

# 目次

1	SYSTEM REQUIREMENTS (システム要件)	6
1.1	DETAILED SYSTEM REQUIREMENTS (システム要件詳細)	6
2	INSTALLATION (インストール)	10
2.1	DOWNLOADING THE SOFTWARE (ソフトウェアダウンロード)	10
2.2	UPGRADING TO VERSION 7 FROM PREVIOUS VERSIONS (v.7 へのアップグレード)	10
2.3	INSTALLATION OF A PRTG CORE SERVER (PRTG コアサーバーのインストール)	11
2.4	ENTERING A LICENSE KEY (ライセンスキーの入力)	14
2.5	INSTALLATION OF A PRTG REMOTE PROBE (PRTG リモートプローブの設定)	15
2.6	UNINSTALLATION (アンインストール)	16
3	INTRODUCTION (概要)	18
3.1	KEY FEATURES (基本機能)	19
3.2	AVAILABLE LICENSES (ライセンスの種類)	19
3.3	ABOUT THIS DOCUMENT (本マニュアルについて)	20
4	BASIC CONCEPTS OF PRTG NETWORK MONITOR (PRTG NETWORK MONITOR の基本概念)	22
4.1	ARCHITECTURE: PRTG CORE SERVER AND PRTG PROBE (アーキテクチャ: PRTG コアサーバー、PRTG プロブ)	22
4.2	OBJECT HIERARCHY: PROBES, GROUPS, DEVICES, SENSORS, CHANNELS (オブジェクト階層: プロブ、グループ、デバイス、センサー、チャンネル)	25
4.3	INHERITANCE OF SETTINGS (設定の継承)	26
4.4	NOTIFICATIONS, SCHEDULES, AND DEPENDENCIES (通知、スケジュール、ディペンデンシー (依存性))	27
4.5	REPORTS, MAPS, AND TODOS (レポート、マップ、TODOS)	28
4.6	PRIORITIES AND FAVORITE SENSORS (優先順位とお気に入りセンサー)	29
4.7	DEFAULT VALUES (デフォルト値)	30
5	USER INTERFACES (ユーザーインターフェース)	32
5.1	WEB INTERFACE NAVIGATION (WEB インターフェースナビゲーション)	34
5.2	WEB PAGE OVERVIEW (WEB ページ概要)	36
5.3	CONTEXT MENUS (コンテキストメニュー)	40
5.4	LISTS (リスト)	40
5.5	MONITORING STATUS INFORMATION AVAILABLE THROUGH THE WEB INTERFACE (WEB インターフェース	

スからの監視ステータス情報) .....	41
5.6 SYSTEM TRAY NOTIFIER (システムトレイ通知) .....	43
5.7 IPHONE USER INTERFACE IPHONE (ユーザーインターフェース) .....	43
<b>6 SENSOR SETUP (センサー設定) .....</b>	<b>46</b>
6.1 REVIEWING SETTINGS OF THE ROOT GROUP (ルートグループの設定確認) .....	46
6.2 CREATING GROUPS, DEVICES AND SENSORS MANUALLY (グループ、デバイス、センサーの手動作成) .....	48
6.3 CREATING DEVICES AND SENSORS USING THE AUTO DISCOVERY (オートディスカバリーでのデバイス / センサーの作成) .....	51
<b>7 SENSOR TYPES (センサータイプ) .....</b>	<b>55</b>
7.1 SNMP SENSOR TYPES (SNMP センサータイプ) .....	55
7.2 WMI SENSOR TYPES (WMI センサータイプ) .....	58
7.3 HTTP SENSOR TYPES (HTTP センサータイプ) .....	60
7.4 PACKET SNIFFING SENSOR TYPES (PACKET SNIFFING (パケットスニフing) センサータイプ) ...	62
7.5 NETFLOW SENSOR TYPES (NETFLOW センサータイプ) .....	64
7.6 SQL SERVER SENSOR TYPES (SQL サーバーセンサータイプ) .....	66
7.7 FILE SERVER SENSOR TYPES (ファイルサーバーセンサータイプ) .....	68
7.8 MAIL SERVER SENSOR TYPES (メールサーバーセンサータイプ) .....	68
7.9 VMWARE SERVER SENSOR TYPES (VMWARE サーバーセンサータイプ) .....	70
7.10 INTERNET PROTOCOL SENSOR TYPES (インターネットプロトコルセンサータイプ) .....	70
7.11 CUSTOM SENSOR TYPES (カスタムセンサータイプ) .....	71
7.12 SENSOR FACTORY (センサーファクトリー) .....	72
7.13 COMPARISON OF BANDWIDTH MONITORING SENSOR TYPES (帯域監視センサータイプの比較) ....	77
<b>8 NOTIFICATIONS (通知) .....</b>	<b>80</b>
<b>9 MAPS (マップ) .....</b>	<b>85</b>
<b>10 REPORTS (レポート) .....</b>	<b>93</b>
<b>11 TODOS (TODO) .....</b>	<b>99</b>
<b>12 USER MANAGEMENT (ユーザー管理) .....</b>	<b>101</b>
<b>13 SYSTEM SETTINGS AND ADMINISTRATION (システム設定と管理) .....</b>	<b>105</b>
13.1 ACCOUNT SETTINGS - MY ACCOUNT (アカウント設定 - マイアカウント) .....	105
13.2 ACCOUNT SETTINGS • SCHEDULES (アカウント設定 - スケジュール) .....	106
13.3 ACCOUNT SETTINGS • NOTIFICATIONS (アカウント設定 - 通知) .....	108

13.4	SYSTEM SETUP - WEB SERVER(システム設定 - WEB サーバー) .....	110
13.5	SYSTEM SETUP ・ PROBES(システム設定 - プロブ) .....	111
13.6	SYSTEM SETUP ・ NOTIFICATIONS(システム設定 - 通知) .....	111
13.7	CORE SERVER ADMIN TOOL(コアサーバー管理ツール) .....	113
13.8	PROBE ADMIN TOOL(プロブ管理ツール) .....	116
14	ADVANCED TOPICS(追加トピック) .....	120
14.1	TOPLISTS(トップリスト) .....	120
14.2	MULTIPLE PROBES AND REMOTE PROBES(複数プロブとリモートプロブ) .....	123
14.3	COPYING DEVICES BY CLONING OR USING DEVICE TEMPLATES(クローニング/デバイステンプレートによるデバイスのコピー) .....	130
14.4	IMPORTING DATA FROM PRTG TRAFFIC GRAPHER 6 / IPCHECK SERVER MONITOR 5(PRTG TRAFFIC GRAPHER 6 / IPCHECK SERVER MONITOR 5 からのデータのインポート) .....	131
14.5	INSTALLING AN SSL CERTIFICATE FOR THE WEB SERVER(WEB サーバーの SSL サーバ証明書の設定) .....	131
14.6	USING THE PRTG API (APPLICATION PROGRAMMING INTERFACE) (PRTG API の使用) .....	131
14.7	INTERFACE DEFINITION FOR CUSTOM EXE SENSORS(カスタム EXE センサーのインターフェイス定義) .....	132
14.8	ACKNOWLEDGEMENTS(謝辞) .....	133

# Part

# I

## System Requirements (システム要件)

## 1 System Requirements (システム要件)

PRTG Network Monitor をインストールして実行するには、以下の環境が必要です。

- ・ 2007 年以降に生産された平均的な性能の PC、サーバー、バーチャルマシン
- ・ OS: Microsoft Windows XP/2003/Vista/2008 (32 ビット、もしくは 64 ビット)
- ・ ブラウザ: Google Chrome/Firefox 3/Internet Explorer 7/8 (web インターフェースに接続するため)

より詳しい情報が必要な場合や、大規模な設定をお考えの場合は、**1.1 システム要件詳細**をご参照ください。

### 100 センサー以上のインストール

2007 年以降に生産された平均的な PC/サーバーであれば、1000 センサーの監視は可能と考えられます (SNMP V3、WMI、Packet Sniffing (パケットスニフing) の場合、例外あり)。大規模な設定をお考えの場合、Paessler 社ナレッジベースの "Planning Large Installations of PRTG Network Monitor 7" をご参照ください。

[http://www.paessler.com/support/kb/prtg7/system\\_requirements](http://www.paessler.com/support/kb/prtg7/system_requirements)

### 1.1 Detailed System Requirements (システム要件詳細)

#### PRTG コアサーバー、PRTG コアプロブの OS 要件

32 ビット版もしくは 64 ビット版の以下の OS に対応しています。

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

#### PRTG コアサーバー、PRTG コアプロブのハードウェア要件

ハードウェア要件は、主にセンサータイプと設定間隔によって異なります。以下の数字は、一般的 PRTG 7 の使用を想定したもので参照ください (デフォルトの 60 秒間隔の監視で換算)。

- CPU: 2008 年製の平均的な PC であれば、1000 センサーは容易に監視可能です (センサータイプについては以下をご覧ください)。
- RAM: 150KB/センサー
- ハードディスク: 1 センサーにつき、約 200KB のディスク空き容量/日 (60 秒間隔の監視)

- ライセンスのアクティベーションには、インターネット接続が必要になります (HTTP もしくは E メール経由)。

WMI や SNMP V3 センサーといったセンサータイプには、ハードウェア以外のものに依存する制限がありますが、これら制限は、複数のリモートプローブセンサーを分配ことで解決できます。500-1000 センサー以上、或いは、10Packet Sniffing (パケットスニフing) / NetFlow センサーの設定をお考えの場合、PRTG Site Planner tool ("Help"メニュー)をご参照下さい。

大規模な設定の例:

弊社では以下の条件で PRTG Network Monitor 動作検証に成功しました。30,000SNMP センサーで実行する PRTG Network Monitor を Windows2003、64 ビット、2x-Quad コア CPU システム (Dell 2900 III) で検証。このシナリオでは、PRTG 処理に約 3GB の RAM が必要となり、CPU は負荷 20% で作動、約 1.5TB/年のデータがディスク上に生成されます。このサイズで設定した場合、645 台の 48 ポート SNMP 対応スイッチの監視が可能です。

## バーチャルマシン上での PRTG の実行

PRTG プローブや PRTG コアサーバーは、バーチャルプラットフォーム上でも実行可能です。以下のバーチャルプラットフォームは検証済みです。

Technology	Client OS
VMware ESX Server 3.5	Windows XP, Windows 2003 (32/64 bit), Windows Vista, Windows 2008
VMware Server 2.0	Windows XP, Windows 2003 (32/64 bit), Windows 2008
XEN Server 5.0	Windows XP
Parallels Virtuozzo Containers	Windows 2003 Server (32/64 bit)
Amazon EC2	Windows Server 2003

## Web ブラウザ要件

PRTG Web インターフェースは、そのパフォーマンスと信頼性において、以下のブラウザに対応しています。

- Google Chrome 1.0 (推奨)
- Mozilla Firefox 3.0
- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 7

## 監視デバイス要件

- SNMP 監視: 監視デバイスには SNMP v1/v2c/v3 のいずれかの実装が必要で (デバイス上に必ず SNMP 対応ソフトウェアがインストール済みであること)。デバイスは必ず SNMP を有効にし、PRTG 実行マシンにおいては必ず SNMP インターフ

エースのアクセス許可をして下さい。

- WMI 監視： WMI (Windows Management Instrumentation) 監視には、Windows ネットワークが必要です。WMI で監視するクライアント PC は、Windows XP 以降 (XP/2003/Vista/2008 等) のみが対応しています。Windows 2000 は対応していません。
- NetFlow 監視： PRTG プローブ実行マシンに NetFlow データパケット (NetFlow Version 5) を送信するよう、デバイス設定して下さい。
- Packet Sniffing (パケットスニフing)： ローカルマシンのネットワークカードを通過するデータパケットだけが分析可能です。スイッチド・ネットワーク内のネットワーク全体の監視には、“モニタリングポート”を装備したスイッチが必要です。

### Tray Tool、iPhone インターフェース要件

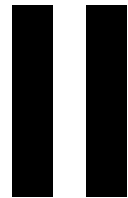
PRTG Tray Tool はオプションで、Windows の全てのバージョン (Windows 95 以降) でお使いいただけます。iPhone インターフェースもオプションで、iPhone firmware 2.0 に対応しています。

### 100 センサー以上のインストール

2007 年以降に生産された平均的な PC/サーバーであれば、1000 センサーの監視は可能と考えられます (SNMP V3、WMI、Packet Sniffing (パケットスニフing) には例外有)。大規模な設定をお考えの場合、弊社ナレッジベースの "Planning Large Installations of PRTG Network Monitor 7" をご参照ください。

[http://www.paessler.com/support/kb/prtg7/system\\_requirements](http://www.paessler.com/support/kb/prtg7/system_requirements)

# Part



## Installation (インストール)

## 2 Installation (インストール)

PRTG Network Monitor をご利用頂くにあたり、ソフトウェアのダウンロードとインストールが必要です。以下のセクションで説明します。

- ソフトウェアのダウンロード: Paessler 社からの最新バージョンの入手方法
- v.7 へのアップグレード: PRTG Traffic Grapher 6/IPCheck Server Monitor 5 以前をご利用の方
- PRTG コアサーバーの設定: PC/サーバーへの PRTG コアサーバーの設定方法
- ライセンスキーの入力
- アンインストール: PC/サーバーからのソフトウェアの削除方法

### 2.1 Downloading the Software(ソフトウェアダウンロード)

ライセンス購入時にライセンス CD にソフトウェアが含まれています。最新ライセンスでない場合はインストール後、プログラムから直接ダウンロードすることが可能です。

#### トライアル版(評価用)とトライアルキーのお申し込み

トライアル版(評価用)のソフトウェアとトライアルキーは弊社 web サイト <http://www.jtc-i.co.jp/> からお申し込み下さい。トライアルキーの有効期限は 30 日間です。

#### 商用版のお申し込み

価格、機能、ライセンスのご注文等のお問合せは弊社ジュピターテクノロジー(株)へお願いいたします。

### 2.2 Upgrading to Version 7 from Previous Versions (v.7 へのアップグレード)

PRTG Network Monitor の旧版 (V7.x) をご利用の方は、旧バージョンに最新バージョンをインストールしていただけます。

#### PRTG Traffic Grapher 6/IPCheck Server Monitor 5 からのアップグレード

PRTG7 の前身商品 (PRTG Traffic Grapher v.6 と IPCheck Server Monitor v.5) をご利用の方は、PRTG7 ヘデータ (監視設定と履歴データ) をインポートできます。それ以前のバージョンからのデータインポートは出来ません。

詳細は Paessler 社 web サイトのナレッジベースをご参照下さい。

[http://www.paessler.com/support/kb/prtg7/tricks/data\\_import\\_from\\_prtg6\\_or\\_ipcheck5/](http://www.paessler.com/support/kb/prtg7/tricks/data_import_from_prtg6_or_ipcheck5/)

### 2.3 Installation of a PRTG Core Server (PRTG コアサーバーのインストール)

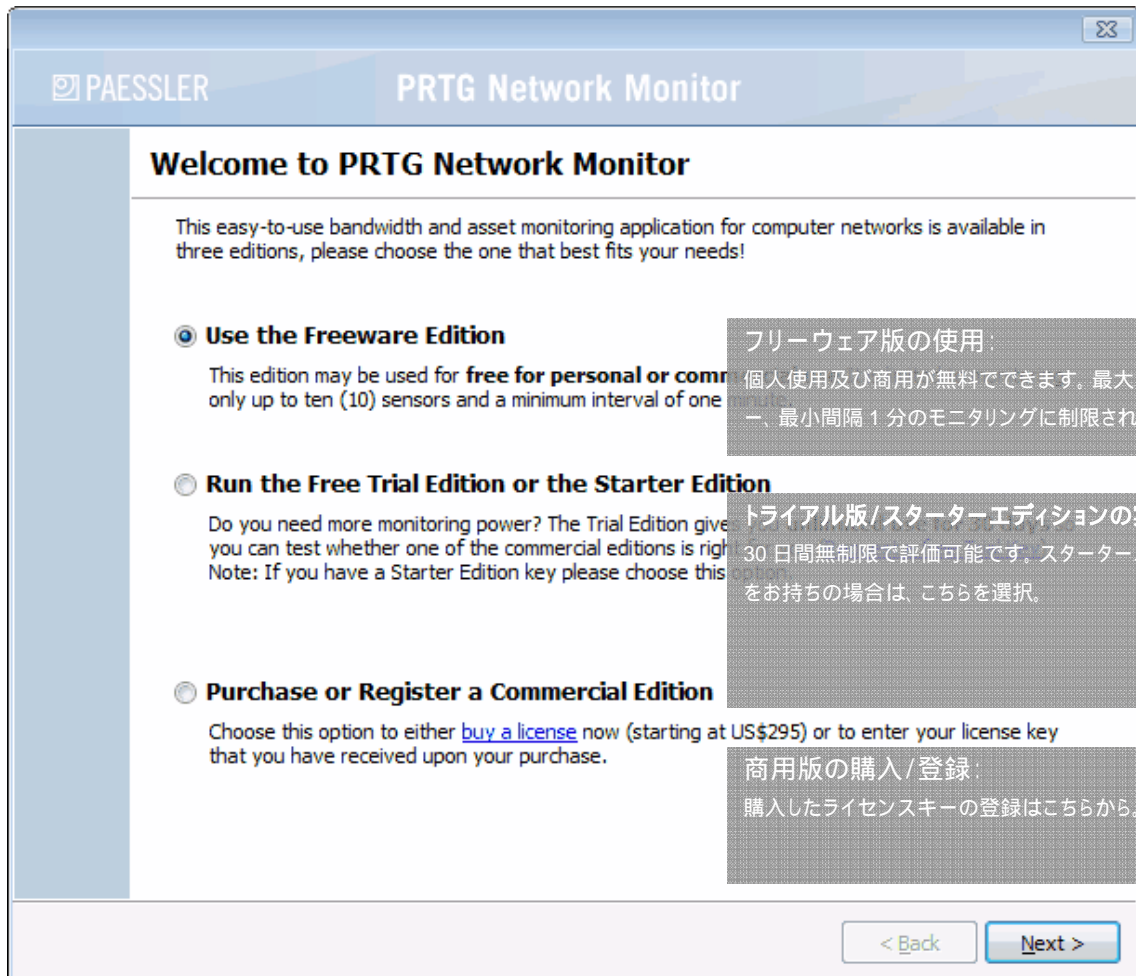
ソフトウェアのインストールは他の Windows ベースのアプリケーションと同様です。本アプリケーションをインストールする時、PC に弊社が送付した CD-ROM を挿入して頂き、ダウンロードした ZIP ファイルを解凍し、インストール・セットアップ・ルーチンを開きます。

ソフトウェア・インストール・ウィザードに従ってインストールを完了することができます。



ウィザードを次に進めるには、「Next」をクリックしてください。

ライセンス契約書に同意後、インストールしたいソフトウェアのフォルダを選択して下さい。「Next」をクリックすると、必要なファイルがディスクにコピーされ、ライセンスタイプを確認するダイアログが現れます。



該当するものを選択し、必要なデータを入力してください。

“Next”をクリックすると、基本設定ダイアログが現れます。

**Essential Settings for PRTG Network Monitor**

**Administrator Account**

Login Name: prtgadmin Password: \*\*\*\*\*

Email Address: Confirm Password: \*\*\*\*\*

**Web Server IPs**

Localhost only (127.0.0.1, no external access)

Specify IPs

192.168.2.212

**Web Server Port**

Standard Web Server Port 80 (recommended setting)

HTTPS/SSL on port 443

Specify Port: 80

**Site Info**

Site Name: PRTG Network Monitor

< Back Next >

通常、この画面で変更するのは"Email Address"欄だけです。ユーザーのEメールアドレスを入力して下さい。

ここで変更、確認できるのは、以下の設定です。

- 任意で、ユーザー自身が選択した"Login Name"と"Password"を入力できます(デフォルトは、ユーザー名"prtgadmin"、パスワード"prtgadmin")。ユーザーPRTG webサイトをインターネットで利用する場合、初期パスワードの変更は特に重要です。
- "Web Server IP's"(webサーバーIPアドレス)と"Web Server Ports"(webサーバーポート)の設定を確認して下さい。基本的に、デフォルト値で問題ありません。
- 任意で、"Site Name"をユーザーのPRTGwebサイトに設定できます。(例;"My Company Monitoring")

もう一度"Next"をクリックして、インストールを終了して下さい。

インストール終了後、インストールを完了するために、再起動するかどうか確認されます。後で再起動することもできますが、すぐ再起動させて、インストールを完了させることをお勧めします。

以上で、完了です。

## 2.4 Entering A License Key (ライセンスキーの入力)

PRTG Network Monitor のライセンスキーは、ライセンシーユーザー名と 70 個の文字/数列で構成されています。通常、キーは、ユーザーに E メールで送付されます。

- ユーザー名(例): Paessler AG
- ライセンスキー(例):  
0223515-FFSEJC-ZHGRDFM-URDCS8-U7TFGK-G665F2-YVFCDD-H8823ND99HG9-MFDRG

ライセンスキーの入力は、インストール時、または PRTG Server Administrator tool を使用してのいずれでも可能です。

**Step 1: 正しいエディションのものをインストールしたか、確認して下さい。**

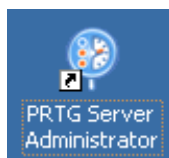
PRTG で使用できるインストーラは 2 つあります (2.1 ソフトウェアダウンロード参照)

- 公開インストーラ: フリーウェア版、スターター版、トライアル版にのみ付属。
- The Commercial Installer: ライセンス購入者用。

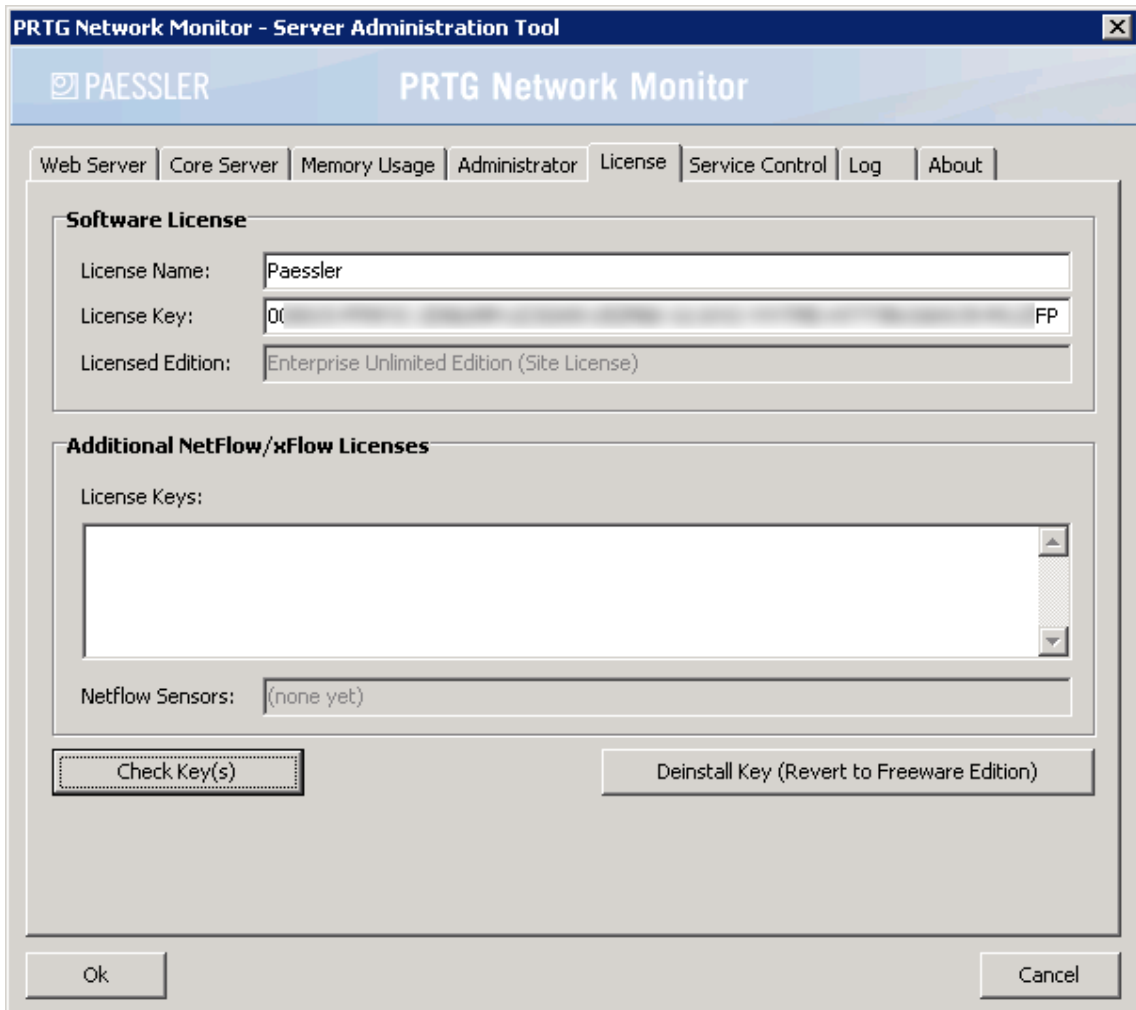
The Commercial Installer は、PRTG Network Monitor 商用版の実行に必要です。PRTG のライセンスキーを購入したユーザーは、ライセンスキーを適用するために、弊社の出荷 CD の Commercial Installer または Paessler 社の web サイトより最新の The Commercial Installer をダウンロード、インストールしてください。

**Step 2: Server Admin Tool にライセンスキーを登録してください。**

サーバー管理プログラムにライセンスキーを入力してください。PRTG Server Administrator を起動させるには、次のアイコンをダブルクリックします。



“License” タブを選択し、ライセンスキーを入力してください。入力ミスを防ぐために、ライセンス名とライセンスキーは、弊社より送付したライセンスファイルよりコピー & ペーストしてください。



正しくキーが入力されたか確認するために、"Check Key(s)"をクリックしてください。間違いがなければ、"Licensed Edition"の欄に、正しいキーが表示されます。

### Netflow/xFlowライセンスキーの入力

NetFlowのキーはコード(70個の数字と文字)のみで構成され、ユーザーの企業名にあてはまるものではありません。NetFlowライセンスキーを購入した場合、Server Administrator toolも起動してライセンスキーを入力する必要があります。"License"タブを選択し、"Additional NetFlow Licenses"ボックスにキーをペーストしてください。正しくキーが入力されたか確認するために、"Check Key(s)"をクリックしてください。

## 2.5 Installation of a PRTG Remote Probe (PRTG リモートプローブの設定)

PRTGは監視を実行する2つのモジュールで構成されています。

コアサーバー： データストレージやwebサーバーなどの管理を行う。

プローブ: 1つまたは複数で実際の監視を行う。  
詳しくは、14.2 複数プローブとリモートプローブをご参照下さい。

## 2.6 Uninstallation(アンインストール)

PRTG をアンインストールするには、

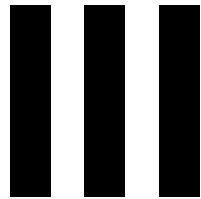
- コンピュータのコントロールパネルより”プログラムの追加と削除”を選択
- プログラムリストから PRTG Network Monitor を選択
- 削除ボタンをクリックして、プログラムをアンインストールする

または、スタート|全てのプログラムメニューの PRTG Network Monitor グループより、"Uninstall PRTG Network Monitor" アイコンを選択してください。

注意:アンインストール作業中、監視データは自動的に削除されません。

ソフトウェアのアンインストール処理完了後、PRTG Network Monitor インストールフォルダをチェックし、保存する必要のない全てのファイル(データベースなど)を削除して下さい。また、¥Documents and Settings¥All Users¥Application Data¥Paessler¥PRTG Network Monitor¥V7 フォルダ(Windows XP の場合)にデータファイルは自動的に削除されないデータファイルが残っているので確認してください。

# Part



## Introduction (概要)

### 3 Introduction (概要)

今日、ビジネスのほとんどは、インターネットや内部経営、電話や E メールのために、コンピュータおよびネットワーク基盤に依存しています。

複合的に設置されたサーバーやネットワーク機器に求められるのは、顧客、オフィス、従業員間におけるスムーズなビジネスデータ送信を確実にすることです。ビジネスの経済的な成功は、データフローに関連しています。

#### ネットワーク監視が重要な理由

ビジネスの成功には、コンピュータネットワークの信頼性、速度、効率性が不可欠です。しかし、他の機器同様、ネットワークデバイスは時折、障害が起こる可能性があります。これらの障害は、潜在的にトラブル、または営業上の損失を引き起こす恐れがあります。これらは、事前のどのような軽減策をもってしても防ぐことはできません。

その為、ネットワーク管理者は以下の3つのキー・ステップにより、ネットワークの稼働、信頼性、スピードを確保しなければなりません。

1. 信頼性の高いコンポーネントによる、計画性の高いネットワークの設定
2. デバイスの障害時における復旧計画の作成
3. 実際におこる障害について知るために、ネットワークを監視

本マニュアルで解説するソフトウェア、PRTG Network Monitor は、小、中、大規模ネットワークを監視する他に類のないソリューションです。

#### PRTG Network Monitor によるネットワーク監視

PRTG Network Monitor は Windows ベースのアプリケーションに対応した高性能なネットワーク監視ソフトウェアです。小規模～大規模ネットワークに適応し、LAN, WAN, 無線 LAN, VPN の監視が可能です。

本製品はネットワーク可用性や帯域使用状況だけでなく、メモリや CPU 使用状況などの様々なネットワークパラメータを監視します。リアルタイムな解釈や、定期的な使用状況をシステム管理者に提供し、専用回線、ルーター、ファイアーウォール、サーバー、その他のネットワークコンポーネントの効率性、レイアウト、設定を最適化します。

このソフトウェアは設定と使用が容易で、SNMP, WMI, パケットスニффイング、Cisco NetFlow のみならず多くの業界標準プロトコルを用いて、ネットワークの監視を行います。ネットワークの Windows マシンで毎日 24 時間連続して実行され、ネットワーク使用パラメータやネットワークシステムの可用性を記録します。記録データは、内蔵データベースに保存され、後で参照できます。

### 3.1 Key Features (基本機能)

PRTG Network Monitor の機能は以下の通りです。

- サーバーのアップタイム/ダウンタイムやスローダウンの監視とアラート
- 帯域やネットワークデバイス使用状況の監視
- システム使用状況の監視 (CPU 負荷、空きメモリー、空きディスク容量)
- 発信元、宛先、コンテンツによるネットワークトラフィックの分類
- ユーザーまたはデバイスの異常、不審、悪質な行為の検出
- SLA (サービスレベル・アグリーメント / サービス品質保証契約) の管理
- ネットワークデバイスの検出と評価

PRTG インストーラーにはシステム監視を実行するのに必要な、下記のソフトウェアとモジュールが全て含まれています。第三者モジュールは必要ありません。

- 未加工の監視結果を保存する Paessler 社独自の高速、効率的なデータベースシステム
- ユーザーインターフェースに HTTP/HTTPS 対応の内蔵 web サーバー
- 自動 E-Mail 送信機能のメールサーバー
- 監視イベントの保存用 SQLite, SQL サーバー
- PDF レポート作成用レポートジェネレーター
- ユーザーが使いやすいチャート作成用のグラフィックエンジン
- デバイス及びセンサーの自動検出の為にネットワーク分析モジュール

PRTG Network Monitor は数千のセンサーをサポートします。また、任意で、複数のリモートブローブ (エージェント) により、複数のサイトやネットワーク・セグメントを 1 箇所から監視することも可能です。このソフトウェアは Paessler 社が開発した監視テクノロジーに基づきます。このテクノロジーは 1997 年より絶えず改良され、既に毎日、世界中の 150,000 人以上のユーザーに使用されています。

フリーウェア版 (10 センサー以下) から数千センサー対応の商用レベルまでの魅力的なライセンスパッケージで、各ユーザーに最適な解決策をご提供致します。

### 3.2 Available Licenses (ライセンスの種類)

以下 3 種類のライセンスがあります。

#### フリーウェア版/スターター・エディション

フリーウェア版は PRTG を初めて使用する場合や個人使用に適しています。

- 無償で個人または商業用として使用可能
- 10 センサーまで監視可能 (スターター・エディション: 20 センサーまで)
- (NetFlow 以外) 全てのセンサーに対応

- 最短で 1 分間隔の監視可能

インストール後、ライセンスキーを入力しない場合、フリーウェア版として実行します、

### トライアル版

商用ライセンス購入をお考えのユーザーのための評価目的ライセンスです。

- 500 センサーまで監視可能
- (NetFlow も含めて) 全てのセンサーをサポート
- 最短で 1 秒間隔の監視可能

弊社 Web ページよりトライアル版ライセンスキーをお申し込み下さい。  
試用期限は 30 日です (期限後はフリーウェア版に戻ります)

### 商用版

商用版 PRTG Network Monitor には数種類のライセンスがあります。小規模だけでなく、大規模ユーザーまで、ご要望に応じて対応できます。

- 最大センサー数はライセンスによって異なります (100 以上)
- (NetFlow も含めて) 全てのセンサーをサポート
- 最短で 1 秒間隔の監視可能

価格、機能、ライセンスのご注文等のお問合せはジュピターテクノロジー(株)へお願いいたします。

## 3.3 About This Document (本マニュアルについて)

本マニュアルで紹介するのは PRTG Network Monitor のシステムの設計概念です。最良の結果を引き出せるように本製品の設定方法を解説します。監視設定計画及び、センサー、レポート、マップ、ユーザーアカウントの設定を学べます。

本マニュアルは、ユーザーインターフェースの個々の項目やボタンについて全て説明しているわけではありません。それら詳細は、PRTG の Web インターフェイスで簡単なコンテキストヘルプやヒントとして確認いただけます。同様に本マニュアルはファイル形式、API、その他バックグラウンド情報について、技術的に踏み込んだ説明はしていません。

上記の情報はオンライン上の Paessler ナレッジベースをご参照下さい。

<http://www.paessler.com>

# Part

# IV

## Basic Concepts of PRTG Network Monitor (PRTG Network Monitorの基本概念)

## 4 Basic Concepts of PRTG Network Monitor ( PRTG Network Monitor の基本概念 )

PRTG Network Monitor の機能性と使いやすさを認識していただくための基本概念をいくつか紹介します。本章を注意深く読んでいただければ、本ソフトウェアのすばらしさをご理解いただけると思います。

- アーキテクチャ: PRTG コアサーバー、PRTG プロブ
- オブジェクト階層: プロブ、グループ、デバイス、センサー、チャンネル
- 設定の継承
- 通知、スケジュール、依存関係
- レポート、マップ、ToDo
- 優先順位とよく使うセンサー
- デフォルト値

### 4.1 Architecture: PRTG Core Server and PRTG Probe(アーキテクチャ: PRTG コアサーバー、PRTG プロブ)

PRTG Network Monitor は主に 2 つのパートで構成されています。

- PRTG コアサーバー: "Core Server" は PRTG の中核部分です。コアサーバーにはデータストレージ、web サーバー、レポートエンジン、通知システムが含まれています。
- PRTG プロブ: "probe" が実際の監視を行います。コアサーバーからの設定を受けて、監視プロセスを実行、監視結果をコアサーバーへ返します。コアサーバーは常時ローカルプロブを同一サーバー内に走らせます。加えて、コアサーバーは、リモートプロブの管理も無制限に行い、複数個所のモニタリングを実行することができます。

これら 2 つは Windows サービスです。このサービスは、ユーザーのログインなしで、Windows 動作中は常時バックグラウンドで動作します。

また、"PRTG Server Administrator" と "PRTG Probe Administrator" の 2 種類の管理ツールがあります。管理者ログインや web サーバーの IP アドレス等の基本設定を行うのに利用します。

#### コアサーバー

コアサーバーは PRTG システムの中心であり、以下の処理を行います。

- オブジェクト監視の設定管理
- 接続したプロブの設定と管理
- 未加工の監視結果を保存
- 送信用メールサーバを含めた通知管理

- レポートジェネレーターとスケジューラー
- ユーザーアカウント管理
- データ消去(例:365 日経過後のデータを削除)

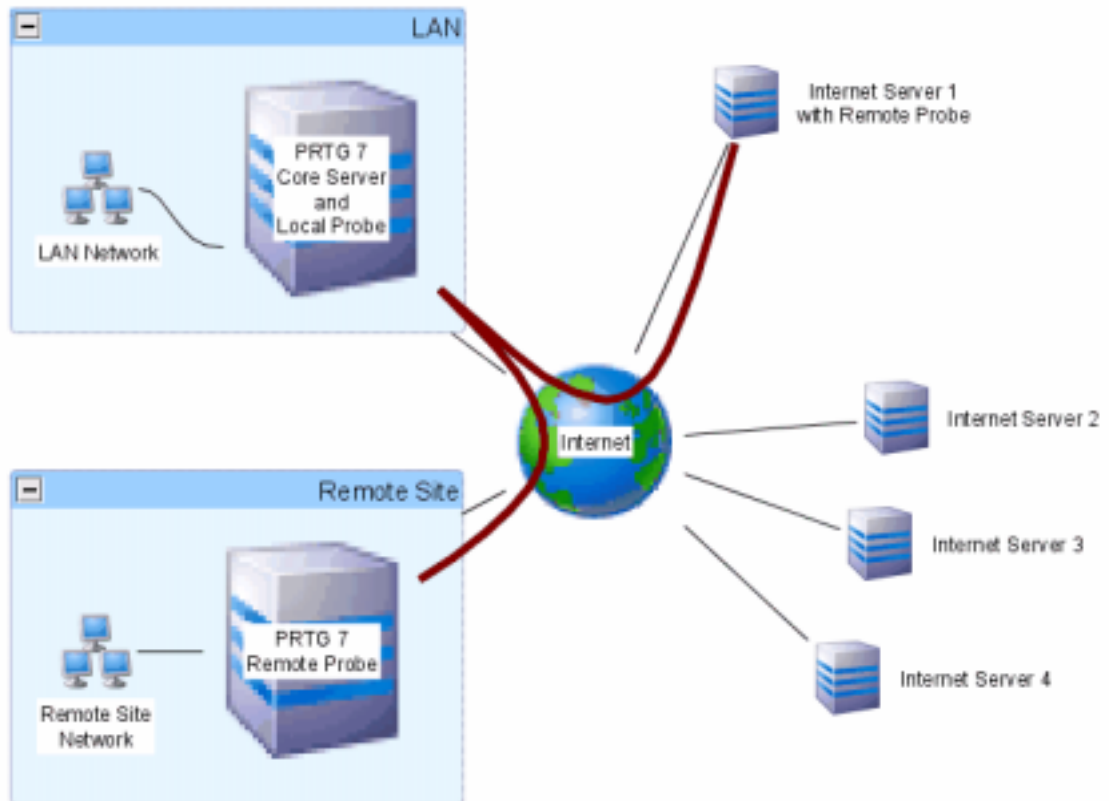
コアサーバーは、高速で安全な内蔵 Web サーバー機能を含んでいます。(IIS や Apache 不要)。この Web サーバーは HTTP や(SSL 経由する)安全な HTTPS 対応です。 Ajax ベースのインターフェースで、デバイスやセンサーの設定や監視結果の確認ができるようになっています。この web インターフェースは高度な対話型となっていて、Ajax を採用することで、ユーザーにとって、より強力で使いやすいものになっています。ユーザーがログイン中、画面のデータは(Ajax 経由の通信で)常に更新されます。その為、現時点の監視結果が常時表示されます(更新間隔と方法はユーザーによる設定が可能です)。すべての監視結果の統計 エラー、警告、ダウン、一時停止、またはステータスが異常なセンサーの数や、全てのセンサーについてのアラームや、帯域使用状況、CPU 使用状況と速度指数の最近の履歴を表すグラフが、常時ページ上部に表示されます。

## プローブ

実際の監視を実行するのは 1 台、または複数のコンピューター上で作動する PRTG プローブプロセスです。インストール中に、いわゆる"Local Probe"(ローカルプローブ)がシステムにより自動的に生成されます。シングルプローブ設定(デフォルト設定)では、全ての監視はローカルプローブで実行されます。

リモートプローブの追加は、ユーザー側で行います。リモートプローブは、SSLでコアサーバーと接続し、非公開のネットワークや、ファイアウォールが設置された遠隔地のネットワーク内で安全にサービスとシステムを監視します。以下の図は、LAN(図左上)内部でのPRTGコアサーバーの機能の例です。

- ローカルプローブを使って、“LAN”内の保護されたサービスを監視。
- 専用のプローブサーバー上のリモートプローブを使って、“Remoto Site(図左下)”内の保護されたサービスを監視。
- リモートプローブを直接設定した"Internet Server 1"上での保護されたサービスを監視。
- 任意のプローブを使ってインターネット経由で“"Internet Servers1/2/3”の公開されたサービスを監視。



リモートプローブについての詳しい情報は、[14.2 複数プローブとリモートプローブ](#)をご参照ください。

コアシステムからの設定を受けると、例えば、接続障害によってプローブ-コアサーバー間の接続がきれた場合などに備えて、どのプローブも、接続コアサーバーとは独立して一定時間動作することができるようになっています。接続できなくなっている間、バッファで、最大500,000センサーの結果をリモートプローブシステムのRAM(50-200MBまで)に保存します。つまり、100センサーにつき1分間隔で、最大3日分の監視結果をバッファリングすることができます(10,000センサーなら、1分間隔で52分間隔)。プローブは復旧後直ちに、自動でコアサーバーと再接続し、接続できなかった間の全ての監視結果を転送します。

PRTG は自動的にコアサーバーと個々のプローブの"system health" (システムの健全性)を監視します。それによって、過重負荷の状況を検出し、正しい監視結果が得られるようにします。そうすることで、システムは多数のセンサーを自動的に生成し、各プローブはシステムのステータスを監視することができるようになります。

#### Local probe (127.0.0.1)

Probe Device	Probe Health	CPU Load	Memory Free	Disk Free
	100 %	2 %	27 %	38 %
Ethernetadapt	81 kbit/s	MS TCP Loopb	5 kbit/s	

上記のセンサー設定を使用することをお勧めしますが、"Probe Health"センサー以外の全セ

ンサーを削除する事もできます。 "Probe Health" センサーはプローブで最も重要なセンサーです。 このセンサーは、プローブシステムのハードウェアやプローブの内部プロセスにおける多数の内部システムのパラメータを測定し、結果の値を算出します。 100%未満の値が頻繁にでる場合は、検査する必要がありますので、センサーチャンネルをよく確認してください。

## 4.2 Object Hierarchy: Probes, Groups, Devices, Sensors, Channels (オブジェクト階層: プローブ、グループ、デバイス、センサー、チャンネル)

PRTG Network Monitor における実際の監視は"sensors"が実行します。 個々のセンサーはネットワークデバイスの一つのアスペクトを監視します。 例えば、

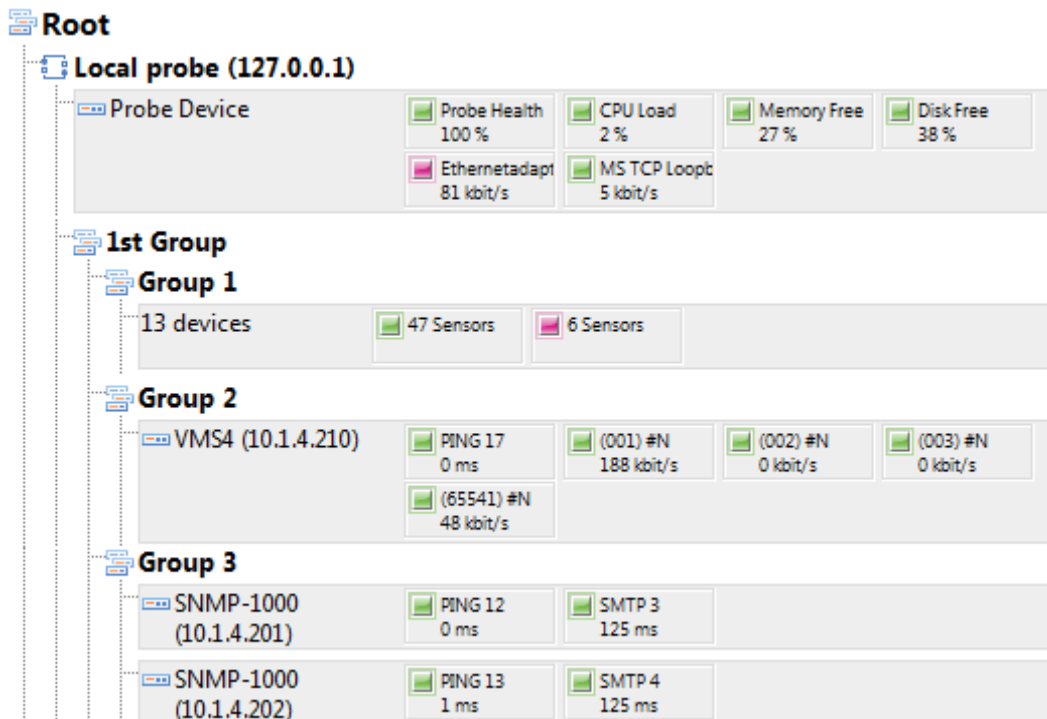
- SMTP, FTP, HTTP 等の 1 ネットワークサービス
- 1 ネットワークスイッチ或いは、1 ポートにおけるトラフィック
- 1 デバイスの CPU またはメモリ負荷
- 1 ネットワークカードのトラフィック
- 1 NetFlow デバイス など

センサーはツリー状の階層状に形成されます。 これにより、操作しやすいナビゲートリストを生成し、ユーザーは、センサーを、類似するデバイス、ロケーション、サービスを監視するグループに分けることができます。

ユーザーはネスト状の"groups" (グループ) を生成できます。 各グループには多数の"devices" (デバイス)、各デバイスには多数の"sensors" (センサー)、最後に各センサーには単一または複数の"channels" (チャンネル)、を含みます。 (例えば、入出力チャンネル、マルチプロセッサシステム上の各 CPU の 1 チャンネルなど)

階層内の"Probes" (プローブ) レベルを見ることが出来ます。 任意のプローブの下に設定された全てのグループ/デバイス/センサーはプローブを経由して監視されています。 (14.2 複数プローブとリモートプローブ参照)

設定サンプルは以下の通りです。



### 4.3 Inheritance of Settings (設定の継承)

階層はセンサーをグルーピングするだけでなく、"Inheritance" (継承) と呼ぶ重要な一面もあります。迅速、かつ容易な管理のために、- 特に大規模な監視設定のために 上位階層の設定を"継承"します。例えば、最上位の"ルート"グループの間隔設定を変更するだけで、全センサーの監視間隔を変更できます。

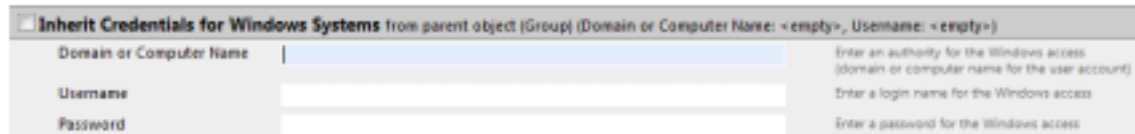
ある特定のグループ/デバイス/センサーに対して異なる値を設定することで、どのレベルの階層においてもこの値が優先されます。つまり、すぐ上のレベルからの設定ではなく、設定を再定義したオブジェクトの支配下にある全てのオブジェクトにおいて、その設定が継承されます。

全オブジェクト間で引継ぎされる設定は以下の通りです。

- 監視間隔
- 通知/トリガー
- Windows 認証設定(WMI センサーなど)
- ESX サーバー認証設定 (VMware サーバ)
- SNMP 認証設定と互換設定
- チャンネル・ユニット設定
- ユーザーアクセス権
- 一時停止ステータス:あるオブジェクトが、ユーザーやスケジュール、ディペンデンシー(依存性)により、オブジェクトが一時停止すると、同様に全センサーも一時停止します。

デバイスとセンサーに対して、一つだけ例外があります。デバイスの IP アドレス(或いは、DNS 名)、SNMP と WMI 設定は常にセンサーが継承します。これらはセンサーレベルで変更できません。

オブジェクト設定ページのラジオボタン”Specify settings for this(object)”を選択する事で、親設定の再定義ができます。以下のスクリーンショットは、Windows 認証設定画面です。



#### 4.4 Notifications, Schedules, and Dependencies (通知、スケジュール、ディペンデンシー (依存性))

PRTG が提供する下記 3 つのコンセプトで、監視構成の設定が行えます。

##### 通知

PRTG がダウンタイム、システム過負荷、閾値超過など、類似の状況を検出すると、"notification" (通知) が送信されます。E-Mail、SMS、ポケベルメッセージなど、さまざまな方法で通知することができます。システム設定で通知生成後、グループ/デバイス/センサー設定ページで、通知方法を選択できます。詳細は **Part VIII 通知** をご参照下さい。

##### スケジュール

グループ、デバイス、センサー監視はユーザーの介入、または "schedule" (例: 日曜日午前 4 時~8 時は監視しない、等) で一時停止できます。スケジュールを利用することで、監視時間を制限することができます。PRTG には多数の標準設定スケジュールがありますが変更可能です。また独自スケジュールも追加できます。

##### ディペンデンシー (依存性)

"dependencies" (ディペンデンシー: 依存性) を利用して、他センサーのステータスに基づきセンサー監視を一時停止できます。これは誤った警告や不正確なダウンタイム記録を避ける為です。ある特定のセンサーがダウンまたは一時停止すると、ディペンデンシー (依存性) は一つ、または一連のセンサーの監視を停止します。(例: 付随するファイアウォールが接続トラブルによりダウンした場合、リモートネットワークサービスの監視停止)

ディペンデンシー (依存性) には 3 つのオプションがあります。

- " Use Parent": デフォルトでは、全てのオブジェクトはペアレント(親)オブジェクトに依存します。ユーザーがグループに依存性を指定し、依存センサーがダウンまたは一時停止すると、グループ内の全センサーが一時停止します。

- ” Select Object”：ディペンデンスを設定するには、あるオブジェクトに「依存」させるオブジェクトの設定ページへ進んでください。リストから、依存させるオブジェクトを選択してください。



リスト内より選択したオブジェクトが”赤”(ダウン)または一時停止すると、依存オブジェクト(および全ての子オブジェクト)に対する監視が一時停止しますが通知は送信されません。

- ” Master Object”：この設定でセンサーは親デバイスに対してマスターオブジェクトと呼ばれます。親デバイスの全センサーはマスターセンサーがダウンすると一時停止します。基本センサー(例:PING)をマスターセンサーに設定する事を推奨します。(例えば、オートディスクバリーは各デバイスに対し PING センサーをマスターオブジェクトにします。)

## 4.5 Reports, Maps, and Todos(レポート、マップ、Todos)

### レポート

"Reports"(レポート)は監視データを分析するのに使用されます。この機能は一度または指定した間隔で利用できます。レポートの数を任意で定義したり、レポートする対象のセンサーを特定したり、テンプレートを選択し、任意の間隔で実行(例:一回、毎日、毎週、毎月)できます。

詳しくは、Part X レポートをご参照ください。

### マップ

"Maps"(マップ)を使用すると、監視しているネットワークについて独自の概要とダッシュボードを作成することができます。マップにネットワーク図などの背景画像を取り込むことができます。また、ステータス・アイコンやセンサーリストを配置できます。同様にマップ上に現在の監視ステータスのグラフも配置可能です。

任意の数のマップを定義することが可能で、NOC ダッシュボード、イントラネットにおけるネットワーク・ステータスの概要、最重要センサーのグラフの web ページ、等の作成などに使用することができます。公開マップ機能を使えば、他ユーザーに対してマップの URL を提供できます。これにより、ユーザーアカウント無しでデータを閲覧できます。

詳しくは、Part IX マップをご参照ください。

## Todos

管理者が注意する必要があるイベントや監視オブジェクトを PRTG が検出すると、"ToDo list" (ToDo リスト) に追記し、管理ユーザー宛に E メールを送信します。

Todos が生成されるのは、次のような場合です。

- Autodiscovery 処理で新規デバイスやセンサーが生成され、ユーザーに知らせる必要があるとき
- 新しい PRTG プロブがコアに接続され、ユーザーに知らせる必要があるとき
- 新しいバージョンのソフトウェアが利用可能になった場合
- 新しいレポートが閲覧可能になったとき
- その他の状況 (ディスク・スペース不足、ライセンスに関する問題など)

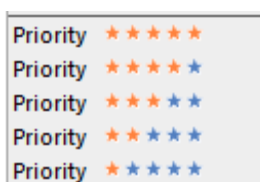
詳しくは、Part XI Todos を参照してください。

## 4.6 Priorities and Favorite Sensors (優先順位とお気に入りセンサー)

### 優先順位

ユーザーはセンサーツリー内の各オブジェクトの優先順位を指定できます。星 1 つ ("\*") / 重要性低 から、星 5 つ ("\*\*\*\*\*") / 最重要 まで表示されます。PRTG センサーはデフォルトで最初に優先度でソートされ、その後は "Alarm" や "Sensor" といったリスト内名称のアルファベット順でソートされます。

デフォルト優先度は星 3 つです。設定内で素早くオブジェクトを優先順位付けできます。オブジェクトを右クリックし、コンテキストメニューより希望の設定を選択します。



優先順位コンセプトの基本的な考え方は、確実に、最も重要なセンサーを最初にセンサー / アラームリストに常時表示させるということです。これによって、確実に重要な動作停止を見逃しません。

## Favorite (お気に入り) センサー

重要なセンサーを目立たせる別の方法として、"favorite" (お気に入り) センサーとして目印をつける方法があります。センサーのコンテキストメニューからアクセス可能です。お気に入りセンサーのリストはダッシュボードページ ("Home/Dashboard") やセンサーメニュー ("Sensor/Favorite") にあります。

## 4.7 Default Values (デフォルト値)

PRTG では、多くの設定に、デフォルト値が設定されています。これによりすぐにソフトウェアを利用することが可能です。

例えば、"Root Group" (ルートグループ) から全センサーに、以下の設定が継承されています。

- デフォルト監視間隔は 1 分
- 「公開」コミュニティ名をもった SNMP v1 (多くのデバイスのデフォルト値)
- 各種 SNMP 互換性オプション
- 各種チャンネルユニット設定
- スケジュール、依存性、Windows 認証アカウントの設定なし

さらに、以下のデフォルト値は自動的に設定されています。

- 非管理者ユーザーとして使用する 1 ユーザーグループ (PRTG ユーザー)
- 1 通知 (システム管理者宛の E-Mail)
- 各種 web インターフェース設定 (リフレッシュ、自動フォルダ、他)
- 1 組のスケジュール設定
- 各種データ削除設定

ユーザーインターフェースをより使いやすくする為、多数の上記デフォルト値を変更する必要があるかもしれません。しかし、はじめのうちは、上記の設定で、多くの状況に対応できるはずです。

# Part

# V

## User Interfaces (ユーザーインターフェイス)

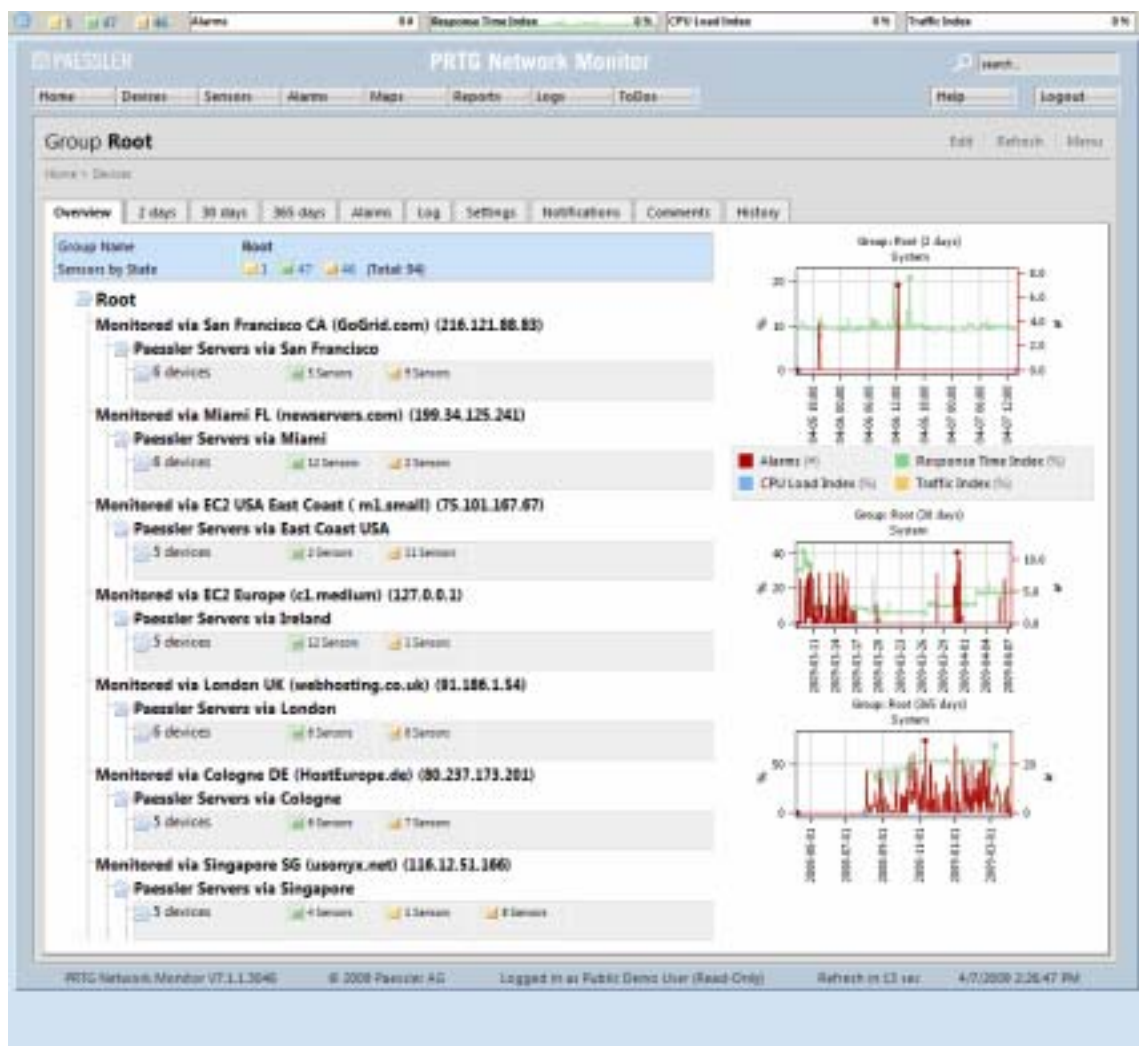
## 5 User Interfaces (ユーザーインターフェース)

PRTG Network Monitorには、3種類のインターフェースがあります。

### webベースのユーザーインターフェース

メインのインターフェースは、ソフトウェア、センサーの設定、現在のステータスの確認、リモート作成の際に利用する、ブラウザベースのインターフェースです。

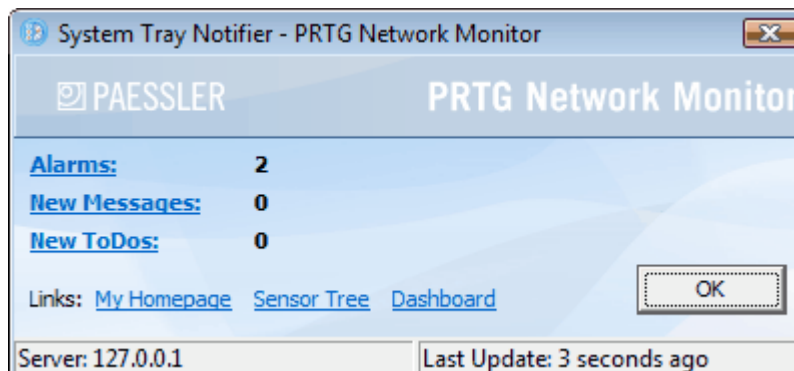
画面は、以下の通りです。



詳細は、5.1 webインターフェースナビゲーションを参照してください。

### Windowsツール

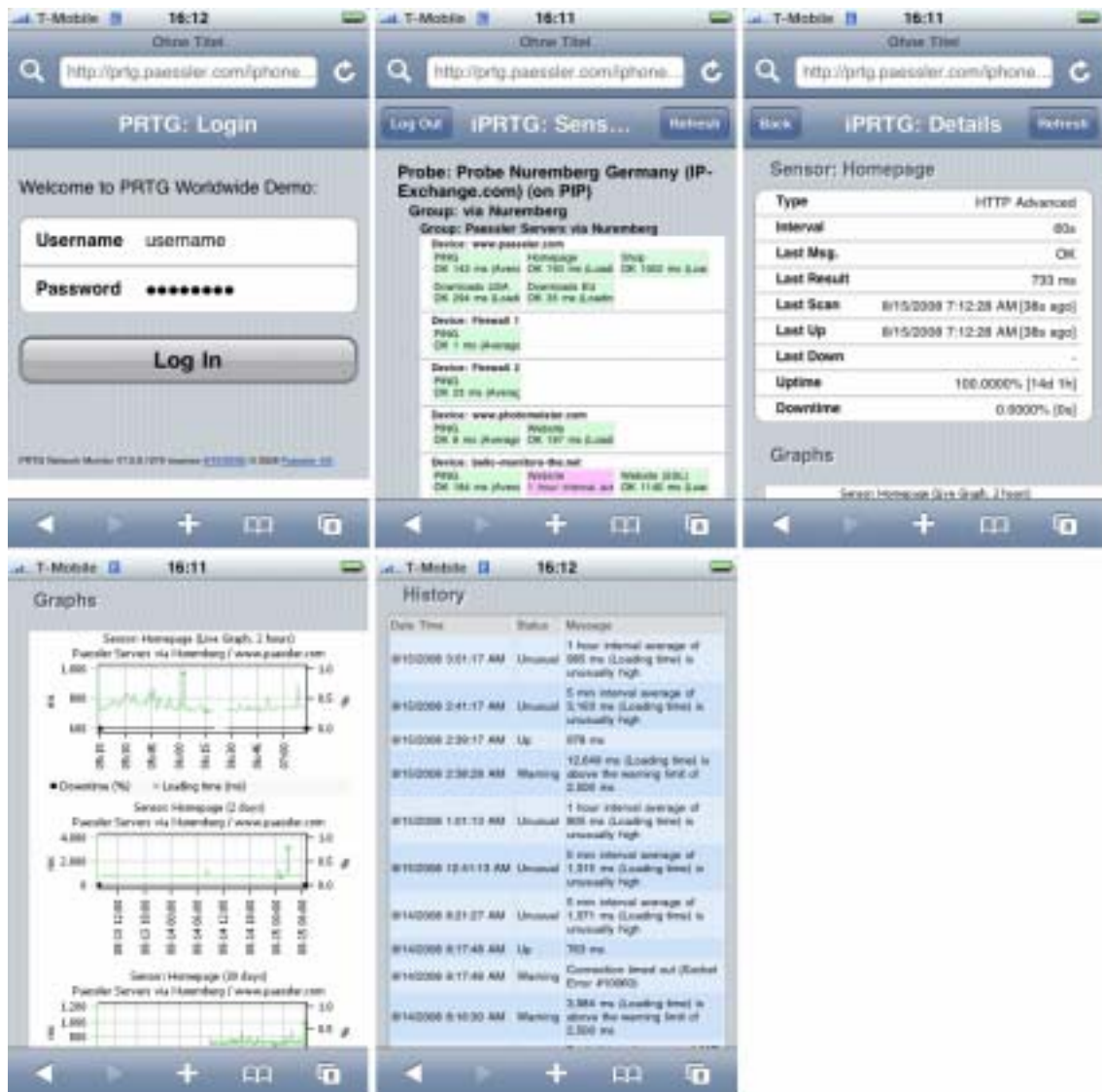
システムトレイ通知が、ユーザのPC上のバックグラウンドで起動しています。PRTGがネットワーク上の変化を検出すると、ポップアップと警告音でユーザーに通知します。



詳細は、**5.6 システムトレイ通知**を参照してください。

### iPhoneインターフェース

iPhoneをお持ちの場合は、専用に最適化されたユーザーインターフェースにアクセスすることができます。



詳細は、5.7 iPhoneユーザーインターフェースをご参照ください。

## 5.1 Web Interface Navigation (web インターフェースナビゲーション)

PRTGwebインターフェース画面は、以下のようになっています。



主なレイアウトは、トップにステータスバー、その下にメインメニューやクイック検索ボックスを配置したヘッダーエリア、そしてメインページコンテンツ(これらについては、次のセクションで説明します)で構成されています。

PRTGwebインターフェースを利用する場合、以下の5つの操作のうちのいずれかを使うことになります。

- "Main Menu" (メインメニュー): ソフトウェアの重要事項へのアクセスが可能です。
- "Quick Search" (クイック検索): オブジェクトをすばやく検索できます。
- "Tabs" (タブ): オブジェクトに関するさまざまなサブページに切り替え可能です。
- "Context Menu" (コンテキストメニュー): オブジェクトを右クリックすると、ポップアップで現れます。
- オブジェクトをクリックすると、オブジェクトツリーの状態で、プローブ/グループ/デバイス/センサー等のオブジェクト階層を表示することができます。

上記5つによって、PRTGのあらゆる機能をすぐに利用することができます。webベースのユーザーインターフェースでは珍しいコンテキストメニューを除いて、これらの機能については、既にその他多くのwebサイトやwebベースのユーザーインターフェースで、よく見られるものです。

しかし、すぐに、インターフェースを効果的に利用するにあたって、PRTGのコンテキストメニューがいかに強力な機能を持つか、ご理解いただけると幸いです。

詳細は、以下をご参照ください。

- 5.2 webページ概要
- 5.3 コンテキストメニュー
- 5.4 リスト
- 5.5 webインターフェース上でのステータス情報の監視

## 5.2 Web Page Overview (web ページ概要)

PRTGのwebページの構成を詳しく見てみましょう。

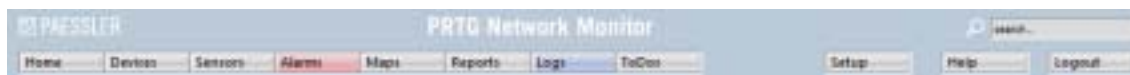
### グローバルステータスバー



このバーは全てのページ上部に常時表示されます。ユーザーが監視するよう設定した全てのセンサーのステータスをまとめて表示します。センサーのステータスによって、数字と色付の正方形が現れます。(上の図では、23 センサーがエラー(赤)、3 センサーが警告(黄)、95 センサーは OK(緑)、129 センサーが一時停止(青)、40 センサーが"UNUSUAL"(異状)ステータス(橙)です。)

4つのグラフが表示するのは、過去24時間の全センサーに対する、アラーム数と帯域使用状況、リクエストタイム、CPU使用状況の3つの"Index Graphs"(指数グラフ)です。これらのグラフは、株価指数のような"index"(指数)のグラフです。これらの値は、全てのセンサー/あるグループ/あるデバイスなどの数値に基づいて、統計的計算を用いたり、過去の最高値と最低値と比較したりして、算出されています。例えば、CPU負荷指数が90%の場合、現在の設定している全てのCPUセンサーへの平均CPU負荷は、過去に計測されたCPU使用値の最高値の90%であるということを意味します。

### webサイトヘッダーエリア、検索ボックス、メインメニュー



webインターフェース内の移動には、メインメニューを使います。全てのメニュー項目やサブ項目へすぐ移動することができます。

"Alarms"は、警告があった場合に、赤色になります。"Logs"と"ToDos"は、新しいメッセージや新しい登録項目があった場合に青色になります。

監視オブジェクトを検索するには、ページ右側の検索ボックスに、名称、名称の一部、IPアドレス、DNS名、またはタグを入力して、エンターキーを押して下さい。検索語に合致した全ア

## 37 PRTG Network Monitor 7.1 - ユーザーマニュアル

アイテムが web ページに反映されます。オンライン上のヘルプ項目も表示されます。

### ページヘッダーとタブ



各ページのコンテンツは、ヘッダーエリアの下に表示されています。ページのコンテンツによって、右側にメニューとアクションリンクが確認できます。ページ上部にある "Breadcrumbs" (ブレッドクラム機能) で、ホームからのルートを常に表示しています。

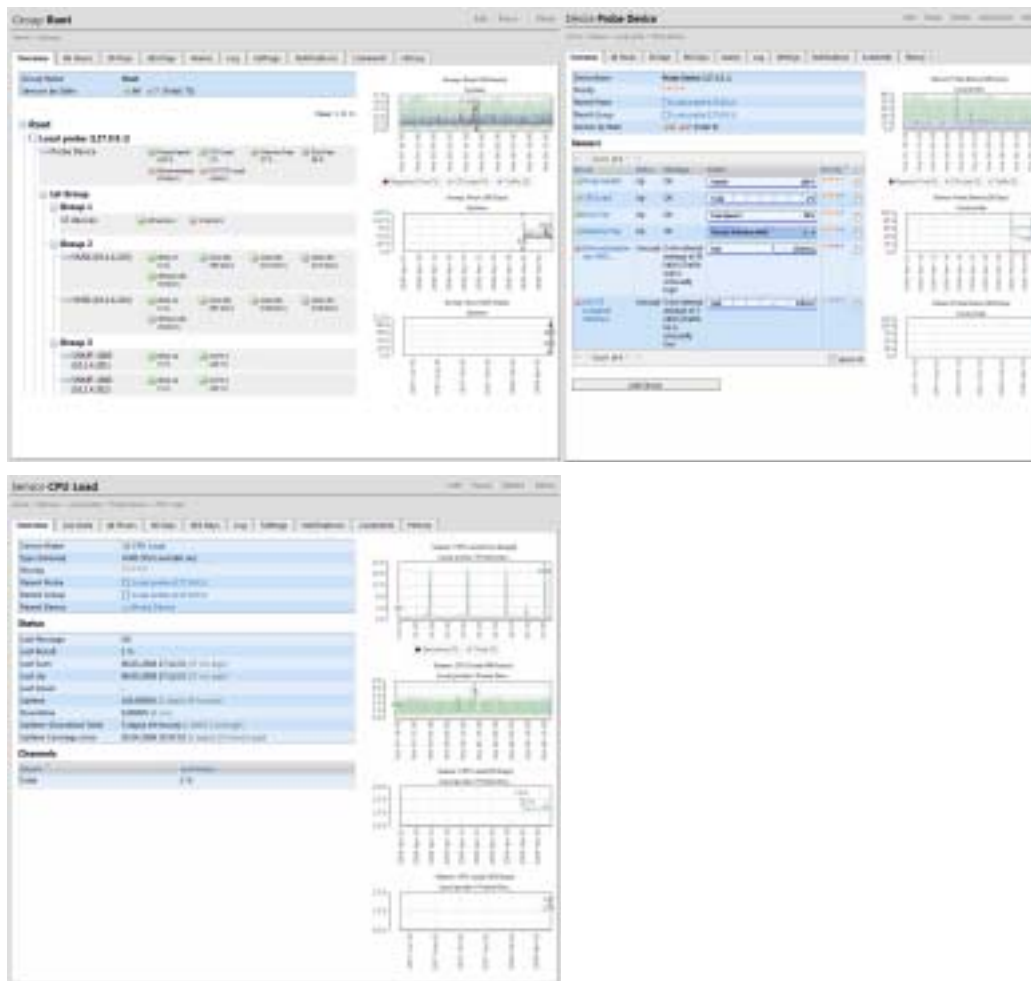
多くのページは、タブ状のインターフェースになっています。これらのタブを使いながら、オブジェクトに関するさまざまなサブページへ移動します。

Overview タブ	全ての監視オブジェクトの全パラメータとステータスをすばやく確認できます。
Livedata/48Hours/30days/365Days タブ	グループ/デバイス/センサーの過去データのグラフや表を表示します。(注:Livedataは、センサーにのみ適用)
Alarms/Log タブ	オブジェクトやその子オブジェクトの現在のアラームやイベント履歴を表示します。
Settings/Notifications タブ	オブジェクトの設定や通知を変更できます。
Comments タブ	ユーザー独自のコメントをノートパッドで作成。
History タブ	各オブジェクトのログ履歴を表示します(作成者、変更者など)

注意:他のオブジェクトに関するその他のタブについてもご確認ください。

### グループ、デバイス、センサーの概要ページ

次の3つの画面をご覧ください。グループ、デバイス、センサーの "Overview" 概要タブを表示しています。



3つは、共通したレイアウトになっています。

- 左上にオブジェクト名、基本設定、センサーのステータス
- その下に、子オブジェクトのリスト(グループに対するデバイス、デバイスに対するセンサー、センサーに対するチャンネル)
- 右側に3~4種類のグラフを配置し、最近のデータを表示しています。グラフを拡大するには、グラフをクリックしてください(または、該当タブを選択)。

センサーについては、4種類のグラフがあり、過去48時間、30日、365日、現在のグラフで、そのセンサーについてのすべての"channels"(チャンネル)が表示されます。グループとデバイスに対しては、3種類のグラフがあり、過去48時間、30日、365日の警告、CPU負荷指数、トラフィック指数、応答時間指数(上述)が表示されます。

### CPU指数、トラフィック指数、応答時間指数の算出方法

全ネットワーク(或いは、その一部分)のステータスをすばやくグラフ表示するために、PRTGは、全てのセンサーの測定値に基づいた、いわゆる"index"(指数)値を算出しています。"index"グラフは、現在のセンサーの測定値と過去の最高値を総合した、0%~100%までの値になっています。これら指数値の算出は、主要銘柄の現在の株価を元に算出される株価指数の算

出と似ています。各グループやデバイスに対して、PRTGは、グラフで4つの値を表示します。それらは、グループ(或いはデバイス)の全てのセンサーの測定値を基にしています。“Alarms”(アラーム)グラフは、過去のあるタイミングでのアラームの数を単に表示します。指数には、次の3つあります-"Response Time Index"(応答時間指数)、“CPU Load Index”(CPU 負荷指数)、“Traffic Index”(トラフィック指数)です。

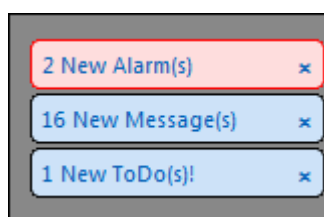
あるグループのCPU負荷指数が10%の場合、このグループの全てのCPUセンサーに対する現在のCPU平均負荷は、過去に測定されたそのグループのCPU負荷の最大値の10%であることを意味しています。応答時間については、平均値は、過去の最大値を下回ることがほとんどです。例えば、あるLANにおけるpingの応答時間は、最大値が数100ミリ秒でも異常ではなく、通常だと、2-10ミリ秒です。これは、ほとんどの応答時間指数は、通常10%~20%だからです。

それでは、指数とはどのような仕組みになっているのでしょうか。

- 通常のネットワーク監視プロセスの間、PRTGは各センサーについて最大測定値を記録します。
- 現在の測定値は、境界値と比較され、センサーについて0%~100%の指数を算出します。
- 各デバイスについて、CPU負荷センサー、トラフィックセンサー、応答時間を測定するセンサーについての指数が統合されます。
- 各グループについて、全てのデバイスの指数が統合されます。
- センサーの設定(センサーの数やタイプ)を変更すると、指数も当然変わってきます。それは、計算の基になる数字が変わってくるからです。つまり、設定前後の数字は比較できない可能性があります。例えば、プローブの接続障害などで、一部のセンサーを監視できなくなった場合などにも、同じことが言えます。

## アラートボックス

PRTG Network Monitorのwebインターフェースにログイン中、新しいイベントが起こった場合、常にアラートボックスが、ブラウザウィンドウの右下に表示されます。



これらは、PRTGがネットワークの変化を検出したり、その他の原因でユーザーの対応が必要な場合に表示される重要なメッセージですので、十分に確認してください。赤いバーの中のテキストをクリックするだけで、詳しい情報ページへ移動することができます。あるいは、“x”をクリックして、アラートを隠すこともできます。ユーザーアカウント設定で、どのイベントについてポップアップを起動させるか管理することができます。

### 5.3 Context Menus(コンテキストメニュー)

コンテキストメニューは web ベースのアプリケーションにおいては馴染のないものですが、PRTG のユーザーインターフェースを容易にお使い頂く為の要となります。ユーザーインターフェース内でリンクとして現れるオブジェクトは、ほぼ全て、右クリックするとコンテキストメニューが表示されます。

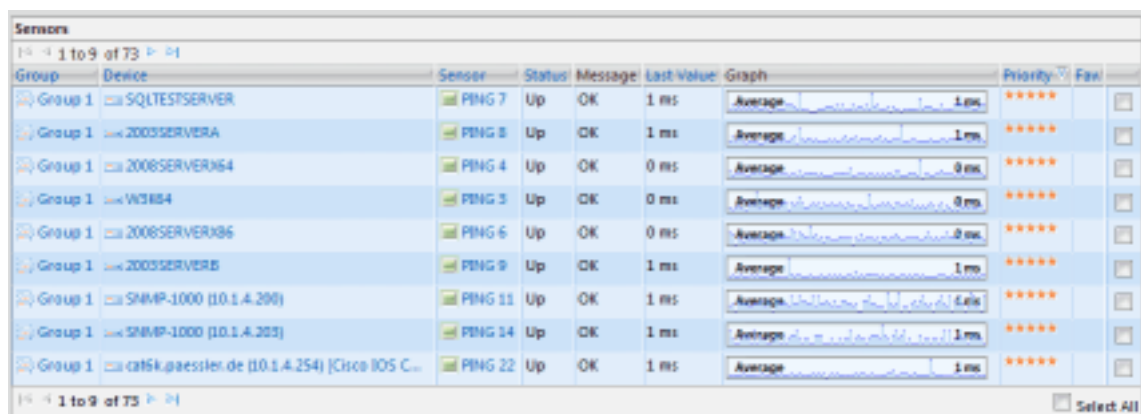
以下3つはグループ/デバイス/センサーのコンテキストメニューの例です。Windows 環境においては、どのコンテキストメニューも同様です。

Group Menu	Device Menu	Sensor Menu
Details...	Details...	Details...
Settings...	Settings...	Settings...
Add Group...	Add Sensor...	Create Report...
Add Auto-Discovery Group...	Run Auto-Discovery	Check Now
Add Device...	Create Device Template...	Delete...
Run Auto-Discovery	Create Report...	Clone...
Create Report...	Check Now	Pause
Check Now	Delete...	» Fold
Delete...	Clone...	» Move
Clone...	Pause	» Priority/Favorite
Pause	» Fold	» Historic Data
Fold	» Move	» Tools
Move	» Priority/Favorite	
Priority/Favorite	» Historic Data	
Historic Data	» Tools	

注意: ブラウザ独自のコンテキストメニューへアクセスするには、右クリック時に CTRL キーを押したままにしてください。

### 5.4 Lists(リスト)

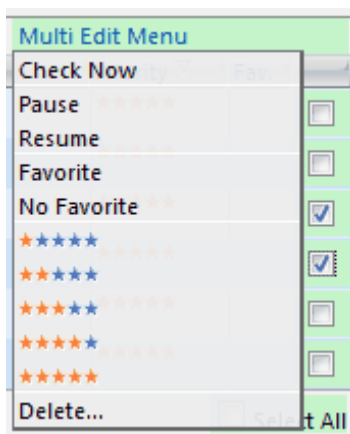
web インターフェースにおいて、共通機能を共有するアイテムリストが確認できます。以下2つの例はセンサーとログエントリーです。



Log Entries with Status =						
Date Time	Parent	Type	Object	Status	Message	Date Range Item Count
05.05.2008 17:37:53	None	Probe	<input type="checkbox"/> Local probe	Connected	Probe 'local probe' at 127.0.0.1:2902 has connected	
05.05.2008 17:22:28	None	Probe	<input type="checkbox"/> Local probe	Disconnected	Probe 'local probe' at 127.0.0.1:2902 has disconnected	
05.05.2008 12:24:36	None	Probe	<input type="checkbox"/> Local probe	Connected	Probe 'local probe' at 127.0.0.1:2902 has connected	
05.05.2008 12:23:42	None	Probe	<input type="checkbox"/> Local probe	Disconnected	Probe 'local probe' at 127.0.0.1:1187 has disconnected	
30.04.2008 20:55:00	None	Probe	<input type="checkbox"/> Local probe	Connected	Probe 'local probe' at 127.0.0.1:1187 has connected	

このリストにおいて、以下の機能を利用できます。

- ページ移動: ページ上/下にある小さい三角形アイコンを利用して、ページごとのリストへ移動できます。
- ソート: ソートインデックスとして使用したい列のタイトルをクリックしてリストの再ソートができます。
- 日付範囲: ログリスト閲覧時に”Date Range”をクリックすると、希望の日付範囲に変更します。
- アイテム数: ”Item Count”をクリックすると、リスト内のエントリー数を変更できるリストがあります。
- マルチ編集: チェックボックス列のあるリストがあります。1 つ以上のチェックボックスを選択すると即座に追加メニューが表示されます。チェックボックスが選択されたリスト内の全アイテムに適用される機能を表示します。以下、メニューの画面例です。



## 5.5 Monitoring Status Information Available Through the Web Interface (web インターフェースからの監視ステータス情報)

監視システムが稼動すると、PRTG は現在のステータスに関してさまざまな情報を提供します。

センサーのステータスは以下のステータスメッセージと色で表示されます。

- OK (緑): センサーが正常に稼働、計測値も異常なし。
- WARNING (警告・黄): センサーが遅い、または計測値がユーザー定義の警告閾値以上/以下。
- ERROR (エラー・赤): センサーが監視不能 (例; デバイスダウン)、または計測値がユーザー定義のエラー閾値以上/以下。
- PAUSED (一次停止・青): センサーが一時的に停止中。ユーザー、ディペンデンス (依存性)、スケジュールによる。
- UNUSUAL (異常・橙): センサーは正常に稼働しているが、最新の計測値が異常に高いまたは低い (PRTG は、センサーの履歴データと最新の計測結果を使った統計的計算を適用して、計算します)。
- UNKNOWN (不明・黒): センサーが確認されない。例) プログラム開始直後、または関連するプローブが使用不可。

Web インターフェースは、各センサーについてさらに詳しい情報も提供します。

- 4 種類のグラフ (ライブデータ、2 時間内、48 時間内、30 日以内、365 日以内)
- 4 種類のデータテーブル (各グラフに対して 1 つ)
- トップトーカー、トップ接続、トッププロトコルなどのトップリスト (パケットスニффイング / NetFlow センサーのみ)
- 現在のステータスとエラーメッセージ (ある場合)
- 各チャンネルに対する前回の計測値
- 稼働時間と非稼働時間の総計
- 前回のリクエストの結果
- カバー率 (タイムモニタリング情報のカバー率を % で表示)
- センサー編集履歴 (どのユーザーが、どの設定を変更したか)
- センサーアクティビティログ
- ユーザーコメント

現時点のセンサーとデバイスのステータスは各種方法で確認できます。

- "Sensor Tree" (センサーツリー): 全センサー/デバイス/グループを階層ツリー状に表示
- "Lists" (リスト): 各種センサーリスト
- "Alarms" (アラーム): エラーや警告の状態、異常値が表示された全センサーのリスト
- "Dashboard" (ダッシュボード): 最重要リストを見やすく表示 (アラーム、最近のログエントリ、お気に入りセンサーのステータス、最近の Todos)
- "Maps": ユーザーが監視するネットワークに対し、独自の概要とダッシュボードを生成します。

各種パラメータに基づき、ソートしたセンサーとフィルタリングしたリストのステータスを確認できます (センサータイプ、タグ、デバイス、ステータス、測定値など)。

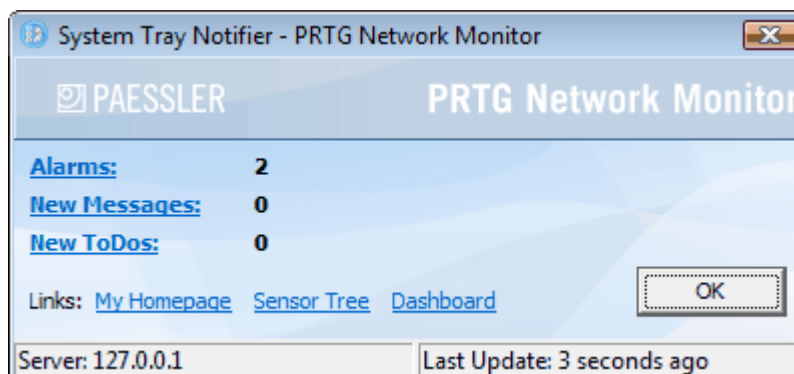
- 各種トップ 10 リスト
- 可用性 ベスト/ワースト
- PING 最高速/最低速

- 帯域使用最高値 / 最低値
- Web サイト最高速 / 最低速
- CPU 使用 最高値 / 最低値
- 空きディスク・スペース 最高値 / 最低値

グループやデバイスのグラフが表示するのは、関連するセンサーのアラーム、"bandwidth index" (帯域インデックス)、"speed index" (スピードインデックス)、"CPU load index" (CPU 負荷インデックス) です。これらの値は洗練されたアルゴリズムにより計算されます。このアルゴリズムは様々なタイプのセンサーのデータを1つのグラフに統合します。このグラフは最新グループ / デバイスのセンサー動作の状態を大まかな概要で表示します。これらのグラフは異常なネットワーク活動を見つけるのに非常に役立ちます。

## 5.6 System Tray Notifier (システムトレイ通知)

システムトレイ通知は、PC 上のバックグラウンドで実行します。PRTG がネットワーク上の変化を検出するといつでも警告音やポップアップで通知します。



PRTG インストール時に自動的にコンピュータにインストールされます。別 PC でトレイツールをご利用になる場合、PRTG Web インターフェースよりソフトウェアをダウンロードの上、インストールして下さい(メニュー項目 "Setup Downloads" を選択)。

ソフトウェアを起動すると PRTG アイコンが確認できます。画面右下のコーナー、Windows システムトレイにあります。ソフトウェアを設定するには、アイコンを右クリックして "Options" を選択して下さい。アカウント認証(クレデンシャル)と PRTG サーバの DNS 名を入力して下さい。このプログラムはバックグラウンドで実行し、ポップアップの表示、警告音、またはトレイアイコンの点滅により、アラームやメッセージ、Todos を通知します。

## 5.7 iPhone User Interface iPhone (ユーザーインターフェース)

PRTG Network Monitor は Apple 社 iPhone に対し最適化したユーザーインターフェースをご提供します。この機能により離れた場所にあるセンサーやサーバーのステータスを素早く確認することができます。



iPhone の Safari ブラウザで URL を [https://\(御社 PRTG サーバー\)/iphone](https://(御社 PRTG サーバー)/iphone) に指定すると、ログインダイアログが確認できます。 クレデンシャルを入力すると、数秒後に iPhone ディスプレイ上にセンサー/デバイス/グループ毎のセンサーツリーがご確認いただけます。 センサーにタッチすると、そのセンサーについて詳細情報、最近のエントリー・ログファイルのグラフ表示を受信します。

現行では iPhone インターフェースは”読取専用”(ステータス監視のみ)です。

セキュリティ面で下記事項にご注意下さい。

- HTTP でサーバーに接続可能ですが、パスワードを保護するために、SSL/HTTPS による暗号化アクセスを推奨します。
- さらに安全性を高めるために、iPhone ログイン専用ユーザーを作成して下さい。このユーザーは、“Root Group”(ルートグループ)、または予め選択したグループに対して、読取アクセス専用です。

# Part

# VI

## Sensor Setup (センサー設定)

## 6 Sensor Setup (センサー設定)

センサーの作成開始前に、"Root Group's"設定を確認してください。この設定は全オブジェクトによりひきつがれます(6.1章の「ネットワークの基本設定」参照)

確認後、すぐに手動もしくはオートディスカバリー(6.3章参照)使用で自動的に、ネットワーク監視の為の新規センサーの作成を開始します(6.2章参照)。以下、本章で上記の設定について説明します。

注意: マルチ PRTG プロブ設定を作製する場合、はじめに、必要な PRTG プロブを追加し設定しなければなりません。(14.2 複数プロブとリモートプロブ参照)

### 6.1 Reviewing Settings of the Root Group(ルートグループの設定確認)

"設定の引継ぎ"(4.3章参照)で説明した通り、センサーツリー内のオブジェクトは親オブジェクトより多数の設定を引き継ぎます。"Root Group"(ルートグループ)はその他全てのオブジェクトに対して、親オブジェクトになりますので、特に重要です。

その為、ユーザーが独自のセンサーを作成する前に、ルートグループ設定が貴社ネットワークへ適合しているか、確認してください。メインメニューより、"Devices"の項目を選択し、"Settings"タブをクリックします。以下は関連する設定のいくつかです。



設定を確認し、右側にある、各設定について詳細説明したヘルプテキストをご参照下さい。全ての子オブジェクトに対し、これらの設定は、いつでも変更できます。

以下、参照ください。

- Windows システムのクレデンシャル: ここで提供されるアクティブディレクトリのユーザーアカウントは、全ての WMI ベースの監視や、オートディスカバリープロセスの間に使用できます。管理者権限のあるユーザーアカウントの使用を推奨します。
- VMware サーバーのクレデンシャル: VMware ESX サーバーや VMware Virtual Centers で実行する場合は、オートディスカバリーや監視で使用するユーザーアカウントが必要です。
- SNMP デバイス及び SNMP Compatibility Options: SNMP のバージョンを選択し、ネットワークで使用している認証文字列を入力してください。デフォルトは、"SNMP V1"、コミュニティ名 "public"、ポート 161 です。
- スキャン間隔: 全センサーの監視間隔を選択してください。
- 異状検出: 有効/無効を選択できます。
- アクセス権: オブジェクトの読み取り/編集をさせるユーザーグループを定義します。
- チャネルユニット設定: それぞれのチャンネル・タイプについてユニット設定できません。

## 6.2 Creating Groups, Devices and Sensors Manually (グループ、デバイス、センサーの手動作成)

### グループ作成

新規グループを作成するには、デバイスリストへ行き ("Devices" はメインメニュー下にありません)、新規グループを組み入れたいプロパティグループを選択します。オブジェクトを右クリックして、コンテキストメニューより "Add Group" を選択します。もしくは、"Devices" メニューより、"Add Group" を選択することもできます。但し、その場合、親グループを選択しなければなりません。

The screenshot shows a dialog box titled "Add Group to Group 'Group 1'". It has a section for "Group Name and Tags" with a text input for "Group Name" containing "Group 5" and a "Tags" input. Below are two checked options for inheriting credentials from the parent object, one for Windows Systems and one for SNMP Devices. At the bottom are "Continue >" and "Cancel" buttons.

新規グループの名称を入力してください。必要に応じて、クレデンシャル設定の継承を選択し、"Continue"をクリックしてください。

## デバイスの作成

新規デバイスの作成は、任意のデバイスを右クリックし、「Add Device」をコンテキストメニューより選択してください。もしくは、「Devices」メニューより、「Add Group」を選択することもできます。但し、その場合、親グループを選択しなければなりません。

The screenshot shows the 'Add Device to Group' dialog box. The title is 'Add Device to Group "Group 1"'. The 'Device Name and Address' section has a 'Device Name' field with 'Device 8', an 'Ip-Address/DNS Name' field, and a 'Tags' field. The 'Device Type' section has four radio button options: 'Manual (No AutoDiscovery)' (selected), 'Automatic Device Identification (Standard, recommended)', 'Automatic Device Identification (Detailed, may create many sensors)', and 'Automatic Sensor Creation with specific Device Templates'. Below this are two checked options: 'Inherit Credentials for Windows Systems' and 'Inherit Credentials for SNMP Devices'. At the bottom are 'Continue >' and 'Cancel' buttons.

この設定では、デバイス名称と IP アドレス(或いは、DNS 名)の設定が必要です。必要に応じて、クレデンシャル設定の継承を選択し、「Continue」をクリックしてください。

## センサーの作成

新規センサーの作成では、センサーを追加したいデバイスを右クリックし、「Add Sensor」をコンテキストメニューより選択してください。もしくは、「Sensors」メニューより、「Add Sensor」を選択してください。この場合、親デバイスを選択しなければなりません。

センサーを作製する場合、次の 2 つのステップが必要となります。

1. センサータイプを選ぶ。
2. センサー設定を決める。



ステップ1では、リストからセンサータイプを選択します。40種類以上のタイプがあり(詳細は **Part VII センサータイプ**を参照)、さまざまなグループに対応させています。グループの見出しをクリックし、センサータイプを選択してください。その後、"Continue to Step 2"をクリックします。

**Add Sensor to Device "Device 6" (Step 2 of 2)**

Basic Sensor Settings		
Sensor Name:	Basic Sensor 1	The name of the sensor.
Tags:	http:sensor	Enter a list of tags (case insensitive) for filtering purposes (e.g. the Top 10 list use these tags for filtering). Use spaces or comma as separator. Use this value for sorting the object in lists.
Priority:	***	
PING Settings		
Timeout (s):	60	If the reply takes longer than the value the request is aborted and you get an error message. If too consecutive requests will fail (for whatever reason) the sensor enters a "Down" state. This has consequences e.g. for visual feedback or notifications.
Packet Size (Bytes):	32	The default packet size for PING is 32 bytes, but you can choose any other packet size between 1 and 20000 bytes.
PING Count:	1	PRTG can send only one PING for a simple connectivity test or optionally a series of PINGS in order to measure packet loss and utilization/maximum PING time. A setting of "1" is good for availability monitoring. Choose higher values to measure packet loss (e.g. 10 or 100 pings).
Limits for Warnings and Errors		
Show Error when above:		If the sensor result is higher than this value the "Down" state of the sensor is triggered.
Show Warning when above:		If the sensor result is higher than this value the "Warning" state of the sensor is triggered.
Warning of packet loss above (%)		If the Packet Loss is above this value the "Warning" state of the sensor is triggered.
<input checked="" type="checkbox"/> Inherit Sensor Interval from parent object (Device) (Scanning Interval: 60s)		
Schedules and Dependencies		
Schedule:	None	Using Schedules you can pause monitoring at specific days and hours throughout the week. You can edit schedules in the system settings.
Dependency Type:	<input checked="" type="radio"/> Use Parent <input type="radio"/> Select Object <input type="radio"/> Master object for parent	Select the dependency behaviour for this object. "Use Parent" means this object will be paused when the parent object is not UP. With "Select object" you can select an object from a dropdown for as dependency. If you select "Master object" the parent object will use the current object as dependency and it is ensured that this object is not dependent from its parent in order to avoid a dependency loop.

Continue >      Cancel

ステップ2では、センサータイプによって、できる設定が異なります。設定を確認し、必要な変更を加え、"save"をクリックしてください。新しく設定したセンサーが直ちに監視を始めます。

### 6.3 Creating Devices and Sensors Using the Auto Discovery (オートディスカバリーでのデバイス/センサーの作成)

PRTG のオートディスカバリーは、ユーザーのネットワーク全体において、巧みにかつ無駄なく、センサーを自動的に作成します。この機能は、主に LAN の検出に適しています。多くの SNMP や WMI が含まれているのがその理由です。

#### 動作について

PRTG のオートディスカバリーのプロセスは、次の3段階となっています。

- ステップ1: PING を使って、デバイスのネットワーク・セグメントのスキャン(グループ

のみ)

- ステップ 2: 1 で検出した全デバイスに対し、デバイス種類を査定 (SNMP, WMI その他プロトコル使用)
- ステップ 3a: 2 で検出したデバイスに適合するセンサーの作成 (事前に組み込まれたデバイステンプレートに基づきます。テンプレートには、多くのデバイスタイプに適合したセンサーが含まれています。)
- ステップ 3b (必要に応じて): ユーザー独自のデバイステンプレートでセンサーを作成 (14.3 クローニング/デバイステンプレートによるデバイスのコピー参照)

オートディスカバリーは、さまざまな IP アドレスやユーザーが手動で作成した個々のデバイスについてのグループレベルで使用できます。また、1 回限り、或いは、コンテキストメニュー経由で適宜、または、毎時間、毎日、毎週ごとと、定期的に行うことができます。オートディスカバリーを毎日 (毎週) 実行することで、新しいデバイスがネットワークに接続されると、自動的に新しいセンサーが生成されます。新規デバイスやセンサーが見つかったと即座に、新規の”Todo”が生成され、システム管理者に E メールで通知されます。

オートディスカバリーについて、以下の制限がありますので、ご注意ください。

- ステップ 1 で PING を使用するため、PING を送ることができないデバイスは検出できません (例: エコー要求がファイアーウォールでブロックされる場合)。
- 上記の機能を十分に利用するために、SNMP や Windows/WMI/VMware サーバーに認証設定が必要です。
- デバイスの IP アドレスが 1 つ以上ある場合、検出結果が 1 つ以上表示される事があります。

## オートディスカバリーグループの作成

プローブ、あるいは、グループを右クリックし、コンテキストメニューより、"Add Auto-Discovery Group" を選択して、新規グループを作成してください。

グループ名称を入力し、"Sensor Management" 設定の選択肢を選んでください。

Group Type		
Sensor Management	<input type="radio"/> Manual (No Autodiscovery) <input checked="" type="radio"/> Automatic Device Identification (Standard, recommended) <input type="radio"/> Automatic Device Identification (Detailed, may create many sensors) <input type="radio"/> Automatic Sensor Creation with specific Device Template(s)	Choose the "Manual" option if you want to create and manage sensors manually. The other settings will scan your network for available sensors and create the appropriate sensors. "Automatic Device Identification" is mainly based on PING, SubIP and WMI. It should only be used in LANs and is not suitable for WAN connections.
Discovery Schedule	Once	
IP Base	192.168.0	Enter a Class C network IP base, e.g. 192.168.0
IP Range Begin	1	Enter the IP of the above specified Class C network at which PRTG shall start to discover new devices
IP Range End	254	Enter the IP of the above specified Class C network at which PRTG shall stop to discover new devices

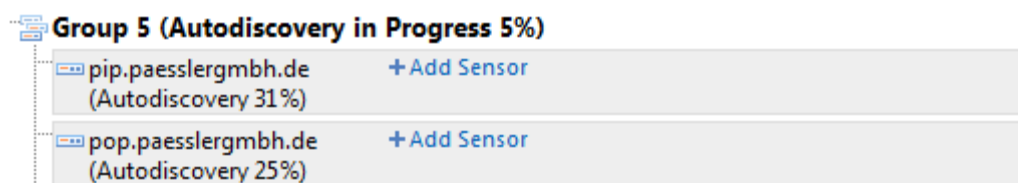
選択できるのは、次の 4 つです。

- Manual (マニュアル・オートディスカバリーなし)
- Automatic Device Identification (Standard, recommended) (自動デバイス認識・標

準、推奨): 推奨です。ほとんどの場合に適しています。

- Automatic Device Identification (Detailed, may create many sensors)(自動デバイス認証・詳細、多数センサーを作成): 小規模ネットワーク・セグメントで、有効センサーの最大数の監視を随時行う場合などに適しています。
- Automatic Sensor Creation with specific Device Template(s)(所定のデバイスプレートによる自動センサー生成): 自動デバイス認識を使いたくない場合、手動でデバイスプレートを使用したい場合(例: ユーザー独自のプレートを使用したい場合)に、こちらを選択してください。デバイスプレートのリストから、1 つ以上のプレートを選択できます。

続いて、IP ベースを入力し(IP アドレスレンジの最初の 3 バイト)、IP アドレスレンジの最初と最後の 4 バイトを入力します。"continue"をクリックすると、ディスカバリー処理を開始し、センサーツリー(メインメニュー > "Devices"メニュー)に表示します。

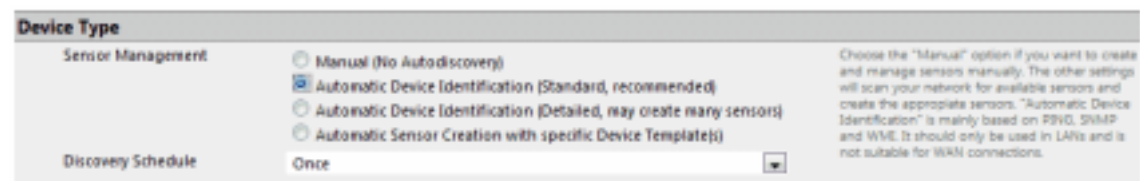


次々にリストにデバイスやメニューが表示されます。オートディスカバリー処理は、設定やネットワークによりますが、IP アドレスごとに 10 から 50 秒かかります。

この処理で作製されたセンサーは全て、すぐに監視を開始し、障害が発生しだい、通知します。

### オートディスカバリーデバイスの作成

オートディスカバリー機能によってデバイスに対するセンサーを作成することは、オートディスカバリーグループを作成することと似ています。任意のグループを右クリックし、コンテキストメニューより"Add Device"を選択して、新しいデバイスを作成してください。



デバイスの名称と、IPアドレス(もしくはDNS名)を入力したら、"Sensor Management"(上図参照)の選択肢を一つ選んでください。

"Continue"をクリックすると、デバイス評価が開始され、デバイスにあったセンサーが作成されます。

# Part

# VII

## Sensor Types (センサータイプ)

## 7 Sensor Types (センサータイプ)

PRTGには、さまざまなネットワークサービスに対して、40種類以上の異なるセンサータイプを用意しています。全てのセンサータイプには、たくさんのタイプ別の設定に加え、全センサー共通の設定も数多くあります。その他全ての設定についての詳細は、webインターフェースのヘルプテキストを参照してください。

### センサー概要

新規のセンサーを生成する場合、次のセンサータイプのグループがあります。センサータイプによっては、リストに何度も出てくるものもあります。それは、複数のカテゴリーに該当するからです。

- 一般センサー： ネットワーク監視において、もっとも一般的なセンサータイプ。
- 帯域監視： SNMP、WMI、NetFlow、Packet Sniffingを使った帯域利用の監視。
- HTTP(Webサーバー)： HTTPプロトコルに基づいたセンサー。
- SNMP： Simple Network Management Protocol (SNMP)に基づいたセンサー。
- WMI： Windows Management Instrumentation (WMI)を使ったWindowsシステムの監視。
- インターネットプロトコル： インターネットで使用されるサービスについてのさまざまなセンサータイプ(PING, PORT, FTP, DNS, RDP)。
- メールサーバー： メールサーバーのためのセンサー(SMTP, POP3, IMAP, TP&IMAP Round Trip, SMTP&POP3Round Trip)。
- SQLサーバー： SQLサーバーを監視。(MySQL, MS-SQL and Oracle)
- システム診断センサー： システムの状態を監視するセンサー。(ディスク温度など)
- VMwareサーバー： VMwareサーバーのためのセンサー。
- カスタムセンサー： センサースクリプトのユーザー定義を可能にするさまざまなセンサータイプ。

### 7.1 SNMP Sensor Types(SNMP センサータイプ)

Simple Network Management Protocol (SNMP)は、もっとも帯域やネットワーク利用データを収集する最も標準的な方法です。

#### SNMP監視の働き

SNMPは、メモリーやCPU負荷などといったデバイスの記録や、ポートごとのルーターやスイッチの帯域使用を監視します。



SNMPによる監視の際、PRTGは、デバイス(ルーター、スイッチ、サーバーなど)にそれぞれのポートのトラフィックカウンターについて、非常に小さなデータパケットで問い合わせを出します。それによって、デバイスは応答パケットを出します。3つの方法のうち、こちらがCPUおよびネットワークの負荷が最小になります。

#### SNMP監視を選択する理由

SNMPは、もっとも一般的に使用されているプロトコルです。なぜなら、セットアップが容易で、最小限の帯域とCPUサイクルしか必要としないからです。ユーザーのネットワークデバイスがSNMPに対応している場合、もしくは、数百、数千センサーもの大規模ネットワークの監視を検討している場合、SNMPによる監視をお勧めします。

ネットワーク利用監視に加え、もう一つのSNMPの有名な機能は、CPU負荷、ディスク使用状況、温度といった他のネットワークパラメーターや、デバイスによりますが、その他さまざまな要素を監視することです。

#### ネットワークにおける注意点:

SNMPを監視目的でご利用になる場合、必ず、PRTG実行機と監視するデバイス間において、UDPパケットを許可しておいてください。LANやイントラネットの場合は通常そうですが、インターネット接続、DMZやWAN接続の場合は、そうではなく、通過するファイアウォールに若干の変更が必要となります。SNMP V1、V2cは、安全なプロトコルではなく、インターネットや、安全でないデータ接続において使用するべきではありません。唯一、SNMPバージョン3が、暗号化に対応しています。

#### SNMPセンサータイプ

以下のセンサーは、Simple Network Management Protocolを使用しています。(SNMP V1、V2c、V3に対応)

- SNMP Traffic: PC/サーバー/スイッチ/ファイアウォール/プリンター上のポート/ネットワークカードに対する、SNMP経由の、パケット数、帯域(ビット/秒)、容量(バイト)の監視に対応
- SNMP Custom: ユーザーが指定した特定のOIDを監視
- SNMP Library: SNMP Libraryによって、MIBに基づいてシステム固有のセンサーを用意に作成できます。(既実装されているものもあり、フリーのMIBインポートツールで標準のSNMP MIBファイルから新しいセンサーを作成することも)

きます。以下参照)

### SNMPバージョン1、2c、3

PRTGは、SNMPプロトコルの3つのバージョンに対応しています。

SNMPバージョン1: 最も古く、最も標準的なバージョンです。

- 長所: ほとんどのSNMP互換デバイスに対応。設定容易。
- 短所: 簡単なパスワード("community string")しか使わず、平文データを送信(暗号化なし)。ファイアーウォールの後ろのLANの中でしか使用できない。WANでの使用不可。32ビットカウンタにのみ対応で、高負荷帯域監視(ギガビット/秒)には、不向きです。

SNMPバージョン2c: 64ビットカウンタを追加。

- 長所: 64ビットカウンタ対応で、ネットワークにおけるギガビット/秒の帯域利用を監視。
- 短所: セキュリティに問題あり(SNMP V1と同様)。

SNMPバージョン3: 認証と暗号化機能を追加。

- 長所: ユーザーアカウントと認証機能を複数ユーザーに提供。データの暗号化が可能に。セキュリティ向上。バージョン2cの長所は継承。
- 短所: 設定が複雑。

監視するサーバーやデバイスが対応していないSNMPのバージョンを選択すると、エラーメッセージが出ます。また、これらのエラーメッセージには、はっきりとしたSNMPのバージョンミスの可能性についての説明がないことがほとんどです。エラーメッセージには、"cannot connect" (接続不可)などの最小限の情報しか表示されていません。コミュニティ名や、ユーザー名、パスワードミスの場合にも、同じようなことが言えます。

### SNMPのオーバーロードとSNMPシステムの制限

SNMP V1 やV2は、直接ハードウェアのパフォーマンスやネットワークの速度を計測します。弊社では、1台のPRTGサーバー(コアとローカルプローブ)と2つのリモートプローブ(各プローブに10,000センサー)、60秒間隔で、30,000 SNMP V1センサーの監視に成功しました。

しかし、SNMP V3には、SSL暗号化機能のため、ソフトウェアに依存したパフォーマンス制限があります。弊社は、SNMP V3の要求に対して、10ミリ秒から1000ミリ秒の要求時間を計測しました。PRTGにおける全てのSNMP V3のリクエストは、各プローブに連続して出されるため、60秒間隔で、60から6000 SNMP V3センサーの監視が可能です。ただし、使用するネットワークの要求時間にもよります。"Probe Health"センサーの"SNMP Interval Delay"チャンネルに注意してください。値が0%の場合、SNMP要求が指定した間隔で実行されていない可能性があります。

SNMPオーバーロード障害が起こった場合の対応は、次の3つのうちのいずれかとなります。

す。

- SNMP V3センサーの監視間隔を増やす。
- SNMP V3センサーを2つ以上のプローブへ割り振る。
- 暗号化不要の場合は、SNMP V1 か V2へ変更する。

“SNMP Community String”とは？

“SNMP Community String”は、ユーザーIDやパスワードのようなもので、ルーターもしくはその他デバイスの統計データへのアクセスを許可するものです。PRTG Network Monitorは全てのSNMP要求と一緒にコミュニティストリングを送信しています。コミュニティストリングが正しい場合、デバイスは、要求された情報で応答します。コミュニティストリングが間違っていれば、デバイスは要求を無視して、応答しません。

**注意：** SNMP community stringsは、SNMPv1 ならびに SNMPv2cプロトコル対応のデバイスでのみ使用されます。SNMPv3は、ユーザー名/パスワード認証を暗号鍵とともに用います。

慣例により、ほとんどのSNMPv1-v2c機器は、デフォルトとして"public"に設定された読み出し専用のコミュニティストリングを実装しています。ネットワーク管理者が、全てのコミュニティストリングをデバイス設定の中で、独自の値に変更するのが普通です。

## ツール

Paessler MIBインポーター： MIB(Management Information Base)ファイルをインポートし、OIDライブラリーへ変換し、PRTG Network Monitorで使えるようにします。

<http://www.paessler.com/tools/>

Paessler SNMPテスター： SNMPテスターは、SNMP監視設定における通信/データの障害を検出するために、ネットワーク内のデバイスに対する簡単なSNMP要求を実行し、SNMP要求をプロトコルレベルまでデバッグします。

<http://www.paessler.com/tools/>

参照： 7.13 帯域監視センサータイプの比較

## 7.2 WMI Sensor Types(WMI センサータイプ)

Windows Management Instrumentation (WMI)は、Windowsベースシステムの監視と管理のためのMicrosoftの基本技術です。WMIによって、多くのWindows設定パラメータや、現在のシステムのステータス状況のデータへアクセス可能になります。アクセスは、ネットワークを経由して、ローカルでもリモートでも可能です。WMIは、COMやDCOMの技術に基づいていて、Windows 2000/XP/2003/Vistaに統合されています(アドオンは、Windows 9x / NT4で使用可能です)。

遠隔マシンを監視するには、PRTGのWMIセンサーは、WMIインターフェースにアクセスするためにActive Directoryアカウントが必要です。親デバイス/グループにこれらのクレデンシャルを入力できます。センサーは、その際、これらの設定を継承します。

## WMI Sensor Types

PRTGは以下のWMIベースのセンサータイプに対応しています。

- WMI CPU Load: システムのCPU負荷を計測(トータル・CPU当りの負荷)
- WMI Memory: システムの空きメモリ容量を表示(MB・%)
- WMI Disk Space: 固定ディスクの空きディスク容量を表示(MB・%、ドライブ当り)
- WMI Network Card: ネットワークカードを通過するトラフィックを計測
- WMI Page File: Windowsページファイルの使用状況を確認
- WMI Service: サービスが実行されているか確認したり、実行されていない場合は、サービスを再起動する。
- WMI Event Log Sensor: 特定のイベントに対する、アプリケーション、システム、セキュリティイベントログを監視
- WMI Process: WMI経由の1プロセスを監視
- WMI File: ファイルのサイズ、存在、変更をWMI経由で監視
- WMI Vital System Data: 20種類以上の重要なWindowsシステムパラメーターから、ユーザーが選択することができます。((CPU: Percent Processor Time(プロセッサがアイドル以外のスレッドを実行する時間), CPU: Processor Queue Length(プロセッサ待ち行列中のスレッド数), CPU: Processor Percent Privileged Time, CPU: Processor Percent User Time, Thread Context Switches(スレッドコンテキストスイッチ), メモリ: Free Physical Memory(物理メモリ空き容量), メモリ: Total Visible Memory(可視メモリ合計), メモリ: Pages/sec(ページ/秒), メモリ: Page Faults/sec(ページフォールト/秒), メモリ: Page Reads/sec(ページ読み込み/秒), メモリ: Page Writes/sec(ページ書き込み/秒), メモリ: Pool Non-paged bytes(ノンページドプール、バイト), Page file Usage(ページファイル使用状況), ディスク: Percent Disk Time(ディスクビジー率), ディスク: Current Disk Queue Length(ディスク待ち数), Disk: Reads/sec読み込み/秒, ディスク: Writes/sec(書き込み/秒), ネットワーク: Bytes Total/sec(合計バイト/秒), ネットワーク: Bytes Received/sec(受信バイト/秒), ネットワーク: Bytes Sent/sec(送信バイト/秒), サーバー: Bytes Total/sec(合計バイト/秒), サーバー: Bytes Received/sec(受信バイト/秒), サーバー: Bytes Sent/sec(送信バイト/秒)など)
- WMI Exchange Server 2003: Exchange Server 2003 の重要な値を監視。
- WMI Custom: カスタムWMIクエリの実行

## WMIオーバーロードとWMIシステムの制限

WMIシステムの内部的な制限のために(内在するWindowsのプロトコルの制限であり、PRTGの制限ではありません)、ある一定間隔のプロープ当りに監視できるWMIセンサーの数が制限される場合があります。これらの制限は、さまざまな要素によって異なります(例えば、ネットワークのスピードや、監視システムのWMIクエリ結果を返す際に要する時間など)。プロープあたりのWMIセンサーの数が、120以下(60秒間隔)か、600以下(300秒間隔)であれば、そのような制限はないでしょう。WMIセンサーの数がそれ以上の場合、Probe Healthセンサーの"WMI Delay"チャンネルをよく確認してください。0%に近い値の場合、WMIオーバーロードであることを表しています。

WMIオーバーロードが発生した場合の対応は、以下の3つのうちのいずれかとなります。

- いくつか、或いは全てのWMIセンサーの監視間隔を増やす
- WMIセンサーを、2つ以上のプローブに割り振る
- 長時間のカスタムWQLクエリを避ける

### WMI関連記事へのリンク

Paessler社ガイド-WMI障害のトラブルシューティング

[http://www.paessler.com/support/kb/prtg7/wmi\\_not\\_working/](http://www.paessler.com/support/kb/prtg7/wmi_not_working/)

Paessler WMIテスター: WMI接続を検証するのに役立つフリーウェアツールです。WMIカウンターの接続をすばやく、簡単に検証します

<http://www.paessler.com/tools/wmitester>

Microsoft: Windows Management Instrumentation Technical Articles: WMI実装Windowsの管理

<http://msdn2.microsoft.com/en-us/library/ms811533.aspx>

Microsoft: WMI Reference

<http://msdn.microsoft.com/en-us/library/aa394572.aspx>

参照: 7.13 帯域監視センサータイプの比較

## 7.3 HTTP Sensor Types (HTTP センサータイプ)

HTTPプロトコル(Hypertext Transfer Protocol)は、World Wide Webで、もっとも一般的に使用されています。このプロトコルを使用して、webブラウザがwebページやグラフィックスなどをwebサーバーからリクエストします。

一般的なパラメーターには次のようなものがあります。

- URL - 監視するwebページのURLアドレス (http://で始まるものを含む)
- Mode 使用するHTTPリクエストモード (GET、POST、HEAD)
- POSTDATA - POSTメソッドを使用する際のデータ部

簡単なWebページの場合は、単にURL (http://で始まる) を入力し、デフォルトmodeをGETに選択しておきます。POSTフォームのURLを監視する場合は、POSTメソッドを選択し、POSTDATAを入力する必要があります。HEADメソッドは、実際のwebページではなく、サーバーからHTTPヘッダーを要求する場合にのみ使用します。この方法は、データ転送量が少ないため、帯域を節約しますが、以下の理由でお勧めしません。計測された要求時間が、実際の要求時間とは異なり、結果の遅延や、タイムアウトが通知されない可能性があるからです。

**注意:** ネットワークにおいてHTTPリクエストのためにプロキシが必要であったり、URLが認証を要求する場合、HTTP Advancedセンサーを使用する必要があります。

## 帯域とログファイル分析関連

### 重要:

HTTPセンサーには相当量の帯域負荷がかかりますので、ご注意ください。なぜなら、要求ごとに、大量のデータを転送するセンサーの一つだからです(簡単なpingに対して、その1000倍ものデータ量を送ることもあります)。帯域(もしくは、接続やWebサーバー)に費用をかける必要がある場合、データ量の少ないHTMLページを返すだけのURLを選択することをお勧めします。これは、ほとんどのLANやイントラネットでは、大きな問題ではありません。が、帯域使用状況は常に監視する必要があります。25kbのWebページを1分間隔でリクエストした場合、1日に36MBの、また、1ヶ月に1ギガバイト以上のトラフィックとなります。

また、監視要求がユーザーのwebサーバーのログ分析上に表示されますので、ご注意ください(1分間隔での1ヶ月の監視だと、43,200回のリクエストになります)。ログファイルを分析する際、PRTGからの要求を取り除く必要があります。その除去は、PRTG事項サーバーのIPアドレスに基づいて、或いは、PRTGブラウザエージェントからのフィルタリングリクエストで、簡単に行うことができます。

```
Mozilla/5.0 (compatible; PRTG Network Monitor Vxxxx; Windows)
```

## HTTPセンサータイプ

PRTGには、以下のHTTPベースのセンサーがあり、Webサーバーを監視します。

- HTTP: HTTPプロトコルを経由して、Webサーバーを監視。
- HTTP Advanced: さまざまな詳細設定で、HTTPプロトコル経由でWebサーバーを監視(Webページの内容のチェック、認証やプロキシサーバーの使用など)
- HTTP Transaction: ログインやショッピングカートが正常に機能しているかどうかを監視するためにURLを使用してwebサーバーを監視。ユーザーはURL(GET/POST要求)をトランザクションを監視するパラメータと一緒に設定する必要があります。URLリスト(下記参照)を作成するために、Paessler URL Recorderをご利用ください。
- HTTP Content: HTTPリクエストによる戻り値を監視。このセンサーは、HTTPのURLを要求し、カッコで括られた値"[value]"を解析します。もっとも一般的な使い方は、Webサーバーの特定の値の有効性を監視します。例えば、単にハードディスクの空き領域や現在のCPU使用率だけを表示するwebサーバー上でスクリプトやCGIを実行している場合、この値を実際に監視することができます。もちろん他の使用率についても多く監視可能です。
- HTTP Full Web Page: 画像などを含んだWebページのダウンロード時間を監視。(ページ全体のダウンロードにInternet Explorerを使用。)

全てのセンサーは、HTTPとHTTPSに対応しています。

## HTTPセンサーの作動

HTTPセンサーのステータスがUP(作動)の場合、WebサーバーがHTTPプロトコルにしたがって正しいHTTP結果を送信し、URLが有効であることを意味しています。つまり、Webサーバーのソフトウェアが作動中であっても、その結果が正しいかどうか、例えば、Webページ

にエラーメッセージが含まれている場合など、ユーザーにはわからないということです。ユーザーは、CGIスクリプトなどが正しく作動しているかどうか、また、例えば、Webサーバーのデータベースが正常かどうかについてもわかりません。信頼性を高めるために、単なるHTTPセンサーではなく、HTTP Advancedセンサーを使うことで、Webページの内容をチェックすることをお勧めします。

### HTTPセンサーのダウン

HTTPセンサーの障害の理由はたくさんあります。通常の接続障害に加えて、もっとも一般的な問題は、サーバー内部の障害(エラーコード50x)や誤ったURLが原因の問題(エラーコード404, page not found)です。

### ツール

Paessler URL Recorder: URLサーフィン中にユーザーがWebサーバーに送信したURLやPOSTDATAの検索。HTTP Transactionセンサーの設定時に、便利です。

<http://www.paessler.com/tools/>

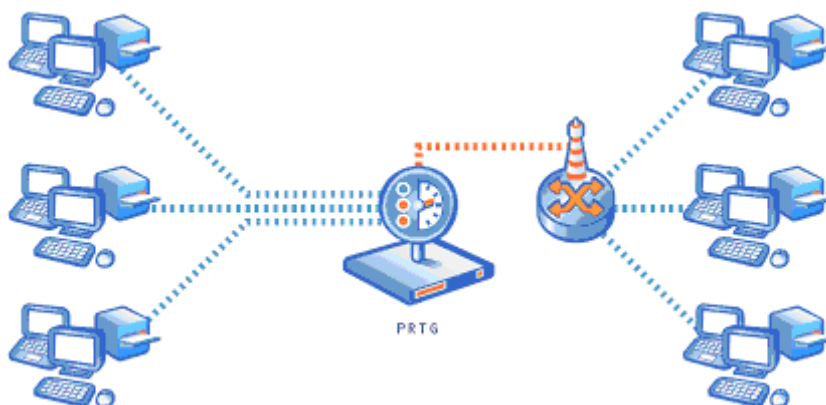
## 7.4 Packet Sniffing Sensor Types (Packet Sniffing (パケットスニフing) センサータイプ)

ネットワークデバイスが帯域使用状況の計測において SNMP 対応でない場合、またはネットワークプロトコルや IP アドレスの帯域使用状況それぞれ区別する必要がある場合、Packet Sniffing (パケットスニフing) をご検討ください。

注意:パケットスニフingセンサーは、トップリスト(Top Talkers/Top Connections など)に対応しています。14.1 トップリストを参照してください。

### パケットスニファの動作について

ネットワーク内部のトラフィックが、どのアプリケーションまたはIPアドレスによるものか知る必要があれば、パケットスニファを使用します。たとえばアカウントing目的で貴社ネットワーク内部を移動する個々のデータパケットを監視できます。



PRTG は PC のネットワークカードを通過するパケットを分析できます。また、スイッチのいわゆるモニタリング・ポートに接続することができます。帯域使用を計算する為、PRTG は PC ネットワークカードを通過するデータパケット(上図左側)やスイッチの監視ポートから送信されたデータパケット(上図右側)を組み込みパケットスニファで精査します。

PRTG が提供する 4 つの帯域監視テクノロジー (SNMP, WMI, NetFlow, パケットスニファ)の中で、この方法が最も CPU とネットワークに負荷がかかります。この方法は小規模のネットワーク、大規模ネットワークの専用コンピュータ、または単独のコンピュータに使用することをお勧めします。

### パケットスニファを選択する理由

パケットスニファは PRTG 実行マシンのネットワークインターフェイスを実際に通過するパケットのみについてのみ監視とアクセスが可能です。このマシン(例;ウェブサーバー)のトラフィックのみを監視する場合は、この方法で十分です。しかし、スイッチネットワークでは、あるマシンに対するトラフィックだけが各マシンのネットワークカードに送信されるため、PRTG はネットワーク内の他のマシンのトラフィックを認識できません。

ネットワーク上の、他のデバイスのトラフィックを監視する場合、“monitoring port”(監視ポート)や“port mirroring”(ポートミラーリング)設定が可能なスイッチを使用して下さい(Cisco では“SPAN”と呼びます)。この場合、スイッチは、スイッチを通過する全てのデータパケットのコピーを監視ポートに送信します。接続すると即座に、パケットスニファで監視するポートに接続された PRTG 実行マシンは、スイッチを通過するトラフィックを解析できるようになります。他に、PRTG 実行マシンを他の全てのコンピュータのゲートウェイとして使用することもできます。

### ヘッダベース/コンテンツベースのパケットスニファ

PRTG はパケットスニファに対して2つの基本テクノロジーを提供します。

- **ヘッダベース：** PRTG が監視するのはプロトコルにアクセスする IP やポートの送信元と宛先です。この方法は高速ですが、時として正確性に欠けます。例えば、80,8080、及び 443 (HTTP) 以外のポートにおける HTTP トラフィックの識別は不可能です。
- **コンテンツベース：** PRTG は TCP パケットを捕らえて、データストリームを再構築し、データ内容を分析します。内部で設定したルールを用いて、トラフィックの種類を識別します。この方法は極めて正確です(どのポート番号上の HTTP トラフィックも HTTP として認識されます)が、特にネットワークカードに大量のトラフィックが通過する場合などに、大量の CPU やメモリのリソースが必要です。

ヘッダベースのスニファの方が早いのですが、認識の信頼性は低いです(例;標準的でないポート上の HTTP パケットは HTTP パケットとみなされません)。コンテンツベーススニフィ

ングはきわめて正確ですが、CPU負荷は上がります。

Packet Sniffing(パケットスニフing)は、以下のプロトコルで区別されます。

- WWW トラフィック: HTTP, HTTPS
- ファイル転送: FTP
- メールトラフィック: IMAP, POP3, SMTP
- チャット、インスタントメッセージ: IRC, AIM
- リモートコントロール: RDP, SSH, Telnet, VNC
- ネットワークサービス: DHCP, DNS, Ident, ICMP, SNMP
- NetBIOS: NETBIOS
- その他: Socks, その他UDP, その他TCP

### Packet Sniffing(パケットスニフing)センサータイプ

PRTGはPacket Sniffing(パケットスニフing)をベースにした3つのセンサータイプを提供します。

- Packet Sniffer(ヘッダー): データパケットのヘッダーでIP、ポート、プロトコル等による、トラフィックを識別。
- Packet Sniffer (コンテンツ): データパケットをストリームに再構築し、ストリームのペイロードを監視して、トラフィックの種類を判断します。(例; SMTP, HTTP, IMAP, ファイルシェアリング、NETBIOS、等)
- Packet Sniffer(カスタム): ユーザー独自のルール(ヘッダーベース)を利用したデータパケットの識別。

センサー設定により、使用プロトコルによってトラフィックを識別する時、精密度を選択できます。また、フィルターをインクルード/エクスクルードして、IP アドレスやポート、特定パケットの監視をすることができます。

### ツール

Paessler Card Packet Counter: ローカルネットワークを通過するネットワークデータパケットについて、短期間の統計を表示します。

<http://www.paessler.com/tools/>

ご参照ください。

7.13 帯域監視センサーのタイプ比較

14.1 トップリスト

## 7.5 NetFlow Sensor Types (NetFlow センサータイプ)

NetFlow監視は、Ciscoのスイッチを利用したネットワークのドメインです。

注意: NetFlowセンサーは、トップリスト((Top Talkers, Top Connectionsなど)に対応しています。14.1 トップリストをご参照ください。

### NetFlow監視の動作

"IP アドレス"、または"アプリケーション"による帯域使用の計測する方法の一つとして、Cisco の NetFlow プロトコルがあります。Cisco の NetFlow プロトコルは通信量の多いネットワークに最適です。多くの Cisco ルーターやスイッチはこのプロトコルに対応しています。



NetFlow対応のCiscoデバイスは、内部でネットワークの帯域利用を追跡し、識別のためにPRTGシステムへ予め集約したデータを伝送します。こうすることで、PRTGの演算負荷は、減少します。こちらは、通信量の多いネットワークに推奨されます。

### NetFlow監視を選択する理由

NetFlow監視は、Ciscoスイッチを利用したネットワークのドメインです。これらのスイッチは、ネットワークの使用状況データのデータストリームを、データを分析するPRTG実行マシンに送るよう設定することができます。スイッチは、トラフィックデータの事前のアグリゲーションを実行しているため、PRTGへのデータフローは、監視されたトラフィックより小さくなっています。これによって、NetFlowは、ネットワークプロトコルとIPアドレスの帯域使用を識別する必要のある通信量の多いネットワークに最適となります。

### NetFlow監視のためのPRTGの機能

NetFlowは、Cisco製の帯域監視技術です。PRTGは、以下、2つのセンサーとNetFlow Version5を利用したフロー監視に対応しています。

- NetFlow: NETFLOW V5を使用したCiscoスイッチの監視
- NetFlow(カスタム): ユーザ設定可能なNetFlowセンサー

NetFlowセンサーを作成する前に、ユーザー側のスイッチ/ルーターでNetFlowを設定してください。NetFlowパケットがPRTGプローブの実行マシン送信されるよう、スイッチを設定してください。また、NetFlowポートとフローのタイムアウトを設定してください。これら2つの値は、PRTG内で新しいNetFlowセンサーを作成する際に定義しておく必要があります。必ず、

PRTGシステムのファイアウォールでNetFlowポートを開けておいてください。

### 制限

2008/2007年製の高性能PC(Dual Core, 2.5Ghz)では、1NetFlowストリームに対して約100,000フロー/秒の処理が可能です。複雑なフィルタを使用した場合は、値は下がります。例えば、約2,000フロー/秒送信するルーターに対して(ギガバイト/秒レベルの混合トラフィックで通信)、最大50個のNetFlowセンサーが正しく作動するように設定が可能です。PRTGは独自のNetFlow処理を内部で監視します。過負荷によりNetFlowパケットが処理されないと、PRTGプローブの健全性(Health)の減少が確認できます。

過負荷を感じた場合、複数のPRTGプローブを設定し、NetFlowストリームをそれらに分散することを検討して下さい。PRTGプローブにつき、400以上のNetFlowセンサー追加は、お勧めできません。

### ツール

Paessler NetFlow Generator: Netflow Generatorは、NetFlow互換機がなくてもNetFlow Version 5のデータストリームを作成することができます。PRTGのNetFlow機能や他のNetFlow互換プログラムを検証するのに最適なツールです。

<http://www.paessler.com/tools/netflowgenerator>

Paessler NetFlow テスター: NetFlow テスターは、コンピュータがCiscoルーターから受信した、全NetFlowパケットのデータをダンプします。NetFlowプロトコルに基づいた帯域監視設定のデバッグ時にご利用頂けます。

<http://www.paessler.com/tools/>

ご参照ください。

- 7.13 帯域監視センサータイプの比較
- 14.1 トップリスト
- Paesslerナレッジベース: Configuration Tips for Cisco Routers and PRTG (CiscoルーターとPRTG設定のコツ)

<http://www.paessler.com/support/kb/questions/20/>

## 7.6 SQL Server Sensor Types (SQL サーバーセンサータイプ)

SQLサーバーセンサーを利用して、最も一般的に実装されているMySQL, Microsoft SQL, Oracle SQLといったSQLサーバーをネイティブに監視できます。基本的に、これらのセンサーが監視するのは、いつデータベースサーバープロセスが処理要求を受け付けて処理したかどうかです。さらに、カスタムSQLコマンドを実行して戻り値をチェックすることが可能です。

PRTGは以下のSQLサーバーのネイティブ監視が可能です。

- Microsoft SQLサーバー: Microsoft SQLサーバーの接続を確認。
- MySQLサーバー: MySQLサーバーの接続確認。

- Oracle SQL サーバー: Oracle SQL サーバーの接続確認。

#### 全SQLセンサーにおける共通設定

- Database Name - データベース情報にアクセスするために、このフィールドには、データベースの名称か、データベースのパスを入力してください。
- User and Password - データベースログイン用にユーザー名とパスワードを設定してください。
- SQL Expression - データを取得する式を設定してください。カーソルが戻ると、最初の行だけを取得します。
- Result Set - このチェックボックスにチェックを入れると、SQL文は結果を戻します。そして、結果における最初の行の最初の列の値は、監視要求の戻り値として利用されます(例えば、極限值との比較など)。または、“変更された行 (affected rows) の数”が、監視要求の戻り値と見なされます。

#### MS-SQL センサーに関する注意事項

- SQL Server 2005、SQL Server 2000、SQL Server 7、MSDE に対応(サーバーにアクセスする PRTG プローブ実行機に、OLE DB のインストールが必要)
- インスタンス名 - 名前付きインスタンスにアクセスする場合、インスタンス名を設定します。それ以外の場合は、空欄にしてください。  
**注意:** データベースクライアントに SQLSERVER \ SQLINSTANCE という文字列を見かけることがあります。前半部分は、一般的なサーバー設定で設定されるサーバー名です。後半部分は、上記のインスタンス名です。センサー設定ページのインスタンス欄に、この形で、文字列を入力しないで下さい。後半部分のみ入力してください(バックスラッシュを除いて)。
- ポート - SQLサーバーが1433以外の固定ポートでインスタンスを実行している場合、ポート番号をこの欄で定義することができます。SQLサーバーがデフォルトの1433を使用している場合、或いは、ダイナミックポート設定がされている場合は、空欄にしておいてください。

#### Oracle SQL センサーに関する注意事項

- Oracle 10g、9i、8i、Oracle 7に対応(デフォルトのTCPポート設定は、1521にしてください)
- インターフェイス - Oracleは、サーバー接続の際、2つの方法に対応。直接TCP/IPで通信(SQL-NET)、或いは、Oracle Client Interface (OCI)経由。どちらか好きな用を選択して下さい。
- ポート - SQL-NETの場合、この欄に接続に使用するTCO/IPポートを設定してください。通常、デフォルト値は1521です。OCI接続の場合、ポートプロパティの設定は、無視してください。

#### My-SQLサーバーに関する注意事項

- MySQL Server 5.0、4.1、4.0、3.23に対応。

## 7.7 File Server Sensor Types(ファイルサーバーセンサータイプ)

ファイルサーバーの監視には、以下のセンサーが使用可能です。

- WMIディスクスペース：このセンサーは、WMI経由でディスクの空きスペースを監視します。(7.2 WMIセンサータイプ参照)
- WMIファイル：WMI経由でファイルを監視。(7.2 WMIセンサータイプ参照)
- Shareディスクスペース：SMB sharesの空きディスクスペースを監視。(Windows/Samba)
- ファイル：ファイルの存在、サイズ、作成時期、更新有無を監視。
- フォルダ：フォルダの存在、数、作成時期、サイズ、内容の更新有無を監視。

## 7.8 Mail Server Sensor Types(メールサーバーセンサータイプ)

メールサーバーで多くのセンサーを使用して、メールシステムの動作を確実にします。

### 標準Eメールプロトコル

- SMTP：メールサーバーでSMTPの可用性を監視(Simple Mail Transfer Protocol)。
- POP3：メールサーバーでPOP3の可用性を監視(Post Office Protocol V3)。
- IMAP：メールサーバーでIMAPの可用性を監視(Internet Message Access Protocol)。

### Eメール・ラウンドトリップセンサー

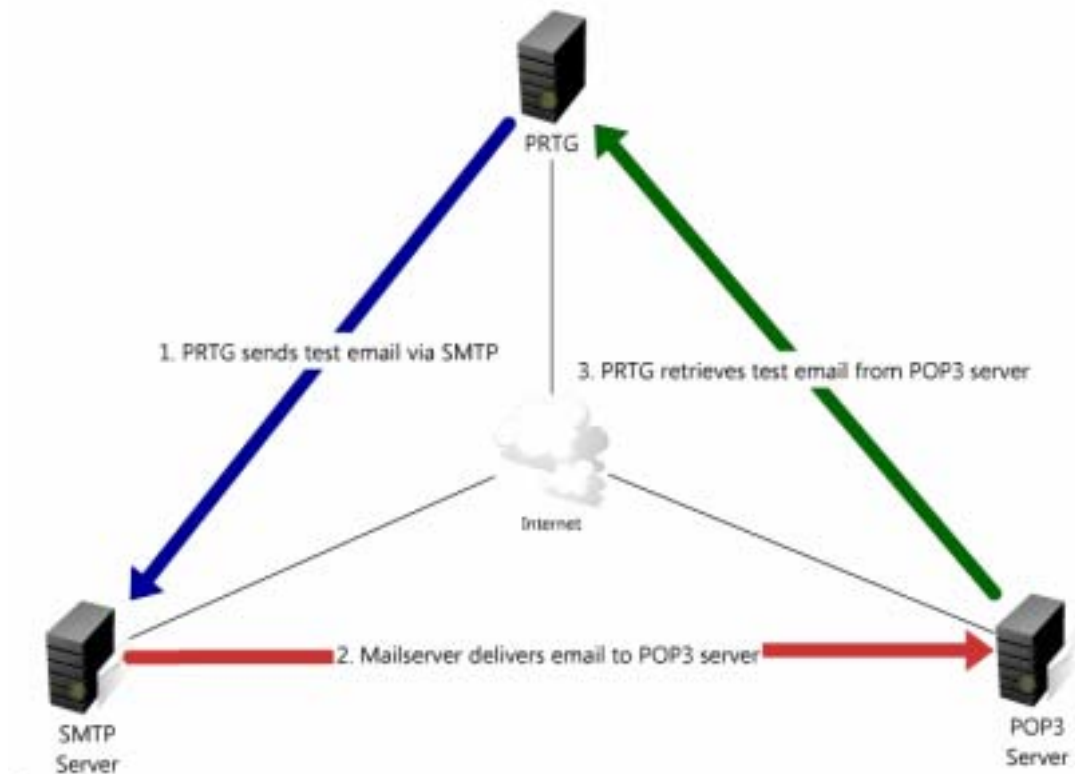
Eメール・ラウンドトリップセンサーは、Eメールのエンド・ツー・エンド伝達を確実にし、完全なEメール伝達システムの可用性やパフォーマンスを可能にします。このタスクのために、2つのセンサータイプがあります。

- SMTP & IMAPラウンドトリップセンサー
- SMTP & POP3ラウンドトリップセンサー

どちらも、初めはSMTPを使用してメールサーバーへメールを送ります。その後、そのメールが到着する前に、POP3かIMAPを用いてメールボックス内をスキャンします。グラフで設定例が表示されます。

- ステップ1：PRTGは、SMTPプロトコル経由で、メールサーバーまでEメールを送信します。(Eメールクライアントと同様)
- ステップ2：SMTPサーバーは、そのEメールをPOP3/IMAPサーバー(遠隔地、ローカルLANもしくは同一サーバー内のいずれにも設置可能)へ送信します。
- ステップ3：テストメールが到着するまでに、PRTGは、数秒間隔で、POP3/IMAPサーバーからEメールを受信します。

テストメールには、Eメールを識別するためのトピックに一意のコードが含まれています(例：“PRTG7 Roundtrip Mail: {6D136420-5A3E-46CF-871A-1DAF0C4F3D5D}”)



### 推奨設定

組織内外へのEメールの送受信の確認についてまとめると、次のようになります。

- メールシステムでのテスト用に専用のメールアカウントを作成
- メール全てを企業のメールアカウントに送信する外部メールアカウント(ホストメールサーバー、フリーメールなど)を設定
- LAN内のメールサーバーを利用して外部メールアカウントへメールを送信し、メールシステム上のメールボックスにメールが届いているか確認するためのPRTGラウンドトリップセンサーを設定

これによって、センサーが緑色に点灯している間、メールサーバー設定について次のような様々な面を監視可能です。

- メールサーバーが、SMTP経由でメールを受信すること。
- 外部へメールが送信されていること(インターネット接続サービス、MXルックアップサービスなど)。
- 外部メールサーバーからのメールが、ユーザーのメールサーバーへ送信されること(ユーザーのドメインのMXレコードが正しく、ユーザーのメールサーバーと外部とが通信可能であること、ユーザーのメールフィルタリングが作動していることなども含みます)。
- POP3(または、IMAP)を用いて、メールを受信できること。

### 結論

これら2つの新しいセンサータイプは、ユーザーのメールサーバーのメールの送受信を確実にを行う優れたツールです。標準的なSMTP、POP3、IMAPセンサーは、これらのサービスの可用性をチェックするだけですが、それらに比べて、この2つの新しいセンサータイプは、実際に、メールを最初のメールサーバーに受信するところから、最後のPOP3/IMAPサーバーがメールを送信するまでの全ての処理の監視を可能にします。

## 7.9 VMware Server Sensor Types (VMware サーバーセンサータイプ)

PRTGで、VMware ホストサーバーの重要なパラメータや、VMware で実行中のバーチャルマシンを監視できます。

センサータイプ:

- VMware ESX ホストサーバー: VMware ESX ホストサーバーの監視
- VMware バーチャルマシン: シングル バーチャルマシンの監視

ESX ホストサーバーセンサーが、VMware ESX3x サーバーを親デバイスとして、直接作動している場合、バーチャルマシンセンサーを以下2つの方法でご利用頂けます。

- サーバー上で実行中のバーチャルマシンの監視をするために、VMware ESX3x サーバーで直接通信するのに使用します。
- VMware バーチャルセンターを使って、通信するのに使用します。このバーチャルセンターで管理された全てのバーチャルマシンを監視します。こちらは、VMware サーバー2.x 上のバーチャルマシンとVMwareのVモーション機能をもつバーチャルマシンにのみ対応です。

VMware センサーに対して、PRTG はホストサーバーへ管理者 (Administrator) ログインを要求します。親デバイス、もしくはグループの、VMware クレデンシャルセクションへ上記のクレデンシャルを入力します。センサーは、これらの設定を継承します。

**注意:**

動作制限により、同じバーチャルサーバーへの問い合わせや同じユーザーアカウントを使用するVMware センサー数を20以下に留める事を推奨します。20以上センサーが必要な場合、2つ以上のユーザーアカウントをご使用頂くか、センサーを複数のプローブに振り分けて下さい。

VMware は VMware Inc.の商標登録です。

## 7.10 Internet Protocol Sensor Types (インターネットプロトコルセンサータイプ)

次のセンサータイプで、TCP や UDP ベースのさまざまなサービスを監視することができます。

- PING: 1つ以上のPINGを実行し、デバイスの可用性を監視したり、必要に応じてパケットロスパーセンテージを測定します。

- PORT: TCP ベースのネットワークサービスの可用性をチェックします。
- FTP: FTP サーバーの可用性を監視します。
- DNS: DNS(ドメインネームサービス)サーバーをチェックします。
- RDP(リモートデスクトップ): デバイスの RDP サービスが使用できるかどうかを確認します。

これら全てのセンサーは、プロトコル標準を使用しています。

HDD Health センサーは、プローブデバイス上でのみ使用可能で、物理ディスクドライブの様々なパラメーターを監視します。

## 7.11 Custom Sensor Types(カスタムセンサータイプ)

カスタムセンサーによって、設定された標準センサーではできない多くの監視タスクの実行が可能になります。SNMP、スニファ、NetFlow のパラメーター化されたバージョンとは別に、WQL (WMI Query Language)を使用したり、EXE ファイルをコンパイル、また、その他 Windows ソフトウェアの開発ツールを使用して、ユーザ独自のセンサーを作成することができます。

PRTG は、次の 4 つのカスタムセンサータイプに対応しています。

- EXE: カスタムプログラム (EXE、DLL) やスクリプト/バッチファイルを実行します。
- WMI カスタム: WQL (WMI Query Language) で書かれたカスタム WMI クエリを実行します。7.2 **WMI センサータイプ**を参照してください。
- SNMP カスタム: 特定の OID を監視します (センサーに OID を設定する必要があります)。7.1 **SNMP センサータイプ**を参照してください。
- パケットスニファ(カスタム): ユーザー定義ルールを用いてデータパケットを識別します。7.4 **Packet Sniffing(パケットスニフing) センサータイプ**を参照してください。
- NetFlow(カスタム): NetFlow センサーのユーザー設定バージョンです。7.5 **NetFlow センサータイプ**を参照してください。
- センサーファクトリー: 7.12 **センサーファクトリー**を参照してください。

### カスタム EXE/DLL/BAT/CMD/VBS/PowerShell /WQL Sensors

PRTG プローブを実行しているシステム上に特定のフォルダを作り、そこにファイルとしてセンサーを作成してください。(つまり、リモートプローブを使用している場合は、ファイルは、リモートシステムにコピーする必要があります。)

- 実行ファイル(EXE、.DLL)、バッチファイル(.CMD、.BAT)、VBS スクリプト(.VBS)、或いは、PowerShell スクリプト(.PS1)は、"PRTG Network Monitor¥custom sensors¥EXE"サブフォルダに作成してください。
- WQL スクリプトの.WQL ファイルは、"PRTG Network Monitor¥custom

sensors¥WMI WQL scripts"サブフォルダに作成してください。

これらのフォルダには、デモセンサーのサンプルがあります。上記フォルダにファイルを作成すると、カスタム EXE センサーや WMI カスタムセンサーの作成や編集ができ、ファイルリストから新しいファイルを選択することができます。

それからプローブがファイルをプローブシステム上で実行します。ローカルプローブは、ローカル PRTG コアサーバーシステム上でファイルを実行します。ただし、リモートプローブに関しては、ファイルは実際、リモートシステム上で実行されます。ユーザーのカスタムセンサーコードが他のファイル(DLLs, .NET framework, Windows PowerShell など)に依存している場合は、これらのファイルをプローブマシンに手動でコピー/インストールする必要があります。

詳細は、**14.7 カスタム EXE センサーのインターフェース定義**を参照してください。

パラメータフィールドには、次のプレースホルダーがあります。

- %host: デバイスの IP/DNS
- %device: デバイス名
- %probe: プローブ名
- %name: センサー名

#### 注意

- PowerShell スクリプトを実行する場合には、ファイルに署名するか、Powershell.exe のセキュリティポリシーを変更するかが必要です。
- カスタム EXE センサーの API インターフェースは、IPCheck Server Monitor 5 で提供されるカスタム EXE センサーと互換性があります。

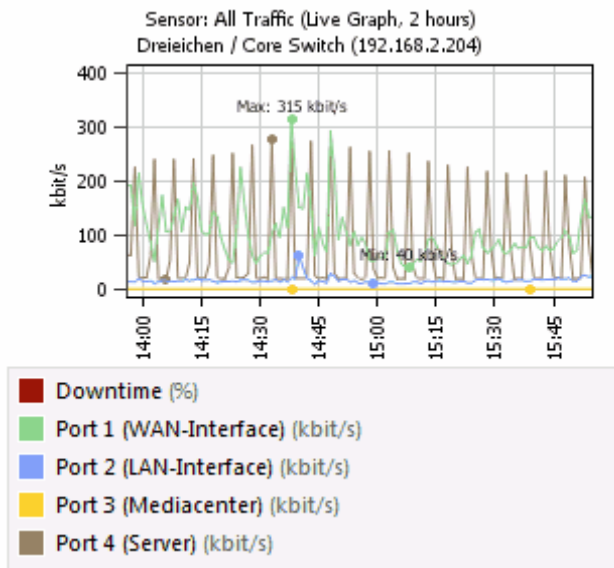
## 7.12 Sensor Factory (センサーファクトリー)

特別な機能をもつセンサーのことを "Sensor Factory" (センサーファクトリー) と呼びます。それによって、複数センサーからの測定結果を一つの新しいセンサーに統合することができます。

使用例は、次の通りです。

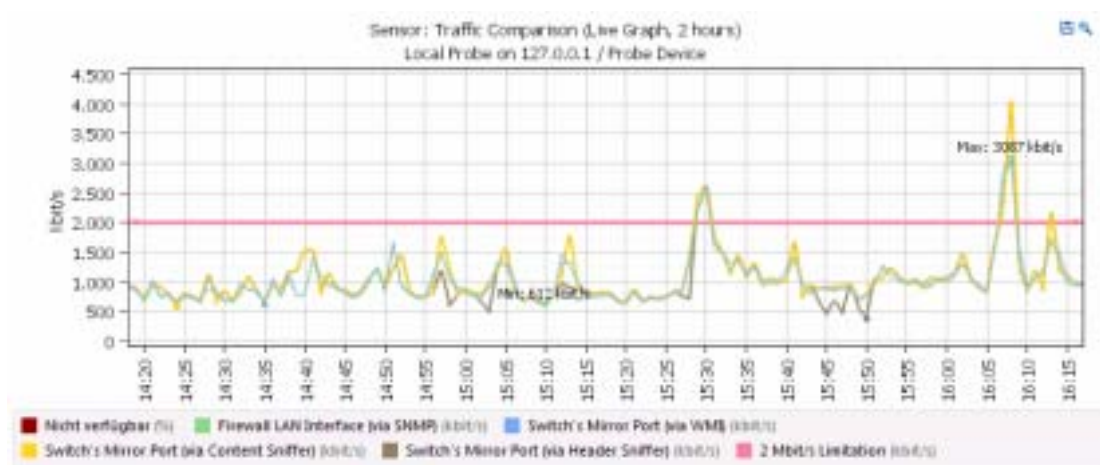
- 1つ/複数のセンサーの複数チャンネルを一つのグラフに表示。
- 1つ/複数のセンサーの複数チャンネルの値の和を算出(差、積、商も可能)
- 特定の縦軸に1つ/複数の折れ線や特定の1つ/複数の横軸を用いた表を作成。

4つの異なるセンサーからのデータを使用する4つのチャンネルをもつセンサーファクトリーのグラフです。



別の使用例です。

1つのデータ回線に対するSNMPセンサー、WMIセンサー、2つのパケットスニファセンサーの結果を比較したセンサーファクトリーです。横線は、2メガビット/秒です。



センサーファクトリーは、新しいセンサーを作成する際、"Custom Sensors"セクションにあります。

### チャンネル定義基本構文

センサーファクトリーセンサーの動作は、"Channel Definition" (チャンネル定義) と呼ばれるテキストフィールドで管理されています。チャンネル定義の基本構文は、次のようになります。

```
#<id>:<name>[<unit>]
```

```
<formula>
```

**74** PRTG Network Monitor 7.1 - ユーザーマニュアル

それぞれのチャンネルについて、#で始まる1つのセクションが使われます。こちらが2つのチャンネルを使った例です。

```
#1:Sample
```

```
Channel(1000,0)
```

```
#2:Response Time[ms]
```

```
Channel(1001,1)
```

パラメーターは、次の通りです。

- <id> は、一意の数字。(1以上)
- <name>は、チャンネルの名称です。(グラフや表に表示されます。)
- [<unit>]は、任意です(バイトなど)。指定がない場合は、自動で適合するユニット名が選択されます(推奨)。
- <formula>には、チャンネルを計算する公式が含まれます。

公式には、次の要素が使用できます。

- 基本演算子: + - \* / (例:3+5\*2)
- カッコ:( ) (例:3\*(2+6))
- 比較演算子: = (等しい)、< > (等しくない)、> (より大きい)、< (より小さい)、> = (より大きいか等しい)、< = (より小さいか等しい)。もし比較の結果が真であれば、値は1に、偽の場合は、0になります。デルタセンサーについては、速度が比較されます。
- 関数: channel,min,max,avg,percent

### channel() 関数

The channel() 関数によって、異なるセンサーのチャンネルからのデータを読み取ることができます。構文は、次の通りです。

```
channel(<SensorId>,<ChannelId>)
```

- SensorIDは、センサー"Overview"ページのセンサー名の中に表示されています。
- ChannelIDは、"Channels"ページ > "Edit Channel"セクションのそれぞれのチャンネルに表示されています。

例: センサー2001のチャンネル2のデータを読み込む。

```
channel(2001,2)
```

チャンネルは、測定値(例:PING ms)やデルタ値(トラフィック キロビット・秒)で表示されます。全ての統合がこの公式で可能なわけではありません。以下のことは、できません。

- 測定チャンネルとデルタの和/差
- 2つのデルタチャンネルの積
- デルタと測定チャンネルの比較

- 公式で、集合チャンネルのチャンネルを使用すること。

### min() and max() 関数

min() and max()関数は、2つの値の最大(最小)値を返します。構文は次の通りです。

```
min(<a>,<b>)
```

```
max(<a>,<b>)
```

aとbの値は数字、もしくは、channel()関数になります。

例:

```
min(10,5) -> return 5
```

```
min(channel(2001,1),channel(2002,1))
```

2行目は、センサー2001と2002のチャンネル1の最小値を返す、という意味です。

### avg() Function

avg() 関数は、2つの値の平均値を返します。(a+b) / 2と同じ意味です。構文は、次の通りです。

```
avg(<a>,<b>)
```

例:

```
avg(20,10) -> returns 15
```

### percent() function

値(チャンネルなど)の割合(%)を計算し、固定値と比較します。構文は次の通りです。

```
percent(<source>,<maximum>,<unit>)
```

<source>は、算出された割合です。通常は、channel()関数です。<maximum>は、百分率計算の限界値です。<unit>は任意で、最大値が与えられた<unit>のことです。この値は、最大値が増えれば、大きくなります。以下の定数を使用することができます(下表参照)。ゲージ(Pingなど)センサーや、デルタ(トラフィックセンサーなど)に適用できます。

以下は、最大帯域(100キロビット/秒)に対するトラフィックセンサーの割合の表示例です。

```
#1:Usage IN
```

```
percent(channel(2001,0),100,kilobit)
```

```
#2:Usage OUT
```

```
percent(channel(2001,1),100,kilobit)
```

もう一つは、200ミリ秒に対するセンサー値の割合の表示例です。

```
#1:Ping %
```

```
percent(channel(2002,0),200)
```

## 横線

channel() 関数を使わずに公式を使用してグラフに横線を加えることができます (固定値を返します)。この場合、座標軸を設定する必要があります。以下の定数を使うことができます。

例:

```
#1:Line at 100ms[ms]
100
#2:Line at 50 kbit[kbit/s]
50
#3:2 Mbit/s [kbit/s]
2000
```

## 定数

以下の定数は、計算に使用できます。

- one = 1
- kilo = 1000
- mega = 1000 \* kilo
- giga = 1000 \* mega
- tera = 1000 \* giga
- byte = 1
- kilobyte = 1024
- megabyte = 1024 \* kilobyte
- gigabyte = 1024 \* megabyte
- terabyte = 1024 \* gigabyte
- bit = 1/8
- kilobit = kilo / 8
- megabit = mega / 8
- gigabit = giga / 8
- terabit = tera / 8

## チャンネル設定

色、線の太さ、警告/エラーの限界などは、センサー作成後、"Channels"タブで編集できます。どのセンサーについても同様です。通知を送信するためにトリガーを使うこともできます。

## その他

- データは、可能であれば、センサーの過去データを用いて、即計算されます。
- センサーファクトリーセンサーのライブデータ表示は、全ての使用チャンネルのデータを待つため、遅れる場合があります。
- 新しいチャンネルを作成する際、異なる監視間隔のセンサーのチャンネルを使用することができます。ただし、ソースセンサーやセンサーファクトリーには同じ値を使用することをお勧めします。

- アグリゲーションセンサーでアップタイム/ダウンタイムの合計の計算はできません。
- センサーファクトリーの範囲は、全てのセンサーファクトリーチャンネルの最小範囲で定義されます。
- センサーファクトリーチャンネルの範囲は、計算で使用されるセンサーの加重平均の範囲です。
- センサーファクトリーセンサーのダウンタイムチャンネルは、全ての使用チャンネルのダウンタイムの平均で定義されます。

### 7.13 Comparison of Bandwidth Monitoring Sensor Types (帯域監視センサータイプの比較)

以下の表は、帯域監視で使用できるPRTGの4つのメソッドの違いを表しています。

	WMI	SNMP	Packet Sniffing (パケットスニフing)	Netflow
設定	普通	易	易～難(フィルタールールによる)	難(スイッチの設定など)
トラフィックのフィルタリング	なし	なし	あり	あり
プロトコルやIPアドレスによる帯域使用の識別	なし	なし	あり	あり
トップリストの表示 (TopTalker、トップ接続、トッププロトコルなど) (V7.1)	なし	なし	あり	あり
IPによる帯域使用のフィルタリング	なし	なし	あり	あり
MACアドレスによる帯域使用のフィルタリング	なし	なし	あり	なし
物理ネットワークポートによる帯域使用のフィルタリング	あり	あり	なし	なし
帯域使用以外のネットワークパラメーターの監視	あり	あり	なし	なし

帯域使用以外のネットワークパラメーターの監視	あり	あり	なし	なし
PRTG実行マシンのCPU負荷	低	低	高(トラフィック量による)	高(トラフィック量による)
監視における帯域使用の超過	小	小	なし(モニタリングスイッチポート使用時間をのぞく)	トラフィックによる

# Part

# VIII

## Notifications (通知)

## 8 Notifications (通知)

“Notifications”は、遅い、或いは停止したセンサーや閾値に達したときなど、定義された状態、をPRTGが検出した場合に、ユーザーに警告を送る際に使われます。通知は無制限に定義でき、Eメールや、ポケットベル、SMSメッセージ、インスタントメッセージ、実行プログラム(EXEファイル/バッチファイル)やHTTPリクエスト、といったネットワークブロードキャスト(NET SEND)、サウンドファイル再生、Windowsイベントログエントリーなどの様々な通信チャンネルの一つ、もしくは複数の使用が可能となります。

通知は、次の場合に実行されます。

- センサーのステータスが変ったとき(センサーのダウン/アップ、レスポンスの遅延、センサーがステータスの異常を表示した場合など)
- 測定値が、ある閾値に到達した場合(30分以上の間に応答時間が1000ミリセカンドを超える場合など)
- 速度が、ある閾値に到達した場合(5分以上の間に1メガビット/秒を超える場合など。トラフィックセンサーのみ。)
- データ量が、ある閾値に達した場合(24時間の伝送量が1ギガバイトを超える場合など。トラフィックセンサーのみ。)

通知は、次の手段で送信されます。

- Eメール: PRTGが、ビルトインメールサーバーを提供(メール送信にMXレコードを使用)、もしくは、使用できるSMTPリレーを用います。
- SMS/ポケットベルのメッセージ(第三者のサービス経由)
- ネットワークブロードキャスト(注意: NetSendは、Windows Vista/Windows Server 2008には対応していません)
- インスタントメッセージ(ICQ, MSN, Yahoo, AIM)。
- HTTPリクエスト
- SNMPトラップ
- シスログメッセージ
- 外部プログラムやバッチファイルの実行
- PRTGコア実行システムの外部スピーカーを経由したサウンド(サウンドカードが必要)
- ローカルシステムログへのエントリーの書き込み

通知には、次のような重要なセンサー情報が含まれています。

- 直近のエラーメッセージ
- 直近の成功した/失敗したリクエスト
- ダウンタイム合計
- アップタイム合計
- 最近のセンサー履歴

**81** PRTG Network Monitor 7.1 - ユーザーマニュアル

- Eメールテキスト、SMSメッセージなど(プレースホルダーを使ってユーザー編集が可能です。)

**【事前に確認してください - 通知設定の確認について】**

通知設定通知の中には、管理者による追加設定が必要な場合があります。13.6 通知システムセットアップを参照してください。

**通知の作成**

通知の確認や編集には、メインメニューから、"Setup\Notifications"を選択します。編集する通知の名前をクリックするか、新規作成の場合は、"add notification"をクリックしてください。

Basic Notification Settings

Notification Name: Notification

Status:  started  paused

Schedule: None

Postpone:  No  Yes

Access Rights

User Group	Rights
PRTG Users Group	None
readonly user	None
testusers	None

Send Email

Add Entry to Event Log

Send Network Broadcast (NET SEND)

Send Syslog Message

Send SNMP Trap

Send ICQ Message

Send MSN Message

Send Yahoo Message

Send SMS/Pager Message

Execute HTTP Action

Execute Program

Play sound file

Save Cancel

チェックボックスにそれぞれチェックすることで、一つ、もしくは複数の通信タイプが可能です。それから、それぞれに固有の設定を決めていきます。

## トリガー作成によるセンサー/通知接続

通知は、トリガーによって送信されます。PRTGは4つのトリガータイプに対応しています。

- ステータストリガー：センサーがUP/DOWN/UNUSUAL状態になった場合、通知が送信されます。
- スピードトリガー：トラフィックセンサーが所定の時間内に所定の帯域限界に達した場合、通知が送信されます。
- ボリュームトリガー：トラフィックセンサーが所定の時間に、所定の容量限界に達した場合、通知が送信されます。
- 閾値トリガー：所定量がセンサーによって測定されたとき、通知が送信されます。

通知についてのトリガーをグループ或いはデバイスレベルで定義することを推奨します。センサーはこれらの設定を継承します(4.3 設定の継承を参照)。こうすることで、ただ単にグループレベルの通知設定を変更するだけで、複数のセンサーの設定を変更できます。

通知設定の編集は、グループ/デバイス/センサーの"notifications"タブで行います。

The screenshot displays the 'Notifications' configuration page in PRTG Network Monitor. It features a navigation bar at the top with tabs for Overview, 48 Hours, 30 Days, 365 Days, Alarms, Log, Settings, Notifications, Comments, and History. The main content area is divided into four sections for different trigger types:

- State Trigger(s)**: A table with columns for Condition, Latency (sec.), On Notification, Off Notification, Exc. Latency (sec.), Exc. Notification, and Repeat every (min.). A row is shown with 'Down' as the condition, '60' as latency, and 'Mail to Admin' for both on and off notifications. A 'Delete' button is present for this row. Below the table is an 'Add State Trigger' button.
- Speed Trigger(s)**: A table with columns for Channel, Condition, Value, Scale, Time, Latency (sec.), On Notification, and Off Notification. The first row is labeled '(no trigger defined)'. Below the table is an 'Add Speed Trigger' button.
- Volume Trigger(s)**: A table with columns for Channel, Value, Scale, Period, On Notification, and Off Notification. The first row is labeled '(no trigger defined)'. Below the table is an 'Add Volume Trigger' button.
- Threshold Trigger(s)**: A table with columns for Channel, Condition, Value, Latency (sec.), On Notification, and Off Notification. The first row is labeled '(no trigger defined)'. Below the table is an 'Add Threshold Trigger' button.

At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons.

それぞれのタイプについて要望に応じたトリガーを追加することができます("DOWN"イベ

ントに対してトリガーを1つ追加、また"UNUSUAL"イベントに対して1つトリガーを追加するなど)。Add Triggerをクリックして、編集欄へ入力後、Saveをクリックします。

トリガーの編集には、以下の設定があります。

- レイテンシー:レイテンシーは所定の時間で通知を遅らせる場合に使用します。例えば、サーバーやサービスで処理ミスから復旧する時間を与える場合や、データ回線が3秒間オフラインとなったことによって、通知が大量に送られてくるのを避ける場合などです。例として、トリガーに60秒の待ち時間を設置すると、通知は、障害が61秒間続いた場合に送信されます。
- オン通知:この通知はトリガーが有効になった場合に送信されます。("down"設定のステートトリガーのセンサーが、オフになった場合など)
- オフ通知:この通知はトリガーが無効になった場合に送信されます。("down"設定のステートトリガーのセンサーが、オンになった場合など)

### エスカレーション通知

エラーが一定時間解決されなかった場合、エスカレーション通知という追加通知を送信します(例:受信者リストの追加)。いつエスカレーションを送信するかを管理するレイテンシータ임을設定することができ、任意の時間(分)ごとにエスカレーションメールを再送することも可能です。

- エスカレーションレイテンシー:ここで設定した時間が経過した後、エスカレーション通知が送信されます。
- エスカレーション通知:送信される通知のことです。
- 再送間隔(分):この値が0でなければ、通知は一定間隔で再送されます。

### 補足

- 13.3 アカウント設定-通知
- 13.6 システムセットアップ-通知

# Part

# IX

## Maps (マップ)

## 9 Maps (マップ)

PRTGのマップ機能はユーザーが最新の監視ステータス情報を使って、ユーザーがカスタマイズしたレイアウトでWebページを作成することができる独自の概念です。マップを使用することで、可能性が無数になります。例えば、この機能は、次の用途に用いることができます。

- マップ上にそれぞれのデバイスのステータスアイコンのオーバーレイを使ってネットワークマップを作成
- ネットワークオペレーションセンタースクリーン上に表示される、"dashboard"ビューを作成
- イン트라ネット上にクイックネットワークオーバービューを作成し、従業員が管理しやすい一目でわかる情報を提供
- 監視設定の中で最重要センサーのカスタムビューを作成
- 特定のグループ/デバイスのセンサーでトップ10リストを作成

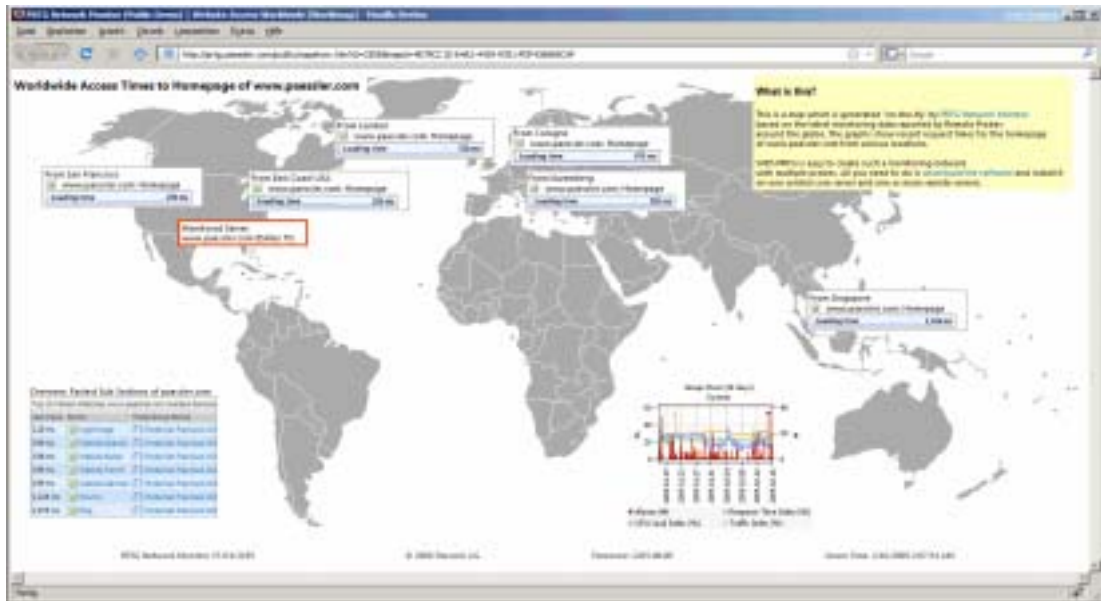
技術的に、マップは通常のWebページで、以下の内容を含みます。

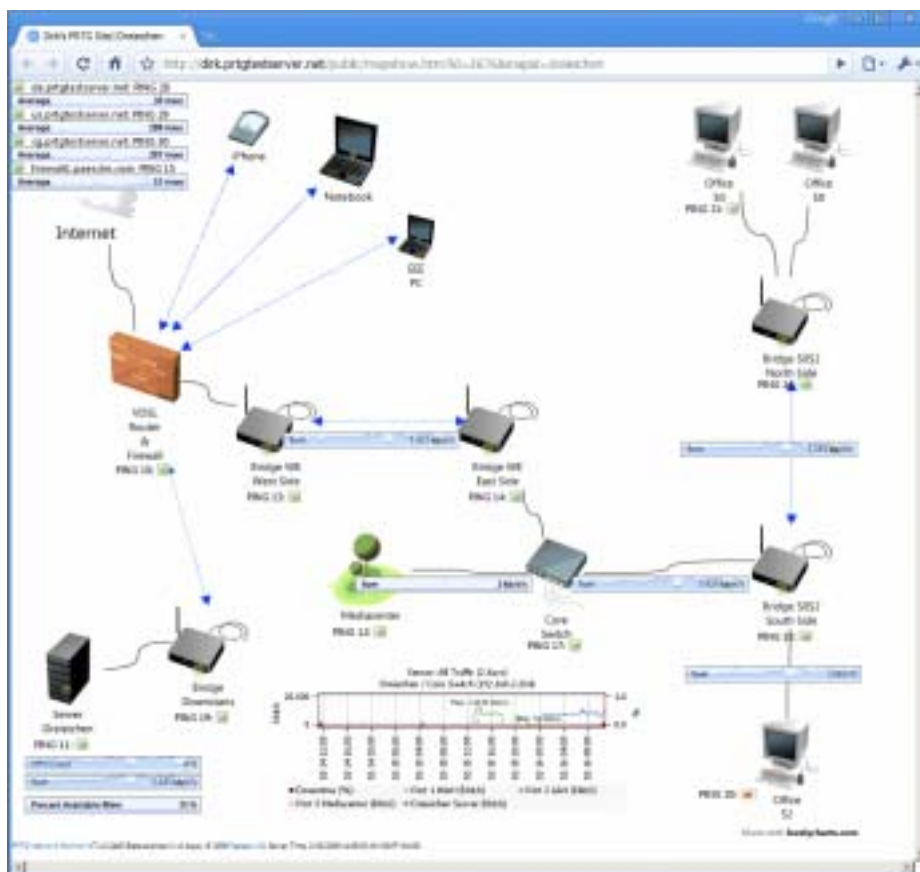
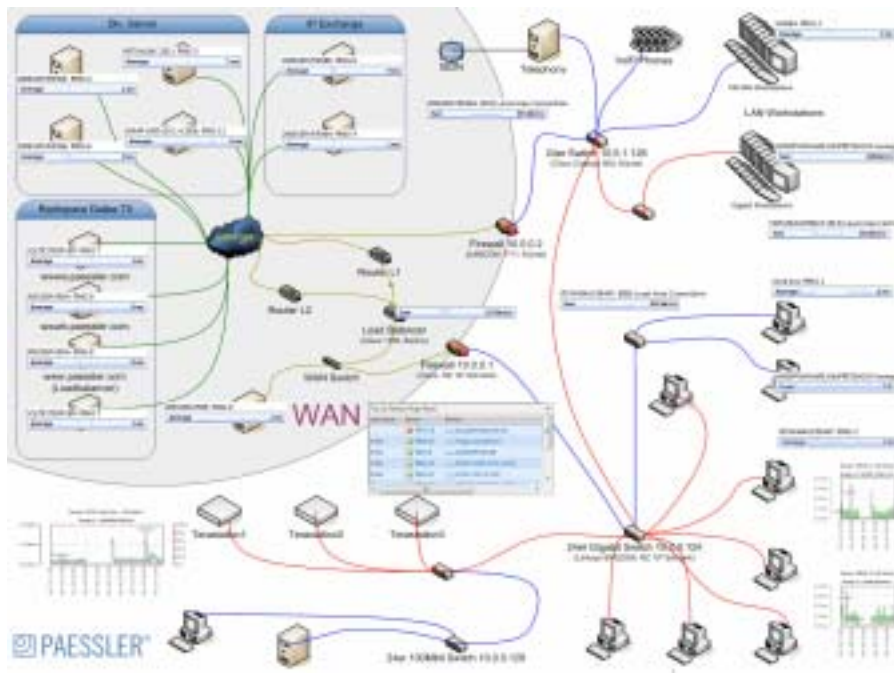
- オプションルバックグラウンドイメージ(PNG/GIF/JPGファイル、企業ロゴやネットワークイメージなど)
- マップアイテム(センサーステータスアイコン、グラフ、センサーリストなど)

マップの大きさを設定することも可能です。AJAXベースのマップエディターを使用して、アイテムをマップ上の好きなところに配置することができ、アイテムの大きさを変えることもできます。マップはそれぞれ固有のURLをもちます。マップにアクセスしたいユーザーは、PRTGで設定したアカウントを使うか、"Public Map"機能が有効の場合は、マップの"public URL"にアクセスするかのどちらかになります。パブリックマップには、URL上に一意のアクセスキー("Map ID")があり、マップを不本意な訪問者から保護しています。

### サンプルマップ

ライブ監視データのサンプルマップです。





**Step 1: 新規マップの作成**

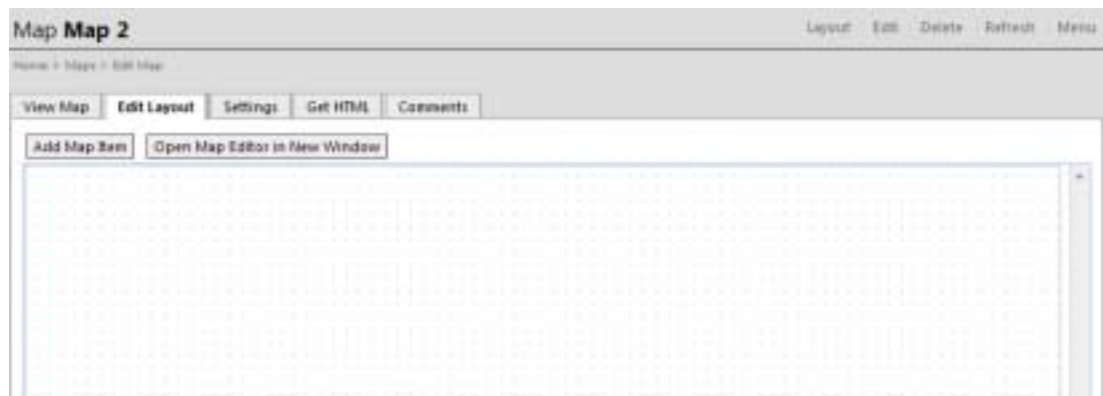
はじめに、"Map:Add New Map"をメインメニューから選択します。

The screenshot shows the 'Add Map (Step 1 of 2)' configuration form. It is divided into three main sections: 'Map Name', 'Map Layout', and 'Public Access'.  
1. **Map Name**: A text input field labeled 'Map Name' contains the text 'Map 5'. A help text to the right says: 'Choose a new name of your choice to describe the Map.'  
2. **Map Layout**: This section contains three fields: 'Map Width' with the value '800', 'Map Height' with the value '600', and 'Background-Image (optional)' with a 'Choose File' button and the text 'No file chosen'. Help text for width and height says: 'Please specify the width/height of the map in pixels.' The help text for the background image says: 'Choose a file to be used as background for your map. This can be a JPG, PNG or GIF image. (Width must be below 2 MB)'.  
3. **Public Access**: This section has two radio button options. The first is 'No Public Access' (selected), with the description 'This map will not be accessible without a login'. The second is 'Allow Public Access', with the description 'This map will be viewable without a login if the user enters the correct URL'. A help text to the right says: 'You can choose between two options: Only allow users that are logged into PRTG to view the map or allow any user to access the map. If he knows the correct URL.'  
At the bottom, there are two buttons: 'Continue to step 2 >' and 'Cancel'.

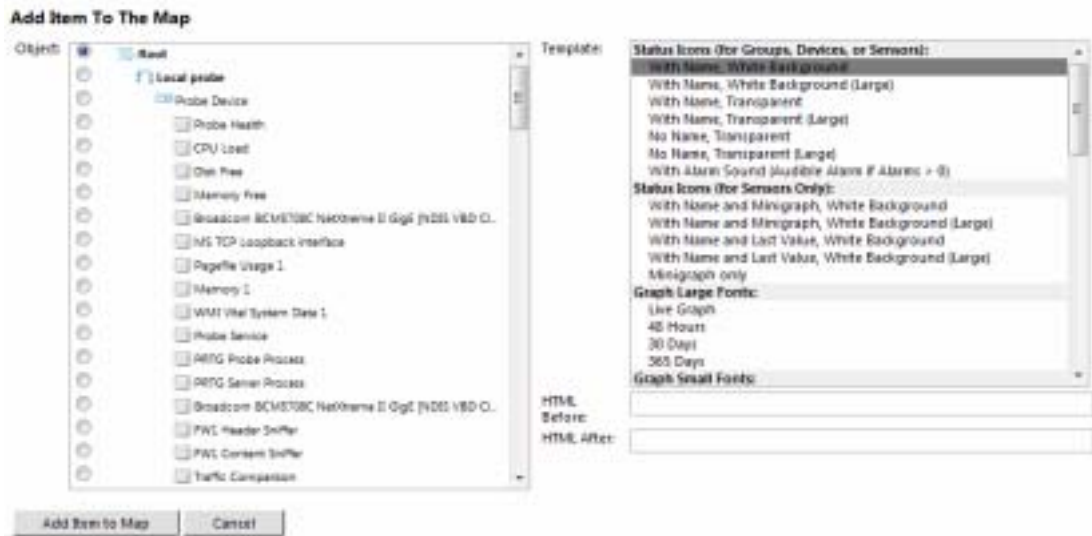
必要な項目を入力し、任意で背景を選択します。PRTGのユーザーアカウントを持たない人もマップの閲覧ができるようにするには、"Allow Public Access"を有効にしてください。"Continue to Step 2"をクリックすると、新しいマップに進みます。

### Step 2: マップにアイテムを追加

"Edit Layout"をクリックして、マップエディターを有効にします。



マップにアイテムを追加する場合は、"Add Map Item"をクリックします。



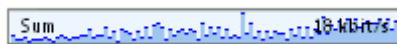
センサーツリーからグループ/デバイス/センサーを選択し、下のリストからマップアイテムテンプレートを選びます。任意で、マップ要素の前後にユーザー独自のHTMLコードを追加することもできます。

40種類以上のマップアイテムテンプレートが使えます。基本的なものは、次の通りです。

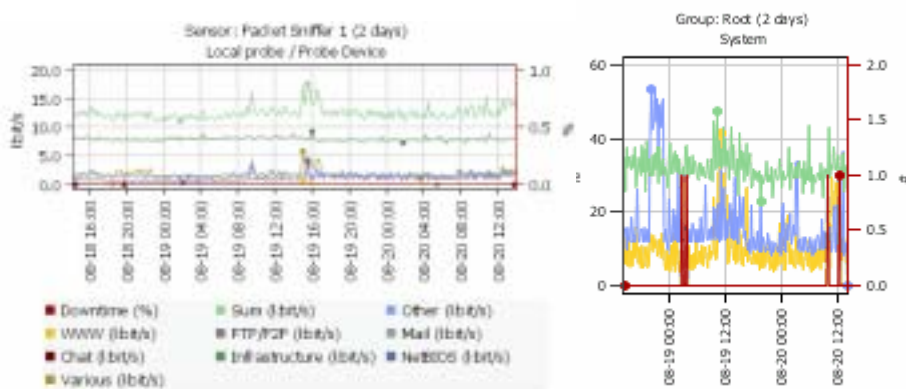
- ステータスアイコン

Root: 1 1 167 6

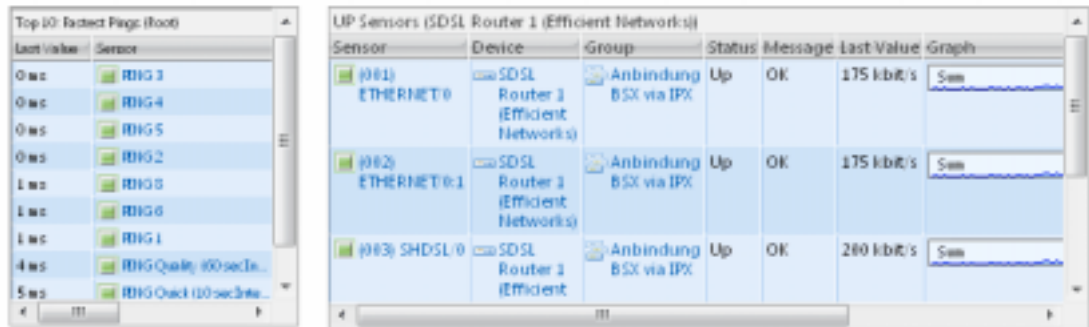
- ミニグラフ (センサーのみ)



- グラフ

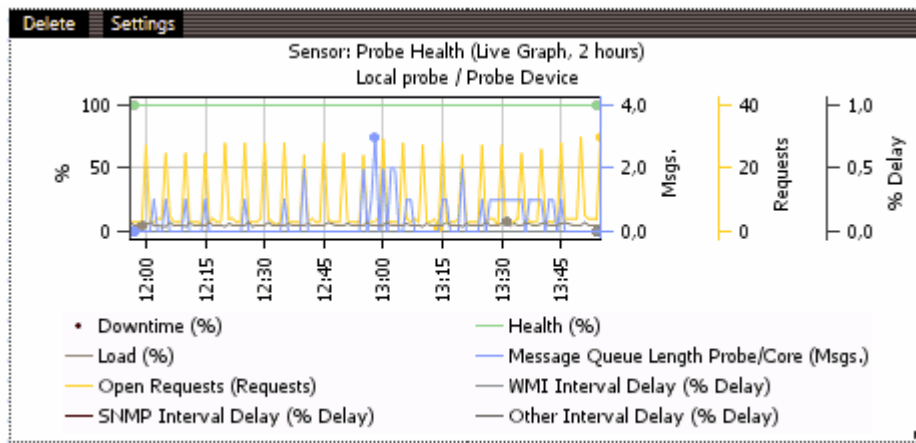


- 表

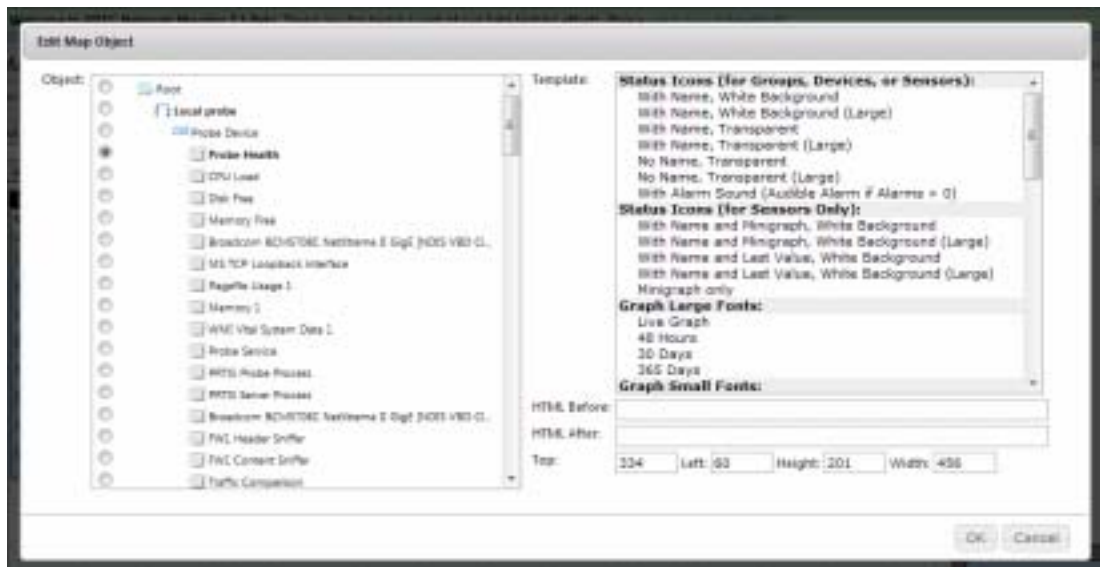


### Step3: マップアイテムの移動と編集

マップにアイテムを追加したら、次のように修正することができます



- 一番上の黒い"grip bar"をクリック&ドラッグして、アイテムを移動。
- 右下隅の小さい矢印をドラッグして、サイズの調整。
- "Delete"をクリックして、アイテムを削除。
- "Settings"をクリックして、アイテム設定の編集。関連した監視アイテム、テンプレート、HTML、位置や大きさを変更できます。



#### Step 4: マップの表示と共有

"View Map"をクリックすると、最終レイアウトを確認できます。

PRTGの外からマップを利用する場合は、次の2つから選択する必要があります。

- オプション1: マップのある web ページにリンクを張る
- オプション2: IFRAME を使用して、他の web ページ内にマップを表示する。

必要な URL、HTML コード、詳しい方法については、"Get HTML"をクリックしてください。

# Part

# X

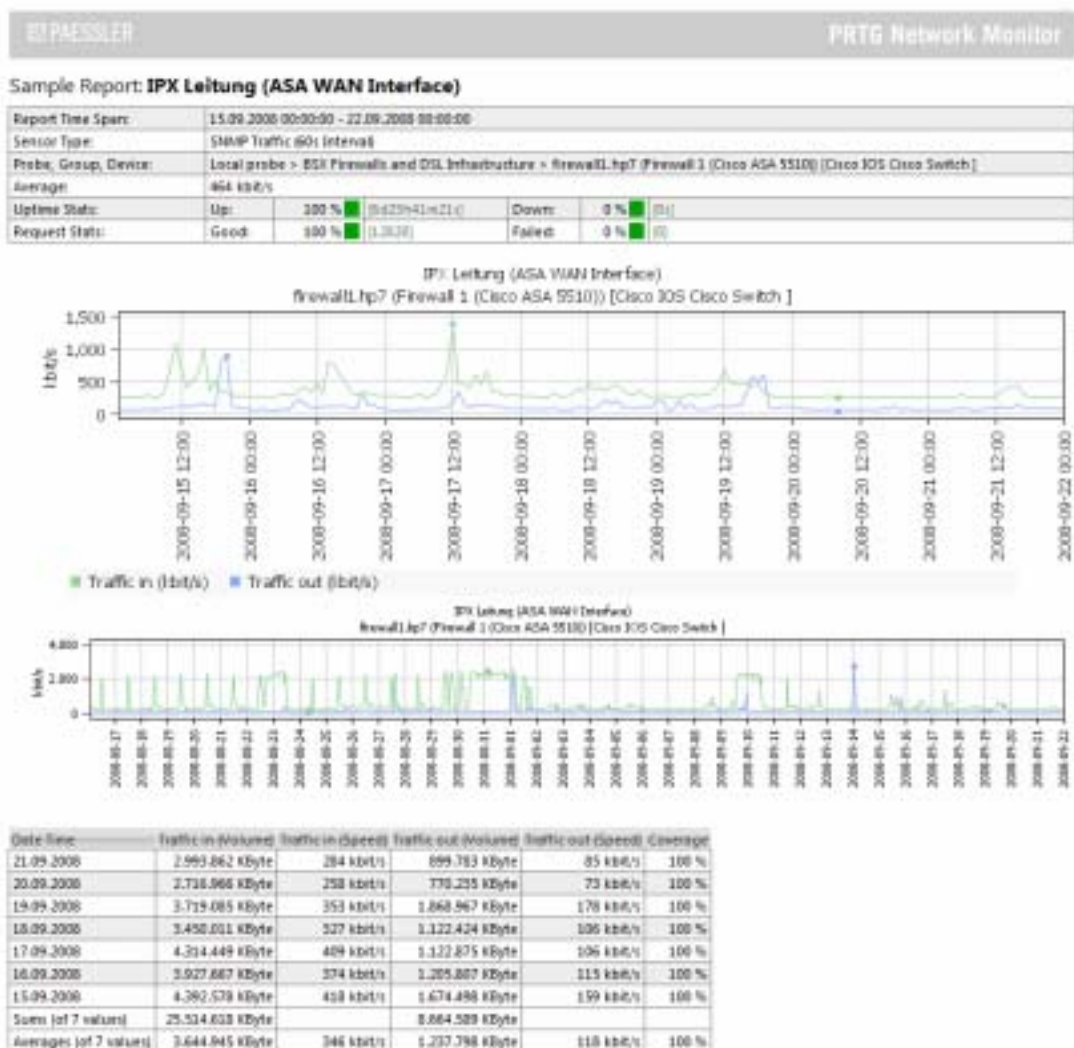
## Reports (レポート)

## 10 Reports (レポート)

レポートは、特定の期間(1~複数日、1ヶ月、1年などといった)にわたる監視結果の履歴を分析するのに用います。

PRTG では、ad-hoc に対応する高性能のレポートエンジンや、PDF フォーマットで定期的なレポート作成が可能です。レポートは、オンデマンドで実行でき、定期的にも実行することも可能です(1日1回など)。レポートは1つもしくは複数のセンサーについて作成できます。レポートの内容やレイアウトは、レポートテンプレートで独自に変更でき、全てのセンサーについてのレポートで統一されます。

以下は、1つのセンサーのサンプルレポートです。2つのグラフ(今月のグラフと、過去365日のセンサー履歴のグラフ)とデータテーブルです。



レポートの作成には、3つのステップがあります。

### Step 1: レポート設定

はじめに、メインメニューより"Reports/Add Report"を選択します。

#### Add Report

Home > Report > New object

---

##### Basic Report Settings

Report Name	Report	Please choose a descriptive name
Template	<please select a file>	Please choose a report template from the list of available templates. There are templates that offer optional data tables to the graphs. You also specify the graph/calculation intervals by selecting a template. Note: You can edit the HTML templates in the "webtools/reporttemplates" subfolder of your PRTG installation.
Timezone	(GMT+01:00) Amsterdam, Berlin, Bonn, Rome, Stockholm, Wien	Timezone setting for all data regarding this report. This includes schedule dates, report timestamps and dates in tables/tables.
Paper size	Letter	Please specify the paper size for which the report shall be formatted.
Orientation	Landscape	Please specify the paper orientation for which the report shall be formatted.

---

##### Sensors ("What sensors will be included in the report?")

Add Sensors Manually	There are too many sensors to show here. Please edit sensors and channels for this report on the tab "Select sensors manually" later	When selecting sensors manually you can also select/deselect individual channels of each sensor.
Add Sensors by Tag	<input type="text"/>	Enter tags to add all sensors from the sensor tree to the report which have one of the tags. Tip: Tags are inherited from parent objects. i.e. If you enter a specific tag into a group's tag setting and into the report setting, all sensors of that group will be included in the report - additionally to the sensors selected manually. Use spaces to separate the filter tags.

---

##### Schedule ("When will this report be run?")

Report Schedule	<input checked="" type="radio"/> No schedule (Run interactive/on-demand only) <input type="radio"/> Every Full Hour <input type="radio"/> Every day at a specific hour <input type="radio"/> Every specific day of a week <input type="radio"/> Every specific day of a month <input type="radio"/> Every specific date	You can create reports just for manual "on-demand use" or automatically every hour, day, day of week, day of month or a specific date. If you choose scheduled processing you will receive a ToDo email everytime the report is run.
Scheduled Processing	<input type="radio"/> Save report to disk and send it by email <input checked="" type="radio"/> Save report to disk only <input type="radio"/> Send report by email only	When PRTG runs the report due to a schedule it can simply email the report to an email address or write the PDF file to the disk or both.

---

##### Period ("What time span will the report cover?")

Reported Period	<input type="radio"/> Current <input checked="" type="radio"/> Previous	Specify which period it to be reported. Please choose between daily, weekly, monthly or yearly reports. Examples: Current is "today" for daily reports, "current month" for monthly reports. Previous means "yesterday" for daily reports, "last month" for monthly reports.
Report Period Type	<input type="radio"/> Day <input checked="" type="radio"/> Week <input type="radio"/> Month <input type="radio"/> Year	
Week Period	Monday-Sunday	

設定が完了したら、"Save"をクリックしてください。

### Step 2: オブジェクト/チャネルリストの編集

次のページで、レポートに含めるグループ/デバイス/センサー/チャネルのリストを編集

## 95 PRTG Network Monitor 7.1 - ユーザーマニュアル

することができます。

The screenshot shows the PRTG Network Monitor interface. The top section is titled "Select Sensors Manually" and displays a list of sensors for a "Probe Group Device". The list has columns for "Object", "Sensor Channel Selection", and "Actions". The "Object" column lists various system metrics like "Memory Free", "Broadcom BCM5700C NetXtreme 2 G...", "MS TCP Loopback Interface", "Pagefile Usage 1", "Memory 1", "Probe Service", "PRTG Probe Process", "PRTG Server Process", and "Header Packet ASA". The "Sensor Channel Selection" column shows checkboxes for various channels like "Percent Av", "Available 1", "Downtime", "Traffic in", "Traffic out", "Packets", "Sum", and "Total". The "Actions" column has a "Delete" button for each sensor.

Below this is a section titled "Add Sensors Manually" with a search box. It shows a list of 364 available sensors. The "Object" column lists sensors like "Probe Device", "Probe Health", "CPU Load", "Disk Free", "Memory Free", "Broadcom BCM5700C NetXtreme 2 G...", "MS TCP Loopback Interface", "Pagefile Usage 1", "Memory 1", "VMW VM System Data 1", and "Probe Service". The "Actions" column has an "Add" button for each sensor.

チェックボックスで、センサーの個々のチャンネルを有効/無効にすることができます。"Delete"をクリックすることで、レポートからオブジェクトを削除することができます。レポートにさらにオブジェクトを追加する場合は、下半分の全センサーのリストから一つ選択し、"Add"をクリックしてください。特定のセンサーを見つける場合は、表のページング機能を使うか、検索ボックスに検索語を入力して"Search"をクリックしてください。

### Step 3: インタラクティブ形式のレポート実行

"Run Now"タブをクリックし、レポートを実行します。

希望の設定を選択し、"Run Report"をクリックします。

- HTML レポートは、すぐに表示されます。
- PDF レポートは、バックグラウンドで作成され、完了すると、ToDo と一緒にメール受信します。

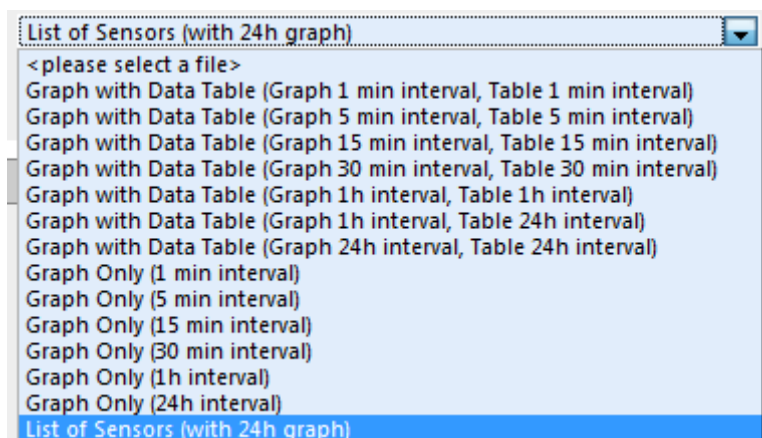
#### Step 4: 過去のレポートにアクセス

"Stored Reports"タブで、ディスク上に保存された過去のレポートにアクセスできます。

#### レポート設定の編集

レポートを設定するには、次の主な設定を編集する必要があります。

- 名称: 内容がよくわかる名称を選んでください。
- テンプレート: 使用できるテンプレートのリストから選択できます。このリストには、グラフと一緒にデータテーブルも提供するテンプレートが含まれています。テンプレートを選択することで、グラフ作成/計算間隔を指定することができます。注意: PRTG 設定の "website/reporttemplates" サブフォルダで \*.htm テンプレートの編集が可能です。



- レポートタイプ: 毎日/毎週/毎月/毎年のいずれかを選択して下さい。レポート

に現在のデータを含めたい場合は"Current"を選択し(毎月 20 日に実行されるマンスリーレポートは、その月の 1 日 ~ 20 日のデータを反映します)、それ以外は、"previous"を選択してください(そうするとマンスリーレポートは、常に前月の全データを反映します)。

- センサー: レポート対象のセンサーを選択してください。(注意:500 センサー以上ある場合は、レポート作成中にセンサーを追加することができません。後で追加してください。)
- スケジュール: 手動の"on-demand use"か、毎時間/毎日/毎週/毎月/もしくは指定した日付での自動作成かのいずれかで、レポートを作成することができます。
- 処理: PRTG は、任意のアドレスにレポートをメール送信したり、PDF ファイルをディスクに保存したり、あるいはその両方を行うことができます。

自動処理を選択した場合は、ToDo メールをレポートが実行されるたびに受信することになります。

# Part

# XI

**Todos (Todo)**

## 11 Todos (Todo)

Todo("To Dos")は、PRTG において、処理に注意を要するイベントが発生した場合、管理者であるユーザーにタスクを引き継ぐ方法です。

新しい Todo は、次のような状況が発生した場合に表示されます。

- オートディスカバリーが新しいデバイスを検知したり、新しいセンサーを作成したことを、ユーザーに知らせる場合。
- 接続されていなかったプローブが接続したことを管理者に知らせる場合。
- PRTG のビルトインチェックが、Paessler 社からソフトウェアの新しいバージョンのリリースを検知した場合。
- PDF レポートが作成され、閲覧可能になったとき
- サーバーシステムに深刻な障害が発生した場合 (システムの空きディスク容量がなくなった場合やライセンス障害など)

新しい Todo が作成されると、管理者に対応を要求するメールが送信されます (システム設定で自動メール通知を無効にすることができます)。Todo は、確認が完了するまで ("acknowledge" がクリックされるまで) リストに残っています。

メインメニューの "Todos" をクリックすると、全ての Todo のリストが表示されます。

Date Time	Object	Status	Priority	Message	Links
16-02-2009 13:14:03	Probe on Virtuozzo	New Probe	5	A new probe has connected: Probe on Virtuozzo (10.0.10.23426)	Go there Acknowledge
16-02-2009 11:27:22	Root	New Version	4	Software update available for PRTG Network Monitor: Recommended update V7.0.9.2048 is a maintenance release covering multiple bugfixes, particularly covering a number of WMI issues. Please visit www.paessler.com/prtg/download to download the latest version and to view the change log! You are using V7.0.0.270, the new version is V7.0.9.2048. Visit the Paessler website	Acknowledge
31-01-2009 00:03:39	Root	SMTP Configuration	5	E-Mail via MX: Sending E-Mail via MX failed. Please consider using a SMTP Server Configuration	Acknowledge

注意: Todo メニューから該当するアイテムを選択すると、すぐに全ての Todo を確認することができます。

# Part

# XII

## User Management (ユーザー管理)

## 12 User Management (ユーザー管理)

デフォルト管理者は、PRTG を、ユーザー1名で使用、或いは、無制限のユーザーを作成することもできます。ユーザーは無制限のグループで構成されます(そのグループごとにセキュリティ設定を変更することも可能です)。

ユーザーには、3種類あります。

- 管理者ユーザー: "PRTG Administrator"グループで唯一、ユーザーアカウントの作成や編集ができ、全ての監視オブジェクトの閲覧、編集が可能です。
- Read/Writeユーザー: 監視設定の変更に必要な全てのメニューやリンクにアクセスすることができます(編集権限の有無を問わず)。
- Read Onlyユーザー: どの編集リンクやメニューにもアクセスできません。また設定の変更もできません。

全てのセキュリティ設定や権限管理は、ユーザーグループ経由で実行されます。つまり、グループで、ユーザーができることやログイン後にアクセスできるオブジェクトを管理しています。

### 新規ユーザーの作成

それぞれの新規ユーザーについて管理者はログイン名とEメールアドレスを設定する必要があります。メインメニューより"Setup|Users"を選択し、"Add new user"をクリックして、新規ユーザーを作成します。

**補足:** 個々のユーザーの権限を管理する場合は、それぞれのユーザーに対して、ユーザーグループを作成する必要があります。新規ユーザーの作成時に"Primary Group"ドロップダウンリストより"Create new user group for this user"を選択すると、自動的にグループが作成されます。新規ユーザーとユーザーグループの名称が同じになっています。そして、このユーザーグループを使って、ユーザーの権限を個々に管理することができますようになります。

### ユーザーアカウント設定

それぞれのユーザーアカウントは、ユーザー(メインメニューから"Setup|My Account"を選択)、あるいは管理者が変更可能な数々の設定があります。設定は、次の通りです。

- Password: ここで、ログインパスワードを変更できます。
- Time zone: ユーザーがログインすると、そのタイムゾーンで全ての時間が表示されます。
- Auto refresh type and interval: PRTGは自動でブラウザ内のコンテンツを最新の内容に更新します。ここで、リフレッシュ不可/リフレッシュ間隔の設定(推奨: 30秒)の2種類の中から選択できます。
- Audible alarm: アラームの数が0でない限り、ブラウザのリフレッシュのたびにアラーム音がなります。

- Chart Rendering and Flash Graph Delay: 静止画像ベースのグラフか(読込速度 - 速)、フラッシュベースのグラフか(マウスポインタをそれぞれの値に乘せると、ポップアップテキスト表示されるなど、よりインタラクティブ)を選択します。
- Autofolding Settings: ユーザーに素早い操作性を実感していただくために、PRTG は、たくさんのアイテムを持つグループやデバイスを"folding"する(折りたたむ)ことによって、センサーツリーページの大きさを小さくしています。"Max. Groups/Devices per Group"と"Max. Sensors per Device"の2つの設定で、グループ/デバイス或いはセンサーが最大いくつ表示されると折りたたむかを設定できます。推奨する値はそれぞれの設定で 10-30 です。ツリービューの個々のセンサーの確認をしない場合は、"Max. Sensors per Device"の値を0にしてください。
- Account Type: Read/Write ユーザーか、Read Only ユーザーかを選択してください(上述)。
- Primary Group: それぞれのユーザーは、権限を管理するプライマリーグループを持っています。
- Active/inactive: 管理者はユーザーを無効に設定できます。その場合、ユーザーはログオンできなくなります。

### 新規ユーザーグループの作成

新規ユーザーグループの作成は、メインメニューから"Setup|User Groups"を選択し、"Addnew user group"をクリックしてください。

### ユーザーの権限管理

PRTGのwebインターフェイスで、以下の設定を用いて、監視オブジェクト(グループ/デバイス/センサー/マップ/レポートなど)へのアクセスを管理することができます。



センサーツリーオブジェクトに対して、デフォルトの設定は、"Inherit Access Rights"です。これは、ユーザーがオブジェクト自体にアクセス権を持っていると、それと同じ権限を全ての子オブジェクトに対して持つということを意味しています。

これは、"User Group Access"オプションで無効にすることができます。ドロップダウンリストから選択肢を選ぶことで、それぞれのユーザーグループに対するカレントオブジェクトへのアクセス件を設定することができます。

Inherited (None)

None  
Read  
Write  
Full

オプションは、次の通りです。

- Inherited: 親オブジェクトの設定を利用
- None: ユーザーはオブジェクトの閲覧/編集のいずれも許可されていません。子オブジェクトの表示があり、センサーツリー上にオブジェクトが表示されていても、アクセスできない場合は、オブジェクトはリストにもセンサーツリーにも表示されません。
- Read: ユーザーはオブジェクトを見ることができ、監視ステータスを確認できます。
- Write: ユーザーはオブジェクトの閲覧、監視ステータスの確認、オブジェクトの設定(グループアクセス設定を除く)が許可されます。
- Full: "Write"と同じですが、ユーザーはさらにグループアクセス設定を管理できます。

ユーザーが親オブジェクトに対して、"Write"か"Full"アクセスの権限を持っている場合のみ、オブジェクトの追加/削除が可能です。

グループ/デバイスについてのさらにチェックボックス、"Revert children's access rights to inherited"があります。このボックスを選択すると、全ての子オブジェクトのアクセス権が、オブジェクトに対する全ての個々の権限設定を削除する"inherited"にリセットされます。この方法は、簡単に全てのアクセス権限をリセットしてしまうため、注意が必要です。

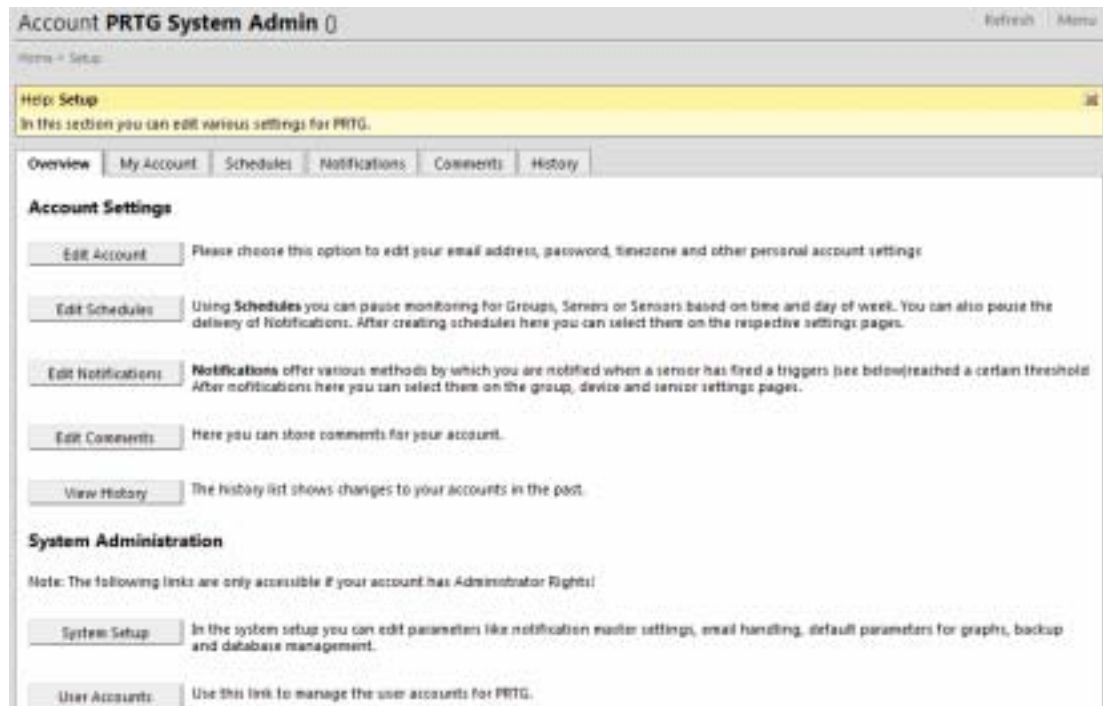
# Part

# XII

## System Settings and Administration (システム設定と管理)

## 13 System Settings and Administration (システム設定と管理)

アカウントに対する設定やシステム設定、システム管理設定のほとんどは、Webインターフェースの"Setup"メニューから可能です。WebサーバーIP、ポート、ライセンスキーなどの設定は、Server Admin Tool、Probe Admin Toolにあります。



以下のセクションを参照してください。

- 13.1 アカウント設定 - マイアカウント
- 13.2 アカウント設定 - スケジュール
- 13.3 アカウント設定 - 通知
- 13.4 システム設定 - webサーバー
- 13.5 システム設定 - プロ - プ
- 13.6 システム設定 - 通知
- 13.7 Core Server Admin Tool(コアサーバーアドミニツール)
- 13.8 Probe Admin Tool(プローブアドミニツール)

### 13.1 Account Settings - My Account(アカウント設定 - マイアカウント)

"My Account"で、自分のユーザーアカウントの設定を変えることができます。

Overview | My Account | Schedules | Notifications | Comments | History

### User Account Settings

Login Name: prtgadmin Enter the login name of the user. This name will be used to log into the web interface.

Username: PRTG System Admin Enter a name for the user for display purposes (not used for login).

Email Address: support@paessler.com

Timezone: (GMT+01:00) Amsterdam, Berlin, Bonn, Rome, Stockholm, Vienna

Password:  Don't change  Specify new password

### Auto Refresh Settings

Auto Refresh Type:  Refresh Page Elements (Recommended)  Refresh Whole Page  No Auto Refresh PRTG automatically refreshes the content in your browser. Here you can choose between two different refresh methods and you can specify the refresh time (30s recommended).

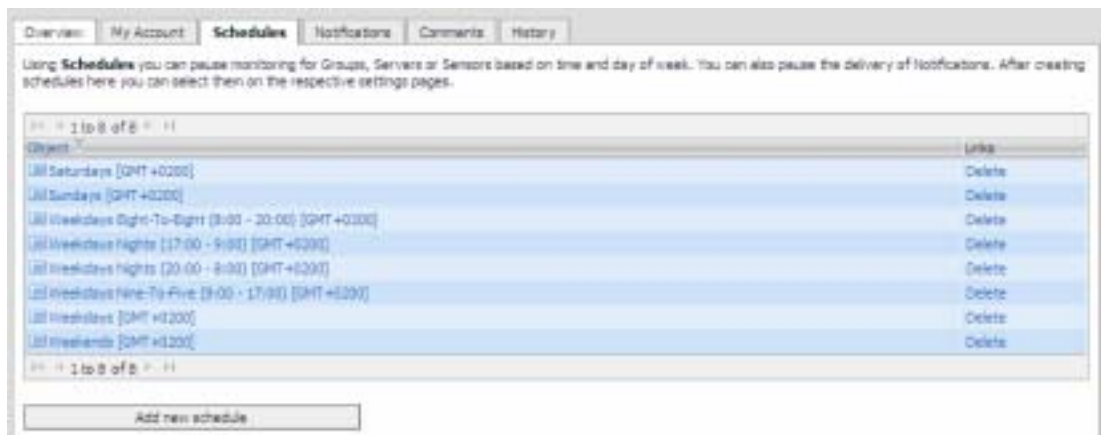
Auto Refresh Interval (sec): 30

このページで、次の情報の詳細を定義することができます。

- User Account Settings: ここで、ログイン名、ユーザー名、ユーザーのEメールアドレス、タイムゾーンの変更ができ、新しいパスワードの設定も可能です。
- Auto Refresh Settings: ここで、ブラウザのコンテンツの自動リフレッシュの有無、ページ要素のみ/ページ全体のリフレッシュ、リフレッシュ間隔(秒単位)を選択できます。
- Web Interface Settings: ここで、図表の表示モードを選択できます(グラフ処理の速度を求める場合は静止画像モード、よりインタラクティブ性を重視する場合は、フラッシュモードを選択)。さらにコンテキストヘルプの有無も選択できます。
- Autofolding Settings for the Sensortree: PRTGは、アイテムの多いグループ/デバイスを自動で"folding"(折りたたむ)ことによって、センサーツリーページの大きさを小さくしています。ここで、グループ/デバイス/センサーが最大いくつ表示されると折りたたむかを設定することができます。
- Account Control: ここでは、どのグループにユーザーが属するかを定義します(ユーザーのアクセス権は、他で定義されます)。管理者でないユーザーは、それぞれのラジオボタンを選択することで、有効/無効が設定されます(管理者のみ設定可能)。

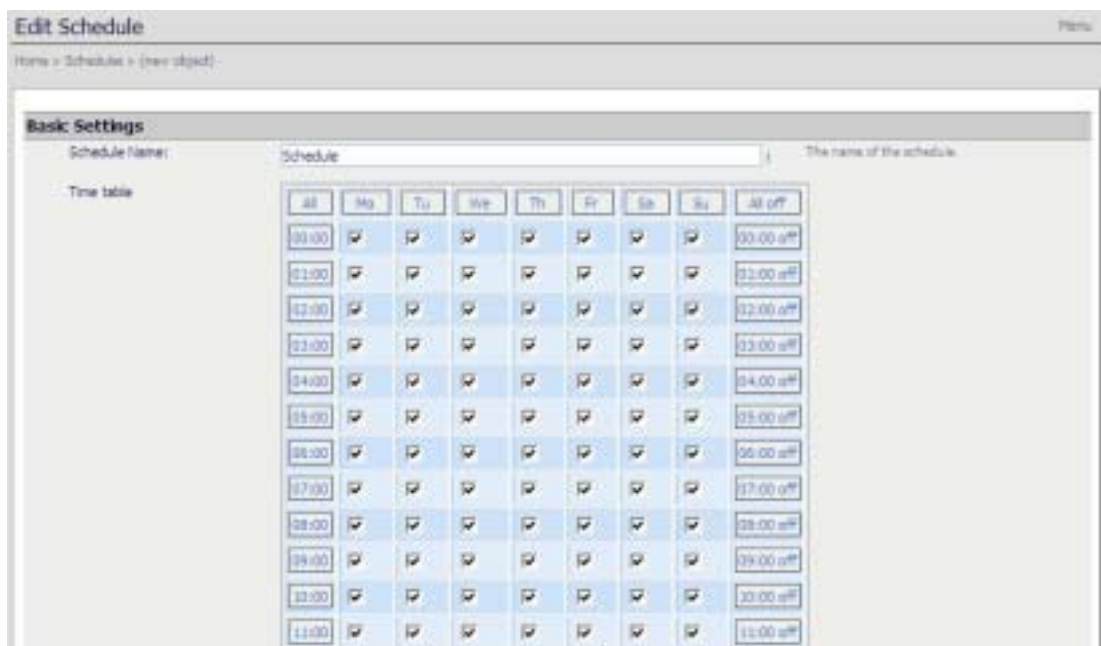
## 13.2 Account Settings – Schedules(アカウント設定 - スケジュール)

"Schedules"では、ユーザーはグループ/サーバー/センサーの監視を時間や曜日に基づいて停止させたり、通知の送信を停止させたりするために使用するタイムテーブルを定義することができます。



さまざまな共通スケジュールがデフォルトで可能です。"Add new schedule" ボタンで、スケジュールの追加ができます。

既存のスケジュールを選択するか、新しいスケジュールを追加すると、次のウィンドウが表示されます。



ここで、目的がわかるようなスケジュール名を設定したり、スケジュールのタイムレンジを設定するチェックボックスにチェックを入れることができます。一番上にある曜日アイコン、あるいは一番下にある曜日 "off" アイコンをクリックすることで、その曜日の全てのチェックボックスについて選択/非選択を設定することができます。左側の時刻アイコン、もしくは右側の時刻 "off" アイコンをクリックすることで、その時刻の全てのチェックボックスについて選択/非選択を設定することができます。

ウィンドウの一番下で、選択したスケジュールに関連したユーザーグループアクセス権を設定することもできます。以下の権限の設定が可能です。

- None: このユーザーグループはスケジュールにアクセス権がありません。また、特定のスケジュールの閲覧/編集が許可されていません。
- Read: このユーザーグループは、スケジュールの読取のみ許可されています。特定のスケジュールの閲覧はできますが、編集はできません。
- Write: このグループはスケジュールの読取/書き込みの両方が許可されています。特定のスケジュールの閲覧/編集が可能です。
- Full: このグループはスケジュールの読取/書き込みの両方が許可されているだけでなく、他のユーザーグループにスケジュールのアクセス権を付与することもできます。

### 13.3 Account Settings – Notifications(アカウント設定 - 通知)

"Notifications"では、全設定済み通知の概要を確認できます (Part [通知参照](#))。



任意の通知をクリックすると、その設定ページが開きます。"Add new notification" ボタンをクリックして新しい通知を追加することも可能です。"Delete" をクリックして、任意の通知を削除したり、"Test" をクリックして、任意の通知をテストしたりできます。

編集ページは次の通りです。

User Group Access	User Group	Rights
	PRTG Administrators	Full
	PRTG Users Group	None

ユーザーは選択した通知に関するアクセス権をユーザーグループに与えることができます。権限は次の通りです。

- None: このユーザーグループは、通知へのアクセス権がありません。特定の通知の編集/閲覧が許可されていません。
- Read: このユーザーグループは通知の読取のみ許可されています。特定の通知の閲覧は可能、編集は不可です。
- Write: このユーザーグループは通知の読取/書き込みの両方が許可されています。特定の通知の閲覧/編集ともに可能です。
- Full: このユーザーグループは通知の読取/書き込みの両方が可能で、さらに通知へのアクセス権を他のユーザーグループに付与することも可能です。

はじめに通知の名称を入力し、ユーザーグループの権限を設定します(例: あるユーザー

**110** PRTG Network Monitor 7.1 - ユーザーマニュアル

についてある特定の通知の利用を許可/不許可にする場合など)

チェックボックスを使って、さまざまな通知形式を有効にすることができます。それぞれの形式について、受信アドレスを入力してください。必要に応じて、通知テキストを変更することも可能です(利用可能なプレースホルダーの説明は、その右側にあります)。

**注意:** インスタントメッセージャを使った通知には、それを使った通知のために、常に2種類のアカウントが必要になります。メッセージを送信するアカウントと、受信するアカウントの2つです。

**重要:** ほとんどの通知形式には、System Setup Notifications画面(13.6章参照)で、送信者情報を入力する必要があります。

### 13.4 System Setup - Web Server(システム設定 - web サーバー)

"Web Server"タブでは、webサーバー関連の詳細を定義することができます。

ここでは、次の詳細情報を定義することができます。

- Site Information: ここでは、サイト名称や(webインターフェイスとEメールの件名で使用)サイトのURL(Eメールにリンクを張るのに使用)を定義できます。DNS名をPRTGのWebサーバーにアクセスする際に使用する場合は、その名前もここで入力します。
- Sensor Intervals: ここでは、設定にオブジェクトを追加するときに選択できる間隔を定義できます。新しい値を追加する場合は、数値をtime span enumerator (s/m/h/d. それぞれs-秒/m-分/h-時間/d 日を定義します)の前に追加します。

- Email Options: ここではフッタ(テキストのみのメール)や、送信メール用のHTMLテンプレート(プレースホルダー有)を編集したり、"ToDo"メールの送信先(管理者や特定のメールアドレス)や送信の有無などを定義したりできます。"specific email" を選択した場合は、新しい欄が追加され、その場合のメールアドレスを定義できるようになっています。
- Data Purging Limits: ここでは、何日分のデータ履歴までアクセスできるようにするかを選択できます。可能な各エントリーについて、過去データを保管する日数を入力してください。
- Unusual Detection: ここでは、"unusual"(異常)検知機能の検出精度を定義できます。
- Settings from the PRTG Server Administrator program: これらのエントリーは、"for your information"オンリーです。ここでは、Start | PRTG program group の PRTG Server Administrator アプレットからこれらのエントリーを編集できます。(13.7 Core Server Admin Tool 参照)

### 13.5 System Setup – Probes(システム設定 - プロブ)

"Probes"タブでは、プロブ関連の詳細を定義することができます。



- Probe Connection Settings: ここでは、アクセスキーや、IPアドレスのプロブへのアクセスの許可/不許可の詳細を定義できます。14.2 複数プロブとリモートプロブを参照してください。
- Settings from the PRTG Server Administrator program: これらのエントリーは、"for your information"オンリーです。ここでは、Start | PRTG program group の PRTG Server Administrator アプレットからこれらのエントリーを編集できます。(13.8 Probe Admin Tool参照)

### 13.6 System Setup – Notifications(システム設定 - 通知)

"Notification"タブでは、通知関連の詳細を定義することができます (Part 通知 参

照)。

**注意：** 通知でインスタントメッセージを使う場合は、必ず2種類のアカウントが必要です。送信用アカウントと受信用アカウントの2つです。

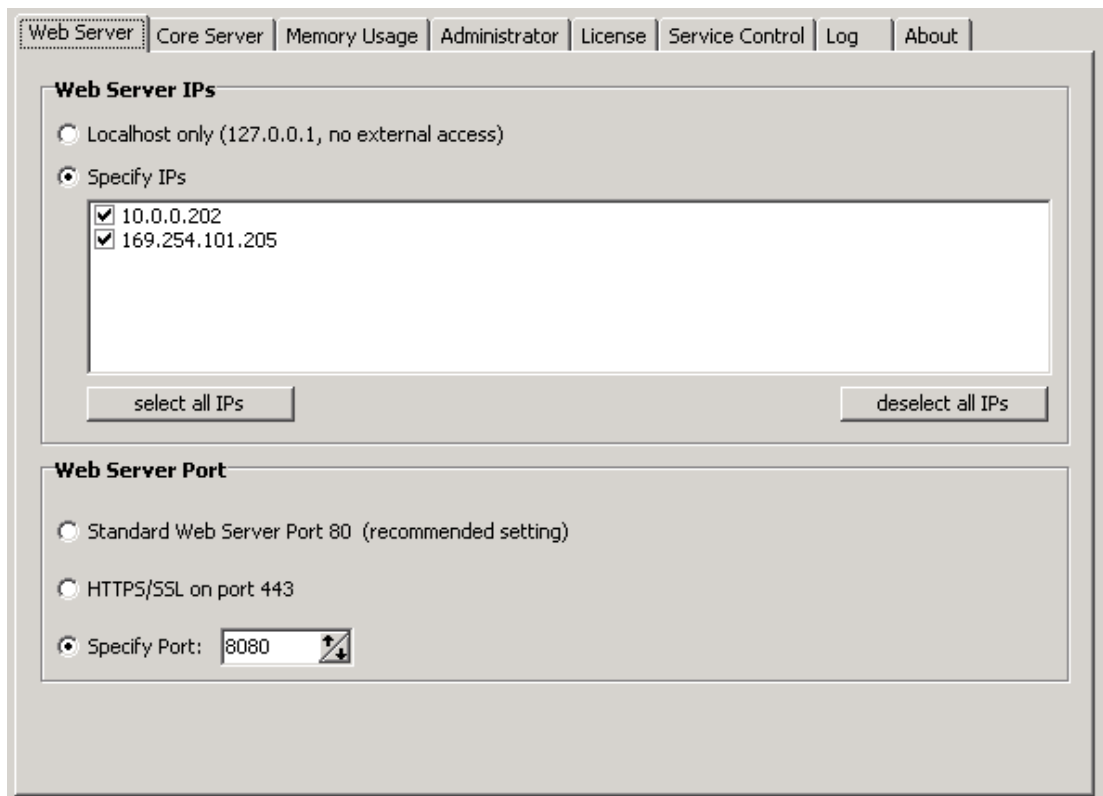
このページでは、次の情報の詳細を定義することができます。

- SMTP Delivery: ここでは、SMTP送信機能 (PRTGの自動リレーを使用するか、ユーザーのSMTPサーバーを定義するか) やメール転送のあらゆる関連情報を定義することができます。ユーザーのSMTPサーバー定義を選択した場合は、サーバー本体 (IPアドレス使用かDNS名使用か)、SMTPポート、リレー認証形式 (標準かSASL) などのサーバー情報が必要です。認証が必要な場合、ユーザー名とパスワードを要求されます。また、通知最大数を設定して、どの段階で個々の通知をまとめるかを定義することができます (これによって、受信メールの数を削減することができます)。
- SMS Delivery: ドロップダウンリストから、SMSゲートウェイプロバイダーを選択してください。また、ゲートウェイアクセスのユーザー名とパスワードを入力してください。
- ICQ Delivery: ICQ通知を送信するアカウントのICQナンバーとパスワードを入力してください。
- Windows Live Messenger (MSN Messenger) Delivery: MSN通知を送信するアカウントのMSN IDとパスワードを入力して下さい。
- Yahoo! Messenger Delivery: Yahoo! Messenger通知を送信するアカウントのYahoo! Messenger IDとパスワードを入力してください。
- AOL Instant Messenger Settings: AIM通知を送信するアカウントのAIM IDとパスワードを入力してください。

### 13.7 Core Server Admin Tool(コアサーバー管理ツール)

Core Server Admin Toolは、"START | PRTG Network Monitor"プログラムグループから始めることができ、実装プロンプトの設定が可能です。Core Server Admin Toolは8つのタブに分かれています。

#### Webサーバー



Web Serverタブでは、WebサーバーのIPアドレスの定義ができます。local host only(外部アクセス不可です。安全性は最も高い。)を選択するか、個々のIPアドレスをリストの表示から指定するか選ぶことができます。使用するWebサーバーのポートを定義することもできます。以下から、選択します。

- Standard Web Server Port 80:これはほとんどの設定で推奨の標準ポートです。
- HTTPS/SSL on port 443: SSL経由("https://(ユーザーの IP)")でのみ使用できるWebサイトです。
- Specify Port: 任意のポート番号を入力してください。

#### コアサーバー

The screenshot shows the 'Core Server' configuration window with the 'IPs for Probe Connections' tab selected. The window has a menu bar with 'Web Server', 'Core Server', 'Memory Usage', 'Administrator', 'License', 'Service Control', 'Log', and 'About'. The main content area is divided into three sections:

- IPs for Probe Connections:** Contains three radio buttons: 'Use all IPs for probe connections', 'Localhost only (127.0.0.1, no remote probes)', and 'Specify IPs for probe connections (127.0.0.1 is automatically active as it is needed for the local probe)'. The third option is selected. Below it is a list box containing '10.0.0.202' (checked) and '169.254.101.205' (unchecked).
- Port for Probe Connections:** A text box containing '23560' with a spinner icon and '(Standard: 23560)' next to it.
- Path for data files:** A text box containing 'C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Paessler\PR...', a browse button (...), and a checked 'Use Compression' checkbox. Below the text box is a note: 'Note: Please copy your PRTG data files to the desired location BEFORE changing the path here.' and a 'Revert to default path' button.

Core Serverタブでは、プローブ接続のためのIPアドレスを定義することができます。コア・プローブ間の接続は、プローブ9(14.2 複数プローブとリモートプローブ参照)で起動します。use all IPs、localhost only、リストに表示された個々のIPアドレスのいずれかを選択することができます。また、プローブ接続するポートを定義したり、全てのコアサーバーデータファイルのパスを定義したりできます(必要に応じて、圧縮を選択したり、個別の要素をクリックして、デフォルトパスに戻すことも可能です)。

## メモリー使用量

The screenshot shows the 'Core Server' configuration window with the 'Memory Usage' tab selected. The window has a menu bar with 'Web Server', 'Core Server', 'Memory Usage', 'Administrator', 'License', 'Service Control', 'Log', and 'About'. The main content area is titled 'Memory Used for Graphs and Tables' and contains the following text:

The RAM memory usage of PRTG depends on the memory required to store the data for the graphs of groups, devices and sensors. This is necessary for fast display of the graphs. You can minimize this memory requirement by choosing shorter time frames with longer intervals below.

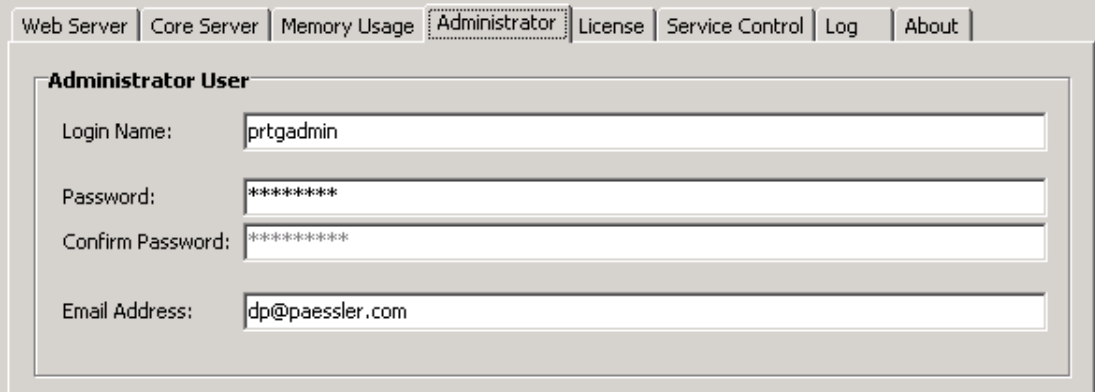
Please select the period and average interval used for the graphs and tables. Note: If you change these values the data cache must be recalculated. During recalculation the graphs may show incomplete data.

Below the text are four dropdown menus:

- Live: 120 Values (= 2 Hours with 1 min scanning interval)
- Graph 1: 2 Days with 5 Minutes averages
- Graph 2: 30 Days with 1 Hour averages
- Graph 3: 365 Days with 1 Day averages

**115** PRTG Network Monitor 7.1 - ユーザーマニュアル

Memory Usageタブでは、現在のグラフや、その他PRTGで表示される3つの標準グラフについての時間枠を定義することができます。グラフの時間枠を少なくし、間隔を増やすことで、メモリー使用量を減らすことができます。

**Administrator(管理者)**

Web Server | Core Server | Memory Usage | Administrator | License | Service Control | Log | About

**Administrator User**

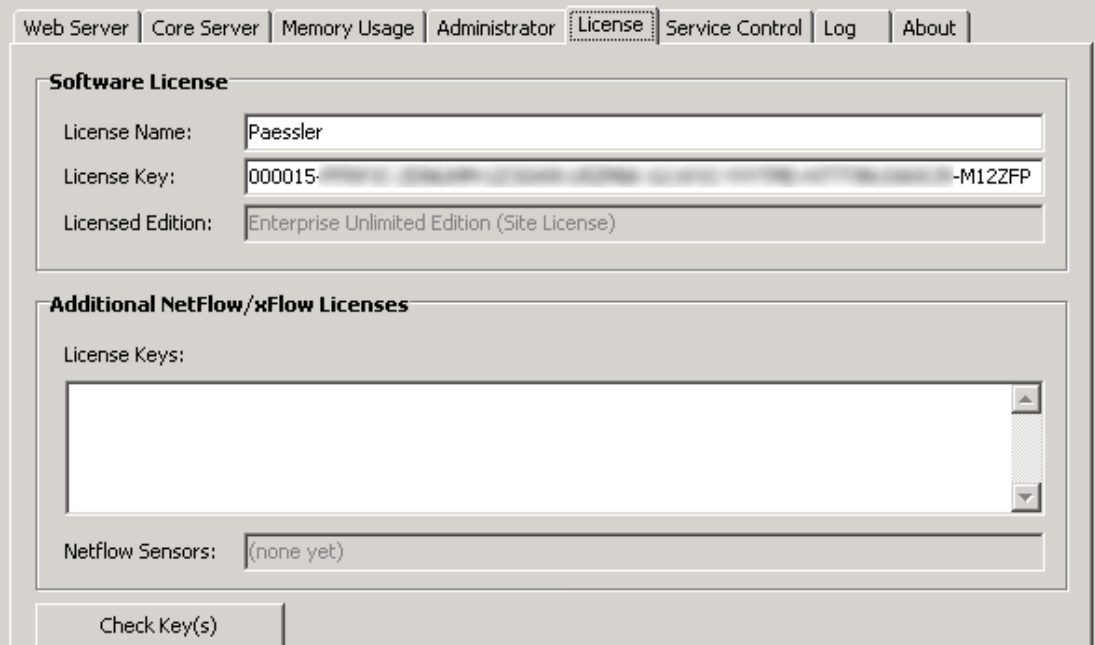
Login Name:

Password:

Confirm Password:

Email Address:

Administratorタブでは、管理ユーザーのログイン名、パスワード、Eメールアドレスを定義することができます。

**ライセンス**

Web Server | Core Server | Memory Usage | Administrator | License | Service Control | Log | About

**Software License**

License Name:

License Key:

Licensed Edition:

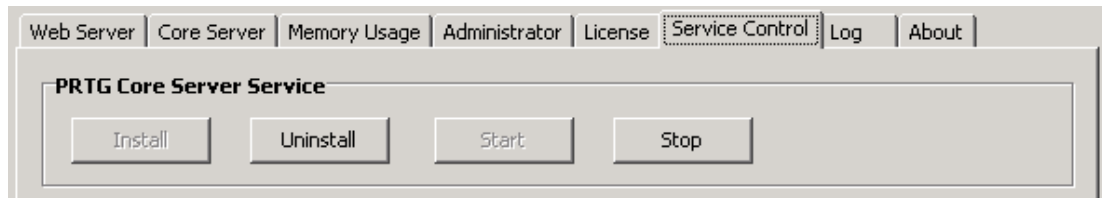
**Additional NetFlow/xFlow Licenses**

License Keys:

Netflow Sensors:

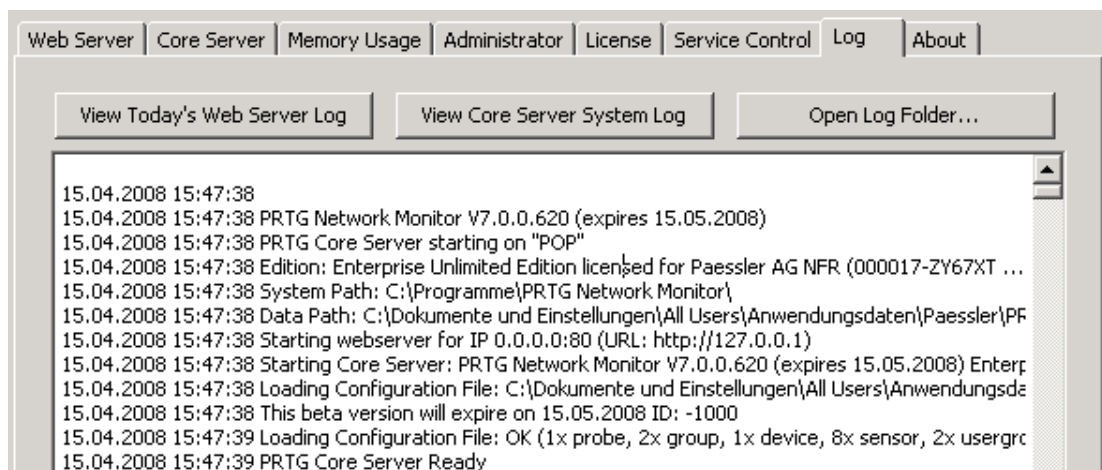
Licenseタブで、ライセンス情報(名称やキー。それによって、ライセンスエディションの値が返ります。)や、Netflow/xFlowアドオンライセンスを入力することができます。ライセンス情報の入力が完了したら、"Check Key(s)"ボタンをクリックし、同じかどうか確認し、アクティベートしてください。

## Service Control (サービス管理)



Service Controlタブでは、コアサービスを、インストール/アンインストール、スタート/ストップすることができます。

## Log (ログ)



Logタブでは、当日のwebサーバーのログ、コアサーバーのシステムログを確認したり、或いは、直接コアのログファイルディレクトリを開くことができます。

## 13.8 Probe Admin Tool (プローブ管理ツール)

Probe Admin Toolは、"START | PRTG Network Monitor" プログラムグループからはじめることができ、実装プローブの設定をすることができます。Probe Admin Toolは、4つのタブに分かれています。

### Probe Control (プローブ管理)

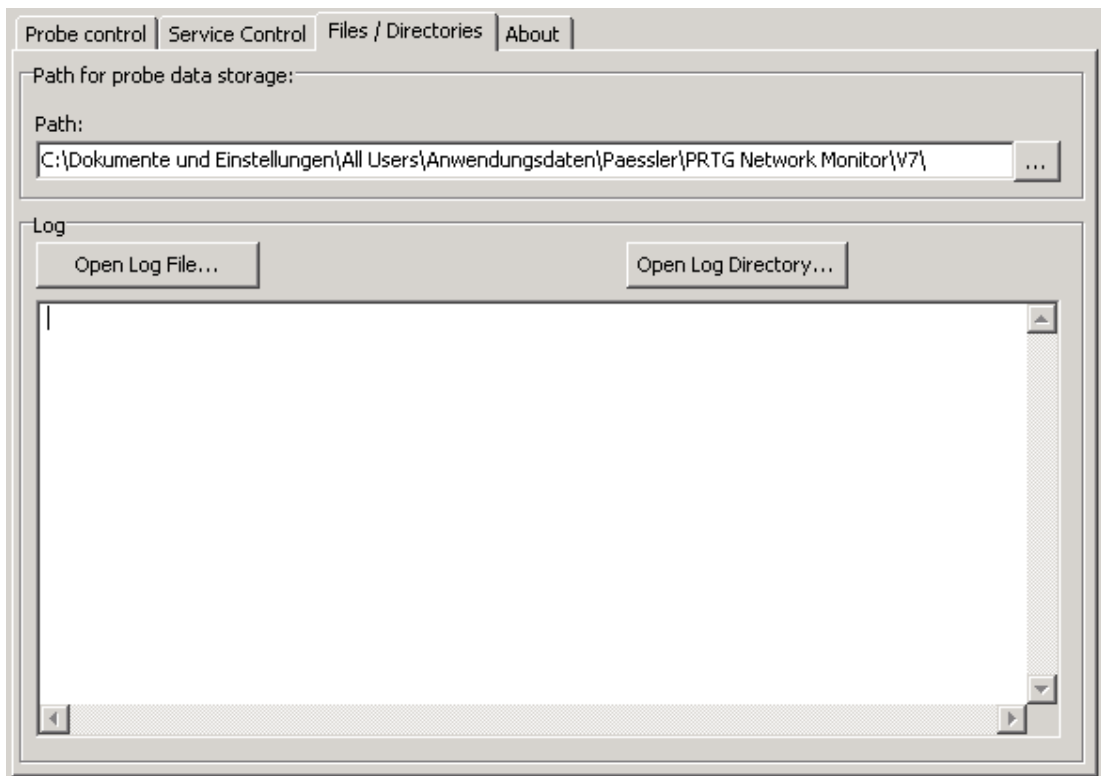
Probe Controlタブでは、以下の定義が可能です。

- Name of the probe (webインターフェイスに表示されるプローブの名称)
- Server Connection: サーバーのIPアドレスかDNS名、サーバーのポート、プローブのアクセスキー (これらの設定は、Core Admin Toolの設定と一致させる必要があります。14.2 複数プローブとリモートプローブ参照)。
- Probe's GID (各プローブの唯一の識別子。要注意！)
- Reconnect time (秒): コアに接続できない場合に再接続を試みる間隔。
- Outgoing IP for monitoring requests: 全ての監視要求の送信に使用するIPアドレスを選択してください。推奨は、"auto"設定です (そうすると、自動でマルチホームシステム上の正しいIPアドレスを選択してくれます)。

### Service Control (サービス管理)

Service Controlタブで、プローブサービスをinstall/uninstall、start/stopすることができます。

## Files / Directories (ファイル/ディレクトリ)



Files/Directoriesタブで、どこにプローブデータが保存されているかを特定するパスを選択することができます。さらに、プローブのログファイルやプローブのログファイルディレクトリを開くことも可能です。

# Part

# XIV

## Advanced Topics (追加トピック)

## 14 Advanced Topics (追加トピック)

この章では、PRTG Network Monitorのについてさらに詳しい情報を扱います。

- 14.1 Toplists(トップリスト)
- 14.2 複数プローブとリモートプローブ
- 14.3 クローニング/デバイスプレートによるデバイスコピー
- 14.4 PRTG Traffic Grapher 6/IP check Server Monitor 5からのデータインポート
- 14.5 webサーバーへのSSL認証設定
- 14.6 PRTG API(アプリケーションプログラミングインターフェイス)の使用
- 14.7 カスタムEXEセンサーへのインターフェース定義

### 14.1 Toplists(トップリスト)

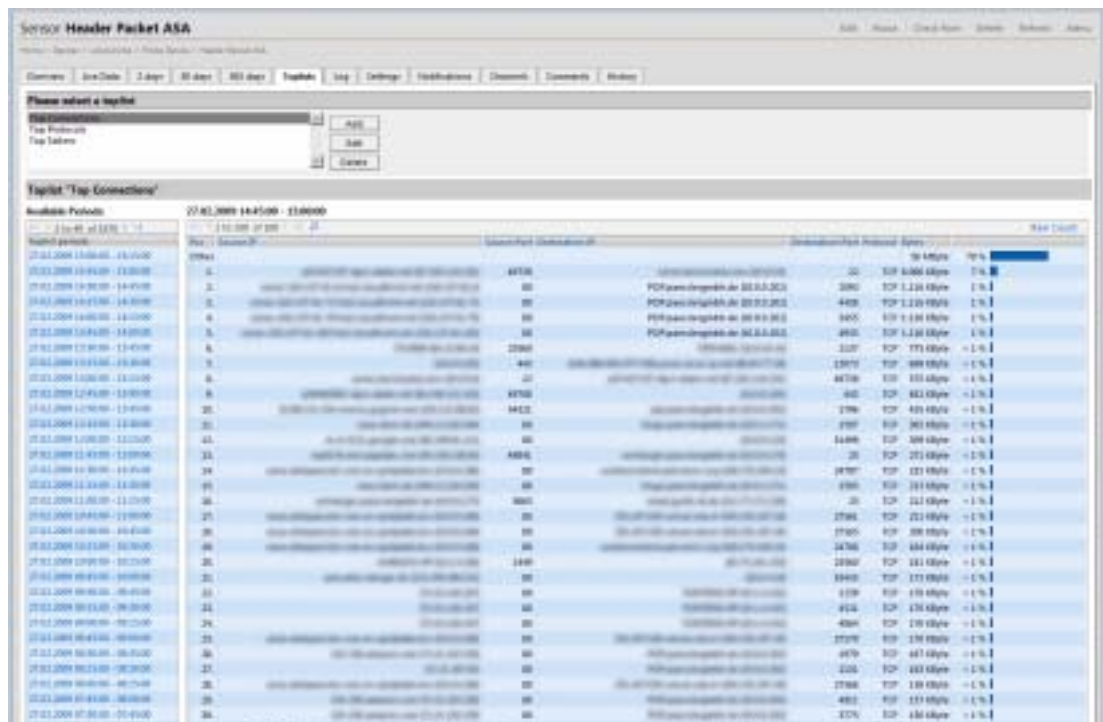
Packet Sniffing(パケットスニフing)やNetFlowのセンサーは総帯域使用量を測定するだけでなく、IPアドレス、ポート、プロトコル、他のパラメーターなどによってトラフィックを分析することができます。その結果は、いわゆる"toplists"に表示されます。この方法で、PRTGは、どのIPアドレス、接続、プロトコルが最も帯域を使用しているかを表示することができます。PRTGはあらゆるネットワークパケット(ストリーム)を監視し、全IPアドレス/ポート/プロトコルの帯域情報を収集します。最後に、PRTGはデータベースの各トップエントリーだけを保存します。

#### トップエントリーだけが保存される理由

分析中に、有効なデータベースの全てのデータを保管すると、データ量が巨大になってしまい、プローブ・コア間の転送速度が低下、また、データの読み込み速度も低下します。短い期間での上位100位のエントリーのみ保存することで、回線を占有するデータ量の大きな通信を検出する一方で、データ量は最小に削減することが可能になります。

#### トップリストへのアクセス

パケットスニフingやNetFlowセンサーのトップリストにアクセスする場合は、センサー詳細ページの"toplist"タブをクリックしてください。



ページ上部よりトプリストを選択することができます。また左側より、時間帯を選択することができます。

2/27/2009 2:45:00 PM - 3:00:00 PM

Pos	Source IP	Source Port	Destination IP	Destination Port	Protocol	Bytes	%
Other						807 KByte	24 %
1.	backup (192.168.2.104)	1208	[65.75.243.170]	23560	TCP	357 KByte	10 %
2.	mail2.myzms.com (62.146.10.41)	80	backup (192.168.2.104)	3932	TCP	203 KByte	6 %
3.	mail2.myzms.com (62.146.10.41)	80	backup (192.168.2.104)	4497	TCP	203 KByte	6 %
4.	mail2.myzms.com (62.146.10.41)	80	backup (192.168.2.104)	4220	TCP	201 KByte	6 %
5.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	4254	TCP	132 KByte	3 %
6.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	4529	TCP	131 KByte	3 %
7.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	3964	TCP	129 KByte	3 %
8.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	3929	TCP	120 KByte	3 %
9.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	4492	TCP	120 KByte	3 %
10.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	4216	TCP	120 KByte	3 %
11.	noname (192.168.2.102)	1036	[209.255.255.250]	8082	UDP	98 KByte	2 %

PRTGは、DNSの逆引きを行って、それぞれのIPアドレスからドメイン名を表示します。リストの各エントリーは、IPアドレス、ポートなどを表示し(トプリストのタイプによる)、対象期間のエントリーの総バイト数も表示します。最後の欄は、各エントリーの帯域を総帯域における割合でパーセント表示しています。

### トプリストの設定

既存のトプリストを編集したり、新規トプリストを追加する場合は、トプリストの表の隣にあるそれぞれのボタンをクリックしてください。

トプリストのタイプには、4つの選択肢があります。

- Top Talkers(トプトーカー：最も帯域を使用しているIPアドレス)
- Top Connections(トップ接続：最も帯域を使用している接続)
- Top Protocols(トッププロトコル：最も帯域を使用しているプロトコル)
- Custom(カスタム：独自のトプリストを作成)

"Custom"については、トプリスト作成中に使用するパラメーターを選択することができます。入力できる項目は、センサータイプによって異なり、ソースIPアドレス、ソースポート、デスティネーションIP、デスティネーションポート、ソースMAC、デスティネーションMAC、プロトコル、イーサタイプ、ToS、チャンネル、IP(統合)、ポート(統合)、MAC(統合)を含みます。リストタイプのほかには、期間やリスト中のエントリーの数を設定することができます。

### 大量トラフィックの接続についてのトプリスト

使用量の多いデータ回線(例:常時10メガビット/秒以上の帯域)のトプリストを作成する場合、或いはトラフィックが多岐にわたる場合(例:少ないトラフィックにたくさんのIPアドレス/ポート)、次の点を検討してください。

- プローブは各期間中にRAMメモリーのトプリストに必要な全ての情報を集めます。コアには、上位100位のエントリーのみが転送されます。トプリストのタイプとトラフィックのパターンによって、必要とされるメモリーは、大量(メガバイト級)になります。
- メモリー使用量を最小にするために、期間はできる限り短くしてください(トラフィックが多岐にわたる場合は、特に重要です)
- メモリー所要量は、トプリスト定義の各項目に伴って、急激に増加します(トラフィックパターンによる)。通信量の多い、多岐にわたるトラフィックの複雑なトプリストは避けましょう("Top Connections"(5項目)は、"Top Talkers"(1項目)より多くのメモリーを要します)。
- コア・プローブ間で広帯域となった場合、"Wait until toplist period ends"を選択し

てください(データは、期間中に一度コアに転送されるだけです)。

- "Data incomplete, memory limit was exceeded" のメッセージが表示された場合は、トプリスト設定でメモリーの限界を増やしてください。但し、プローブプロセスメモリーの使用量には注意してください。

#### 注意

- 注意1: トプリストを扱う場合は、この機能の設定にプライバシーの問題が関わってくることに注意してください。トプリストを使って個々のPCの接続は全て、ネットワーク外部まで追跡することができるようになります。よって、管理者としてのユーザーは、このマニュアルに従ってPRTGの設定をすることが法的に求められていることを認識する必要があります。
- 注意2: トプリストはwebインターフェースに経由で閲覧可能です。ネットワーク上で使用されているドメインのリストを他者に見せたくない場合は、トプリストを持つセンサーへのアクセスを制限してください。

## 14.2 Multiple Probes and Remote Probes(複数プローブとリモートプローブ)

PRTGには、監視を実行する2つのモジュールがあります。コアサーバー(データ保存、Webサーバー、その他をつかさどる)と1つもしくは複数の"probes"(プローブ)です(実際の監視を実行)。

### プローブの働き

プローブが作動開始すると、自動的にコアサーバーに接続し、センサー設定をダウンロードし、監視タスクを開始します。ユーザーによって監視設定が変更されると、コアサーバーはプローブに新しい設定データを送信します。プローブは自立的に監視し、実行したそれぞれのチェック項目についての監視結果をコアサーバーに戻します。何らかの理由(コアの再起動など)でコア・プローブ間の接続が切れた場合でも、プローブは監視を続行し、結果を保存します。

プローブ・コア間の接続は、プローブから開始され、SSL(Secure Sockets Layer)で保護されます。つまり、データパケットを捕らえたとしても、誰もコア・プローブ間で送受信されるデータの中身を見ることはできません。コアサーバーは、TCP/IPポートをオープンにして、プローブからの接続を待ちます。新しいプローブが初めて接続されると、管理者は、ToDoを受け取ることができ、センサーツリーでその新しいプローブを確認することができます。安全上の注意として、センサーを作成/監視する前に、プローブは管理者が手動で許可("accept"をクリック)してください。管理者は接続させないプローブを不許可にすることもできます。すると、以降、どのような接続も許可されません(プローブのIPアドレスは、プローブシステム設定の"Deny IPs"リストに追加されます)。これによって、確実に、権限のないプローブはコアサーバーに接続できなくなります。

プローブが接続を始めたら、ネットワーク外部から自分のコアサーバー上にプローブを作成できるようにしてください。例えば、ファイアーウォールの必要なポートをオープンにしたり、ネットワークのNATルールを設定したりなどです。プロセスは、ポート80を經由して、コアサーバーのWebサーバーへのアクセスを許可する場合と同様です。

**注意:** ローカルプローブは、ローカルホスト(127.0.0.1) と SSL経由で、自動的に設定、許可、コアへ接続されます。

### リモートプローブを使っての監視が必要となる場合

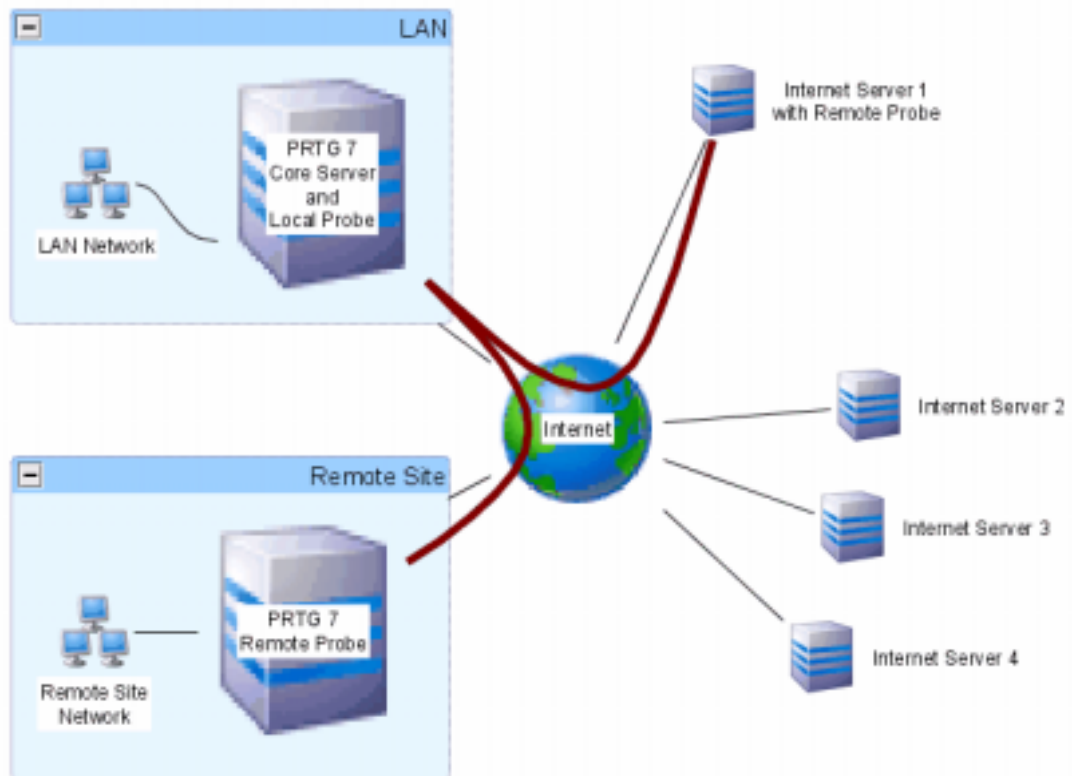
インストール時に、PRTGは自動的に、"local probe" (ローカルプローブ)と呼ばれる最初のプローブを自動的に作成します。ローカルプローブは、コアサーバーと同じマシン上で実行され、そのシステムの全てのセンサーを監視します。LAN監視や、監視する場所が1箇所のみの場合は、ローカルプローブ1つで十分です。

しかし、プローブが複数、もしくはリモートプローブが必要な場合もいくつかあります。

- 監視箇所が1箇所以上で、全てのロケーションからサービスを利用可能にする必要がある場合。
- ネットワークがファイアウォールによっていくつかのLANに分かれていて、ローカルプローブでは、ファイアウォールを超えて特定のサービスを監視できない場合。
- 公衆回線、或いは、安全でないデータ回線を経由した、VPNにあるシステムを監視する場合。
- 別のコンピュータにあるパケットを監視する場合。
- 別のコンピュータにあるNetFlowデータを監視する場合。
- パケットスニффングやNetFlowセンサーのようなCPUに負担をかけるセンサーに関するパフォーマンスに問題が起き、複数のPCに負荷を分散しなければいけない場合。

以下の図は、LAN内のPRTGコアサーバー (図左上)の機能の例です。

- ローカルプローブで、"LAN"内の保護されたサービスを監視。
- 専用のプローブサーバーに設定されたリモートプローブで、"Remote Site" (図左下)内の保護されたサービスを監視。
- サーバーに直接設定したリモートサーバーで、"Internet Server 1"上の保護されたサービスを監視。
- プローブのいずれかを用いて、インターネット経由した"Internet Servers 1, 2, 3"上の公共のサービスを監視します。



### 自動プローブアップデート

PRTGの新しいバージョンがコアサーバーにインストールされると、全てのリモートプローブは更新されたコアに再接続し、プローブの更新版をダウンロード・インストールします。これは、PRTG最新版に更新されたコアサーバーを再起動した直後の、PRTGインストレーションの“Devices”ページのスクリーンショットです。

**Root**

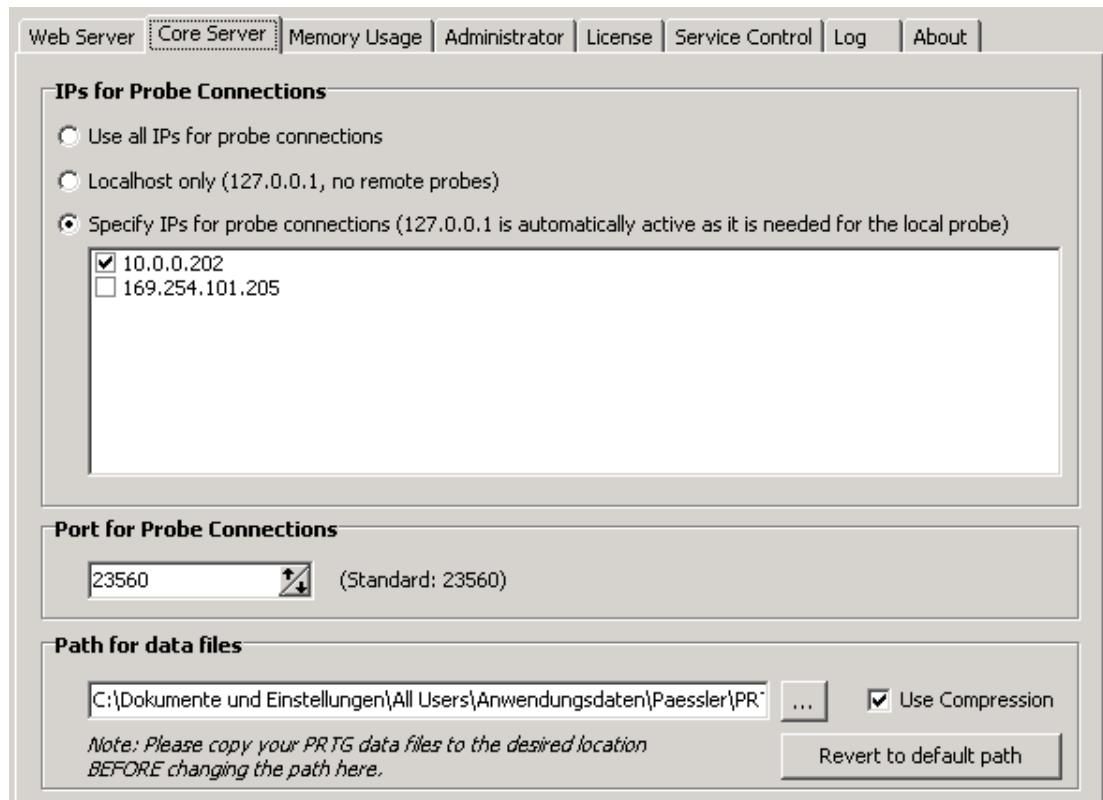
- Local probe (Local Probe on 127.0.0.1)**
  - 3 sub-groups with 9 devices
    - 20 Sensors
    - SMTP 10
    - 9 Sensors
- Probe Health (Sending update)**
  - 3 sub-groups with 23 devices
    - 12 Sensors
    - Probe Health
    - HTTP 33
- Probe Health (Sending update)**
  - 1 sub-groups with 4 devices
    - 6 Sensors
    - Probe Health
    - Sample Senso
- Probe Health (Sending update)**
  - 1 sub-groups with 46 devices
    - 903 Sensors
    - Probe Health
    - Sample Senso

ローカルプローブはコアのインストール中にアップデートされます。その他すべてのプローブは、SSLで保護されたプローブ/コア接続を使って、自動的に“PRTG probe”の新しいバイナリをダウンロードします。4メガバイトファイルのダウンロードには、使用可能な帯域に

よって、数秒から (LAN) 数分 (WAN接続) かかります。最新版がダウンロードされると、プローブは接続を中断し、最新版をインストール、そしてコアサーバーに再接続します。所要時間は、20 ~ 100秒間です。更新中は、ダウンロードに必要な帯域の関係で、ローカルプローブの監視に影響があります。

### Step1: リモートプローブのためにコアサーバーを準備

リモートプローブがコアサーバーと接続する前に、PRTGのスタートメニューグループのあるコアサーバー管理ツールで関連する設定を編集する必要があります。



デフォルトでは、コアサーバーは、ローカルホスト(127.0.0.1)経由の接続のみ許可します。つまり、ローカルプローブだけが接続できるようになっています。これが最も安全な設定です。外部のプローブの接続を許可する場合は、"Use all IPs..."にチェックを入れるか、"Specify IPs..."にチェックを入れて、サーバーのIPアドレスのうちの一つをするかのいずれかとなります。TCP/IPポートの番号も設定してください。

完了したら、"OK"をクリックし、設定を保存します。コアサーバープロセスが再開し、変更内容が有効になります。

### Step2: リモートプローブの設定

リモートプローブを設定するために、コアサーバー設定のwebインターフェイス > "Setup\Download"へ進み、Remote Probe Installerをダウンロードし、実行してください。インストールが終わると、Probe Administratorが起動し(もしくは、後でスタートメニューから手動で起動)、設定を入力します。

Probe control | Service Control | Files / Directories | About

Probe details

Name of the probe:  Reconnect Time:  s

Server connection

Connect to local core server (via 127.0.0.1 and port specified below)

Connect to remote core server (via settings specified below)

Server (IP or DNS name):  Port:  (Standard: 23560)

Probe GUID:  ...

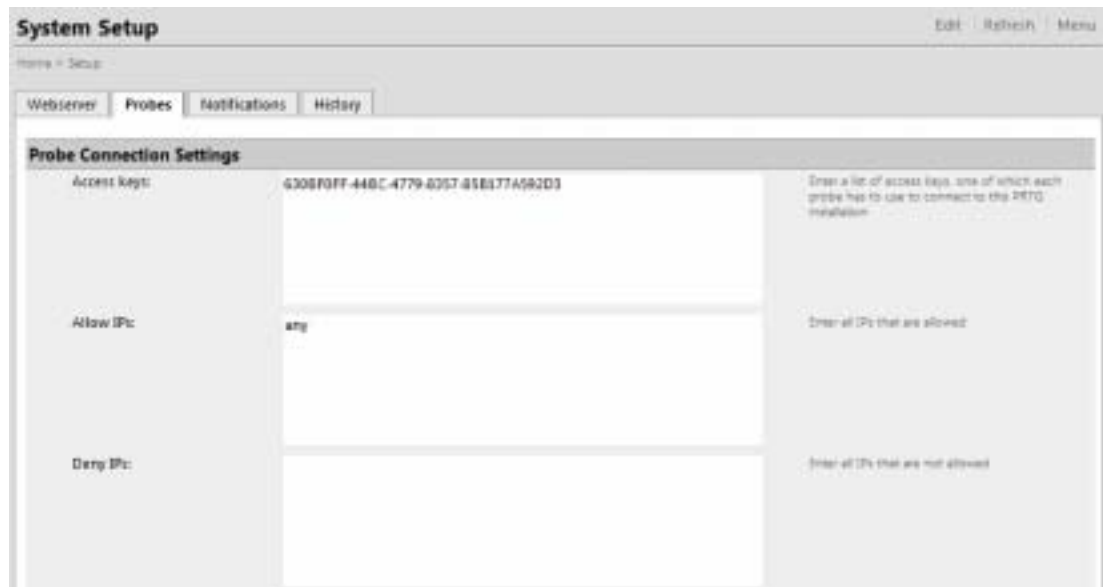
Access Key:  Confirm Access Key:

Outgoing IP for monitoring requests

重要な設定は、以下の通りです(詳しくは、[13.8 プローブ管理ツール](#)参照)

- Name of the probe(プローブ名): 任意の名前。Webインターフェイスのセンサーツリーで表示されます。
- Server Connection(サーバー接続): "Connect to remote core server"を選択してください。
- Server (IP or DNS name)(サーバー (IPアドレス/DNS名)): サーバーのIPアドレスかDNS名(上記core server administrator tool(コアサーバー管理ツール)で設定したもの)を入力してください。注意: ファイアーウォールの後ろのNATを使用するネットワークにコアサーバーがある場合、ファイアーウォールのNAT設定を変更し、外部Mapped IPを入力してください。
- Port(ポート): 上記コアサーバーで設定したのと同じポート番号を入力してください。

Webインターフェイス経由のサーバーへのアクセスキーを変更することができます。Webインターフェイスのメインメニューから"Setup!System Setup"を選択してください。次の画面が表示されます。




Webインターフェイスに1つ、もしくは複数のアクセスキーを入力でき(各プローブにつき1つが推奨です)、全く同じキーが、プローブ設定でも入力される必要があります。でなければ、コアサーバーは接続を許可することができません。デフォルトでは、PRTGはどのIPアドレスからの接続も許可します。次の2つの設定を使って、特に権限のあるIPアドレスのみ許可することで、より安全な設定にすることができます。"Allow IPs"欄にIPアドレスを入力するだけです。特定のIPからのプローブをブロックする必要がある場合は、"Deny IPs"欄にそのIPアドレスを入力してください。

プローブ設定が完了したら、プローブのサービスは自動的に開始され、コアサーバーへの接続を試みます。

### Step3: 新しいプローブの許可

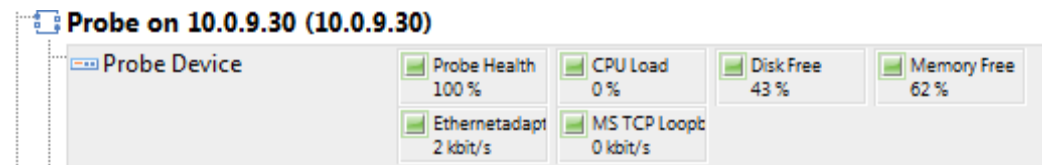
新しいプローブがコアサーバーに接続されると、Webユーザーインターフェイスでそれを許可する必要があります。

 **Probe on 10.0.9.30 (10.0.9.30)**

**Approve New Probe**

**Deny New Probe**

"Approve New Probe"をクリックして、完全にプローブを有効化してください。PRTGは自動的にプローブにセンサーを作成し、プローブ上のボトルネックが常に検知されるようにします。これらのセンサーを保存することを推奨します。



これで、新しいプローブを経由して監視するグループ/デバイス/センサーの作成ができるようになります。

### プローブ接続障害のデバッグ

リモートプローブの設定で問題が発生した場合、プローブシステムの次のフォルダに通常あるプローブのログファイルをチェックしてください。

Windows XP/ Server 2003:

```
C:\documents and settings\All Users\application  
data\Paessler\PRTG Network Monitor\V7\Logs (System)
```

Windows Vista/ Server 2008:

```
C:\ProgramData\Paessler\PRTG Network Monitor\V7\Logs (System)
```

プローブのプロセスは、"PRTG Probe Log (1).log" と "PRTG Probe Log (2).log" の2つのログファイルへ交互に書き込みをします。最新の日付のファイルを開いてください。

正しい接続の場合、プローブログは次のような感じになっています。

```
23.05.2008 16:15:15 PRTG Probe Server V7.0.1.821  
23.05.2008 16:15:15 Starting Probe on "WINXPVMWARE"  
23.05.2008 16:15:15 Data Path: C:\documents and settings\All  
Users\...  
23.05.2008 16:15:15 Local IP: 0.0.0.0  
23.05.2008 16:15:15 Core Server IP and Port: 10.0.2.167:23560  
23.05.2008 16:15:15 Probe ID: -1  
23.05.2008 16:17:01 Connected to 10.0.2.167:23560  
23.05.2008 16:17:06 Login OK: Welcome to PRTG
```

例えば、誤ったアクセスキーパスワードのために接続が失敗した場合は、次のように表示されます。

```
23.05.2008 16:31:02 Try to connect...  
23.05.2008 16:31:02 Connected to 10.0.2.167:23560  
23.05.2008 16:31:07 Login NOT OK: Access key not correct!
```

## 14.3 Copying Devices by Cloning or Using Device Templates (クローニング/デバイステンプレートによるデバイスのコピー)

1つ、もしくは複数のセンサーを持つデバイスの設定後、コピーする方法が2つあります。

- デバイスのクローニング: 全てのセンサーや設定をそのままにデバイスを数回のみ複製する場合に最適です。
- デバイステンプレートの使用: たくさんの類似したデバイスがあり、Webインターフェイス経由で手動で全てのデバイスを作成したくない場合に、よいでしょう。デバイスが同一のポート番号を持たない場合にも好ましいです。

### デバイスのクローニング

デバイスのコンテキストメニューより、"Clone"を選択してください。PRTGは新しい親グループとデバイスの新しい名前を求めてきます。新しいデバイスは、必要であれば、はじめ、停止して、センサー設定の編集ができるようにしてくれます。全てのセンサーが正しく設定されると、それらセンサーを持つデバイスの監視を再開することができます。

### デバイステンプレートの使用

デバイステンプレートを作成するために、PRTGはデバイステンプレートファイルにデバイスのセンサーについての定義を保存します。後でこのテンプレートファイルは、そのセンサーに対するセンサーを再生するのに使われます。デバイステンプレートを作成するために、デバイスのコンテキストメニューより"Create Device Template"を選択してください。PRTGは、ファイル名とテンプレート名を求めてきます。テンプレートファイルはPRTGインストールの'devicetemplate'フォルダに保存されています。同じセンサーをもつ新しいデバイスを作成するには、2つの方法があります。

- オートディスカバリーグループの作成: "Automatic sensor creation using specific device template(s)"を選び、テンプレートリストから特定のデバイステンプレートを選択してください。
- 新しいデバイスの作成: "Automatic sensor creation using specific device template(s)"を選び、テンプレートリストから特定のデバイステンプレートを選択してください。

### デバイステンプレートの制限

デバイステンプレートを使ったデバイスの複製は、次の制限があります(クローニングには、これらの制限はありません)。

- 次のセンサータイプにのみ対応: DNS, FTP, HTTP, HTTP Advanced, IMAP, PING, POP3, PORT, SMTP, SNMP Custom, SNMP Traffic, WMI Custom, WMI Disk Space, WMI Memory, WMI Service, WMI Processor, WMI Network, WMI Event Log, WMI Page File, WMI File, WMI Process, WMI Selection, EXE, Remote Desktop
- デバイステンプレートにデバイスのクレデンシャル設定が保存されません。デバイステンプレートを使ってデバイスを作成する前にグループレベルでクレデンシャルを入力する必要があります。
- 使用できるオブジェクトに基づいて作成されたセンサー(例: デバイスの使用可能

なポートを監視するSNMPトラフィックやWMIネットワークカードセンサーなどは、新しいデバイス上の全ての使用可能なポートについて再生されます。

- スケジュール、トリガー、dependencies (依存性)、チャンネル設定はデバイステンプレートに保存されません。

#### 14.4 Importing Data from PRTG Traffic Grapher 6 / IPCheck Server Monitor 5 (PRTG Traffic Grapher 6 / IPCheck Server Monitor 5 からのデータのインポート)

PRTG 7の過去の製品 - PRTG Traffic Grapher V6やIPCheck Server Monitor 5 - から、PRTG Network Monitor 7へインポートツールを使って、センサー設定や過去の監視データをインポートすることができます。

詳細は、Paessler社のwebサイト上、ナレッジベースを参照してください。

[http://www.paessler.com/support/kb/prtg7/tricks/data\\_import\\_from\\_prtg6\\_or\\_ipcheck5/](http://www.paessler.com/support/kb/prtg7/tricks/data_import_from_prtg6_or_ipcheck5/)

#### 14.5 Installing an SSL Certificate for the Web Server(web サーバーのSSL サーバ証明書の設定)

PRTG Network MonitorはSSLサーバ証明書をデフォルトで実装しており、追加設定無しでHTTPS経由のWebインターフェイスの安全な使用が可能になっています。しかし、ユーザーのPRTG設定のドメイン名やIPアドレスに合う公式の証明書ではないため、PRTGがこのサーバーに接続すると、通信が既に安全であっても、webブラウザは常にアラート("the certificate is not correct")を表示します。

詳細は、Paessler社のナレッジベースをご参照ください。

[http://www.paessler.com/support/kb/prtg7/tricks/install\\_ssl\\_certificate/](http://www.paessler.com/support/kb/prtg7/tricks/install_ssl_certificate/)

#### 14.6 Using the PRTG API (Application Programming Interface) (PRTG API の使用)

PRTG Network Monitorは、外部プログラム用として内部データへのアクセスを可能にするAPIを実装しています。これによって、ユーザーは、監視データベースからの情報にアクセスしたり、また、PRTGのオブジェクトデータベースをコントロールする独自のプログラムやスクリプトを作成することができます。APIは、HTTPベースで、データにアクセスするのにURLを使用します。

詳細は、"Help"メニューの"PRTG API"を参照して下さい。

## 14.7 Interface Definition for Custom EXE Sensors(カスタム EXE センサーのインターフェイス定義)

センサーが作動するたび、選ばれたEXEもしくはDLLファイルが実行されます。

### EXEセンサー

センサー設定のパラメーターフィールドに入力された文字列は、コマンドラインに配置されます。EXEファイルは結果をStandard OUTに出力します。データは以下の形式になっている必要があります。

```
value:message
```

値は、32ビット整数で、このセンサーの結果値として使用されます(バイト、ミリセカンドなど)。メッセージは任意の文字列で、データベースに保存されます。

EXEの終了コードは、次の値のうちいずれか一つでなければいけません。

- 0: ok
- 1: warning(警告)
- 2: system error(システムエラー(例:ネットワーク/ソケットエラー))
- 3: protocol error(プロトコルエラー(例:webサーバーが404を返す場合))
- 4: content error(コンテンツエラー(例:webページが要求された語を含まない場合))

もしEXEがPRTGプロセスへ制御を返さない場合、このセンサーに設定されたタイムアウト値に達するとすぐにそのプロセスは終了します。

センサーに使用したいEXEファイルとコマンドライン(cmd.exe)で簡単にテストすることができます。EXEファイルを開始し、結果をファイルに送信します。

例:

```
sensorexec parameter > result.txt
```

この場合、結果はresult.txtに書き込まれ、ノートパッドやその他テキストエディターでその結果を確認することができます。

### DLLセンサー

センサーがチェックされるたびに、選択されたDLLファイルが呼び出されます。DLLは、関数をエクスポートする必要があります。

```
function perform(para,msg:pchar):integer; stdcall;
```

paraとmsgは、0(ゼロ)で終わる文字列です。msgに割り当てられたバッファは255バイトです。DLLは必ずそれ以下のバイトで返されます。msgは、次の形式である必要があります。

```
value:message
```

値は、必ず32ビット整数で、このセンサーの結果値として使用されます(バイト、ミリ秒など)。メッセージは任意の文字列で、データベースに保存されます。

この関数の整数の戻り値は、次の値のうちのいずれか一つとなります。

- 0: ok
- 1: warning(警告)
- 2: system error(システムエラー(例:ネットワーク/ソケットエラー))
- 3: protocol error(プロトコルエラー(例:webサーバーが404を返す場合))
- 4: content error(コンテンツエラー(例:webページが要求された語を含まない場合))

**警告:** DLLの関数呼び出しが、制御を返さない場合は、全てのPRTGシステムはブロックされます。必ず、タイムアウトを確認し、信頼性のあるエラー管理を構築してください。この理由で、EXEセンサーを推奨します。

#### リンク

これらのカスタムセンサーについてのプロジェクト例が以下にあります。

- PRTGインストールの"PRTG Network Monitor¥custom sensors¥EXE"サブフォルダ内
- Paessler社webサイト内ナレッジベース: <http://www.paessler.com/support>
- オープンソースプラットフォームGoogle Codeのprt7addons webサイト: <http://code.google.com/p/prtg7addons/>

## 14.8 Acknowledgements(謝辞)

Build using Indy Internet Direct (<http://www.indyproject.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Uses the net-SNMP library, see "netsnmp-license.txt". Uses the DelphiZip library distributed under the GNU LESSER GENERAL PUBLIC LICENSE(<http://www.delphizip.net/>). Uses the Info.Zip library, license info in the provided "info-zip-license.txt". Uses FastMM (<http://sourceforge.net/projects/fastmm/>) and TPLockBox (<http://sourceforge.net/projects/tplockbox>) under the Mozilla Public License 1.1 (MPL 1.1, available from <http://www.mozilla.org/MPL/MPL-1.1.html>).