイスが開いていて使用不能である場合、DTR ラインを無効にします。
DTR 制御 有効	デバイスが開いていて使用可能である場合、DTR ラインを有効にします。
DTR 制御 ハンドシェイク	DTR ハンドシェイクを有効にします。

RTS フロー制御

RTS（Request to Send： 送信要求）フロー制御を指定します。以下のいずれかを選択します。

RTS フロー制御	説明
RTS 制御 無効	デバイスが開いていて使用不能である場合、RTS ラインを無効にします。
RTS 制御 有効	デバイスが開いていて使用可能である場合、RTS ラインを有効にします。
RTS 制御 ハンドシェイク	RTS ハンドシェイクを有効にします。ドライバーは、「タイプアヘッド（type ahead）」バッファが 2 分の 1 未満の場合は RTS ラインを上げ、バッファが 4 分の 3 を超えた場合は RTS ラインを下げます。
RTS 制御 トグル	バイトが送信可能な場合に RTS ラインが高くなります。バッファされたすべてのバイトが送信されると、RTS ラインが低くなります。

送信メッセージ

デバイスに送信するメッセージを指定します。テキストを簡潔に入力することも現在のイベントのすべての

プロパティを含めることもできます。たとえば、シリアル監査プリンターを使用していて、受信したメッセージをそのプリンターに記録したい場合は、実際の受信メッセージと改行（CRLF）を示す "%msg%%$CRLF%"を入力します。

「**挿入**」ボタンをクリックすることで、プロパティを挿入することができます。挿入可能なプロパティについては、別紙「WinSyslog プロパティリスト」をご参照ください。

5.6.3.5 MS キューの送信

このアクションは、Microsoft メッセージキュー（MSMQ）にメッセージを送信します。

> **注記：**
> このアクションを使用するには、「Microsoft Server メッセージ キュー (MSMQ) サーバー」をインストールする必要があります。

コンピュータ名

問い合わせを行うメッセージキュー（MSMQ）を含むマシンの IP アドレスまたはコンピューター名を指定します。IPv4 アドレス、IPv6 アドレス、IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを使用できます。

キュー名

書き込みたいキュー名を指定します。

キューのプライオリティ

キューの優先度を指定します。0 から 7 までの数値から選択できます。

キューのメッセージラベル

キューアイテムのラベルを指定します。

出力メッセージ

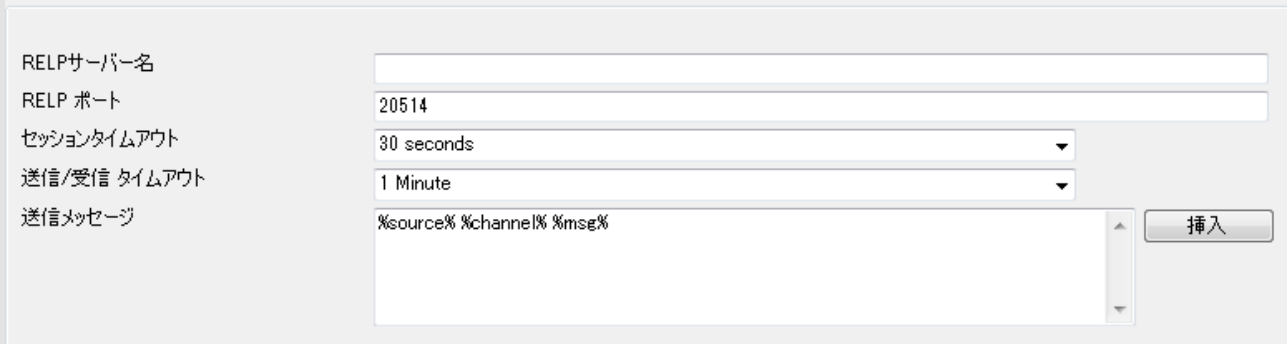
キューアイテムのボディ(メッセージ本文)を指定します。

5.6.3.6 RELP 送信

このアクションは、RELP (Reliable Event Logging Protocol) を使用して受信したメッセージを RELP 対応レシーバーに送信します。

> **メモ:**
> メッセージ送信に新しいプロトコル(RELP: Reliable Event Logging Protocol)を使用する点を除けば「Syslog 転送」アクションとほぼ同じです。RELP を使用することで通信プロセスの信頼性が向上します。

> **注記:**
>
> 受信側も RELP に対応していなければなりません。
>
> RELP はネットワーク経路の信頼性を高めたプロトコルであり、サービスダウンなどローカルで発生した問題からメッセージを守ることはできません。サービスシャットダウン時のメッセージ保護のためには「ディスクキャッシュのキュー管理を有効にする」オプションを有効にする必要があります。
>
> このアクションは、フリー版、Basic 版、Professional 版では使用できません。



RELP サーバー名

RELP メッセージの送信先システムの名前、または IP アドレスを入力します。IPv4 アドレス、IPv6 アドレス、IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを使用できます。

RELP ポート

RELP サーバーと通信する際に使用するポート番号を指定します。不明な場合は、デフォルト値 20514 のまま使用してください。一般的には 20514 番ポートが使用されます。別のポート番号は、例えばセキュ

リティへの配慮が必要な場合などに使用されます。

ポート番号の代わりにサービス名を指定することもできます。その場合、このサービス名はソケットサービス データベース関数を介して検索されます。

セッションタイムアウト

RELP サーバーへのセッションを開いたままにする最大時間を指定します。

送信/受信 タイムアウト

サーバーがリモートサーバーの応答を待つ最大待ち時間を指定します。応答がないまま設定した時間が経過すると、接続は切断され、(ルールの設定に基づいて)再試行されます。このオプションは、リモートシステムがなんらかの原因により接続を切断し、送信側システムがそのことを通知されない場合(例えば、ファイアーウォール構成のために発生する可能性がある場合)などに役立ちます。

送信メッセージ

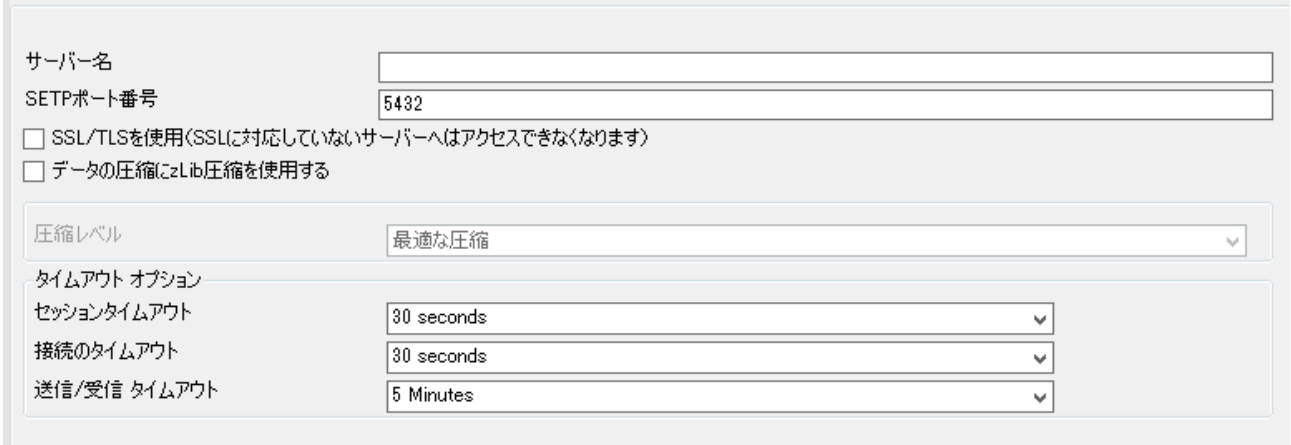
送信したいメッセージを入力します。

「**挿入**」ボタンからプロパティを挿入することができます。挿入可能なプロパティについては、別紙「WinSyslog プロパティリスト」をご参照ください。

5.6.3.7 SETP 送信

このアクションは、受信したメッセージを SETP サーバー(「SETP サーバー」サービスを使用している WinSyslog Enterprise 版サーバー)に送信します。

> **注記:** このアクションは、Basic 版では使用できません。



サーバー名

SETP の送信先サーバーを指定します。IPv4 アドレス、IPv6 アドレス、IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを指定できます。

SETP ポート番号

SETP 送信に使用するポート番号を指定します。デフォルトは 5432 です。0 を指定すると、システムが提供するデフォルト値（システム管理者が変更しない場合、デフォルト値は 5432）が使用されます。

ポート番号の代わりに、サービス名を使用することができます。その場合、名前はソケットサービスデータベースを介して検索されます。TCP プロトコルが検索されます。

> **注記：**
> ここで設定した SETP ポート番号は、受信側のサーバーで設定されたポート番号（WinSyslog Enterprise 版）と同じでなければなりません。同じでない場合は、SETP 送信セッションを開始できません。ルールエンジンはこれを Windows イベントログに記録します。

SSL/TLS を使用（SSL に対応していないサーバーへはアクセスできなくなります）

このチェックボックスをオンにすると、SSL/TLS SETP サーバーに接続できるようになります。

> **注記：**
> オンの場合、受信側の SETP サーバーで SSL/TLS の使用が有効になっていることを確認してください。SSL に対応していない SETP サーバーへは接続できなくなります。

データの圧縮に zLib 圧縮を使用する

このチェックボックスをオンにすると、zLib 圧縮を使用できます。

> **注記：**
> オンにした場合、受信側の SETP サーバーで zLib 圧縮の使用がオンになっていることを確認してください。zLib 圧縮に対応していない場合は機能しません。

- **圧縮レベル**

  「**データの圧縮に zLib 圧縮を使用する**」オプションを有効にした場合に、圧縮レベルを指定します。「最適なスピード」、「低い圧縮」、「通常の圧縮」、「最適な圧縮」のいずれかから選択できます。圧縮率が高いほどパフォーマンスは低下します。

タイムアウト オプション

ここでは「タイムアウト オプション」セクションについて説明します。

セッションタイムアウト

SETP サーバーへのセッションをオープン状態のままにする最大待ち時間を指定します。

接続のタイムアウト

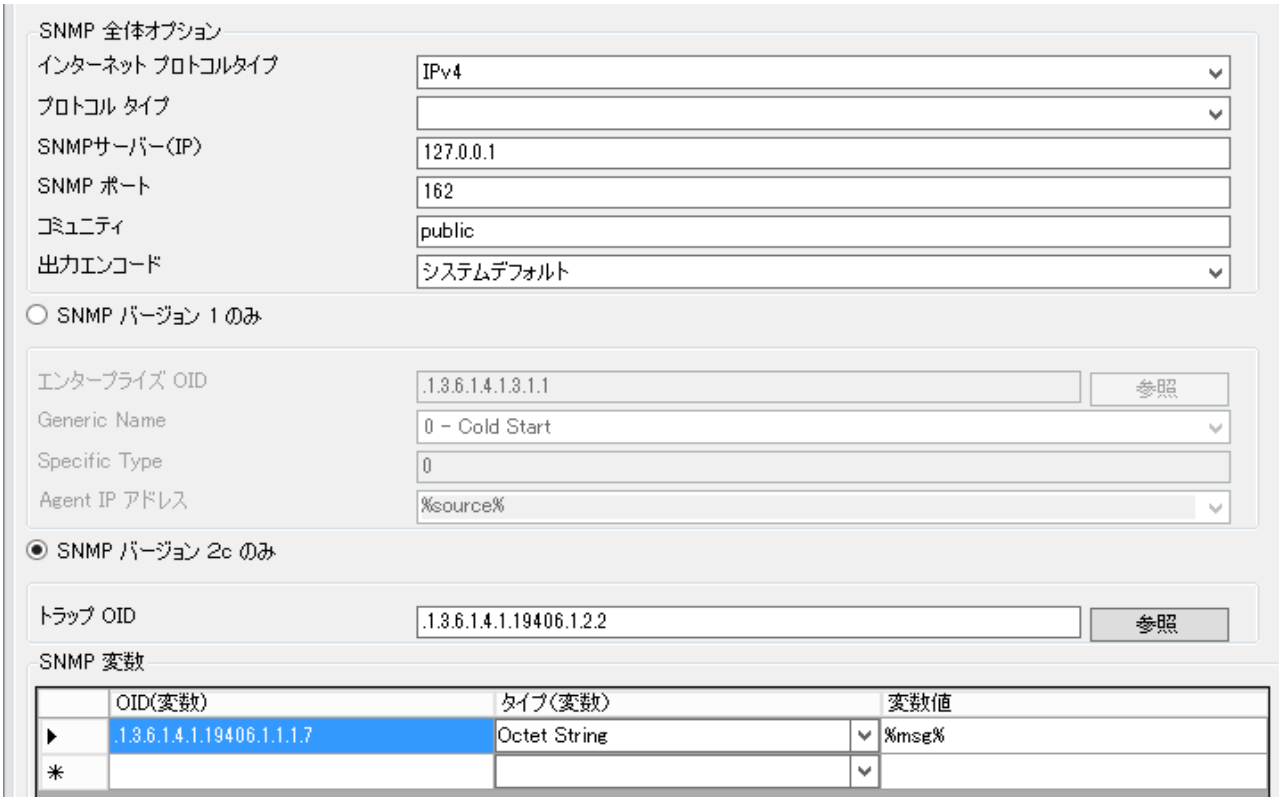
接続されるまで、または接続が切断されるまでにかかる最大待ち時間を指定します。

送信/受信 タイムアウト

データの送受信時にここで設定したタイムアウトが適用されます。

5.6.3.8 SNMP トラップの送信

このアクションは、受信したメッセージを SNMP トラップ送信します。



SNMP 全体のオプション

ここでは「SNMP 全体のオプション」セクションについて説明します。

インターネットプロトコルタイプ

使用するプロトコルタイプを指定します。IPv4、IPv6 のどちらかを選択します。IPv6 プロトコルは使用するためには適切にインストールする必要があります。どちらか 1 つしか設定できないため、両方のプロトコルを使用する場合は、別のサービスを作成する必要があります。

プロトコル タイプ

プロトコルタイプを指定します。UDP または TCP のいずれかを選択します。

SNMP サーバー（IP）

SNMP トラップを受信するサーバーの IP アドレスを指定します。ホスト名を指定すると、DNS 名前解決に失敗した場合（例えば DNS サーバーの障害時など）に送信に失敗する可能性があります。これを避けるために、IP アドレスを指定してください。IPv4 アドレス、IPv6 アドレス、IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを使用できます。

SNMP ポート

SNMP トラップ送信に使用するポート番号を指定します。

コミュニティ

SNMP コミュニティを指定します。

出力エンコード

出力エンコードを指定します。「システムデフォルト」、「Unicode(UTF-8)」、「SHIFT-JIS」、「JIS (ISO-2022JP)」、「EUC-JP」のいずれかを選択します。

「SNMP バージョン 1」を使用する場合は、以下を設定します。

SNMP バージョン 1 のみ

SNMP バージョン 1 を使用する場合に選択します。

- **エンタープライズ OID**

  Enterprise OID を指定します。OID の選択には、「**参照**」ボタンを使用できます。「**参照**」ボタンをクリックすると、「**MIB ブラウザ(OID)**」が表示されます。

- **Generic Name**

  Generic Trap Type を指定します。「0-Cold Start」、「1-Warm Start」、「2-Link Down」、「3-Link Up」、「4-Authentication Failure」、「5-EGP Neighbor Loss」、「6-Enterprise Specific」のいずれかから選択します。

- **Specific Type**

  Specific Trap Type を数字で指定します。

- **Agent IP アドレス**

  SNMP v1 の Agent Address フィールドを他の IP アドレスに設定できます。可能であれば、ホスト名は自動的に解決されます。デフォルトは、%source%プロパティです。トラップデータに含まれる agent IP のプロパティを設定する場合は、%snmp_agentip% とします。プルダウンから選択することもできます。

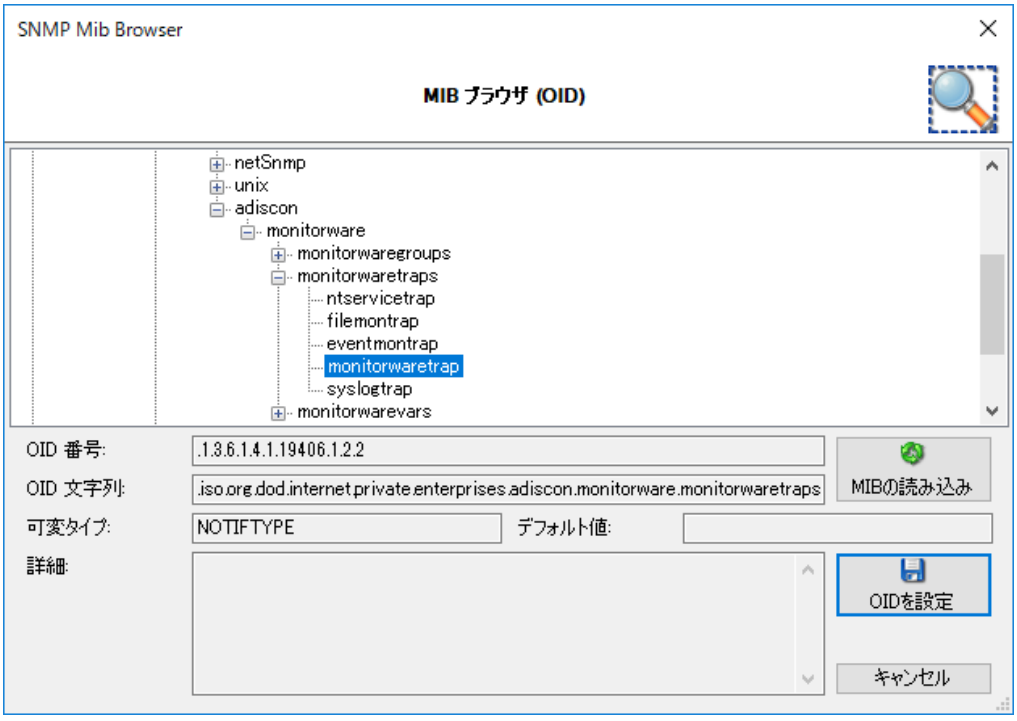
「SNMP バージョン 2c のみ」を使用する場合は、以下を設定します。

SNMP バージョン 2cのみ

SNMP バージョン 2c を使用する場合に選択します。

- **トラップ OID**

  SNMP トラップの OID を指定します。OID の選択には、「**参照**」ボタンを使用できます。「**参照**」ボタンをクリックすると、「MIB ブラウザ（OID）」画面が表示されます。



SNMP 変数

SNMP トラップで送信する変数を指定します。トラップコードがわかっている場合は、手動で入力できます。そうでない場合は、「**MIB ブラウザ（OID）**」をご利用下さい。次のフィールドがあります。

OID（変数）

SNMP トラップの OID です。利用可能な OID については、「**MIB ブラウザ（OID）**」をご利用下さい。

タイプ（変数）

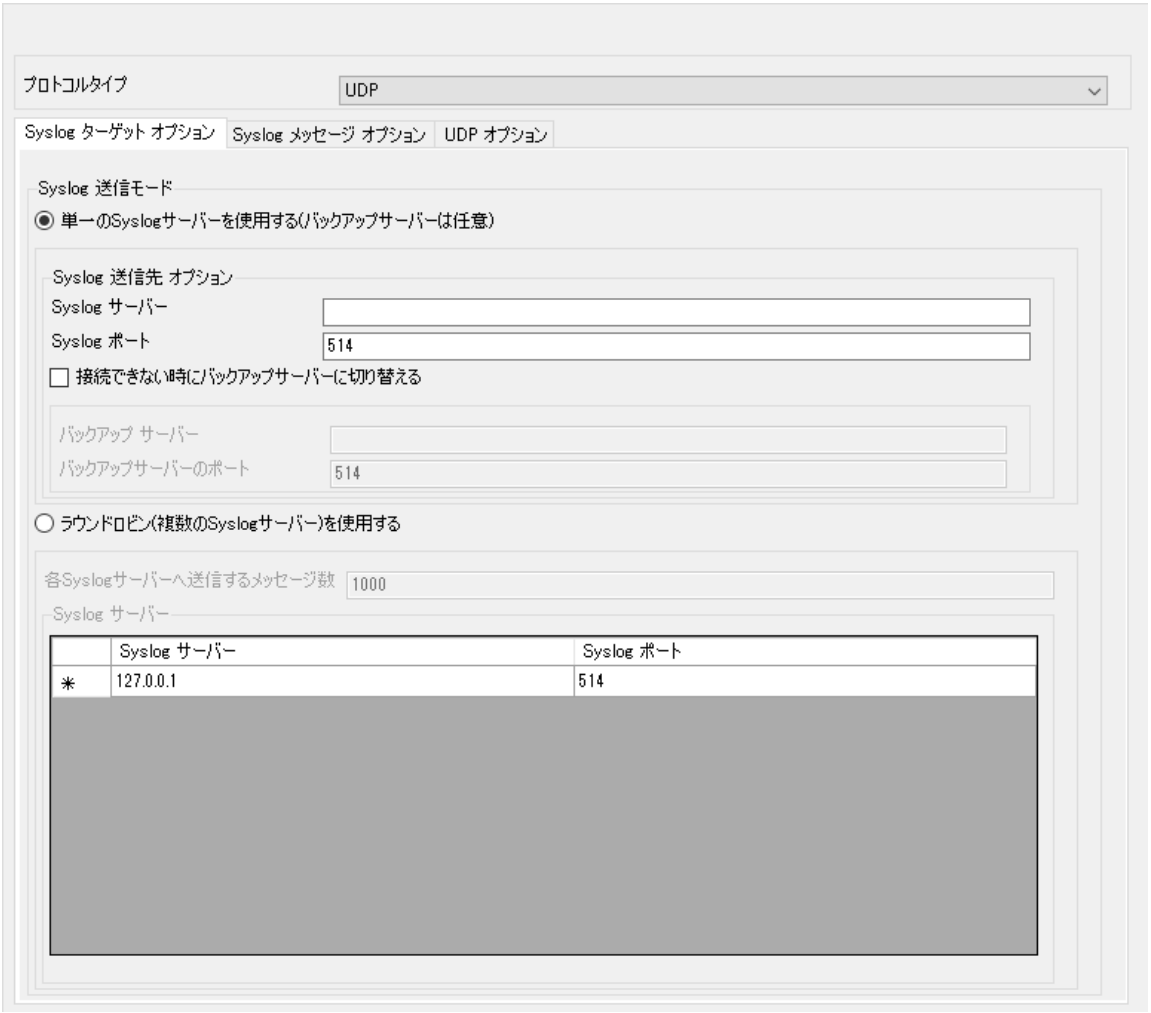
変数の型を指定します。このタイプに合わせて、変数値を正確にフォーマットする必要があります（例： IP Address など）。

変数値

変数値を指定します。「タイプ（変数）」に合わせてフォーマットを設定する必要があります。

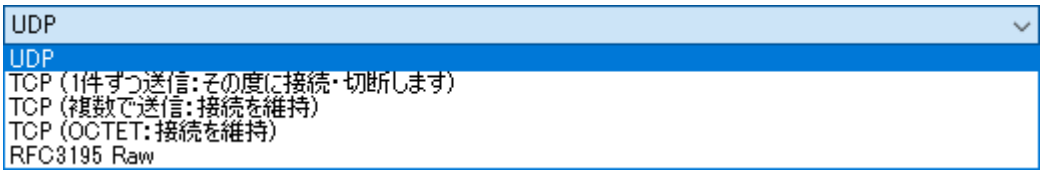
5.6.3.9 Syslog 転送

このアクションは、受信したメッセージを別の Syslog サーバーへ転送します。



プロトコルタイプ

Syslog メッセージの転送に使用するプロトコルを指定します。



Syslog メッセージは、一般的に UDP、TCP、RFC 3195 Raw で送信できます。通常、Syslog メッセージはデフォルトである UDP プロトコルを介して受信されます。UDP はほとんどすべてのサーバーで使用できますが、確実な通信ではありません。つまり、ネットワークエラーが発生したり、ネットワークが輻輳したり、(ルーターやスイッチなどの)デバイスのバッファ容量が不足したりすると、UDP 経由で送信された Syslog メッセージが失われる可能性があります。通常 UDP で問題なく動作します。ただし少ない数であってもメッセージの損失が許容できない場合は使用するべきではありません。

TCP と RFC 3195 ベースの Syslog メッセージは、UDP よりも信頼性に優れています。RFC 3195 は特別な標準化された転送モードです。Adiscon 製品は RFC 3195 を実装していますが、実際のところ RFC 3195 はあまり使用されていません。このため本当に必要でない限りは RFC 3195 モードを使用しないことをお勧めします。

TCP については、既存のすべての実装に最適な互換性を提供するために、次の 3 つのモードをサポートしています。

- **TCP(1 件ずつ送信:その度に接続・切断します)**
  2006 年以前の Adiscon サーバーのための互換モードです。他のベンダーでも要求される場合があります。必要な場合を除いては、このモードを使用しないことをお勧めします。

- **TCP(複数で送信:接続を維持)**
  1 度の接続で複数のメッセージを送信します。この接続は長時間維持されたままになります。このモードはほとんどすべての実装と互換性があり、優れたパフォーマンスが期待できます。ただし制御文字が Syslog メッセージに存在する場合、問題が発生する可能性があります。

- **TCP(OCTET:接続を維持)**
  IETF 標準のアルゴリズムを実装しています。このモードも接続が維持されます。このモードは信頼性が高く、埋め込みの制御文字も問題なく処理します。しかし、このモードに対応したレシーバーは非常に限られています。そのため、このモードは、Adiscon 製品間の通信でご利用になることをお勧めします。

  経験則では、Adiscon 製品のみを使用する場合は、「**TCP(OCTET:接続を維持)**」を使用することをお勧めします。そうでない場合は、おそらく「**TCP(複数で送信:接続を維持)**」が最適です。この 2 つのオプションのいずれかを選択した場合は、TCP オプションタブから、「**セッションタイムアウト**」を選択することができます。メッセージが送信されずタイムアウトした場合は接続が切断されます。「**セッションタイムアウト**」にはデフォルトの 30 分(30 minutes)を使用することをお勧めします。たまにしかメッセージが送信されない場

合は、より短いタイムアウト値を使用する方が適切かもしれません。

Syslog ターゲットオプション

ここでは「Syslog ターゲットオプション」タブについて説明します。
Syslog 送信モードを次の 2 つのオプションから選択できます:

- **単一の Syslog サーバーを使用する（バックアップサーバーは任意）**

  これは、設定されている場合、プライマリ syslog サーバとセカンダリバックアップ syslog サーバを使用する、古典的な syslog 送信モードです。

- **ラウンドロビン（複数の Syslog サーバー）を使用する**

  この新しい方法では複数の Syslog サーバーを設定できます。設定した数のメッセージを転送すると、リストの次の sysylog サーバーに転送先を切り替えます。

単一の Syslog サーバーを使用する

Syslog サーバー

Syslog メッセージの送信先システムの名前または IP アドレスを指定します。IPv4 アドレス、IPv6 アドレス、IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを指定できます。

Syslog ポート

Syslog 送信に使用するポート番号を指定します。よくわからない場合は、デフォルト値の 514 のままにし

ておいてください。異なるポートは、例えばセキュリティへの配慮が必要な場合などに使用されます。
0 を指定すると、システム提供のデフォルト値が使用されます（デフォルトではほとんどすべてのシステムで 514 が設定されています）。

接続できない時にバックアップサーバーに切り替える

このチェックボックスをオンにすると、（「Syslog サーバー」フィールドで指定した）プライマリの Syslog サーバーへの接続が失敗した場合に、バックアップサーバーが動的に使用されます。プライマリサーバーは次の Syslog セッションがオープンされると自動的に再試行されます。

> **注記：** このオプションは「TCP」を使用している場合にのみ使用できます。

- **バックアップサーバー**

  「**接続できない時にバックアップサーバーに切り替える**」がオンの場合に、バックアップサーバーとして使用する Syslog メッセージの送信先システムの名前または IP アドレスを指定します。

- **バックアップサーバーのポート**

  「**接続できない時にバックアップサーバーに切り替える**」がオンの場合に、Syslog 送信に使用するポート番号を指定します。

ラウンドロビン（複数の Syslog サーバー）を使用する

各 Syslog サーバーへ送信するメッセージ数

ひとつの syslog サーバーに連続して送信するメッセージ数を入力します。送信したメッセージ数がここで指定した値に達すると、送信先がテーブルのリストの次の sysylog サーバーに切り替わります。

Syslog サーバー （テーブル）

- **Syslog サーバー**

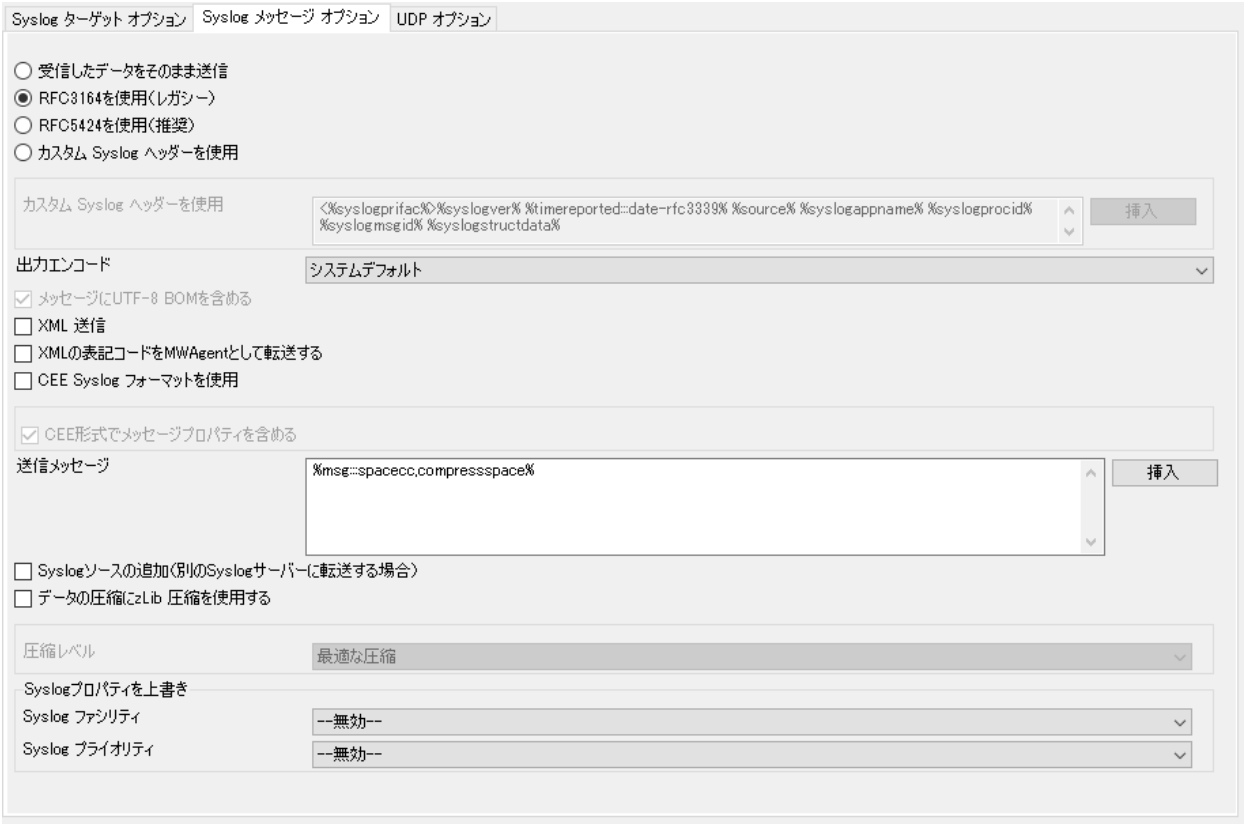
  Syslog メッセージの送信先システムの名前または IP アドレスを指定します。IPv4 アドレス、IPv6 アドレス、IPv4 または IPv6 アドレスに解決されるホスト名のいずれかを指定できます。

- **Syslog ポート**

  Syslog 送信に使用するポート番号を指定します。

Syslog メッセージ オプション

ここでは「Syslog メッセージオプション」タブについて説明します。



Syslog メッセージの処理方法を次の 4 つのオプションから選択できます:

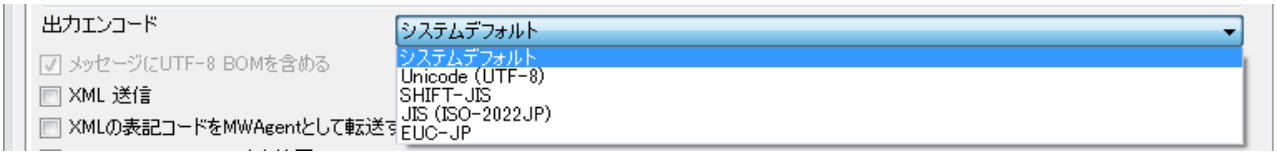
- **受信したデータをそのまま送信**
  受信した Syslog を処理せずそのまま転送したい場合にオンにします。
- **RFC3164 を使用(レガシー)**
  受信した Syslog を RFC3164 形式で転送したい場合にオンにします。
- **RFC5424 を使用(推奨)**
  受信した Syslog を RFC5424 形式で転送したい場合にオンにします。
- **カスタム Syslog ヘッダーを使用**
  受信した Syslog の Syslog ヘッダーをカスタマイズして転送したい場合にオンにします。

  カスタム Syslog ヘッダーを使用 (テキストボックス)

  Syslog メッセージの処理方法として「**カスタム Syslog ヘッダーを使用**」ラジオボタンがオンの場合に、使用するカスタム Syslog ヘッダーの内容を指定できます。(直接テキストを書き込む)固定メッセージと(プロパティを挿入する)動的コンテンツの両方を使用できます。プロパティは「**挿入**」ボタンから指定することができます。挿入可能なプロパティについては、別紙「WinSyslog プロパティリスト」をご参照ください。

出力エンコード

Syslog メッセージ転送の際に使用する文字コードを設定します。「システムデフォルト」、「Unicode (UTF-8)」、「SHIFT-JIS」、「JIS (ISO-2022JP)」、「EUC-JP」から選択します。



この設定はアジア言語で最も重要です。別のエンコードが必要であることがわかっている場合以外は、「システムデフォルト」のままにすることをお勧めします。「システムデフォルト」はアジア言語（例えば日本語）の Windows であってもほとんどの場合、問題なく機能します。

- **メッセージに UTF-8 BOM を含める**

  「**出力エンコード**」で「Unicode (UTF-8)」を選択している場合にのみ使用できます。
  このチェックボックスをオンにすると、UTF-8 BOM コードが出力メッセージの先頭に追加されます。
  Syslog 受信側が UTF-8 BOM を処理して削除できない場合は、オフにすることができます。

XML 送信

このチェックボックスをオンにすると、転送された Syslog メッセージは完全な XML 形式の情報レコードになります。これには、タイムスタンプや送信元（オリジナル）システムなどの追加情報が、簡単に解析できる形式で含まれています。

XML フォーマットのメッセージは、受信側のシステムが XML データを解析できる場合に特に便利です。しかし、他の方法では転送できない追加の情報が含まれているため、閲覧するユーザーにとっても有用かもしれません。

XML の表記コードを MWAgent として転送する

MWAgent（MonitorWare エージェント）は、イベントの特定の XML 表記をサポートしています。このチェックボックスをオンにすると、転送された Syslog メッセージに XML 表記が使用されます。その場合、インフォメーションユニットタイプ、オリジナルソースシステム、受信時刻などの追加情報が提供されますが、人間にとっては読みづらくなります。ですが、この形式は、解析を容易に行うことができるようになります。

> **注記：** このオプションは、実験的なものであり、公式な標準ではありません。

CEE Syslog フォーマットを使用

このチェックボックスをオンにすると、新しい CEE 拡張 Syslog 形式が（作業中に）使用されます。有用なプロパティはすべて JSON ストリームに含まれます。メッセージ自体も含めることができます。
例：セキュリティイベントログメッセージ形式

@cee: {"source": "machine.local", "nteventlogtype": "Security", "sourceproc": "Microsoft-Windows-Security-Auditing", "id": "4648", "categoryid": "12544", "category": "12544", "keywordid": "0x8020000000000000", "user": "N¥¥A", "SubjectUserSid": "S-1-5-11-222222222-333333333-4444444444-5555", "SubjectUserName": "User", "SubjectDomainName": "DOMAIN", "SubjectLogonId": "0x5efdd", "LogonGuid": "{00000000-0000-0000-0000-000000000000}", "TargetUserName": "Administrator", "TargetDomainName": " DOMAIN ", "TargetLogonGuid": "{00000000-0000-0000-0000-000000000000}", "TargetServerName": "servername", "TargetInfo": " servername ", "ProcessId": "0x76c", "ProcessName": "C:¥¥Windows¥¥System32¥¥spoolsv.exe", "IpAddress": "-", "IpPort": "-", "catname": "Logon", "keyword": "Audit Success", "level": "Information", }

- **CEE 形式のメッセージプロパティを含める**

  「**CEE Syslog フォーマットを使用**」がオンの場合にのみ使用できます。

  このチェックボックスがオンの場合、メッセージそのものが JSON ストリームにプロパティとして含まれます。メッセージ自体を CEE 形式にしたくない場合は、このチェックボックスをオフにします。

  > **注記:**
  > Syslog サーバーへの転送中に実際の Syslog メッセージの一部を Event ID にすることもできます。その場合「Syslog 転送」アクションをいくつか変更する必要があります。設定については、こちら（英語）をご参照ください。

送信メッセージ

メッセージフォーマットを指定することができます。

「**挿入**」ボタンからメッセージに加えたいプロパティを追加することができます。挿入可能なプロパティについては、別紙「WinSyslog プロパティリスト」をご参照ください。

Syslog ソースの追加（別の Syslog サーバーに転送する場合）

このチェックボックスをオンにすると、発信元システムの情報が実際のメッセージテキストの前に追加されます。これにより、受信者はメッセージのオリジナルの発信元を追跡できます。

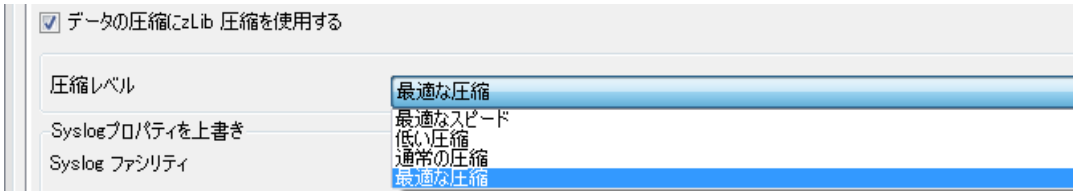
> **注記:**
> このオプションは、RFC 3164 と互換性がありません。WinSyslog のインタラクティブ Syslog ビューアへのメッセージ転送を目的とする場合は、このチェックボックスをオンにすることをお勧めします。

データの圧縮に zLib 圧縮を使用する

このチェックボックスをオンにすると、Syslog メッセージを圧縮することができます。

- **圧縮レベル**

  「**データの圧縮に zLib 圧縮を使用する**」チェックボックスがオンの場合にのみ使用できます。
  Syslog メッセージの圧縮レベルを設定できます。「最適なスピード」、「低い圧縮」、「通常の圧縮」、「最適な圧縮」から選択できます。



Syslog プロパティを上書き

ここでは「Syslog プロパティを上書き」セクションについて説明します。

- **Syslog ファシリティ**

  Syslog ファシリティを設定された値で上書きします。

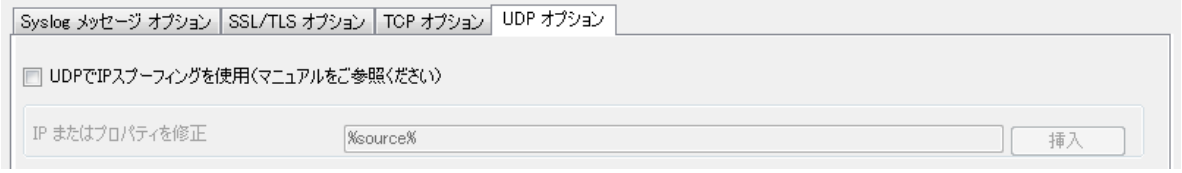
- **Syslog プライオリティ**

  Syslog プライオリティを設定された値で上書きします。

UDP オプション

ここでは「UDP オプション」タブについて説明します。

「UDP オプション」タブは「**プロトコルタイプ**」に「**UDP**」が選択されている場合にのみ使用できます（「TCP」または「RFC3195 Raw」が選択されている場合は使用できません）。



UDP で IP スプーフィングを使用（マニュアルをご参照ください）

このチェックボックスをオンにすると、UDP 経由で Syslog メッセージを送信するときに IP スプーフィング（IP 偽装）を行うことができます。

IP スプーフィングに関する注意事項:

UDP プロトコルかつ IPv4 のみがサポートされます。IPv6 はサポートされません。

Microsoft によって導入されたシステムの制限により、Windows Server 2003, 2008 またはそれ以降でのみ使用できます(Windows XP, Vista, 7 またはそれ以降では使用できません)。詳細については Microsoft の説明をご参照ください。

多くのルーターおよびゲートウェイはスプーフィングされた IP アドレスを持つネットワークパッケージを破棄する可能性があることにご注意ください。この場合、この機能はローカルネットワークでのみ動作します。

- **IP またはプロパティを修正**

  「**UDP で IP スプーフィングを使用**」がオンの場合にのみ使用できます。

  静的 IP アドレス、またはプロパティを指定できます。プロパティを使用した場合は、プロパティの内容から IP アドレスへの名前解決が実行されます。デフォルトでは %source% が設定されています。この場合は、ソース名から IP アドレスへの名前解決が行われます。指定したプロパティを IP アドレスへ名前解決できない場合は、デフォルトのローカル IP アドレスが使用されます。

SSL/TLS オプション

ここでは「SSL/TLS オプション」タブについて説明します。
プロトコルタイプで「TCP」を選択時に使用します

SSL/TLS を使用（SSL に対応していないサーバーへはアクセスできなくなります）

このチェックボックスをオンにすると、SSL に対応していないサーバーと通信できなくなります。暗号化に使用される方法は、RFC 5424 (Transport Layer Security (TLS) Transport Mapping for Syslog) と互換性があります。

- **TLS モード**

  次のモードから選択できます：

  - **匿名認証**
    デフォルトの証明書が使用されます。デフォルトで選択されています。
  - **証明書を使用**
    独自の証明書を指定できます。OpenSSL などにより作成した証明書が必要となります。

- **共通の CA PEM の選択**

  認証局（CA： Certificate Authority）の証明書を選択します。Syslog の受信側も同じ認証局証明書を使用する必要があります。

- **PEM 証明書を選択**

  クライアント証明書（PEM フォーマット）を選択します。

- **PEM 鍵を選択**

  クライアント証明書の鍵ファイル（PEM フォーマット）を選択します。

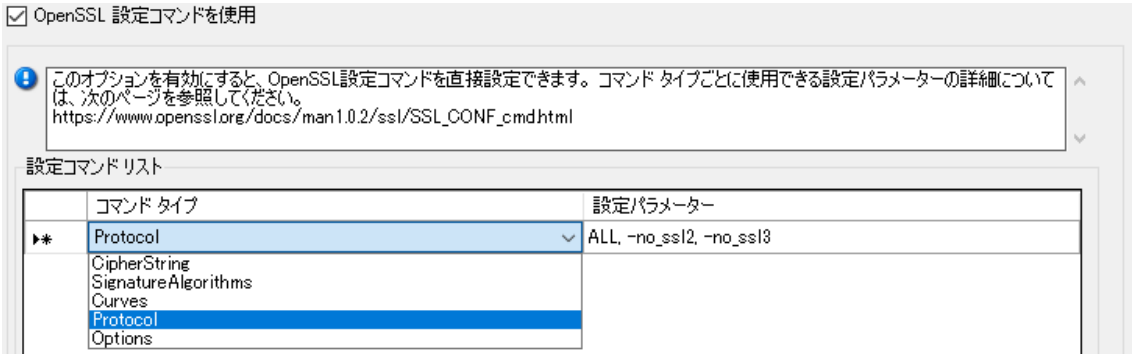
Advanced TLS Options

暗号化方式を選択します。以下の 4 つの項目をそれぞれチェックボックスで設定できます。

・SSL v3 を有効にする（脆弱）
・TLS v1.0 を有効にする（脆弱）
・TLS v1.1 を有効にする
・TLS v1.2 を有効にする

OpenSSL 設定コマンドを使用する

デフォルトはオフになっています。このオプションを有効にすると、OpenSSL 設定コマンドを直接設定できます。 コマンド・タイプごとに使用可能な構成パラメーターの詳細については、以下のリンクを参照してください。
https://www.openssl.org/docs/man1.0.2/ssl/SSL_CONF_cmd.html



TCP オプション

ここでは「TCP オプション」タブについて説明します。

「TCP オプション」タブは「**プロトコルタイプ**」に「**TCP**」が選択されていて、かつ送信モードが「単一の Syslog サーバーを使用する」が選択されている場合にのみ使用できます。「UDP」または「RFC3195 Raw」が選択されている場合は使用できません。

セッションタイムアウト

> **注記:**
> 「**プロトコルタイプ**」で「**TCP(複数で送信:接続を維持)**」または「**TCP(OCTET:接続を維持)**」を選択した場合にのみ使用されます。

セッションのタイムアウト時間を指定します。メッセージが送信されずタイムアウトした場合は接続が切断されます。「**セッションタイムアウト**」にはデフォルトの 30 分(30 minutes)を使用することをお勧めします。たまにしかメッセージが送信されない場合は、より短いタイムアウト値を使用する方が適切かもしれません。

サーバーに接続できない時にディスクキューを使用する

このチェックボックスをオンにすると、ディスクキューを使用できます。リモート Syslog サーバーへの接続に失敗すると、アクションが Syslog メッセージを一時ファイルにキャッシュします。

一時ファイル名はアクションごとに自動生成される一意の GUID を使用して生成されるため、複数アクションでこの機能を使用できます。

リモートの Syslog サーバーが再び利用可能になると、キャッシュされたメッセージが自動的に送信されます。Syslog キャッシュがアクティブである（キャッシュが存在する）間に WinSyslog サービスを再起動した場合、サービスの開始中にリモートの Syslog サーバーが利用可能かどうかチェックすることができません。アクションが再度呼び出されると、リモートの Syslog サーバーとの接続が確認され、Syslog サーバーが利用可能であればメッセージが送信されます。

キャッシュのサイズは、特に制限はありません（ディスクのサイズに依存します）。

- **設定値に達した場合にファイルを分割する**

  一時キャッシュファイルサイズの上限値をバイト単位で指定します。サポートされるファイルの最大サイズは 2GB です。

- **ディスクキュー ディレクトリ**

  一時ファイルの作成先ディレクトリを指定します。

- **接続の待ち時間**

  接続を試行する間の待ち時間を指定します。

- **オーバーラン防止の遅延（ミリ秒）**

  オーバーラン防止のための待ち時間をミリ秒で指定します。

- **リトライ後の待ち時間を二倍にする**

  このチェックボックスをオンにすると、リトライ後の待ち時間が指定した待ち時間の2倍になります。

  - **二倍の待ち時間の制限値**

    リトライ後の待ち時間を2倍にする上限（回数）を指定します。

- **待ち時間のランダムな遅延を有効にする**

このチェックボックスをオンにすると、ランダムな遅延時間を使用します。

- **ランダムな遅延の最大値**

  ランダムな最大待ち時間を指定します。

5.6.4. 内部アクション

ここでは、「内部アクション」グループに属するアクションについて説明します。

以下のアクションを含みます:

- ルールセットを呼び出し
- ステータス変数の算出
- 破棄
- イベントを標準化(イベントの正規化)
- 再構成(Post Processing)
- ホスト名の解決
- プロパティの設定
- ステータスの設定

5.6.4.1 ルールセットを呼び出し

このアクションは、別のルールセットを既存のルールセット内で呼び出すために使用します。

このアクションが実行されると、ルールエンジンは、通常のフローを止めて呼び出された(多くのルールが含まれている)ルールセットへ移動し、呼び出されたルールセットで定義されているすべてのルールを実行します。すべてを実行した後、元のフローが中断された場所に戻ります。

例:
「ルール 1」に「アクション 1」と「アクション 2」が存在し、「アクション 1」には「ルールセットを呼び出し」アクションが使用されているとします。

「ルール 1」の「フィルタの条件」の結果が「真（True）」であると評価されると、「アクション 1」が実行されます。「アクション 1」は「ルールセットを呼び出し」であるため、ここで指定されている「ルールセット」へ移動します（①）。呼び出されたルールセットの「フィルタの条件」を評価します。「フィルタ条件」が「真（True）」の場合は、すべてのアクションを実行した後、（通常のフローの）「ルール 1」の「アクション 2」に戻ります（②）。呼び出したルールセットの「フィルタの条件」が「偽（False）」の場合は、このルールセットに含まれるすべてのアクションをスキップし、（通常のフローの）「ルール 1」の「アクション 2」に戻ります（③）。

> **注記：**
> ルールの組み込み（呼び出し）に制限はありません。他のルールで呼び出されているルールが別のルールを呼び出している場合があります。

処理を実行するルールセット

呼び出すルールセットを選択します。

5.6.4.2 ステータス変数の算出

このアクションは、ステータス変数を計算するために使用します。

この機能は、カウンタベースで作用するルールセットに必要です。

ステータス変数

ステータス変数名を入力します。「**挿入**」ボタンからプロパティを指定できます。

オペレーションタイプ

「オペレーションタイプ」セクションでは、次のいずれかを選択します。

値を増加（＋）

「**オペレーション値**」に指定された値を加算します。

値を減少（－）

「**オペレーション値**」に指定された値を減算します。

オペレーション値

使用するオペレーション値を設定します。

5.6.4.3 破棄

このアクションは、現在のインフォメーションユニットと「破棄」アクション実行後に定義されたルールのアクションを直ちに破棄するために使用します。

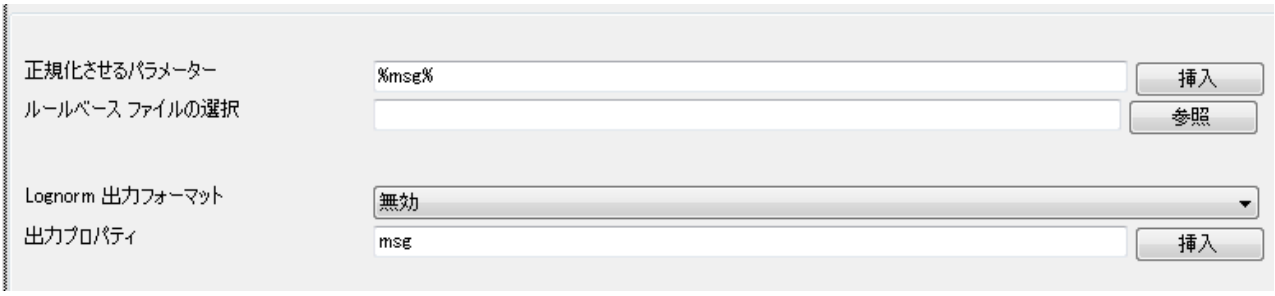
このアクションは何も設定する必要がないため、何も表示されません。

5.6.4.4 イベントを標準化（イベントの正規化）

このアクションは、パラメーターを正規化し、XML、CSV、JSON フォーマットに変換するために使用します。

正規化の結果は、フィルタ処理の決定および出力アクションに使用できる内部プロパティに保管されます。

このアクションでは、rsyslog でも使用されている liblognorm を使用します。
liblognorm 用に作成されたルールベースは、簡単に使用でき、適合させることができます。



正規化させるパラメーター

正規化するプロパティを指定します。

ルールベース ファイルの選択

ルールベース定義を含むテキストファイルを指定します。
詳しくは liblognorm ドキュメント（http://www.liblognorm.com/files/manual/index.html）をご参照ください。

Lognorm 出力フォーマット

出力フォーマットを指定します。以下のいずれかを選択できます。

- **無効**
  追加の出力フォーマットはありません。
- **JSON フォーマット**
  出力プロパティに格納されている文字列を JSON フォーマットで出力します。
- **XML フォーマット**
  出力プロパティに格納されている文字列を XML フォーマットで出力します。
- **CSV フォーマット**
  出力プロパティに格納されている文字列を CSV フォーマットで出力します。

出力プロパティ

正規化されたフォーマットを保存するプロパティを指定します。

5.6.4.5 再構成（Post Processing）

このアクションは、処理後のメッセージを再構成（例： タブ区切りのフォーマット）するために使用します。

非標準の Syslog フォーマットを使用している場合や、メッセージから特定のプロパティを取り出したい場合に便利です。

「再構成」アクションは、受信したメッセージを受け取り、解析マップに従って解析します。解析マップ（プロパティリスト）には、メッセージのどの位置に、どのタイプのどのプロパティが存在するかを指定します。メッセージが実際に解析マップと一致する場合は、すべてのプロパティが抽出され、イベントの一部として設定されます。メッセージが解析マップと一致しない場合は、最初に一致しなかったエントリで解析が停止します。

解析マップ（プロパティリスト）はルールファイル（.fxm）にエクスポートすることができます。また、ルールファイルをインポートすることで解析マップ（プロパティリスト）をルールファイルから読み込むこともできます。

解析マップ（プロパティリスト）の作成について
解析マップの作成は、簡単な作業ではありません。進め方が分からない場合は、弊社カスタマーポータルからお問い合せください（ただし保守契約期間中のお客様に限ります）。

ルールをインポート

再構成ルールファイル（.fxm）をインポートすることができます。

ルールをエクスポート

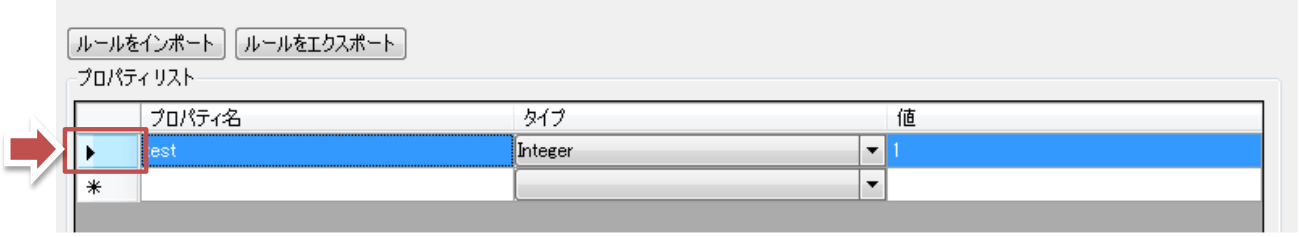
プロパティリストに作成した解析マップを再構成ルールファイル（.fxm）として保存することができます。

プロパティリスト

このセクションで解析マップを定義します。

解析マップは「**プロパティ名**」、「**タイプ**」、「**値**」の 3 つの列から構成されます。

既存の行を削除したい場合は、削除したい行の一番左の列（下図の赤枠部分）を選択してキーボードの「**Delete**」キーを押します。



プロパティ名

解析されるプロパティ名を入力します。ここには任意のプロパティ名を追加することができます。独自のプロパティを追加する場合は、標準プロパティとの重複を避けるために、名前の先頭に「u-」を付けることをお奨めします。例えば、「MyProperty」という名前のプロパティを作成したい場合は、「u-MyProperty」を使用することをお奨めします。

> **メモ**: Adiscon 社では「u-」から開始するプロパティを使用しません。

「Filler」というプロパティ名は予約されています。この「Filter」プロパティに割り当てられた値は破棄されます。このプロパティは、不要な充填文字などを取り除くことができます。

タイプ

解析するフォーマットを指定します。以下のいずれかから選択します。

タイプ	説明
Integer	整数を解析します。例: 12345
IP V4 Address	IPv4 アドレスを解析します。例:192.168.0.1
Character Match	文字を解析します。
Rest of Message	メッセージの残りの部分を指定します。
Single Word	次の単語を解析します。
UpTo	指定した値の先頭文字まで移動します。
ISO-like Timestamp	ISO 形式(例: 2017-07-24 13:37:00)のタイムスタンプを解析します。
UNIX/LINUX-like Timestamp	Unix/Linux 形式(15 桁の数字)のタイムスタンプを解析します。

値

値の追加が必要な場合に値を入力します。

メッセージのプレビュー

読み込み専用のボックスです。設定された解析ルールに一致する仮定のメッセージを表示します。

詳しくは、英語マニュアルの「Post-Process Event」をご参照ください。

5.6.4.6 ホスト名の解決

このアクションは、ホスト名を名前解決するために使用します。

> **メモ:**
> この機能はアクションとして実装されています。アクションはすべてのサービスで使用することができ、サービスの作業を遅延させることはありません。

名前解決するソースプロパティを選択

名前解決を実行するプロパティを指定します。「**挿入**」ボタンからプロパティを選択することができます。

名前解決の保存先プロパティ

名前解決の結果を保存するプロパティを指定します。「**挿入**」ボタンからプロパティを選択することができます。

名前解決されたホストをキャッシュに入れる

このチェックボックスをオンにすると、名前解決されたホストエントリをキャッシュに入れます。

既にソースプロパティに名前が入っている場合、完全な名前解決(FQDN)を行う

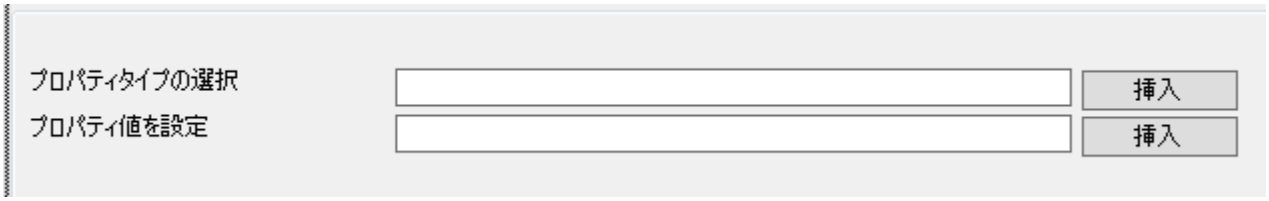
このチェックボックスをオンにすると、その名前を持つソースプロパティがすでに存在する場合、名前も解決されるという機能を有効にします。

5.6.4.7 プロパティの設定

このアクションは、受信したメッセージの一部のプロパティを変更するために使用します。

これは、管理者が例えば2つの同じ名前のデバイスの名前を変更したいような場合に特に役立ちます。

注記:
このアクションが実行されるとすぐに、変更または作成したプロパティの値が変更されます。プロパティ値はこのアクションの実行前は変更されていません。このアクションの実行後は、以前のプロパティ値は利用できなくなります。新しい値が設定された後は、すべてのアクションとフィルタの条件は新しい値を使用します。従って、例えば名前を変更したい場合は、このアクションをルールベースの先頭に定義してください。



プロパティタイプの選択

変更したいプロパティのタイプを選択します。「**挿入**」ボタンからプロパティを選択することができます。

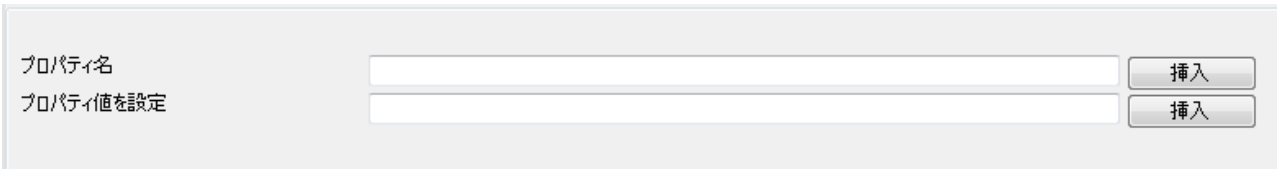
プロパティ値を設定

プロパティに割り当てる新しい値を入力します。任意の有効なプロパティ値を入力できます。

5.6.4.8 ステータスの設定

このアクションは、ステータス変数に値を設定するために使用します。

それぞれのインフォメーションユニットは特定のプロパティ(例えば、イベント ID、プライオリティ、ファシリティなど)を持っています。そして、これらのプロパティは、いくつかの値を持っています。イベント ID がプロパティ値 01 を持つと仮定します。既存のプロパティセットに「新たに自分で選んだプロパティ」を追加したい場合に、このアクションでこれを実行できます。



注記:
このアクションが実行されるとすぐに、変更または作成したプロパティの値が変更されます。プロパティ値はこのアクションの実行前は変更されていません。このアクションの実行後は、以前のプロパティ値は利用できなくなります。新しい値が設定された後は、すべてのアクションとフィルタの条件は新しい値を使用します。従って、例えば名前を変更したい場合は、このアクションをルールベースの先頭に定義してください。

プロパティ名（ステータス変数名）

プロパティ名を入力します。以降はルールベースの内部（フィルタの条件とアクション）で使用されます。

プロパティ値を設定（ステータス変数値）

プロパティに割り当てる値を入力します。任意の有効なプロパティタイプ値を入力できます。

5.6.5. その他のアクション

ここでは、「その他のアクション」グループに属するアクションについて説明します。

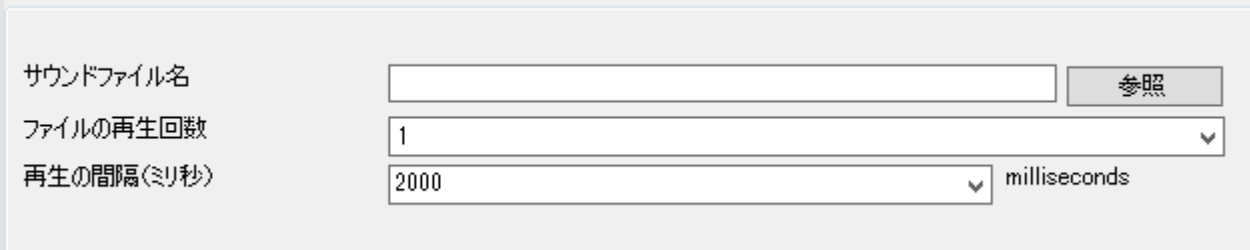
以下のアクションを含みます：

- サウンド再生
- プログラム開始

5.6.5.1 サウンド再生

このアクションは、サウンドファイルを再生するために使用します。

> **注記：**
> **このアクションは Windows Vista/2008 以降のシステムでは使用できません。**
> Microsoft 社により実施された仕様変更により、サービスとデスクトップとの対話（サウンドカードへのアクセスも含む）が Windows Vista 以降の OS で実行できなくなったため、それらの OS 上ではこのアクションは利用できません。



> **注記：**
> お使いのマシンに複数のサウンドカードがインストールされている場合、最初にインストールされたカードが常に使用されます。

サウンドファイル名

再生させるサウンドファイルのファイル名を指定します。.wav ファイルでなければなりません（MP3 など他

のフォーマットはサポートされていません)。ローカルマシン上のファイルのみを使用することをお奨めします。リモートマシン上にあるファイルの使用は公式にはサポートされません。

ファイルが見つからない、または有効なフォーマットでない場合には、代わりにシステムビープ音がなります(API 定義によりどのシステムでも可能であるはずです)。

ファイルの再生回数

ファイルの再生回数を指定します。100 回まで選択できます。

> **注記:**
> サウンドを再生するとパフォーマンスが低下し、WinSyslog はサウンドの再生中、他のすべてのアクションをブロックします。このため、必要最小限の回数に制限することをお勧めします。

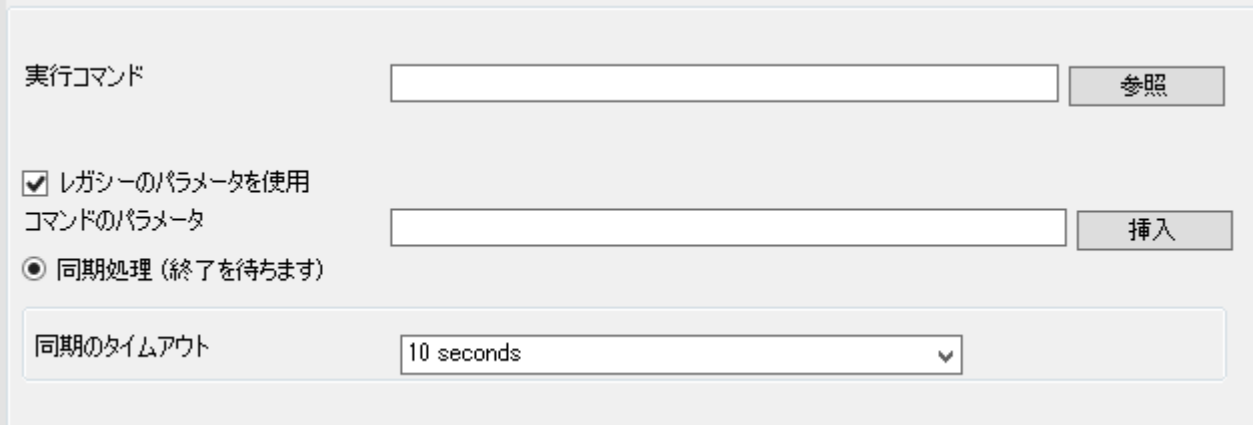
再生の間隔(ミリ秒)

「**ファイルの再生回数**」で 1 以外の回数が指定されている場合、各サウンド再生の待ち時間を指定します。

5.6.5.2 プログラム開始

このアクションは、外部プログラムを起動するために使用します。

実際のプログラム(.exe)、バッチファイル(.bat)、VB スクリプト(.vbs)など、有効な Windows 実行可能プログラムであればどんなものでも起動できます。



実行コマンド

実行させたい実際のプログラムファイルを指定します。有効な実行可能ファイルであればどのようなものでも指定できます。オペレーティングシステムのデフォルト検索パスでファイルを見つけることができる場合は、相対ファイル名を指定できます。

レガシーのパラメーターを使用

このチェックボックスをオンにすると、旧いスタイルのパラメーター処理が使用されます。オフの場合は、すべてのプロパティを使用できます。

コマンドのパラメーター

実行するプログラムに渡すパラメーターを指定します。これらは、コマンドラインパラメーターとして渡されます。特定のフォーマットはありません。スクリプト次第です。

パラメーターには、イベントの詳細をカスタマイズするために、置換文字列を含めることができます。これにより、イベントデータをスクリプトに渡すことができます。次の置換文字列を使用できます:

置換文字	説明
%d	日付と時間(ローカルタイム)
%s	メッセージを送信したソースシステムの IP アドレス、もしくはホスト名(「ホスト名の解決」の設定に左右されます)
%f	受信したメッセージのファシリティコードの数値
%p	受信したメッセージのプライオリティコードの数値
%m	メッセージ本体
%%	% 記号

例えば、このフィールドに「e1"%s""%m"」と設定し、「172.16.0.1」から「This is a test.」というメッセージを受信した場合、スクリプトは3つのパラメーターで開始されます。

1つ目のパラメーターは「e1」です。これはスクリプトに何らかの意味があるとみなされます。2つ目は、「%s」なので IP アドレス(172.16.0.1)、3つ目は、「%m」なのでメッセージ本体(「This is a test.」)になります。

> **注記:**
> 2つの引用符(")で置換文字列を挟むことによって、メッセージが1つのパラメーターとして処理されます。
> 引用符がない場合は、通常、複数に分割されます(3つ目のパラメーターが「This」、4つ目のパラメーターが「is」となります)。置換文字列を使用する場合には、引用符を忘れずに入力してください。

同期のタイムアウト

プログラムが実行されると、サービスはこれが完了するのを待ってから次のアクションを実行します。これは、すべてのアクションが正しい順番で確実に実行されるようにするためです。

外部のプログラムは、限られた時間のみで実行されるべきです。何らかの理由でブロックされた場合、

WinSyslog サービスはそれ以降の処理を実行できなくなります。このため、タイムアウト値を指定する必要があります。設定したタイムアウト時間を過ぎてもプログラムが終了しない場合、ルールエンジンはそれをキャンセルし、アクションを失敗としてフラグが立ててから、それ以降の処理を続行します。

> **重要:**
> タイムアウトの値は最高 30 秒まで設定できますが、外部プログラムの実行時間を 5 秒未満に制限することをお勧めします。そうしないと、全体のパフォーマンスに多大な影響が出る可能性があります。平均実行時間が 5 秒である場合、デフォルトの設定値である 10 秒は、システム活動が激しいときでも、そのプログラムの終了を待つことができることを保証します。

パフォーマンス上の理由から、「**プログラム開始**」アクションは、頻繁に適用されないルールに対してのみ使用することを強くお勧めします。

6. 参考情報

Adiscon WinSyslog に関する情報は以下にあります:

- **製品紹介:**

製品紹介ページ	WinSyslog の製品紹介ページです。
製品ラインアップ	WinSyslog ラインナップの紹介ページです。
製品ガイド	WinSyslog の製品紹介ガイド(PDF)です。

- **サポート関連:**

Adiscon WinSyslog ドキュメント	WinSyslog ドキュメント一覧ページです。
バージョンヒストリー	WinSyslog の更新履歴です。
FAQ - WinSyslog に関するご質問	WinSyslog に関するよくあるご質問とその回答です。
サポート仕様	サポート仕様です。WinSyslog を選択してください。
カスタマーポータル	ご購入後の製品に関するお問合せ・履歴管理窓口です。

- **ソフトウェアダウンロード:**

ソフトウェアダウンロード	フリー版、評価版ソフトウェアのダウンロードページです。
フリー版ご紹介	フリー版の紹介ページです。

- **その他関連情報:**

シスログ談話室	Syslog 全般に関する情報提供ページです。
EventReporter 製品紹介ページ	EventReporter の製品紹介ページです。

お問い合わせ

弊社では、Adiscon WinSyslog に関するご意見、フィードバックをお待ちしております。
Adiscon WinSyslog についてご不明な点がございましたら、以下までお問い合わせください。

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

住所: 〒183-0023 東京都府中市宮町 2-15-13 第 15 三ツ木ビル 8F
URL: http://www.jtc-i.co.jp/
電話番号: 042-358-1250
FAX 番号: 042-360-6221

購入前のお問い合わせ
お問い合わせフォーム: https://www.jtc-i.co.jp/contact/scontact.php
メール: sales@jtc-i.co.jp
購入後のサポートお問い合わせ
カスタマーポータル: https://www.jtc-i.co.jp/support/customerportal/

免責事項について

本書に掲載されている内容は、Adiscon「WinSyslog」英文マニュアルの参考訳です。あくまでもお客様の便宜のためのものであり、この内容が英文と合致することを保証するものではありません。また、翻訳された情報が最新であることを保証するものではありません。万一、本書の内容に誤りもしくは不足ががあった場合でも、弊社は記載されている情報の利用による損害や損失に対するいかなる責任も負いません。十分にご検証の上ご利用ください。

日本語マニュアル発行日 2018 年 10 月 5 日

原文: Adiscon WinSyslog 15.0

ジュピターテクノロジー株式会社 技術グループ