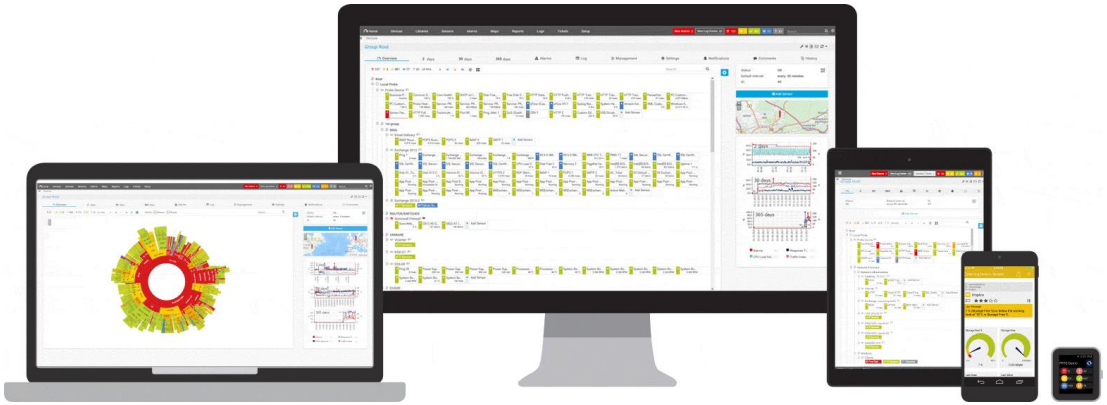
PRTGネットワークモニター

センサー紹介：「Syslog レシーバー」センサー



ジュピターテクノロジー

2023/12/05
v1.2

「Syslog レシーバー」センサー

できること

・Syslogメッセージを受信

・受信するSyslogメッセージをフィルタリング

・ Syslogメッセージの受信をトリガーとして、通知を実行

・受信したSyslogメッセージのログ、メッセージ内容の確認

できないこと

・受信したSyslogメッセージ内容をエクスポート

※Syslogメッセージの長期保存は想定していません。
（デフォルトの保存期間　32日）

Syslog レシーバーの監視をはじめる前に

はじめる前の確認事項

監視対象機器で確認

Syslog 機能の有効化

Syslogメッセージの送信先を
PRTGサーバーのIPアドレスに設定

Syslog送信先ポート
（デフォルト:UDP514）

一致させる

PRTGウェブGUIで確認

Syslog レシーバーセンサーの設定

リッスン対象ポート
（デフォルト:UDP 514）

監視対象機器からPRTGサーバー間のSyslog通信の許可を確認
（デフォルト:UDP 514）
ファイヤーウォール、セキュリティソフトなど

※Syslog レシーバー センサーはUDPのみを対応しています。
（TCPは対応していません。）

「Syslog レシーバー」センサーの追加

「Syslog レシーバー」センサーの追加

・”プローブデバイス”または、監視対象の”デバイス”にセンサーを追加
・[センサー追加]から「Syslog レシーバー」センサーを追加

“プローブデバイス”に追加した場合
・PRTGサーバーに送られる全てのSyslogメッセージを受信するセンサーになる

監視対象の”デバイス”に追加した場合
・送信元IPアドレスが監視対象”デバイス” のSyslogメッセージのみを受信するセンサーになる

※設定の詳細は別紙「簡易マニュアル」から”センサーの追加”を参照

「全般」画面

監視間隔（デフォルトは1分）の間に受信したSyslogメッセージ数をカウント

メッセージ数

監視間隔の間に48件のメッセージを受信

監視間隔の間に37件のメッセージを受信
そのうち1件を”エラー”としてカウント

「エラー」、「警告」のカウントはフィルター設定（後述）で処理。
カウントは監視間隔のたびにリセット。累積しない。

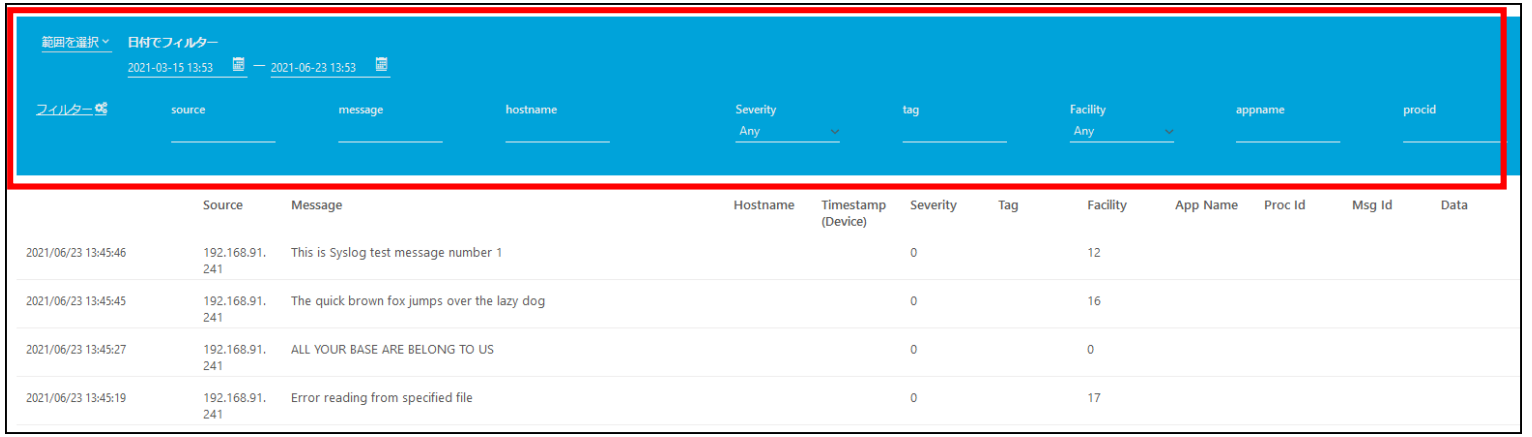
※監視間隔の最大値は”1日”

「メッセージ」画面

Syslog メッセージを表示

受信したSyslogメッセージは保存され、「メッセージ」から確認できる

表示するメッセージは
フィルタリングできる



※メッセージの保存期間はデフォルト32日

フィルター設定

フィルター設定でSyslogメッセージを処理

包含フィルター	severity[0-6]	メッセージを受信・保存
除外フィルター	facility[1-3]	受信しない
警告フィルター	message[warning]	メッセージを受信・保存 **"警告"** にカウント
エラーフィルター	message[error]	メッセージを受信・保存 **"エラー"** にカウント

フィルターに一致した場合

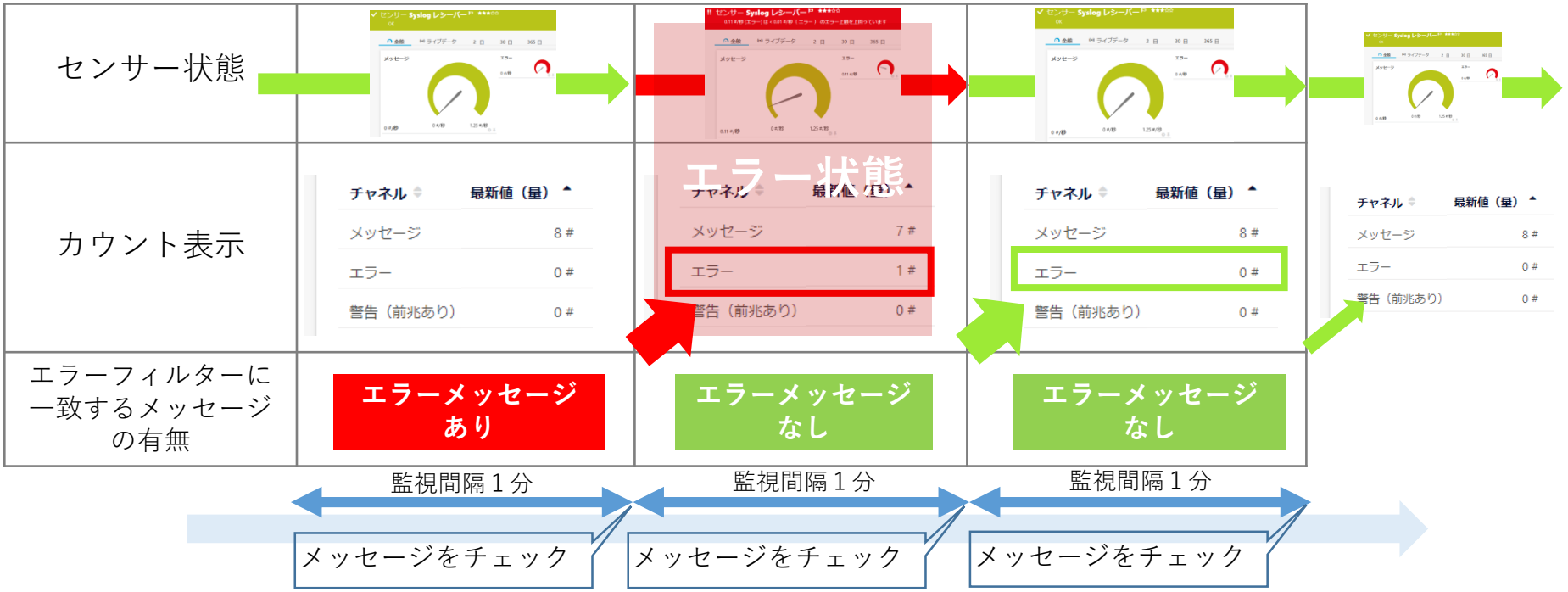
センサー状態変化

受信したメッセージは保存され、「メッセージ」画面から確認できる

※フィルター構文は後述

センサーの状態変化

Syslogメッセージの受信からセンサーの状態変化の流れ（エラーの場合）



受信したメッセージを監視間隔ごとにチェック。
エラーフィルターに一致するメッセージを受信していた場合、センサーがエラー状態に変化。
エラーフィルターに一致するメッセージを受信していなかった場合、アップ状態（緑）に変化。

※エラー状態に変化した後にエラーメッセージを受信しなかった場合、センサーは機器の実際の状態にかかわらずアップ状態に戻ります。
機器がエラーメッセージを最初の一度しか出さない場合などは、センサーの状態と機器の実際の状態が一致していない可能性があります。

通知

センサーの状態変化をトリガーとして通知を実行

※センサー状態変化ですぐに通知が実行されるように「通知トリガー」を設定することを推奨します。

※設定の詳細は別紙「簡易マニュアル」から”センサーの追加”を参照

「Syslog レシーバー」センサーの制限

センサー数の制限

・負荷の高いセンサーのためプローブあたり、**50個以下**の使用を推奨
→ 50個を超える場合はリモートプローブで負荷分散

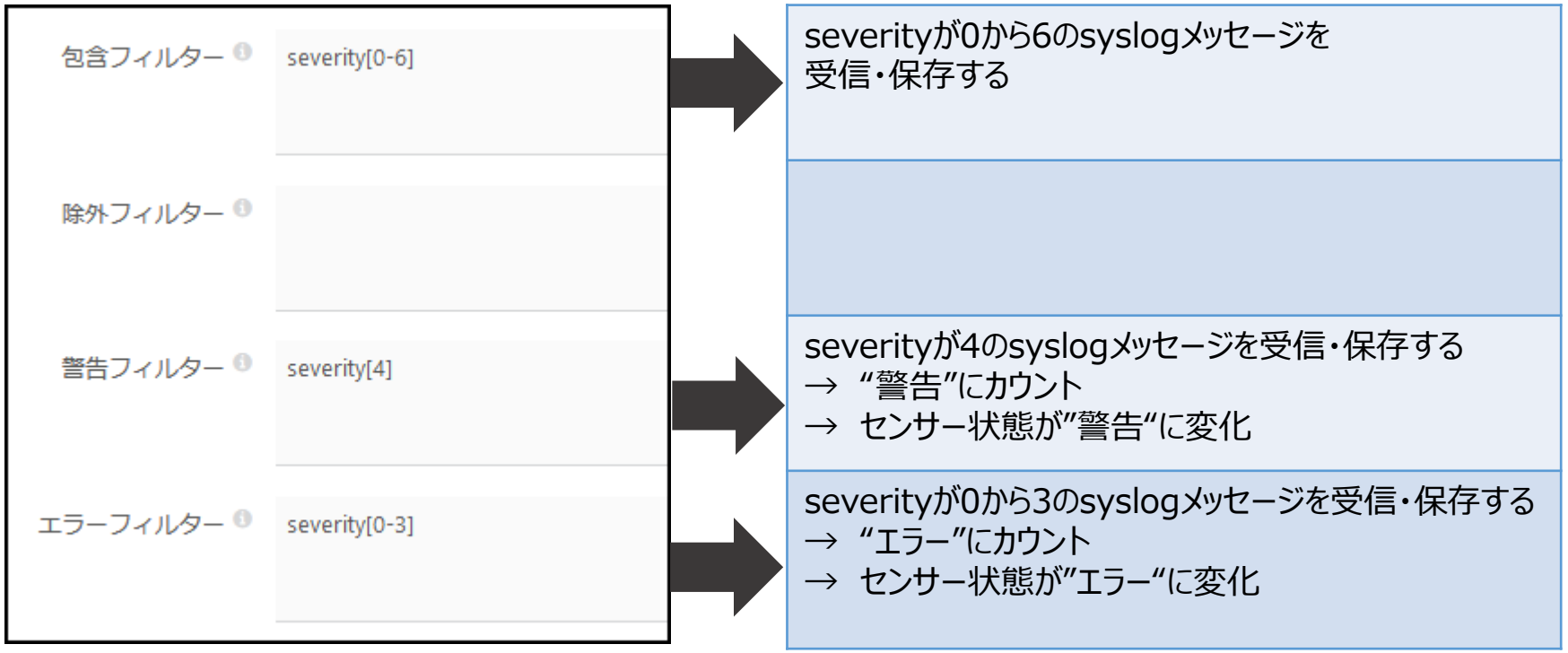
PRTGクラスター機能での制限

・PRTGクラスター機能で冗長化できない
・クラスター構成で「Syslog レシーバー」センサーを追加できるのは
マスターノードのPRTGサーバーのみ

Syslogレシーバーセンサー
参考情報

参考情報: フィルターのデフォルト設定

Syslog レシーバー センサーフィルターのデフォルト設定



参考情報: フィルター構文

フィルターは AND、 OR、 NOT、 括弧および以下のフィールドを使用する式です。

フィールド	パラメーター	例
source[ip]	UDP ソース IP、IP 範囲、または IP ホストマスクを入力します	source[10.0.23.50] source[10.0.23.10-50] source[10.0.23.10/24]
facility[number]	facilityコードを 0 ～ 23 までの数字または範囲で入力します	facility[2] facility[5-7] facility[5] OR facility[6]
severity[number]	severityコードを 0（緊急）～ 7（デバッグ）までの単数または範囲で入力します	severity[4] severity[1-3] severity[1] AND severity[2]
hostname[text]	一致するホスト名文字列を入力します（完全一致、大文字と小文字を区別	hostname[www.example.com]
tag[text]	一致するタグ文字列を入力します（完全一致、大文字と小文字を区別）	tag[su]
appname[text]	一致するアプリ名文字列を入力します（完全一致、大文字と小文字を区別）	appname[myproc] appname[demo] AND msgid[m42]
procid[text]	一致するプロセス ID 文字列を入力します（完全一致、大文字と小文字を区別）	procid[1860]
msgid[text]	一致するメッセージ ID 文字列を入力します（完全一致、大文字と小文字を区別）	msgid[ID47]
message[parttext]	メッセージフィールドと一致するサブストリングを入力します（部分、大文字と小文字を区別）	message[Error]
data[id,param,value] data[parttext] data[id,param]	テーブルに表示された構造データに一致するサブストリングを入力します（部分、大文字と小文字を区別）； または、ID およびパラメーター（カンマで区切る）を入力してパラメーターが ID 要素に含まれているか確認します; もしくは、構造データの値に一致する ID、パラメーター、および値（カンマで区切る）を入力します（RFC 5424）	data[exampleSDID@12345,eventSource,Application] data[exampleSDID@1234] data[exampleSDID@1234,eventSource]

※詳細はメーカーマニュアル（英語）をご参照ください。
https://www.paessler.com/manuals/prtg/syslog_receiver_sensor.htm#filter_rules

参考情報: フィルター例

- 「Error」を含むメッセージをフィルタリング

```
message[Error]
```

- 「Error」または「Warning」を含むメッセージをフィルタリング

```
message[Error] OR message[Warning]
```

- 「Error」と「Warning」の両方を含むメッセージをフィルタリング

```
message[Error] AND message[Warning]
```

- severity値をフィルタリング

```
severity[4]
```

- 文字列「exampleSDID@1234」と一致するデータをフィルタリング

```
data[exampleSDID@1234]
```

※詳細はメーカーマニュアル（英語）をご参照ください。
https://www.paessler.com/manuals/prtg/syslog_receiver_sensor.htm#filter_rules

お問い合わせ先

- **国内販売元：**　ジュピターテクノロジー株式会社
- **住所：**　〒183-0023　東京都府中市宮町一丁目40番地　KDX府中ビル6F
- **URL：**　https://www.jtc-i.co.jp
- **電話番号：**　042-358-1251
- **FAX番号：**　042-360-6221

- **評価用にセンサー数無制限で30日間利用可能なライセンスを提供**
- **簡易マニュアル、製品ガイド、などをご用意**

お問い合わせは　www.jtc-i.co.jp/contact/scontact.php　**まで**

PRTG NETWORK MONITOR

免責事項・使用限定事項

ジュピターテクノロジー株式会社（以下当社と略記します）が作成した本ドキュメントに関する免責事項および本ドキュメント使用に関する限定事項は以下の通りです。

本ドキュメントに関する免責事項

本ドキュメントは作成時点においてメーカーより提供された情報および当社での検証結果により作成されたものですが、当社は本ドキュメントの内容に関していかなる保証をするものではありません。万一、内容についての誤りおよび内容に基づいて被った損害が発生した場合でも一切責任を負いかねます。本ドキュメントの内容によりなされた判断による行為で発生したいかなる損害に対しても当社は責任を負いません。

本ドキュメント使用に関する限定事項

別に定める場合を除いて、本ドキュメントの取り扱いは当社より提供を受けたお客様による私的かつ非営利目的での使用に限定されます。お客様は、本ドキュメントについて、変更、コピー、頒布、送信、展示、上映、複製、公開、再許諾、二次的著作物作成、譲渡、販売のいずれも行うことができません。

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

住所：　〒183-0023　東京都府中市宮町一丁目40番地　KDX府中ビル6F
URL：　https://www.jtc-i.co.jp/
電話番号：　042-358-1250
FAX番号：　042-360-6221
お問い合わせ先：　https://www.jtc-i.co.jp/support/customerportal/