|  |
| --- |
| momentum OrcaBasic  要求仕様書 |

Ver 0.1

**目　次**

[変更履歴 5](#_Toc346719093)

[1. 本ドキュメントの目的 6](#_Toc346719094)

[2. 製品の位置づけ 7](#_Toc346719095)

[3. システム概要 8](#_Toc346719096)

[3.1. システム概要図 8](#_Toc346719097)

[3.2. 動作の概要 8](#_Toc346719098)

[4. モジュール別動作概要 10](#_Toc346719099)

[4.1. M（Model）部 10](#_Toc346719100)

[4.1.1. Data Retrieve 10](#_Toc346719101)

[4.1.1.1. GET SERVICE INFO COMMAND 10](#_Toc346719102)

[4.1.1.2. SEARCH FLOW COMMAND 10](#_Toc346719103)

[4.1.1.3. SEARCH PCAP COMMAND 10](#_Toc346719104)

[4.1.1.4. ZeroMQ 11](#_Toc346719105)

[4.1.2. Probe Selector 11](#_Toc346719106)

[4.1.3. Historical Data 11](#_Toc346719107)

[4.2. V（View）部 11](#_Toc346719108)

[4.2.1. Traffic Report Gen 11](#_Toc346719109)

[4.2.1.1. Traffic Report Genレポート設定画面 12](#_Toc346719110)

[4.2.1.1.1. レポート名称指定 12](#_Toc346719111)

[4.2.1.1.2. プローブ指定 12](#_Toc346719112)

[4.2.1.1.3. 5tupple指定 12](#_Toc346719113)

[4.2.1.1.4. 検索スタート時刻指定 12](#_Toc346719114)

[4.2.1.1.5. 検索間隔指定 12](#_Toc346719115)

[4.2.1.1.6. 表示間隔指定 13](#_Toc346719116)

[4.2.1.1.7. 計算方法指定 13](#_Toc346719117)

[4.2.1.1.8. 表示幅指定 13](#_Toc346719118)

[4.2.1.2. 大量データ検索に対する警告 13](#_Toc346719119)

[4.2.1.3. レポートの識別子 13](#_Toc346719120)

[4.2.1.4. Traffic Report Genレポート表示画面 14](#_Toc346719121)

[4.2.1.2.1. レポート名称一覧部 14](#_Toc346719122)

[4.2.1.2.2. グラフ表示部 14](#_Toc346719123)

[4.2.2. Life Cycle Report Gen 15](#_Toc346719124)

[4.2.2.1. Life Cycle Report Genレポート設定画面 15](#_Toc346719125)

[4.2.2.1.1. レポート名称指定 15](#_Toc346719126)

[4.2.2.1.2. 5tupple指定 15](#_Toc346719127)

[4.2.2.1.3. 検索範囲時間指定 15](#_Toc346719128)

[4.2.2.2. Life Cycle Report Genレポート表示画面 16](#_Toc346719129)

[4.2.3. PCAP Download 16](#_Toc346719130)

[4.2.4. Download URL Gen 17](#_Toc346719131)

[4.2.5. Login 17](#_Toc346719132)

[4.2.6. Menu 17](#_Toc346719133)

[4.2.7. Alert Setting 17](#_Toc346719134)

[4.3. C（Control）部 17](#_Toc346719135)

[4.3.1. Report Manager 17](#_Toc346719136)

[5. アプリケーションプログラミングインターフェース 19](#_Toc346719137)

[5.1. APIによる接続可否 19](#_Toc346719138)

[5.2. 登録プローブ検索 19](#_Toc346719139)

[5.3. 検索サービスステータス 19](#_Toc346719140)

[5.4. PCAPダウンロード 19](#_Toc346719141)

[6. システム管理 21](#_Toc346719142)

[6.1. DB接続情報管理 21](#_Toc346719143)

[6.2. ユーザ情報管理 21](#_Toc346719144)

[6.3. プローブ登録 21](#_Toc346719145)

[6.4. システムステータス表示 21](#_Toc346719146)

[6.5. システムアラート設定 22](#_Toc346719147)

[6.6. API機能のOn/Offおよびポート番号の指定 22](#_Toc346719148)

[6.7. データのバックアップ 22](#_Toc346719149)

[7. 性能要件 23](#_Toc346719150)

[7.1. Webページ移動 23](#_Toc346719151)

[7.2. データ取得とグラフへの描画 23](#_Toc346719152)

[7.3. Life Cycle Report用データの収集 23](#_Toc346719153)

[7.4. 過去のグラフデータの検索と描画 23](#_Toc346719154)

[7.5. バックアップ時の性能 23](#_Toc346719155)

[7.6. 冗長化 23](#_Toc346719156)

[Appendix 24](#_Toc346719157)

[Pcap Header 24](#_Toc346719158)

[Global Header 24](#_Toc346719159)

# 変更履歴

|  |  |  |  |
| --- | --- | --- | --- |
| バージョン | 更新日 | 更新者 | 更新内容 |
| V0.1 | 2013/1/22 | 松浦洋一 | 初版 |

# 本ドキュメントの目的

本ドキュメントはmomentum OrcaBasicの開発を開発パートナーに依頼するにあたり、設計に盛り込むべき要求事項をまとめたものであり、実現されるべき機能について、当社と開発パートナーの間で齟齬が発生しないようにすることを目的としています。これらの要求事項を実現するにあたり利用される具体的な技術や実装の方式については、開発パートナーから当社に提案し、当社の承認を得たうえで決定するようにしてください。

# 製品の位置づけ

momentum OrcaBasic（以降OrcaBasic）は、momentumがPacket Search Service（以降PSS）により外部に提供する統計データやPCAPデータを使いやすい形でユーザに提供することを目的とします。具体的には、以下のような特徴的な機能を提供することを目指します。

* Webブラウザをユーザインターフェースとする
* 検索条件はIPプロトコル、送信元アドレス、送信先アドレス、送信元ポート番号、送信先ポート番号を基本とし、オプションでHTTPヘッダのURL、EthernetフレームのETYPE、VLANタグが利用可能[[1]](#footnote-1)  
  **→検索条件は日時のみ可能（from, to を必須指定）**
* 設定した検索条件に従って取得された統計情報を可視化しレポート提供
* レポート上で動的な時間範囲の絞り込みを可能とし、絞り込んだ時間のデータを再表示
* レポートのデータプロット間隔は1秒以上の任意の時間を指定可能
* 絞り込んだグラフから該当するPCAPダウンロードが可能
* ~~パケットの移動を追尾するパケットライフサイクル表示~~

# システム概要

## システム概要図

以下にシステム概要図を示します。



水色部分が本ドキュメントの記述範囲となります。（Extended PSSは含まれていません）

## 動作の概要

クライアントは手元のBrowserによりOrcaBasicのすべての機能を操作します。OrcaBasicはBrowserからの指示内容により、必要に応じてZeroMQインターフェースを通じ、momentum プローブ内のPSSに検索要求を送り、検索結果を自身の持つDBに格納してGUI表示に利用します。

本システムの基本アーキテクチャはMVCモデルを前提にしています。画面の生成指示、画面からの入力情報の処理、グラフへのデータの描画、描画に必要なデータ検索の要求などはReport Manager によって行われます。Report Manager からの指示に従い、Traffic Report Gen、LifeCycle Report Gen、PCAP Downloadの各モジュールがGUI画面を生成します。また、同じくReport Managerからの指示により、Data RetrieveモジュールがPSSに対してデータ検索を要求します。複数プローブにまたがる検索が必要なLifeCycle情報の検索の場合は、Report ManagerはProbe Selectorに検索を要求します。検索された情報はHistorical Dataに蓄積され、ユーザ要求に従いグラフに描画されます。また、各グラフのコンフィグレーション（プローブ、５タプルなどの設定）はReport Configに蓄積されます。Historical DataとReport Configは機能的に異なるので上図では別データベースとして記載していますが、物理的なデータベース設計については開発パートナーの専門的助言の元で決定します。

また、SevOneなどの他のレポーティングツールでPCAPデータを絞り込む情報を生成し、これをOrcaBasicに送信することで、指定条件に基づくPCAPファイルを入手するためのURLが出力されるAPIを用意します。

# モジュール別動作概要

MVCモデルに従い、各部分ごとに関連するモジュールの概要を説明します。

## M（Model）部

### Data Retrieve

このモジュールは1台または複数台のmomentumのPSSに対してデータ検索要求を送ります。検索結果としては、そのプローブのサポートしているデータの種類やインターフェースのリスト、指定した条件に基づく統計データまたはPCAPデータが出力されます。

このモジュールが呼び出すのはPSSに用意されている以下の3つのAPIです。各APIの詳細はパケット検索システムの概要設計書を参照ください。

#### GET SERVICE INFO COMMAND

検索サービスの各種情報を取得します。

#### SEARCH FLOW COMMAND

指定した絞り込み条件に一致するパケット総数と総パケット長を取得します。統計情報として利用するほか、PCAPダウンロード前にサイズを確認するためにも使用します。

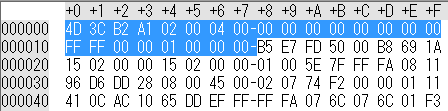
#### SEARCH PCAP COMMAND

指定した絞り込み条件に一致するパケットのファイル（PCAP）を取得します。取得されたデータはグローバルヘッダがついていないので、OrcaBasic内で付与する必要があります。参考までにグローバルヘッダ部の構造を記載します。

struct pcap\_file\_header構造体

|  |  |  |
| --- | --- | --- |
| 型 | 変数名 | 説明 |
| uint32\_t | magic |  |
| uint16\_t | version\_major |  |
| uint16\_t | version\_minor |  |
| int32\_t | thiszone | GMT to local correction |
| int32\_t | sigfigs | accuracy of timestamps |
| int32\_t | snaplen | max length saved portion of each packet |
| int32\_t | linktype | data link type |

具体的なグローバルヘッダの値についてはAppendixを参照してください。また、一般的なPCAPファイルをバイナリエディタで参照するのも参考になります。以下の例では一般的なPCAPファイルをバイナリエディタで開いたところです。青反転している部分がグローバルヘッダです。



#### ZeroMQ

Data RetrieveはPSSのAPIを呼び出すためのトランスポートレイヤプロトコルとして、ZeroMQ（Ver2.2）を使用します。ZeroMQについての詳細はパケット検索システムの概要設計書を参照ください。

### Probe Selector

このモジュールはパケットの移動を追尾するLifeCycle Reportに必要なデータを収集するために、複数のmomentumプローブに対する検索を実行するようData Retrieveに要求します。追尾したい特定のパケットが通過したプローブをリストするため、そのOrcaBasicに登録されたすべてのmomentumプローブに対して、指定時間内に指定の5タプルを持ったパケットが記録されているか検索し、タイムスタンプ順にプローブ名をリストします。その際、Sourceアドレス－Sourceポート、Destinationアドレス－Destinationポートの組み合わせを入れ替えたものを同一セッションの逆方向のパケットとして検索します。この手続きによってリストされたパケットを時系列に並べると、パケットの追尾情報になります。

### Historical Data

このデータストアは検索された情報を格納します。いったんプローブから検索された情報を再度検索する手間をなくし、検索時間を短縮することが目的です。

## V（View）部

### Traffic Report Gen

このモジュールはレポート設定画面、レポート表示画面からなります。レポートは特定の１つのプローブ上で測定された情報を可視化して表示します。以下、それぞれの画面の機能概要を説明します。

#### Traffic Report Genレポート設定画面

Traffic Report Genのレポート設定画面では、以下の項目についての指定を行います。

* レポート名称指定
* プローブ指定
* 5tupple指定
* 検索スタート時刻指定
* 検索間隔指定
* 表示間隔指定
* 計算方法指定
* 表示幅指定

##### レポート名称指定

レポート名称はユーザがわかりやすい名称を自分で決定し、レポート設定に名前を付けるためのものです。256バイトまでのUTF-8文字列での指定が可能です。

##### プローブ指定

検索対象となるプローブはあらかじめOrcaBasicに登録しておきます。プローブ指定では、登録されているプローブの中から必ず１つ選択しなくてはなりません。

##### 5tupple指定

5tuppleは任意指定で、全く指定しないことも許容されます。すなわち、Srcアドレス、Srcポート、Dstアドレス、Dstポート、プロトコルのどれも指定しない、または1つ以上の条件を指定することが可能です。

##### 検索スタート時刻指定

検索スタート時刻は指定必須で、秒単位のスタート時刻を指定します。現在時刻より新しい時刻を指定した場合、エラーが表示されます。

##### 検索間隔指定

検索間隔は検索を行う間隔を指定するためのもので、ユーザは1秒、5秒、15秒、30秒、1分のいずれかの間隔を選択します。PSSは1秒ごとのデータ管理を行っているので、検索間隔1秒を指定した場合はプローブでの測定値そのものが戻されますが、5秒、15秒、30秒、1分を指定した場合は集計結果が戻されます。すなわち、例えば5秒を指定すると、その5秒間にキャプチャされたすべてのパケットを対象とした検索が実行されます。

##### 表示間隔指定

表示間隔指定は検索結果を可視化データとしてグラフにプロットする間隔の指定で、ユーザは1秒、5秒、15秒、30秒、1分、5分、15分、1時間、6時間、12時間、1日、1週間、1ヶ月、1年のいずれかの間隔を選択します。表示間隔指定は検索間隔指定と同じかそれ以上でなくてはならず、このルールを逸脱した指定はエラーとなります。

##### 計算方法指定

計算方法指定は検索間隔＜表示間隔となるような指定を行った場合に、検索されたデータを表示用にサマライズする方法の指定です。平均、最大、最小のいずれかを選択指定することができます。例として、検索間隔1秒、表示間隔5秒の指定で計算方法に平均を選択した場合、グラフ上に表示されるデータは1秒データ5つ分の平均が5秒間隔でプロットされていきます。検索間隔＝表示間隔となるような指定の場合、検索されたデータの値がそのままグラフにプロットされていきます。サマライズされたデータは検索データとは別にHistorical Dataに蓄積されますが、この時サマライズされたデータに付与されるタイムスタンプは対象となるデータの最も新しい検索データのタイムスタンプが使用されます。すなわち、0時0分1秒から0時0分5秒までの5つのデータをサマライズしたデータには0時0分5秒というタイムスタンプが付与されます。

##### 表示幅指定

表示幅指定は、グラフのX軸の表示量の指定です。X軸は時間を示しているので、この指定はグラフにどれぐらいの時間分のデータを表示させるかを指定することになります。この幅は5秒以上であれば5秒刻みで任意の値を指定できます。ただし、グラフ画面に表示されるプロットデータ数（表示幅指定÷表示間隔指定）が720個を超えるような指定をするとエラーとなります。

#### 大量データ検索に対する警告

5tuppleに指定される条件が少なく検索量が増大する場合、あるいは時間帯の指定が長時間で検索量が増大する場合、結果の表示に時間がかかる旨を警告表示してユーザの了解を得たうえで検索をReport Managerに依頼します。

#### レポートの識別子

各レポート設定には内部的に一意のIDが付与され、そのIDと指定された情報がセットにされてReport Configデータストアに蓄積されます。また、Data Retrieveに対する検索要求もこのIDとともに送信され、検索結果はIDとセットでHistorical Dataデータストアに蓄積されます。

#### Traffic Report Genレポート表示画面

Traffic Report Genのレポート表示画面は、レポート名称一覧部（左ベイ）とグラフ表示部（右ベイ）からなります。

##### レポート名称一覧部

Traffic Report Genレポート設定画面で指定したレポート名称の一覧がリスト表示され、クリックすると該当するグラフがグラフ表示部（右ベイ）に表示されます。

##### グラフ表示部

レポート名称一覧部でレポート名称を選択すると、グラフ表示部に該当するグラフが表示されます。グラフ上のデータは、グラフ表示はレポート名称一覧部からクリックした直後の初期表示では、現在時刻がグラフの右端になるように行われます。また、過去にさかのぼってグラフ表示できるよう、表示時間帯を過去・未来に移動するためのボタンが画面上に配置されます。現時点では、グラフ描画のためにHighCharts JSライブラリ[[2]](#footnote-2)の利用を想定しています。

レポート表示直後のデフォルト状態では、グラフ上のデータは表示間隔指定ごとに自動的に更新されますが、ユーザ操作により自動更新が止められるように、更新のOn/OffのためのスイッチをGUI上に設置します。

表示されたグラフ上でマウスを左クリックボタンでドラッグすることで、表示幅内でのデータのズームを行います。ズームが行われるとグラフの自動更新は自動的にOffに変更されます。ただし、1プロットの精度は1秒であるため、ズームを行っても1秒より細かいデータが表示できるわけではありません。ズームした場合の新しい表示幅指定はズーム範囲の左端から右端までとなります。

1秒よりも小さい単位でデータを参照したい場合、GUI上に用意される「マイクロバーストの単位指定」メニューから単位を選択したうえでドラッグを行います。指定できる単位は0.1秒、0.01秒、0.001秒のいずれかです。この指定をしたうえでグラフ上でのズームが行われると、そのグラフで使用されているプローブ指定と5tuppleはそのまま、ズーム範囲の左端を検索スタート時刻指定、検索間隔指定を0.001秒、表示間隔指定は「マイクロバーストの単位指定」で指定された単位、計算方法指定は常に「最大」を指定、表示幅指定はズーム範囲の右端の時間を指定してTraffic Report Genに要求します。

グラフ上で右クリックを行うと、その時点のグラフの表示幅分のデータを含むPCAPファイルをダウンロードするメニューが表示されます。このメニューを選択すると、ダウンロード対象となるパケット数とパケットサイズが検索されてダイアログ表示され、本当にダウンロードを実行するかどうか尋ねられます。「はい」を押下するとPCAPファイルに付ける名前の入力が求められ、入力してOKするとダウンロードが開始されます。保存したPCAPファイルはWiresharkで利用します。このためには、エンドユーザがWebBrowserを利用する端末にWireSharkをインストールしておく必要があります。「いいえ」を押下するとダウンロードはキャンセルされます。一度ダウンロードされたPCAPファイルは、それ以降はPCAP Download画面に一覧で保持されます。

### Life Cycle Report Gen

このモジュールはレポート設定画面、レポート表示画面からなります。レポートは特定の１つのパケットが複数のプローブを通過していく様子を可視化して表示します。以下、それぞれの画面の機能概要を説明します。

#### Life Cycle Report Genレポート設定画面

Life Cycle Report Genのレポート設定画面では、以下の項目についての指定を行います。

* レポート名称指定
* 5tupple指定
* 検索範囲時刻指定

##### レポート名称指定

レポート名称はユーザがわかりやすい名称を自分で決定し、レポート設定に名前を付けるためのものです。256バイトまでのUTF-8文字列での指定が可能です。

##### 5tupple指定

5tuppleは追尾するパケットを一意に定めるため、5項目すべてを指定します。どの項目も省略することはできません。記入漏れがあるとエラーになります。実際の検索はSrcアドレス、ポートとDstアドレス、ポートを入れ替えた組み合わせでも行われます。

##### 検索範囲時間指定

検索範囲時間とは、該当パケットを追尾する時間帯の指定です。開始の時刻と終了の時刻を指定してください。最大指定範囲は5分です。指定範囲が長ければ長いほど、結果の生成の時間を要します。また、時間による範囲指定となりますので、必ずしもトランザクションの最初から最後までを含む結果にならないことがあり得ます。

#### Life Cycle Report Genレポート表示画面

Life Cycle Report Genのレポート表示画面は、縦軸に時間（上から下へ経過）、横軸には左端にSrc、右端にDst、その間に通過したプローブのプローブ名が配置され、検索範囲時間指定によって指定された時間の中でタイムスタンプの早い順に上から下へ、左から右へと通過ポイントがプロットされます。行きのパケットがSrc側からDstに到達した後、今度はDst側からSrcに戻るパケットが上から下へ、右から左へとプロットされます。以下はそのイメージ図です。



この例では「P2-eth0」と「P2-eth1」の間で時間がかかっていることがわかります。また、途中でパケットが喪失している場合も発見できる可能性があります。

なお、momentumプローブは複数インターフェースでキャプチャできるので、1台のプローブに対する入力インターフェースは１つだけでなく２つ以上存在する場合があります。そのような場合、Life Cycle Report Genはグラフに表示するプローブ名称の後ろにつけられたインターフェース名で識別します。この識別子は、PSSに対してGET SERVICE INFOを送信した結果として返される「入力インターフェースに指定できる値」にあらかじめつけられているので、OrcaBasicではその値をそのまま利用します。

### PCAP Download

このモジュールは、Traffic Reportのグラフ上で右クリックしてダウンロードを行ったPCAPファイルを一覧で保持し、ユーザが再度PCAPファイルを必要とする際にmomentumプローブから再ダウンロードすることなくPCAPを提供するために用意されています。PCAPファイルはどのレポートからダウンロードされたか判別できるよう、レポート名称とダウンロード時にユーザが指定したPCAPファイル名の組み合わせで一覧表示されます。「Load」のリンクをクリックすると、WireSharkが起動され、PCAPが開かれます。

### Download URL Gen

このモジュールは、サードパーティのアプリケーションからPCAPファイルダウンロード用のOrcaAPIが呼び出された時、そのPCAPファイルをリモートからダウンロードするためのURLを生成して返送します。このモジュールはGUIを持ちません。APIリクエストには次の引数を付与する必要があります。

* プローブ指定
* 5tupple指定
* PCAPスタート時刻指定
* 集計秒指定

詳細は後述の[アプリケーションプログラミングインターフェース](#アプリケーションプログラミングインターフェース)のページをご確認ください。

### Login

このモジュールはユーザ認証のためにユーザ名とパスワードの入力を受け付けます。ユーザ情報はReport Configに保管されています。Loginはサブ画面としてパスワード変更用の画面を持ちます。

### Menu

このモジュールは認証済みユーザに、各画面へのリンクを提供します。また、レポートに対して設定された閾値を超えるデータが検出された場合、そのアラートが画面にリスト表示されます。

### Alert Setting

このモジュールは、各レポートに設定した閾値を超えたデータが検出された場合にアラートをユーザに通知するための情報を設定します。アラートを送信する先の情報はすべてのレポートに共通の設定となり、メールアドレス（最大3アドレス）とSNMP Trap送信先アドレスを指定できます。

## C（Control）部

### Report Manager

Report ManagerはV部に入力されたユーザ要求を処理するため、V部の各モジュールからリクエストを受け取り、M部のメソッドを呼び出して結果をV部に戻します。また、V部の各レポート設定画面において指定されたパラメータは、Report ManagerからReport Configデータストアに保存されます。

ユーザがBrowserから最初に呼び出すURLはReport ManagerモジュールのURLになります。ReportManagerは初期画面としてユーザ認証画面を表示するためにLoginモジュールを呼び出します。認証をパスするとアラートリストおよびユーザーメニューを表示するためにMenuモジュールを呼び出します。その後は各画面に実装された画面移動用メニューを選択することで任意の画面に移動できます。移動のリクエストはいったんReport Managerに送られ、Report Managerが必要な画面モジュールを呼び出します。

# アプリケーションプログラミングインターフェース

## APIによる接続可否

APIによる外部からの接続は、システム管理画面に用意された「API接続可否指定」部分で機能がOnに指定された状態でのみ利用可能です。Off時にAPIによる接続が試みられた場合、APIはエラーを返します。

## 登録プローブ検索

API名称：OrcaGetProbeList

API引数：

* OrcaのIPアドレス
* API接続ポート番号
* リスト：プローブID<TAB>プローブのアドレス（戻り値用）

API戻り値：

* API接続可否指定がOffの場合はエラー

## 検索サービスステータス

## PCAPダウンロード

API名称：OrcaGetServiceInfo

API引数：

* プローブID
* 5tupple指定
* PCAPスタート時刻指定
* 集計秒指定
* PCAPダウンロード用URL（戻り値用）

API戻り値：

* API接続可否指定がOffの場合はエラー

API名称：OrcaGetPCAPURL

API引数：

* プローブID
* 5tupple指定
* PCAPスタート時刻指定
* 集計秒指定
* PCAPダウンロード用URL（戻り値用）

API戻り値：

* API接続可否指定がOffの場合はエラー

# システム管理

システム管理の項目として以下の機能が提供されます。

## DB接続情報管理

データベースに接続するためのユーザ名、パスワードなど、必要な情報を設定するためのGUIを備えます。DBの選択は開発パートナーの意見をふまえた上で決定しますが、本ドキュメント執筆時にはMySQLを想定しています。

|  |
| --- |
| データベース名 |
| ユーザ名 |
| パスワード |
| 備考 |

## ユーザ情報管理

以下の情報を管理し、新規追加・削除・更新を行うためのGUIを備えます。パスワードは一方向関数によりHashしたうえで格納します。

|  |
| --- |
| ユーザ名 |
| パスワード |
| 本名 |
| 所属 |
| 備考 |

## プローブ登録

OrcaBasicにmomentumプローブの情報を登録します。

|  |
| --- |
| プローブIPアドレス |
| プローブ名 |

## システムステータス表示

システム稼働に必要なプロセスの状態を表示するGUIを備えます。本システムにおいて稼働に問題が生じたときのトラブルシュートなどに利用します。この機能を提供するため、各プロセス実装時には、そのプロセスが稼働していることを外部から確認できる機能（isAlive）を用意する必要があります。

また、データベースの容量についても監視し、DB容量不足によりデータ保存に支障が出る前に管理者に通知します。

## システムアラート設定

システム稼働に問題が生じた場合に管理者に通知する機能を提供し、その通知先のメールアドレス（最大3つ）を設定するためのGUIを提供します。

## API機能のOn/Offおよびポート番号の指定

OrcaBasicからmomentumにAPI接続する際に利用するポートの指定および、外部からAPI経由で検索を実施する機能のOn/Offと、Onの場合の接続先Portを指定します。Offの場合、ポート番号入力フィールドは使用できなくなります。

## データのバックアップ

設定データおよび過去データの保全のため、データベースのバックアップの手続きを準備します。ただし、本バージョンではGUIは用意しません。

# 性能要件

本システムはPSSとの連係で動作するため、PSSのパフォーマンスがシステム全他のパフォーマンスに大きく影響しますが、OrcaBasic単体のパフォーマンスも以下の点において配慮する必要があります。

## Webページ移動

メニュー選択などでページ移動する際の新ページの表示は、ユーザが要求を送信してから5秒以内で完結することを目安とします。

## データ取得とグラフへの描画

PSSから統計情報を取得した後に実施する事項として、

1. DBへのデータ保存
2. グラフへの描画

があります。描画の即時性とデータの保全性を合わせて検討し、１）と２）のどちらを先行処理とするか決定する必要があります。

## Life Cycle Report用データの収集

Life Cycle Report用のデータは接続された全プローブから収集することになり、ある程度時間を要する処理になると思われます。よって、以下の機能を用意することでユーザが感じる処理待ちの不満を軽減します。

1. 処理開始前に、該当処理はある程度時間がかかるという予告表示を出す
2. 処理の進捗がユーザにわかるような画面表示を行う

このうち、２）の処理を実現するためには処理の全体量を事前に把握する必要があるので、その方法について検討が必要です。

## 過去のグラフデータの検索と描画

GUI操作で過去のレポートを参照する際、DB検索とグラフへの描画はおおむね3秒以内に完結することが望まれます。

## バックアップ時の性能

バックアップのタスク実行時に、データ取得、保存、描画に欠損が出ないようにします。

## 冗長化

本バージョンでは冗長化機能は実装しません。

# Appendix

## Pcap Header

### Global Header

* This header starts the libpcap file and will be followed by the first packet header:
* typedef struct pcap\_hdr\_s {
* guint32 magic\_number; /\* magic number \*/
* guint16 version\_major; /\* major version number \*/
* guint16 version\_minor; /\* minor version number \*/
* gint32 thiszone; /\* GMT to local correction \*/
* guint32 sigfigs; /\* accuracy of timestamps \*/
* guint32 snaplen; /\* max length of captured packets, in octets \*/
* guint32 network; /\* data link type \*/
* } pcap\_hdr\_t;
  + magic\_number: used to detect the file format itself and the byte ordering. The writing application writes 0xa1b2c3d4 with its native byte ordering format into this field. The reading application will read either 0xa1b2c3d4 (identical) or 0xd4c3b2a1 (swapped). If the reading application reads the swapped 0xd4c3b2a1 value, it knows that all the following fields will have to be swapped too.
  + version\_major, version\_minor: the version number of this file format (current version is 2.4)
  + thiszone: the correction time in seconds between GMT (UTC) and the local timezone of the following packet header timestamps. Examples: If the timestamps are in GMT (UTC), thiszone is simply 0. If the timestamps are in Central European time (Amsterdam, Berlin, ...) which is GMT + 1:00, thiszone must be -3600. In practice, time stamps are always in GMT, so thiszone is always 0.
  + sigfigs: in theory, the accuracy of time stamps in the capture; in practice, all tools set it to 0
  + snaplen: the "snapshot length" for the capture (typically 65535 or even more, but might be limited by the user), see: incl\_len vs. orig\_len below
  + network: link-layer header type, specifying the type of headers at the beginning of the packet (e.g. 1 for Ethernet, see [tcpdump.org's link-layer header types page](http://www.tcpdump.org/linktypes.html) for details); this can be various types such as 802.11, 802.11 with various radio information, PPP, Token Ring, FDDI, etc.

/!\ Note: if you need a new encapsulation type for libpcap files (the value for the network field), do **NOT** use **ANY** of the existing values! I.e., do **NOT** add a new encapsulation type by changing an existing entry; leave the existing entries alone. Instead, send mail to [tcpdump-workers@lists.tcpdump.org](mailto:tcpdump-workers@lists.tcpdump.org) , asking for a new link-layer header type value, and specifying the purpose of the new value.

1. オプション検索機能を追加する場合、PSSはExtended PSSが必要となります。 [↑](#footnote-ref-1)
2. このライブラリの詳細については<http://www.highcharts.com/products/highcharts> を参照してください。 [↑](#footnote-ref-2)