



**東陽テクニカ**

**Synesis**

**取扱説明書**

---

2018/01/09

A010-1799-90 Rev.J

# 改訂履歴

版数	改訂日	内容
Rev.A	2015/03/25	初版
Rev.B	2015/06/01	Synesis 1.0
Rev.C	2016/02/24	Synesis 1.1
Rev.D	2016/03/16	Synesis 2.0
Rev.E	2016/06/10	Synesis 2.1
Rev.F	2016/08/10	Synesis 2.2
Rev.G	2016/11/22	Synesis 2.5
Rev.H	2017/02/28	Synesis 3.0
Rev.I	2017/05/15	Synesis 3.1
Rev.J	2018/01/09	Synesis 3.5

# 安全上の注意

---



本製品をお使いになる前に、この「安全上のご注意」を良くお読みください。

下記に反する取り扱いをした場合、人体への傷害、または機器の破損が発生する可能性があります。

- 感電事故防止のため、電源コードの保護導体端子を必ず接地してご使用ください。
- 付属の電源コード以外の電源コードを使用しないでください。
- 本装置の仕様範囲外の電源電圧は使用しないでください。
- 機器の吸気口、排気口をふさがないようにしてください。
- 各機器の分解、改造は絶対に行わないでください。メンテナンスやサービスが必要な場合には弊社へご連絡ください。
- 異臭や煙、その他異常を感じた場合には直ちに使用を中止し、電源コードを抜いてください。その後弊社へご相談ください。
- 本製品を改造しないでください。認定されていないソフトウェア、ハードウェアがインストールされた場合、製品が正常に動作しない場合があります。
- 本製品はクラス 1 レーザ対象製品です。

# ソフトウェアライセンス契約

---

本ソフトウェアライセンス契約(「ライセンス契約」)を注意深くお読みください。本ライセンス契約の諸条件に同意されない場合は、本ソフトウェアをインストールもしくはご使用にならないでください。本ソフトウェアを使用した時点で、お客様は、本契約の諸条件に従うことに同意したものと見なされます。

## 1. ライセンスの許諾

東陽テクニカは、1 台のコンピュータにつき 1 本の本ソフトウェアをインストール及び使用する非独占的实施権をお客様に付与します。しかし、本ソフトウェアのライセンスが「同時使用」用として付与されている場合、共有サーバ上に本ソフトウェアをインストールできますが、同時使用に認可された「最大数」を超えるユーザが本ソフトウェアを同時使用することはできません。

「使用」とは、文書と本契約に従って、アクセス、保存、ロード、インストール、実行、表示または本ソフトウェアの機能によりその他の便益を得ることを意味します。

## 2. 所有権、著作権および知的財産権

本ソフトウェアは、東陽テクニカまたはその第三者サプライヤに独占的に所有権、著作権及びその他の知的財産権が帰属します。

お客様が本ソフトウェアを使用するライセンスは、本ソフトウェアの所有権をお客様に移転するものではなく、また本ソフトウェアに係るいかなる権利をもお客様に売却するものではありません。

東陽テクニカ及び東陽テクニカの第三者サプライヤは、本契約の違反があった場合には、自らの権利を防御することができます。

## 3. 複製と改造の禁止

お客様は、本ソフトウェアには、第三者サプライヤに所有権、著作権が帰属するソフトウェア(「第三者ソフトウェア」)が含まれていることを了解しています。お客様は、本ソフトウェアをアーカイブ目的以外に複製すること、またいかなる改造を加えることはできません。ただし、本ソフトウェアに含まれる、第三者ソフトウェアについては、当該第三者ソフトウェアのライセンス条件に従うものとします。お客様は、本項の規定に従って許可された複製や改造されたソフトウェアに関しては、その全てに、本ソフトウェアのオリジナル上の全ての著作権情報を正確に記載しなくてはなりません。お客様は、社内外を問わず、掲示板やこれに類するシステム上に本ソフトウェアを複製してはなりません。東陽テクニカの書面による事前の許可がある場合を除いて、いかなる書類や文書もコピーしてはなりません。



#### 4. 逆コンパイル、逆アセンブルおよび暗号解読の禁止

お客様は、マシン上で実行可能な本ソフトウェアのオブジェクトコードのみを使用することをライセンスされます。また、お客様は前項にて規定される第三者ソフトウェアのライセンス条件にて許可される場合を除き、本ソフトウェアやその一部を逆コンパイル、逆アセンブルおよび暗号解読することは、いかなる形であれ禁じられます。

本ソフトウェアの分解・逆コンパイル・暗号解読を何者かが試みているとの情報を得た場合には、お客様はかかる試みに関して知っている全ての情報を直ちに東陽テクニカに提供することに同意します。

#### 5. 合法的使用への限定

お客様は本ソフトウェアのいかなる違法使用、または違法な活動を助長するための本ソフトウェアの使用を固く禁じられます。

お客様の本ソフトウェアの使用に適用される、全ての日本法ならびに適用される全ての法律を理解し遵守することは、全てお客様の責任です。

本ソフトウェアの使用に際してお客様が行った、いかなる不正な又は非合法的な行為に伴う責任や負担に関しては、東陽テクニカはこれを明確に否認します。

お客様が本ソフトウェアを違法に使用したことが原因で、東陽テクニカが請求を受けたり、訴訟を提起されたり、裁判費用を請求されたりした場合には全て、お客様は東陽テクニカを免責することに同意します。

#### 6. 譲渡

本ソフトウェアを使用するお客様のライセンスが、他の個人とその所属する組織に合法的に譲渡された場合には、お客様のライセンスは自動的に終了します。

譲渡にあたっては、全てのコピーや関連文書を含む本ソフトウェアを譲受者に引き渡さなくてはなりません。譲渡の条件として、譲受者は本ライセンス条項を受け入れなければなりません。

#### 7. 契約の解除

東陽テクニカは、本ライセンス条項のいずれかが遵守されなかったと通知することにより、直ちにお客様のライセンスを解除することができます。解除に伴い、本ソフトウェアと複製および改造された部分の全てを、その形態を問わずお客様が破棄しなくてはなりません。

#### 8. 輸出要件

お客様は、適用されうるいかなる法律又は規制に違反して、本ソフトウェア、複製又はその改造品を輸出または再輸出してはなりません。

## 9. 保証の制限

全てのソフトウェアは、材料や製造上の欠陥のない記憶媒体で配布されることを東陽テクニカは保証しますが、これは正常にインストールされ使用されることを条件とします。

もし東陽テクニカがお客様よりご購入後最初の 30 日間以内にそのような欠陥の連絡を受けた場合、お客様がその欠陥のある記憶媒体をお客様の費用負担でお客様の購入レシートのコピーとともに東陽テクニカに返送いただくという条件で東陽テクニカは欠陥のある記憶媒体を無償で交換します。本欠陥が事故、悪用、または不正使用による場合は、この保証は適用されません。記憶媒体の交換が行われた場合は、元の保証期限の残りの期間について保証が継続します。

## 10. 保証の免責事項

本ソフトウェアは、“現状のまま”でお客様に提供されており、上記の「保証の制限」で認められる以外は、口頭、書面、明示又は黙示を問わず、いかなる保証や条件も伴いません。

東陽テクニカは、商品性または十分な品質、および特定の目的への適性に関する黙示的保証および/または条件といった、ただしこれらに限定されない、本ソフトウェアに関する、明示的または黙示的なあらゆる保証を否認することをここに明確に宣言します。

東陽テクニカは、本ソフトウェアに含まれる機能がお客様の要件に適合すること、あるいは本ソフトウェアの動作が中断せず、エラーの発生しないこと、または本ソフトウェアの不具合が修正されることを保証しません。さらに東陽テクニカが、本ソフトウェアもしくは関連するドキュメンテーションの使用または使用結果について、その正確性、精度、信頼性等を保証するか、なんらかの表明を行うことはありません。

## 11. 責任の制限

東陽テクニカの過失や、損傷したり不具合があるとされる製品を含むあらゆる原因により引き起こされる、お客様またはお客様の所属する組織が被るいかなる損失や損害に関する東陽テクニカの責任は、上記の不具合等が発見できるものであっても潜在的なものであっても、すべての場合に、損失や損害の申し立ての対象となる特定のソフトウェア製品のライセンス単価を上回らないものとします。

ただし、東陽テクニカは自らの裁量で、不具合のあるまたは損傷を受けた製品の交換をもって、上記の保証(ライセンス購入代金の返還)に代えることができます。

東陽テクニカの過失であるとの申し立てを含み、いかなる場合であってもデータの滅失又は直接的、特別的、偶発的、結果的（利益損失を含む）またはその他の損失に対して、東陽テクニカは契約責任、不法行為責任その他の法的責任などを根拠とする責任の一切を、負わないものとします。

本契約は、日本の法律に準拠します。

# 著作権・商標

---

このマニュアルのいかなる部分も株式会社東陽テクニカの書面による許可なしに、形態、方法を問わず、複写、送信、転載、検索システムへの保存、及び他言語に翻訳することを禁じます。

Synesis は、株式会社 東陽テクニカの登録商標または商標です。

Microsoft は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows の正式名称は、Microsoft Windows Operating System です。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標または商標です。

Ubuntu は、Canonical Ltd.の商標または登録商標です。

Intel、Pentium、Xeon、Celeron は、Intel Corporation またはその子会社の米国およびその他の国における登録商標または商標です。

Java およびすべての Java 関連の商標は、米国 Oracle Corporation の米国およびその他の国における登録商標または商標です。

Apache、Tomcat は、Apache Software Foundation の登録商標または商標です。

Ethernet は、米国 XEROX Corporation の登録商標です。

DELL、PowerEdge は、Dell Inc.の米国およびその他の国における登録商標または商標です。

本文中のその他の登録商標及び商標はそれぞれの所有者に帰属します。

本文中、®（登録商標）、©（コピーライト）等の各商標マークは省略しています。

# 問い合わせ先

---

本製品に関するお問い合わせ先は以下の通りです。

## 営業的なお問い合わせ

資料請求・価格・納期・オプション追加・打ち合わせ/デモ依頼・保守更新など

(株) 東陽テクニカ 情報通信システムソリューション部

TEL : 03-3245-1250

FAX : 03-3246-0645

E-mail : synesis-sales@toyo.co.jp

受付時間: 月曜～金曜 9:30～17:30 (土日、祝日、年末年始および弊社指定休日を除く)

## 技術的なお問い合わせ

操作/設定方法・各種調査・ハードウェア異常など

(株) 東陽テクニカ 第1技術部 第1課

TEL : 03-3279-0771

FAX : 03-3246-0645

E-mail : synesis-support@toyo.co.jp

受付時間: 月曜～金曜 9:30～17:30 (土日、祝日、年末年始および弊社指定休日を除く)

いずれの場合も、電話にてご連絡の際は、「Synesis 担当」とお申し付けください。

# 目次

改訂履歴.....	i
安全上の注意 .....	ii
ソフトウェアライセンス契約 .....	iii
著作権・商標 .....	vi
問い合わせ先 .....	vii
1. Synesis の概要 .....	1
2. 起動と終了 .....	2
2.1. Synesis の起動 .....	2
2.1.1. Synesis Distributed .....	2
2.1.2. Synesis Portable .....	2
2.2. Synesis へのアクセス .....	3
2.3. リモートデスクトップ .....	4
2.4. Synesis の終了 .....	6
2.4.1. Synesis Distributed .....	6
2.4.2. Synesis Portable .....	6
3. Synesis の画面構成 .....	7
3.1. メインメニュー .....	9
3.2. ツールバーメニュー .....	10
4. ダッシュボード .....	11
4.1. ダッシュボード・タブ .....	12
4.2. ダッシュボードの追加 .....	12
4.3. 時間範囲の選択 .....	13
4.4. ダッシュボードの名称変更 .....	13
4.5. グラフの追加、並べ替えと削除 .....	14
4.5.1. グラフの種類と設定方法 .....	15
4.6. グラフの設定変更 .....	17
4.6.1. チャネルの表示/非表示の切り替え .....	18

5. エージェント.....	19
5.1. エージェント・ペイン .....	19
5.2. 全てのエージェント・ワークスペース .....	20
5.3. エージェント・ワークスペース.....	21
5.3.1. 概要 タブ.....	22
5.3.2. レコード タブ .....	36
5.3.3. ロック タブ .....	41
5.3.4. トレースファイル タブ .....	43
5.3.5. 外部データソース タブ .....	46
5.3.6. リアルタイムデコードタブ.....	47
5.3.7. デコード.....	48
5.4. キャプチャレコード・ワークスペース .....	52
5.4.1. 時間範囲を指定しての拡大表示 .....	55
5.4.2. トレースの保存 .....	56
5.4.3. 統計のエクスポート .....	59
5.5. リモートエージェント .....	60
5.5.1. 機能の概要.....	60
5.5.2. 各エージェントの操作方法.....	60
6. アラート .....	61
6.1. 検索 .....	62
6.1.1. アラートの設定 .....	62
6.1.2. 検索する時間範囲設定 .....	62
6.1.3. 検索条件の指定 .....	63
6.2. グラフとアラートリスト .....	64
6.2.1. 指定範囲の拡大表示 .....	65
7. レポート .....	66
7.1. レポートリスト.....	67
7.1.1. 検索 .....	67
7.1.2. 削除 .....	67
7.1.3. レポートの保存場所 .....	67
7.2. レポートテンプレート .....	68
7.2.1. 検索 .....	68
7.2.2. 新規 .....	68
7.2.3. 削除 .....	71

7.2.4.	エクスポート.....	71
7.2.5.	インポート.....	71
7.3.	レポートプラン.....	72
7.3.1.	検索.....	72
7.3.2.	新規.....	73
7.3.3.	削除.....	75
7.3.4.	レポートプランの編集.....	75
7.4.	レポートの形式.....	76
8.	APM/NPM 解析.....	77
8.1.	解析する時間範囲の指定.....	78
8.2.	APM 解析.....	79
8.2.1.	APM 解析での検索.....	80
8.2.2.	APM 解析のフローテーブル.....	81
8.3.	NPM 解析.....	82
8.3.1.	NPM 解析での検索.....	82
8.3.2.	NPM 解析でのフローテーブル.....	83
8.4.	解析結果の絞込みとデータの抽出.....	84
8.4.1.	指定範囲の拡大.....	84
8.4.2.	トレースファイルの保存.....	85
8.4.3.	フローテーブルを CSV として保存.....	85
9.	マイクロバースト.....	86
9.1.	マイクロバーストのアラートグラフとテーブル.....	88
9.2.	回線使用率の設定と時間範囲選択.....	89
9.2.1.	選択範囲の拡大表示.....	90
9.2.2.	閾値の変更.....	91
10.	パケットリプレイヤー.....	92
10.1.	プロファイルの作成.....	93
10.1.1.	トレースファイルの追加.....	93
10.1.2.	キャプチャレコードの追加.....	95
10.2.	プロファイルの設定.....	97
10.2.1.	パケットフィルタと置換フィルタ.....	99
10.2.2.	置換アイテムの種類と設定方法.....	100
10.3.	プロファイルの再生.....	105

10.3.1.	リプレイの開始・停止 .....	106
10.3.2.	リプレイの一時停止 .....	106
10.4.	オーバービュー画面 .....	107
11.	パスワードの変更 .....	108
12.	構成 .....	109
12.1.	Synesis の初期化 .....	111
12.1.1.	初期化対象一覧 .....	112
12.2.	設定のバックアップ・リストア .....	113
12.2.1.	設定のバックアップ作成とダウンロード .....	113
12.2.2.	設定のリストア .....	114
12.2.3.	バックアップファイルの削除 .....	114
12.2.4.	バックアップ対象一覧 .....	115
12.3.	ユーザ .....	116
12.3.1.	ユーザの新規登録と登録情報の編集 .....	117
12.3.2.	ユーザの削除 .....	117
12.4.	時刻同期 .....	118
12.5.	アドレス帳 .....	119
12.6.	保存フィルタ .....	120
12.6.1.	保存フィルタの新規登録 .....	120
12.6.2.	保存フィルタの削除 .....	130
12.6.3.	保存フィルタの編集 .....	130
12.7.	トレースの保存 .....	131
12.8.	アラート .....	132
12.9.	通知設定 .....	133
12.10.	通知グループ .....	134
12.11.	通知先 .....	135
12.11.1.	通知先の新規登録 .....	135
12.11.2.	通知メールのサーバ設定 .....	136
12.12.	解析 .....	137
12.13.	サイト .....	139
12.14.	サーバ グループ .....	140
12.15.	プロトコル .....	141
12.15.1.	全て タブ .....	141



12.15.2.	L2 イーサタイプ タブ .....	142
12.15.3.	L3 プロトコル タブ .....	143
12.15.4.	L4 プロトコル タブ .....	144
12.16.	アプリケーショングループ .....	145
12.17.	マイクロバースト .....	147
Appendix A 用語集 .....		148
A.1	略語一覧 .....	148
Appendix B キャプチャフィルタの種類と設定方法 .....		149
B.1	MAC アドレス .....	150
B.2	VLAN .....	151
B.3	イーサタイプ .....	151
B.4	IP フロー .....	152
B.5	フロー .....	153
B.6	アプリケーション .....	154
B.7	パターン .....	155
Appendix C 統計値の CSV ファイル .....		157
Appendix D チャネルグループとデータソース .....		158
D.1	チャネルグループ .....	158
D.1.1	概要 .....	158
D.1.2	エージェント画面 .....	158
D.2	データソース .....	159
D.2.1	概要 .....	159
D.2.2	チャネルグループ無しの場合 .....	159
D.2.3	リモートエージェント有り、チャネルグループ無しの場合 .....	160
D.2.4	チャネルグループ有りの場合 .....	160
D.2.5	リモートエージェント有り、チャネルグループ有りの場合 .....	162
Appendix E タイムサーバとのインテグレーション .....		163
E.1	概要 .....	163
E.2	準備と作業手順 .....	164
E.2.1	PPS 時刻同期の設定手順 .....	165
E.2.2	PTP 時刻同期の設定手順 .....	168
E.3	設定の切り戻し .....	173

Appendix F Synesis のディスク構成.....	175
F.1 概要 .....	175
F.2 パケットデータ領域 .....	175
F.3 OS・統計解析データ領域 .....	175
F.4 データバンク領域 .....	176
Appendix G 使用するポートの一覧 .....	177
Appendix H モデルによる違い.....	178
Appendix I 各モデルのポートとチャネルの配置 .....	179
I.1 Synesis Distributed(1U 版)ポート図.....	179
I.2 Synesis Distributed (2U 版)ポート図.....	180
I.3 Synesis Portable-1 .....	181
I.4 Synesis Portable-2 .....	182
I.5 Synesis Portable-3 .....	183
I.6 Synesis Portable-4 .....	184
Appendix J RESTful API .....	185

# 1.Synesis の概要

「Synesis」は、イーサネット回線を通るパケットをキャプチャし、パケットの翻訳や統計を表示するLANアナライザです。大容量のパケットを連続して取りこぼしなくキャプチャすることができ、高トラフィックなネットワーク通信も正確に解析することが可能です。

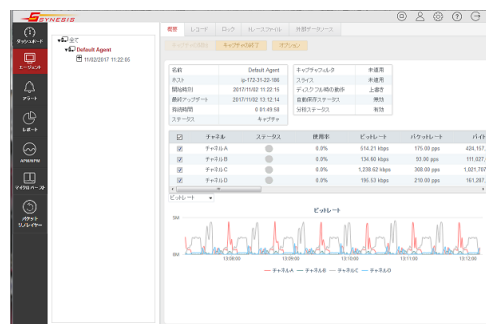
通信障害の解決やセキュリティリスクの低減、通信品質劣化の防止にお役立てください。

キャプチャの実行から解析までの主な流れは以下の通りです。

## 1) パケットキャプチャの実行

パケットのキャプチャを実行します。

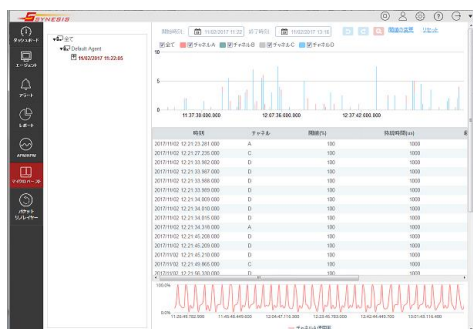
キャプチャ開始から終了までの 1 回のキャプチャが 1 キャプチャレコードとして保存されます。キャプチャフィルタやスライス機能、キャプチャデータのロック設定などは、採取するパケットの選択や保存形式に直接影響するので、キャプチャを開始する前に設定を行ってください。



エージェント画面(概要タブ)

## 2) データの切り出し

リアルタイムなトラフィックデータや異常検知の結果を確認して、解析したい部分(時間範囲)を特定します。その特定された部分や、その前後を含めたトラフィックを切り出して、トレースファイルを作成することができます。



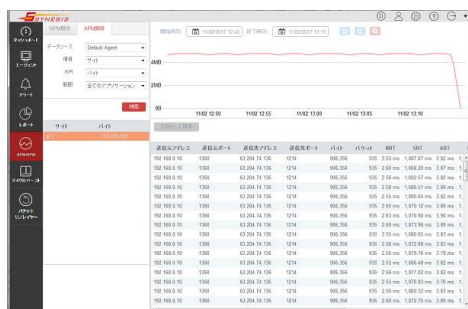
マイクロバースト画面



エージェント画面(キャプチャレコード)

## 3) 解析

1)でキャプチャしたキャプチャレコードや、2)で切り取ったトレースファイルを解析します。他の Synesis でキャプチャされたデータを解析することも可能です。



APM 解析画面



レポート

## 2.起動と終了

---

### 2.1. Synesis の起動

---

下記の手順に従って Synesis を起動してください。

#### 2.1.1. Synesis Distributed

- 1) 拡張ストレージ・ユニットがある場合は、拡張ストレージ・ユニットの電源を ON にしてください。その後、ディスクドライブのフロントパネル上にある緑色 LED の点滅が終わる（点灯状態になる）まで待ちます。拡張ストレージ・ユニットがないモデルでは、この操作は必要ありません。
- 2) メインユニットの電源ボタンを押し、電源を ON にしてください。

#### 2.1.2. Synesis Portable

Synesis Portable の電源ボタンを押し、電源を ON にしてください。

## 2.2. Synesis へのアクセス

Synesis には Web ブラウザを用いてアクセスします。PC の推奨環境は下記の通りです。

推奨 OS : Windows7, Windows10

推奨ブラウザ : Firefox, Internet Explorer 11

3 ユーザまで同時にアクセス可能です（アクセスユーザ数は変更可能）。

- 1) Web ブラウザを起動してください。
- 2) 下記のアドレスをアドレスバーに入力してください。Synesis のログイン画面が表示されます。

**http://[IP Address]:8080/** （[IP Address] の部分は Synesis の IP アドレスを入力します）

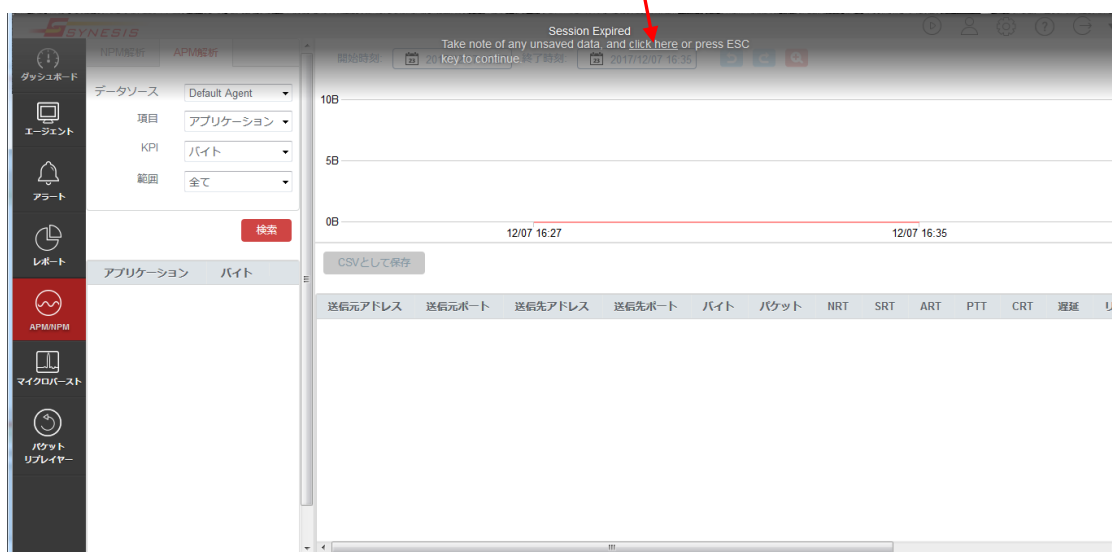
Synesis の Web ブラウザを使用する場合は、下記のアドレスでもアクセス可能です。

**http://localhost:8080/**



- 3) 上の欄に ID を、下の欄にパスワードを入力して「ログイン」ボタンをクリックしてください。

無操作のまま 30 分経過すると自動的にサインアウトし、下図のように画面の上部に影が下りた状態になります。サインアウトしてしまった場合は“click here”の部分をクリックしてください。




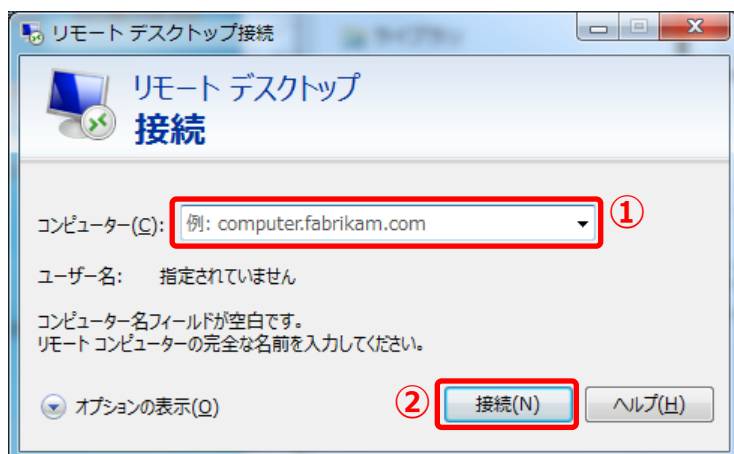
Synesis のログイン画面が表示されますので、再度ログインしてください。

サインアウトするまでの時間は変更可能です。

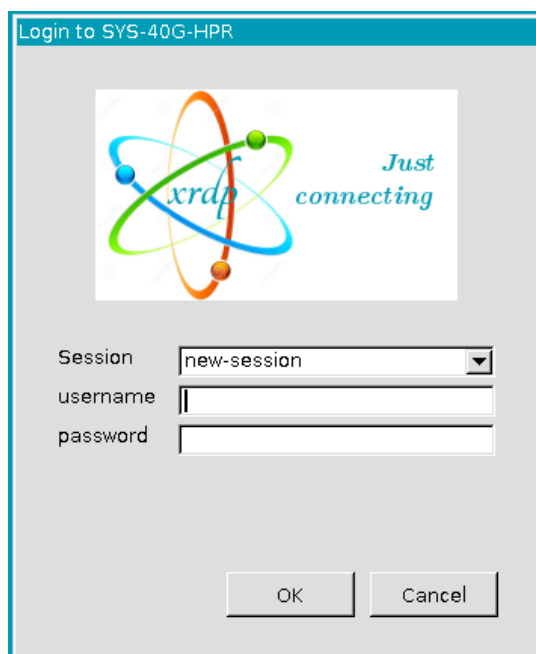
## 2.3. リモートデスクトップ

Windows のリモートデスクトップ機能で Synesis の OS にログインすることができます。  
手順は以下の通りです。

- 1) Windows のスタートボタン  をクリックし、「すべてのプログラム」 をクリックします。
- 2) 「アクセサリ」をクリックしてメニューを展開し、「リモートデスクトップ接続」 をクリックしてください。下図の「リモートデスクトップ接続」が表示されます。



- 3) コンピュータ(C) の欄(下図①)に Synesis の IP アドレスを入力し、「接続」ボタン(下図②)をクリックしてください。接続に成功すると、下記のログイン画面が表示されます。
- 4) OS のユーザ名とパスワードを入力し、「OK」ボタンをクリックしてください。



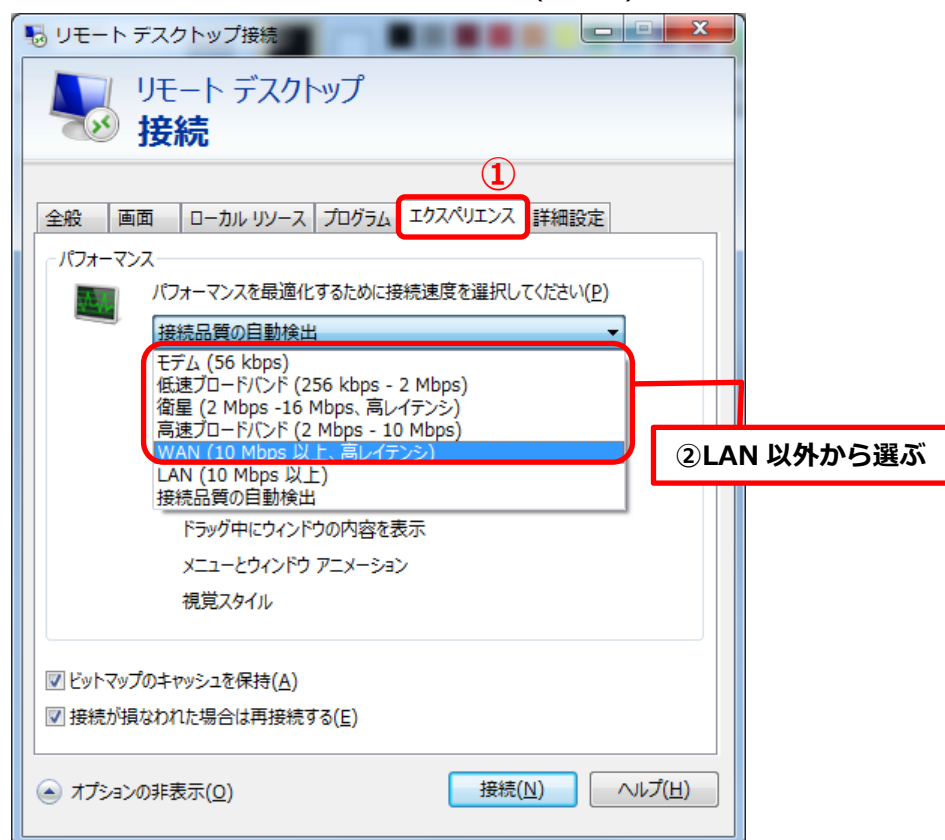
5) ログインに成功すると、OS のデスクトップ画面が表示されます。



ログインしても上図のデスクトップ画面が表示されない場合は、一旦接続を解除し、以下の手順でリモート接続のオプションを設定してください。

6) リモートデスクトップ接続の「オプションの表示」をクリックしてください。

オプションメニューが表示されます。エクスペリエンス タブ(下図①)を選択してください。



「接続品質の自動検出」をクリックすると選択項目が表示されます。

**“LAN (10 Mbps 以上)”以外**(上図②)を選択して「接続」ボタンをクリックしてください。

- 7) ログアウトする場合は、メニューバーから「システム」―「[ユーザ名]のログアウト…」を選択してください。



リモートデスクトップからシャットダウンや再起動は出来ません。

Synesis 本体の画面で操作するか、ターミナルの shutdown コマンドで行なってください。

## 2.4.Synesis の終了

Synesis の電源を落とす際は、下記の手順に従ってください。

### 2.4.1. Synesis Distributed

- 1) OS をシャットダウンします。
- 2) 拡張ストレージ・ユニットの電源を OFF にします。拡張ストレージ・ユニットがないモデルでは、この操作は必要ありません。

### 2.4.2. Synesis Portable

OS をシャットダウンします。または Synesis Portable の電源ボタンを押します。



### 3.Synesis の画面構成

Synesis にログインすると上図のような画面が表示されます。



画面の左端に表示されているアイコン(図①)は Synesis のメインメニューです。

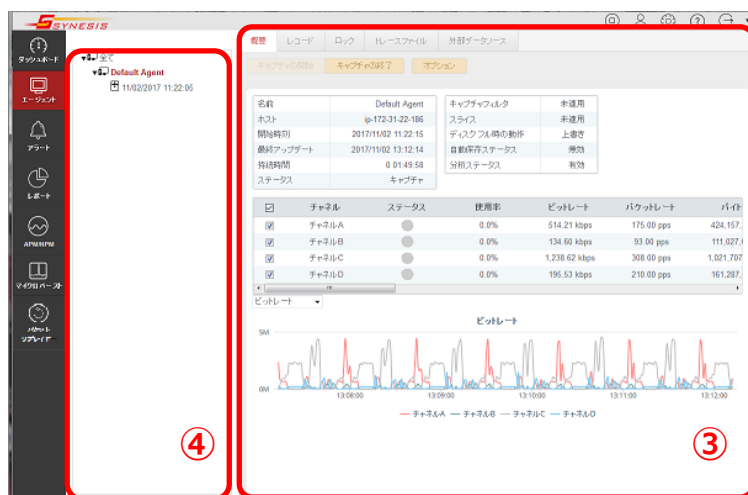
ここからキャプチャの実行や解析を行うための各種メニューにアクセスできます。

画面の右上に表示されているアイコン(図②)はツールバーメニューです。

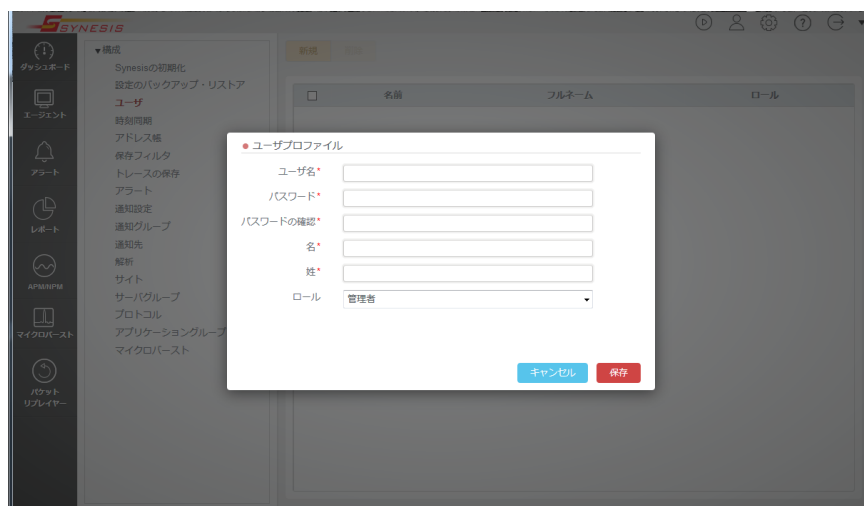
使用頻度も多く、すぐに使いたいキャプチャ開始/終了アイコンやヘルプ表示アイコン、各種設定を行える構成メニューアイコンが集められています。

各メニューの種類と概要は **3.1 メインメニュー**と **3.2 ツールバーメニュー**を参照してください。

メニュー画面によっては、メインのワークスペース(下図③)と、接続されている Synesis の情報がツリー形式で表示されるエージェント・ペイン(下図④)が表示されます。



画面がグレイアウトし、各種設定ダイアログが表示されます。



\*がついている項目は入力必須項目になります。

「保存」ボタンや「適用」ボタンをクリックすると、入力した内容が保存され、ダイアログが閉じられます。「キャンセル」ボタンをクリックすると、保存されずにダイアログが閉じられます。

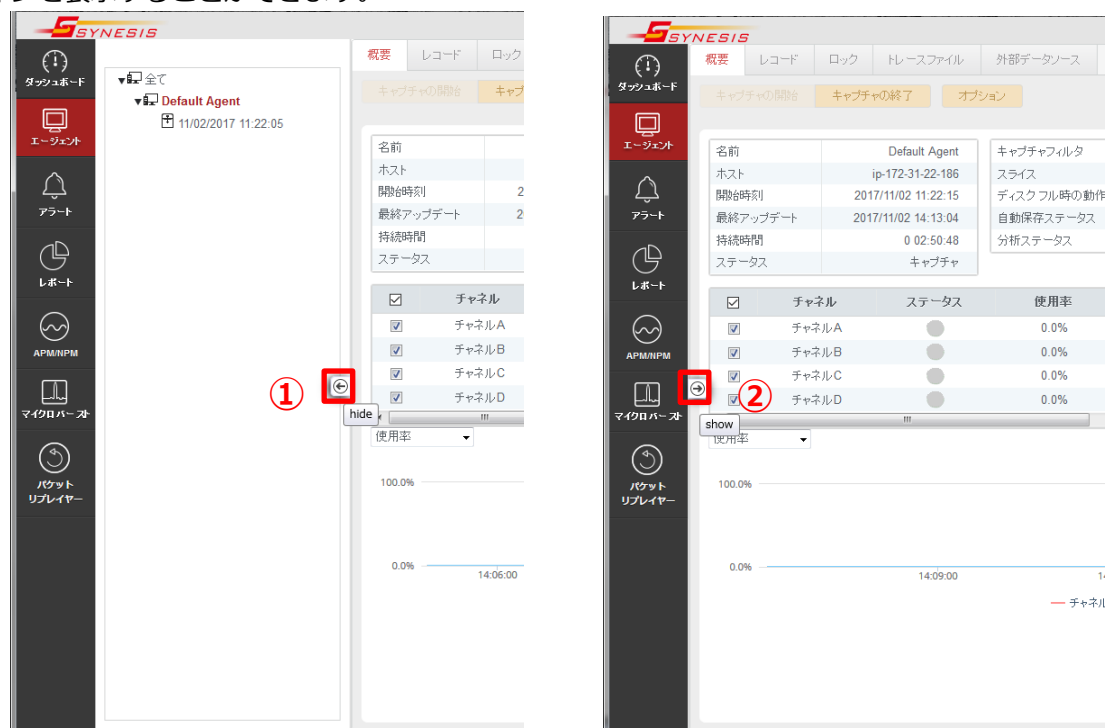
## ワークスペースの拡大表示

ワークスペースを拡大表示したい場合は、ワークスペースとエージェント・ペイン(APM/NPM 解析では検索ペイン)の境界にカーソルを合わせてください。

hide ボタン(⊖)(下図①)が表示されますので、このボタンをクリックしてください。エージェント・ペインが非表示となり、ワークスペースが拡大表示されます。

拡大表示を解除したい場合はワークスペースの左端にカーソルを合わせてください。





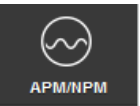
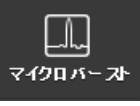

show ボタン(⊕)(下図②)が表示されます。このボタンをクリックすることで、再度エージェント・ペインを表示することができます。



### 3.1. メインメニュー

Synesis 画面左端に表示されるメインメニューのアイコンから、キャプチャの実行や解析を行うための各メニューにアクセスできます。









メインメニューの種類と概要は以下の通りです。

表示	メニュー名	概要
	ダッシュボード	トラフィックの状態がリアルタイムで確認できます。 詳細は <b>4.ダッシュボード</b> を確認してください。
	エージェント	キャプチャの開始・終了やデータ保存などの操作が行えます。 複数の Synesis をこの画面から一括管理できます。 詳細は <b>5.エージェント</b> を確認してください。
	アラート	異常が疑われるトラフィックを検索・解析できます。 詳細は <b>6 アラート</b> を確認してください。
	レポート	解析結果から定型のレポートを作成することができます。 詳細は <b>7 レポート</b> を確認してください。
	APM/NPM 解析	APM 解析では各通信の応答時間を詳細に確認でき、遅延や異常が発生している箇所を特定することができます。 NPM 解析では通信のデータ量が送信側と受信側で個別に確認することができます。 詳細は <b>8. APM/NPM 解析</b> を確認してください。
	マイクロバースト	マイクロバースト(トラフィックバースト)の発生状況を確認できます。 詳細は <b>9.マイクロバースト</b> を確認してください。
	パケット リプレイヤー	キャプチャレコードやトレースファイルを元に、トラフィックを再生して実環境に出力することができます。 再生時にパケットを詰めて送ったり、パケットのデータ IP アドレスを変更したり、パケットのデータを置き換えたりすることができます。 ご使用になる場合は「パケットリプレイヤーオプション」が必要になります。 詳細は <b>10.パケットリプレイヤー</b> を確認してください。

## 3.2. ツールバーメニュー

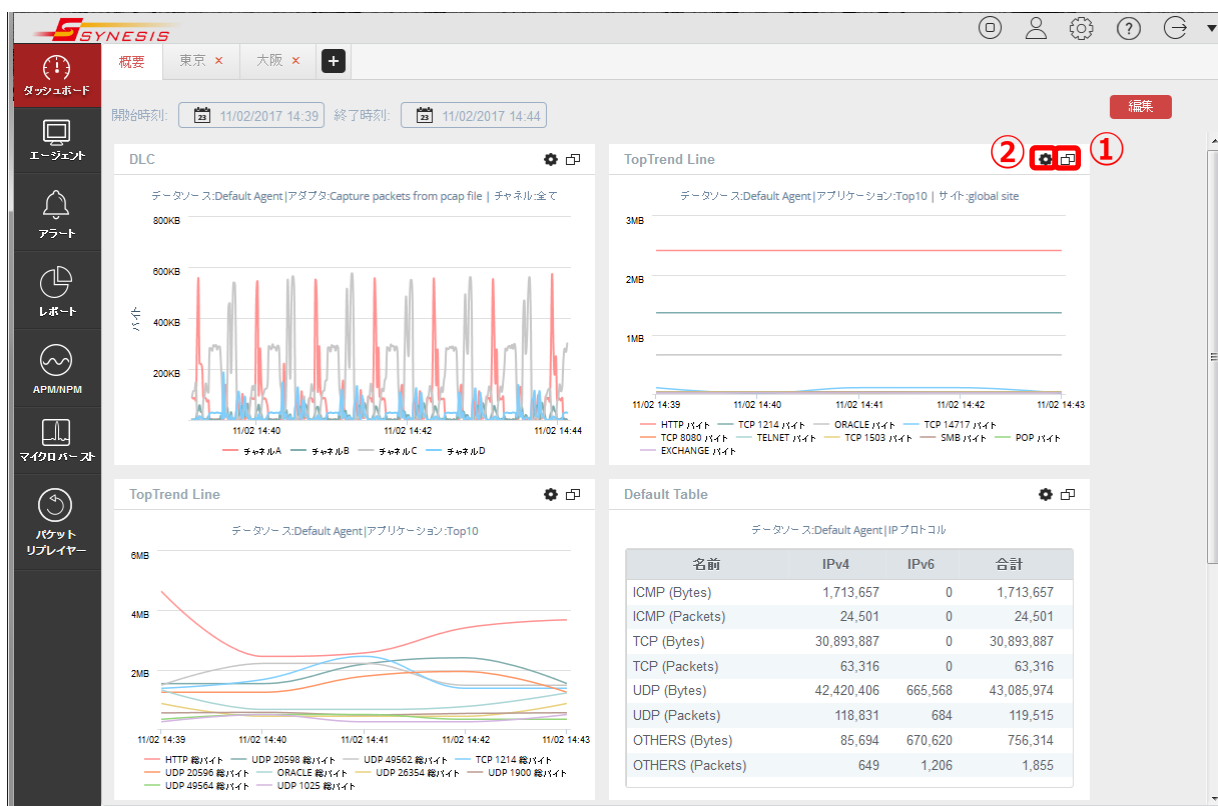
Synesis 画面右上には、使用頻度の高い機能や各種設定項目などにアクセスするためのツールバーメニューアイコンが表示されています。

表示されているアイコンの種類と機能は以下の通りです。

表示	メニュー名	動作
	キャプチャの開始	パケットキャプチャを開始します。 メインメニューのエージェント画面からキャプチャを開始する場合と手順は同じです。 詳細は <b>5.3.1.1 キャプチャの開始・終了</b> を確認してください。
	キャプチャの終了	パケットキャプチャを終了します。
	アクティブユーザ プロフィール	サインインユーザ（自分自身）の登録情報が変更できます。 表示名の変更やパスワードの変更がこちらから行えます。 詳細は <b>11.パスワードの変更</b> を参照してください。
	<b>構成</b>	キャプチャ済みのパケット解析用のフィルタやアラートなど、解析に必要な設定項目がまとめられた「構成」メニュー画面にアクセスできます。 その他、ユーザ管理やシステムバックアップのメニューなどもこちらにあります。 詳細は <b>12.構成</b> を参照してください。
	ヘルプ	本取扱説明書が表示されます。
	サインアウト	サインアウトし、ログイン画面に戻ります。
	アイコンの 表示/非表示選択	ツールバーに表示するアイコンを選択できます。  をクリックするとこの表で説明されているアイコンのリストが表示されます。表示したいアイコンの左端のチェックボックスにチェックをいれてください。そのアイコンがツールバー上に表示されます。 非表示にしたい場合はチェックボックスからチェックを外してください。



## 4. ダッシュボード

ダッシュボードはリアルタイムなトラフィック統計情報が確認できるページです。

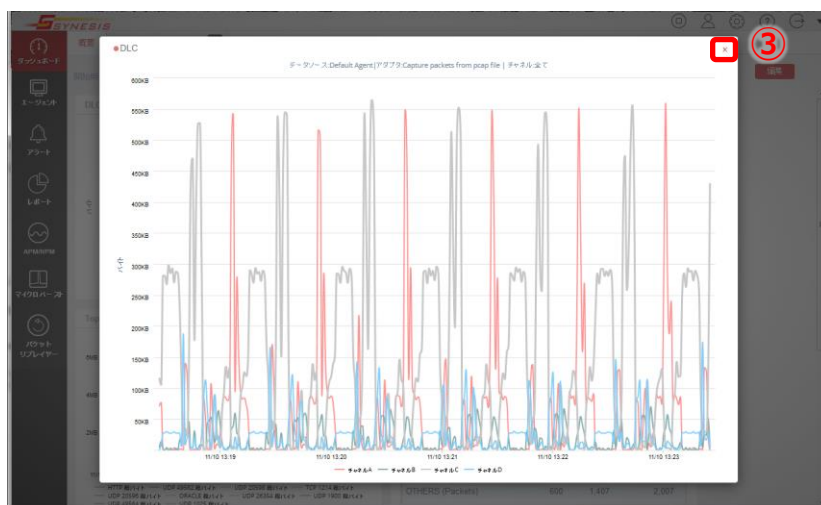


ユーザごとに複数のダッシュボードを設定し、ダッシュボードごとに複数の表やグラフを表示させることが可能です。グラフの種類や表示データも個々に設定可能です。


ダッシュボードやグラフの追加や削除を行っても、他のユーザのダッシュボードには影響しません。

各グラフの右上には「新しいウィンドウで開く」アイコン(上図①)と、グラフや表の設定が変更できる「プロファイルの設定」アイコン(上図②)が配置されています。

アイコンをクリックすると、グラフが別ウィンドウで拡大表示されます。

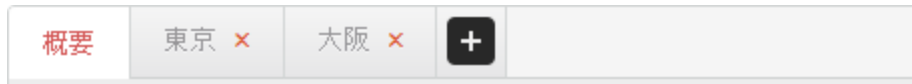


拡大表示中のウィンドウはXボタン(上図③)をクリックすると閉じることができます。

 アイコンをクリックした際の動作については、**4.6 グラフの設定変更**を参照してください。

## 4.1. ダッシュボード・タブ

画面最上部のタブはダッシュボードのリストです。



タブをクリックすることで表示するダッシュボードを切り替えることができます。

ダッシュボードを追加したい場合は、タブリストの左側にある **+** ボタンをクリックしてください。

「新規ダッシュボード」ダイアログが表示され、新しいダッシュボードを作成できます。

追加方法の詳細は次節、ダッシュボードの追加を参照してください。

追加したダッシュボードを削除したい場合は、ダッシュボード名の左側の **x** ボタンをクリックしてください。

**x** ボタンのない概要タブはデフォルトのタブで、削除できません。

## 4.2. ダッシュボードの追加

ダッシュボードを追加したい場合はタブリスト右端にあるボタンをクリック **+** してください。

下図の「新規ダッシュボード」ダイアログが表示されます。

「ダッシュボード名」欄に追加するダッシュボードの名前を入力し、「適用」ボタンをクリックしてください。新しくダッシュボードが追加され、ダッシュボード・タブの右端に指定した名前のタブが追加されます。

「ダッシュボードテンプレート」欄では、「DLC」と「Top Site」の2種類のテンプレートを選択できます。初期状態で表示されるグラフはそれぞれ以下の通りです。

テンプレート名	配置されるグラフ
DLC	DLC 折れ線グラフ/データソース : DefaultAgent/パケット
Top Site	NPM : Top Site 棒グラフ/データソース : DefaultAgent/サイト : Top10/総パケット
	APM : Top Site 円グラフ/データソース : DefaultAgent/サイト : Top10/パケット

ダッシュボードの追加後にグラフの追加・削除または設定変更が行えます。

詳細は **4.6 グラフの設定変更**を参照してください。

### 4.3. 時間範囲の選択

ダッシュボード画面ではリアルタイムなトラフィックを確認できるように、現在の時刻から一定時間遡ったトラフィックデータやその統計情報が表示されます。

ウィンドウ左上の開始時刻、終了時刻をクリックしてください。

下図の「期間」ダイアログが表示され、表示される期間を変更できます。



A dialog box titled "期間" (Period) with a red header bar. It contains five buttons stacked vertically: "5分" (5 min) in red, "30分" (30 min), "1時間" (1 hour), "8時間" (8 hours), and "24時間" (24 hours). At the bottom right is a blue button labeled "閉じる" (Close).

表示期間は 5 分、30 分、1 時間、8 時間、24 時間から選択できます。

### 4.4. ダッシュボードの名称変更

ダッシュボードの名前を変更したい場合は、名前を変更したいダッシュボードのタブを選んで開き、ダッシュボードページ右上の「編集」ボタンをクリックしてください。

「編集」ボタンが表示されていたあたりに「リネーム」ボタンと「保存」ボタンが表示されます。

「リネーム」ボタンをクリックしてください、以下の「ダッシュボードのリネーム」ダイアログが表示されます。



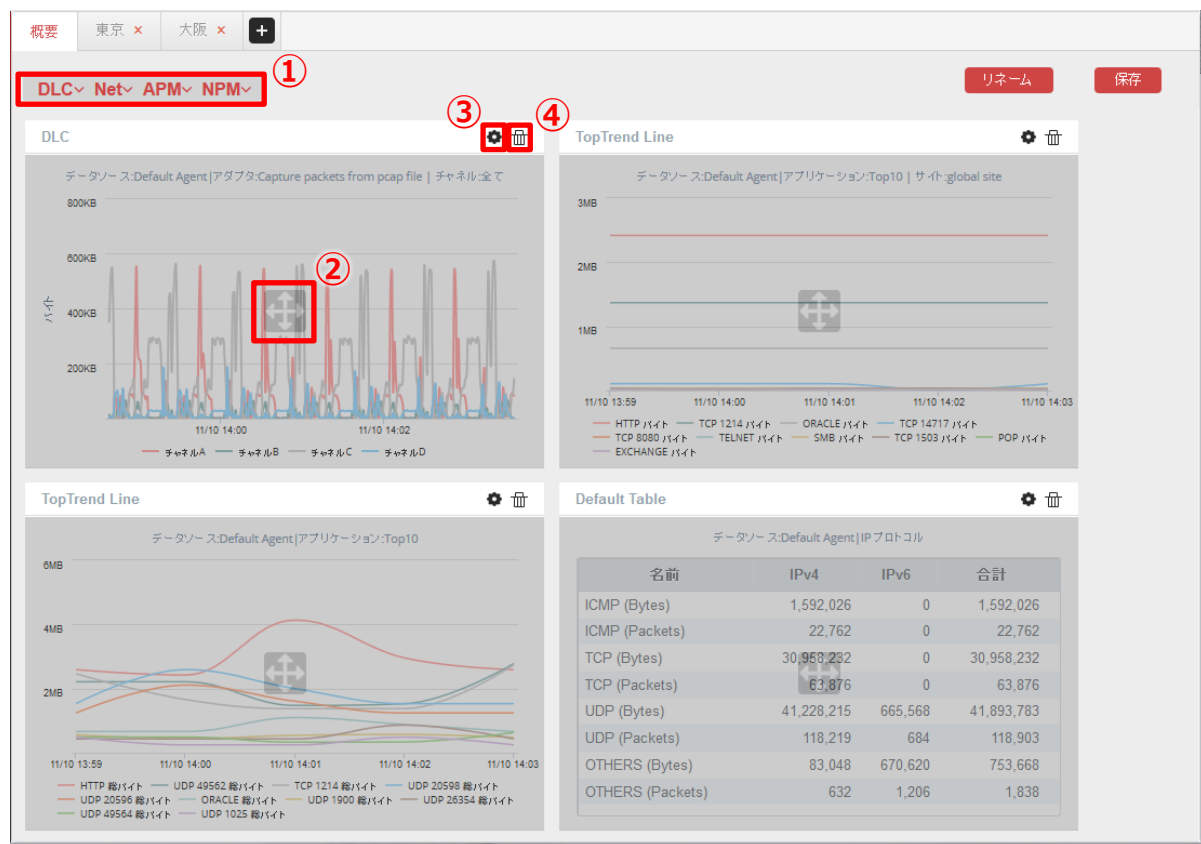
A dialog box titled "ダッシュボードのリネーム" (Rename Dashboard) with a red header bar. It contains a text input field labeled "名前" (Name). At the bottom right are two buttons: "キャンセル" (Cancel) in blue and "適用" (Apply) in red.

「名前」欄に新しい名前を入力し、「適用」ボタンをクリックしてください。タブに表示されているダッシュボードの名前が変更されます。

## 4.5. グラフの追加、並べ替えと削除

ダッシュボードには複数の表やグラフを配置することが可能です。

ダッシュボードにグラフを追加したい場合は、画面右上の「編集」ボタンをクリックしてください。



画面左上に追加するグラフの種類を選択するためのメニュー(上図①)が表示されます。

メニューの中から解析方法のカテゴリを選択し、グラフタイプを指定してグラフを追加します。


追加グラフの指定方法などは、**4.5.1 グラフの種類と設定方法**を参照してください。

なお、推奨されるグラフの数はモデルによって異なります。詳細は **Appendix H モデルによる違い**を参照してください。

### グラフの並べ替えと削除

ダッシュボードの「編集」中は、グラフの並べ替えや削除も行えます。

移動したいグラフにカーソルを合わせ、移動したい位置までドラッグ&ドロップしてください。自動的にグラフの順序が並べ替えて表示されます。

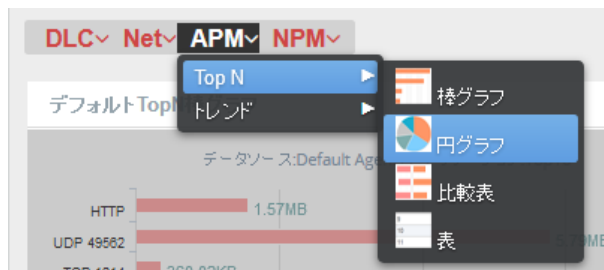
グラフを削除したい場合は、削除したいグラフの右上の  アイコン(上図③)をクリックしてください。**削除を確認するメッセージが表示されない**ので、削除する際にはご注意ください。

「保存」ボタンをクリックすると変更内容が保存されます。



### 4.5.1. グラフの種類と設定方法

グラフを「追加」するには、ページの左上に表示される解析方法のカテゴリから 1 つを選択してください。カテゴリを選んでクリックすると、グラフタイプのサブリストが表示されます。



選択可能なグラフの種類は下記の通りです。

カテゴリ	サブカテゴリ	グラフの形状
DLC	—	折れ線グラフ
	イーサタイプ	表
Net	IP プロトコル	表
APM/NPM	Top N	棒グラフ 円グラフ 比較表 表
	トレンド	折れ線グラフ 面グラフ 縦棒グラフ トップトレンド折れ線グラフ

グラフタイプを選択すると、各グラフの設定ダイアログが表示されます。

構成トレンド折れ線グラフ

タイトル \*

デフォルトトレンド折れ線グラフ

説明

説明を入力してください

アドオン

APM

タイプ \*

サイト

範囲 \*

アプリケーション

インデックス \*

バイト

パケット

NRT(ms)

SRT(ms)

ART(ms)

PTT(ms)

CDT(ms)

>>

<<

上限を固定する



☐

キャンセル


保存

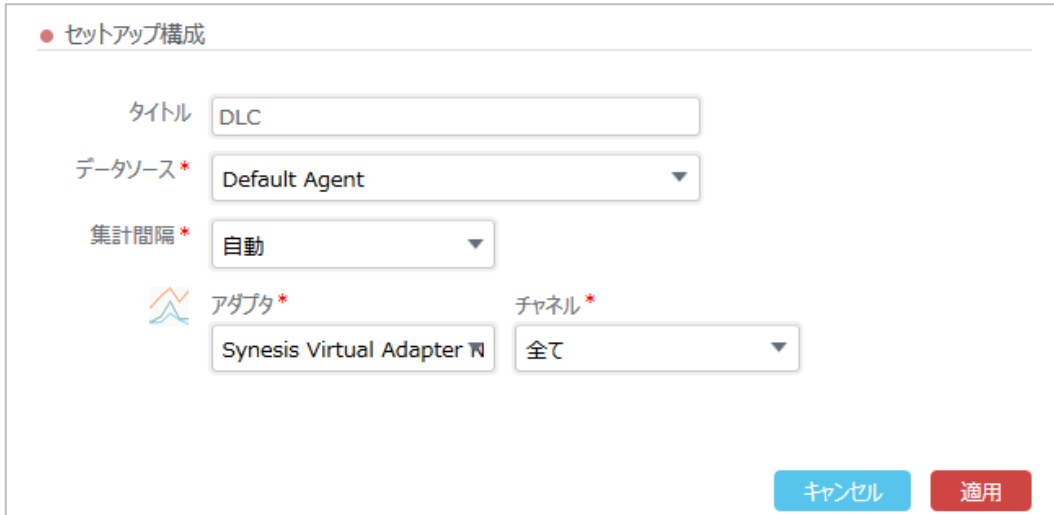
各項目を設定して「保存」 ボタンをクリックしてください。画面にグラフが追加されます。

グラフの種類によって項目は異なりますが、主な設定項目は以下の通りです。

項目	説明
タイトル	グラフのタイトルです。
説明	グラフの説明です。
アドオン	グラフ追加時に選択したカテゴリです。ここでは変更できません。
タイプ	グラフに表示するデータタイプです。ドロップダウンリストから選択します。
範囲	「タイプ」で指定したデータタイプの中で、さらに表示対象を限定するためのフィルタとして用いるデータタイプを指定します。
インデックス	<p>グラフの系列として使用するデータを選択します。</p> <p>右側のリストにあるデータが表やグラフに表示されます。</p> <p>左側はグラフの系列として利用可能なデータのリストです。1つ以上のデータを選択し、 アイコンをクリックしてください。選択したデータが右側のリストに移動します。</p> <p>右側のリストから削除する場合は、1つ以上のデータを選択して  アイコンで移動します。</p>
上限を固定する	トレンド系のグラフでは、プロットされた KPI 指標の上限を定義することができます。実際のプロット指標値が上限値を超えた場合、プロット値がユーザ定義の上限値になります。（実際の値を表示するには点の上にマウスポインタを置いてください）
KPI の上限	<p>「上限を固定する」が有効の場合に表示されます。</p> <p>テキストボックス右側のドロップダウンリストで、単位（K、M、G、u、m など）を変更できます。グラフの単位ラベルも変更されます。</p> <p>入力できる最大値は 1,000,000,000（総サイズ）までです。</p>

## 4.6. グラフの設定変更

グラフは追加した後も、データソースや集計間隔、表示チャンネルを変更することが可能です。  
グラフの種類や表示するデータ(インデックス)を変更したい場合は、グラフを作り直してください。  
設定を変更したい場合は、グラフ右上の「プロファイルの設定」アイコンをクリックしてください。  
下図の「セットアップ構成」ダイアログが表示され、設定を編集できるようになります。




● セットアップ構成

タイトル

データソース\*

集計間隔\*

 アダプタ\*  チャンネル\*

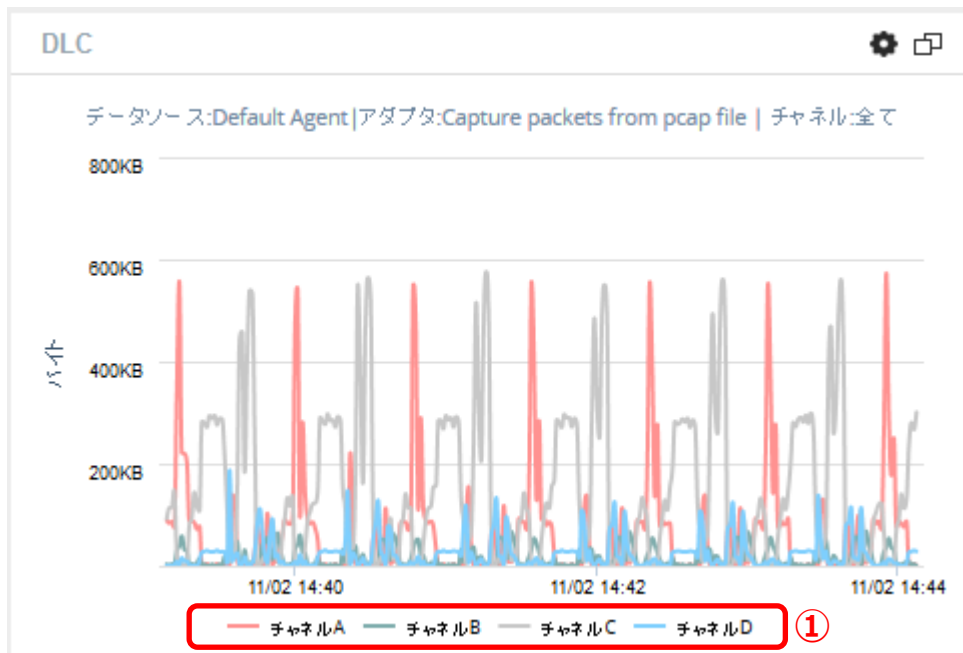
編集内容を保存する場合は「適用」ボタンをクリックしてください。

変更可能な設定項目は以下の通りです。

項目	説明
タイトル	グラフのタイトル文字列です。
データソース	グラフに表示するデータのデータソースを選択します。 選択可能な項目は Synesis の設定により異なります。詳細は <b>D.2 データソース</b> を参照してください。
集計間隔	時系列グラフの集計間隔を設定します。次の中から 1 つ選択します。 DLC: 自動、5 秒、1 分、15 分、1 時間 APM/NPM: 自動、1 分、15 分、1 時間
アダプタ	データソースとしてエージェントを選択した場合、そのエージェントに属する有効なアダプタリストから選択します。エージェント以外を選択した場合、この項目は表示されません。
チャンネル	データソースとしてエージェントを選択した場合、上述の「アダプタ」にて選択したアダプタ内の有効なチャンネルから選択します。任意のチャンネル、または全てのチャンネルが選択できます。 チャンネルグループが設定されている場合は、チャンネルグループの OUT、IN、全ての中から選択することができます。チャンネルグループについての詳細は <b>D.1 チャンネルグループ</b> を参照してください。

#### 4.6.1. チャンネルの表示/非表示の切り替え

グラフ下部に表示されたチャンネル名（下図①）などの要素をクリックすることで、対応するグラフの表示/非表示を切り替えることができます。



チャンネル以外の要素でも表示/非表示の切り替えが可能です。

また、ウィンドウによる拡大表示中でも切り替え可能です。

## 5. エージェント

エージェント画面ではキャプチャの開始・終了やデータ保存などの操作が行えます。

The screenshot shows the SYNESIS Agent interface. On the left, a sidebar (labeled 1) contains navigation icons for Dashboard, Agent, Alert, Report, APM/NPM, MicroProfile, and Packet Replay. The main area (labeled 2) displays the 'Default Agent' configuration. It includes a list of agents with timestamps, a table of agent details (Name, Host, Start Time, Last Update, Duration, Status), a table of channel statistics (Channel, Status, Usage, Bit Rate, Packet Rate, Bytes), and a packet capture graph.

名前	Default Agent	キャプチャフィルタ	未適用
ホスト	ip-172-31-28-84	スライス	未適用
開始時刻	2017/11/15 14:55:15	ディスクフル時の動作	上書き
最終アップデート	2017/11/15 15:16:23	自動保存ステータス	無効
持続時間	0 00:21:08	分析ステータス	有効
ステータス	キャプチャ		

チャンネル	ステータス	使用率	ビットレート	パケットレート	バイト
チャンネルA	●	0.0%	512.63 kbps	174.00 pps	81,251,477
チャンネルB	●	0.0%	134.82 kbps	93.00 pps	21,368,813
チャンネルC	●	0.0%	1,247.44 kbps	310.00 pps	197,719,111
チャンネルD	●	0.0%	195.27 kbps	210.00 pps	30,950,045

エージェント画面はエージェント・ペイン(上図①)とワークスペース(上図②)で構成されます。

エージェント・ペインで選択される箇所によって、表示されるワークスペースが変わります。

### 5.1. エージェント・ペイン

エージェント・ペインには利用可能なエージェントがツリー形式で表示されます。

▶アイコンをクリックするとツリーを展開し、▼をクリックすると展開したツリーを折り畳みます。

The screenshot shows the SYNESIS Agent interface. The left sidebar contains navigation icons for Dashboard, Agent, Alert. The main area shows a tree view of agents. The '全て' (All) node is expanded, showing a list of agents with timestamps. The 'Default Agent' node is selected and expanded, showing a list of agents with timestamps.

ルート階層の「全て」ノード(上図③)をクリックすると、右側に **5.2 全てのエージェント・ワークスペース**が表示され、利用可能なエージェントの情報が表示されます。

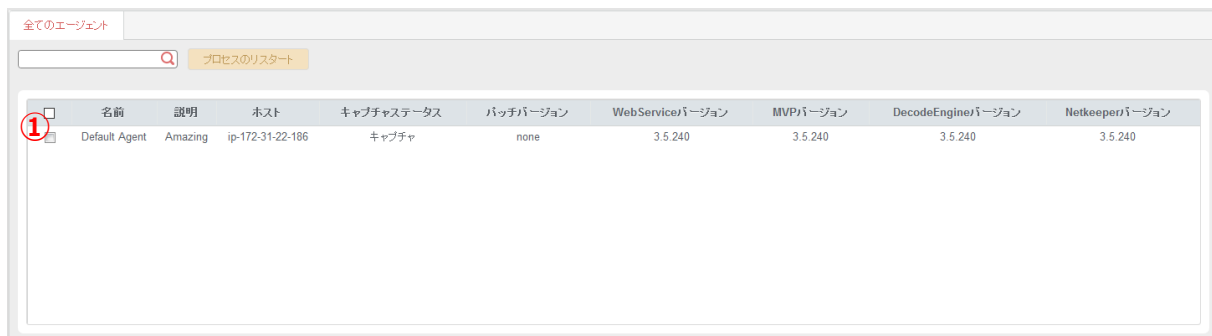
エージェントノード(上図④)をクリックすると **5.3 エージェント・ワークスペース**が表示されます。

トラフィックの確認とキャプチャの開始/終了の操作が行えます。

各レコードのノード(上図⑤)をクリックすると、**5.4 キャプチャレコード・ワークスペース**が表示されます。個々のキャプチャレコードの確認と、トレースの保存などの操作が行えます。

## 5.2. 全てのエージェント・ワークスペース

全てのエージェント・ワークスペースでは利用可能なエージェントが一覧で表示されます。それぞれのエージェントの基本情報が確認できます。



確認できる情報は以下の通りです。

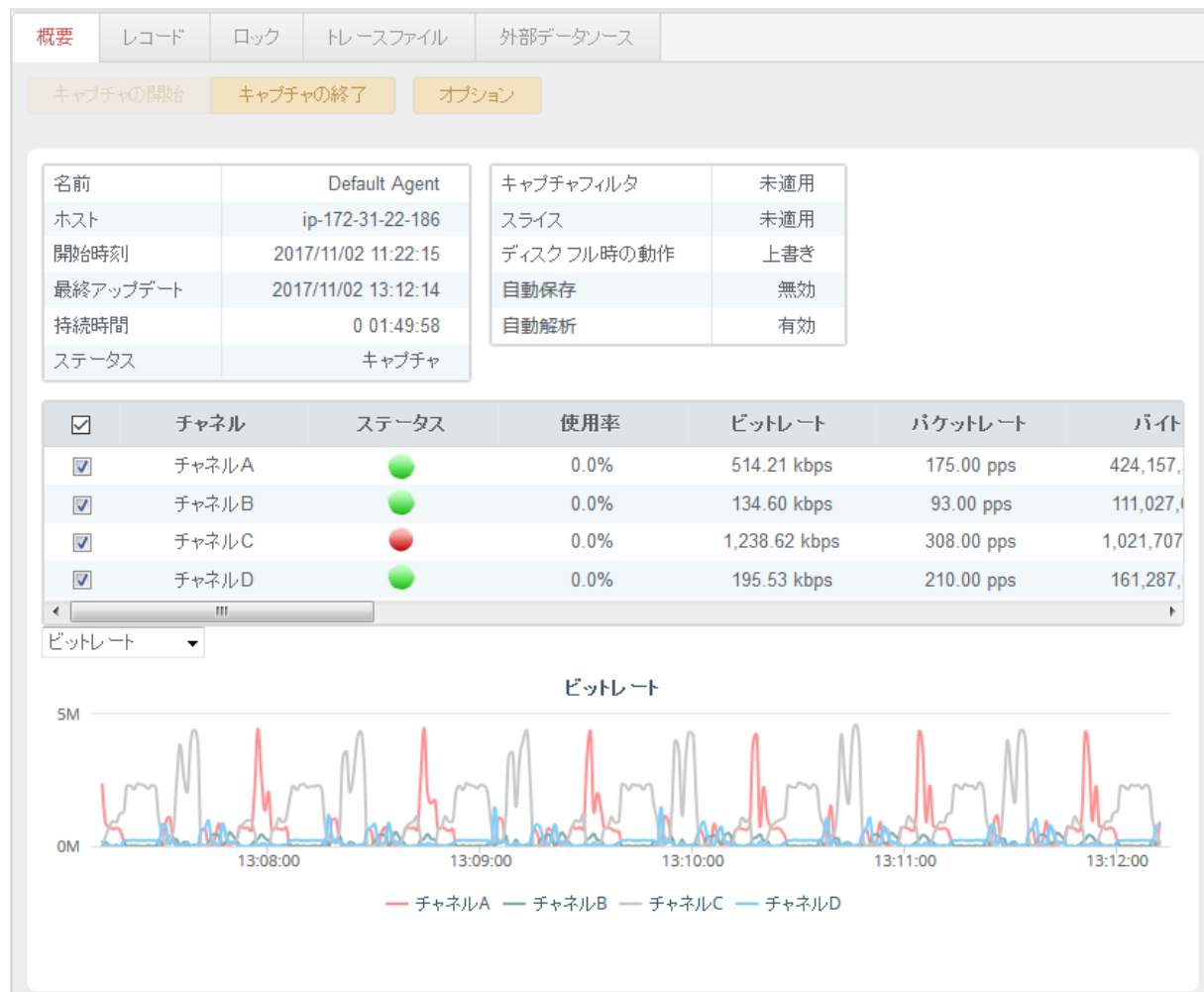
項目	説明
名前	エージェントの名前です。
説明	エージェントの説明です。
ホスト	エージェントのホスト名です。
キャプチャステータス	キャプチャ中は「キャプチャ」、終了すると「停止」になります。キャプチャを開始/終了する手順は <b>5.3.1.1 キャプチャの開始・終了</b> を参照ください。
パッチバージョン	Synesis インストール後に当てられたパッチがあればそのバージョンを、なければ「none」と表示します。
WebServiceバージョン	インストールされている Synesis の各ソフトウェアのバージョンです。
MVPバージョン	
DecodeEngineバージョン	
Netkeeperバージョン	

検索テキストボックスに文字列を入力してエージェントを検索できます。検索ボックスに入力した文字列が、エージェントの名前の一部と一致するものを表示します。

エージェントに対してリモートで設定変更の適用を実行できます。設定を適用したいエージェントの左側のチェックボックスにチェックを入れ、「プロセスのリスタート」ボタンをクリックします。全てのエージェントに対して適用したい場合は、先頭行のチェックボックス（上図①）にチェックを入れ、「プロセスのリスタート」ボタンをクリックします。

## 5.3. エージェント・ワークスペース

エージェント・ワークスペースにはキャプチャの開始・終了やキャプチャの設定、キャプチャデータの保存や読み込みに関するメニューなど、解析以外の操作メニューが集められています。



エージェント・ワークスペースは以下の5画面で構成されています。

<b>概要 タブ</b>	キャプチャ中のトラフィックの状態を確認しながら、キャプチャの開始/終了の操作が行えます。
<b>レコード タブ</b>	エージェントが保有するキャプチャレコードが一覧で表示されます。 レコードにロックを掛け保護する、レコードをトレースファイルに保存する、統計情報を CSV ファイルに書き出す、などの操作が可能で、作成したファイルをダウンロードすることも可能です。
<b>ロック タブ</b>	ロックされているキャプチャレコードが一覧で表示されます。 この画面からロックされているレコードのロックを外せます。
<b>トレースファイル タブ</b>	保存された全てのトレースファイルが表示されます
<b>外部データソース タブ</b>	保存されたバックアップデータを一覧で表示します。他の Synesis で作成したバックアップデータをこちらから読み込むことも可能です。

詳細は次頁以降の各項を参照してください。

### 5.3.1. 概要 タブ

キャプチャ中のトラフィックの状態を確認しながら、キャプチャの開始/終了の操作が行えます。

画面上部のテーブルでは実行中のキャプチャに関する情報が、中央のテーブルには統計情報が表示されます。テーブルの下には、チャンネルごとのトレンドグラフが表示されます。

表示するグラフは使用率、ビットレート、パケットレートなどの中から選択できます。

#### 実行中のキャプチャの情報

画面上部のテーブルには実行中のキャプチャに関する情報が表示されます。

名前	Default Agent	キャプチャフィルタ	未適用
ホスト	ip-172-31-22-186	スライス	未適用
開始時刻	2017/11/02 11:22:15	ディスクフル時の動作	上書き
最終アップデート	2017/11/02 13:12:14	自動保存	無効
持続時間	0 01:49:58	自動解析	有効
ステータス	キャプチャ		





表示される情報は以下の通りです。

項目	説明
名前	エージェントの名前です。
ホスト	エージェントのホスト名です。
開始時刻	キャプチャの開始日時です。
最終アップデート	統計情報を最後にアップデートした日時です。
持続時間	実行中のキャプチャをスタートしてからの経過時間です。
ステータス	キャプチャ実行中の場合は「キャプチャ」、終了すると「停止」になります。
キャプチャフィルタ	キャプチャに適用されているフィルタの有無を表示します。
スライス	キャプチャに適用されているスライス設定の有無を表示します。
ディスクフル時の動作	ディスクフル時に停止するかどうかの設定を表示します。
自動保存	自動保存のステータスです。表示されるステータスは以下の通りです。 <ul style="list-style-type: none"><li>● 無効：自動保存が行われない設定になっています。</li><li>● プライマリ：プライマリに指定したフォルダに保存しています。</li><li>● セカンダリ：セカンダリに指定したフォルダに保存しています。</li><li>● 失敗：自動保存に失敗しています。</li></ul>
自動解析	自動解析のステータスです。表示されるステータスは以下の通りです。 <ul style="list-style-type: none"><li>● 有効：「キャプチャオプション」で選択した項目について自動解析が実行されます。</li><li>● 無効：自動解析が無効になっています。</li></ul>



## キャプチャの統計情報

中央のテーブルにはチャンネルごとのキャプチャの統計情報が表示されます。

<input checked="" type="checkbox"/>	チャンネル	ステータス	使用率	ビットレート	パケットレート	バイト
<input checked="" type="checkbox"/>	チャンネルA		0.0%	513.82 kbps	175.00 pps	44,789,325,595
<input checked="" type="checkbox"/>	チャンネルB		0.0%	134.49 kbps	93.00 pps	11,723,292,574
<input checked="" type="checkbox"/>	チャンネルC		0.0%	1,238.05 kbps	308.00 pps	107,919,231,811
<input checked="" type="checkbox"/>	チャンネルD		0.0%	195.40 kbps	210.00 pps	17,032,986,756

表示される情報は以下の通りです。

項目	説明
チャンネル	どのチャンネルをテーブルやトレンドグラフ（次頁参照）に反映するか、個別に選択することができます。先頭行のチェックボックスにチェックを入れると、すべてのチャンネルが選択されます。 チャンネルグループの設定をしている場合、「チャンネルグループに設定した名前 + IN または OUT」の形式(例：チャンネルグループ 1 IN)で表示されます。詳細は <b>D.1 チャンネルグループ</b> を参照してください。
ステータス	各チャンネルの接続状況を表示します。リンクアップ時には緑、リンクダウン時には赤が表示されます。未対応のモデル※は灰色が表示されます。
使用率	回線の使用率を%で示します。
ビットレート	1 秒間に受信したビット数です。
パケットレート	1 秒間に受信したパケット数です。
バイト	受信した総バイト数です。
パケット	受信した総パケット数です。
ドロップ	ドロップしたパケット数です
ブロードキャスト	ブロードキャストパケット数です
マルチキャスト	マルチキャストパケット数です。
ユニキャスト	ユニキャストパケット数です。
CRC※	CRC エラーのパケット数です。フラグメントおよびジャバーは含みません。
フラグメント※	CRC エラーのうち、64byte 未満のパケット数です。
ジャバー※	CRC エラーのうち特定の値(byte) より大きいパケット数です。 特定の値(byte) はモデルによって異なります。※
オーバーサイズ※	CRC エラー以外で特定の値(byte) より大きいパケット数です。 特定の値(byte) はモデルによって異なります。※
ラント※	CRC エラー以外で、64 byte 未満のパケット数です。
アダプタ	アダプタの名称です。

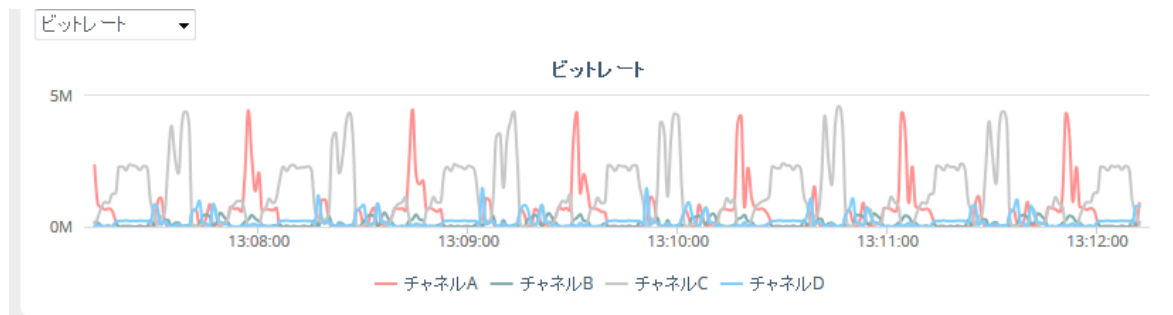
※ CRC～ラントのエラーパケットの検出はモデル(アダプタ)によっては統計が取れず「N/A」と表示されます。対応している場合も、ジャバーやオーバーサイズとカウントされるパケットのサイズ(byte)はモデルによって異なります。

対応モデルやパケットサイズ(byte)の詳細は **Appendix H モデルによる違い**を参照してください。

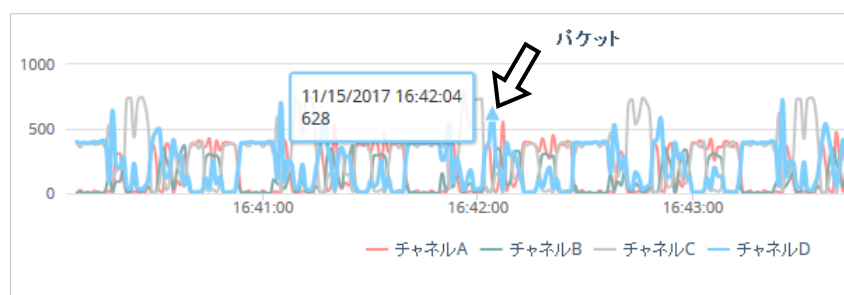
## 各チャンネルのトレンドグラフ

一番下のグラフは各チャンネルの時間経過による変化を示すトレンドグラフです。

横軸は全体で 5 分間、1 秒ごとの統計値が表示されます。



各チャンネルのグラフにカーソルを合わせると、時間と値が表示されます。



グラフ左上のリストボックスで表示データを指定できます。選択可能なデータは以下の通りです。

項目	説明
使用率	回線の使用率を%で示します。
ビットレート	1 秒間に受信したビット数です。
バイト	受信した総バイト数です。
パケット	1 秒間に受信した総パケット数です。
ドロップ	ドロップしたパケット数です
ブロードキャスト	ブロードキャストパケット数です
マルチキャスト	マルチキャストパケット数です。
ユニキャスト	ユニキャストパケット数です。
CRC※	CRC エラーのパケット数です。フラグメントおよびジャバーは含みません。
フラグメント※	CRC エラーのうち、64byte 未満のパケット数です。
ジャバー※	CRC エラーのうち特定の値(byte)より大きいパケット数です。 特定の値(byte) はモデルによって異なります。
オーバーサイズ※	CRC エラー以外で特定の値(byte)より大きいパケット数です。 特定の値(byte) はモデルによって異なります。
ラント※	CRC エラー以外で、64 byte 未満のパケット数です。

※ CRC～ラントのエラーパケットの検出はモデル(アダプタ)によっては統計が取れず、「N/A」と表示されます。対応している場合も、ジャバーやオーバーサイズとカウントされるパケットのサイズ(byte)はモデルによって異なります。

対応モデルやパケットサイズ(byte)の詳細は **Appendix H モデルによる違い**を参照してください。

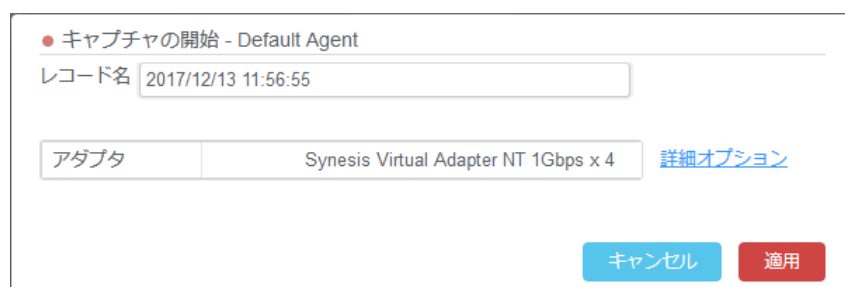
### 5.3.1.1 キャプチャの開始・終了

初めてキャプチャを開始する場合は、キャプチャを開始する前に「オプション」ボタン(下図①)をクリックし、使用するアダプタ(キャプチャカード)を設定してください。

キャプチャフィルタやスライスなどのキャプチャオプションを適用したい場合も、こちらから設定が行えます。設定手順の詳細は次項**キャプチャオプション**を参照してください。



2回目以降の場合は、「キャプチャの開始」ボタン(上図②)をクリックしてください。「キャプチャの開始」ダイアログが表示されます。



「詳細オプション」リンクをクリックすると、「オプション」ボタン(図①)と同様にキャプチャオプションが設定できます。一度行った設定は保存され、次回から自動的に適用されます。

「適用」ボタンをクリックするとキャプチャが開始されます。

ツールバーのキャプチャの開始アイコン (上図③)からも同様にキャプチャを開始できます。



キャプチャを終了する場合は、「キャプチャの終了」ボタン(上図④)、もしくはツールバーのキャプチャの終了 (上図⑤)アイコンをクリックしてください。実行中のキャプチャを停止します。

### 5.3.1.2 キャプチャオプション

エージェント・ワークスペースの概要タブ「オプション」ボタンをクリックすると、下図のキャプチャオプションダイアログが表示され、キャプチャに適用するキャプチャオプションを設定できます。

● キャプチャオプション

共通

キャプチャフィルタ

ロックトリガ

自動保存

チャネル設定

通知設定

アダプタリスト

Capture packets from pcap file

☐ スライス

64

バイト

ディスク フル時の動作

☒ 上書き

☐ 停止

☐ システム起動時に自動でキャプチャを開始する

☐ リアルタイムデコードを有効にする

☒ キャプチャ中の自動解析

モジュール: APM解析, NPM解析 TopN: 100

キャンセル

適用

キャプチャの開始時に表示される「キャプチャの開始」ダイアログの「詳細オプション」ボタンをクリックすると、同様にキャプチャオプションの設定が行えます。

各項目を設定した上で「適用」ボタンをクリックしてください。設定が保存され、キャプチャを実行する際に設定したオプションが自動的に適用されるようになります。

キャプチャオプションダイアログは以下の6画面で構成されています。

タブ名	説明
共通	アダプタ選択、スライス機能、ディスクフル時の動作など、基本的なキャプチャオプションの設定が行えます。
キャプチャフィルタ	キャプチャの段階でパケットをふるいにかけるキャプチャフィルタを設定します。モデルによっては適用できません。
ロックトリガ	指定された条件に合致する区間のパケットデータをロック(保護)し、上書きされないようにします。
自動保存	キャプチャ中のパケットをトレースファイルで自動保存する、自動保存機能の有効/無効と、有効時の動作の詳細を設定します。
チャネル設定	チャネルごとにラインスピードが設定できます。
通知設定	エラー発生時に通知する、など通知を飛ばすイベントを指定できます。

画面ごとに設定できる項目が異なります。詳細は本項の各項を参照してください。

### 5.3.1.2.1.共通 オプション

キャプチャを行うアダプタや、スライス機能などの基本的なキャプチャ設定を行います。

● キャプチャオプション

共通

キャプチャフィルタ

ロックトリガ

自動保存

チャネル設定

通知設定

アダプタリスト

Capture packets from pcap file

☐ スライス

64

バイト

ディスク フル時の動作

☒ 上書き

☐ 停止

☐ システム起動時に自動でキャプチャを開始する

☐ リアルタイムデコードを有効にする

☒ キャプチャ中の自動解析

モジュール: APM解析, NPM解析, TopN: 100

キャンセル

適用

設定項目の詳細は以下の通りです。

項目	説明
アダプタリスト	キャプチャを行うアダプタ(キャプチャカード)を選択します。
スライス	各フレームからキャプチャ対象とするサイズを、フレームの先頭から数えたバイト数の単位で指定します。指定可能なサイズは <b>Appendix H モデルによる違い</b> を参照してください。
ディスクフル時の動作	ディスクが満杯になった場合の動作を定義します。「ディスク」とはパケットを保存する領域を示します。(詳細は <b>Appendix F Synesis のディスク構成</b> をご確認ください) 「上書き」を選択すると、キャプチャを継続し、ハードディスク内の古いパケットから順に上書きして保存します。「停止」を選択すると、その時点でキャプチャが停止します。既に満杯の状態からキャプチャを開始した場合、現在のキャプチャ以外のパケットを上書きし終えた時点でキャプチャが停止します。
システム起動時に自動でキャプチャを開始する	チェックを入れると、システム起動時に自動的にキャプチャを開始します。

リアルタイムデコードを有効にする	チェックを入れると、「リアルタイムデコード」タブを作成し、キャプチャしたパケットをデコードした内容を自動で表示します。詳細は <b>5.3.6 リアルタイムデコードタブ</b> を参照してください。
キャプチャ中の自動解析	チェックを入れると、キャプチャ中の自動解析が有効になります。
モジュール; TopN; (リンク/図①)	有効になっている自動解析の種類(モジュール)と、グラフ表示させるフローの数(TopN)が表示されます。 このリンクをクリックすると、有効にする自動解析の種類が指定できる画面が表示されます。

### キャプチャ中の自動解析の指定

有効にする自動解析の種類を変更したい場合は、設定項目の一番下にある、有効になっている自動解析リストのリンク部分(前頁図①)をクリックしてください。

下図の「上位 N の構成モジュールと分析」ダイアログが表示されます。

● 上位Nの構成モジュールと分析

モジュール ☒ APM解析 ☒ NPM解析 ☐ L2/L3 プロトコル ☐ マイクロバースト

上位のフロー 100 ▼

キャンセル 適用

設定項目は以下の通りです。設定が完了したら「適用」ボタンをクリックしてください。

項目	説明
モジュール	<p>どの自動解析を有効にするかを選択します</p> <p>APM 解析: APM 解析を有効にします。</p> <p>NPM 解析: NPM 解析を有効にします。</p> <p>L2/L3 プロトコル: L2/L3 プロトコル解析を有効にします。</p> <p>マイクロバースト: マイクロバースト解析を有効にします。</p> <p>なお、上記の自動解析項目内の 1 つでも選択すると、自動的に ARP 解析が有効になります。</p> <p>ARP 解析は ARP パケットをカウントする機能です。</p>
上位のフロー	<p>グラフ表示させるフローの数を指定します。20, 50, 100, 200, 500 が選択できます。</p> <p>Synesis 内部のメモリには 40000 フロー(IP アドレスとポートのペアにより定義されたフロー)保持されています。その上位の、指定された数のフローがグラフに表示されます。</p>

### 5.3.1.2.2.キャプチャフィルタ オプション

キャプチャ時に適用するキャプチャフィルタを設定します。

画面左上の「フィルタ有効」チェックボックスにチェックを入れると、フィルタ指定のリストボックスが有効になりますので、適用したいキャプチャフィルタを選択してください。

● キャプチャオプション

共通 **キャプチャフィルタ** ロックトリガ 自動保存 チャンネル設定 通知設定

☒ フィルタ有効 フィルタ ▼

追加 削除

<input type="checkbox"/>	名前	説明
<input checked="" type="checkbox"/>	<a href="#">Filter</a>	{[イーサタイプ - イーサタイプ: 86dd]}
<input checked="" type="checkbox"/>	<a href="#">フィルタ</a>	{[フロー - TCP Any:18-20 --> Any]}
<input checked="" type="checkbox"/>	<a href="#">フィルタ (1)</a>	{[IPフロー - 0.0.0.0/24 --> Any]}

キャンセル 適用

画面中央のキャプチャフィルタリストでは「名前」と「説明」が確認できます。

キャプチャフィルタを追加したい場合は、「追加」ボタンをクリックしてください。設定方法や種類などの詳細は **Appendix B キャプチャフィルタの種類と設定方法**を参照してください。

キャプチャフィルタリストの名前のリンクをクリックすると、登録済みのキャプチャフィルタを編集することができます。登録したキャプチャフィルタを削除したい場合は、そのキャプチャフィルタのチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。選択したキャプチャフィルタが削除されます。

なお、キャプチャフィルタはキャプチャしたパケットがディスク内に保存される前、アダプタの段階でパケットをふるいに掛ける物理的なフィルタです。

キャプチャ後のパケットに適用される「**保存フィルタ**」とは異なりますのでご注意ください。

Synesis のモデルによってはキャプチャフィルタが使用できません。対応しないモデルの場合は「この機種はキャプチャフィルタに対応しないモデルです」と表示されます。キャプチャフィルタが使用可能かどうかは **Appendix H モデルによる違い** の表でご確認ください。

### 5.3.1.2.3.ロックトリガ オプション

指定された条件に合致する区間のパケットデータにロックを掛け、上書きされないようにします。  
ロックすることで重要なパケットデータを保護することができます。

● キャプチャオプション

共通

キャプチャフィルタ

ロックトリガ

自動保存

チャンネル設定

通知設定

☒ ロックトリガを有効にする

時間トリガ

☐ リピートリガ

+

+

☐

トリガ

☐

08:00:00 - 09:00:00

☐

20:00:00 - 21:00:00

SNMPトラップトリガ

☒ SNMPトラップトリガを有効にする

コミュニティ

public

ポート番号

162

ロック開始時間

5

秒前

ロック終了時間

5

秒後

キャンセル

適用



「ロックトリガを有効にする」のチェックボックスにチェックを入れると、設定したロックトリガが有効になり、パケットデータがロック（保護）されます。ロックトリガが有効になっていない場合、ストレージ領域がいっぱいになるとキャプチャされたパケットは古いものから順番に上書きされて消えていきます。

指定できるトリガは以下の2種類です。

種類	説明
時間トリガ	指定した時間範囲のパケットデータをロック（保護）します。
SNMPトラップトリガ	特定の SNMP トラップを受信した場合、その前後の指定された時間範囲のパケットデータをロック（保護）します。



## 時間トリガ

時間トリガを指定したい場合は、 アイコンをクリックしてください。ここで指定した時間範囲がロック（保護）され、キャプチャ中に上書きされなくなります。時間トリガを削除したい場合は  アイコンをクリックしてください。時間トリガを有効にしたい場合は、「トリガ」のリストボックス 内で有効にしたいトリガにチェックを入れてください。

**リピートトリガ**：チェックを入れると、時間トリガが繰り返し有効になります。チェックが入っていない場合は、時間トリガは 1 回に限り有効となります。

## SNMP トラップトリガ

「SNMP トラップトリガを有効にする」のチェックボックスにチェックマークを入れると、SNMP トラップトリガが有効になります。設定項目は以下の通りです。

項目	説明
コミュニティ	SNMP のコミュニティ名を指定します。
ポート番号	SNMP トラップの送信先ポート番号を指定します。
ロック開始時間	トラップトリガの何秒前からロックするかを指定します。
ロック終了時間	トラップトリガの何秒後までロックするかを指定します。

### 5.3.1.2.4.自動保存 オプション

キャプチャ中のパケットをトレースファイルで自動保存します。

● キャプチャオプション

共通

キャプチャフィルタ

ロックトリガ

自動保存

チャンネル設定

通知設定

☒ 自動保存を有効にする

ファイル形式

pcapng

分割ファイルサイズ

256

 MB

最大ファイル数

1

☒ オートローテーション

期間

ローテーション期間

7

 日

保存フィルタ

フィルタなし

☒ スライス

32

 バイト

保存先フォルダ

プライマリ

/pvc/data/databank/autobackup

☒ セカンダリを有効にする

セカンダリ

/pvc/data/databank/autobackup2

プライマリ復旧時に

プライマリに戻る

自動保存機能は、平均1Gbps以下のキャプチャレートでのみサポートされています。

キャンセル

適用

なお、自動保存オプションを有効にすると、自動保存の対象となるファイルの保存処理が行われるため、キャプチャの停止までに数分以上かかる場合があります。

設定項目は以下の通りです。

項目	説明
自動保存を有効にする	チェックを入れると自動保存が有効になります。
ファイル形式	ファイルフォーマットを指定します。 指定できるフォーマットは pcap, pcap(ナノ秒単位), pcapng です。
分割ファイルサイズ	1 ファイルのサイズを指定します。最大値は「構成」メニューの「トレースの保存」から設定できます。デフォルトサイズは 256MB です。 詳細は <b>12.7 トレースの保存</b> を参照してください。
最大ファイル数	保存するファイルの上限数を指定します。 “0” を入力すると無制限になります。オートローテーションオプションを有効にした場合は、この項目は無効になります。 保存先に データバンク領域である/pvc/data/databank/以下のフォルダを指定して、“0” を入力する場合はご注意ください。自動保存されたファイルがデータバンク領域を圧迫して、Synesis の動作に影響を与える可能性があります。
オートローテーション	保存したファイルの使用容量が一定を超えた場合、または一定の期間が経過した場合に古いファイルを上書きするように設定できます。「期間」「サイズ」「パーティションサイズ」を指定できます。 詳細は <b>5.3.1.2.4.2 オートローテーション</b> を参照してください。
保存フィルタ	保存するトレースファイルにフィルタを適用したい場合、フィルタ名を選択します。
スライス	パケットのスライスサイズを指定できます。 指定できるサイズはモデルによって異なります。詳細は <b>Appendix H モデルによる違い</b> を参照してください。
保存先フォルダ	自動保存で保存するトレースファイルの保存場所を指定します。 保存先フォルダとして、Synesis の内部を指定する際には、データバンク領域である /pvc/data/databank 以下のフォルダを指定してください。
プライマリ	自動保存の保存先フォルダパスを指定します。
セカンダリを有効にする※	チェックを入れると、システムがプライマリフォルダへの保存に失敗した場合、セカンダリに指定したフォルダへ保存されます。
セカンダリ	プライマリへの保存に失敗した場合の保存先フォルダパスを指定します
プライマリ復旧時に	プライマリフォルダが復旧した場合「保存先フォルダをプライマリに戻す」か「セカンダリのまま保存を継続する」のどちらかを指定できます

※セカンダリを有効にしない状態でプライマリへの書き込みに失敗した場合は、一時的に自動保存を停止します。1 分後に再度自動保存を試み、失敗した場合はさらに 1 分後に自動保存を試みます。  
自動保存の再開が成功した場合は、成功時刻の 30 秒前のデータから自動保存が再開されます。

プライマリへのデータの書き込みの失敗と、それに伴うセカンダリへの移行や自動保存の再開への試みが発生した場合には指定した通知先にメールなどで通知することができます。

詳細は **5.3.1.2.6 通知設定 オプション**を参照してください。

#### 5.3.1.2.4.1.自動保存ファイルの保存先フォルダ構成

キャプチャした日時を用いてフォルダを作成し、その中にトレースファイルを保存します。デフォルトのフォルダ構成は以下の通りです。

[指定したフォルダ]

```
└[yyyymmdd]
  │  └[HH]
  │    └[HHMMSS.id.pcapng]
  │    └[HHMMSS.id.pcapng]
  │    └[HHMMSS.id.pcapng]
  :    :    :
```

[yyyymmdd]はキャプチャした年月日が、HHMMSS はキャプチャした時刻が用いられます。Id には 0~9999 までの数字が自動的に割り当てられます。

#### 5.3.1.2.4.2.オートローテーション

オートローテーション機能を有効にすることによって、ファイルを保存している時間フォルダの中で最も古いものを自動で削除することができます。削除が実行されるトリガとして、期間、ディスクの使用量、ディスクの空き容量が指定できます。

項目	説明				
期間	日数でトリガを設定し、古いファイルの削除を実行します。 設定できる範囲は 1~365 日です。 保存先として指定したフォルダ内に存在する日付フォルダの数を確認します。 新しい日付フォルダを作成する際に、その数が設定した数に達していた場合、保存されている時間フォルダの中で最も古い時間フォルダが削除されます。				
サイズ	保存先として指定した先のディスクの使用容量が、設定した容量に到達、または超えていた場合に、保存されている時間フォルダの中で最も古い時間フォルダを削除します。 指定可能な使用容量の最大値は 10240 GB です。最小値は「分割ファイルサイズ」で指定される値によって、以下のように場合分けされます。 <table><tr><td>1024 MB 以下</td><td>10GB</td></tr><tr><td>1024 MB を超える</td><td>「構成」メニュー「トレースの保存」の「分割ファイルサイズの上限」で指定したサイズの 10 倍。</td></tr></table> 詳細は <b>12.7 トレースの保存</b> を参照してください。	1024 MB 以下	10GB	1024 MB を超える	「構成」メニュー「トレースの保存」の「分割ファイルサイズの上限」で指定したサイズの 10 倍。
1024 MB 以下	10GB				
1024 MB を超える	「構成」メニュー「トレースの保存」の「分割ファイルサイズの上限」で指定したサイズの 10 倍。				
パーティション サイズ	保存先に指定したフォルダが存在するディスクの空き容量が、0 に近づいた場合に、保存されている中で最も古い時間フォルダを削除します。				

### 5.3.1.2.5.チャンネル設定

チャンネルごとのラインスピードの設定が行えます。

● キャプチャオプション

共通

キャプチャフィルタ

ロックトリガ

自動保存

チャンネル設定

通知設定

☒ チャンネル設定を手動で変更する

チャンネル	状態	マニュアルラインスピード
チャンネルA		<input type="text" value="1"/> Gb ▼
チャンネルB		<input type="text" value="1"/> Gb ▼
チャンネルC		<input type="text" value="1"/> Gb ▼
チャンネルD		<input type="text" value="1"/> Gb ▼

キャンセル

適用

「チャンネル設定を手動で変更する」にチェックを入れると、ラインスピードの手動設定が有効になります。

項目	説明
状態	各チャンネルの接続状況を表示します。 リンクアップ時には緑、リンクダウン時には赤が表示されます。 未対応のモデルは灰色が表示されます。
マニュアルラインスピード	ラインスピードの値を設定できます。 ここで設定した値が、使用率計算、及びマイクロバースト使用率の計算の際に 100%の基準として使用されます。 単位は Kb, Mb, Gb から選択できます。手動で設定しない場合は、アダプタ(キャプチャカード)の各ポートで受け取ることができる最大のビットレートがラインスピードとして使用されます。

### 5.3.1.2.6.通知設定 オプション

通知が飛ぶイベントを指定できます。

● キャプチャオプション

共通

キャプチャフィルタ

ロックトリガ

自動保存

チャネル設定

通知設定

自動保存

test

▼

☒ 有効

リンクステータス

test

▼

☒ 有効

ドロップ

test

▼

☒ 有効

キャンセル

適用

設定できるイベントは下記の通りです。

項目	説明
自動保存	自動保存はキャプチャ中のパケットをトレースファイルで自動的に保存する機能です。その自動保存機能でトレースファイルの保存の失敗や保存先の変更、自動保存の再開が発生した際に通知を出します。 自動保存機能についての詳細は <b>5.3.1.2.4 自動保存 オプション</b> を参照してください。
リンクステータス	各チャネルの接続状況が変化した際に通知を出します。 リンクアップしていたチャネルがリンクダウンした時だけでなく、リンクダウンしていたチャネルがリンクアップした際にも通知が出ます。
ドロップ	キャプチャされたパケットがディスクに書き込めずにドロップしたエラー(パケットドロップ)が発生した際に通知が出ます。

「有効」のチェックボックスにチェックを入れると、「通知グループ」が指定できるようになります。

登録されている「通知グループ」の中から、通知を出したい「通知グループ」を選択してください。

希望する「通知グループ」がなければ、「通知グループの編集」や「通知グループの作成」を選択し、新しく「通知グループ」を作成することも可能です。

「通知グループ」の作成方法は「構成」メニューの **12.10 通知グループ**を参照してください。

### 5.3.2. レコード タブ

エージェント・ペインで選択されたエージェントが保有しているキャプチャレコードが一覧で表示されます。一覧にあるキャプチャレコードの「名前」リンクをクリックすると、キャプチャレコード・ワークスペースに移動します。

概要

レコード

ロック

トレースファイル

外部データソース

Q

レコードのロック

トレースの保存

統計のエクスポート

解析

削除

バックアップ

リネーム

ストレージ情報

<input type="checkbox"/>	名前	開始時刻	終了時刻	ステータス	キャプチャフィルタ ▾	解析	解析ステータス	統計データ
<input type="checkbox"/>	<a href="#">2017/02/14 10:07:30</a>	2017/02/14 10:07:33	--	キャプチャ中	未適用		解析中...	
<input type="checkbox"/>	<a href="#">2017/02/13 16:21:19</a>	2017/02/13 16:21:22	2017/02/13 16:26:31	ロック期間あり	未適用		完了	<a href="#">ダウンロード可</a>
<input type="checkbox"/>	<a href="#">2017/02/13 15:59:08</a>	2017/02/13 15:59:14	2017/02/13 16:04:22	通常	未適用		完了	未エクスポート
<input type="checkbox"/>	<a href="#">2017/02/13 15:39:15</a>	2017/02/13 15:39:18	2017/02/13 15:49:28	通常	未適用		完了	未エクスポート
<input type="checkbox"/>	<a href="#">2017/02/13 13:08:17</a>	2017/02/13 13:08:21	2017/02/13 14:51:58	通常	未適用		完了	未エクスポート
<input type="checkbox"/>	<a href="#">2017/02/13 10:24:50</a>	2017/02/13 10:24:55	2017/02/13 10:55:25	パケットなし	未適用		完了	未エクスポート

一覧表で確認できる情報は以下の通りです。

項目	説明								
名前	キャプチャレコードの名前です。デフォルトでは「キャプチャ開始」ボタンをクリックした時刻になります。変更可能です。								
開始時刻	キャプチャを開始した時刻です。								
終了時刻	キャプチャを終了した時刻です。 キャプチャ中の場合は「--」と表示されます。								
ステータス	表示されるステータスの種類は以下の通りです。 <table><tr><td>キャプチャ中</td><td>現在キャプチャ中のレコードに表示されます。</td></tr><tr><td>ロック期間あり</td><td>レコード全体がロックされている、または、レコード内にロックされた期間がある時に表示されます。</td></tr><tr><td>パケットなし</td><td>データベース内にレコード期間内のパケットが存在しない場合に表示されます。</td></tr><tr><td>通常</td><td>上記以外の場合に表示されます。</td></tr></table>	キャプチャ中	現在キャプチャ中のレコードに表示されます。	ロック期間あり	レコード全体がロックされている、または、レコード内にロックされた期間がある時に表示されます。	パケットなし	データベース内にレコード期間内のパケットが存在しない場合に表示されます。	通常	上記以外の場合に表示されます。
キャプチャ中	現在キャプチャ中のレコードに表示されます。								
ロック期間あり	レコード全体がロックされている、または、レコード内にロックされた期間がある時に表示されます。								
パケットなし	データベース内にレコード期間内のパケットが存在しない場合に表示されます。								
通常	上記以外の場合に表示されます。								
キャプチャフィルタ	キャプチャ実行時に適用されたキャプチャフィルタです。 適用されていない場合は「未適用」と表示されます。								
解析	それぞれの解析ページにジャンプできます。 : APM/NPM 解析のページにジャンプします。 : マイクロバースト解析のページにジャンプします。								
解析ステータス	解析中か、解析が完了しているかが表示されます。 表示されるステータスは「未解析」「解析中・・・」「完了」です。								
統計データ	統計データが作成済みの場合、対象データへのリンクが表示されます。 詳細は <b>5.3.2.3 統計のエクスポート</b> を参照してください。								

「検索」 テキストボックスに文字列を入力してキャプチャレコードを検索できます。入力した文字列が、キャプチャレコードの名前と一致するものを表示します。部分一致検索も可能です。

### 5.3.2.1 レコードのロック

キャプチャレコードにロックをかけて保護することができます。

ロックしたいレコードにチェックを付けて、「レコードのロック」ボタンをクリックしてください。

選択したキャプチャレコード全体がロックされます。キャプチャ中のキャプチャレコードは、キャプチャ開始から、「レコードのロック」ボタンをクリックした時までのレコードがロックされます。

ロック後はキャプチャレコードリストの「ステータス」欄の表示が「ロック期間あり」に変わります。ロックタブのロックリストにもロックの情報が追加されます。

なお、保存先ディスクの容量の 80 パーセント以上を占める、キャプチャレコードをロックすることはできません。ロックする範囲を絞ってロックをかけてください。

キャプチャレコードの一部にのみロックをかけたい場合は、ロックタブに移動し、「新規」ボタンをクリックしてください。期間を指定してロックをかけることができます。

詳細は **5.3.3 ロックタブ** を参照してください。

### 5.3.2.2 トレースの保存

キャプチャレコードをトレースファイルに保存することができます。

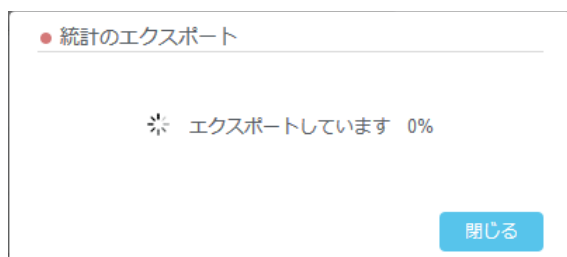
トレースファイルに保存したいキャプチャレコードにチェックマークを付け、「トレースの保存」ボタンをクリックしてください。「トレースの保存」ダイアログが表示され、選択しているキャプチャレコードをトレースファイルに保存することができます。

トレースファイル保存の手順は **5.4.2 トレースの保存** を参照してください。

### 5.3.2.3 統計のエクスポート

キャプチャレコードの 1 秒ごとの統計値をカンマ区切り (CSV) ファイルで保存し、ダウンロードすることができます。

統計ファイルを保存したいキャプチャレコードにチェックマークを付け、「統計のエクスポート」ボタンをクリックしてください。エクスポート中のステータスを示す下図のダイアログが開きます。



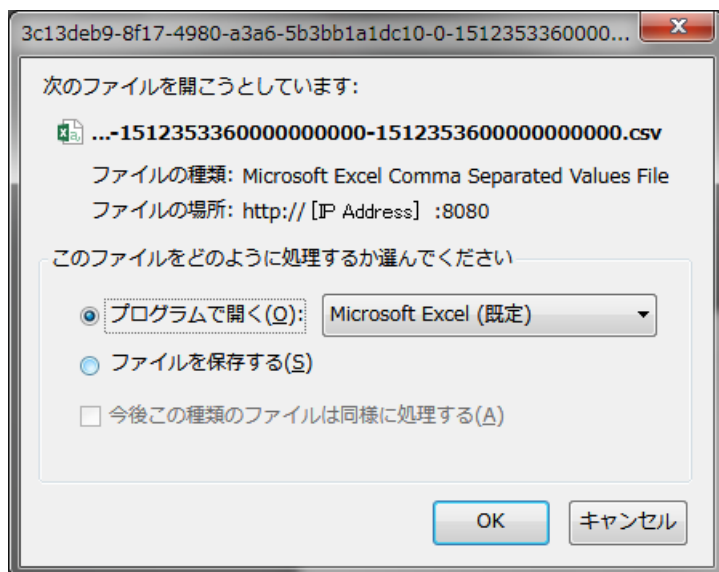
そのまましばらくお待ちください。ダイアログの表示が「ダウンロード可」に変わります。



この時、キャプチャレコードリストの「統計データ」欄の表示も「ダウンロード可」に変わります。

「統計のエクスポート」ダイアログの「ダウンロード可」リンクをクリックしてください。

下図のダウンロードダイアログが表示されます。



「ファイルを保存する」を選択すると、ダウンロードフォルダに CSV ファイルが保存されます。

なお、「統計のエクスポート」ダイアログで、「ダウンロード可」が表示される前に「閉じる」ボタンをクリックしても、統計値のエクスポートは実行されます。

その場合はキャプチャレコードリストの「統計データ」欄の表示が「ダウンロード可」に変わるのを待って、「ダウンロード可」リンクをクリックしてください。同様に統計値の CSV ファイルをダウンロードすることができます。

CSV ファイルに出力される統計値の種類については **Appendix C 統計値の CSV ファイル**を確認してください。

#### 5.3.2.4 解析

「解析」 ボタンをクリックすると、選択されたキャプチャレコードを解析処理できます。

どの解析モジュールを有効にするかは、「構成」メニューの「解析」セクションで選択できます。

詳細は **12.12 解析**を参照してください。

#### 5.3.2.5 削除

キャプチャレコードを選択して「削除」 ボタンをクリックすることにより、キャプチャレコードを削除することができます。



### 5.3.2.6 バックアップ

キャプチャレコードを選択して「バックアップ」ボタンをクリックすることにより、下記のデータをバックアップすることができます。

- 1) キャプチャレコードリスト
- 2) 統計データ
- 3) 解析結果

保存されたバックアップデータは外部データソースとして取り扱われ、ローカルのエージェントあるいは他のエージェントで閲覧することができます。具体的な手順は、**5.3.5 外部データソース タブ**を参照してください。

キャプチャレコードの名前の左側のチェックボックスにチェックを入れ、「バックアップ」ボタンをクリックすると、下記のバックアップ設定画面が開きます。

● バックアップ

期間

開始/終了 ▼

開始時刻 2017/02/08 17:56:06 

800 ms

終了時刻 2017/02/08 18:25:31 

346 ms

ファイルパス

/pvc/data/databank/backup

キャンセル

バックアップ

項目	説明
期間	バックアップの時間範囲です。開始/終了またはセンタースパンから指定方法を選択できます。センタースパンの場合は中央の時刻と前後の時間範囲（秒またはミリ秒）を指定します。
ファイルパス	バックアップデータを保存するフォルダを指定します。

「バックアップ」ボタンをクリックすると、バックアップデータの作成が開始されます。自動的に「外部データソース」画面に遷移し、バックアップ中のデータソースの状態が「実行中」と表示されます。バックアップが完了すると状態が「無効」に変わります。

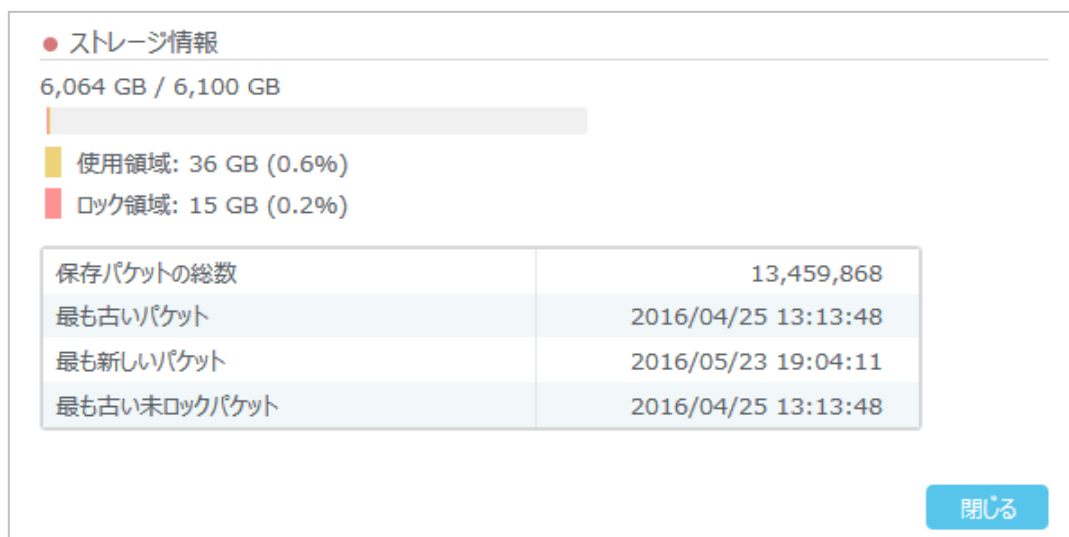
作成したバックアップデータを実際に閲覧する手順は、**5.3.5 外部データソース タブ**を参照ください。

### 5.3.2.7 リネーム

キャプチャレコードを選択して「リネーム」ボタンをクリックすることにより、キャプチャレコードの名前を変更できます。

### 5.3.2.8 ストレージ情報

「ストレージ情報」をクリックすると、パケットを格納するストレージの情報を表示します。



項目	説明
使用領域	パケットが格納されている領域を GB 単位で表示します。
ロック領域	ロックされたパケットが格納されている領域を GB 単位で表示します。
保存パケットの総数	保存された総パケット数を表示します。
最も古いパケット	最も古いパケットの保存日時を表示します。
最も新しいパケット	最も新しいパケットの保存日時を表示します。
最も古い未ロックパケット	ロックされていないパケットのうち、最も古いものの保存日時を表示します。

### 5.3.3. ロックタブ

ロックが設定されているキャプチャレコードが一覧で表示されます。

概要	レコード	ロック	トレースファイル	外部データソース
新規	レコードのロック解除	トレースの保存		
<input type="checkbox"/>	名前	開始時刻	終了時刻	ロック期間
<input type="checkbox"/>	<a href="#">Capture Session 05/06/2016 19:57</a>	2016/05/06 19:57:43.000	2016/05/09 09:52:42.000	2 13:54:59.000

一覧表で確認できる情報は以下の通りです。

項目	説明
名前	レコードのロックされた部分に付けられた名前です。
開始時刻	データのロックが掛けられている部分の開始日時です。
終了時刻	データのロックが掛けられている部分の終了日時です。
ロック期間	ロックの開始時刻から終了時刻までの時間です。

キャプチャレコードに新しくロック部分を追加したり、掛けられたロックを解除したりすることができます。一覧にあるレコードをトレースファイルとして保存することも可能です。

#### 5.3.3.1 新規

新しくロック部分を追加したいときは、「新規」ボタン(上図①)をクリックしてください。

● 新規

名前

New Lock

ロック期間

センタースパン

前

10

秒

日時

2017/12/05 14:24:16

0

ms

後

10

秒

2017/12/05 14:24:06.000 - 2017/12/05 14:24:26.000


キャンセル

適用

「名前」と「ロック期間」を指定して、「適用」ボタンをクリックしてください。

指定したレコードのロックが設定され、一覧に追加されます。設定項目の詳細は下記の通りです。

項目	説明
名前	ロックする期間に対する名前です。
ロック期間	ロックする時間範囲を指定します。 選択できる設定は「開始/終了」と「センタースパン」です。 「開始/終了」は時間範囲を開始時刻と終了時刻で指定します。 「センタースパン」は時間範囲の中央の「日時」を指定して、その前後の期間(秒/ミリ秒)で指定します(次頁参照)。

期間指定アイコンをクリックすると、下記のようにカレンダーと時計が表示されます。



The screenshot shows a web form titled "新規" (New). It has a text input for "名前" (Name) with the value "New Lock". Below it, there is a "ロック期間" (Lock Period) section. It includes a dropdown menu currently set to "開始/終了" (Start/End), and two time selection fields. The "開始時刻" (Start Time) is set to "2017/12/07 18:15:03" and the "終了時刻" (End Time) is also set to "2017/12/07 18:15:03". Each time field has a calendar icon to its left and a numeric input for milliseconds (ms) set to "0". A calendar and time picker overlay is visible, showing the date "12月 2017" (December 2017) and the time "18:15:03". The calendar grid shows the days of the month, with the 7th highlighted. The time picker shows hours (18), minutes (15), and seconds (03).

カレンダーで日付を指定し、下の時計で時間を指定してください。

ミリ秒(ms)単位でロック期間を指定したい場合は、ミリ秒の部分を手入力で入力してください。

#### 5.3.3.2 レコードのロック解除

レコードのロックを解除したい場合は、ロックを解除したいレコードのチェックボックスにチェックを入れて、「レコードのロック解除」ボタンをクリックしてください。

指定したレコードのロックが解除されます。

#### 5.3.3.3 トレースの保存

ロックされたレコードをトレースファイルに保存することができます。

トレースファイルに保存したいレコードのチェックボックスにチェックを入れて、「トレースの保存」ボタンをクリックしてください。「トレース保存」ダイアログが表示され、ロックされているそのレコードをトレースファイルとして保存することができます。

この機能は、キャプチャレコード・ワークスペースのトレースの保存機能と同様です。

詳細は **5.4.2 トレースの保存** を参照してください。

#### 5.3.3.4 ロック名の変更

ロック名を変更したい場合は、一覧表の「名前」のリンクをクリックしてください。

登録されているロック名が入ったテキストボックスが表示されて、ロック名を変更することができます。



### 5.3.4.2 カスタムファイル タブ

ユーザが定義した任意のカスタムフォルダに保存されているトレースファイルが一覧で表示されます。  
カスタムフォルダを指定して保存されたトレースファイルはダウンロード、デコードが行えません。

概要

レコード

ロック

トレースファイル

外部データソース

更新

削除

説明の編集

ビルトインファイル

カスタムファイル

トレースバンカー

<input type="checkbox"/>	ステータス	ファイルパス	期間	保存フィルタ	エージェント	作成者	トレースファイルの説明
<input checked="" type="checkbox"/>	完了	/pvc/data/custom_traces/1513738534285-1341.pcapng	2017/12/19 20:57:18.000 - 2017/12/19 20:58:23.000	なし	Default Agent	admin	

確認できる情報は以下の通りです。

項目	説明
ステータス	保存中は「ロード中...」と表示されます。 完了すると「完了」と表示されます。
ファイルパス	保存されたファイルパスとファイル名を表示します。
期間	トレースファイル内のデータの時間範囲を示しています。
保存フィルタ	トレースファイルの保存時に適用されたフィルタ名です。
エージェント	キャプチャを実行したエージェント名です。
作成者	トレースファイルを作成したアカウントを表示します。
トレースファイルの説明	トレースファイルの保存時に入力した説明文です。 詳細は <b>5.3.4.6 説明の編集</b> を参照してください。

### 5.3.4.3 トレースバンカー タブ

外部から読み込んだトレースファイルが一覧で表示されます。  
新しく外部からトレースファイルを読み込むことも可能です。

概要	レコード	ロック	トレースファイル	外部データソース
更新	削除	説明の編集		
ビルトインファイル	カスタムファイル	トレースバンカー		
アップロード				
<input type="checkbox"/>	名前	サイズ	更新日時	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> AANPMSample_interval0.1sec.pcap	21 KB	2017/12/19 16:51	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> AANPMSample_interval10sec.pcap	21 KB	2017/12/19 16:51	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> AANPMSample_interval1sec.pcap	21 KB	2017/12/19 16:51	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> AANPMSample_interval60sec.pcap	21 KB	2017/12/19 16:51	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> send.pcap	15 MB	2017/12/19 16:50	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> send2.pcap	11 MB	2017/12/19 16:50	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> send3.pcap	13 MB	2017/12/19 16:50	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> send4.pcap	251 MB	2017/12/19 16:51	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> test001.pcap	5 MB	2017/12/19 16:51	
<input checked="" type="checkbox"/>	<a href="#">デコード</a> test002.pcap	5 MB	2017/12/19 16:51	

一覧で表示される情報は「名前」「サイズ」「更新日時」です。

「デコード」のリンクをクリックすると、エージェント・ワークスペース画面にデコードタブが追加され、選択したトレースファイルの packets がデコードされて表示されます。

デコード機能については **5.3.7 デコード** を参照してください。

外部からトレースファイルを読み込みたい場合は、「アップロード」ボタンをクリックしてください。

下図の「アップロード」ダイアログが表示されます。



「参照」ボタンをクリックして読み込むファイルを指定し、「トレースファイルをアップロード」ボタンをクリックしてください。指定したトレースファイルが一覧に追加されます。

#### 5.3.4.4 更新

「更新」ボタンをクリックすると、トレースファイルリストを更新します。

#### 5.3.4.5 削除

トレースファイルを削除したい場合、トレースファイル左側のチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。選択されたトレースファイルが削除されます。

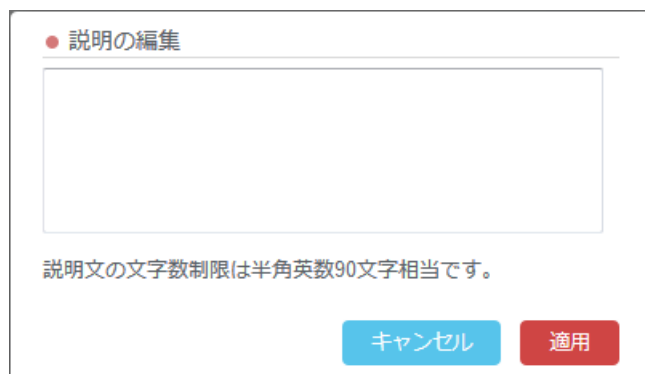
全てのトレースファイルを削除したい場合は、先頭行のチェックボックスにチェックを入れ、「削除」ボタンをクリックします。

#### 5.3.4.6 説明の編集

保存したトレースファイルの説明の内容を編集することができます。

「トレースファイルの説明」欄に表示される説明内容を変更したい場合は、説明を変更したいトレースファイルのチェックボックスにチェックを入れ、「説明の編集」ボタンをクリックしてください。

下記の「説明の編集」ダイアログが表示され、説明の内容を編集できます。



保存したトレースファイルは「トレースファイルの説明」以外の項目は編集できません。

複数のトレースファイルの説明をまとめて編集することはできません。

### 5.3.5. 外部データソース タブ

この画面では、レコード・タブからのバックアップ手順で保存したバックアップデータのリストを表示します。また、他の Synesis で作成したバックアップデータを本画面に追加することもできます。この画面でバックアップデータを有効化することにより、データを閲覧することが可能になります。

概要

レコード

ロック

トレースファイル

外部データソース

追加

削除

有効化

無効化

<input type="checkbox"/>	名前	ファイルパス	開始時刻	終了時刻	ステータス	バックアップの中止
<input type="checkbox"/>	Backup 2017/02/09 10:19:22	/pvc/data/databank/backup/bac	2017/02/01 14:02:33	—	実行中	<a href="#">キャンセル</a>
<input type="checkbox"/>	Backup 2017/02/09 10:18:30	/pvc/data/databank/backup/bac	2017/02/01 16:53:48	2017/02/01 16:54:02	無効	
<input type="checkbox"/>	Backup 2017/02/09 10:15:49	/pvc/data/databank/backup/bac	2017/02/08 14:29:20	2017/02/08 14:54:56	無効	
<input type="checkbox"/>	Backup 2017/02/09 09:53:05	/pvc/data/databank/backup/bac	2017/02/08 17:56:06	2017/02/08 18:25:31	無効	

#### 5.3.5.1 追加

バックアップデータをリストに追加する場合は「追加」ボタンをクリックしてください。パスを入力するダイアログが表示されますので、データが格納されているフォルダパスを入力して「追加」ボタンをクリックしてください。指定したパスのサブディレクトリに複数のバックアップデータが存在している場合は、それらが全てリストに追加されます。

#### 5.3.5.2 削除

データソースを削除したい場合は、チェックボックスにチェックを入れて「削除」ボタンをクリックしてください。選択したデータソースが削除できます。この操作では実際のデータファイルはディスク上から削除されません。

#### 5.3.5.3 有効化

「有効」なデータソースのみがエージェント・ペインに表示されます。

「無効」なデータソースを有効化したい場合は、データソースのチェックボックスにチェックを入れ、「有効化」ボタンをクリックしてください。ステータスが「実行中」あるいは「失敗」のデータソースは有効化できません。また同時に有効化できるデータソース数の上限は 2 個です。

名前	パス
Backup 2016/05/23 13:48	/home/toyo/databank/backup/backup_20160523
<input checked="" type="checkbox"/> Backup 2016/05/20 15:17	/home/toyo/databank/backup/backup_20160520
Backup 2016/05/20 11:58	/home/toyo/databank/backup/backup_20160520
Backup 2016/05/20 10:48	/home/toyo/databank/backup/backup_20160520
Backup 2016/05/20 10:39	/home/toyo/databank/backup/backup_20160520
Backup 2016/05/19 16:49	/home/toyo/databank/backup/backup_20160519

#### 5.3.5.4 無効化

「有効」状態のデータソースを無効化したい場合は、データソースのチェックボックスにチェックを入れ、「無効化」ボタンをクリックします。



## 5.3.6. リアルタイムデコードタブ

キャプチャしたパケットをリアルタイムにデコードし、デコードした結果を表示します。

デコードされるパケットは 1 秒間に 1 パケットのみです。

The screenshot shows the SYNESIS Real-time Decode tab. It features a sidebar on the left with navigation icons. The main area is divided into three sections: ① a list of captured packets, ② details of the selected packet, and ③ the packet data in hexadecimal and ASCII.

時間	送信元	送信先	プロトコル	長さ	サマリー
14:35:25.882776000	3fe:831f:4004:1952:8000:d36:2efc:f47a	:::2::1	IPv6	82	IPv6 no next header
14:35:29.601211000	167.144.23.56	10.159.63.127	TNS	520	Response, Data (6), Data
14:35:32.405622000	167.144.23.54	10.159.63.127	TCP	721	[TCP segment of a reassembled PDU]
14:35:34.343736000	10.159.63.126	10.158.17.104	TCP	1434	80 >=2>x86v92 1139 [ACK] Seq=1 Ack=1 Win=16560 Len=1380
14:35:38.634187000	Dell_28.43.d4	Broadcast	ARP	60	Who has 192.168.0.48? Tell 192.168.0.131
14:35:43.005690000	192.168.0.12	192.168.0.1	TCP	60	1103 >=2>x86v92 3143 [ACK] Seq=1 Ack=1 Win=17520 Len=0
14:35:48.001358000	192.168.0.15	192.168.0.14	UDP	411	49562 >=2>x86v92 49566 Len=369
14:35:51.729053000	63.204.74.136	192.168.0.10	TCP	1454	1214 >=2>x86v92 1360 [ACK] Seq=1 Ack=1 Win=16462 Len=1400
14:35:54.307338000	64.165.201.248	192.168.0.10	TCP	590	1214 >=2>x86v92 1379 [ACK] Seq=1 Ack=1 Win=1838 Len=536
14:35:58.824996000	192.168.0.14	192.168.0.15	UDP	703	49566 >=2>x86v92 49562 Len=661
14:36:02.751809000	192.168.0.12	192.168.0.24	UDP	154	20598 >=2>x86v92 20598 Len=112
14:36:05.952471000	192.168.0.12	192.168.0.24	UDP	1312	20596 >=2>x86v92 20596 Len=1270

② Details of the selected packet (Frame 82):

- Frame: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
- Ethernet II, Src: Toshiba\_5f:36:c7 (00:08:0d:5f:36:c7), Dst: IPv4mcast\_fc (01:00:5e:00:00:fc)
- Internet Protocol Version 4, Src: 192.168.0.63, Dst: 224.0.0.252
- User Datagram Protocol, Src Port: 4689, Dst Port: 3544
- Teredo IPv6 over UDP tunneling
- Internet Protocol Version 6, Src: 3fe:831f:4004:1952:8000:d36:2efc:f47a, Dst: :::2::1

③ Packet data (Hexadecimal and ASCII):

アドレス	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000	01	00	5E	00	00	FC	00	08	0D	5F	36	C7	08	00	45	00	. . . * . . . . . 6 . . . . E .
0010	00	44	EC	EF	00	00	01	11	2A	D6	C0	A8	00	3F	E0	00	. . . D . . . . . * . . . . ? .
0020	00	FC	12	51	0D	D8	00	30	D6	45	60	00	00	00	00	00	. . . Q . . . . . 0 . . . . E . . .
0030	3B	15	3F	FE	83	1F	40	04	19	52	80	00	0D	36	2E	FC	. . . ? . . . . . @ . . . . R . . . 6 .
0040	F4	7A	FF	02	00	00	00	00	00	00	00	00	00	00	00	00	. . . z . . . . . . . . . . . . . .
0050	00	01															. . . . .

リアルタイムデコード画面は、キャプチャされたパケットが時間順に表示される「パケット一覧」(上図①)と、「パケット一覧」で選択されたパケットの詳細が表示される「パケット詳細」(上図②)、同じく選択されたパケットの中身が 16 進数で表示される「パケットデータ」(上図③)で構成されます。

「パケット一覧」の内容はキャプチャが行われるごとに更新され、最新のパケットが一番下に追加されます。確認できる情報は以下の通りです。

項目	説明
時間	そのパケットがキャプチャされた時間です。
送信元	パケットの送信元です。
送信先	パケットの送信先です。
プロトコル	通信プロトコルです。登録された名前※で表示されます。
長さ	パケットの長さです。
サマリー	パケット内容の要約です。

※ツールバー「構成」メニューの「プロトコル」に登録されています。

「パケット詳細」の各ヘッダのノード▶をクリックすると、中身が展開され詳細を確認できます。

「パケット詳細」で特定のヘッダを選択すると、「パケットデータ」で選択された部分に該当する 16 進数の部分がフォーカスされます。

リアルタイムデコードタブはキャプチャ中にのみ表示されます。キャプチャを終了するとこのタブは閉じられます。

### 5.3.7. デコード

トレースファイルをデコードして、Synesis 上で表示させることができます。

検索機能やフィルタ機能を使って必要なパケットだけを表示させることができます。

概要 レコード ログ トレースファイル 外部データソース **デコード 1 x**

検索タイプ サマリー  🔍 パケットNo.:  移動 総パケット数: 1728389

フィルタ フィルタなし 適用 トレースの保存

デコード機能でサポートしていない保存フィルタの項目: チャンネル、エラー、パターン

No.	時間	デルタ時間	送信元	送信先	プロトコル	長さ	サマリー
1	16:35:03.0000(0.000000)	44.107.128.25	192.55.53.24	UDP	64	4022 --> 23 Len=18	
2	16:35:03.0000(0.000001)	158.51.103.78	96.27.154.140	UDP	64	4022 --> 23 Len=18	
3	16:35:03.0000(0.000001)	79.25.179.167	48.13.205.70	UDP	64	4022 --> 23 Len=18	
4	16:35:03.0000(0.000001)	175.138.126.2	24.6.230.163	UDP	64	4022 --> 23 Len=18	
5	16:35:03.0000(0.000001)	87.197.63.113	132.5.212.96	UDP	64	4022 --> 23 Len=18	
6	16:35:03.0000(0.000001)	163.228.56.13	66.2.234.48	UDP	64	4022 --> 23 Len=18	

▶ Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0

▼ Ethernet II, Src: Performa\_00:00:02 (00:10:94:00:00:02), Dst: Superlan\_00:00:01 (00:00:01:00:00:01)

▶ Destination: Superlan\_00:00:01 (00:00:01:00:00:01)

▶ Source: Performa\_00:00:02 (00:10:94:00:00:02)

**Type: IPv4 (0x0800)** ← ④

Frame check sequence: 0xd663146e [correct]

FCS Status: Good

▶ Internet Protocol Version 4, Src: 158.51.103.78, Dst: 96.27.154.140

▶ User Datagram Protocol, Src Port: 4022, Dst Port: 23

▶ Data (18 bytes)

アドレス	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	00	00	01	00	00	01	00	10	94	00	00	02	08	00	45	00
0010	00	2E	ED	6D	00	00	FF	11	CE	27	9E	33	67	4E	60	1B
0020	9A	8C	0F	B6	00	17	00	1A	50	AE	00	00	00	00	00	00
0030	00	00	00	00	00	00	00	00	00	00	9F	15	D6	53	14	6E

デコード画面はファイル内のパケットがキャプチャ順に表示される「パケット一覧」(上図①)と、「パケット一覧」で選択されたパケットの詳細が表示される「パケット詳細」(上図②)、同じく選択されたパケットの中身が 16 進数で表示される「パケットデータ」(上図③)で構成されます。

「パケット一覧」で確認できる情報は以下の通りです。


項目	説明
No	トレース内で時間の昇順に並べた場合の通し番号です。
時間	そのパケットがキャプチャされた時間です。
デルタ時間	1 つ前のパケットがキャプチャされてからの時間の差分です。
送信元	パケットの送信元です。
送信先	パケットの送信先です。
プロトコル	通信プロトコルです。ツールバー「構成」メニューの <b>プロトコル</b> で登録された名前が表示されます。詳細は <b>12.15 プロトコル</b> を確認してください。
長さ	パケットの長さです。
サマリー	パケット内容の要約です。

「パケット詳細」の各ヘッダのノード▶をクリックすると、中身が展開され詳細を確認できます。特定のヘッダを選択すると(上図④)その部分に該当する 16 進数部分(上図⑤)がフォーカスされます。

### 5.3.7.1 検索

文字列やパケット No を指定して、パケットトレース内を検索することが可能です。

#### 文字列での検索

文字列で検索を行うには検索タイプ(上図①)で検索対象を選択し、検索したい文字列をテキストボックス(上図②)に入力して、「検索」  アイコンをクリックしてください。指定された文字列の検索が実行されます。キーボードの Enter を押下しても、同様に検索が実行されます。

検索条件に一致する文字列が検知されると、パケット一覧上のフォーカス（上図オレンジ部⑥）がその文字列を持つパケットの行へ移動します。

選択可能な検索タイプは以下の通りです。

検索タイプ	検索対象
サマリー	パケット一覧の「サマリー」の項目内の文字列を検索します。
パケット詳細部	パケット詳細内の文字列を検索します。
(Hex)パケットデータ部	パケットデータの Hex 文字列で検索します。
(ASCII)パケットデータ部	パケットデータの ASCII 文字列で検索します。

#### パケット No での検索

パケット No はデコードされたトレースファイル内のパケットを、時間の昇順に並べた場合の通し番号です。

このパケット No で検索を行う場合は、「パケット No」のテキストボックス(上図③)に検索対象のパケット No を入力し、「移動」ボタン(上図④)をクリックしてください。

パケット一覧上のフォーカス(上図オレンジ部⑥)が、指定した「パケット No」の行に移ります。

パケット No として指定できる番号は "1" から総パケット数（上図⑤）です。

### 5.3.7.2 表示フィルタ

パケット一覧で表示するパケットをフィルタリングするための表示フィルタとして、保存フィルタを使用します。

管理者ロールで操作している場合は、保存フィルタを追加・編集して使用することもできます。

フィルタのテキストボックスの▼アイコン(下図①)をクリックしてください。設定済みの保存フィルタのリスト(下図②)が表示されます。



使用したい保存フィルタを選択し、「適用」ボタン(上図③)をクリックしてください。

条件に一致するパケットのみが抽出され、一覧表に表示されます。

但し、デコード機能の表示フィルタでは、下記の種類のフィルタはサポートしていません。

- チャンネル
- エラー
- パターン

適用した表示フィルタを解除したい場合は、「フィルタなし」を選択して「適用」ボタン(上図③)をクリックしてください。

管理者ロールで操作している場合は保存フィルタを追加・編集して使用することが出来ます。

「新規フィルタの作成」を選択すると、新規フィルタ登録画面が表示されます。フィルタの設定を行い「保存」ボタンをクリックすると、設定したフィルタが登録され、表示フィルタに設定されます。

「既存フィルタの編集」を選択すると、登録済みの保存フィルタの一覧が表示されます。

保存フィルタを編集後、編集した保存フィルタにチェックマークを付け、「適用」ボタンをクリックしてください。チェックマークを付けた保存フィルタが表示フィルタに設定されます。

保存フィルタの種類や登録方法など、詳細は **12.6 保存フィルタ**を確認してください。

### 5.3.7.3      トレースの保存

デコードしてフィルタリングしたパケットを、トレースファイルに保存することが出来ます。

デコード画面の「トレースの保存」ボタンをクリックしてください。

下図の「トレースの保存」ダイアログが表示されます。

● トレースの保存

説明

期間

センタースパン ▼

前

10

秒 ▼

日時

2017/02/01 14:03:27

0

ms

後

10

秒 ▼

2017/02/01 14:03:17.000 - 2017/02/01 14:03:37.000

ファイル形式

pcapng ▼

☒ 現在のフィルタを適用する

保存先フォルダ

カスタムフォルダ ▼

/pvc/data/custom\_traces

キャンセル

トレースの保存

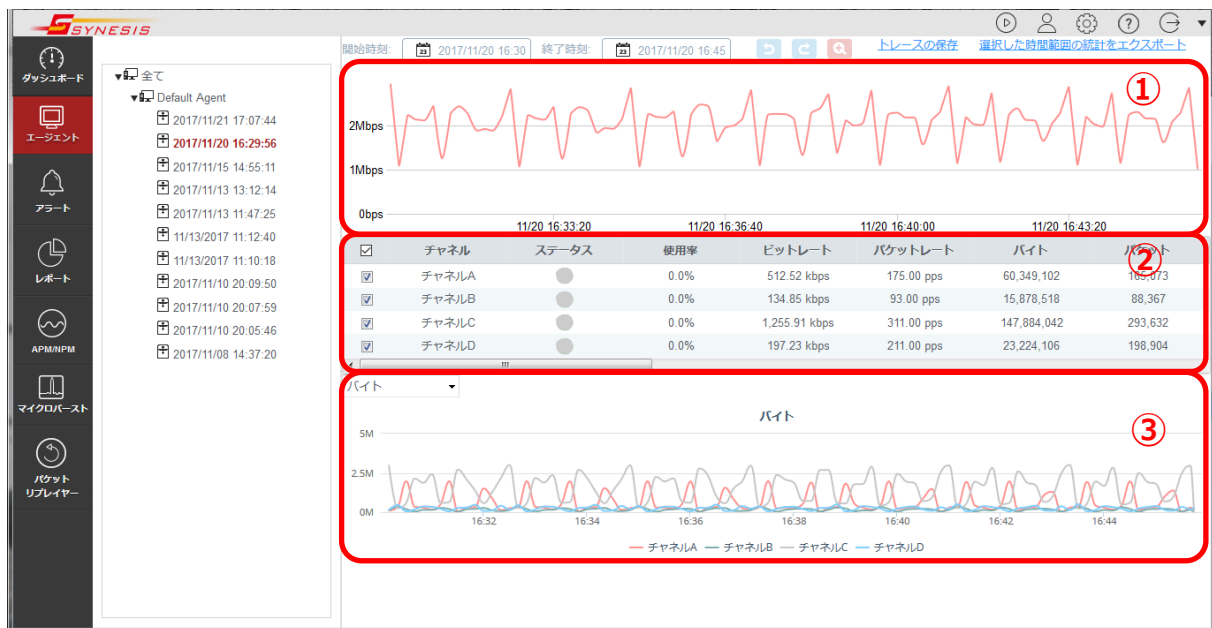
設定項目の詳細は以下の通りです。

項目	説明
説明	任意の説明文を入力することができます。
期間	トレースファイルを作成する時間範囲を指定します。 選択できる設定は「開始/終了」と「センタースパン」です。 「開始/終了」では時間範囲を「開始時刻」と「終了時刻」で指定します。 「センタースパン」では「日時」で中心となる時刻を指定し、「前」と「後」でそれぞれその前後の期間(秒/ミリ秒)を指定します。トレースファイルとして保存される期間が「後」の下に表示されます。
ファイル形式	保存するファイル形式を選択してください。 選択可能なファイル形式は pcap、pcap (ナノ秒単位)、pcapng です。
現在のフィルタを適用する	表示フィルタを適用している場合、トレース保存時のパケットのフィルタリングにもそのフィルタを適用するか否かを選択します。
保存先フォルダ	トレースファイルの保存先を選択します。 「ビルトインフォルダ」を選択すると、トレースファイルの保存先として指定されているフォルダにトレースファイルが保存されます。 「カスタムフォルダ」を選択すると右側にテキストボックスが表示され、Synesis 内の任意のフォルダを指定できます。ただしこの場合、保存後にダウンロードやデコードが行えなくなりますのでご注意ください。

設定後、「トレースの保存」ボタンをクリックしてください。

## 5.4. キャプチャレコード・ワークスペース

キャプチャレコード・ワークスペースでは、レコードの時間範囲を指定してのトレースファイルの保存と、選択された時間範囲での統計値を CSV ファイルで出力させることが可能です。



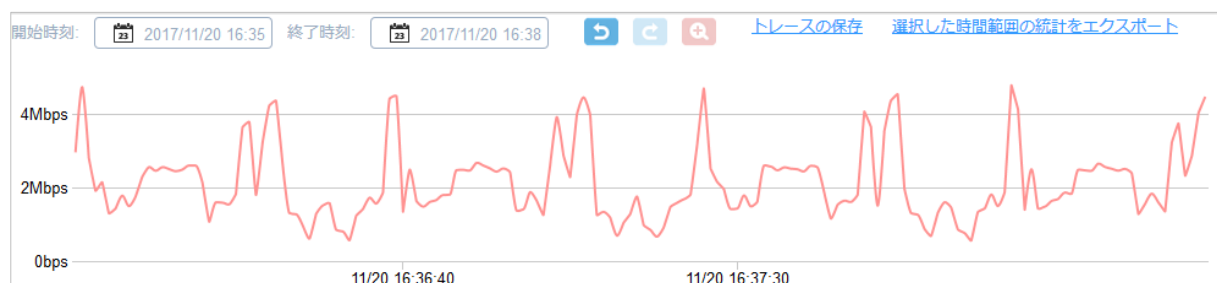
キャプチャレコード・ワークスペースを表示させるには、エージェント・ペインやでキャプチャレコードを選択するか、エージェント・ワークスペースのレコード タブで、キャプチャレコードの「名前」リンクをクリックしてください。


画面の一番上には全チャンネルの合計値のトレンドグラフ(上図①)が表示されます。このグラフはビットレートの合計値のグラフになります。

その下にはチャンネルごとの統計値のテーブル(上図②)と、トレンドグラフ(上図③)が表示されます。チャンネルごとのこのグラフにはどのグラフを表示させるかを選択することができます。

### チャンネルの合計値のトレンドグラフ

キャプチャレコード・ワークスペースの一番上の段には、全チャンネルの合計値のトレンドグラフが表示されます。このグラフはビットレートのグラフになります。



このグラフで値を確認しながら、マウスドラッグ操作で時間範囲を指定し、「拡大」 ボタンをクリックすると、グラフを拡大表示させることができます。

詳細は **5.4.1 時間範囲を指定しての拡大表示**を確認してください。

## チャンネルごとの統計値とトレンドグラフ

キャプチャレコード・ワークスペースの 2 段目と 3 段目には、チャンネルごとの統計値のテーブルとトレンドグラフが表示されます。



テーブルに記載される項目は以下の通りです。

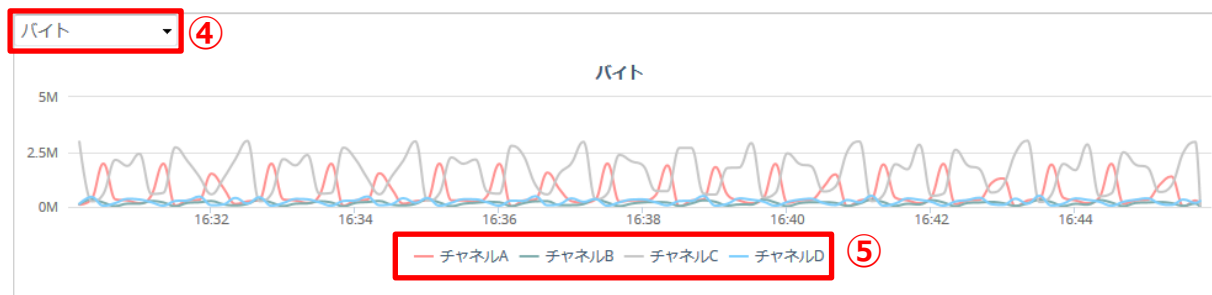
項目	説明
チャンネル	キャプチャを行っているチャンネルです。 チャンネルグループの設定をしている場合、「チャンネルグループに設定した名前 + IN または OUT」の形式（例：チャンネルグループ 1 IN）で表示されます。
ステータス	各チャンネルの接続状況を表示します。リンクアップ時には緑、リンクダウン時には赤が表示されます。未対応のモデルに対しては灰色が表示されます。※
使用率	回線の使用率を%で示します。
ビットレート	1 秒間に受信したビット数です。
パケットレート	1 秒間に受信したパケット数です。
バイト	受信した総バイト数です。
パケット	受信した総パケット数です。
ドロップ	ドロップしたパケット数です。
ブロードキャスト	ブロードキャストパケット数です。
マルチキャスト	マルチキャストパケット数です。
ユニキャスト	ユニキャストパケット数です。
CRC※	CRC エラーのパケット数です。フラグメントおよびジャバーは含みません。
フラグメント※	CRC エラーのうち、64 byte 未満のパケット数です。
ジャバー※	CRC エラーのうち特定の値(byte)より大きいパケット数です。 値(byte)はモデルによって異なります。※
オーバーサイズ※	CRC エラー以外で特定の値(byte)より大きいパケット数です。 値(byte)はモデルによって異なります。※
ラント※	CRC エラー以外で、64 byte 未満のパケット数です。
アダプタ	キャプチャ時に選択されたアダプタの名称です。

※ CRC～ラントのエラーパケットの検出はモデル(アダプタ)によっては統計が取れず「N/A」と表示されます。対応している場合も、ジャバーやオーバーサイズとカウントされるパケットのサイズ(byte)はモデルによって異なります。

対応モデルやパケットサイズ(byte)の詳細は **Appendix H モデルによる違い**を参照してください。



テーブルの下に表示されているチャンネルごとのトレンドグラフは、グラフ左上のドロップダウン・リスト(下図④)で、どのグラフを表示するかを選択することができます。



また、グラフ下部に表示されたチャンネル名(上図⑤)などの要素をクリックすると、そのチャンネルのグラフの表示/非表示を切り替えることができます。

選択可能なデータの種類の通りです。

項目	説明
使用率	回線の使用率を%で示します。
ビットレート	1 秒間に受信したビット数です。
バイト	受信した総バイト数です。
パケット	受信した総パケット数です。
ドロップ	ドロップしたパケット数です。
ブロードキャスト	ブロードキャストパケット数です。
マルチキャスト	マルチキャストパケット数です。
ユニキャスト	ユニキャストパケット数です。
CRC※	CRC エラーのパケット数です。フラグメントおよびジャバーは含みません。
フラグメント※	CRC エラーのうち、64 byte 未満のパケット数です。
ジャバー※	CRC エラーのうち特定の値(byte)より大きいパケット数です。 値(byte)はモデルによって異なります。※
オーバーサイズ※	CRC エラー以外で特定の値(byte)より大きいパケット数です。 値(byte)はモデルによって異なります。※
ラント※	CRC エラー以外で、64 byte 未満のパケット数です。
アダプタ	キャプチャ時に選択されたアダプタの名称です。

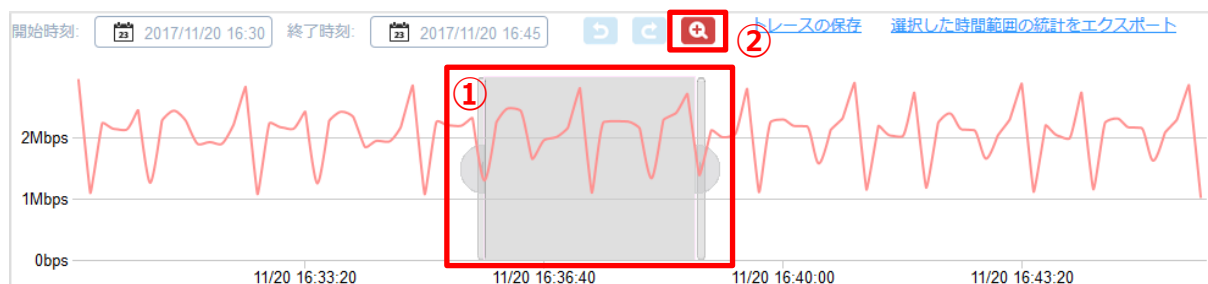
※ CRC～ラントのエラーパケットの検出はモデル(アダプタ)によっては統計が取れず「N/A」と表示されます。対応している場合も、ジャバーやオーバーサイズとカウントされるパケットのサイズ(byte)はモデルによって異なります。


対応モデルやパケットサイズ(byte)の詳細は **Appendix H モデルによる違い**を参照してください。



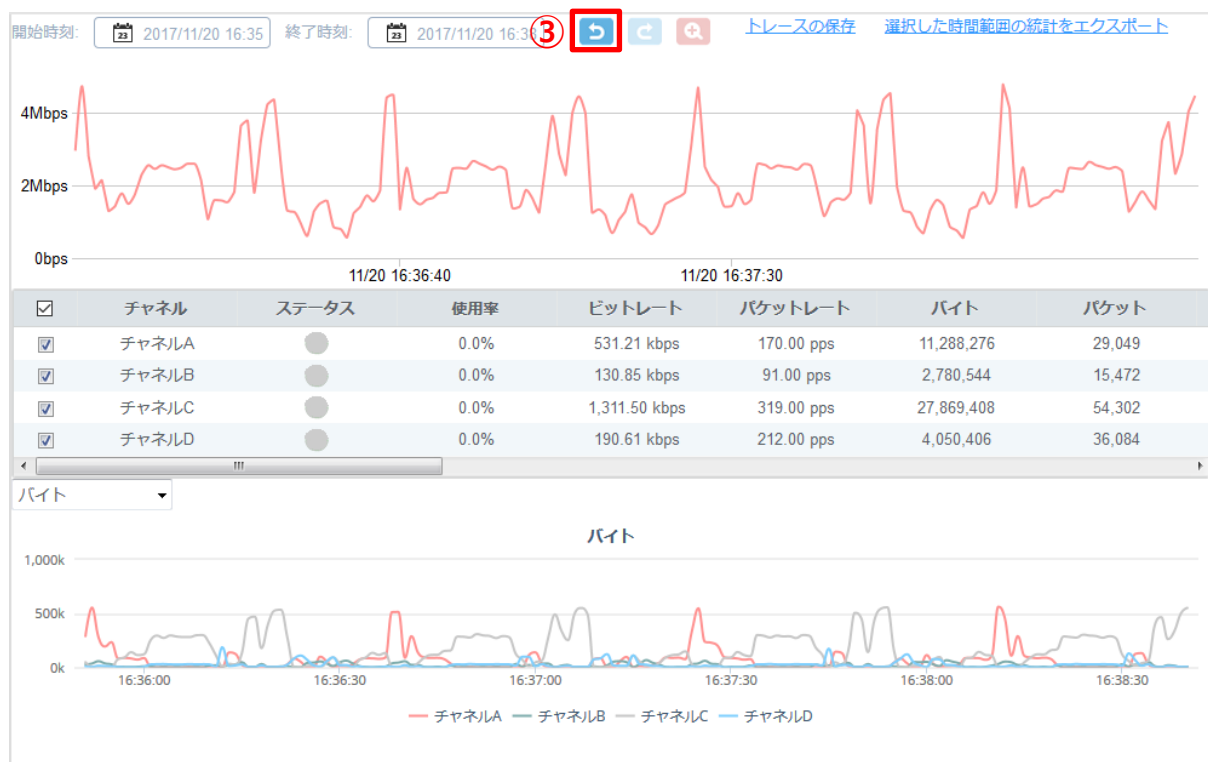
### 5.4.1. 時間範囲を指定しての拡大表示

時間範囲を指定してグラフを拡大表示したい場合は、まず、1 段目の、合計値のトレンドグラフをマウスドラッグして、拡大表示したい時間範囲を選択してください (下図①)。





時刻表示の右横に並んだ「拡大」アイコン  (上図②) をクリックすると、グラフが選択した時間範囲で拡大表示されます。

このとき、統計情報のテーブルやチャンネル毎のグラフも、指定した時間範囲の表示に更新されます。



「開始時刻」と「終了時刻」の時刻表示部分をクリックすると、カレンダーと時計が表示されます。このカレンダーと時計で開始時刻と終了時刻を指定し、拡大表示させることも可能です。

ナビゲーションバーの「元に戻す」アイコン  (上図③) をクリックすると、直前に行った拡大処理が取り消され、「やり直す」アイコン  をクリックすると、直前に行った「元に戻す」処理がキャンセルされます。

拡大表示させた状態で「トレースの保存」や「選択した時間範囲の統計をエクスポート」のリンクをクリックすると、拡大表示させた部分のみのトレースファイルや統計値の CSV ファイルを保存することができます。

## 5.4.2. トレースの保存

時間範囲を指定したトレースファイルを保存することができます。

時間範囲を指定して拡大表示を行っている場合は、改めて時間範囲を指定することなく、その拡大表示している時間範囲のトレースファイルが保存できます。

トレースファイルの保存を行う場合は「トレースの保存」リンク(下図④)をクリックしてください。



下図の「トレースの保存」ダイアログが表示されます。

● トレースの保存

ファイル名

説明

期間

センタースパン

前秒

日時

ms

後秒

2017/12/04 11:49:39.000 - 2017/12/04 11:49:59.000

ファイル形式

pcapng

最大ファイルサイズ 1024MB

☐ 詳細設定

キャンセル

トレースの保存

期間やファイル形式など、必要な項目を指定して「トレースの保存」ボタンを押してください。

設定項目の詳細は以下の通りです。

項目	説明
ファイル名	トレースファイルの名前です。
説明	任意の説明文を入力することができます。
期間	トレースファイルを作成する時間範囲を指定します。 選択できる設定は「開始/終了」と「センタースパン」です。 「開始/終了」では時間範囲を「開始時刻」と「終了時刻」で指定します。 「センタースパン」では「日時」で中心となる時刻を指定し、「前」と「後」でそれぞれその前後の期間(秒/ミリ秒)を指定します。トレースファイルとして保存される期間が「後」の下に表示されます。
ファイル形式	保存するファイル形式を選択してください。 選択可能なファイル形式は pcap、pcap (ナノ秒単位)、pcapng です。
詳細設定	チェックを入れると、より詳細な設定を行えるようになります。 詳細は次頁を参照してください。

「詳細設定」にチェックを入れると、分割ファイルサイズや保存先フォルダなど、より詳細な項目を設定することができます。「詳細設定」にチェックを入れた場合の画面は下図の通りです。

● トレースの保存

ファイル名

1512464615253-5885

説明

期間

開始/終了

開始時刻

2017/12/04 11:48:32

0

ms

終了時刻

2017/12/04 11:51:06

0

ms

ファイル形式

pcapng

分割ファイルサイズ

1024

MB (1-4096)

最大ファイル数

1

(0-99, 0: 制限なし)

保存フィルタ

フィルタなし

☐ スライス

32

バイト

保存先フォルダ

カスタムフォルダ

/pvc/data/custom\_traces

☒ 詳細設定

キャンセル

トレースの保存

具体的には以下の項目が設定可能になります。

項目	説明
<b>分割ファイル サイズ(MB)</b>	トレースファイルを分割するサイズを設定します。 指定するサイズを超えた場合に、自動的に分割されます。
<b>最大ファイル数 (0-99, 0 = 無制限)</b>	トレースファイルを分割して保存する際に、生成する最大のファイル数を設定します。
<b>保存フィルタ</b>	適用する保存フィルタを選択できます。 詳細は次頁の「保存フィルタについて」を参照してください。
<b>スライス</b>	キャプチャレコード中の各パケットについて、パケットの先頭から決められたバイト数分だけ取り出してトレースファイルに保存します。 設定可能なサイズは <b>Appendix H モデルによる違い</b> を参照してください。
<b>保存先フォルダ</b>	トレースファイルの保存先を選択します。 「ビルトインフォルダ」を選択すると、トレースファイルの保存先として指定されているフォルダにトレースファイルが保存されます。 「カスタムフォルダ」を選択すると右側にテキストボックスが表示され、Synesis 内の任意のフォルダを指定できます。ただしこの場合、保存後にダウンロードやデコードが行えなくなりますのでご注意ください。

## 保存フィルタについて

保存フィルタのドロップダウンリストを開くと保存フィルタの一覧が表示されます。管理者ロールで操作している場合は、保存フィルタの操作メニューも表示されます。(下図は管理者ロール表示です)

保存フィルタ

スライス

保存先フォルダ

詳細設定

フィルタなし

フィルタなし

既存フィルタの編集

新規フィルタの作成

チャンネルフィルタ

エラーフィルタ ⑤

パケットサイズフィルタ

MACアドレスフィルタ

VLANフィルタ

L2フィルタ

L3フィルタ

フローフィルタ

TCPフラグフィルタ

TCPウィンドウサイズフィルタ

アプリケーションフィルタ

パターンフィルタ

キャンセル

トレースの保存

使用したい保存フィルタが定義済みであれば、その保存フィルタの中から選択してください(上図⑤)。選択した保存フィルタを取り消したい場合は「フィルタなし」を選択してください。

「新規フィルタの作成」を選択すると、新規フィルタ登録画面が表示されます。フィルタの設定を行い「保存」ボタンをクリックすると、設定したフィルタが登録され、保存フィルタに設定されます。

「既存フィルタの編集」を選択すると、登録済みの保存フィルタの一覧が表示されます。

● 保存フィルタ

新規 削除

<input type="checkbox"/>	名前	説明
<input type="checkbox"/>	<a href="#">チャンネルフィルタ</a>	{[チャンネル - チャンネルA]}
<input type="checkbox"/>	<a href="#">エラーフィルタ</a>	{[エラー - エラーパケット]}
<input type="checkbox"/>	<a href="#">パケットサイズフィルタ</a>	{[パケットサイズ - サイズ >= 100]}
<input type="checkbox"/>	<a href="#">MACアドレスフィルタ</a>	{[MACアドレス - 01:23:45:67:89:ab --> Any]}
<input type="checkbox"/>	<a href="#">VLANフィルタ</a>	{[VLAN - VLAN ID: 200]}
<input type="checkbox"/>	<a href="#">L2フィルタ</a>	{[L2 Ether Type - L2 Ether Type: IPv4;]}
<input type="checkbox"/>	<a href="#">L3フィルタ</a>	{[L3 Protocol - L3 Protocol: TCP;]}
<input type="checkbox"/>	<a href="#">フローフィルタ</a>	{[フロー - 172.0.0.0:1-4 --> Any]}
<input type="checkbox"/>	<a href="#">TCPフラグフィルタ</a>	{[TCPフラグ - TCPフラグ: SYN]}
<input type="checkbox"/>	<a href="#">TCPウィンドウサイズフィルタ</a>	{[TCPウィンドウサイズ - TCPウィンドウサイズ: 300]}
<input type="checkbox"/>	<a href="#">アプリケーションフィルタ</a>	{[アプリケーション - 第4層タイプ: TCP; HTTP(80;443);]}

キャンセル 適用

編集したい保存フィルタの名前のリンクをクリックしてください。その保存フィルタを編集できます。

「新規」ボタンをクリックすると、新しい保存フィルタを登録できます。

適用させたい保存フィルタにチェックマークを付け、「適用」ボタンをクリックしてください。

保存フィルタの種類や登録方法など、詳細は **12.6 保存フィルタ**を確認してください。

### 5.4.3. 統計のエクスポート

選択された時間範囲の統計値をカンマ区切り (CSV) ファイルで保存することができます。

時間範囲を指定してグラフを拡大表示している場合は、改めて時間範囲を指定することなく、その拡大表示している時刻範囲の統計値の CSV ファイルを保存することができます。


画面上部の「選択した時間範囲の統計をエクスポート」リンク(下図⑥)をクリックしてください。



下図の「統計のエクスポート」ダイアログが表示されます。

A screenshot of the 'Statistics Export' dialog box. It has a title bar with a red dot and the text '統計のエクスポート'. Below the title bar, there is a section labeled '期間' (Period). Under '期間', there are two date and time pickers. The first picker shows '2017/12/04 11:09:20' and the second shows '2017/12/04 11:13:20'. At the bottom of the dialog, there are two buttons: 'キャンセル' (Cancel) and 'エクスポート' (Export).

画面中央のテキストボックスに統計を取りたい期間の開始時刻と終了時刻を入力してください。

時刻は手入力でも変更できますが、時刻指定のアイコン  をクリックすると、カレンダーと時計が表示され、日時を指定することができます。

「期間」を指定したら「エクスポート」ボタンをクリックしてください。

選択した時間範囲での統計値の CSV ファイルが作成され、下図のダイアログが表示されます。

A screenshot of the 'Statistics Export' dialog box. It has a title bar with a red dot and the text '統計のエクスポート'. Below the title bar, there is a large text area with the text 'ダウンロード可' (Downloadable) in blue. At the bottom right of the dialog, there is a button labeled '閉じる' (Close).

「ダウンロード可」リンクをクリックして、CSV ファイルをダウンロードしてください。

この時作成された CSV ファイルはサーバには保存されません。

再度 CSV ファイルを取得したい場合は、「選択した時間範囲の統計をエクスポート」リンクをクリックして、再度時間範囲を指定してください。

キャプチャレコードを拡大表示しておらず、統計の時間範囲も変更も行わなかった場合は、キャプチャレコード全体の統計値の CSV ファイルが作成されます。

この時作成された CSV ファイルはサーバに保存され、エージェント・ワークスペースのレコード タブの「統計データ」欄の「ダウンロード可」リンクからダウンロードできるようになります。

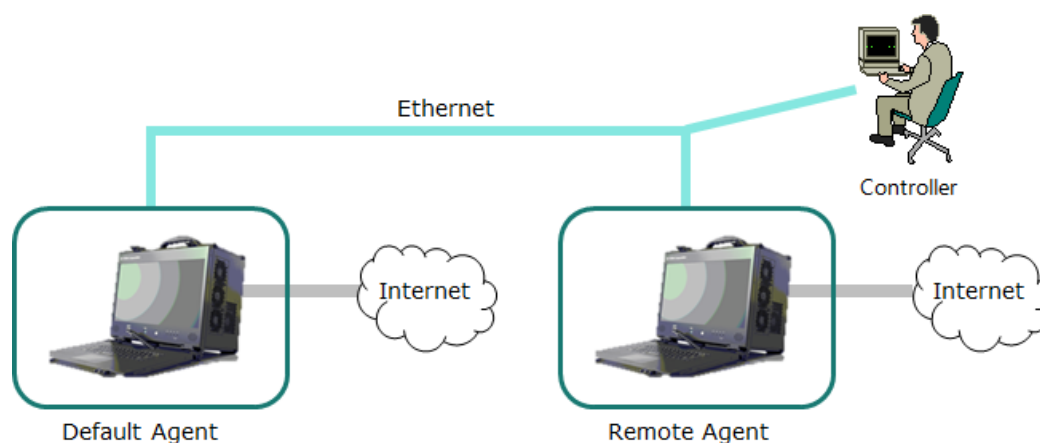
CSV ファイルの内容や形式については **Appendix C 統計値の CSV ファイル**を参照してください。

## 5.5. リモートエージェント

### 5.5.1. 機能の概要

リモートエージェントとは、複数の Synesis を 1 画面の Web ブラウザで操作する機能です。複数の Synesis が Ethernet で接続されている場合に利用可能です。

リモートエージェントはお客様の使用環境に合わせて出荷時に設定されています。追加・変更・削除を行う際は弊社までご連絡ください。



### 5.5.2. 各エージェントの操作方法

リモートエージェントが構成されていると、下図のようにツリービューに複数のエージェントが表示されます。操作するエージェントを切り替える場合は、エージェント名のノードをクリックします。

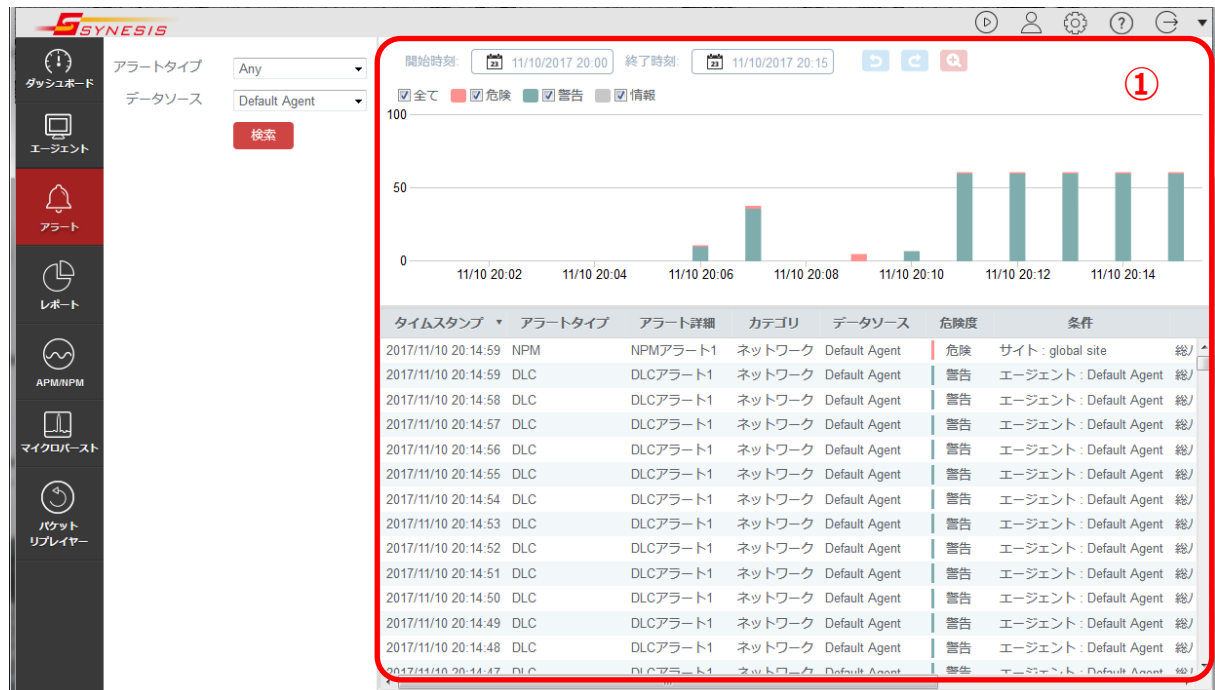
- ① **Default Agent** をクリックすると、ワークスペースで Default Agent の操作ができます。同様に
- ② **Remote Agent** をクリックすると、ワークスペースで Remote Agent の操作ができます。

The screenshot shows the Synesis web interface. On the left is a sidebar with navigation icons: ダッシュボード, エージェント, アラート, レポート, APM/NPM, and マイクロバースト. The main area is divided into two panels. The left panel, labeled 'ツリービュー' (Tree View), shows a list of agents under '全て' (All). The 'Default Agent' is selected with a blue arrow and circled with a red box and the number 1. Below it, the 'Remote Agent' is also selected with a blue arrow and circled with a red box and the number 2. The right panel, labeled 'ワークスペース' (Workspace), shows a table with agent details for the selected 'Default Agent'.

概要	レコード	ロック	トレースファイル	外部データソース
キャプチャの開始	キャプチャの終了	オプション		
名前	Default Agent			
ホスト	SYS-8G2-HPR			
開始時刻	--			
最終アップデート	--			
持続時間	--			
ステータス	停止			
<input type="checkbox"/>	チャンネル	使用率	ビットレート	

## 6.アラート

アラート画面では、キャプチャ済みのパケットを解析して、異常が疑われるデータを検索・閲覧することができます。確認したいアラートタイプと時間範囲を指定して、アラートを検索してください。



検索結果がアラート・ワークスペースに表示されます。ワークスペース画面上部(上図①)にはアラート発生回数のグラフが、その下にはアラートごとの情報が記載されたテーブルが表示されます。

タイムスタンプ	アラートタイプ	アラート詳細	カテゴリ	データソース	危険度	条件	指標	トレースの保存
2017/11/10 20:10:02	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 802 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:10:01	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 797 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:10:00	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 783 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:59	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 792 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:59	NPM	NPMアラート1	ネットワーク	Default Agent	警告	サイト: global site	総/パケット: 83 (100/10/1)	<a href="#">トレースの保存</a>
2017/11/10 20:09:58	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 802 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:57	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 774 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:56	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 784 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:55	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 783 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:54	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/パケット: 783 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:08	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/パケット: 4,188 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:07	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/パケット: 6,678 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:06	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/パケット: 6,513 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:05	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/パケット: 5,932 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:04	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/パケット: 6,470 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:06:59	NPM	NPMアラート1	ネットワーク	Default Agent	危険	サイト: global site	総/パケット: 26,346 (100/10/1)	<a href="#">トレースの保存</a>
2017/11/10 20:06:36	NPM	NPMアラート1	ネットワーク	Default Agent	危険	サイト: global site	総/パケット: 356 (100/10/1)	<a href="#">トレースの保存</a>

グラフやテーブルでデータを確認し、トレースファイルとして保存したいトラフィックが見つかりましたら、テーブルの最後の欄の「トレースの保存」のリンクをクリックしてください。関連するトラフィックをトレースファイルに保存することができます。

この機能は、エージェント・ワークスペースのレコード・タブにある「トレースの保存」ボタンの機能と同じものです。詳細は **5.4.2 トレースの保存** を参照してください。



## 6.1. 検索

アラートを検索します。


検索を実行する前に、あらかじめ各タイプ「DLC」「ARP」「NPM」「APM」のアラートを設定してください。設定された条件に従って、指定された時間範囲のトラフィックデータを検索します。

検索結果が右側のワークスペース画面に表示されます。

### 6.1.1. アラートの設定

アラートはエラーや指定された閾値を超えるトラフィックデータを検知したときに発生します。

アラートを発生させるためには、あらかじめアラートの設定をしてください。

アラートの設定を行う場合は、ツールバーの構成  アイコンをクリックし、メニューの中から「アラート」を選択してください。アラート設定画面が表示されます。

詳細は **12.8 アラート** を参照してください。

### 6.1.2. 検索する時間範囲設定

アラートの閲覧・検索を行う時間範囲を設定してください。

画面上部の「開始時間/終了時間」をクリックすると、下図の「期間」ダイアログが表示されます。

● 期間

30 分

1 時間

8 時間

カスタム

« < November 2017 > »

Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

10:39

« < November 2017 > »

Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

11:09

開始時刻: 11/21/2017 10:39 終了時刻: 11/21/2017 11:09

キャンセル 適用

時間範囲は 30 分、1 時間、8 時間で設定できます。

「カスタム」をクリックすれば任意の開始・終了時間を設定することも可能です。



### 6.1.3. 検索条件の指定

アラートの検出条件として、アラートタイプ「Any」「DLC」「ARP」「NPM」「APM」が指定できます。設定項目は以下の通りです。

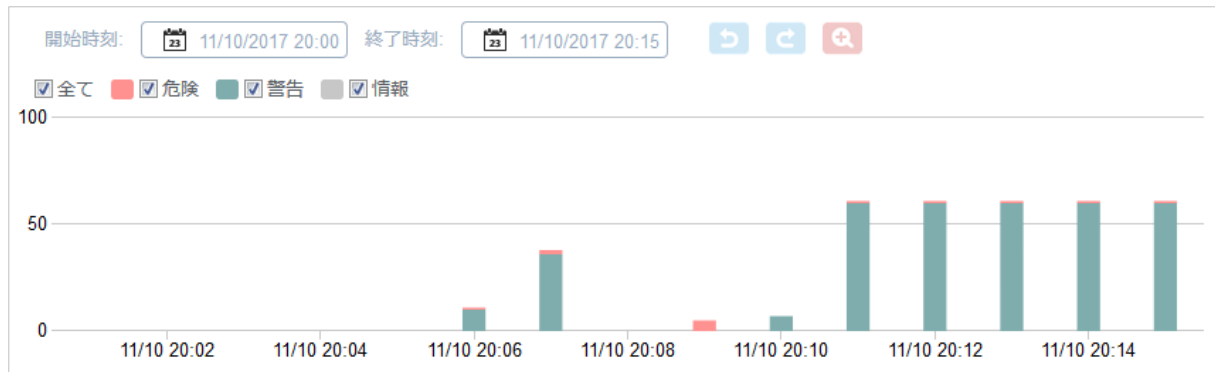
項目	説明
アラートタイプ	検索するアラートタイプを指定します。 Any, DLC, ARP, NPM, APM を選択可能です。 「Any」を指定すると、全てのアラートタイプを検索し、表示します。
サイト	Any (全て)、「構成」で登録した <b>サイト</b> ※、または global site (「構成」で登録していないサイト)が選択可能です。
アプリケーション	デフォルト設定で登録されているアプリケーションプロトコルは下記のとおりです。 BGP, DNS, EXCHANGE, FTP, FTP-DATA, GTP, H.323, HTTP, LDAP, LDP, MEGACO, MGCP, MSSQL, MySQL, NFS, OpenFlow, OpenVPN, ORACLE, PGSQL, POP, RDP, RSYNC, RTSP, sFlow, SIP, SMB, SMTP, SNMP, SSH, T.38, TELNET, YHOO
サーバグループ	Any(全て)、「構成」で登録した <b>サーバグループ</b> ※、または global server group (「構成」で登録していないサーバグループ)が選択可能です。
アプリケーショングループ	Any(全て)、「構成」で登録した <b>アプリケーショングループ</b> ※が選択可能です。
データソース	どのエージェント、またはチャンネルグループをデータソースとするキャブチャレコードでアラートを検索するかを指定します。 <b>D.2 データソース</b> で示される項目に加えて“Any”が選択可能です。ただし、All Channel Group とエージェントごとのチャンネルグループは選択できません。その中から検索に使用するエージェントまたはチャンネルグループを選択可能です。 “Any”を指定して検索した場合、任意のエージェントまたは任意のチャンネルグループについてのアラートが表示されます。合算したデータによるアラートではありません。

※検索を実行する前に、各「項目」で登録を行ってください。詳細は **12.13 サイト**、**12.14 サーバグループ**、**12.15 プロトコル**、**12.16 アプリケーショングループ**を参照してください。

「検索」ボタンをクリックすると、アラート条件に従って検索された結果がワークスペース画面に表示されます。

## 6.2. グラフとアラートリスト

アラート画面上部には時間範囲内で発生したアラートの回数のグラフが表示されます。



グラフの上の危険度のラベル ■ 危険 ■ 警告 ■ 情報 にチェックを入れることで、危険度ごとに表示/非表示を切り替えることができます。

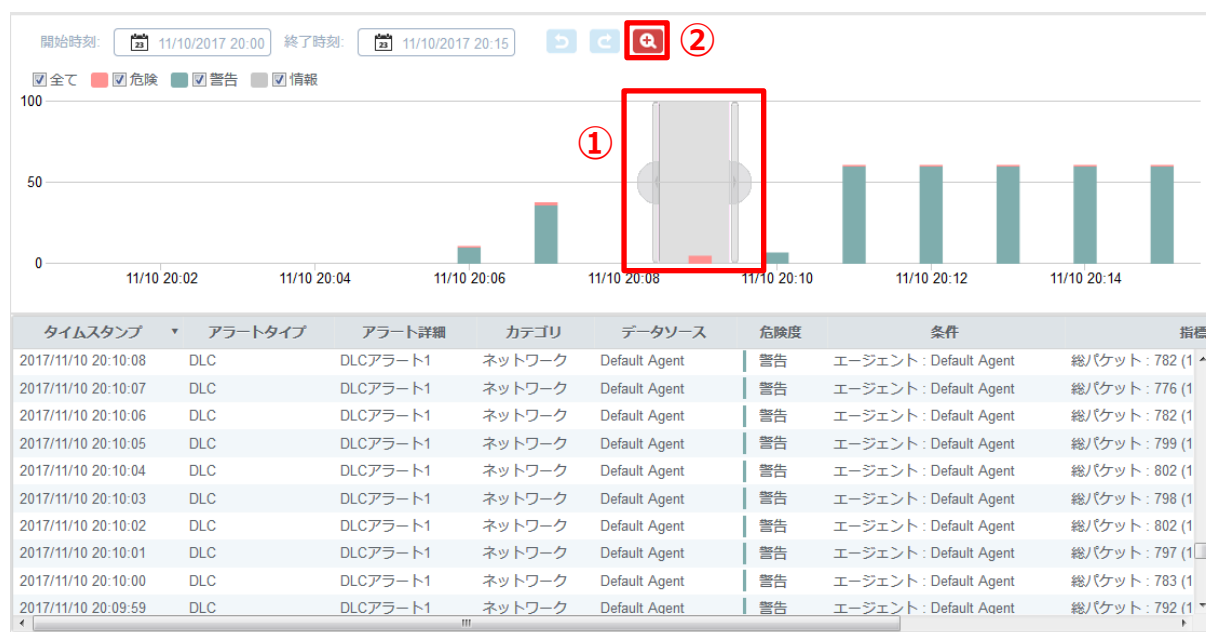
タイムスタンプ	アラートタイプ	アラート詳細	カテゴリ	データソース	危険度	条件	指標	トレースの保存
2017/11/10 20:10:02	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 802 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:10:01	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 797 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:10:00	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 783 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:59	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 792 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:59	NPM	NPMアラート1	ネットワーク	Default Agent	警告	サイト: global site	総/バケット: 83 (100/10/1)	<a href="#">トレースの保存</a>
2017/11/10 20:09:58	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 802 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:57	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 774 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:56	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 784 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:55	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 783 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:54	DLC	DLCアラート1	ネットワーク	Default Agent	警告	エージェント: Default Agent	総/バケット: 783 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:09:08	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/バケット: 4,188 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:07	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/バケット: 6,678 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:06	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/バケット: 6,513 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:05	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/バケット: 5,932 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:08:04	DLC	DLCアラート1	ネットワーク	Default Agent	危険	エージェント: Default Agent	総/バケット: 6,470 (1,000/100/10)	<a href="#">トレースの保存</a>
2017/11/10 20:06:59	NPM	NPMアラート1	ネットワーク	Default Agent	危険	サイト: global site	総/バケット: 26,346 (100/10/1)	<a href="#">トレースの保存</a>
2017/11/10 20:06:36	NPM	NPMアラート1	ネットワーク	Default Agent	危険	サイト: global site	総/バケット: 356 (100/10/1)	<a href="#">トレースの保存</a>


確認できる項目は以下の通りです。

項目	説明
タイムスタンプ	アラート発生時刻です。年月日と時間(hh:mm:ss)が表示されます。
アラートタイプ	検索されたアラートのアラートタイプです。
アラート詳細	構成メニューのアラートの設定で登録されている登録名です。
カテゴリ	検索対象となるデータのカテゴリです。 ここでは「ネットワーク」と表示されます。
データソース	検索時に指定されたデータソースです。
危険度	検出されたアラートの危険度です。 「危険」「警告」「情報」の3種類に分類されます。
条件	NPM/APM で設定したサイトやアプリケーションなどの検索条件です。 DLC、ARP はデータソースが表示されます。
指標	アラートの設定で登録されている指標と閾値です。
トレースの保存	「トレースの保存」リンクをクリックすると、アラートが発生した期間のデータをトレースファイルとして保存できます。 詳細は <a href="#">5.4.2 トレースの保存</a> を参照してください。

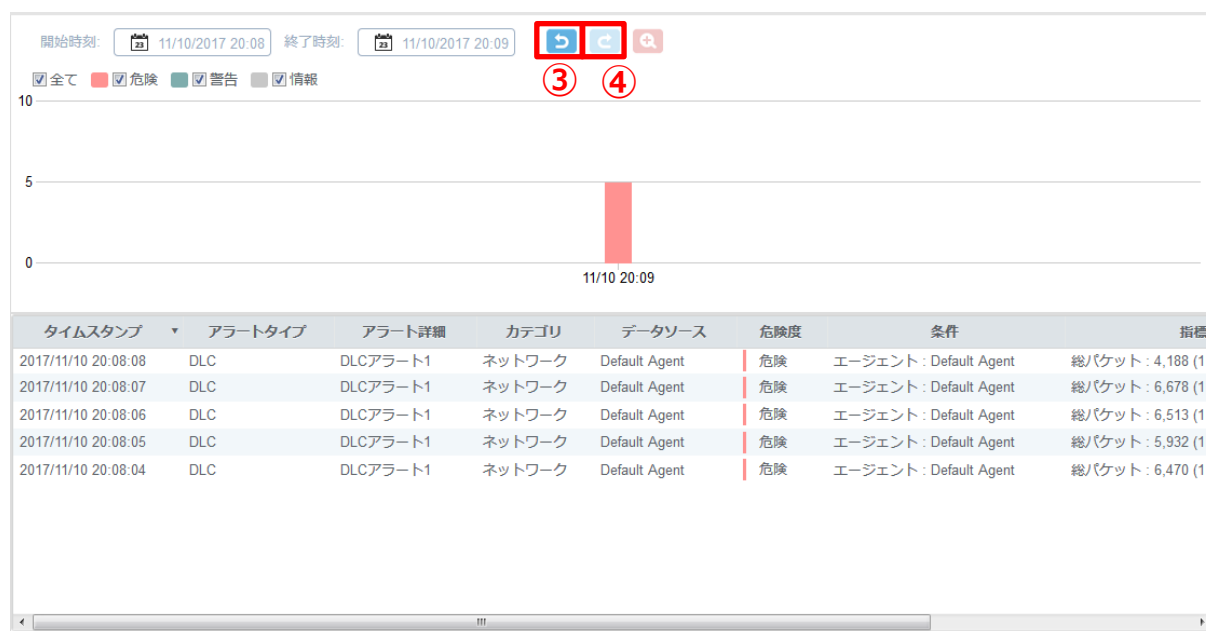
### 6.2.1. 指定範囲の拡大表示

アラートグラフで表示させる時間範囲を絞り込んで、拡大して表示させることができます。





アラートグラフの拡大させたい部分をマウスドラッグで指定し(上図①)、時刻表示の右横に並んだ「拡大」アイコン(上図②)をクリックしてください。

グラフが選択した時間範囲で拡大表示されます(下図)。

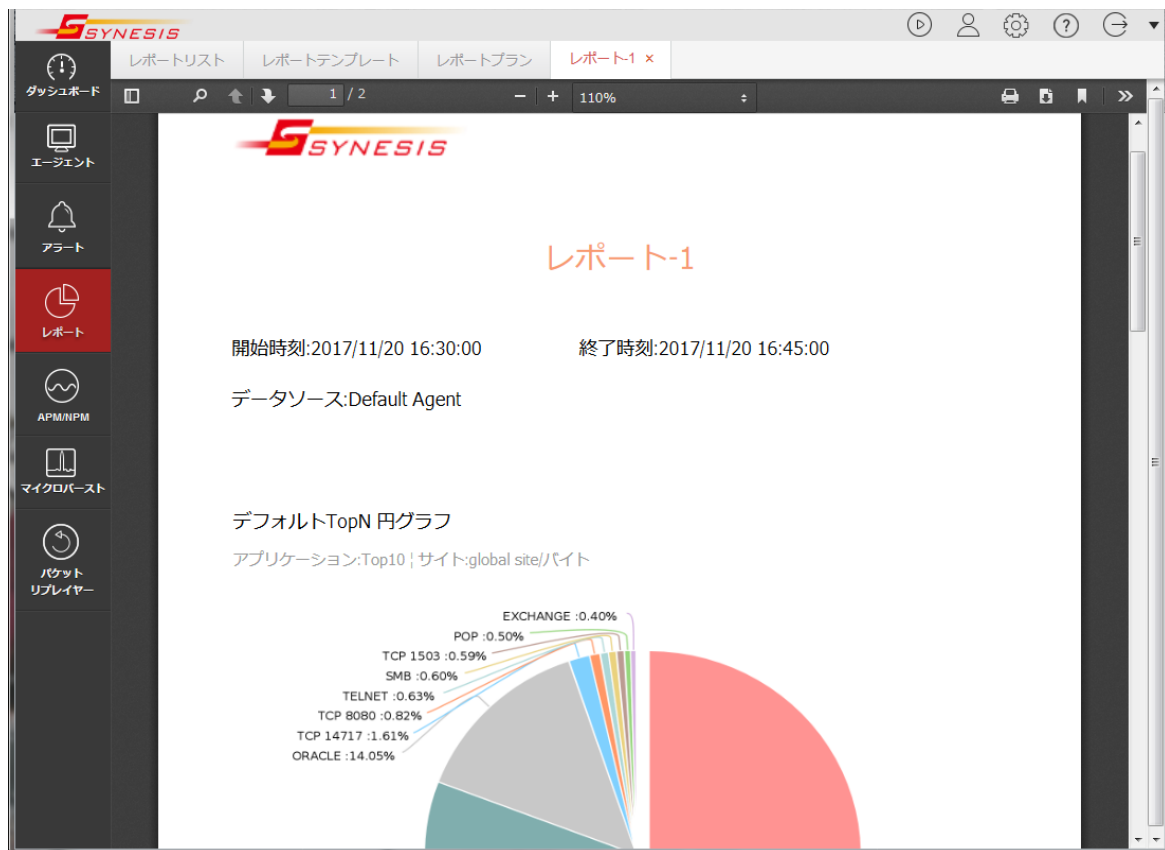


このとき、テーブルに表示される検知されたアラートのリストも、指定した時間範囲のデータのみに更新されます。

ナビゲーションバーの「元に戻す」アイコン (上図③)をクリックすると、直前に行った拡大処理が取り消され、「やり直す」アイコン (上図④)をクリックすると、直前に行った「元に戻す」処理がキャンセルされます。

## 7. レポート

レポート画面ではキャプチャデータを元に、解析結果をまとめたレポートを作成することができます。



レポートを作成するには、まず、記載したいグラフや表などを配置してレポートの書式を設定した「レポートテンプレート」を作成し、「レポートプラン」でデータ解析する時間範囲を指定します。書式が「レポートテンプレート」で保存されていますので、同じ形式のレポートを簡単に繰り返し作成することができます。定期的にレポートを作成することも可能です。

レポート作成の主な流れは以下の通りです。

### (ア) 「レポートテンプレート」の作成・編集

レポートに記載するグラフや表を選択して、解析するデータの種類などを指定します。

詳細は **7.2 レポートテンプレート**を確認してください。

### (イ) 「レポートプラン」の作成・編集

作成済みのレポートテンプレートの中から希望の書式のテンプレートを選択し、データ解析時間範囲を指定してレポートを作成します。定期的にレポートを作成させることも可能です。

詳細は **7.3 レポートプラン**を参照してください。

### (ウ) 「レポートリスト」に保存

生成されたレポートは新規タブで表示されると同時に、自動的に保存され、「レポートリスト」画面のリストに追加されます。

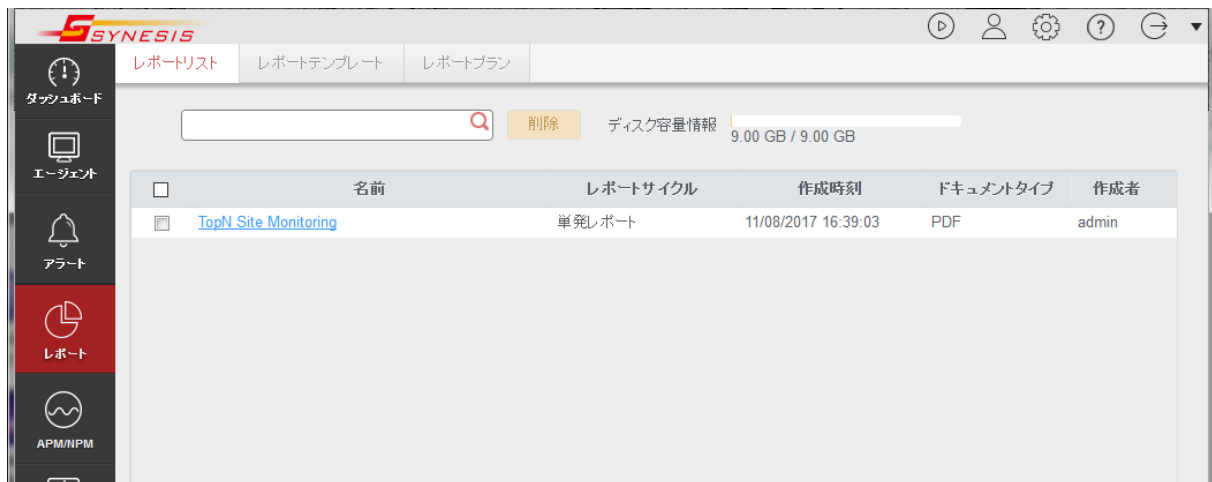
詳細は次頁、**7.1 レポートリスト**を参照してください。

実際に作成できるレポートのサンプルを **7.4 レポートの形式**で紹介します。

## 7.1. レポートリスト

レポートリスト画面では、Synesis 内に保存されているレポートが一覧で確認できます。

レポートの検索・閲覧・削除が可能です。



確認できる情報は以下の通りです。

項目	説明
名前	保存されているレポートの名前です。
レポートサイクル	「単発レポート」か「周期レポート」を表示します。
作成時間	レポートが作成された時間です。
ドキュメントタイプ	保存されているレポートのドキュメントタイプです。
作成者	保存されているレポートの作成者です。

### 7.1.1. 検索

保存されているレポート数が多い場合は、検索フィールドにマッチする文字列を入力し、レポートを検索します。🔍 アイコンをクリックすると検索結果が表示されます。

### 7.1.2. 削除

レポートを削除したい場合は、削除したいレポートの左側のチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。チェックマークを付けたレポートが削除されます。

すべてのレポートを削除したい場合には、「名前」の左側のチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。全てのレポートが一括で削除されます。

### 7.1.3. レポートの保存場所

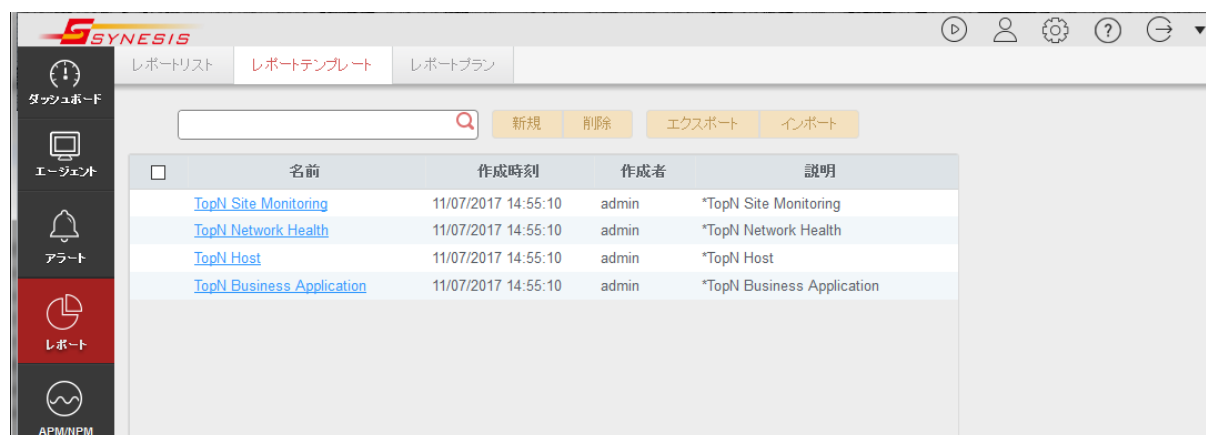
生成されたレポートは下記のフォルダに保存されます。

/pvc/data/databank/generated\_report/

なお、このフォルダは **Appendix F Synesis のディスク構成** の「**F.4 データバンク領域**」になります。

## 7.2. レポートテンプレート

レポートテンプレート画面では、レポートに記載したいグラフや表を配置したレポートのテンプレートを作成・管理します。



作成したレポートテンプレートは一覧表で表示されます。確認できる情報は「名前」「作成時刻」「作成者」「説明」です。

### 7.2.1. 検索

作成したレポートテンプレート数が多い場合は、検索フィールドに文字列を入力して検索を行うことができます。🔍 アイコンをクリックすると結果が表示されます。

### 7.2.2. 新規

「新規」ボタンをクリックすると下図の「新規テンプレート」画面が表示されます。

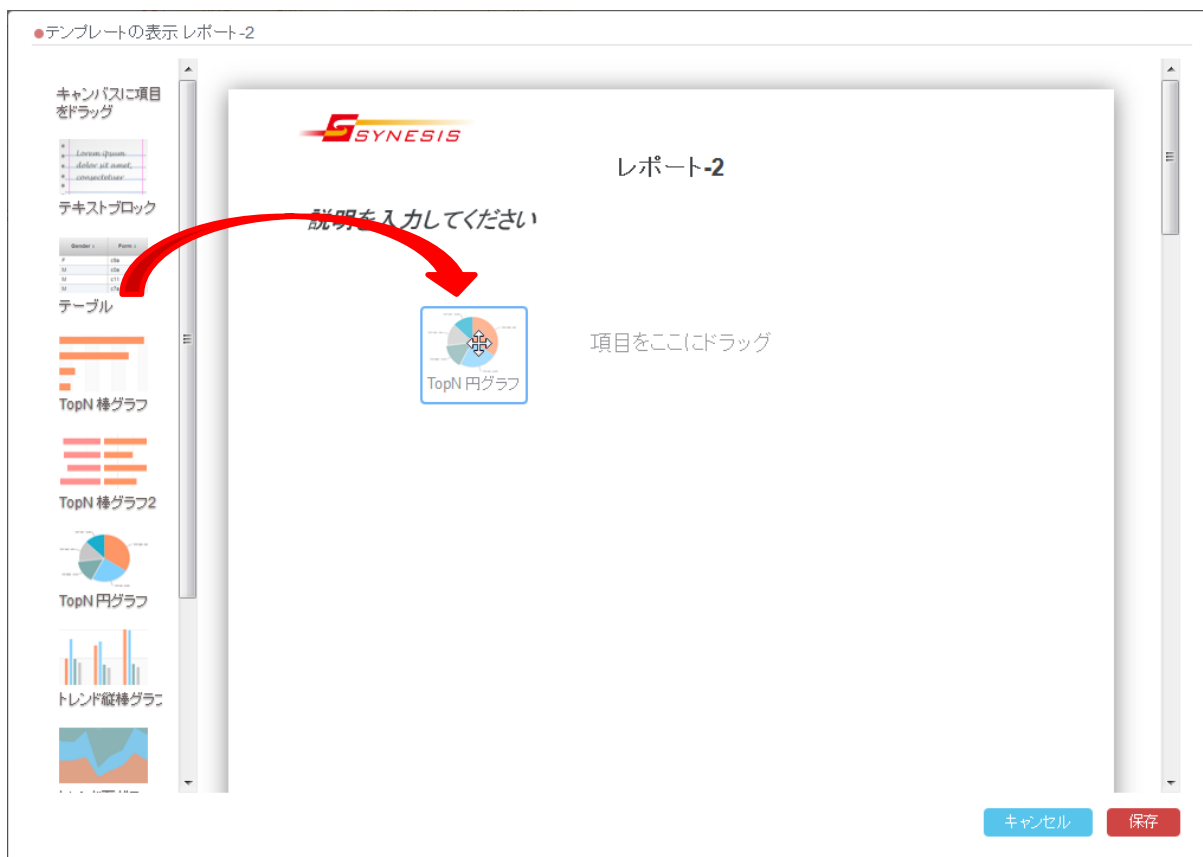


画面左のグラフペインからレポートの空白部分にグラフをドラッグして配置してください。

「保存」ボタンをクリックすると、作成したテンプレートが保存され、リストに追加されます。ロゴ下のテキスト(図①)をクリックすると、レポートテンプレート名を変更できます。テンプレート名下の「インプットの説明」(上図②)をクリックすると、テンプレートの説明を変更できます。

### 7.2.2.1 記載するグラフの選択・配置と設定

左側のペインにはレポートの要素が表示されています。配置したい表やグラフにカーソルを合わせ、右側のキャンバスへドラッグ＆ドロップしてください。



グラフの設定ダイアログが表示され、データの解析方法やグラフに表示する系列などを設定できます。

構成トレンド折れ線グラフ

タイトル \* デフォルトトレンド折れ線グラフ

説明 説明を入力してください

アドオン \* APM

タイプ \* サイト

範囲 \* アプリケーション

インデックス \*

バイト	>> <<	バケット
NRT(ms)		
SRT(ms)		
ART(ms)		
PTT(ms)		
CRT(ms)		
遅延時間(ms)		

上限を固定する ☒

KPIの上限 100 K

キャンセル 保存



保存ボタンをクリックすると、レポートのキャンバスにグラフが追加されます。

追加後も、キャンバス上のグラフをクリックすればグラフの設定を変更できます。

選択できるレポートの要素は以下の通りです。

項目	カテゴリ
テキストブロック	—
テーブル	APM, NPM
TopN 棒グラフ	APM, NPM
TopN 棒グラフ 2	APM, NPM
TopN 円グラフ	APM, NPM
トレンド縦棒グラフ	APM, NPM, DLC
トレンド面グラフ	APM, NPM, DLC
トレンド折れ線グラフ	APM, NPM, DLC
トップトレンド折れ線グラフ	APM, NPM


主な設定項目は以下の通りです。（選択したグラフの種類によって設定項目は変わります）

項目	説明
タイトル	レポートの要素のタイトル文字列です。
説明	レポートの要素の説明です。
アドオン	レポートの要素追加時に選択したカテゴリです。
タイプ	グラフに表示するデータタイプです。ドロップダウンリストから選択します。
範囲	タイプで設定するデータタイプのサブカテゴリになります。
インデックス	グラフに表示する系列です。1 つ以上のインデックスを選択して、左側から右側へ  アイコンで移動します。右側にリストされたインデックスがグラフに適用されます。右側のリストから削除する場合は、1 つ以上のインデックスを選択して  アイコンで移動します。
上限を固定する	トレンド系のグラフでは、プロットされた KPI 指標の上限を定義することができます。実際のプロット指標値が上限値を超えた場合、プロット値がユーザ定義の上限値になります。（実際の値を表示するにはプロットの上にマウスポインタを置いてください）
KPI の上限	「上限を固定する」が有効の場合に表示されます。 テキストボックス右側のドロップダウンリストで、単位（K、M、G、u、m など）を変更できます。グラフの単位ラベルも変更されます。 入力できる最大値は 1,000,000,000（総サイズ）までです。

配置後もレポートの要素をクリックすると、設定を編集できます。



#### 7.2.2.2 レポートロゴの変更

レポートのロゴは変更可能です。レポート画面左上に表示されているロゴ  をクリックしてください。下図のロゴ設定ダイアログが表示されます。



「参照」ボタンをクリックして、ロゴの画像ファイルを選択してください。「アップロード」ボタンをクリックすると画面中央に選んだロゴが表示されますので、間違いがないか確認してください。

「適用」ボタンをクリックすると、レポートテンプレートのロゴが変更されます。

「デフォルト」チェックボックスにチェックを入れると、今後作成するレポートのロゴが選択したロゴになります。指定するロゴのサイズは 50 x 200 ピクセル以下にしてください。

#### 7.2.3. 削除

不要になったレポートテンプレートを削除する際は、削除したいレポートの左側のチェックボックスにチェックを入れます。すべてのレポートを選択する場合は「名前」の左側のチェックボックスにチェックを入れます。「削除」ボタンをクリックすると確認ダイアログが表示され、「はい」を選択してレポートテンプレートを削除します。

チェックボックスが表示されていないテンプレートはデフォルトテンプレートで削除できません。

また、レポートプランで使用されているレポートテンプレートも削除できません。使用中のテンプレートを削除したい場合は、そのテンプレートを使用しているレポートプランを全て削除してください。

#### 7.2.4. エクスポート

作成したレポートテンプレートを任意のローカルフォルダに書き出し、それを他の Synesis で利用することが可能です。

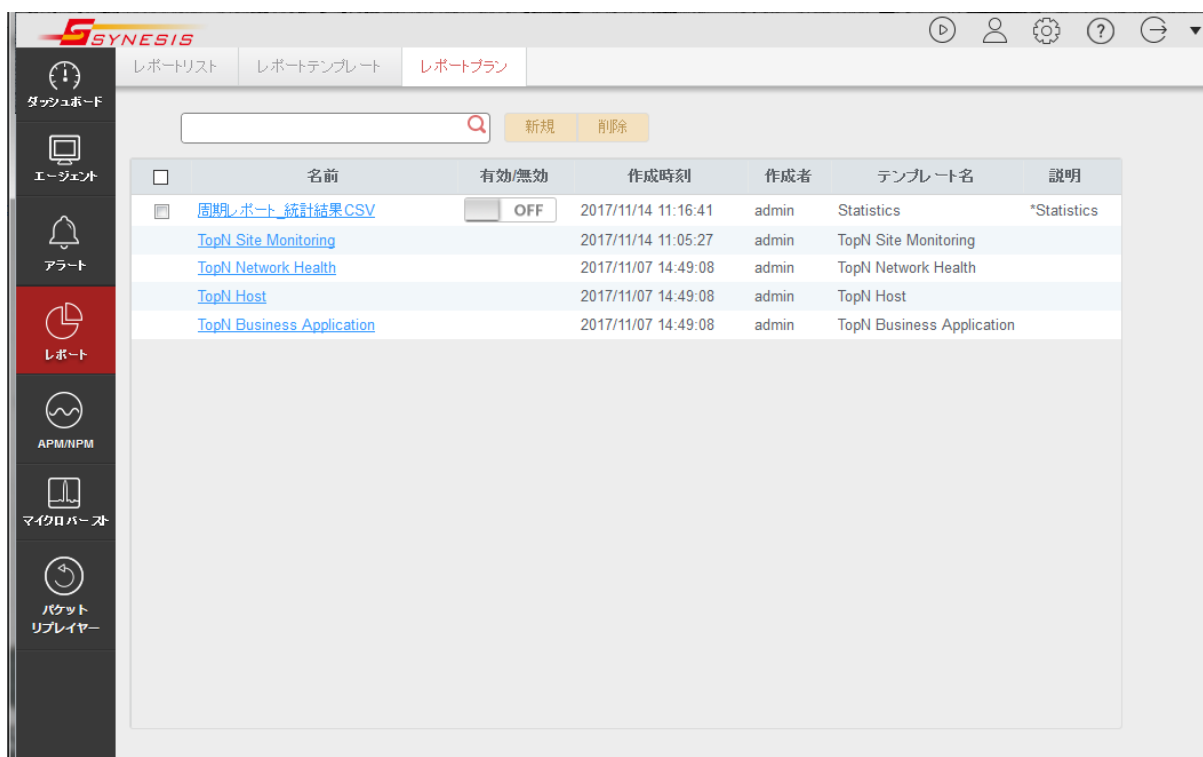
エクスポートしたいレポートテンプレートにチェックを入れ、「エクスポート」ボタンをクリックしてください。エクスポートダイアログが表示されるので、ファイル名を入力してください。「エクスポート」をクリックすると、レポートテンプレートファイルがローカルにダウンロードされます。

#### 7.2.5. インポート

ローカルに存在するレポートテンプレートを読み込むことができます。「インポート」ボタンをクリックし、ローカルフォルダのレポートテンプレートを指定してください。「アップロード」ボタンをクリックすると、レポートテンプレートリストにファイルがインポートされます。

## 7.3. レポートプラン

このタブでは作成済みのレポートテンプレートの中から希望の書式のテンプレートを選択し、データ解析時間範囲などを指定してレポートを作成します。



レポート作成のために指定したデータ解析時間範囲などの設定は、「レポートプラン」として保存されます。作成された「レポートプラン」は一覧表で表示され、確認できます。

レポートプランには「単発レポート」と「周期レポート」の2種類があります。

### 単発レポート

取得済みのキャプチャレコードの日時で時間範囲を指定して、単発のレポートを作成します。



レポートプランを作成・編集し、保存する際にレポートが作成されます。

### 周期レポート

時間範囲を「日」「週」「月」「年」で指定して、周期的にレポートを作成させることが可能です。

周期レポートプランは「有効/無効」欄にステータスを表す ON/OFF スイッチが表示されています。


周期レポートの自動作成を実行させておきたい場合は、スイッチを「ON」にしてください。

- ・  OFF : 無効状態。クリックすると有効になります。
- ・  ON : 有効状態。クリックすると無効になります。

スイッチを「OFF」にしておくと、作成したプランを消さなくてもレポートは自動作成されません。

#### 7.3.1. 検索

レポートプラン数が多い場合は、検索フィールドに文字列を入力して、検索を行うことができます。

 アイコンをクリックすると検索結果が表示されます。

### 7.3.2. 新規

新しいレポートプランを作成したい場合は、「新規」ボタンをクリックしてください。

下図の「新規プランの作成」ダイアログが表示されます。

●新規プランの作成

レポートテンプレート \* レポート-2

レポートタイトル \* レポート-2

プラン名 \* 新規プランの作成\_2017/11/14 11:43:21

説明 情報を入力してください。

ドキュメントタイプ \* PDF

データソース \* Default Agent

レポートサイクル \* ☒ 単発レポート ☐ 周期レポート

開始時刻 \* 2017/11/13 11:43:21 終了時刻 \* 2017/11/14 11:43:21

集計間隔 \* 自動

レポート要素の設定

デフォルトトレンド折れ線グラフ

サイト \* sample アプリケーション \* ORACLE

デフォルトTopN円グラフ

TopN \* Top10

キャンセル 保存

「レポートテンプレート」を選択し、作成するレポートの形式を指定します。作成したいレポートのテンプレートがない場合は、先にレポートテンプレートを作成してください。

詳細は **7.2 レポートテンプレート** を参照してください。

必要な項目を設定し、「保存」ボタンをクリックすると、レポートプランが保存されます。

「レポートサイクル」で「単発レポート」を選択していた場合は、「保存」ボタンをクリックした際に、1度だけレポートが作成されます。

なお、文書形式のレポートだけでなく、バイトやパケット数などの統計情報を “,(カンマ)” 区切りの CSV ファイルで出力させることも可能です。統計情報を CSV で出力させたい場合は、レポートテンプレートの項目で「Statistics」を指定してください。

この CSV ファイルを作成する際に選択できるのは「周期レポート」のみです。1度だけ統計情報の CSV ファイルを作成したい場合は、エージェント・ワークスペースのレコード・タブで「統計のエクスポート」をクリックし、統計情報の CSV ファイルを作成してください。

作成できる CSV ファイルの内容や形式については **Appendix C 統計値の CSV ファイル** を参照してください。

設定項目は以下の通りです。

項目	説明
レポートテンプレート	使用するレポートテンプレートを選択します。統計結果を CSV ファイルで出力したい場合は、「Statistics」を選択してください。
レポートタイトル	レポートのタイトルを設定します。
プラン名	作成する新規プランのタイトルを設定します。
説明	レポートプランリストの「説明」欄に表示される説明文を設定します。
ドキュメントタイプ	PDF, Word, Excel, RTF が選択可能です。 「レポートテンプレート」の項目で「Statistics」が選択された場合は、CSV ファイルになります。
データソース	レポートに記載するデータのデータソースを選択します。 選択可能な項目は Synesis の設定により異なります。詳細は <b>D.2 データソース</b> を参照してください。
レポートサイクル	単発レポートもしくは周期レポートを選択可能です。 単発レポートの場合は「開始時刻」と「終了時刻」を、周期レポートの場合は「周期タイプ」を設定します。詳細は次頁を参照してください。
集計間隔	集計間隔を設定します。単発レポートと周期レポートで選択範囲が異なります。詳細は次頁を参照してください。
レポート要素の設定	テーブルやグラフ要素のより詳細なコンフィグを設定します

### 7.3.2.1 単発レポートの設定

「レポートサイクル」の項目で「単発レポート」を選択した場合は、「開始時刻」と「終了時刻」、もしくは「集計間隔」でデータの時間範囲を指定します。

レポートサイクル \*

☒ 単発レポート
☐ 周期レポート

開始時刻 \*

2017/11/13 11:43:21

終了時刻 \*

2017/11/14 11:43:21

集計間隔 \*

自動

設定項目の詳細は以下の通りです。

項目	説明
開始時刻	レポートに記載するデータの時間範囲の開始時刻です。 年月日と時刻(hh:mm:ss)で指定します。
終了時刻	レポートに記載するデータの時間範囲の終了時刻です。 年月日と時刻(hh:mm:ss)で指定します。
集計間隔	集計間隔を指定します。以下の内から選択してください。 5 分、30 分、1 時間、2 時間、8 時間、1 日、1 週間、1 ヶ月 指定した開始時刻と終了時刻の範囲内で、指定した集計間隔ごとの値が取られ、集計されたレポートが出力されます。 自動の場合は、自動的にマッチした集計間隔が選択されます。

### 7.3.2.2 周期レポートの設定

「レポートサイクル」で「周期レポート」を選択した場合は「周期タイプ」を指定します。



レポートサイクル*	<input type="radio"/> 単発レポート	<input checked="" type="radio"/> 周期レポート
周期タイプ*	<div>日</div>	通知先
		<div>通知なし</div>
		<input type="checkbox"/> 有効
設定した通知グループに含まれるメールアドレスにのみ通知します。		

設定項目の詳細は以下の通りです。

項目	説明
周期タイプ	それぞれ下記に示すスケジュールに従ってレポートを生成します。 1) 「日」：毎日午前 2:00 2) 「週」：毎週日曜日の午前 2:00 3) 「月」：毎月 1 日の午前 2:00 4) 「年」：毎年 1 月 1 日の午前 2:00
集計間隔	集計間隔が設定できます。 周期タイプ【日】：5 分、30 分、1 時間 周期タイプ【週】：30 分、1 時間、1 日 周期タイプ【月】：2 時間、8 時間、1 日 周期タイプ【年】：1 日、1 週間、1 ヶ月
通知先	通知先として「通知グループ」が指定できます。

「通知」のチェックボックスにチェックを入れると、「通知先」の項目が有効になります。

通知先として「通知グループ」を指定しておくと、周期レポートが自動作成された際に、指定された「通知グループ」に含まれるメールアドレス宛に通知されます。Trap と Syslog には通知されません。「通知グループ」の設定方法など詳細は **12.10 通知グループ** を参照してください。

周期レポートの「レポートプラン」を新規作成すると、デフォルトでステータスが「有効」になっています。周期レポートの作成を止めたい場合は、レポートプランリストの「有効/無効」欄の ON アイコン  をクリックし、 に切り替えてください。

### 7.3.3. 削除

レポートプランを削除したい場合は、左側のチェックボックスにチェックを入れて「削除」ボタンをクリックしてください。選択したレポートが削除されます。

全てのレポートプランを削除したい場合はヘッダの「名前」の左側にあるチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。

### 7.3.4. レポートプランの編集

作成された「レポートプラン」の設定を編集したい場合は、編集したい「レポートプラン」の「名前」リンクをクリックしてください。

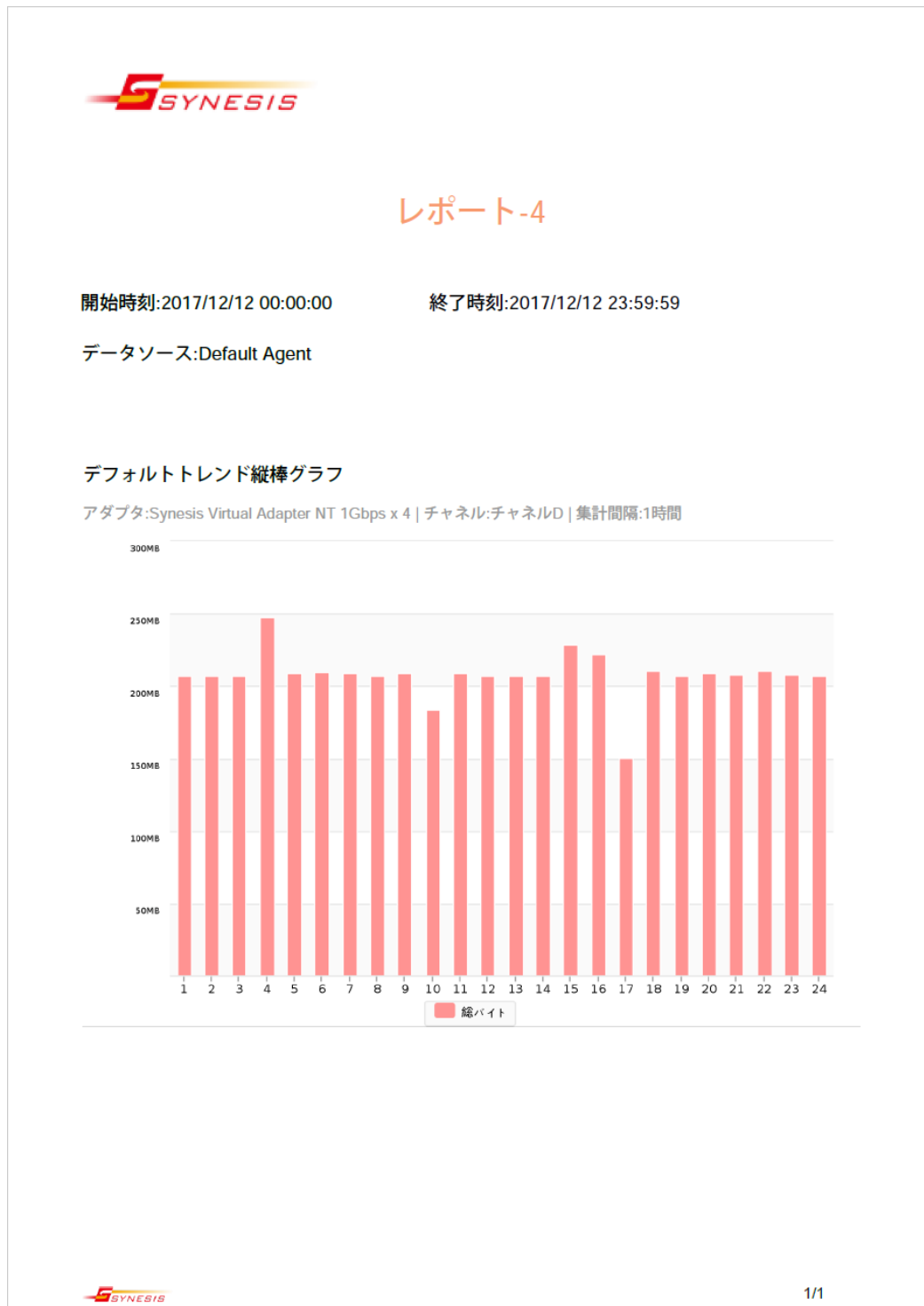
「プランの表示」ダイアログが表示されます。「レポートテンプレート」以外の項目が変更可能です。

## 7.4. レポートの形式

作成されたレポート例を元に、具体的なレポートの形式を説明します。

個々のグラフや表の追加方法は **7.2 レポートテンプレート** を参照してください。

### [レポート例]



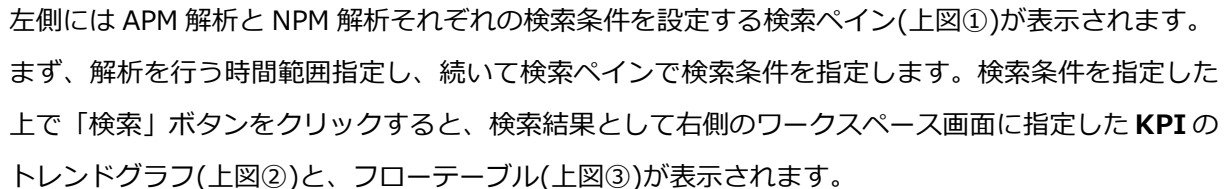
キャプチャデータの開始時刻と終了時刻が yyyy/mm/dd hh:mm:ss の形式で表示されます。

キャプチャデータのデータソースが表示されます。

各グラフや表には、その種類とアダプタ(キャプチャカード)、チャンネル、集計時間が表示されます。

集計間隔 1 時間のグラフでは、09:00:00~09:59:59 のデータが 10:00 の位置にプロットされます。

APM/NPM 解析ではキャプチャレコードの統計値を送信先や送信元、またはアプリケーションプロトコルなどで分類し、個別に表示させることで、通信の問題箇所を探し出していくことができます。




APM 解析と NPM 解析の解析方法の違いは下記の通りです。

通信の応答時間を解析して、遅延や不具合の発生している通信を特定することができます。

各通信のデータ量を送信側と受信側で個別に表示することで、ネットワークの状態を確認することができます。

77 / 185

## 8.1. 解析する時間範囲の指定

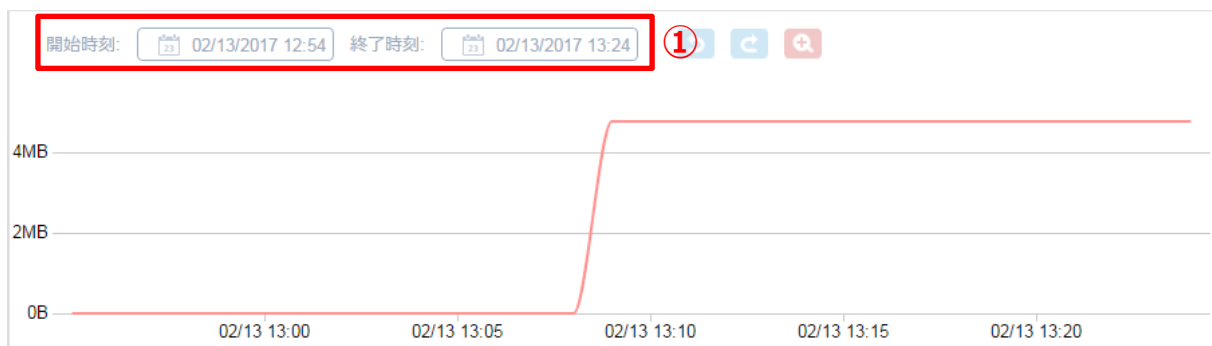
エージェント・ワークスペースのレコードタブ(5.3.2レコードタブ参照)のキャプチャレコード一覧から、解析したいキャプチャレコードを選択し、 APM/NMP 解析リンクアイコンをクリックしてください。

解析範囲として選択したキャプチャレコードの開始時刻・終了時刻が設定された状態で「APM/NMP 解析」画面へ移動できます。

移動後、データを確認して、解析範囲の絞込みやトレースファイルの保存を行ってください。

長期間のトラフィックをまとめて検索したい場合は、解析範囲を手動で指定して、複数のキャプチャレコードを同時に解析することも可能です。

手動で設定したい場合は予め解析したい期間を確認した上で、画面上部の「開始時刻」や「終了時刻」(下図①)の部分をクリックしてください。



下図の「期間」ダイアログが表示されます。

● 期間

30分  
1時間  
8時間  
カスタム

②

開始時刻: 12/08/2017 11:17 終了時刻: 12/08/2017 11:47

キャンセル 適用

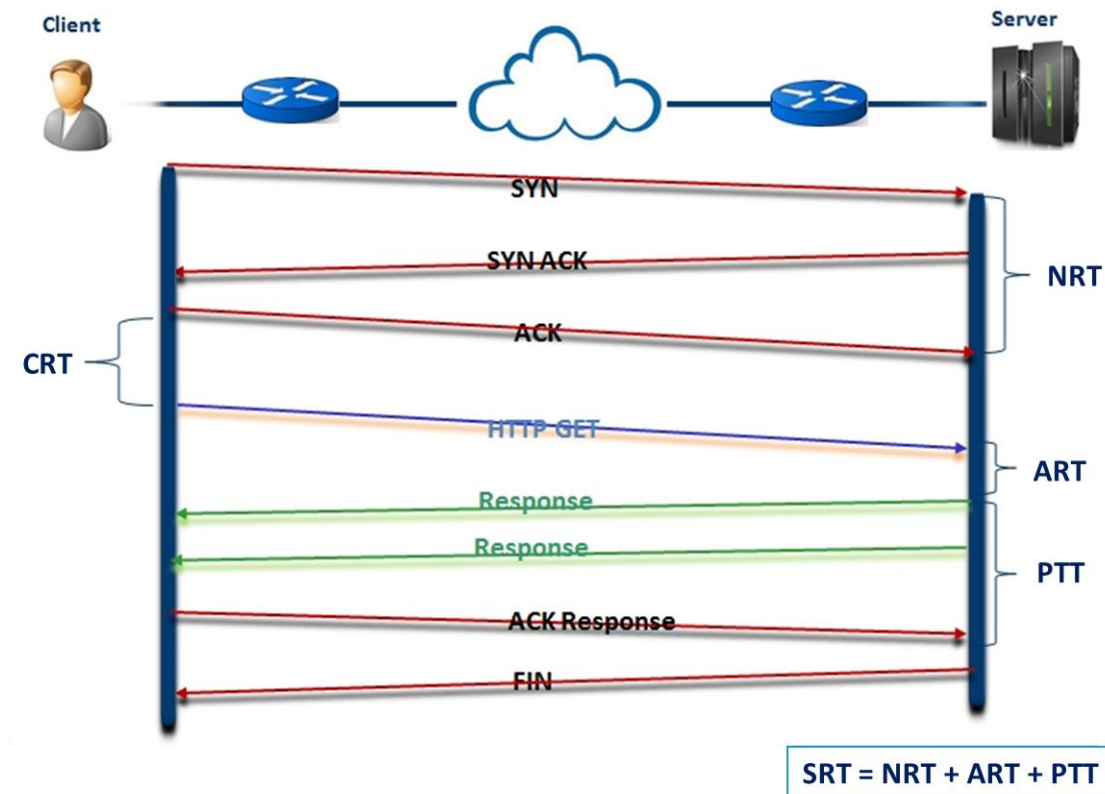
ダイアログボックス左側(上図②)で統計情報を表示する時間の範囲を選択できます。デフォルトでは30分、1時間、8時間から選択できます。「カスタム」を選択して、表示する範囲をカレンダーで指定することもできます。



## 8.2. APM 解析

1つの通信の受信側(クライアント)と送信側(サーバ)間の応答の各段階で要している時間を詳細に解析し、遅延の原因となっている箇所や不具合の発生している通信を特定します。

受信側(クライアント)と送信側の(サーバ)間の通信シーケンスは下図の通りです。



上図のシーケンス図の中で、以下の項目が KPI として確認できます。

項目	詳細
ART	サーバアプリケーションがクライアントリクエストに応答するのにかかる時間です。[応答パケットのタイムスタンプ] - [リクエストパケットのタイムスタンプ] で計算されます。
CRT	クライアントがリクエストを開始するまでにかかる時間です。 ACK とクライアントリクエストのタイムスタンプの差により計算されます。
NRT	ネットワークをパケットが往復するのにかかる平均時間です。ACK と SYN のタイムスタンプの差により計算されます。
PTT	サーバがクライアントリクエストへのレスポンスを送るのに要した平均時間です。 [ACK 応答のタイムスタンプ] - [サーバのレスポンスのパケットのタイムスタンプ] で計算されます。
SRT	サーバがクライアントリクエストに応答し、レスポンスを完了させるのに要した時間です。ART + NRT + PTT で計算されます。

各項目の正式名称は **Appendix A 用語集** を参照してください。

### 8.2.1. APM 解析での検索

「項目」と「KPI」を選択して、「検索」ボタンをクリックしてください。

NPM解析		APM解析		
データソース	Default Agent ▼			
項目	アプリケーション ▼			
KPI	総バイト ▼			
範囲	全て ▼			
<div>検索</div>				

設定項目の詳細は以下の通りです。

項目	説明
データソース	解析するキャプチャレコードのデータソースを選択します。 選択可能な項目は Synesis の設定により異なります。詳細は <b>D.2 データソース</b> を参照してください。
項目	指定された項目での KPI の TopN がトレンドグラフとフローテーブルに表示されます。指定可能な項目は以下の通りです。 <b>サイト</b> <sup>※</sup> ：IP アドレスをサブネットごとにグループ化したものです。 サーバ：単体の IP アドレスです。 <b>サーバ グループ</b> <sup>※</sup> ：登録されたサーバをグループ化したものです。 アプリケーション： <b>12.15 プロトコル</b> で登録されたアプリケーションプロトコルのポート番号です。 <b>アプリケーショングループ</b> <sup>※</sup> ：登録されたアプリケーション(プロトコル)をグループ化したものです。
KPI	選択された KPI の TopN がトレンドグラフとフローテーブルに表示されます。トレンドグラフは TopN の合計値が表示されます。 フローテーブルに表示される各指標が選択可能です。 詳細は <b>8.2.2 APM 解析のフローテーブル</b> を参照してください。
範囲	「項目」で「サイト」を選択すると、選択項目として <b>12.15 プロトコル</b> で登録した「アプリケーション(プロトコル) <sup>※</sup> 」のリストが表示されます 「項目」で「サイト」以外を選択した際に、選択項目として <b>12.13 サイト</b> で登録した <b>サイト</b> <sup>※</sup> のリストが表示されます。

※検索を実行する前に、各「項目」で登録を行ってください。詳細は **12.13 サイト**、**12.14 サーバグループ**、**12.15 プロトコル**、**12.16 アプリケーショングループ** を参照してください。

## 8.2.2. APM 解析のフローテーブル

検索の結果、指定された項目での KPI の TopN がトレンドグラフとフローテーブルに表示されます。

送信元アドレス	送信元ポート	送信先アドレス	送信先ポート	総バイト	総パケット	NRT	SRT	ART	PTT	CRT	遅延	リトライ	トレースファイル
10.2.0.1	1051	10.2.0.2	1066	1,462	22	2.30 ms	2.30 ms	0.00 ms	0.00 ms	4.04 ms	1.15 ms	6	<a href="#">トレースの保存</a>
10.2.0.1	1051	10.2.0.2	1066	1,462	22	2.30 ms	2.30 ms	0.00 ms	0.00 ms	4.04 ms	1.15 ms	6	<a href="#">トレースの保存</a>

フローテーブルに表示される情報は以下の通りです。

項目	説明
送信元アドレス	クライアントのアドレスです。
送信元ポート	クライアントのポートです。
送信先アドレス	サーバのアドレスです。
送信先ポート	サーバのポートです。
総バイト	送信元 IP と送信先 IP の間で送受信されるバイト数です。
総パケット	送信元 IP と送信先 IP の間で送受信されるパケット数です。
NRT	ネットワークをパケットが往復するのにかかる平均のラウンドトリップ時間です。ACK と SYN のタイムスタンプの差により計算されます。
SRT	サーバがクライアントリクエストに応答し、レスポンスを完了させるのに要した時間です。ART + NRT + PTT で計算されます。
ART	サーバアプリケーションがクライアントリクエストに応答するのにかかる時間です。[応答パケットのタイムスタンプ] - [リクエストパケットのタイムスタンプ] で計算されます。
PTT	サーバがクライアントリクエストへのレスポンスを送るのに要した平均時間です。[ACK 応答のタイムスタンプ] - [サーバのレスポンスのパケットのタイムスタンプ] で計算されます。
CRT	クライアントがリクエストを開始するのにかかる時間です。ACK とクライアントリクエストのタイムスタンプの差により計算されます。
遅延	片方向のネットワークを通過するパケットの平均時間です。これは、NRT の半分の値となります。
リトライ	TCP の再送パケットのシーケンス数です。
トレースファイル	「トレースの保存」リンクをクリックすると、その近辺のレコードのトレースを保存できます。詳細は <b>5.4.2 トレースの保存</b> を参照してください。

フローにおけるサーバは次の規則によって決定されます。

1. 一方のポート番号のみがアプリケーションリストで定義されている場合、Synesis はそのポート番号に紐づく IP アドレスをサーバとみなします。
2. 送信元と送信先のポート番号が両方ともアプリケーションリストで定義されていない場合、Synesis は送信元と送信先のポート番号を比較し、小さい方をサーバとみなします。
3. 送信元と送信先のポート番号が同じである場合、Synesis は送信元と送信先の IP アドレスを上位から比較し、小さい方をサーバとみなします。

## 8.3. NPM 解析

各通信のバイト数やパケット数、ビットレートなどを送信側と受信側で個別に表示することで、ネットワークの状態を確認することができます。

### 8.3.1. NPM 解析での検索

「項目」と「KPI」を選択して、「検索」ボタンをクリックしてください。



設定項目の詳細は以下の通りです。

項目	説明
データソース	解析するキャプチャレコードのデータソースを選択します。 選択可能な項目は Synesis の設定により異なります。詳細は <b>D.2 データソース</b> を参照してください。
項目	指定された項目での KPI の TopN がトレンドグラフとフローテーブルに表示されます。指定可能な項目は以下の通りです。 <b>サイト</b> ※：IP アドレスをサブネットごとにグループ化したものです。 ホスト：単体の IP アドレスです。 <b>サーバグループ</b> ※：登録されたサーバをグループ化したものです。 アプリケーション： <b>12.15 プロトコル</b> で登録されたアプリケーションプロトコルのポート番号です。 <b>アプリケーショングループ</b> ※：登録されたアプリケーション(プロトコル※)をグループ化したものです。 アプリケーションホスト：IP アドレスと登録されたアプリケーションプロトコルの組み合わせです。
KPI	選択された KPI の TopN がトレンドグラフとフローテーブルに表示されます。トレンドグラフは TopN の合計値が表示されます。 フローテーブルに表示される各指標が選択可能です。 詳細は <b>8.3.2NPM 解析でのフローテーブル</b> を参照してください。

※検索を実行する前に、各「項目」で登録を行ってください。詳細は **12.13 サイト**、**12.14 サーバグループ**、**12.15 プロトコル**、**12.16 アプリケーショングループ**を参照してください。

## 8.3.2. NPM 解析でのフローテーブル

検索の結果、指定された項目での KPI の TopN がトレンドグラフとフローテーブルに表示されます。

ホスト1アドレス	ホスト1ポート	ホスト2アドレス	ホスト2ポート	総バイト	受信バイト	送信バイト	総パケット	受信パケット	送信パケット	双方向ビットレート	受信ビットレート	送信ビットレート	双方向バーストビットレート	受信バーストビットレート	送信バーストビットレート	表示	トレースファイル
10.158.17.104	1139	10.159.63.126	80	64,976,340	4,825,260	60,151,080	85,980	34,384	50,424	25,111	1,964	23,245	7,675,320	584,880	7,291,040	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1104	10.159.63.126	80	64,674,324	4,923,468	59,750,856	83,292	34,320	48,972	24,994	1,902	23,092	7,639,312	596,784	7,242,528	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1140	10.159.63.126	80	64,260,490	5,983,238	58,265,250	80,454	33,198	47,256	17,668	1,644	16,023	7,625,380	678,512	6,946,768	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1139	10.159.63.126	80	38,762,658	3,849,318	34,913,340	53,658	22,374	31,284	10,656	1,058	9,598	4,635,984	451,216	4,184,768	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1105	10.159.63.126	80	19,634,868	2,823,296	17,811,572	27,192	11,748	15,444	7,588	791	6,806	2,379,984	245,248	2,134,736	<a href="#">表示</a>	<a href="#">トレースの保存</a>
192.168.0.10	1367	206.142.53.2	80	22,949,784	5,638,446	17,311,338	35,640	18,018	17,622	3,923	963	2,959	1,851,360	454,224	1,397,136	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1112	10.159.63.126	80	9,654,876	1,017,588	8,637,288	13,728	6,072	7,656	3,731	383	3,338	1,170,288	123,344	1,046,944	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1108	10.159.63.126	80	8,175,288	820,512	7,354,776	11,816	5,148	6,668	3,159	317	2,842	990,944	99,456	891,488	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1110	10.159.63.126	80	7,111,896	512,688	6,599,208	9,240	3,828	5,412	2,748	198	2,550	862,048	62,144	799,904	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1111	10.159.63.126	80	6,792,860	671,088	6,120,972	8,976	3,696	5,280	2,624	259	2,365	823,280	81,344	741,936	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1109	10.159.63.126	80	5,707,476	1,523,148	4,184,328	8,844	4,488	4,356	2,205	508	1,617	691,808	184,624	507,184	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1116	10.159.63.126	80	4,796,160	273,624	4,482,536	6,972	2,508	3,564	1,830	195	1,724	574,880	33,168	540,912	<a href="#">表示</a>	<a href="#">トレースの保存</a>
3FFE:088:80F:2:FC::	1026	3FFE:591:4619:2000::	80	4,093,518	202,158	3,891,360	5,742	2,508	3,234	1,653	81	1,572	496,184	24,594	471,680	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.2.53.71	3737	216.147.63.146	80	3,177,372	314,820	2,862,552	5,610	3,168	2,442	1,283	127	1,156	385,136	38,160	346,976	<a href="#">表示</a>	<a href="#">トレースの保存</a>
192.168.0.10	1368	206.142.53.2	80	3,975,576	451,902	3,523,674	7,128	3,762	3,366	751	85	666	320,768	36,336	284,432	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1107	10.159.63.126	80	2,636,496	383,856	2,246,640	4,488	1,980	2,508	1,016	148	868	318,848	46,528	272,320	<a href="#">表示</a>	<a href="#">トレースの保存</a>
192.168.0.10	1363	206.142.53.2	80	2,818,464	416,328	2,402,136	4,488	2,310	2,178	556	82	474	307,816	48,928	258,888	<a href="#">表示</a>	<a href="#">トレースの保存</a>
192.168.42.116	60995	192.168.43.11	80	2,457,972	55,572	2,402,400	2,442	792	1,650	993	22	978	297,936	6,736	291,200	<a href="#">表示</a>	<a href="#">トレースの保存</a>
10.158.17.104	1105	10.159.63.126	80	2,180,144	175,296	2,014,848	3,432	1,452	1,980	846	67	778	265,472	21,248	244,224	<a href="#">表示</a>	<a href="#">トレースの保存</a>

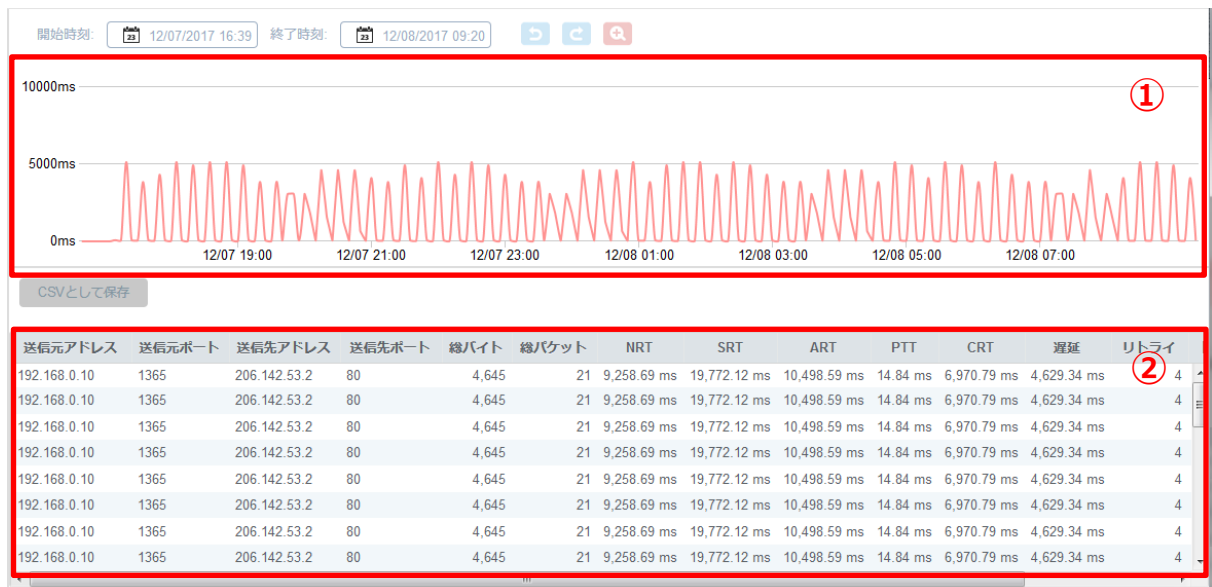
フローテーブルに表示される情報は以下の通りです。

項目	説明
ホスト 1 アドレス	クライアントアドレスです。
ホスト 1 ポート	クライアントポートです。
ホスト 2 アドレス	サーバアドレスです。
ホスト 2 ポート	サーバポートです。
総バイト／ 受信バイト／ 送信バイト	ホスト 1 とホスト 2 の間で送受信されるバイト数です。
総パケット／ 受信パケット／ 送信パケット	ホスト 1 とホスト 2 の間で送受信されるパケット数です。
双方向ビットレート／ 受信ビットレート／ 送信ビットレート	[受信バイト+送信バイト]/サンプル時間[Kbit/sec]で計算される値です。ビットレートは 1 分間ごとに計算されます。
双方向バーストビットレート／ 受信バーストビットレート／ 送信バーストビットレート	時間周期中の最大ビットレートです。例えば周期が 10 分の場合は、1 分ごとのビットレート値が 10 個存在しますが、その中で最大のものをバーストビットレートとします。
表示	「表示」リンクをクリックすると、そのフロー単体のトレンドグラフが表示されます。
トレースファイル	「トレースの保存」リンクをクリックすると、該当する通信をトレースファイルとして保存できます。詳細は <b>5.4.2 トレースの保存</b> を参照してください。

「ホスト 1」「ホスト 2」の意味するパケットフローの方向は、「項目」で選択された検索基準によって異なります。「項目」で「サイト」が選択された場合、「受信」はホスト 2 からホスト 1 の向きを指し、それ以外の場合はホスト 2 からホスト 1 への向きを指します。

## 8.4. 解析結果の絞込みとデータの抽出

検索を実行すると、検索結果として右側のワークスペース画面に検索時に指定した KPI のトレンドグラフ(下図①)と、フローテーブル(下図②)が表示されます。



トレンドグラフにはトラフィックの時間変化が表示されます。グラフの線の上にカーソルを合わせると、その時点でのトラフィック情報が表示されます。

線グラフとフローテーブルは、選択したデータソース内のすべてのチャンネルにおけるデータを集約して描画されます。データソースごとのチャンネル範囲は「D.2 データソース」を参照してください。フローテーブルは、データソースで「All Channel Group」を選択した場合に「エージェント」列が追加され、各フローデータのエージェント名が表示されます。

### 8.4.1. 指定範囲の拡大





トレンドグラフで拡大表示したい時間範囲をマウスドラッグで指定してください(上図③)。

「拡大」ボタン(上図④)をクリックすると、指定した時間範囲が拡大表示されます。

選択した時間範囲で拡大表示されると、フローテーブルに表示されるのも指定範囲のフロー情報のみになります。



画面上部中央の「元に戻す」 ボタン(上図⑤)をクリックすると直前に行った拡大処理が取り消され、「やり直す」 ボタン(上図⑥)をクリックすると、直前に行った「元に戻す」処理がキャンセルされます。

#### 8.4.2. トレースファイルの保存

APM 解析時も NPM 解析時も、フローテーブル各行の左端には「トレースの保存」リンクが表示されます。この「トレースの保存」リンクをクリックすると、関連するトラフィックをトレースファイルに保存することができます。

トレースファイル保存の手順や設定方法はエージェント画面のキャプチャレコード・ワークスペースで行うトレースの保存と同様です。詳細は **5.4.2 トレースの保存** を参照してください。

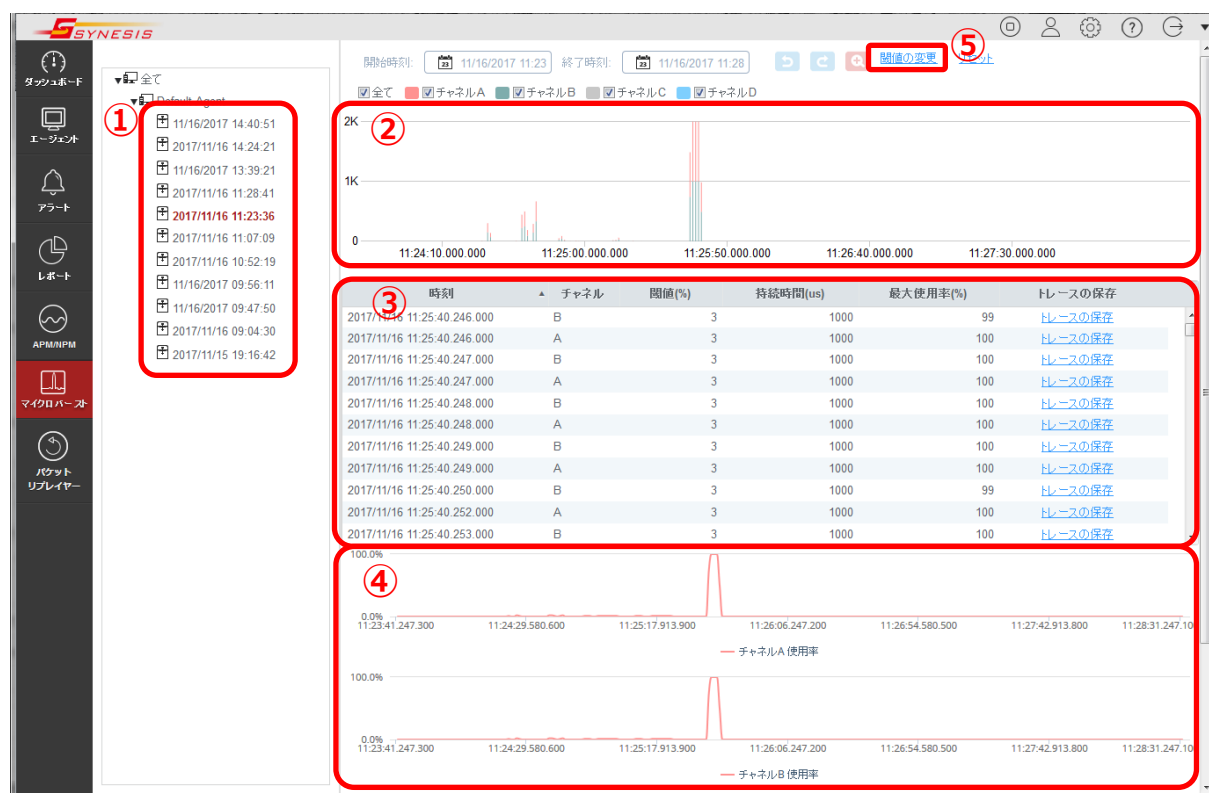
#### 8.4.3. フローテーブルを CSV として保存

フローテーブルの左上に表示される「CSV として保存」ボタン(上図⑦)をクリックすると、その時点でテーブルに表示されているフロー情報をカンマ区切り(CSV)ファイルで保存することができます。CSV ファイルに含まれる項目はそれぞれ **8.2.2 APM 解析のフローテーブル** と **8.3.2 NPM 解析でのフローテーブル** を参照してください。



## 9. マイクロバースト

マイクロバースト解析画面では、瞬間的にトラフィックが集中してしまうマイクロバースト（バーストトラフィック）の発生状況を確認することができます。



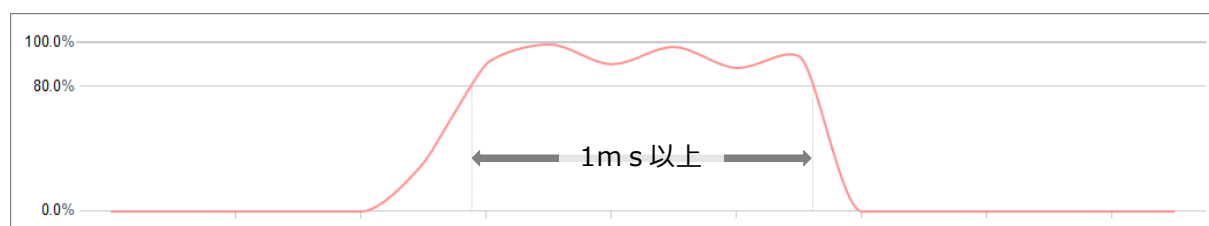
エージェント・ペインで解析したいキャプチャレコード(上図①)を選んでクリックしてください。選んだレコードがマイクロバースト解析されます。解析の結果、検知されたマイクロバーストにアラートが出され、右側のワークスペース画面にアラート情報として表示されます。

ワークスペース画面には一番上にマイクロバーストのアラートグラフ(上図②)、中央にアラートテーブル(上図③)、その下にチャンネルごとの回線使用率のグラフ(上図④)が表示されます。

表示内容の詳細は本章の **9.1 マイクロバーストのアラートグラフとテーブル**を確認してください。

### マイクロバーストの検知とアラート発生の閾値

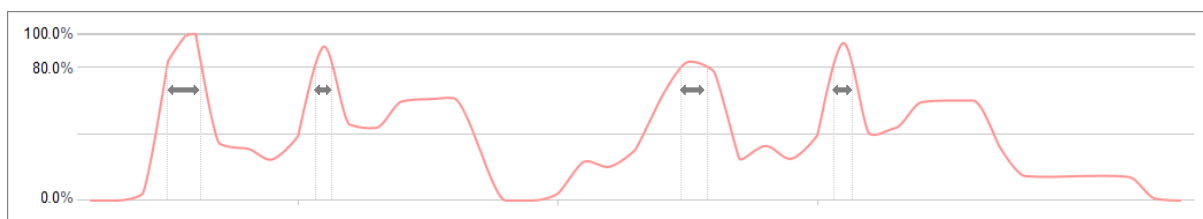
マイクロバーストを検知するには、まずマイクロバーストの発生の判断基準となる「使用率」と「持続時間」が必要です。トラフィックの使用率が指定した「使用率」を超え、その状態が指定した「持続時間」を超えて続いた場合に、マイクロバーストが発生したと判断されます。



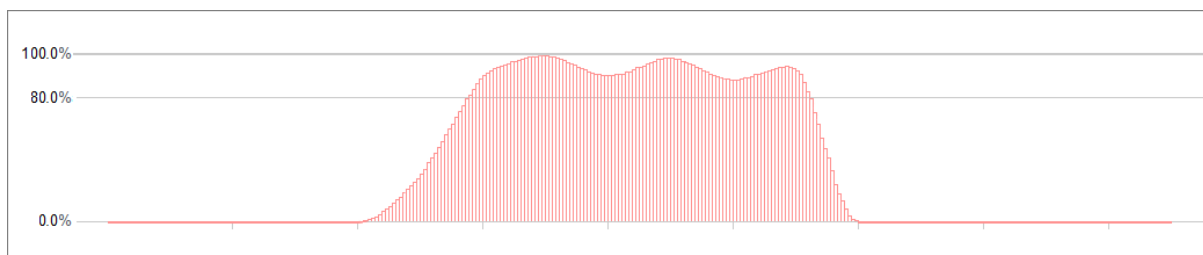
例えば使用率の閾値を 80%、持続時間の閾値を 1ms と指定した場合は、1ms 以上、トラフィックの使用率が 80%を越え続けた時に、マイクロバーストが発生したと判断され、アラートが出ます。



下図のように使用率が閾値を超えていても、持続時間が閾値より短い場合は、マイクロバーストが発生したとは判断されず、アラートも発行されません。



実際の解析過程では、キャプチャレコードを指定された「分解能」で区切って使用率の平均値を取り、その使用率が指定した閾値を超えていないか、確認します。



「持続時間」は「分解能」と閾値を超えた区間の数(「連続発生数」)で計算されます。

区間の数は使用率の平均値が閾値を超えていた時点から使用率の平均値が閾値以下になるまで数えられます。その区間の数が「連続発生数」です。

「持続時間」は「分解能」×「連続発生数」で、「持続時間」の閾値も「分解能」と「連続発生数」で指定されます。

マイクロバーストのアラート閾値を設定したい場合は、「閾値の変更」リンク(前頁図⑤)をクリックしてください。詳細は **9.2.2 閾値の変更** を参照してください。

### マイクロバーストのリアルタイム検知

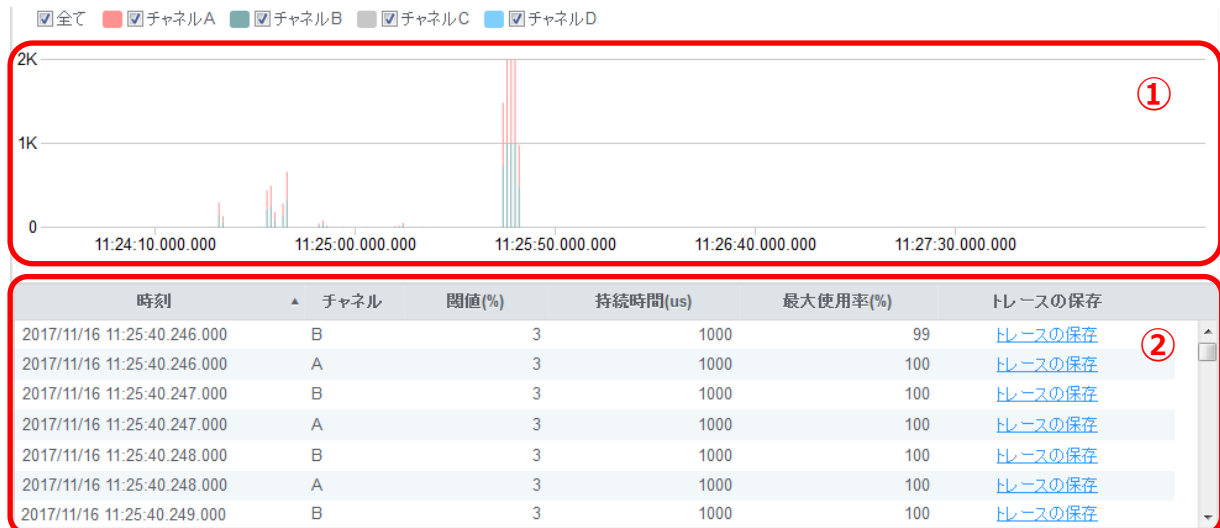
キャプチャ中のレコードをリアルタイムにマイクロバーストを検出させたい場合は、キャプチャ開始前に「構成」メニューの「マイクロバースト」セクションで回線使用率を設定する必要があります。詳細は **12.17 マイクロバースト** を参照してください。

解析結果を更新したい場合はキーボードの「F5」キーを押してください。終了時刻が更新され、最新の解析結果が表示されます。

## 9.1. マイクロバーストのアラートグラフとテーブル

マイクロバースト解析画面には一番上にマイクロバーストのアラートグラフ(下図①)、中央にマイクロバーストのアラートテーブル(下図②)が表示されます。

画面の下部には、チャンネルごとの使用率のグラフが表示されます。



アラートグラフは横軸を時間とし、縦軸にアラート発生回数を表したヒストグラムです。横軸の時間範囲を等間隔に区切り、各区間内に何回アラートが発生したかを示しています。


アラートテーブルには使用率の大きい順にトップ 500 のアラートが表示されています。


表示される情報は以下の通りです。




項目	説明
時刻	マイクロバーストが検知された時刻です。
チャンネル	マイクロバーストが検知されたチャンネルです。
閾値(%)	検知された閾値の回線使用率です。
持続時間	検知された閾値の時間です。
最大使用率(%)	最大使用率です。
トレースの保存	「トレースの保存」リンクをクリックすると、マイクロバーストが検知され、アラートが発生した期間のデータをトレースファイルとして保存できます。 詳細は <b>5.4.2 トレースの保存</b> を参照してください。

## 9.2. 回線使用率の設定と時間範囲選択

マイクロバースト・ワークスペース画面の上部には、回線使用率や時間範囲などを設定するメニューやボタンが表示されています。





開始時刻:  11/16/2017 11:23

終了時刻:  11/16/2017 11:28

   [閾値の変更](#) [リセット](#)

☒ 全て ☐ チャンネルA ☒ チャンネルB ☐ チャンネルC ☒ チャンネルD

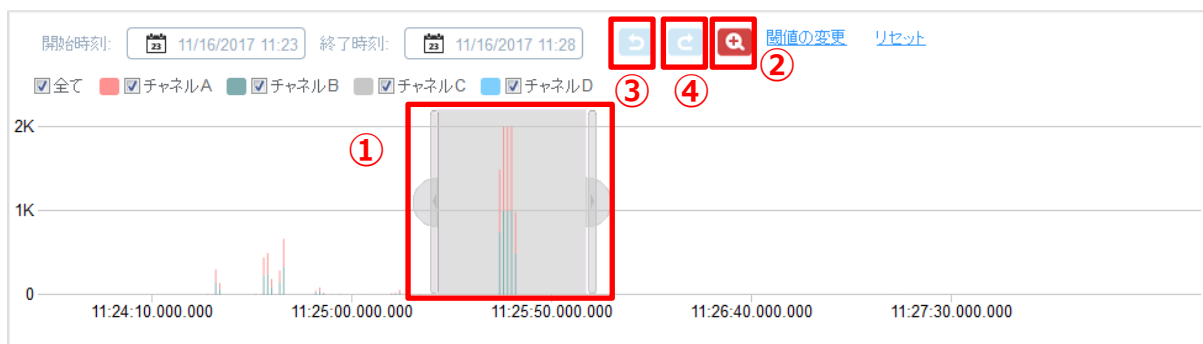
各機能はそれぞれ以下の通りです。

項目/表示	説明
開始時刻 /終了時刻	選択されたキャプチャレコードの開始時刻と終了時刻です。 時間範囲を選択して拡大表示した場合は、表示範囲の時刻になります。 リアルタイム解析を行っている場合は、最新の更新時刻が終了時間になります。 表示を更新したい場合は、キーボードの「F5」キーを押してください。
 ボタン	キャプチャレコードの期間の一部を選択し、拡大表示させることができます。 詳細は次項を参照してください。
 	「元に戻す」ボタンをクリックすると、直前に行った拡大処理がキャンセルされます。「やり直す」ボタンをクリックすると、直前に行った「元に戻す」処理がキャンセルされます。
閾値の変更	マイクロバースト検知のために必要な回線使用率、連続発生数、分解能の設定を変更して、新しい設定でマイクロバースト解析を実行します。 詳細は <b>9.2.2 閾値の変更</b> を参照してください。
リセット	変更した回線使用率や分解能などの設定がデフォルトに戻ります。 デフォルト値は、ツールバーメニュー「構成」  の「マイクロバースト」セクションで設定された値です。 詳細は <b>12.17 マイクロバースト</b> を参照してください。
全て /各チャンネル	グラフやテーブルにどのチャンネルのデータを表示するかを選択できます。 チェックマークの入ったチャンネルのデータのみが表示されます。


詳細は本節の各項を参照してください。

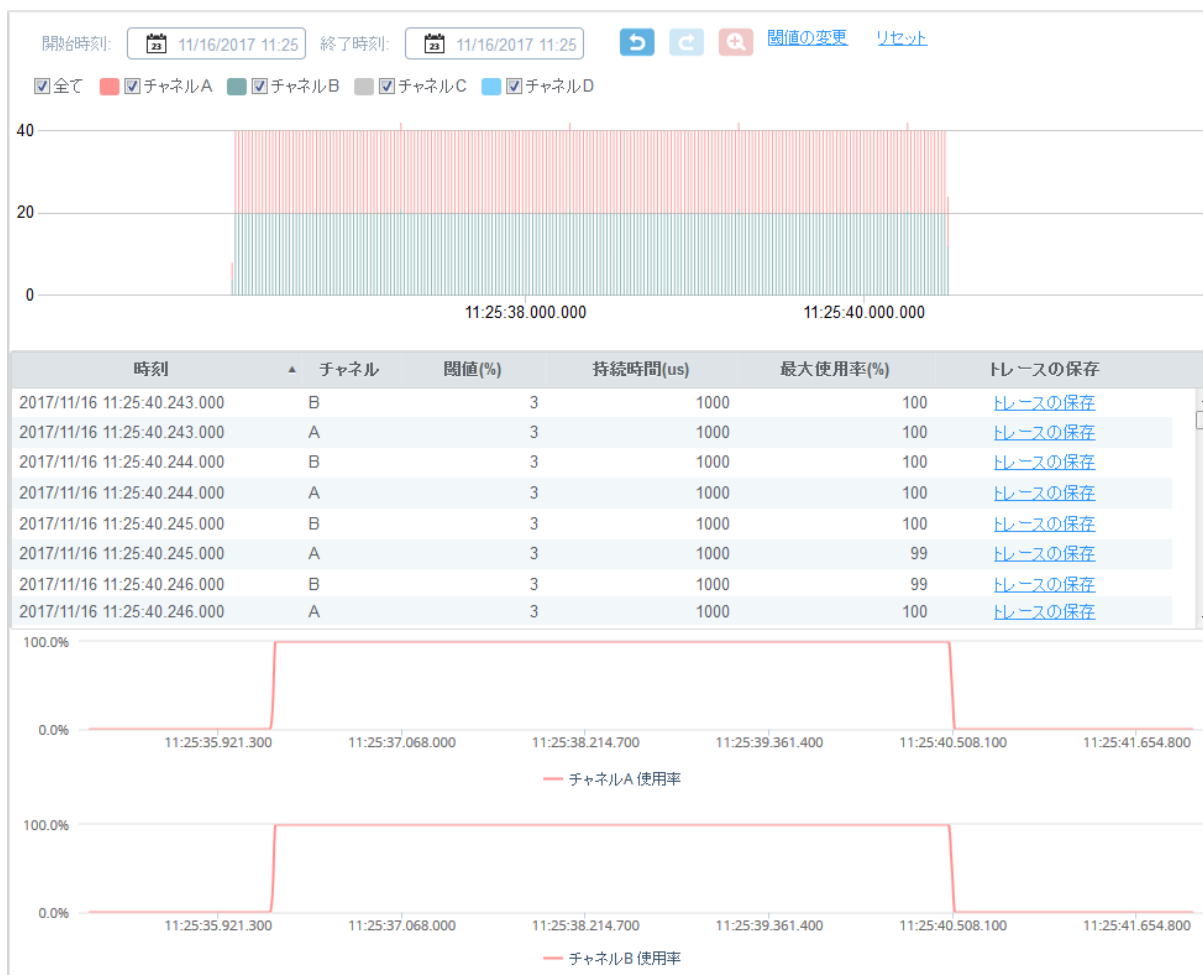
### 9.2.1. 選択範囲の拡大表示

アラートグラフで、データを確認しながら時間範囲を指定して拡大表示させることが可能です。





アラートグラフで、拡大表示したい部分をマウスドラッグで指定してください(上図①)。

画面上部中央の「拡大」 ボタン(上図②)をクリックすると、グラフの時間の表示範囲が選択した部分のみになり、拡大表示されます。このとき、アラートテーブルにリストアップされるデータも、チャンネルごとの使用率のグラフも選択された時間範囲のみに拡大表示されます。



確認したい時間範囲を選んで拡大表示していくと、等間隔に区切られたアラートグラフの1区間の時間は短くなります。集計する時間が短くなるため、アラートの発生回数の合計値は変わります。

「元に戻す」 ボタン(図③)をクリックすると直前に行った拡大処理が取り消されます。「やり直す」 ボタン(図④)をクリックすると、直前に行った「元に戻す」処理がキャンセルされます。

### 9.2.2. 閾値の変更

キャプチャ済みのキャプチャデータを再解析して、マイクロバーストの発生状況を確認することができます。一度に再解析できる時間は最大 120 分です。

再解析を行いたい場合は、画面上部の「閾値の変更」リンクをクリックしてください。

下図の「再解析」ダイアログが表示されます。

● 再解析

開始時刻 2015/05/21 10:43:37.050.000

長さ  分 (1-120)

アラーム閾値設定

☒ 閾値 1

使用率 >=  % (1-100)

連続発生数  (1-70000)

☐ 閾値 2

使用率 >=  % (1-100)

連続発生数  (1-70000)

分解能

キャンセル

適用

各項目を設定して、「適用」ボタンをクリックすると、新しい閾値で再解析が実行されます。

アラート閾値は最大 2 件指定できます。

設定項目の詳細は下記の通りです。

項目	説明
長さ	選択されたキャプチャレコードの「開始時刻」から、解析を行う期間を 1 分刻みで指定します。1 分から最大 120 分まで指定できます。
使用率	閾値となる回線使用率を 1 以上 100 以下、パーセンテージで入力します。 ここで指定した回線使用率を連続して超えた期間が「持続時間」となります。
連続発生数	マイクロバースト発生の判断基準とする「持続時間」を「連続発生数」で指定します。閾値となる「持続時間」は「分解能」×「連続発生数」です。 1 以上 70000 以下の数字を入力してください。
分解能	どれだけ細かくキャプチャレコードを区切って使用率を確認するか、その細かさ (区切られた 1 区間の長さ) を指定します。閾値 1・閾値 2 で共通です。 デフォルトは 1000 us で、1000 us または 100 us に設定できます。

指定された閾値を元に、どのように解析が行われるかは**マイクロバーストの検知とアラート発生の閾値**を参照してください。

「リセット」ボタンをクリックすると、変更した使用率や連続発生数などの閾値の設定が、「構成」メニュー「マイクロバースト」セクションで設定したデフォルトの設定に戻ります。

詳細は **12.17 マイクロバースト** を参照してください。

## 10. パケットリプレイヤー

パケットリプレイヤーは、トレースファイルやキャプチャレコードのトラフィックを再生して、実環境にパケットを送信する機能です。

ご使用になる場合は「パケットリプレイヤーオプション」が必要になります。



再生するトラフィックのソースファイルとして選択可能なのは、トレースファイルと Synesis 内に保存されているキャプチャレコードです。それらのファイルを元にプロファイルを作成し、トラフィックを再生します。プロファイルを編集してフィルタなどを設定したり、特定のパケットを別のパケットに置き換えたりして、再生するトラフィックに変化を加えることも可能です。

主な流れは以下の通りです。

### 1. 「プロファイル」の作成・編集

再生するトラフィックのソースファイルとして、トレースファイルやキャプチャレコードを選択し、プロファイルを作成します。

作成したプロファイルは画面左のプロファイル・ペイン(上図①)に追加されます。

詳細は **10.1 プロファイルの作成**を確認してください。

### 2. 再生時のパラメータ設定

プロファイルを編集して、フィルタなどを設定したり、特定のパケットを別のパケットに置き換えたりして、再生するトラフィックに変化を加えることが可能です。

詳細は **10.2 プロファイルの設定**を参照してください。

### 3. 再生(リプレイ)の開始

プロファイルを選択して「リプレイの開始」ボタンをクリックすると、トラフィックが再生されます。詳細は **10.3 プロファイルの再生**を参照してください。

## 10.1. プロファイルの作成


ソースファイルとなるトレースファイル、またはキャプチャレコードを選択して、トラフィック再生用のプロファイルを作成します。

プロファイルでフィルタリングやデータの置換、再生スピードなどを設定することが可能で、トラフィックをキャプチャしたそのままだけでなく、変更を加えた上で再生することが可能です。

### 10.1.1. トレースファイルの追加

トレースファイルをソースファイルとして、プロファイルを作成することが可能です。自身で作成したトレースファイルはもちろん、外部から読み込んだトレースファイルを利用することが可能です。

利用可能なトレースファイルは「pcap」「pcap(nano)」「pcapng」の3種類です。

トレースファイルを元にプロファイルを作成したい場合は、画面右上の「追加」アイコンをクリックして、ドロップダウンリストから「トレースファイル」を選択してください。



下図の「トレースファイル」ダイアログが表示されます。

● トレースファイル

**追加** ①

プロファイル名

エージェント名

チャンネル

送信  
ポート ☒ チャンネル A ☐ チャンネル B

<input type="checkbox"/>	名前	サイズ	作成日時
--------------------------	----	-----	------

パケットフィルタ   
(説明: すべてのパケットがフィルタリングされ、フィルタを通過したパケットのみが送信されます。)

ストリーム ☐ ワイヤーレート ☒ 元のスピード

再生回数 ☒ 繰り返し ☐ 回数

キャンセル 適用

画面左上、最上段の「追加」ボタン(上図①)をクリックしてください。

ダイアログ画面の中央に、選択可能なトレースファイルが、タブ分けされて表示されます(下図②)。

● トレースファイル

追加 削除

プロファイル名

エージェント名

チャンネル

送信  
ポート ☒ チャンネル A ☐ チャンネル B

名前	サイズ	作成日時
----	-----	------

ビルドインファイル カスタムファイル トレースバンカー

ディスク容量情報 9.00 GB / 9.00 GB

ステータス	名前	サイズ	作成日時
Select	1511229677069-9535.pcapng	1 MB	2017/11/21 11:01

キャンセル 適用

タブの種類や外部からの読み込み手順は **5.3.4 トレースファイル タブ** を参照してください。

ソースとするトレースファイルの「Select」リンクをクリックします。選択したトレースファイルがソースリストに追加されます(下図③)。

③

名前	サイズ	作成日時
<input type="checkbox"/> 1511229677069-9535.pcapng	1 MB	11/21/2017 11:01:27.000
<input type="checkbox"/> 1510198984441-8552.pcapng	1 MB	11/09/2017 12:43:11.000

ビルドインファイル カスタムファイル トレースバンカー

ディスク容量情報 9.00 GB / 9.00 GB

ステータス	名前	サイズ	作成日時
Select	1511229677069-9535.pcapng	1 MB	2017/11/21 11:01
Select	1510198984441-8552.pcapng	1 MB	2017/11/09 12:43

ソースファイルとするトレースファイルは 20 個まで選択可能です。

追加したソースファイルを削除したい場合は、ソースファイルのチェックボックスにチェックを付け、「削除」ボタンをクリックしてください。




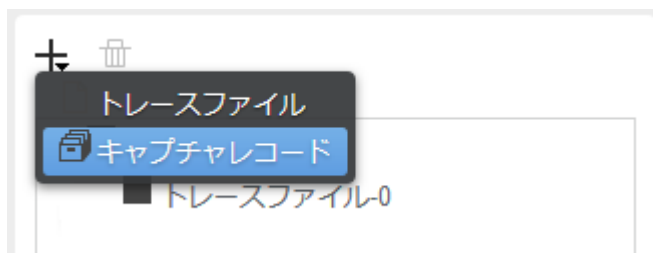
「適用」ボタンをクリックすると、プロファイルが保存され、プロファイル・ペインに追加されます。再生時にフィルタをかけたり、特定の packets を別の packets に置き換えたり、元のキャプチャしたものとは変化したトラフィックを再生したい場合は、ダイアログ画面の「パケットフィルタ」など、各種設定項目をご利用ください。

設定項目の詳細と設定方法は **10.2 プロファイルの設定** を参照してください。

### 10.1.2. キャプチャレコードの追加

選択可能なキャプチャレコードは、その Synesis がキャプチャしたものに限定されます。

キャプチャレコードを元にプロファイルを作成したい場合は、画面右上の「追加」 アイコンをクリックし、ドロップダウンリストから「キャプチャレコード」を選択してください。



下図の「キャプチャレコード」ダイアログが表示されます。

● キャプチャレコード

① 追加

削除

プロファイル名

エージェント名

☒ 元のチャンネル

開始時刻:  終了時刻:

<input type="checkbox"/>	レコード名	開始時刻	終了時刻
--------------------------	-------	------	------

パケットフィルタ   
(説明: すべてのパケットがフィルタリングされ、フィルタを通過したパケットのみが送信されます。)

ストリーム ☐ ワイヤレート ☒ 元のスピード

再生回数 ☒ 繰り返し ☐ 回数

FCS ☒ 元のFCS ☐ 再計算 ☐ 追加する

☐ パケット内容を置換える

キャンセル

適用

画面左上の「追加」ボタン(上図①)をクリックしてください。

ダイアログ画面の中央に、選択可能なキャプチャレコードが一覧で表示されます(下図②)。

● キャプチャレコード

追加 削除

プロファイル名

エージェント名

☒ 元のチャンネル

開始時刻:  終了時刻:

<input type="checkbox"/>	レコード名	開始時刻	終了時刻
<a href="#">Select</a>	2017/11/30 20:03:26	2017/11/30 20:03:50	2017/11/30 23:03:20
<a href="#">Select</a>	2017/12/01 11:14:50	2017/12/01 11:14:59	2017/12/01 11:15:47
<a href="#">Select</a>	2017/12/01 11:28:26	2017/12/01 11:28:34	2017/12/01 11:28:59
<a href="#">Select</a>	2017/12/01 14:15:20	2017/12/01 14:15:25	2017/12/01 15:19:22

キャンセル

パケットフィルタ

(説明: すべてのパケットがフィルタリングされ、フィルタを通過したパケットのみが送信されます。)

ストリーム ☐ ワイヤレート ☒ 元のスピード

キャンセル 適用

ソースとしたいキャプチャレコードの「Select」リンクをクリックしてください。選択したキャプチャレコードがソースリストに追加されます(下図③)。

開始時刻:  終了時刻:

<input type="checkbox"/>	レコード名	開始時刻	終了時刻
<input checked="" type="checkbox"/>	2017/11/30 20:03:26	2017/11/30 20:03:50	2017/11/30 23:03:20

	レコード名	開始時刻	終了時刻
<a href="#">Select</a>	2017/11/30 20:03:26	2017/11/30 20:03:50	2017/11/30 23:03:20
<a href="#">Select</a>	2017/12/01 11:14:50	2017/12/01 11:14:59	2017/12/01 11:15:47
<a href="#">Select</a>	2017/12/01 11:28:26	2017/12/01 11:28:34	2017/12/01 11:28:59
<a href="#">Select</a>	2017/12/01 14:15:20	2017/12/01 14:15:25	2017/12/01 15:19:22

キャンセル

1つのプロファイルで、ソースファイルとして選択できるキャプチャレコードは1レコードのみです。別のキャプチャレコードを選びなおして「Select」リンクをクリックすると、「置換えますか？」と確認のメッセージが表示されます。「はい」ボタンをクリックするとソースファイルが変更されます。「適用」ボタン(図④)をクリックすると、プロファイルが作成されます。

再生時にフィルタをかけたり、特定の packets を別の packets に置き換えたり、元のキャプチャしたものととは変化したトラフィックを再生したい場合は、ダイアログ画面の「パケットフィルタ」など、各種設定項目をご利用ください。詳細は次頁の **10.2 プロファイルの設定** を参照してください。

## 10.2. プロファイルの設定

再生速度を変更したり、パケットフィルタやデータ置換を設定したり、下のトラフィックに変更を加えて再生することができます。

プロファイル・ペインで再生パラメータを設定したいプロファイルを選択したら、「プロファイルの設定」ボタン(下図①)をクリックしてください。



プロファイルの設定ダイアログが表示されます。



設定後、「適用」ボタンをクリックしてください。再生パラメータの設定が保存されます。

プロファイル作成時に再生パラメータを設定することも可能です。

設定項目の詳細は以下の通りです。

項目		説明
プロファイル名		プロファイルの名前です。
エージェント名		再生を実行するエージェントの名前です。
チャンネル	アダプタ	アダプタ(キャプチャカード)を選択します。
	送信ポート	送信ポートを選択します。
ソースファイルリスト		再生するトラフィックの元となるファイルを指定します。
パケットフィルタ		ソフトウェアフィルタを適用し、特定のパケットを抽出、もしくは削除してトラフィックを再生します。 フィルタの種類と設定方法は置換フィルタと共通です。 詳細は次頁を参照してください。
ストリーム	ワイヤーレート	ワイヤーレートスピードで再生します。
	元のスピード	キャプチャ時と同じラインスピードで再生します。
再生回数	繰り返し	停止するまで繰り返し再生します。
	回数	何度、繰り返して再生するかを数値で指定します。
FCS	元の FCS	FCS の正誤に関わらず、パケットをそのまま再生します。
	再計算	FCS の有無に関わらず、パケットの最後の 4byte を FCS として再計算し、再生します。
	追加する	FCS の有無に関わらず、全てのパケットに新しく FCS を追加して再生します。
パケット内容を置換える		チェックマークを付けると置換フィルタが有効になります。 「置換フィルタ」で指定した条件に合致するパケットに対して、置換アイテムリストで指定したデータの置換が実行されます。
置換フィルタ		データの置換を実行するパケット抽出するためのフィルタです。 フィルタの種類と設定方法はパケットフィルタと共通です。 詳細は次頁を参照してください。
置換アイテムリスト		「この MAC アドレスをこの MAC アドレスに置き換える」等具体的な置き換えの内容を定義します。 詳細は <b>10.2.2 置換アイテムの種類と設定方法</b> を参照してください。

作成したプロファイルのソースファイルを変更することも可能です。

削除したいソースファイルのチェックボックスにチェックを付け、「削除」ボタンをクリックしてください。ソースファイルリストから選択したソースファイルが削除されます。

画面右上の「追加」ボタンをクリックすると、ダイアログ中央に選択可能なソースファイルのリストが表示されます。新しくソースファイルするファイルの「Select」リンクをクリックしてください。

詳細は **10.1.1 トレースファイルの追加**と **10.1.2 キャプチャレコードの追加**を参照してください。

### 10.2.1. パケットフィルタと置換フィルタ

「パケットフィルタ」はトラフィックから特定の packets を抽出、もしくは削除して再生するためのフィルタです。「置換フィルタ」は置換アイテムを適用する packets を検出するためのフィルタです。2つのフィルタが適用される目的は異なりますが、共に「構成」メニューで設定される保存フィルタを使用します。

パケットフィルタ（または置換フィルタ）のテキストボックスの▼をクリックしてください。

設定済みの保存フィルタ(下図①)と保存フィルタ追加・編集用のメニュー(下図②)が表示されます。

パケット内容を置換える

置換フィルタ: ICMP(v6)フィルタ

フィルタなし

既存フィルタの編集 ②

新規フィルタの作成

ARPフィルタ

IPv6フィルタ

ICMP(v6)フィルタ ①

L4(HTTP)フィルタ

説明

使用したい保存フィルタが定義済みであれば、その保存フィルタの中から選択してください(上図①)。

選択した保存フィルタを取り消したい場合は「フィルタなし」を選択してください。

「新規フィルタの作成」を選択すると、新規フィルタ登録画面が表示されます。保存フィルタの設定を行い「保存」ボタンをクリックすると、設定したフィルタが登録され、表示フィルタ、もしくは置換フィルタに設定されます。

「既存フィルタの編集」を選択すると、登録済みの保存フィルタの一覧が表示されます。

● 保存フィルタ

新規 削除

<input type="checkbox"/>	名前	説明
<input checked="" type="checkbox"/>	<a href="#">ARPフィルタ</a>	{[L2 Ether Type - L2 Ether Type: ARP; ]}
<input checked="" type="checkbox"/>	<a href="#">IPv6フィルタ</a>	{[L2 Ether Type - L2 Ether Type: IPv6; ]}
<input checked="" type="checkbox"/>	<a href="#">ICMP(v6)フィルタ</a>	{[L3 Protocol - L3 Protocol: ICMPv6; ]}
<input checked="" type="checkbox"/>	<a href="#">L4(HTTP)フィルタ</a>	{[アプリケーション - 第4層タイプ: TCP; HTTP(80;443);]}

キャンセル 適用

編集したい保存フィルタの名前のリンクをクリックしてください。その保存フィルタを編集できます。

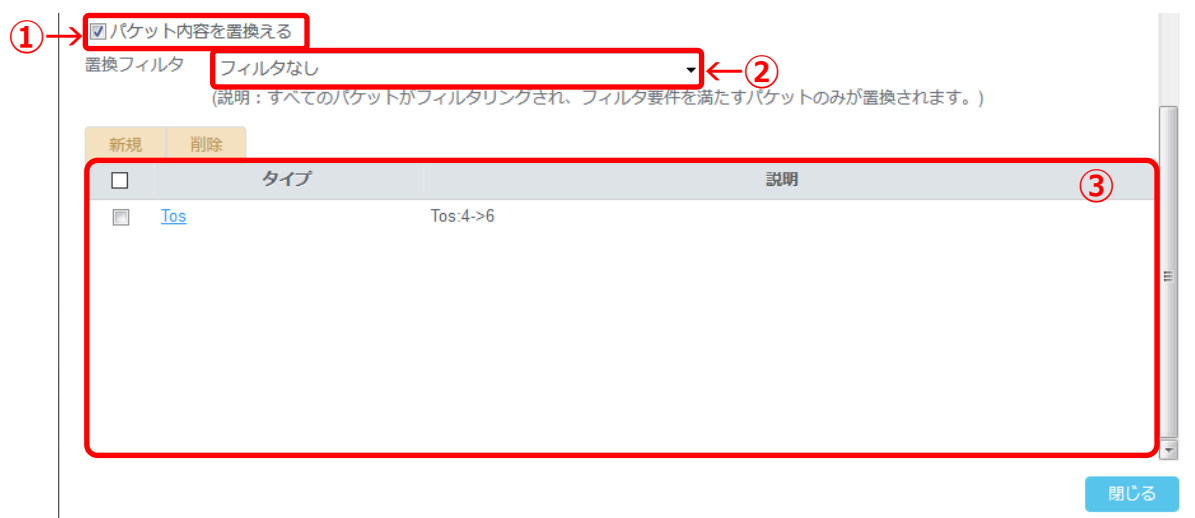
「新規」ボタンをクリックすると、新しい保存フィルタを登録できます。

適用させたい保存フィルタにチェックマークを付け、「適用」ボタンをクリックしてください。

フィルタの種類と設定方法は **12.6 保存フィルタ**を参照してください。

### 10.2.2. 置換アイテムの種類と設定方法

「パケット内容を置き換える」にチェックマークを入れると(下図①)、「置換フィルタ」選択用のドロップダウン・リストボックス(下図②)と、置換アイテムリスト(下図③)が表示されます。



置換フィルタでどのデータの置換を行うパケットを抽出し、抽出されたパケットに置換アイテムとしてリストに登録したデータの置換を実行します。

置換フィルタの設定方法は前項目を参照してください。

「フィルタなし」が設定されている場合は、すべてのパケットに対し置換を実行します。

置換アイテムとして以下の 5 種類のデータ置換が設定可能です。

種類	説明
MAC アドレス	特定の MAC アドレスを特定の MAC アドレスに置換します。 送信元 MAC アドレスと送信先の MAC アドレスを個別に指定できます。
VLAN	特定の VLAN を特定の VLAN に置換します。
フロー	特定の IP アドレスと TCP ポートのペアを、特定の IP アドレスと TCP ポートのペアに置換します。送信元と送信先で個別に指定できます。
ToS/Diffserv	特定の ToS/Diffserv を特定の ToS/Diffserv に置換します。
パターン	特定の 16 進数のパターンを特定の 16 進数のパターンに置換します。 もしくは特定の ASCII 文字列を特定 ASCII 文字列に置換します。 置き換えを行う部分はパケットのスタートを "0" とし、16 進数、もしくは 10 進数で指定されたオフセット値で指定されます。

なお、置換アイテムが複数設定されている場合は、リストの上から順に置換が実行されます。

また、置換が実行されるのは指定された部分のみです。置換後、IP ヘッダ、TCP ヘッダ、UDP ヘッダのチェックサムは再計算されないのをご注意ください。

### 10.2.2.1 MACアドレス

置換前の MAC アドレスと置換後の MAC アドレスを設定してください。

送信元の MAC アドレスと送信先の MAC アドレスを個別に指定することができます。

● 置換アイテム

MACアドレス

VLAN

フロー

ToS / Diffserv

パターン

置換前のMACアドレス

送信元

MACアドレス

送信先

MACアドレス

置換後のMACアドレス

送信元

MACアドレス

送信先

MACアドレス

コロン (:) を使って入力してください。例 01:23:45:67:89:ab

コロン (:) を使って入力してください。例 01:23:45:67:89:ab

コロン (:) を使って入力してください。例 01:23:45:67:89:ab

コロン (:) を使って入力してください。例 01:23:45:67:89:ab

キャンセル

適用

コロン(:)を使って MAC アドレスを指定してください。

### 10.2.2.2 VLAN

置換前の VLAN ID と置換後の VLAN ID を設定してください。

● 置換アイテム

MACアドレス

VLAN

フロー

ToS / Diffserv

パターン

置換前のVLAN ID

VLAN ID

置換後のVLAN ID

VLAN ID

単一の数字(0-4095)

単一の数字(0-4095)

キャンセル

適用

VLAN ID は0 から 4095 の 10 進数の数値で設定してください。

### 10.2.2.3 フロー

置換前と置換後の TCP ポート番号と IP アドレスをペアで指定してください。

送信元と送信先のポート番号と IP アドレスを個別に登録することが出来ます。

10 進数の IPv4 アドレス、もしくは 16 進数の IPv6 アドレスで IP アドレスを指定してください。

● 置換アイテム

MACアドレス

VLAN

**フロー**

ToS / Diffserv

パターン

置換前のフロー

送信元 IPアドレス

ポート

10進数のIPv4、又は、16進数のIPv6

単一の数字(1-65536)

送信先 IPアドレス

ポート

10進数のIPv4、又は、16進数のIPv6

単一の数字(1-65536)

置換後のフロー

送信元 IPアドレス

ポート

10進数のIPv4、又は、16進数のIPv6

単一の数字(1-65536)

送信先 IPアドレス

ポート

10進数のIPv4、又は、16進数のIPv6

単一の数字(1-65536)

キャンセル

適用

登録項目は以下の通りです。

項目	説明
送信元/送信先 IP アドレス	送信元/送信先の IP アドレスを 10 進数の IPv4 アドレス、もしくは 16 進数の IPv6 アドレスで指定します。 空欄の場合は全ての IP アドレスが対象となります。
ポート	送信元/送信先の TCP ポート番号を 10 進数の数値(0-65535)で指定します。 空欄の場合は全てのポート番号が対象となります。



#### 10.2.2.4 ToS/Diffserv

16 進数(HEX)の値で置換前の ToS/Diffserv と置換後の ToS/Diffserv を指定してください。

● 置換アイテム

MACアドレス

VLAN

フロー

ToS / Diffserv

パターン

置換前のToS / Diffserv

ToS

置換後のToS / Diffserv

ToS

キャンセル

適用

設定できる値は 00 から FF です。

### 10.2.2.5 パターン

置換前と置換後のパターンを 16 進数(HEX)、もしくは ASCII 文字列で指定してください。

● 置換アイテム

MACアドレス  
VLAN  
フロー  
ToS / Diffserv  
**パターン**

オフセット  ☒ 16進数 ☐ 10進数

パターン形式

マスク

置換前のパターン

置換後のパターン

キャンセル 適用

登録項目は以下の通りです。

項目	説明
オフセット	パケットのスタートを "0" とし、置換する文字列の位置(ビット列)を指定します。入力形式は「16 進数」か「10 進数」を選択してください。
パターン形式	パターン文字列の表示形式を指定します。 選択可能な項目は「ASCII」もしくは「16 進数」です。
マスク	「マスクパターン」を 16 進数(HEX)文字列で指定します。 パターン形式が「16 進数」の時のみ有効になります。 「パターン」と「マスクパターン」の AND がビットごとに計算され、「オフセット」位置のビット列が一致したパケットが置換されます。
置換前のパターン	置換対象とするパターン文字列を指定します。
置換後のパターン	「置換前のパターン」に置き換えるパターン文字列を指定します。

パターン形式として「ASCII」が指定された場合、指定した「オフセット」位置に「置換前のパターン」文字列があれば、その文字列は「置換後のパターン」文字列に置き換えられます。

パターン形式として「16 進数」が指定された場合は、「置換前のパターン」と「マスクパターン」でビットごとに AND が計算され、そのビット列が完全に一致したものが置換対象になります。

「マスク=1」のビットは置換後のパターンに置換されます。「マスク=0」のビットは現状の値を維持します。

## 10.3. プロファイルの再生

作成したプロファイルからトラフィックの再生を実行します。

プロファイル・ペインに表示されるプロファイルのリストの中から、再生したいプロファイルを選択し、クリックしてください。下図のプロファイル・ワークスペース画面が表示されます。



「リプレイの開始」ボタン(上図①)をクリックするとトラフィックの再生が開始されます。

ワークスペース画面の左上にはプロファイル情報のテーブル(上図②)が表示されます。

プロファイル情報のテーブルの下に表示されるのは「使用率」「ビットレート」「パケット」「バイト」、この4つの指標についてのテーブル(上図③)と、ダッシュボード(上図④)です。

パケットサイズ分布の棒グラフ(上図④)がその右側に、テーブル(上図⑤)が一番下に表示されます。

### プロファイルの情報

プロファイル・ワークスペースの左上のテーブル(上図②)にはプロファイルの情報が表示されます。

プロファイル名	トレースファイル-0	パケットフィルタ	フィルタなし
エージェント名	Default Agent	コンテンツ	置換なし
チャンネル	送信ポート: A	開始時刻	2017/12/01 10:02:58
トラフィックタイプ	トレースファイル	終了時刻	2017/12/01 10:03:23
再生回数	繰り返す	持続時間	0 00:00:25
ストリーム	元のスピード	状態	停止中
FCS	元のFCS		

こちらで再生スピードなどを確認し、必要があれば再生を停止してプロファイルの設定を編集してください。「プロファイルの設定」ボタンをクリックすると、プロファイル設定編集用のダイアログが表示され、プロファイルの設定を変更できます。

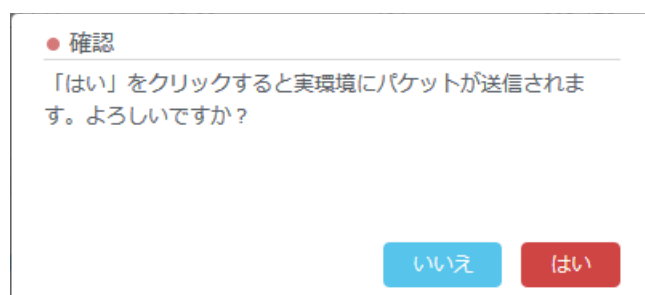
詳細は **10.2 プロファイルの設定** を参照してください。

表示される情報は以下の通りです。

項目	説明
プロファイル名	プロファイルの名前です。
エージェント名	エージェントの名前です。
チャネル	トラフィックを再生して送信するポートです。
トラフィックタイプ	ソースファイルの種類です。 トレースファイルかキャプチャレコードになります。
再生回数	設定されている再生回数です。 「繰り返し」の場合は停止するまで再生を続けます。
ストリーム	トラフィックの再生スピードです。 「元のスピード」か「ワイヤーレート」になります。
FCS	FCS の設定です。「元の FCS」「再計算」「追加する」
パケットフィルタ	設定されているパケットフィルタのフィルタ名です。
コンテンツ	データ置換アイテムの有無を表示します。データの置換が設定されている場合は「置換あり」、ない場合は「置換なし」と表示されます。
開始時刻	再生開始時刻です。
終了時刻	再生終了時刻です。再生中、一時停止中は「--」になります。
持続時間	再生を開始してから終了までの累計時間です。
状態	再生中は「リプレイ中」、一時停止すると「一時停止中」、停止すると「停止中」になります。

### 10.3.1. リプレイの開始・停止

トラフィックの再生を開始する場合は、「リプレイの開始」ボタン(前頁図⑥)をクリックしてください。下図の「確認」ダイアログが表示されます。



「はい」をクリックすると再生が開始され、プロファイル・ペインの表示が▶に変わります。

「リプレイの終了」ボタンをクリックすると再生が終了します。

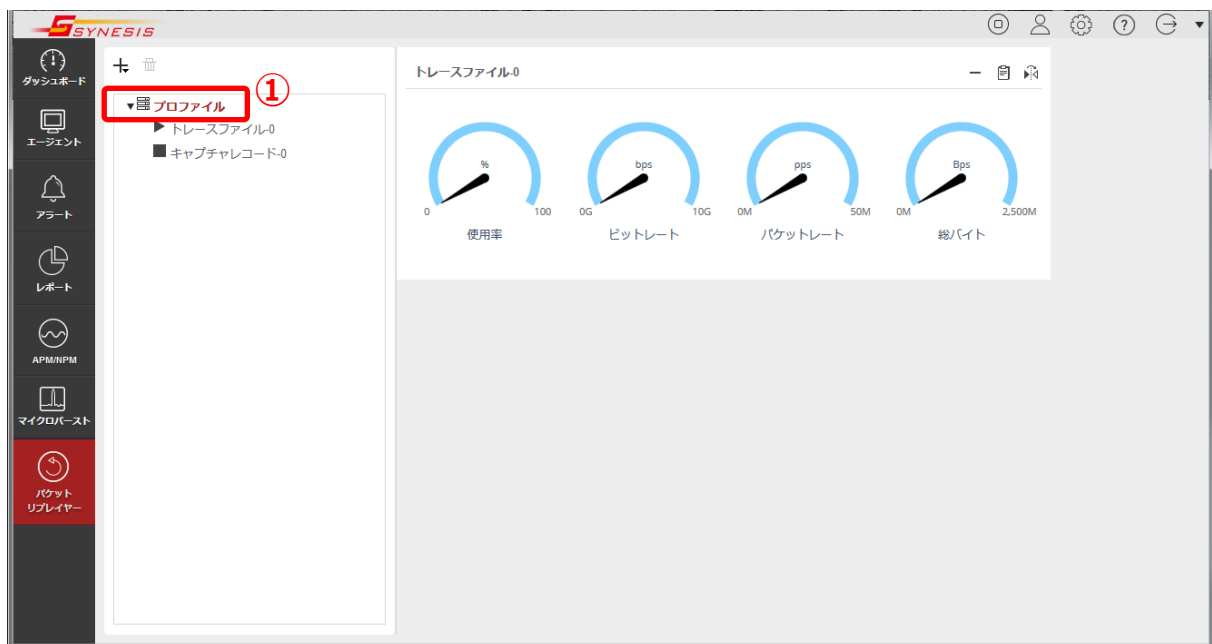
### 10.3.2. リプレイの一時停止

「一時停止」ボタンをクリックすると再生が一時停止状態となります。

「リプレイの開始」ボタンを押すと、一時停止状態が解除され、停まっていた部分からトラフィックの再生が開始されます。

## 10.4. オーバービュー画面

プロファイルの再生中、プロファイル・ペインの「プロファイル」ノード(下図①)をクリックすると、全てのプロファイルのステータスが確認できるオーバービュー画面が表示されます。

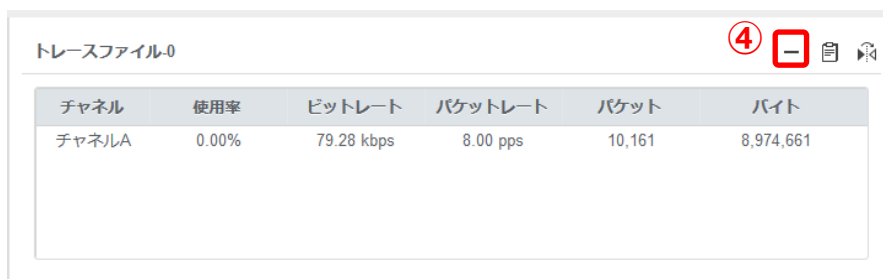


画面には再生中のプロファイルのダッシュボード(下図)が表示されます。



「Detail」📄ボタン(上図②)をクリックすると、オーバービュー画面からボタンをクリックしたプロファイルのワークスペース画面に移動します。

「Flip」🔄ボタン(上図③)をクリックすると、ダッシュボード表示が下図の指標テーブルの表示に切り替わります。



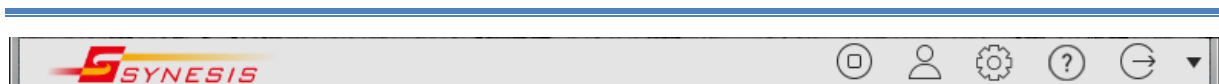
もう一度「Flip」🔄ボタンをクリックすると、指標テーブルがダッシュボード表示に戻ります。


「Size-Min」📄ボタン(図④)をクリックすると、ダッシュボードの表示が折り畳まれます。



「Size-Max」📄ボタン(図⑤)をクリックすると、元の表示に戻ります。

## 11. パスワードの変更



パスワードの変更を行う場合は、画面右上、ツールバー上の  アイコンをクリックします。  
以下の「アクティブユーザプロフィール」画面が表示されます。

● アクティブユーザプロフィール

ユーザー名 \*

パスワード \*

新規パスワード \*

パスワードの確認 \*

名 \*

姓 \*

「パスワード」欄に現在のパスワードを入力してください。

「新規パスワード」欄に新しいパスワードを、「パスワードの確認」欄に「新規パスワード」欄に入力したものと同じ新しいパスワードを入力し、「保存」ボタンをクリックしてください。


パスワードが新しいパスワードに変更されます。

パスワード以外にも、表示名の変更が行えます。ID は変更できません。

ここで変更できるのはサインインしているユーザプロフィールのみです。新規ユーザの追加や他ユーザの登録情報の変更を行いたい場合は、**12.3 ユーザ**を参照してください。

## 12. 構成

ツールバーメニュー「構成」は Synesis の各種設定項目が集められたメニューです。

Synesis 画面右上ツールバーの  アイコンをクリックすると、以下の画面が表示されます。



画面左に「構成」内の設定メニューが一覧で表示されます。

利用したいメニューをクリックすると、そのメニューのワークスペースに移動します。

メニューは以下の 17 項目です。

節番号	メニュー名	説明
12.1	Synesis の初期化	Synesis を初期化します。
12.2	設定のバックアップ・リストア	Synesis の設定のバックアップファイルを作成できます。外部のストレージに保存することも可能です。
12.3	ユーザ	Synesis にアクセスできるユーザの登録・管理が行えます。
12.4	時刻同期	時刻同期を取る NTP サーバの登録・管理が行えます。
12.5	アドレス帳	IP アドレスに名前をつけて登録・管理することができます。 登録された IP アドレスは登録した名前に置換して表示されます。
12.6	保存フィルタ	キャプチャ後のパケットに適用されるフィルタ設定の登録・管理が行えます。
12.7	トレースの保存	キャプチャレコードをトレースファイルとして保存する際のファイルサイズの上限を指定します。
12.8	アラート	アラート発生条件の登録・管理が行えます。

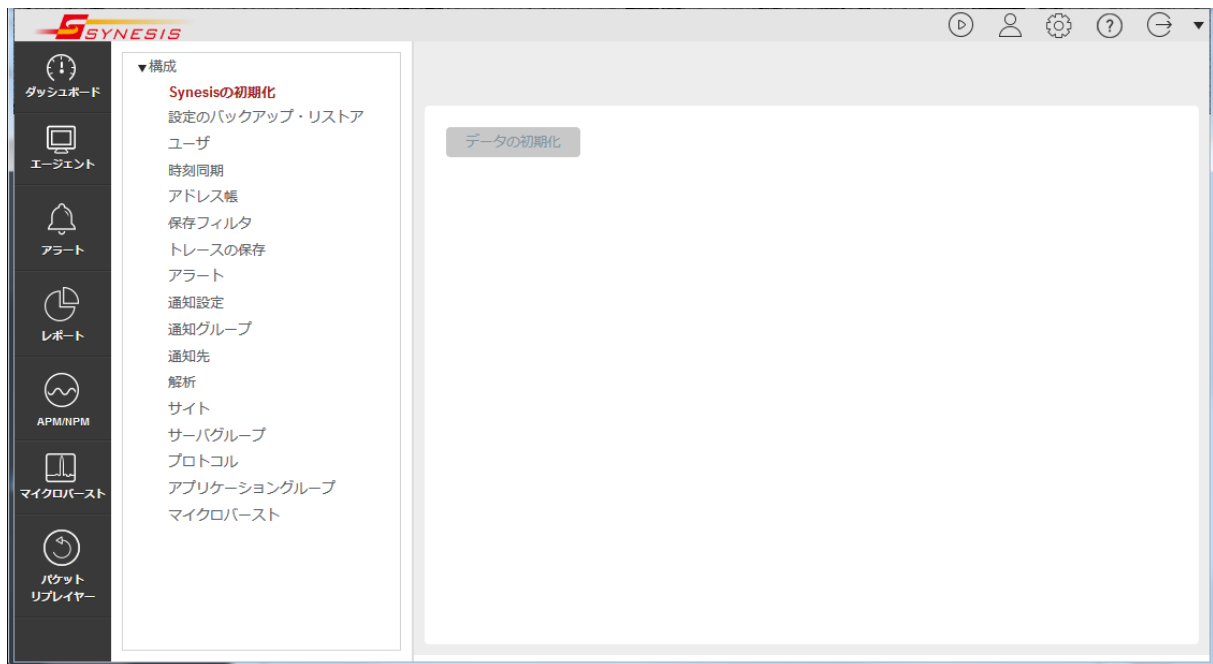
<b>12.9</b>	<b>通知設定</b>	アラート発生時または周期レポート作成時など、通知が設定されているものが一覧で確認できます。
<b>12.10</b>	<b>通知グループ</b>	アラート発生時または周期レポート生成時の通知先として指定する通知グループの登録・管理が行えます。
<b>12.11</b>	<b>通知先</b>	通知グループに登録できる連絡先の登録・管理が行えます。
<b>12.12</b>	<b>解析</b>	キャプチャ時のリアルタイム解析の有効/無効を設定します。
<b>12.13</b>	<b>サイト</b>	送信元 IP アドレスをサブネットでグループ化し、名前をつけて登録・管理することができます。 登録されたサイトは登録した名前に置換して表示されます。
<b>12.14</b>	<b>サーバグループ</b>	送信先 IP アドレス(サーバグループ)に名前をつけて登録・管理することができます。 登録されたサーバグループは登録した名前に置換して表示されます。
<b>12.15</b>	<b>プロトコル</b>	アプリケーションプロトコルのポート番号に名前をつけて登録・管理します。
<b>12.15</b>	<b>プロトコル</b>	登録したプロトコル(ポート番号)をグループ化して管理します。
<b>12.17</b>	<b>マイクロバースト</b>	リアルタイム解析用マイクロバースト閾値を設定します。

詳細は本章の各節を参照してください。



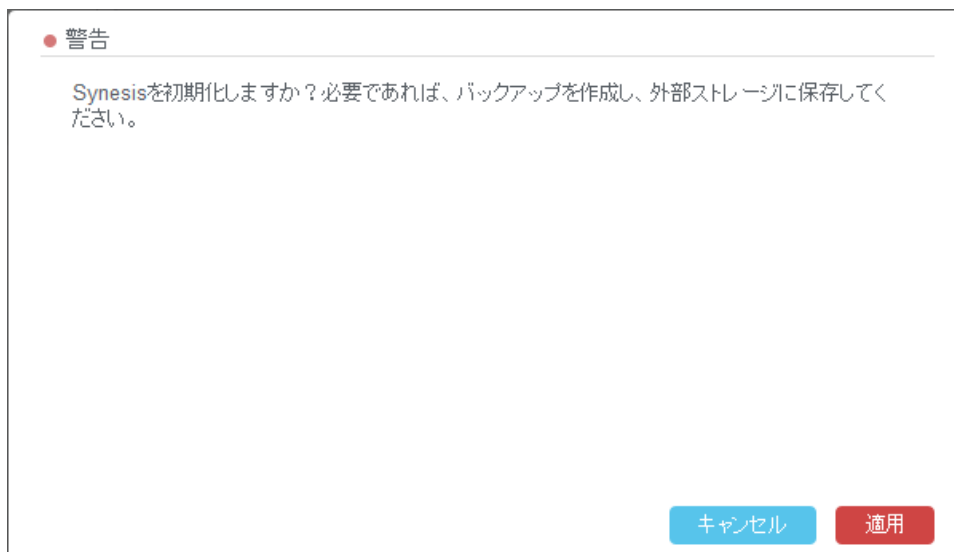
## 12.1. Synesis の初期化

Synesis を初期化します。



初期化を実行したい場合は「データの初期化」ボタンをクリックしてください。

確認のため、下図の警告メッセージが表示されます。



初期化を実行する場合は「適用」ボタンをクリックしてください。

キャプチャレコードや統計情報、ユーザ設定などのデータが消え、設定が初期化されます。

実際に初期化される項目については次頁 **12.1.1 初期化対象一覧**を参照してください。

キャプチャ中のパケットデータは読み出せない状態で残ります。パケットデータを消したい場合は、別途弊社にお問い合わせください。

必要があればバックアップを作成し、外部ストレージに保存してください。

バックアップについての詳細は **12.2 設定のバックアップ・リストア**を参照してください。

### 12.1.1. 初期化対象一覧

初期化される項目は以下の通りです。

ダッシュボード	概要	ダッシュボード	グラフ		
エージェント	概要	全てのエージェント	Default Agent	オプション	共通
					キャプチャフィルタ設定
					ロックトリガ設定
					自動保存設定※
					チャンネル設定
					通知設定
	レコード				
レポート	ロック				
	トレースファイル	ビルドインファイル			
		カスタムファイル ※			
		トレースバンカー			
	外部データソース				
APM/NPM	レポートリスト				
	レポートテンプレート				
	レポートプラン				
マイクログラフ	APM 解析				
	NPM 解析				
マイクログラフ					
バケット リプレイヤー	プロファイル	トレースファイル			
		キャプチャレコード			
構成	設定のバックアップ ・リストア				
	ユーザ				
	時刻同期				
	アドレス帳				
	保存フィルタ				
	トレースの保存				
	アラート				
	通知設定				
	通知グループ				
	通知先				
	解析				
	サイト				
	サーバグループ				
	プロトコル				
	アプリケーショングループ				
	マイクログラフ				

※トレースファイルの保存先として “/pvc/data/databank” とその下のディレクトリ以外を指定した場合は、初期化後もディスク内にファイルが残ります。ディスク内に残ったトレースファイルはカスタムファイルタブには表示されませんが、OS から確認し、操作することができます。

## 12.2. 設定のバックアップ・リストア

Synesis の設定を一括で抽出してバックアップファイルを作成、外部ストレージに保存することができます。バックアップファイルを読み込んで、設定を戻すこともできます。



作成された設定のバックアップファイルと、外部から読み込んだバックアップファイルが一覧で表示されます。表示される情報は「名前」「説明」「バージョン」「作成日時」です。

ここでバックアップファイルとして保存できるのは「構成」メニューなどで設定した項目です。詳細は **12.2.4 バックアップ対象一覧** を参照してください。

キャプチャデータや解析結果、レポートなどは保存できませんので、個別に保存してください。

### 12.2.1. 設定のバックアップ作成とダウンロード

Synesis の設定のバックアップファイルを作成したい場合は、「バックアップ」ボタンをクリックしてください。下図のバックアップダイアログが表示されます。

ファイル名を入力して「適用」ボタンをクリックしてください。Synesis のディスク内に設定のバックアップファイルが ZIP 形式で保存され、一覧に追加されます。

一覧に追加されたバックアップファイルの「名前」欄のリンクをクリックしてください。

下図の「バックアップ」ダイアログが表示されます。



「ダウンロード」ボタンをクリックすると、設定ファイルを外部ストレージに保存できます。

Synesis 初期化後、外部に保存した設定ファイルを再度読み込んでください。

### 12.2.2. 設定のリストア

Synesis を初期化した後で、外部ストレージに保存したバックアップファイルを読み込ませ、設定を戻すことができます。

「アップロード」ボタンをクリックすると、「アップロード」ダイアログが表示されますので、「参照」で外部に保存したバックアップファイルを選択してください。



「アップロード」ボタンをクリックすると、バックアップファイルが一覧に追加されます。

読み込んだファイルのチェックボックスにチェックを入れ、「リストア」ボタンをクリックしてください。Synesis の各設定項目がバックアップアップファイルから読み込まれます。

リストア実施後は Synesis を再起動してください。

### 12.2.3. バックアップファイルの削除

バックアップファイルを削除したい場合は、削除したいバックアップファイルのチェックボックスにチェックを付けて、「削除」ボタンをクリックしてください。選択したバックアップファイルが削除されます。

## 12.2.4. バックアップ対象一覧

バックアップファイルで保存される項目は以下の通りです。

ダッシュボード	概要	ダッシュボード	グラフ		
エージェント	概要	全てのエージェント	Default Agent	オプション	共通
					キャプチャフィルタ設定
					ロックトリガ設定
					自動保存設定
					チャンネル設定
					通知設定
レポート	レポートテンプレート				
	レポートプラン				
パケット リプレイヤー	プロファイル	トレースファイル ※			
		キャプチャレコード※			
構成	ユーザ				
	時刻同期				
	アドレス帳				
	保存フィルタ				
	トレースの保存				
	アラート				
	通知設定				
	通知グループ				
	通知先				
	解析				
	サイト				
	サーバグループ				
	プロトコル				
	アプリケーション グループ				
	マイクロバースト				

※パケットリプレイヤーのプロファイルの設定はバックアップで保存されますが、トレースファイル及びキャプチャレコードなどのデータファイルはバックアップ対象外のため、リストアした後はプロファイルのソースファイルを選択し直してください。

トレースファイルはバックアップ時にトレースファイルを外部ストレージに保存し、リストア後にトレースファイルをアップロードすることで、初期化前と同じパケットが送信できます。

キャプチャレコードは外部ストレージに保存できません。必要な場合はトレースファイルに保存して外部ストレージに保存してください。

## 12.3. ユーザ

「ユーザ」画面では Synesis にアクセスできるユーザの追加・管理が行えます。

「構成」メニューの「ユーザ」を選択すると、登録済みのユーザが一覧で表示されます。

新規

削除

<input type="checkbox"/>	名前	フルネーム	ロール
<input type="checkbox"/>	<a href="#">Test</a>	Test Synesis	ユーザ
<input type="checkbox"/>	<a href="#">Test1</a>	Test1 Synesis	管理者

表示される情報は「名前（登録 ID）」、「フルネーム」、「ロール」です。

サポートされている「ロール」は「管理者」と「ユーザ」です。「管理者」は Synesis の全ての機能を利用できますが、「ユーザ」は主に解析・参照機能が使えるのみです。

詳細は以下の表をご参照ください。

項目	機能制限
管理者	なし
ユーザ	<ul style="list-style-type: none"><li>・キャプチャを開始/終了できない。</li><li>・ツールバーの「構成」メニューが利用できない。 ユーザの新規登録・管理/Synesis の初期化・バックアップ/通知先設定 など</li><li>・キャプチャレコードを削除できない。</li><li>・キャプチャレコードのロック(保護)の設定・解除が行えない。</li><li>・統計値の CSV ファイルを作成できない。</li><li>・キャプチャオプションの登録・設定が行えない。 アダプタ選択/スライス機能/キャプチャフィルタ/ロック設定/通知設定 など</li><li>・ユーザの新規登録・管理が行えない。</li><li>・解析用の保存フィルタの新規作成・編集が行えない。</li><li>・キャプチャレコードの外部書き出しが行えない。</li><li>・外部データソースからのデータ読み込みが行えない。</li><li>・外部データソースから読み込んだデータの削除、有効化/無効化ができない。</li><li>・外部からのトレースファイルの読み込み・参照が行えない。</li><li>・外部から読み込んだトレースファイルの削除が行えない。</li><li>・パケットリプレイヤーのプロファイルの作成・設定変更・再生が行えない。</li></ul>

「ユーザ」のロールで利用できるのは参照・解析機能です。

キャプチャ中のトラフィックの確認、トレースファイル作成とダウンロード、登録済みの設定を利用したのキャプチャデータの各種解析とレポート作成などが利用できます。

### 12.3.1. ユーザの新規登録と登録情報の編集

ユーザを新規登録したい場合はユーザリストの左上の「新規」ボタンをクリックしてください。

下記のユーザプロフィールダイアログが表示されます。



The image shows a 'User Profile' dialog box. It has a title bar with a red dot and the text 'ユーザプロフィール'. Inside, there are several input fields: 'ユーザー名\*' (User Name), 'パスワード\*' (Password), 'パスワードの確認\*' (Confirm Password), '名\*' (First Name), '姓\*' (Last Name), and 'ロール' (Role) which is a dropdown menu currently showing '管理者' (Administrator). At the bottom right, there are two buttons: 'キャンセル' (Cancel) in a light blue box and '保存' (Save) in a red box.

入力する項目は、「ユーザ名」「パスワード」「パスワードの確認」「名」「姓」「ロール」です。

「パスワードの確認」には「パスワード」に入力したものと同じものを入力してください。

「保存」ボタンをクリックすると設定が保存され、ユーザ管理画面に戻ります。

登録済みのユーザの登録情報を編集したい場合は、登録ユーザ一覧表の名前のリンク部分をクリックしてください。ユーザプロフィールダイアログが表示され、ユーザ名以外の登録情報を変更できます。

### 12.3.2. ユーザの削除

ユーザを削除したい場合は、削除したいユーザの左側のチェックボックスにチェックを付けて「削除」ボタンをクリックしてください。

すべての登録ユーザを一度に削除したい場合は、項目名欄「名前」の左側のチェックボックスにチェックをつけて「削除」ボタンをクリックしてください。デフォルトユーザ（Synesis）以外のユーザが一度に削除されます。

## 12.4. 時刻同期

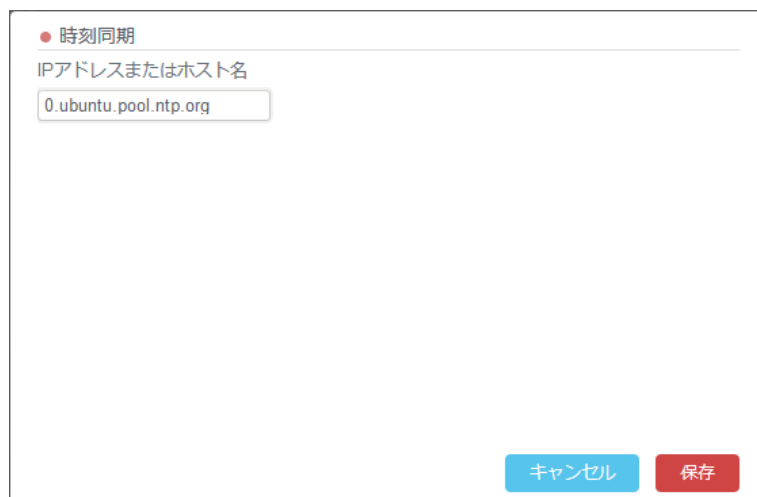
どの NTP サーバと時刻同期を取るかを設定できます。

NTP サーバ以外を利用した PPS 同期や PTP 同期を取る場合は、**Appendix E タイムサーバとのインテグレーション**を参照してください。



デフォルトでは上図にある4つの ubuntu サーバが登録されています。

変更したい NTP サーバのリンクをクリックしてください。「時刻同期」ダイアログが表示されます。



編集・入力を終えたら「保存」ボタンをクリックしてください。

NTP サーバを新規登録したい場合は、「新規」ボタンをクリックしてください。

登録済みの NTP サーバを削除したい場合は、削除したい NTP サーバのチェックボックスにチェックを入れて「削除」ボタンをクリックしてください。選択した NTP サーバがリストから削除されます。

利用したい NTP サーバを登録したら画面左上のスイッチをクリックして、**ON** に切り替えてください。設定内容が反映され、時刻同期が開始されます。

ON にした後で登録内容を変更した場合は、スイッチを一度 OFF にしてから ON に戻してください。

「リセット」ボタン (図①)をクリックすると、NTP サーバのリストが初期状態(図②)に戻り、時刻同期が停止します。

V3.1 以前の Synesis では NTP サーバリストが登録されていません。V3.1 以前の Synesis からバージョンアップを実行した場合は、「リセット」を実行して NTP サーバリストを登録してください。



## 12.5. アドレス帳

「アドレス帳」画面では登録されている IP アドレスと名前が一覧で確認できます。

登録された「IP アドレス」は登録された「名前」に変換されて表示されます。

<input type="checkbox"/>	名前	IPアドレス
<input type="checkbox"/>	<a href="#">Host 1</a>	192.168.0.1
<input type="checkbox"/>	<a href="#">Host 2</a>	192.168.0.2

新しく IP アドレスを登録したい場合は、「新規」ボタンをクリックしてください。下図の「アドレス帳」ダイアログが表示されます。

● アドレス帳

名前

IPv4もしくはIPv6アドレス

キャンセル

保存

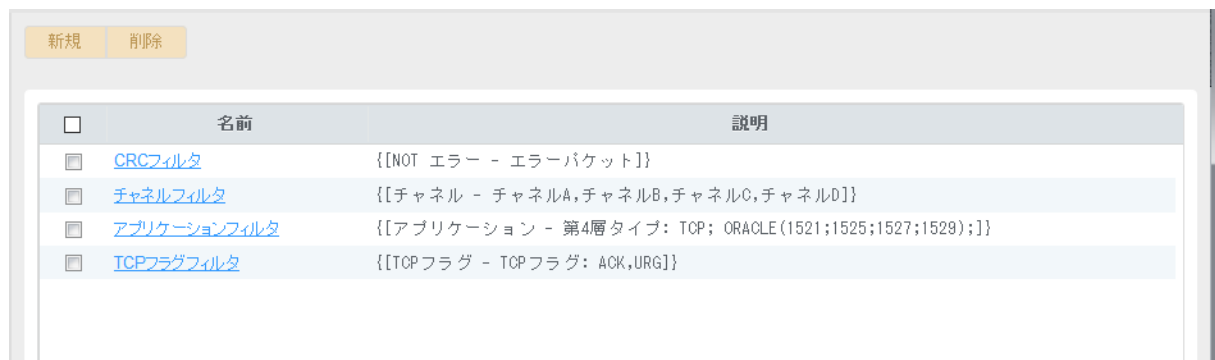
「名前」欄に置換表示させたい名前を、「IPv4 もしくは IPv6 アドレス」欄に IP アドレスを入力してください。「保存」ボタンをクリックすると、入力した IP アドレスが一覧に追加されます。

登録されているアドレスを変更したい場合は、名前の部分をクリックしてください。新規登録時にも表示された「アドレス帳」ダイアログで名前とアドレスを編集することができます。

登録したアドレスを削除したい場合は、それぞれの名前の横にあるチェックボックスにチェックを入れて、「削除」ボタンをクリックしてください。選択されていたひとつ、または複数のアドレスが削除されます。

## 12.6. 保存フィルタ

「保存フィルタ」メニューではキャプチャ後のパケットに適用するフィルタを作成・管理します。



「保存フィルタ」画面には登録済みのフィルタが一覧形式で表示されます。情報として「名前」とフィルタの種類と設定が記された「説明」が確認できます。

キャプチャ時に適用されるキャプチャフィルタの設定・管理については **5.3.1.2.キャプチャオプション**と **Appendix B キャプチャフィルタの種類と設定方法**を確認してください。

### 12.6.1. 保存フィルタの新規登録


フィルタを新規作成する場合は、「新規」ボタンをクリックしてください。下記のフィルタダイアログボックスが表示されます。

A screenshot of the 'Save Filter' dialog box. It has a title bar with a red dot and the text '保存フィルタ'. Below the title bar, there is a '名前' (Name) label and a text input field containing 'フィルタ'. Below that is a 'モード' (Mode) label and a dropdown menu showing '通常' (Normal). Below the dropdown is a large text area containing 'なし' (None) and an edit icon (pencil). At the bottom right, there are two buttons: 'キャンセル' (Cancel) and '保存' (Save).

「名前」欄に登録するフィルタの名前を入力してください。

「モード」でフィルタ定義方法を選択できます。選択項目は以下の通りです。

項目	説明
通常	フィルタ項目を 1 つ設定します
詳細設定	複数個のフィルタ項目を設定して、それらの論理関係を定義します。

「なし」とあるのはフィルタ項目の欄です。右側の  (編集)アイコンをクリックすると、「フィルタ項目」ダイアログが表示されて、フィルタタイプを選んで設定することができます。「適用」ボタンをクリックすると、設定した内容がこの欄に表示されます。

設定可能なフィルタは以下の 12 種類です。(詳細は本項の各項目を参照してください)

フィルタの種類	説明
チャンネル	アダプタ上のチャンネルでフィルタリングします。
エラー	エラーが含まれたパケットをフィルタリングします。対象となるエラーは CRC,フラグメント,ジャバー,オーバーサイズ,ラントの 5 種類です。
パケットサイズ	パケットサイズの範囲でフィルタリングします。
MAC アドレス	送信元・送信先の MAC アドレスでフィルタリングします。
VLAN	特定の VLAN ID をフィルタリングします。
L2 イーサタイプ	L2 イーサタイプのプロトコル(ポート番号)でフィルタリングします。
L3 プロトコル	L3 プロトコル(ポート番号)でフィルタリングします。
フロー	特定の IP アドレスを含むフローのパケットをフィルタリングします
TCP フラグ	TCP ヘッダ内に特定のフラグが含まれるパケットをフィルタリングします。
TCP ウィンドウサイズ	TCP ヘッダのウィンドウサイズでフィルタリングします。
アプリケーション	特定のアプリケーションのパケットをフィルタリングします。
パターン	パケット中に特定のパターンを含むものをフィルタリングします。



## フィルタの詳細設定

詳細設定では複数のフィルタ項目を定義して、それらを関係論理演算子の「AND」「OR」「NOT」で組み合わせることにより、より複雑なフィルタリングを行えます。

● フィルタ

名前



モード 詳細設定

チャンネル ☐ NOT  

▼

チャンネルA

AND



フロー ☐ NOT  

▼

Any --> 192.168.0.1

+ フィルタ項目の追加

OR

VLAN ☐ NOT  

▼

VLAN ID: 200

+ フィルタ項目の追加

横方向に並べた条件が AND で結合されます。また、縦方向に並べた条件が OR で結合されます。既存フィルタの右側または下にある「+ フィルタ項目の追加」をクリックすると、フィルタ項目が新たに 1 つ追加されます。また条件の否定は NOT のチェックボックスで設定します。

### 12.6.1.1 チャンネル

アダプタ上のチャンネルでフィルタリングします。

● フィルタ項目

**チャンネル**

エラー

パケットサイズ

MACアドレス

VLAN

L2イーサタイプ

L3プロトコル

フロー

TCPフラグ

TCPウィンドウサイズ

アプリケーション

パターン

☐ チャンネルA

☐ チャンネルB

☐ チャンネルC

☐ チャンネルD

☐ チャンネルE

☐ チャンネルF

☐ チャンネルG

☐ チャンネルH

すべて選択 選択の解除

キャンセル 適用

チェックボックスにチェックの入ったチャンネルがフィルタリングされます。

「すべて選択」ボタンをクリックすると、すべてのチャンネルにチェックが入った状態になります。

「選択の解除」ボタンをクリックすると、入っていたチェックがすべて外されます。

### 12.6.1.2 エラー

エラーが含まれたフレームをフィルタリングします。

● フィルタ項目

チャンネル

**エラー**

パケットサイズ

MACアドレス

VLAN

L2イーサタイプ

L3プロトコル

フロー

TCPフラグ

TCPウィンドウサイズ

アプリケーション

パターン

☐ CRC

☐ フラグメント

☐ ジャバ

☐ オーバーサイズ

☐ ラント

すべて選択 選択の解除

キャンセル 適用

対応するエラーはCRC、フラグメント、ジャバ、オーバーサイズ、ラントの5種類です。

チェックボックスにチェックを入れたエラーがフィルタリングされます。

なお、モデル(アダプタの種類)によっては保存フィルタのエラーフィルタは適用できません。

詳細は **Appendix H モデルによる違い**を確認してください。

### 12.6.1.3 パケットサイズ

パケットサイズの範囲でフィルタリングします。

● フィルタ項目

チャンネル  
エラー  
**パケットサイズ**  
MACアドレス  
VLAN  
L2イーサタイプ  
L3プロトコル  
フロー  
TCPフラグ  
TCPウィンドウサイズ  
アプリケーション  
パターン

モード >= - <=  
値  -  バイト

◀ 111 ▶

キャンセル

適用

モード	パケットサイズの指定に使用する等号、または不等号を以下から選択します。 「>=」, 「==」, 「<=」, 「>= かつ <=」
値	不等号の境界値をバイト単位で入力します。

### 12.6.1.4 MAC アドレス

解析に含める、もしくは除く送信元/送信先 MAC アドレスを指定します。

● フィルタ項目

チャンネル  
エラー  
パケットサイズ  
**MACアドレス**  
VLAN  
L2イーサタイプ  
L3プロトコル  
フロー  
TCPフラグ  
TCPウィンドウサイズ  
アプリケーション  
パターン

送信元  
MACアドレス   
コロン (:) を使って入力してください。例 01:23:45:67:89:ab

方向  
-->

送信先  
MACアドレス   
コロン (:) を使って入力してください。例 01:23:45:67:89:ab

◀ 111 ▶

キャンセル

適用

送信元/送信先 MAC アドレス	16 進数(HEX)で送信元と送信先の MAC アドレスを入力します。 このフィールドをブランクにすると、全ての MAC アドレスが対象になります。
方向の選択	「-->」「<--」「<-->」から、送信元と送信先のパケットの方向を選びます。

123 / 185

### 12.6.1.5 VLAN

特定の VLAN ID をフィルタリングします。

The screenshot shows a configuration window titled "フィルタ項目" (Filter Items). On the left is a list of filter categories: チャンネル, エラー, パケットサイズ, MACアドレス, **VLAN**, L2イーサタイプ, L3プロトコル, フロー, TCPフラグ, TCPウィンドウサイズ, アプリケーション, and パターン. The "VLAN" item is selected and highlighted in red. To the right of this list is a text input field labeled "VLAN ID". Below the input field is an example: "例: 1; 2; 3-4; 5; 6". At the bottom right of the window are two buttons: "キャンセル" (Cancel) and "適用" (Apply).

フィルタリングしたい VLAN ID を 0 以上 4095 以下の数値で指定してください。

### 12.6.1.6 L2 イーサタイプ

L2 イーサタイプのプロトコルのポート番号でフィルタリングします。

The screenshot shows a configuration window titled "フィルタ項目" (Filter Items). On the left is a list of filter categories: チャンネル, エラー, パケットサイズ, MACアドレス, VLAN, **L2イーサタイプ**, L3プロトコル, フロー, TCPフラグ, TCPウィンドウサイズ, アプリケーション, and パターン. The "L2イーサタイプ" item is selected and highlighted in red. To the right of this list are two list boxes. The left list box contains the following items: IPv4 (0x0800), ARP (0x0806), VLAN (0x8100), and IPv6 (0x86DD). Between the two list boxes are two red circular buttons with white arrows: ">>" and "<<". The right list box is currently empty. Below the list boxes is a text input field labeled "編集:" (Edit:). Below the input field is an example: "例: 0806; 0x0842; 0x0843; 0x0844-0x0845". At the bottom right of the window are two buttons: "キャンセル" (Cancel) and "適用" (Apply).

右側の欄(デフォルトでは空欄)にリストアップされたプロトコルがフィルタとして適用されます。

左側のリストから適用したいプロトコルを選んで **>>** アイコンをクリックしてください。選んだプロトコルが右側のリストに追加されます。


右側のリストから外すには、外したいプロトコルを選んで **<<** アイコンをクリックしてください。


指定したいポート番号がリストにない場合は、「編集」欄に 16 進数で入力してください。

### 12.6.1.7 L3 プロトコル

L3 プロトコルのポート番号でフィルタリングします。

右側の欄(デフォルトでは空欄)にリストアップされたプロトコルがフィルタとして適用されます。

左側のリストから適用したいプロトコルを選んで  アイコンをクリックしてください。選んだプロトコルが右側のリストに追加されます。

右側のリストから外すには、外したいプロトコルを選んで  アイコンをクリックしてください。

指定したいポート番号がリストにない場合は、「編集」欄に 10 進数で入力してください。

### 12.6.1.8 フロー

特定の IP アドレスを含むフローのパケットをフィルタリングします。

● フィルタ項目

チャンネル  
エラー  
パケットサイズ  
MACアドレス  
VLAN  
L2イーサタイプ  
L3プロトコル  
**フロー**  
TCPフラグ  
TCPウィンドウサイズ  
アプリケーション  
パターン

送信元 IPアドレス

ポート

Any

Any

例 : 172.23.1.1, 192.168.1.0/24, 2001:DB8::8:800:200C:417A 例: 1; 2; 3-4

方向

-->

送信先 IPアドレス

ポート

Any

Any

例 : 172.23.1.1, 192.168.1.0/24, 2001:DB8::8:800:200C:417A 例: 1; 2; 3-4

キャンセル

適用

項目	説明
送信元 IP アドレス、送信先 IP アドレス	送信元/送信先となる IPv4 または IPv6 アドレスを数値で入力します。サブネットマスクは '/' を付加することで追加できます (192.168.1.0/24, 2001:1111:2222:3333:0000:0000:0000:0000/64 等)。
方向	パケットの方向を指定します。 送信 '-->'、受信 '<--'、送受信両方 '<-->' から選択します。
送信元ポート、送信先ポート	送信元または送信先となる TCP ポートの番号を 0 以上 65535 以下の数値で入力します。複数のポートを指定する場合は ';' で区切ってポート番号を入力し、範囲で指定する場合は間を '-' (半角マイナス) でつないでください。



### 12.6.1.9 TCP フラグ

TCP ヘッダ内に特定のフラグが含まれるパケットをフィルタリングします。

The screenshot shows a configuration window titled "フィルタ項目" (Filter Item). On the left is a list of filter categories: チャンネル, エラー, パケットサイズ, MACアドレス, VLAN, L2イーサタイプ, L3プロトコル, フロー, TCPフラグ (highlighted in red), TCPウィンドウサイズ, アプリケーション, and パターン. On the right, under the "TCPフラグ" section, there are six checkboxes: URG, ACK, PSH, RST, SYN, and FIN. At the bottom right of the window are two buttons: "キャンセル" (Cancel) and "適用" (Apply).

下記の6種類から、1つ以上にチェックをいれます。

- URG, ACK, PSH, RST, SYN, FIN

### 12.6.1.10 TCP ウィンドウサイズ

TCP ヘッダのウィンドウサイズでフィルタリングします。

The screenshot shows a configuration window titled "フィルタ項目" (Filter Item). On the left is a list of filter categories: チャンネル, エラー, パケットサイズ, MACアドレス, VLAN, L2イーサタイプ, L3プロトコル, フロー, TCPフラグ, TCPウィンドウサイズ (highlighted in red), アプリケーション, and パターン. On the right, under the "TCPウィンドウサイズ" section, there is a text input field with the value "0-65535" and a label "TCPウィンドウサイズ". At the bottom right of the window are two buttons: "キャンセル" (Cancel) and "適用" (Apply).

「TCP ウィンドウサイズ」を0以上65535以下の数値で指定してください。

### 12.6.1.11 アプリケーション

特定のアプリケーションのパケットをフィルタリングします。

● フィルタ項目

チャンネル  
エラー  
パケットサイズ  
MACアドレス  
VLAN  
L2イーサタイプ  
L3プロトコル  
フロー  
TCPフラグ  
TCPウィンドウサイズ  
**アプリケーション**  
パターン

☐ TCP ☐ UDP

BGP(179)  
DNS(53)  
EXCHANGE(135)  
FTP(21)  
FTP-DATA(20)  
GTP(2123;2152;3386)  
H.323(1720-1721)  
HTTP(80;443)  
LDAP(389;636)  
LDP(646)  
MEGACO(2944-2945)  
MGCP(2427;2727)  
MSSQL(1433)  
MySQL(3306)  
NFS(2049)  
ORACLE(1521;1525;1527;1529)  
OpenFlow(6653)  
OpenVPN(1194)  
PGSQL(5432)

>> <<

キャンセル 適用

「TCP」か「UDP」のどちらか、もしくは両方かを指定することが可能です。

右側の欄(デフォルトでは空欄)にリストアップされたプロトコルがフィルタとして適用されます。

左側のリストから適用したいプロトコルを選んで >> アイコンをクリックしてください。選んだプロトコルが右側のリストに追加されます。

右側のリストから外すには、外したいプロトコルを選んで << アイコンをクリックしてください。

### 12.6.1.12 パターン

パケット中に特定のパターンを含むものをフィルタリングします。

● フィルタ項目

チャンネル  
エラー  
パケットサイズ  
MACアドレス  
VLAN  
L2イーサタイプ  
L3プロトコル  
フロー  
TCPフラグ  
TCPウィンドウサイズ  
アプリケーション  
**パターン**

開始位置 フレームの先頭

オフセットタイプ ☒ 固定

オフセット  16進数 10進数

入力例 16進数:1c 10進数:28

パターン形式 16進数

パターン

マスク

キャンセル 適用

設定項目の詳細は以下の通りです。

項目	説明
開始場所	<p>パターンの一致を判定する位置を指定するのに、パケットのどの位置を "0" とするかを選択します。選択項目は以下の 3 種類です。</p> <p>「フレームの先頭」：フレームの先頭を "0" とします (プリアンブル除く)。</p> <p>「IP ヘッダ」：IP ヘッダの先頭を "0" とします。</p> <p>「アプリケーションヘッダ」：アプリケーションヘッダの先頭を "0" とします。</p>
オフセットタイプ	「固定」にチェックを入れて有効にすると、パターンの一致を判定する位置を「固定」します。無効の場合は、指定した位置以降のすべてのバイト列が対象となります。
	「固定」が無効： 「開始場所」と「オフセット」で指定された「以降のすべてのバイト列」でパターン一致を判定します。
	「固定」が有効： 「開始場所」と「オフセット」で指定されたバイト列のみでパターンの一致を判定します。
オフセット	<p>パケットの「開始場所」で指定された位置を "0" として、パターンの一致を判定する位置(バイト列)を指定します。(「固定」にチェックが入っていない場合は、パターン一致の判定を開始する位置になります。)</p> <p>形式は 16 進数と 10 進数のどちらかを右側のラジオボタンから選択できます。</p>
パターン形式	<p>パターン文字列の表示形式を指定します。</p> <p>「ASCII」または「16 進数」から選択します。</p>
パターン	一致文字列を「ASCII」または「16 進数」の文字列で指定します。
マスク	<p>「マスクパターン」を 16 進数(HEX)文字列で指定します。</p> <p>パターン形式が「16 進数」の場合のみ有効です。</p> <p>「パターン」と「マスクパターン」の AND がビットごとに計算され、「オフセット」のビット列が一致したパケットがフィルタリングされます。</p>

「パターン」と「マスク」の指定方法を具体的な例を用いて説明します。

例えば、「パターン」が "1F"、「マスク」が "F1" の場合、ビットごとの値は以下の通りです。

	16 進数	2 進数
パターン	1 F	0 0 0 1 1 1 1 1
マスク	F 1	1 1 1 1 0 0 0 1
AND 演算結果	1 1	0 0 0 1 0 0 0 1

パターンとマスクの AND は "11" になります。したがってオフセット位置のパターンが "11" のパケットのみが通過します。「パターン」が "1F" のフレームは通過しません。

「マスクパターン」で "0" のビットは "no care" ではないことにご注意ください。

## 12.6.2. 保存フィルタの削除



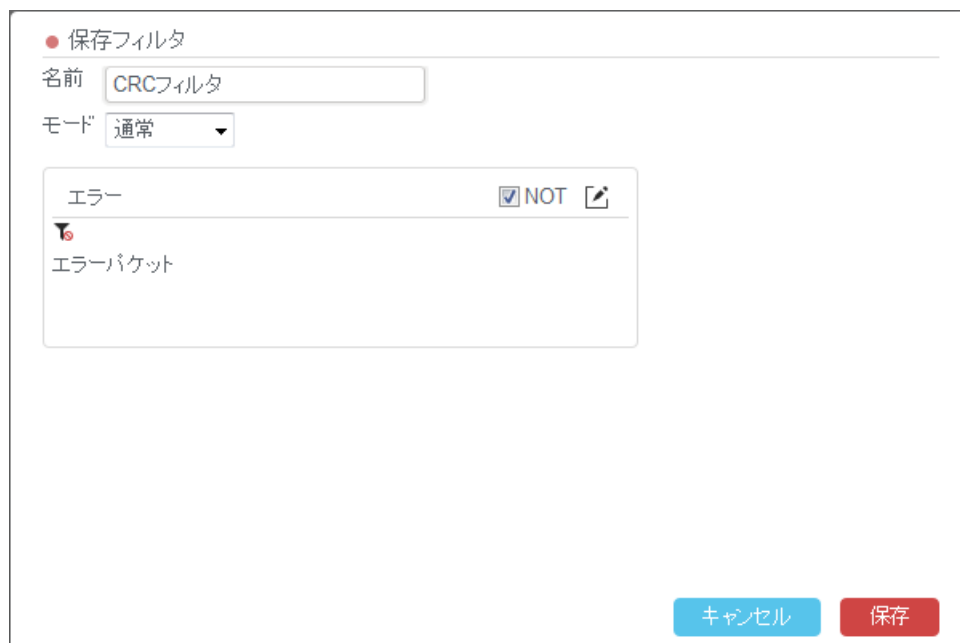
The screenshot shows a dialog box with two tabs: '新規' (New) and '削除' (Delete). The '削除' tab is active. It contains a table with two columns: '名前' (Name) and '説明' (Description). The table lists five filters, each with a checkbox in the '名前' column.

名前	説明
<input type="checkbox"/> <a href="#">CRCフィルタ</a>	{[NOT エラー - エラーパケット]}
<input type="checkbox"/> <a href="#">チャンネルフィルタ</a>	{[チャンネル - チャンネルA,チャンネルB,チャンネルC,チャンネルD]}
<input type="checkbox"/> <a href="#">アプリケーションフィルタ</a>	{[アプリケーション - 第4層タイプ: TCP; ORACLE(1521;1525;1527;1529);]}
<input type="checkbox"/> <a href="#">TCPフラグフィルタ</a>	{[TCPフラグ - TCPフラグ: ACK,URG]}
<input type="checkbox"/> <a href="#">フィルタ1</a>	{[L2 Ether Type - L2 Ether Type: IPv4; 0x0806] AND [L3 Protocol - L3 Protocol: TCP; ]} OR {[パケ...

登録されている保存フィルタを削除したい場合は、削除したい保存フィルタの左端のチェックボックスにチェックを入れて「削除」ボタンをクリックします。選択した保存フィルタが削除されます。登録済みのフィルタをまとめて削除したい場合は、一番上のチェックボックスにチェックを入れて、「削除」ボタンをクリックしてください。

## 12.6.3. 保存フィルタの編集

登録されている保存フィルタの設定を変更したい場合は、変更したい保存フィルタの「名前」欄のリンクをクリックしてください。「保存フィルタ」ダイアログが表示されます。



The screenshot shows the '保存フィルタ' (Save Filter) dialog box. It has a title bar with a red dot and the text '保存フィルタ'. Below the title bar, there are two input fields: '名前' (Name) with the value 'CRCフィルタ' and 'モード' (Mode) with a dropdown menu showing '通常'. Below these fields is a list box containing 'エラー' and 'エラーパケット'. To the right of the list box is a checkbox labeled 'NOT' which is checked, and a small icon. At the bottom right of the dialog box are two buttons: 'キャンセル' (Cancel) and '保存' (Save).

設定を変更して「保存」ボタンをクリックしてください。

設定方法は新規登録時と同じです。

## 12.7. トレースの保存

キャプチャレコードをトレースファイルとして保存するとき、トレースファイルを自動的に指定されたサイズ以下のファイルに分割して保存します。その分割ファイルサイズの上限を指定します。



The screenshot shows a dialog box with a title bar containing a yellow '編集' (Edit) button. The main area is a white box with the text '分割ファイルサイズの上限' (Maximum split file size limit) followed by a text input field containing '1024' and the unit 'MB (1-4096)'.

分割ファイルサイズの上限を変更したい場合は、「編集」ボタンをクリックしてください。

「分割ファイルサイズの上限」テキストボックスが編集可能になります。



This screenshot is identical to the previous one, but it includes two buttons at the bottom right: a blue 'キャンセル' (Cancel) button and a red '保存' (Save) button.

希望するファイルサイズの上限値を MB 単位で入力してください。

指定できるのは 1MB～4096MB です。

指定する数値を入力したら、「保存」ボタンをクリックしてください。

ここで設定する分割ファイルサイズの上限値は、「自動保存」のオートローテーション機能を利用して、トリガに「サイズ」を選択した場合の動作に影響を与えます。

影響するのはトリガで「サイズ」を選択した場合に、保存先フォルダとして設定されたプライマリフォルダで設定できる最小サイズです。

機能と設定項目の詳細は **5.3.1.2.4.2 オートローテーション** を参照してください。

## 12.8. アラート

アラート条件の追加・編集・削除を行います。

全てのアラート設定が表示されます。有効/無効の アイコンをクリックするとアラートの有効/無効化が切り替わります。

新しいアラートを追加する場合は、各タブ（DLC, ARP, NPM, APM）で「新規」ボタンをクリックし、必要なアラートパラメータを入力してください。

データソースには、**D.2 データソース**で示される項目に加えて“Any”が表示されます。All Channel Group とエージェントごとのチャンネルグループは表示されません。表示されるデータソースリストの中から、アラートに使用するエージェントまたはチャンネルグループを選択してください。

アラート設定を削除したい場合は、各アラート設定の左側のチェックボックスにチェックを入れてください。タブ中の全てのアラートを削除する場合はヘッダの「説明」の左側のチェックボックスにチェックを入れてください。「削除」ボタンをクリックするとチェックの入ったアラート設定が削除されます。

## 12.9. 通知設定

アラート発生時または周期レポート生成時の外部通知の設定が一覧で確認できます。

タイプ	名前	有効	通知グループ	通知先
Alarm	DLCアラート1	<input type="checkbox"/> OFF	グループ1	メール通知1 (test123@toyo.co.jp) Syslog通知1 (1.2.3.4:514) Trap通知1 (1.2.3.4:162)

アラート設定、または、周期レポート設定で通知を有効にて通知グループを登録すると、通知設定の一覧に設定内容が追加されます。新規登録された外部通知はデフォルトで有効に設定されます。

外部通知をしない場合は、一覧画面で ☒ ON ☐ アイコンをクリックして無効に設定します。

### アイコン説明：

- ・ ☐ OFF : 無効状態。クリックすると有効になります。
- ・ ☒ ON : 有効状態。クリックすると無効になります。

新しくアラート発生や周期レポート生成の外部通知を追加したい場合は、それぞれツールバー「構成」メニューのアラートやメインメニューのレポートから通知先を指定してください。

## 12.10. 通知グループ

エラー検知やレポート生成などのイベント発生を通知する先を「通知グループ」として登録し、管理します。登録した「通知グループ」は、アラートメニューなどで通知する先を設定すると、選択肢として表示されます。

The screenshot shows a web interface for managing notification groups. At the top, there are two buttons: '新規' (New) and '削除' (Delete). Below them is a table with the following columns: '名前' (Name), '説明' (Description), '通知先' (Notification Destination), and '通知テスト' (Notification Test). The table contains one entry named 'グループ1' (Group 1). The '説明' column for this entry lists three destinations: 'メール通知1 (test123@toyo.co.jp)', 'Syslog通知1 (1.2.3.4:514)', and 'Trap通知1 (1.2.3.4:162)'. To the right of the table, there is a '通知テスト' (Notification Test) button.

新しく通知グループを登録したい場合は画面左上の「新規」ボタンをクリックしてください。

下図の通知グループダイアログが表示されます。

The screenshot shows a dialog box titled '通知グループ' (Notification Group). It has a '名前\*' (Name\*) input field and a '説明' (Description) text area. Below these is a section for '通知先' (Notification Destination). On the left, there is a list of existing destinations: 'メール通知1 (test123@toyo.co.jp)', 'Syslog通知1 (1.2.3.4:514)', 'Trap通知1 (1.2.3.4:162)', 'メール通知2 (test234@toyo.co.jp)', 'Syslog通知2 (2.3.4.5:514)', and 'Trap通知2 (2.3.4.5:162)'. To the right of this list are two red circular buttons with white arrows: '>>' and '<<'. Further right is an empty list box. At the bottom left is a '通知先の作成' (Create Notification Destination) button. At the bottom right are 'キャンセル' (Cancel) and '保存' (Save) buttons.

右側のリストにある通知先が通知グループに登録されます。左側のリストから適用したい通知先を選んで >> アイコンをクリックしてください。選んだ通知先が右側のリストに追加されます。

右側のリストから外すには、外したい通知先を選んで << アイコンをクリックしてください。

通知グループに入りたい通知先が通知先リストにない場合は、「通知先の作成」ボタンをクリックしてください。通知先を追加することができます。詳細は次節を参照してください。

グループ登録後、「通知テスト」ボタンをクリックすると、テスト用の通知が発行され、正しく通知が届くかを確認することができます。



## 12.11. 通知先

個々の連絡先を「通知先」として登録管理します。

新規 削除 通知メール設定

<input type="checkbox"/>	名前	タイプ	有効
<input type="checkbox"/>	<a href="#">メール通知1</a>	eMail	<span>ON</span> <input type="checkbox"/>
<input type="checkbox"/>	<a href="#">Syslog通知1</a>	Syslog	<span>ON</span> <input type="checkbox"/>
<input type="checkbox"/>	<a href="#">Trap通知1</a>	SnmpTrap	<span>ON</span> <input type="checkbox"/>
<input type="checkbox"/>	<a href="#">メール通知2</a>	eMail	<span>ON</span> <input type="checkbox"/>
<input type="checkbox"/>	<a href="#">Syslog通知2</a>	Syslog	<span>ON</span> <input type="checkbox"/>
<input type="checkbox"/>	<a href="#">Trap通知2</a>	SnmpTrap	<span>ON</span> <input type="checkbox"/>

通知先を新規作成すると、デフォルトで有効に設定されます。


通知先を無効にしたい場合は、無効にしたい通知先の ON ☐ アイコンをクリックしてください。

### 12.11.1. 通知先の新規登録

新しく通知先を設定したい場合は「新規」ボタンをクリックしてください。

● 通知

Email

 名前\*

送信先アドレス\*

キャンセル 保存

通知先として Email, Syslog, Trap が選択可能です。

選択した通知方法ごとにパラメータを設定して、「保存」ボタンをクリックしてください。

登録した通知先がリストに追加されます。

#### Email

項目	説明
名前	通知リストに表示される説明文になります。
送信先アドレス	送信先の電子メールアドレスです。

メール通知に利用する SMTP サーバ等の設定は「通知メール設定」から行えます。

詳細は次節を参照してください。

## Syslog

項目	説明
名前	通知リストに表示される説明文になります。
サーバ	Syslog サーバの IP アドレスを指定してください。
UDP プロトコル	Syslog サーバの UDP ポート番号を指定してください。
危険度	通知する Syslog の Severity を、下記のいずれかから選択してください。 Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug

## Trap

項目	説明
名前	通知リストに表示される説明文になります。
通知先 IP アドレス	SNMP マネージャーの IP アドレスを指定してください。
ポート	SNMP マネージャーのポート番号を指定してください。
バージョン	SNMP のバージョン(1 または 2c)を選択してください。
コミュニティ	SNMP のコミュニティ ID を指定してください。

### 12.11.2. 通知メールのサーバ設定

メール通知に利用する SMTP サーバを設定します。

● 通知メール設定

SMTP ホスト\*

eqmail.com

SMTP ポート\*

25

SMTP アカウント

your account

SMTP パスワード

☐ SSL

差出人\*

sample@email.com

件名\*

Synesis通知

キャンセル

保存

各項目を設定したら、「保存」ボタンをクリックしてください。

## 12.12. 解析

キャプチャに対する解析パラメータを設定します。

編集

エージェント Default Agent ▼

モジュール

- ☒ APM解析
- ☒ NPM解析
- ☒ L2/L3 プロトコル
- ☐ マイクロバースト

上位のフロー 100 ▼

---

☒ データベースのエイジアウトを有効にする

解析データ削除範囲の基準日 2017/12/21

削除

設定を変更したい場合は「編集」ボタンをクリックしてください。

下図のように各項目が設定可能になります。

編集

エージェント Default Agent ▼

モジュール

- ☒ APM解析
- ☒ NPM解析
- ☒ L2/L3 プロトコル
- ☐ マイクロバースト

上位のフロー 100 ▼

---

☒ データベースのエイジアウトを有効にする

解析データ削除範囲の基準日 2017/12/21 

削除

キャンセル 保存

各項目の設定が完了したら「保存」ボタンをクリックしてください。

設定項目は以下の通りです。

項目	説明
エージェント	解析パラメータを設定するエージェントです。
モジュール	<p>どの自動解析を有効にするかを選択します</p> <p>APM 解析: APM 解析を有効にします。</p> <p>NPM 解析: NPM 解析を有効にします。</p> <p>L2/L3 プロトコル: L2/L3 プロトコル解析を有効にします。</p> <p>マイクロバースト: マイクロバースト解析を有効にします。</p> <p>なお、上記の自動解析項目内の1つでも選択すると、自動的に ARP 解析が有効になります。ARP 解析は ARP パケットをカウントする機能です。</p> <p>ARP パケットのカウント数は <b>12.8 アラート</b> でアラート閾値に設定可能です。</p>
上位のフロー	<p>グラフに表示するフローの数を指定します。20, 50, 100, 200, 500 が選択できます。Synesis 内部のメモリには 40000 フロー(IP アドレスとポートのペアにより定義されたフロー)保持されています。その上位の、指定された数のフローがグラフに表示されます。</p> <p>フローは、最終パケットが 25 秒以上非アクティブとなった場合に解析の対象外となります。(ただし、FIN/ RESET パケットが送られた場合は 10 秒です)</p>
データベースのエイジアウトを有効にする	<p>解析データがディスク領域を圧迫しないように、過去のデータを自動的に削除させることができます。削除対象となる解析データは、ARP を除く、保存された全解析データ (APM・NPM・L2/L3 プロトコル・マイクロバースト) です。エイジアウトが有効な状態での動作は下記の通りです。</p> <ol style="list-style-type: none"> <li>1. 毎日 AM 01:00 に、OS パーティションの残量をチェックします。</li> <li>2. 残量が 20%以下だった場合、粒度の細かいデータを過去から順に消去します。</li> <li>3. 残量が 40%以上になるか、31 日以上前のデータを全て消去した段階で、消去動作を終了します。</li> <li>4. 30 日前～エイジアウト当日までのデータと、過去のデータ中最も粒度の粗いデータは削除されません。</li> </ol>
解析データの削除	<p>特定の日付以前の解析データを削除することができます。</p> <p>削除対象となる解析データは、保存された解析データの内、APM・NPM・L2/L3 プロトコルの各データです。</p> <p>画面左上の「編集」ボタンをクリックすると、「削除」ボタンも有効になります。</p> <p>「解析データの削除」欄で日付を指定して「削除」ボタンをクリックしてください。指定した日付の 00:00:00 及び、それ以前に作成された解析データが削除されます。</p>

## 12.13. サイト

「IP アドレス」の範囲に名前をつけて登録・管理し、扱いやすくします。  
登録した「IP アドレス」は登録した「名前」に置換されて表示されます。

新規		削除	
<input type="checkbox"/>	名前	説明	範囲
<input checked="" type="checkbox"/>	<a href="#">sample</a>	sample	123.43.12.0/24

IP アドレス、もしくはサブネット付きの IP アドレスを入力します。

複数のアドレスはセミコロン (;) で区切ります (例 : 192.168.2.3/24;192.168.9.7)。サブネットマスクの書式は CIDR (Classless Inter-Domain Routing) 記法を使用します (例 : クラス C のマスクは 255.255.255.0 で /24 と表記)。

サイトを追加したい場合は「新規」ボタンをクリックしてください。

● サイト

名前

説明

範囲  

IPアドレスをセミコロン(;)で区切り、入力してください。例:  
192.168.2.3/24;192.168.9.7;10.0.0.1-10.2.3.4

キャンセル

保存

「名前」、「説明」、「範囲」を入力し、「保存」ボタンをクリックしてください。

入力したサイトの情報が登録され、リストに追加されます

登録済みのサイトを編集したい場合は、「名前」のリンクをクリックしてください。

新規登録時と同様にサイト登録ダイアログが表示され、登録内容を編集できます。

登録済みのサイトを削除したい場合は、削除したいサイトの左端のチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。選択したサイトが削除されます。

登録済みのサイトをまとめて削除したい場合は、項目名欄のチェックボックスにチェックを入れてください。すべてのサイトが選択された状態になり、すべてのサイトが削除されます。

## 12.14. サーバグループ

「サーバ IP アドレス」 の範囲に名前をつけて登録・管理し、扱いやすくします。書式は **12.13 サイト** と同様です。

登録した「サーバ IP アドレス」は登録した「名前」に置換されて表示されます。



<input type="checkbox"/>	サーバグループ名	サーバグループの説明	サーバリスト
<input checked="" type="checkbox"/>	グループ	sample group	192.168.0.1/24;10.0.0.1

「新規」サーバグループを追加するには、「新規」ボタンをクリックして「名前」、「説明」、「サーバリスト」を入力します。入力内容を保存する場合は「保存」をクリックします。入力内容を破棄する場合は「キャンセル」ボタンをクリックします。

サーバグループを編集するには、「名前」ラベルを選択し、「名前」、「説明」、「サーバリスト」を入力してください。入力内容を保存する場合は「保存」をクリックします。入力内容を破棄する場合は「キャンセル」ボタンをクリックします。

サーバグループを「削除」するには、削除したい左側のチェックボックスをクリックして「削除」ボタンをクリックします。先頭行の「サーバグループ名」という見出し左側にチェックを入れると、すべてのサーバグループが選択された状態になります。この状態で「削除」をクリックすると、すべてのサーバグループが削除されます。

## 12.15. プロトコル

アプリケーションプロトコルのポート番号をあらかじめ名前を付けて定義しておくことができます。  
定義済みのプロトコルのポート番号は一覧で表示されます。

全て	L2 イーサタイプ	L3 プロトコル	L4 プロトコル
名前	説明	値	タイプ
IPv4		0x0800	L2 イーサタイプ
ARP		0x0806	L2 イーサタイプ
IPv6		0x86dd	L2 イーサタイプ
ICMP		1	L3 プロトコル
TCP		6	L3 プロトコル
UDP		17	L3 プロトコル
BGP		179	L4 プロトコル
DNS		53	L4 プロトコル
EXCHANGE		135	L4 プロトコル
FTP		21	L4 プロトコル
FTP-DATA		20	L4 プロトコル
GTP		2123;2152;3386	L4 プロトコル
H.323		1720-1721	L4 プロトコル
HTTP		80;443	L4 プロトコル
LDAP		389;636	L4 プロトコル
LDP		646	L4 プロトコル

登録できるのは「L2 イーサタイプ」「L3 プロトコル」「L4 プロトコル」の3種類です。

「L2 イーサタイプ」と「L3 プロトコル」はプロトコル番号ごとの統計値を表でダッシュボードに表示させることができます。詳細は **4.5.1 グラフの種類と設定方法** を参照してください。

「L4 プロトコル」登録したプロトコル番号を **12.16 アプリケーショングループ** に登録して、APM/NPM 解析などでグループごとのフィルタを設定できます。

「全て」タブ(上図)では登録済みのプロトコルが全て表示されますが、閲覧のみとなっています。

「L2 イーサタイプ」「L3 プロトコル」「L4 プロトコル」のそれぞれのタブでは登録済みのプロトコルがタイプ別表示されています。プロトコルの登録・編集はこちらのタイプ別の画面から行えます。

### 12.15.1. 全て タブ

登録済みのプロトコルが全て表示されています。閲覧のみで登録・編集は行えません。

確認できる情報は以下の通りです。

項目	説明
名前	登録されているプロトコルのポート番号の「名前」です。
説明	登録内容に対する説明が表示されます。
値	登録されているプロトコルのポート番号です。
タイプ	プロトコルのタイプが表示されます。タイプは以下の3種類です。 L2 イーサタイプ、L3 プロトコル、L4 プロトコル

## 12.15.2. L2 イーサタイプ タブ

L2 イーサタイプを登録・管理できます。

チェックボックスのないプロトコルはデフォルトで登録されているもので、編集・削除できません。

全て	L2 イーサタイプ	L3 プロトコル	L4 プロトコル
新規	削除		
<input type="checkbox"/>	名前	説明	イーサタイプ
<input checked="" type="checkbox"/>	<a href="#">Test</a>		0x0080
	IPv4		0x0800
	ARP		0x0806
	IPv6		0x86dd

プロトコルを新規追加したい場合は、「新規」 ボタンをクリックしてください。

下図の「L2 イーサタイプ」ダイアログが表示されます。

L2 イーサタイプ

名前 \*

説明

イーサタイプ \*

16進数で0001からFFFFの間の数字を半角で入力してください。

☒ Hex

☐ Decimal

キャンセル

保存

各項目を入力したら、「保存」 ボタンをクリックしてください。

入力した名前とポート番号が登録され、一覧表に追加されます。

登録済みのプロトコルを編集したい場合は、編集対象アプリケーションの「名前」のリンクをクリックしてください。「L2 イーサタイプ」ダイアログが表示され、登録内容が編集できます。

登録したプロトコルを削除する場合は、名前の左側のチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。選択したプロトコルが削除されます。



### 12.15.3. L3プロトコル タブ

L3 プロトコルを登録・管理します。

チェックボックスのないプロトコルはデフォルトで登録されているもので、編集・削除できません。

全て   L2 イーサタイプ <b>L3 プロトコル</b> L4 プロトコル			
新規   削除			
<input type="checkbox"/>	名前	説明	プロトコル番号
	ICMP		1
	TCP		6
	UDP		17
<input checked="" type="checkbox"/>	<a href="#">Test L3</a>		2

プロトコルを新規追加したい場合は、「新規」 ボタンをクリックしてください。

下図の「L3 プロトコル」ダイアログが表示されます。

L3 プロトコル

名前 \*

説明

プロトコル番号 \*

10進数で1から255の数字を半角で入力してください(43,44,51,60を除く)。

☐ Hex

☒ Decimal

キャンセル

保存

各項目を入力したら、「保存」 ボタンをクリックしてください。

入力した名前とポート番号が登録され、一覧表に追加されます。

登録済みのプロトコルを編集したい場合は、編集対象アプリケーションの「名前」のリンクをクリックしてください。「L3 プロトコル」ダイアログが表示され、登録内容が編集できます。

登録したプロトコルを削除する場合は、名前の左側のチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。選択したプロトコルが削除されます。

## 12.15.4. L4プロトコル タブ

L4 プロトコルのポート番号を登録・管理します。

全て	L2 イーサタイプ	L3 プロトコル	L4 プロトコル	
新規	削除			
<input type="checkbox"/>	名前	説明	ポート範囲	
<input type="checkbox"/>	<a href="#">BGP</a>		179	
<input type="checkbox"/>	<a href="#">DNS</a>		53	
<input type="checkbox"/>	<a href="#">EXCHANGE</a>		135	
<input type="checkbox"/>	<a href="#">FTP</a>		21	
<input type="checkbox"/>	<a href="#">FTP-DATA</a>		20	
<input type="checkbox"/>	<a href="#">GTP</a>		2123;2152;3386	
<input type="checkbox"/>	<a href="#">H.323</a>		1720-1721	
<input type="checkbox"/>	<a href="#">HTTP</a>		80;443	
<input type="checkbox"/>	<a href="#">LDAP</a>		389;636	
<input type="checkbox"/>	<a href="#">LDP</a>		646	

プロトコルを新規追加したい場合は、「新規」 ボタンをクリックしてください。

下図の「L4 プロトコル」ダイアログが表示されます。

L4 プロトコル

名前\*

説明

ポート範囲\*

ポートの範囲をセミicolon(;)で区切り入力してください。  
例: 3500-3511;8300;9810-9816

☐ Hex

☒ Decimal

キャンセル

保存

複数のポート番号を指定する場合は “; (セミコロン)” で区切って入力してください。範囲指定する場合は、ポート番号の間に “- (半角マイナス)” を入れて入力してください。入力を終わたら、「保存」ボタンをクリックしてください。入力内容が登録され、一覧表に追加されます。

登録済みのプロトコルを編集したい場合は、編集対象アプリケーションの「名前」のリンクをクリックしてください。「L4 プロトコル」ダイアログが表示され、登録内容が編集できます。

登録したプロトコルを削除する場合は、名前の左側のチェックボックスにチェックを入れ、「削除」ボタンをクリックしてください。選択したプロトコルが削除されます。

## 12.16. アプリケーショングループ

前項 **L4 プロトコル タブ** で登録されたアプリケーションプロトコルをグループ化し、登録・管理することができます。このアプリケーショングループを利用し、APM/NPM 解析などでグループごとのフィルタを設定することができます。




新しいアプリケーションを追加するには、「新規」ボタンをクリックしてください。

下図の「アプリケーショングループ」ダイアログが表示されます。



左側は前項の **L4 プロトコル タブ** で定義されたアプリケーションプロトコルのリストです。右側のリストにあるアプリケーションが、グループに登録されるアプリケーションになります。

左側のリストから適用したいアプリケーションを選んで **>>** アイコンをクリックしてください。選

んだアプリケーションが右側のリストに追加されます。右側のリストから外すには、外したいアプリケーションを選んで  アイコンをクリックしてください。

「保存」ボタンをクリックすると、指定したアプリケーショングループが登録され、一覧表に追加されます。

一覧表に表示される情報は以下の通りです。

項目	説明
名前	登録されているアプリケーショングループの「名前」です。
説明	登録内容に対する説明が表示されます。
アプリケーション	登録されているアプリケーションのリストです。

登録済みのアプリケーショングループを編集したい場合は、「名前」のリンクをクリックしてください。新規登録時と同様に「アプリケーショングループ」ダイアログが表示され、設定を変更することができます。

登録済みのアプリケーショングループを削除したい場合は、削除したいグループの左側のチェックボックスにチェックを入れて「削除」ボタンをクリックしてください。選択したアプリケーショングループが削除されます。

先頭行の「名前」という見出し左側にチェックを入れると、すべてのアプリケーショングループが選択された状態になります。この状態で「削除」をクリックすると、すべてのアプリケーショングループが削除されます。

## 12.17. マイクロバースト

マイクロバースト発生の判断基準とする閾値を設定します。

設定した閾値を有効にすると、マイクロバーストを検出した時にアラートが出ます。アラート閾値は閾値 1、閾値 2 と最大 2 つまで同時に指定できます。

編集

アラート閾値設定

☐ 閾値1

使用率 >= 80 % (1-100)

連続発生数 1000 (1-70000)

☐ 閾値2

使用率 >= 90 % (1-100)

連続発生数 1000 (1-70000)

分解能 1000 us

アラート閾値として設定が必要な項目は「使用率」「連続発生数」「分解能」です。

トラフィックの使用率が指定した「使用率」を超え、その状態が指定した期間(「分解能」×「連続発生数」)以上続いた場合にマイクロバースト発生と判断され、アラートが出ます。

マイクロバーストのアラート閾値を設定したい場合は、「編集」ボタンをクリックしてください。

各項目が編集可能になり、「保存」ボタンが表示されます。設定項目は以下の通りです。

項目	説明
使用率	閾値となる回線使用率を 1 以上 100 以下、パーセンテージで入力します。 ここで指定した回線使用率を連続して超えた期間が「持続時間」となります。
連続発生数	マイクロバースト発生の判断基準とする「持続時間」を「連続発生数」で指定します。閾値となる「持続時間」は「分解能」×「連続発生数」です。 1 以上 70000 以下の数字を入力してください。
分解能	どれだけ細かくキャプチャレコードを区切って使用率を確認するか、その細かさ(区切られた 1 区間の長さ)を指定します。閾値 1・閾値 2 で共通です。 デフォルトは 1000 us で、1000 us または 100 us に設定できます。

指定された閾値を元に、どのように解析が行われるかは**マイクロバーストの検知とアラート発生の閾値**を参照してください。

アラート閾値のそれぞれのチェックボックスにチェックを入れると、そのアラート閾値が有効になります。「保存」ボタンをクリックしていただくと、変更されたアラート閾値が保存されます。

なお、ここで設定される閾値はキャプチャしながらリアルタイムにマイクロバースト検知を行うための閾値です。キャプチャ済みのレコードを再解析する場合のアラート閾値には影響されません。

再解析用の閾値の設定については **9.2.2 閾値の変更** を参照してください。

## Appendix A 用語集

本書で使用する用語について説明します。

### A.1 略語一覧

索引	正式名称	意味
APM	Application Performance Metrics	3 ウェイ・ハンドシェイクが確立した TCP 通信の、主に遅延時間に係る統計情報を得るための解析です。 アプリケーション性能管理と訳されることもあります。
ART	Application Response Time	サーバアプリケーションがクライアントリクエストに回答するのにかかる時間です。 [応答パケットのタイムスタンプ]－[リクエストパケットのタイムスタンプ]で計算されます。※
CRT	Client Response Time	クライアントがリクエストを開始するまでにかかる時間です。 ACK とクライアントリクエストのタイムスタンプの差により計算されます。※
DLC	Data Link Connections	データリンク層です。 Synesis ではイーサネット通信を指します。
KPI	Key Performance Indicators	各種解析の結果、得られる「指標」を指します。 DLC 統計、NPM 解析、APM 解析によって得られる、バイト数、パケット数、ビットレート、リトライ数 (APM 解析のみ) などを指します。
NPM	Network Performance Metrics	TCP・UDP フローの、主にデータ量に係る統計情報です。ネットワーク性能管理と訳されることもあります。
NRT	Network Round-trip Time	ネットワークをパケットが往復するのにかかる平均時間です。ACK と SYN のタイムスタンプの差により計算されます。※
PTT	Payload Transfer Time	サーバがクライアントリクエストへのレスポンスを送るのに要した平均時間です。 [ACK 応答のタイムスタンプ]－[サーバのレスポンスのパケットのタイムスタンプ]で計算されます。※
SRT	Server Response Time	サーバがクライアントリクエストに回答し、レスポンスを完了させるのに要した時間です。 ART+NRT+PTT で計算されます。※

※8.2APM 解析のクライアント－サーバ 通信シーケンス図を参照してください。

## Appendix B キャプチャフィルタの種類と設定方法

こちらの章ではキャプチャフィルタの種類と、その設定方法について説明します。

キャプチャフィルタはディスクに保存する前のパケットをふるいに掛ける、物理的なフィルタです。

キャプチャ時に適用させるため、キャプチャの実行を開始する前に設定します。

キャプチャフィルタを登録するには、「キャプチャオプション」の「キャプチャフィルタ」タブで「追加」ボタンをクリックしてください。下図のキャプチャフィルタダイアログが表示され、キャプチャフィルタが設定できます。

● キャプチャフィルタ

フィルタ名

NOT ☐

**MACアドレス**  
VLAN  
イーサタイプ  
IPフロー  
フロー  
アプリケーション  
パターン

送信元  
MACアドレス   
コロン(:)を使って入力してください。例 01:23:45:67:89:ab

方向

送信先  
MACアドレス   
コロン(:)を使って入力してください。例 01:23:45:67:89:ab

設定項目はフィルタの種類によって異なりますが、共通する設定項目は以下の通りです。

項目名	説明
フィルタ名	登録するフィルタの名前を入力します。
NOT	チェックを入れると、論理演算子「NOT」が適用され、「指定した条件に当てはまらないもの」がフィルタリングされます。
フィルタタイプ	フィルタタイプを選択します。(種類については次頁参照)

各項目の設定を終えたら、「適用」ボタンをクリックしてください。設定したキャプチャフィルタが保存され、キャプチャに適用できるようになります。

キャプチャへの適用手順その他、詳細は **5.3.1.2 キャプチャオプション** を参照してください。

なお、モデル(アダプタの種類)によってはキャプチャフィルタは適用できません。

詳細は **Appendix H モデルによる違い** を確認してください。

キャプチャフィルタとして設定可能なフィルタの種類は以下の7種類です。

節番号	フィルタ・タイプ	説明
B.1	MAC アドレス	MAC アドレスでフィルタを設定します。
B.2	VLAN	Virtual LAN の ID でフィルタを設定します。
B.3	イーサタイプ	イーサタイプのプロトコル番号でフィルタを設定します。
B.4	IP フロー	IP アドレスでフィルタを設定します。
B.5	フロー	TCP もしくは UDP と、IP アドレスとポートのペアでフィルタを設定します。
B.6	アプリケーション	定義済みのアプリケーションポートでフィルタを設定します。
B.7	パターン	フレームの先頭からオフセットとパケットのパターンでフィルタを設定します。

## B.1 MAC アドレス

MAC アドレスでフィルタを設定できます。

● キャプチャフィルタ

フィルタ名

NOT ☐

MACアドレス

VLAN

イーサタイプ

IPフロー

フロー

アプリケーション

パターン

送信元

MACアドレス

コロン(:)を使って入力してください。例 01:23:45:67:89:ab

方向

-->

送信先

MACアドレス

コロン(:)を使って入力してください。例 01:23:45:67:89:ab

キャンセル

適用

設定項目は以下の通りです。

項目	説明
送信元/送信先 MAC アドレス	16 進数(HEX)で送信元と送信先の MAC アドレスを入力します。このフィールドをブランクにすると、全ての MAC アドレスが対象になります。
方向の選択	「-->」「<--」「<-->」から送信元と送信先のパケットの方向を選びます。



## B.2 VLAN

Virtual LAN の ID でフィルタを設定できます。

● キャプチャフィルタ

フィルタ名

NOT ☐

MACアドレス

**VLAN**

イーサタイプ

IPフロー

フロー

アプリケーション

パターン

VLAN ID

例: 1, 2, 3

キャンセル

適用

項目	説明
VLAN ID	VLAN ID を入力します。0 以上 4095 以下の数値を入力してください。

## B.3 イーサタイプ

イーサタイプのプロトコル番号でフィルタを設定できます。

● キャプチャフィルタ

フィルタ名

NOT ☐

MACアドレス

VLAN

**イーサタイプ**

IPフロー

フロー

アプリケーション

パターン

イーサタイプ

16進数を入力してください(例: 86DD)

キャンセル

適用

項目	説明
イーサタイプ	イーサタイプのプロトコル番号を 16 進数(HEX)で入力してください。

## B.4 IP フロー

IP アドレスでフィルタを設定できます。

● キャプチャフィルタ

フィルタ名

NOT ☐

MACアドレス  
VLAN  
イーサタイプ  
**IPフロー**  
フロー  
アプリケーション  
パターン

送信元 IPアドレス

例 : 172.23.1.1, 192.168.1.0/24,  
2001:DB8::8:800:200C:417A

方向

送信先 IPアドレス

例 : 172.23.1.1, 192.168.1.0/24,  
2001:DB8::8:800:200C:417A

キャンセル

適用

設定項目は以下の通りです。

項目	説明
<b>送信元/送信先 IP アドレス</b>	送信元、もしくは送信先となる IPv4 または IPv6 アドレスを数値で入力します。 サブネットマスクは '/' を付加することで追加できます。 (192.168.1.0/24, 2001:1111:2222:3333:0000:0000:0000:0000/64 等) 空白の場合は全ての IP アドレスが対象になります(Any フィルタ)。
<b>方向の選択</b>	「-->」「<--」「<-->」から送信元と送信先のパケットの方向を選びます。

## B.5 フロー

TCP もしくは UDP と、IP アドレスとポートのペアでのフィルタを設定できます。

● キャプチャフィルタ

フィルタ名

NOT ☐

MACアドレス  
VLAN  
イーサタイプ  
IPフロー  
**フロー**  
アプリケーション  
パターン

☒ TCP ☐ UDP

送信元 IPアドレス  ポート   
例 : 172.23.1.1, 192.168.1.0/24, 2001:DB8::8-800:200C:417A 例:80

方向

送信先 IPアドレス  ポート   
例 : 172.23.1.1, 192.168.1.0/24, 2001:DB8::8-800:200C:417A 例:80

キャンセル

適用

設定項目は以下の通りです。

項目	説明
<b>TCP/UDP</b>	TCP もしくは UDP を選び、IP アドレス/ポートのペアを設定します。
<b>送信元/送信先 IP アドレス</b>	送信元、もしくは送信先となる IPv4 または IPv6 アドレスを数値で入力します。 サブネットマスクは '/' を付加することで追加できます。 (192.168.1.0/24, 2001:1111:2222:3333:0000:0000:0000:0000/64 等) 空白の場合は全ての IP アドレスが対象になります(Any フィルタ)。
<b>送信元/送信先 ポート</b>	送信元、もしくは送信先の TCP ポート番号を数値で入力します。 0 以上 65535 以下の値で指定してください。
<b>方向の選択</b>	「-->」「<--」「<-->」から送信元と送信先のパケットの方向を選びます。

## B.6 アプリケーション

定義済みのアプリケーションポートでフィルタを設定できます。

● キャプチャフィルタ

フィルタ名

NOT ☐

MACアドレス

VLAN

イーサタイプ

IPフロー

フロー

**アプリケーション**

パターン

☒ TCP ☐ UDP

BGP(179)

DNS(53)

EXCHANGE(135)

FTP(21)

FTP-DATA(20)

H.323(1720-1721)

HTTP(80;443)

LDAP(389;636)

LDP(646)

MEGACO(2944-2945)

MGCP(2427;2727)

MSSQL(1433)

MySQL(3306)

NFS(2049)

ORACLE(1521;1525;1527;1529)

OpenFlow(6653)

OpenVPN(1194)

PGSQL(5432)

POP(110;110)

>>



<<

GTP(2123;2152;3386)

キャンセル

適用

設定項目は以下の通りです。

項目	説明
<b>TCP/UDP</b>	TCP と UDP、チェックマークの入ったプロトコルが有効になります。 TCP か UDP のどちらか、もしくは両方を指定することが可能です。
<b>アプリケーションリスト</b>	右側のリスト(デフォルトでは空欄)にリストアップされたアプリケーションポートがフィルタとして適用されます。 左側のリストから適用したいアプリケーションポートを選んで  アイコンをクリックしてください。選んだアプリケーションが右側に追加されます。 右側のリストに追加されたアプリケーションポートを外すには、外したいものを選んで  アイコンをクリックしてください。

## B.7 パターン

パケットの先頭から指定されたオフセットの位置にあるビットのパターンでフィルタを設定できます。

2 種類以上のパターンフィルタを AND/OR で組み合わせて指定することができます。

The screenshot shows the 'Capture Filter' configuration window. On the left, a list of filter types includes MAC Address, VLAN, EtherType, IP Protocol, Port, Application, and **Pattern** (highlighted in red). The main area is titled 'Pattern 1' and contains a '+ Filter Item Addition' button. Below this is a table with columns: Offset, Pattern, Mask, and Delete. The table is currently empty. Below the table, there are radio buttons for 'AND' (selected) and 'OR'. Below that is 'Pattern 2' with another '+ Filter Item Addition' button and an identical empty table. At the bottom right are 'Cancel' and 'Apply' buttons.

登録項目として「パターン 1」と「パターン 2」のパターンフィールドが用意されています。

各パターンフィールド(パターン 1,2)には最大 4 つのパターンが登録可能で、同じフィールド内のパターン同士は AND で結合されます。

「パターン 1」と「パターン 2」は「AND」で結合するか「OR」で結合するかを選択できます。

**+ フィルタ項目の追加** ボタンをクリックすると、以下の「パターンフィルタの設定」ダイアログが表示され、個々のパターンフィルタを登録することができます。

The screenshot shows the 'Pattern Filter Settings' dialog box. It has three input fields: 'Offset' with a placeholder 'Offset: Enter value in Decimal(0-992)', 'Pattern' with a placeholder 'Match: Type in Hex; example: 1c', and 'Mask' with a placeholder 'Mask: Type in Hex; example: 1c'. At the bottom are 'Cancel' and 'Apply' buttons.

設定項目は以下の通りです。

項目	説明
オフセット	フィルタリングされるパターン文字列が始まる位置[バイト列]を指定します。 パケットの先頭を "0" として、10 進数で指定します。
パターン	フィルタリングするパターン文字列です。16 進数(HEX)で指定します。
マスク	フィルタに適用される「マスクパターン」です。16 進数(HEX)で指定します。 「マスクパターン」で "0" のビットは "no care" になります。

「パターン」と「マスク」の指定方法を具体的な例を用いて説明します。

例えば、「パターン」が "1F"、「マスク」が "F1" の場合、ビットごとの値は以下の通りです。

	16 進数	2 進数
パターン	1 F	0 0 0 1   1 1 1 1
マスク	F 1	1 1 1 1   0 0 0 1
フィルタリング	—	0 0 0 1   x x x 1

「マスクパターン」の "0" のビットは "no care" なので、フィルタリングされるパターンは「0 0 0 1   x x x 1」になります。"x" のビットは "0" でも "1" でも構いません。

## Appendix C 統計値の CSV ファイル

Synesis ではキャプチャレコードの 1 秒ごとの統計値をカンマ区切り (CSV) ファイルに保存し、ダウンロードすることが出来ます。

ファイルに含まれる項目は以下の通りです。

項目	説明
ヘッダ行	各ポート名(例：チャンネル A)と指標の組み合わせがヘッダ行となります。 指標はこの表のタイムスタンプ以降の各項目です。 ポート名はチャンネルグループを設定している場合は「チャンネルグループに設定した名前 + IN または OUT」の形式(例：チャンネルグループ 1 IN)で表示されます。詳細は <b>D.2 データソース</b> を確認してください。
タイムスタンプ	統計値のタイムスタンプで、表示形式は yyyy/mm/dd hh:mm:ss です。 "ss-1" 秒以降、"ss" 秒より前の 1 秒間の統計値になります。
ステータス	チャンネルの接続状況です。 未対応のモデルは"unkown"と表示されます。
使用率	回線の使用率を%で示した値です。
ビットレート	1 秒間に受信したビット数です。
パケットレート	1 秒間に受信したパケット数です。
バイト	受信した総バイト数です。
パケット	受信した総パケット数です。
ドロップ	ドロップしたパケット数です
ブロードキャスト	有効なブロードキャストパケット数です
マルチキャスト	有効なマルチキャストパケット数です。
ユニキャスト	有効なユニキャストパケット数です。
CRC※	CRC エラーのパケット数です。フラグメントおよびジャバーは含みません。
フラグメント※	CRC エラーの内、64byte 未満のパケット数です。
ジャバー※	CRC エラーのうち特定の値(byte) より大きいパケット数です。 特定の値(byte) はモデルによって異なります。
オーバーサイズ※	CRC エラー以外で特定の値(byte) より大きいパケット数です。 特定の値(byte) はモデルによって異なります。
ラント※	CRC エラー以外で、64 byte 未満のパケット数です。
アダプタ	アダプタの名称です。

※ CRC～ラントのエラーパケットの検出はモデル(アダプタ)によっては統計が取れません。その場合の統計値は「0」と表示されます。対応している場合も、ジャバーやオーバーサイズとカウントされるパケットのサイズ(byte)はモデルによって異なります。

対応モデルやパケットサイズ(byte)の詳細は **Appendix H モデルによる違い**を参照してください。

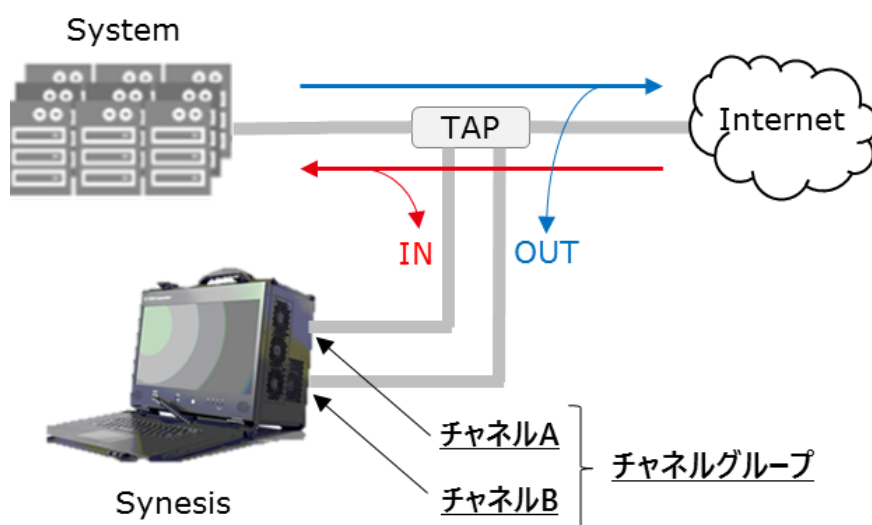
## Appendix D チャネルグループとデータソース

### D.1 チャネルグループ

#### D.1.1 概要

チャネルグループとは、2つのチャネルをグループ化して扱う機能です。外部ネットワークから内部システムへのIN, OUTそれぞれのトラフィックを、別々のチャネルでキャプチャする場合に使用できます。

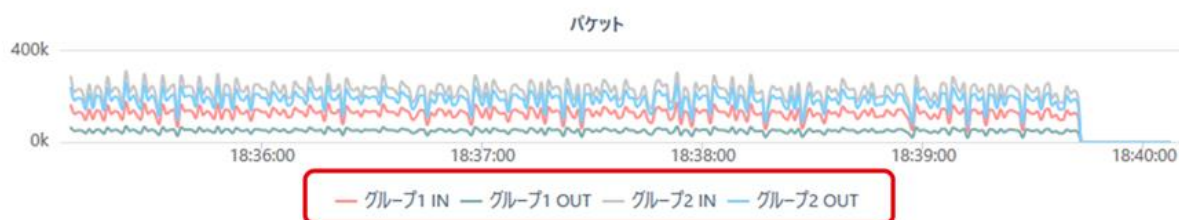
チャネルグループはお客様の使用環境に合わせて出荷時に定義されています。追加・変更・削除を行う際は弊社までご連絡ください。



#### D.1.2 エージェント画面

チャネルグループが定義されている場合のエージェント画面です。チャネル名は、チャネルグループ名に“IN”または“OUT”を付加した名称で表示されます。

<input checked="" type="checkbox"/>	チャネル	使用率	ビットレート	パケットレート	パケット	バイト
<input checked="" type="checkbox"/>	グループ1 IN	2.4%	226,717.78 kbps	125,971.00 pps	52,907,822	11,902,683,679
<input checked="" type="checkbox"/>	グループ1 OUT	0.7%	60,940.60 kbps	49,637.00 pps	20,847,649	3,199,381,726
<input checked="" type="checkbox"/>	グループ2 IN	4.2%	404,253.99 kbps	223,233.00 pps	93,757,978	21,223,334,713
<input checked="" type="checkbox"/>	グループ2 OUT	3.7%	358,015.04 kbps	185,536.00 pps	77,925,125	18,795,789,792





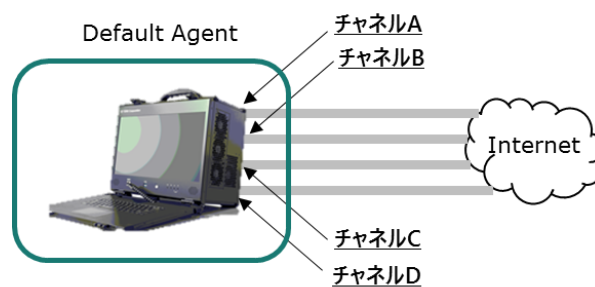
## D.2 データソース

### D.2.1 概要

データソースとは、統計値あるいは解析結果の計算元となるチャンネルの組み合わせです。ダッシュボード、アラート、APM/NPM 解析、レポート機能で指定するパラメータです。

チャンネルグループ、およびリモートエージェントの構成によって、データソースとして選択可能な項目が変化します。

### D.2.2 チャンネルグループ無しの場合

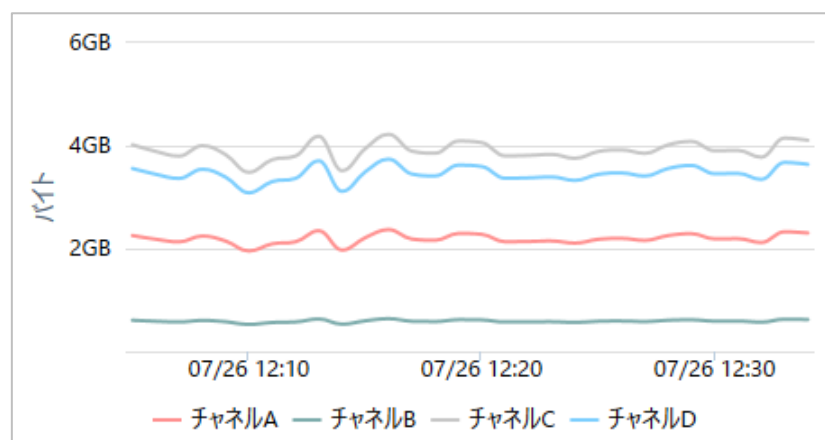


データソースとして選択できるのは Default Agent のみです。その中には Default Agent の全てのチャンネルが含まれています。

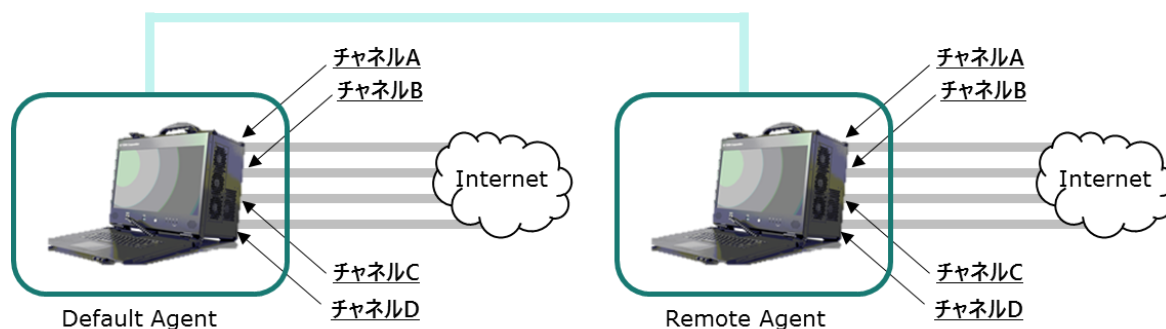
ID	データソース名	含まれるチャンネルまたはグループ
(1)	Default Agent	Default Agent : チャンネル A, B, C, D

#### D.2.2.1 設定例（Default Agent）

ID (1) の Default Agent をデータソースとした DLC グラフです。それぞれのチャンネルが個別の系列としてグラフに描画されます。



### D.2.3 リモートエージェント有り、チャンネルグループ無しの場合

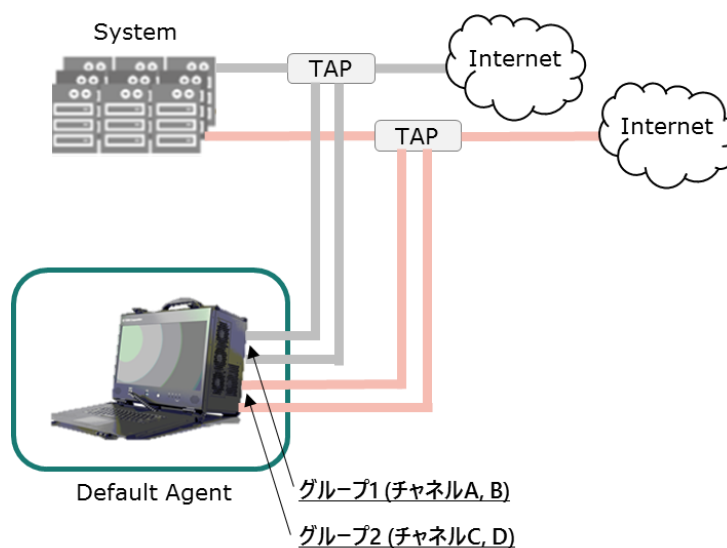


それぞれのエージェントがデータソースとして選択できます。

ID	データソース名	含まれるチャンネルまたはグループ
(1)	Default Agent	Default Agent : チャンネル A, B, C, D
(2)	Remote Agent	Remote Agent : チャンネル A, B, C, D

ID (2) の Remote Agent をデータソースとした場合のグラフは、**D.2.2.1 設定例 (Default Agent)** と同様になります。

### D.2.4 チャンネルグループ有りの場合



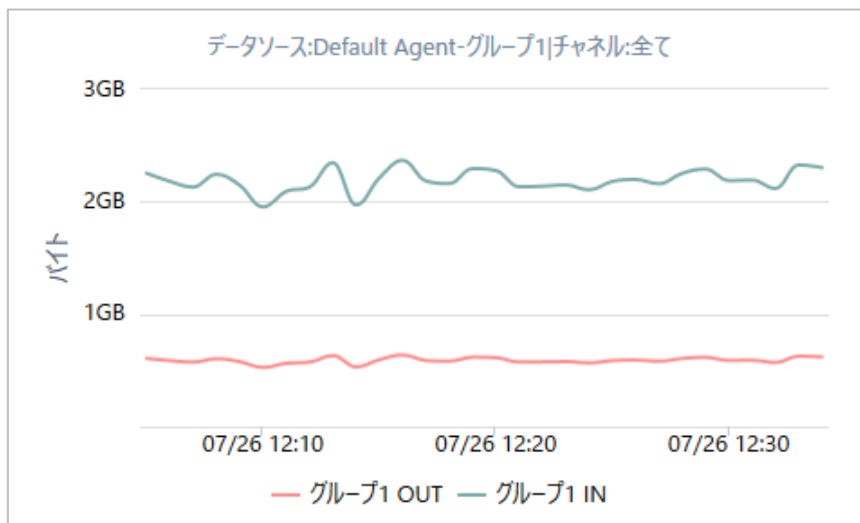
個別のチャンネルグループ、全チャンネルグループの合算がデータソースとして追加されます。

ID (2), (3) が個別のチャンネルグループ、ID (4) が全チャンネルグループの合算です。

ID	データソース名	含まれるチャンネルまたはグループ
(1)	Default Agent	Default Agent : チャンネル A, B, C, D
(2)	Default Agent - グループ 1	Default Agent : チャンネル A, B
(3)	Default Agent - グループ 2	Default Agent : チャンネル C, D
(4)	Default Agent - All Channel Group	Default Agent : グループ 1, 2

#### D.2.4.1 設定例（個別のチャンネルグループ）

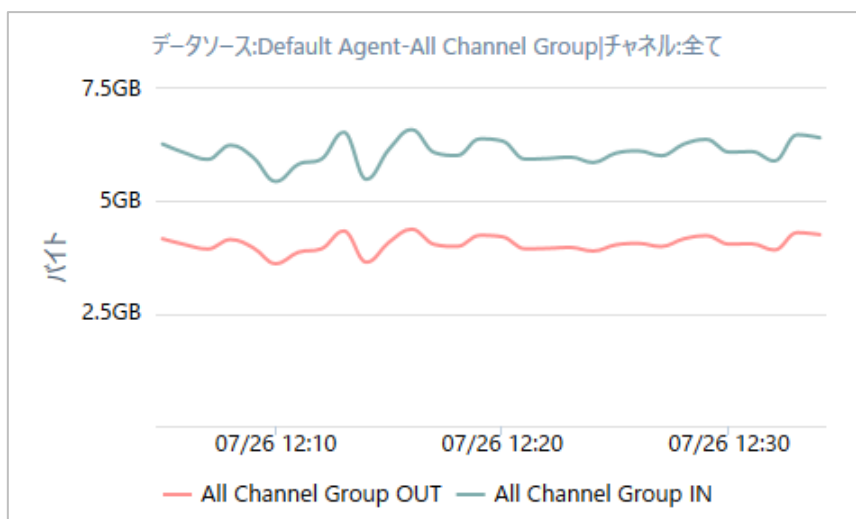
ID (2) の Default Agent - グループ 1 をデータソースとした DLC グラフです。IN, OUT の 2 系列がグラフに描画されます。



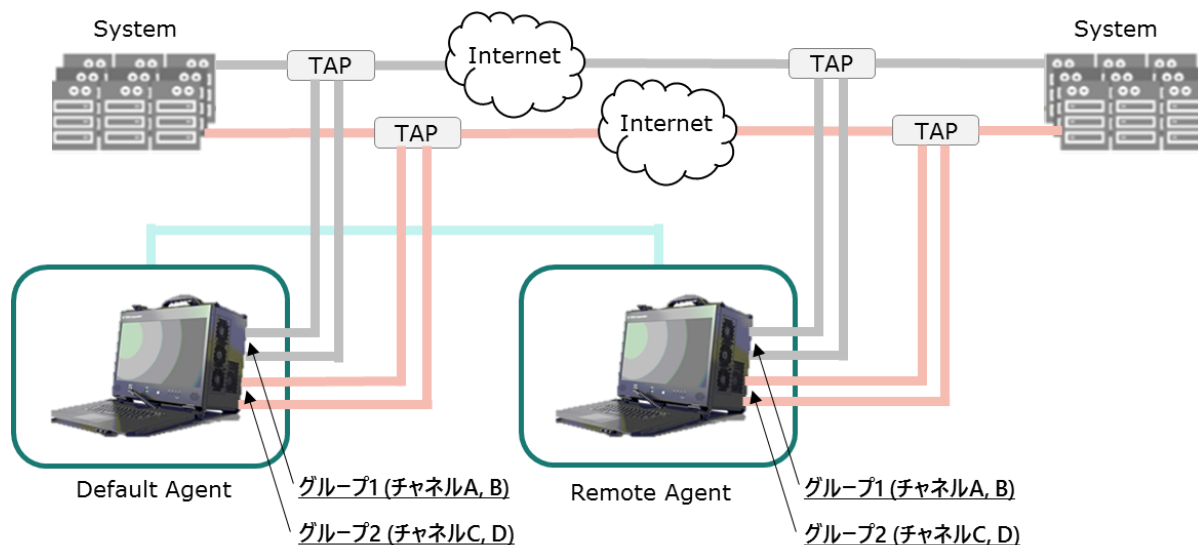
#### D.2.4.2 設定例（全チャンネルグループの合算）

ID (4) の Default Agent - All Channel Group をデータソースとした DLC グラフです。個別チャンネルの場合と同様に、IN, OUT の 2 系列がグラフに描画されます。

“All Channel Group OUT” の系列は、グループ 1, 2 の OUT チャンネルを合算したものです。同様に “All Channel Group IN” の系列は、グループ 1, 2 の IN チャンネルを合算したものです。



## D.2.5 リモートエージェント有り、チャンネルグループ有りの場合



それぞれのエージェントから **D.2.4 チャンネルグループ有りの場合** と同様のデータソースが選択可能です。ID (1) ～ (4) は Default Agent のデータソース、ID (5) ～ (8) は Remote Agent のデータソースです。

それに加えて、ID (9) All Agent - All Channel Group がデータソースとして追加されます。全エージェントの全チャンネルグループを合算するデータソースです。

ID	データソース名	含まれるチャンネルまたはグループ
(1)	Default Agent	Default Agent : チャンネル A, B, C, D
(2)	Default Agent - グループ 1	Default Agent : チャンネル A, B
(3)	Default Agent - グループ 2	Default Agent : チャンネル C, D
(4)	Default Agent - All Channel Group	Default Agent : グループ 1, 2
(5)	Remote Agent	Remote Agent : チャンネル A, B, C, D
(6)	Remote Agent - グループ 1	Remote Agent : チャンネル A, B
(7)	Remote Agent - グループ 2	Remote Agent : チャンネル C, D
(8)	Remote Agent - All Channel Group	Remote Agent : グループ 1, 2
(9)	All Agent - All Channel Group	Default Agent : グループ 1, 2 Remote Agent : グループ 1, 2

ID (9) All Agent - All Channel Group をデータソースとした場合のグラフは、**D.2.4.2 設定例（全チャンネルグループの合算）**と同様になります。

## Appendix E タイムサーバとのインテグレーション

### E.1 概要

Synesis は NTP サーバと連携して、キャプチャしたパケットに高精度のタイムスタンプを付与することができます。また、別売の変換コネクタを使用することで、アダプタ(キャプチャカード)をタイムサーバに連携させて、より高精度のタイムスタンプを付与することが可能になります。

PPS 出力機能を持つタイムサーバや、PTP ネットワークの GrandMaster が連携可能になります。

#### NTP サーバとの時刻同期

TCP/IP ネットワークを通して複数の NTP(Network Time Protocol)サーバに問い合わせを行い、内部時計の時刻を正確に調整します。

NTP サーバの選択と同期させる手順については **12.4 時刻同期**を参照してください。

#### PPS 時刻同期

PPS(Pulse Per Second)信号は一秒毎の正確な間隔で出力されるパルス信号です。

アダプタをこの PPS 信号と連携させ、OS の内部時計から得られる時刻を PPS 信号で補正します。アダプタは PPS 信号でこの内部時計から得られる時刻を補正します。

ご利用になる場合は別売の変換コネクタをご購入ください。

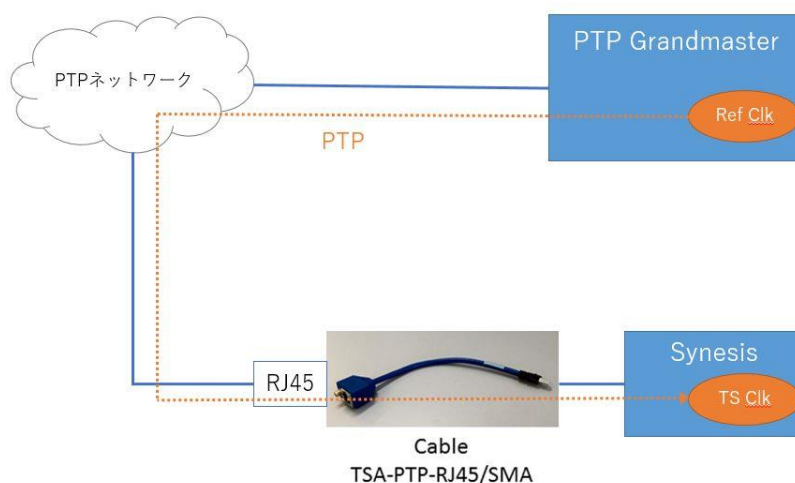
なお、補正が行われるのは外部の作業用 PC から操作が行われている期間のみとなります。

設定の手順は **E.2.1 PPS 時刻同期の設定手順**を参照してください。

#### PTP 時刻同期

アダプタを PTP(Precision Time Protocol)ネットワークに接続し、PTP GrandMaster と時刻同期させることができます。ご利用になる場合は別売の変換コネクタをご購入ください。

NTP サーバの精度が数 ms(ミリ秒)オーダーの精度であるのに対し、PTP の精度は 1 $\mu$ s(マイクロ秒)以下で、より正確なキャプチャデータのタイムスタンプを得ることができます。



“TS Clk”はキャプチャしたパケットのタイムスタンプに使用する TimeStampClock の略です。

## E.2 準備と作業手順

PPS 時刻同期、または PTP 時刻同期は、作業用 PC から Synesis へ SSH でログインし、アダプタ(キャプチャカード)の設定ファイルを編集します。

以下のソフトウェアがインストールされたノート PC を準備してください。

- OS: Windows 7、Windows 10
- Mozilla Firefox 28.0 以降、Internet Explorer 11
- フリーソフトウェア TeraTerm (バージョン 4.91 推奨)

設定作業の主な流れは以下の通りです。

- 1) NTP サーバの設定を確認します。
- 2) TeraTerm を起動し、Synesis にログインします。
- 3) ブラウザで Synesis の管理画面にアクセスし、Netkeeper を停止します。
- 4) SSH でアダプタの設定ファイルのバックアップを作成します。
- 5) アダプタの設定ファイルを編集し、変更を反映させます。
- 6) NetKeeper を再起動させます。

**※キャプチャを実行中の場合、作業の途中でキャプチャが停止しますのでご注意ください。**

## E.2.1 PPS 時刻同期の設定手順

アダプタの時刻同期ポートを使って、PPS 時刻同期を取ることが可能です。

ご利用になる場合は別売の変換コネクタをご購入ください。

TerTerm がインストールされた PC を使用して、アダプタの設定ファイルを編集します。

下記の手順に従って作業を実行してください。


**TeraTem を閉じると PPS 時刻同期は停止し、NTP 時刻同期に戻りますのでご注意ください。**

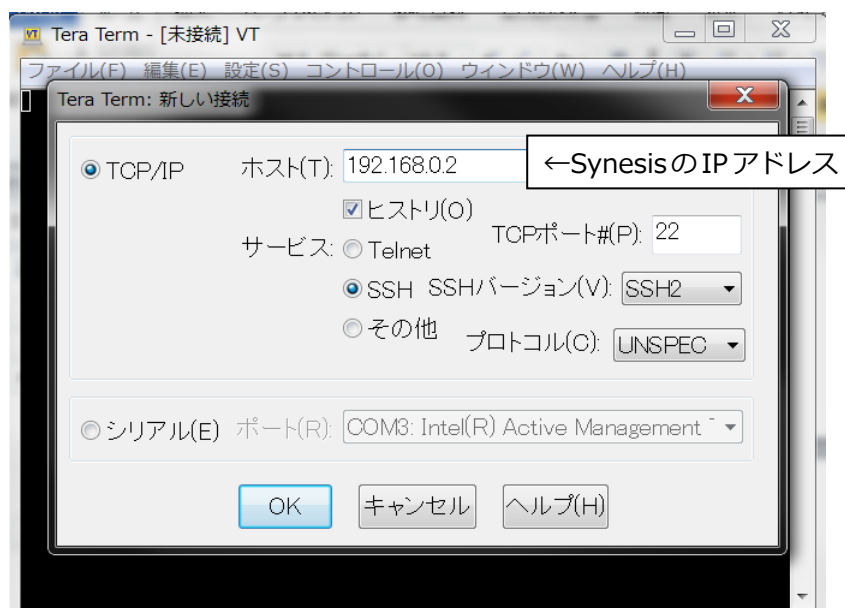
1. NTP サーバの設定を確認します。「構成」  メニュー「時刻同期」を選択してください。



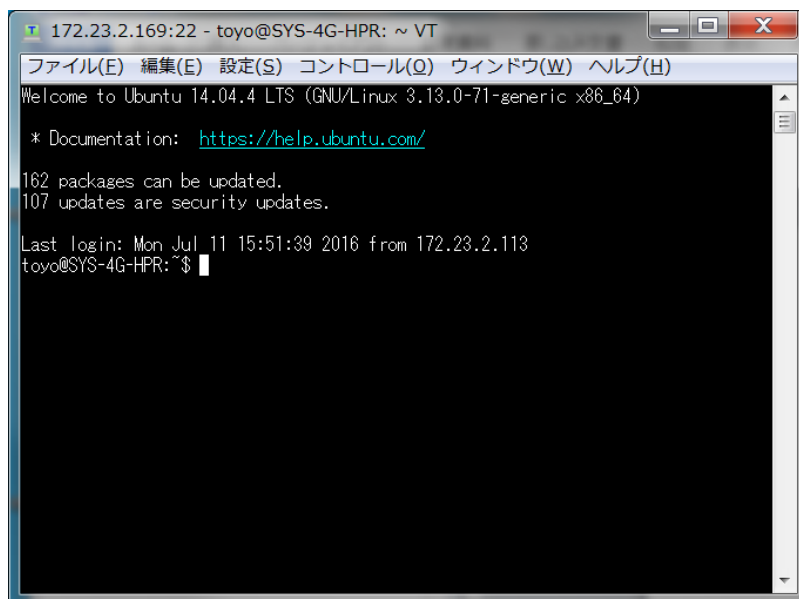
2. PPS 時刻同期は NTP サーバで調整した内部時計の時刻を PPS 信号で補正する時刻同期なので、NTP サーバを使用します。

画面左上の ON/OFF ボタンが **ON** になっていることを確認してください。OFF になっている場合はボタンをクリックして、ON に切替えてください。

3. TeraTerm  を起動します。以下の画面が表示されます。



- TCP/IP の「ホスト(T)」欄に Synesis の IP アドレスを入力して、「OK」ボタンをクリックしてください。(他の項目はデフォルトのまま変更しません。)
- Synesis に SSH で接続されます。デフォルトのアカウントは toyo/admin となります。



- ブラウザを起動し、“http://[Synesis IP]:3000” から Synesis 管理画面にアクセスします。NetKeeper サービスの「Stop」ボタンをクリックしてください。

Synesis All-in-One Capture Box <a href="#">Home</a> <a href="#">Get Logs</a>			
Process ID	Service	Description	Action
1450	Tomcat	Web Service.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1275	mvp	Management Platform, adapter of front end GUI and back end agent service.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1322	VPEyes	Capture Agent Daemon, keep capturing agent running.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1414	NetKeeper	Capture Agent, capturing service provider.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1302	DEService	Decode engine service	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1312	Notifier	Alarm Notifier service	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾

- Netkeeper の Process ID が“n/a”に、「Stop」ボタンが緑の「Start」ボタンに変わったことを確認してください。

Synesis All-in-One Capture Box <a href="#">Home</a> <a href="#">Get Logs</a>			
Process ID	Service	Description	Action
1450	Tomcat	Web Service.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1275	mvp	Management Platform, adapter of front end GUI and back end agent service.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
n/a	VPEyes	Capture Agent Daemon, keep capturing agent running.	<a href="#">Log</a> <a href="#">Start</a> <a href="#">Restart</a> Level ▾
n/a	NetKeeper	Capture Agent, capturing service provider.	<a href="#">Log</a> <a href="#">Start</a> <a href="#">Restart</a> Level ▾
1302	DEService	Decode engine service	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1312	Notifier	Alarm Notifier service	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾

※NetKeeper を停止すると、実行中のキャプチャは停止します。



8. アダプタの設定ファイル "/opt/napatech3/config/ntservice.ini" のバックアップファイルを、"ntservice.ini.org"というファイル名で作成します。

TeraTerm で下記のコマンドを実行してください。

```
$ sudo cp /opt/napatech3/config/ntservice.ini /opt/napatech3/config/ntservice.ini.org
```

9. アダプタの設定ファイルを開きます。

```
$ sudo vi /opt/napatech3/config/ntservice.ini
```

10. 設定ファイルの [TimeSyncConnectorExt1] の項目を [PpsIn] に変更してください。

【修正前】

```
TimeSyncConnectorExt1 = NttsIn          # None - NttsIn* - PpsIn - NttsOut - PpsOut - RepeatInt1 - RepeatInt2
```

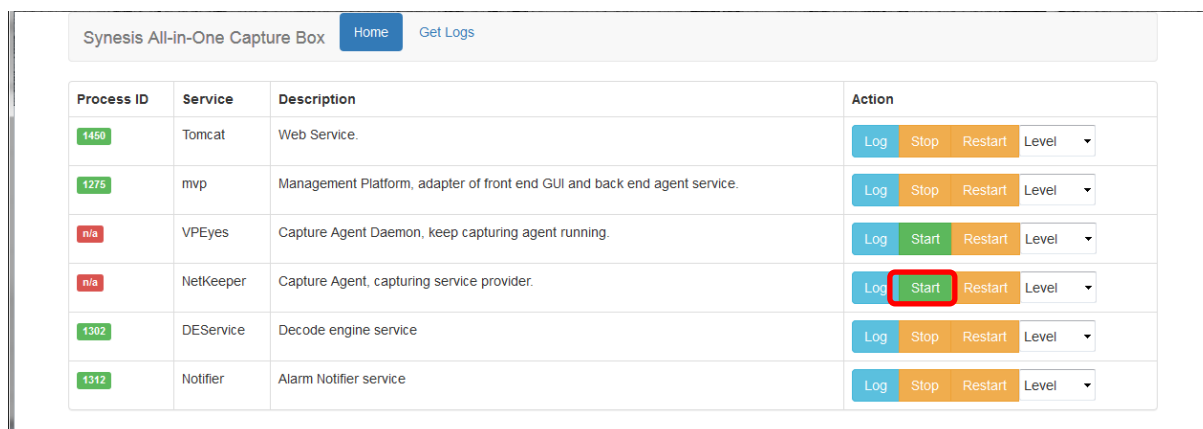
【修正後】

```
TimeSyncConnectorExt1 = PpsIn          # None - NttsIn* - PpsIn - NttsOut - PpsOut - RepeatInt1 - RepeatInt2
```

11. 下記のコマンドを実行し、アダプタの設定の変更を反映させます。

```
$ sudo /opt/napatech3/bin/ntstop.sh
Stopping NTService (this may take a while)
NTService stopped [Done]
$ sudo /opt/napatech3/bin/ntstart.sh
Starting NTService (this may take a while) [Done]
```

12. Synesis 管理画面にアクセスし、NetKeeper サービスの「Start」ボタンをクリックします。



13. 下記コマンドを実行し、OS の内部時計と PPS 信号を同期させます。

```
$ sudo /opt/napatech3/bin/pps_os
```

14. タイムサーバと Synesis が同期した後は、通常通りキャプチャを実行することができます。

キャプチャの開始方法は **5.3.1.1 キャプチャの開始・終了**を参照してください。

15. Ctrl-C を押下し、/opt/napatech3/bin/pps\_os コマンドを終了させると同期は停止します。

## E.2.2 PTP 時刻同期の設定手順

アダプタ(キャプチャカード)の時刻同期ポートを使って、PTP 時刻同期を取ることが可能です。

ご利用になる場合は別売の変換コネクタをご購入ください。


TerTerm がインストールされた PC を使用して、アダプタの設定ファイルを編集します。


下記の手順に従って作業を実行してください。

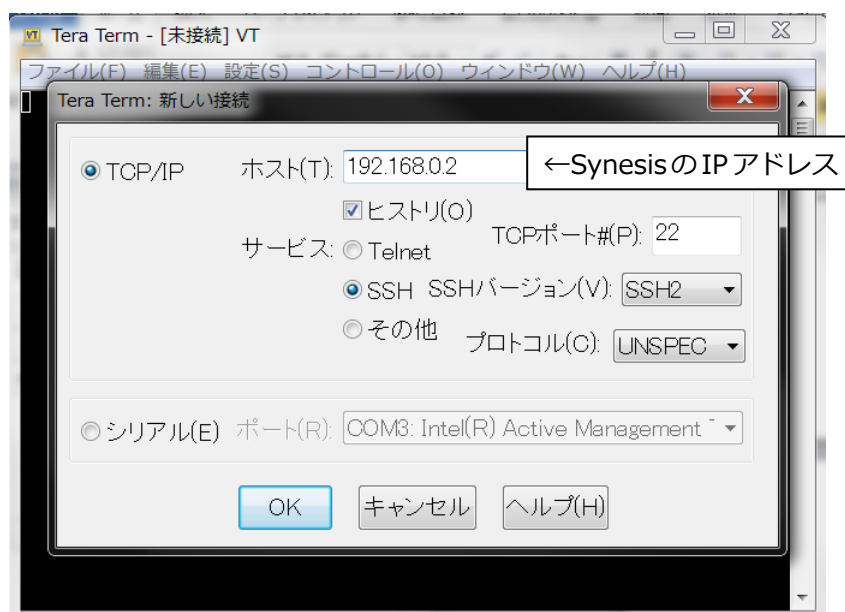
1. NTP サーバの設定を確認します。「構成」  メニュー「時刻同期」を選択してください。



2. PTP 時刻同期では NTP サーバを使用しません。

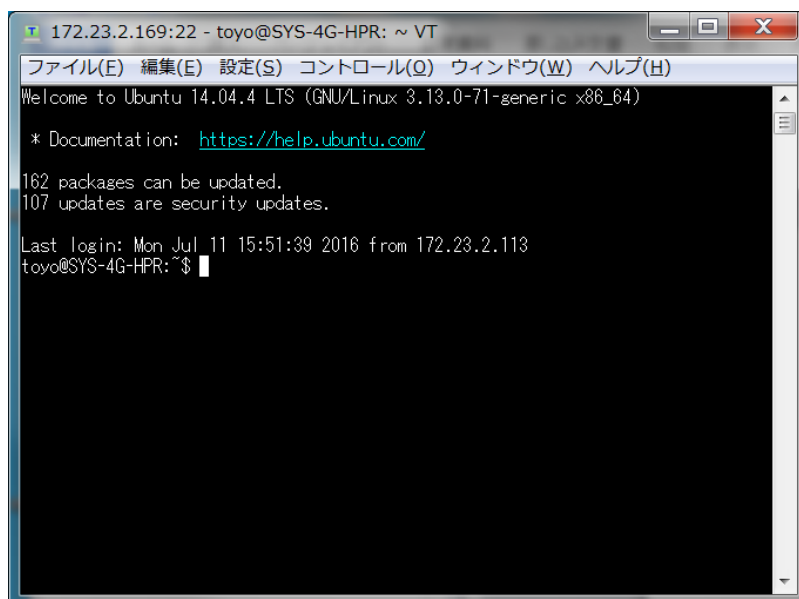
画面左上の ON/OFF ボタンが  OFF になっていることを確認してください。ON になっていた場合はボタンをクリックして、OFF に切替えてください。

3. TeraTerm  を起動します。以下の画面が表示されます。



4. TCP/IP の「ホスト(T)」欄に Synesis の IP アドレスを入力して、「OK」ボタンをクリックしてください。(他の項目はデフォルトのまま変更しません。)

5. Synesis に SSH で接続されます。デフォルトのアカウントは toyo/admin となります。



6. ブラウザを起動し、“http://[Synesis IP]:3000” から Synesis 管理画面にアクセスします。  
NetKeeper サービスの「Stop」ボタンをクリックしてください。

Synesis All-in-One Capture Box			
<a href="#">Home</a> <a href="#">Get Logs</a>			
Process ID	Service	Description	Action
1450	Tomcat	Web Service.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1275	mvp	Management Platform, adapter of front end GUI and back end agent service.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1322	VPEyes	Capture Agent Daemon, keep capturing agent running.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1414	NetKeeper	Capture Agent, capturing service provider.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1302	DEService	Decode engine service	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1312	Notifier	Alarm Notifier service	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾

7. Netkeeper の Process ID が“n/a”に、「Stop」ボタンが緑の「Start」ボタンに変わったことを確認してください。

Synesis All-in-One Capture Box			
<a href="#">Home</a> <a href="#">Get Logs</a>			
Process ID	Service	Description	Action
1450	Tomcat	Web Service.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1275	mvp	Management Platform, adapter of front end GUI and back end agent service.	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
n/a	VPEyes	Capture Agent Daemon, keep capturing agent running.	<a href="#">Log</a> <a href="#">Start</a> <a href="#">Restart</a> Level ▾
n/a	NetKeeper	Capture Agent, capturing service provider.	<a href="#">Log</a> <a href="#">Start</a> <a href="#">Restart</a> Level ▾
1302	DEService	Decode engine service	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾
1312	Notifier	Alarm Notifier service	<a href="#">Log</a> <a href="#">Stop</a> <a href="#">Restart</a> Level ▾

※NetKeeper を停止すると、実行中のキャプチャは停止します。

8. アダプタの設定ファイル "/opt/napatech3/config/ntservice.ini" のバックアップファイルを、"ntservice.ini.org"というファイル名で作成します。

TeraTerm で下記のコマンドを実行してください。

```
$ sudo cp /opt/napatech3/config/ntservice.ini /opt/napatech3/config/ntservice.ini.org
```

9. アダプタの設定ファイルを開き、編集します。

```
$ sudo vi /opt/napatech3/config/ntservice.ini
```

10. アダプタの設定ファイルの [TimeSyncReferencePriority] の項目を [PTP, FreeRun] に変更してください。

【変更前】

```
[Adapter0]
TimeSyncReferencePriority = Ext1, OSTime # FreeRun* - PTP - Int1 - Int2 - Ext1 - OSTime
```

【変更後】

```
[Adapter0]
TimeSyncReferencePriority = PTP, FreeRun # FreeRun* - PTP - Int1 - Int2 - Ext1 - OSTime
```

11. PTP 通信用アドレスに固定 IP アドレスを使用する場合は、[PtpDhcp] を [DISABLE] に変更してください。

【変更前】

```
[Adapter0]
PtpDhcp = ENABLE # DISABLE - ENABLE*
```

【変更後(設定例)】

```
[Adapter0]
PtpDhcp = DISABLE # DISABLE - ENABLE*
PtpIpAddr=192.168.1.2 # IP address
PtpNetMask=255.255.0.0 # IP address
PtpGw=192.168.1.1 # IP address
```

[PtpIpAddr] [PtpNetMask][PtpGw]の各項目には、実際に使用する固定 IP アドレスを入力してください。

12. 使用したい PTP Profile に合わせた設定を反映させます。

対応している Profile は"Default"、"Telecom"です。

- ・ PTP Default profile (profile Id: 00-1B-19-00-01-00)
- ・ Telecom profile (profile Id: 00-19-A7-00-01-00)

【変更前】

```
[Adapter0]
PtpProfile = Default                # Default* - Telecom - Power
```

【変更後】

A) Default、マルチキャストで通信する場合の設定

```
[Adapter0]
PtpProfile = Default                # Default* - Telecom - Power
PtpClockDomain = 0                 # 0 .. 128
```

B) Default、ユニキャストで通信する場合の設定例

```
[Adapter0]
PtpProfile = Default                # Default* - Telecom - Power
PtpClockDomain = 0                 # 0 .. 128
PTPUnicastMasterAddr1 = 0.0.0.0    # IP Address
```

C) Telecom で通信する場合の設定例

```
[Adapter0]
PtpProfile = Telecom                # Default* - Telecom - Power
PtpTelecomDomain1 = 4               # 4 .. 23
PTPUnicastMasterAddr1 = 0.0.0.0    # IP Address
```

※上記の値は実際の環境に合わせて書き換えてください。

※ ユニキャスト通信時に記入する"PTPUnicatMasterAddr1"は GrandMaster の IP アドレスです。

13. Synesis の内部時計(OS 時刻)を PTP 同期したアダプタの時刻に合わせます。

[System]内の[TimeSyncOsTimeRefernce] の項目を [adapter-0] に変更してください。

【変更前】

```
[System]
TimeSyncOsTimeReference = None      # None* - adapter-0 - adapter-1 - adapter-2 - a
adapter-3 - adapter-4 - adapter-5 - adapter-6 - adapter-7
```

【変更後】

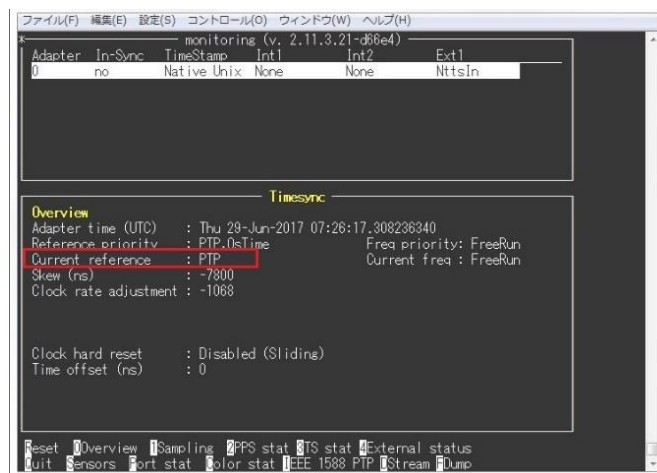
```
[System]
TimeSyncOsTimeReference = adapter-0 # None* - adapter-0 - adapter-1 - adapter-
2 - adapter-3 - adapter-4 - adapter-5 - adapter-6 - adapter-7
```

14. 時刻同期設定が変更されたことを確認します。下記コマンドを実行してください。

```
$ sudo /opt/napatech3/bin/monitoring
```

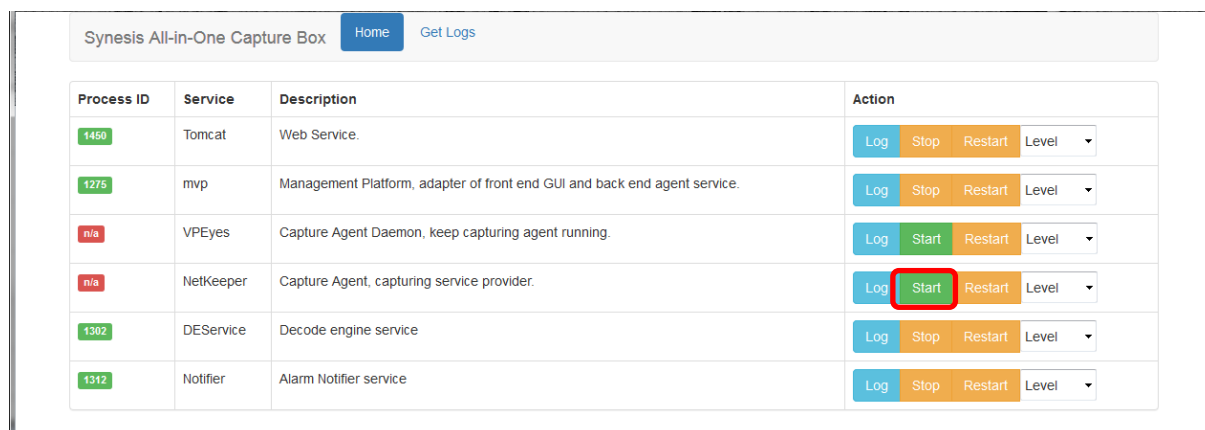
15. アダプタの設定確認ツールが起動します。[Shift]+x で画面を切り替えてください。

Current reference が “PTP” になっていれば成功です。



16. ブラウザから Synesis 管理画面にアクセスします。

NetKeeper サービスの「Start」ボタンをクリックしてください。



この後は、通常通りキャプチャを実行することが可能です。

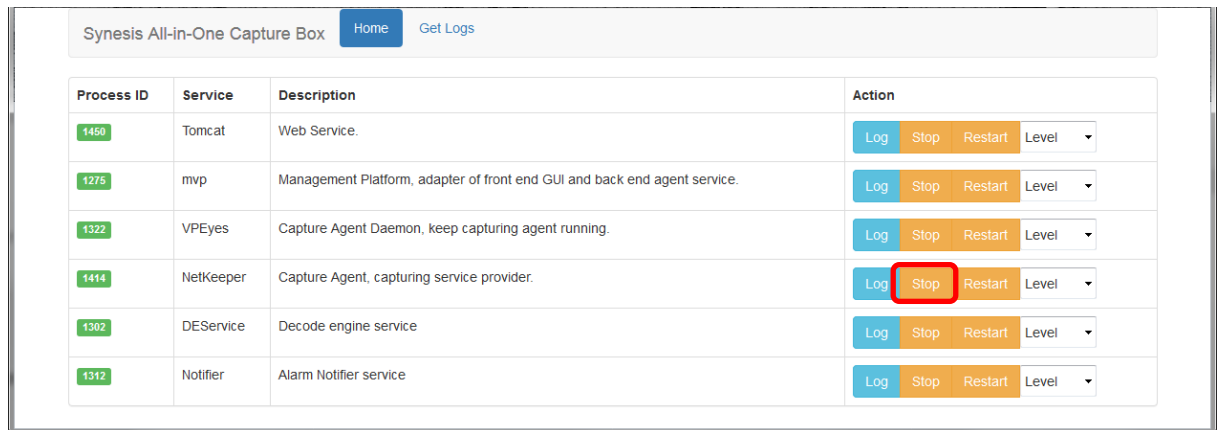
キャプチャの開始方法は **5.3.1.1 キャプチャの開始・終了**を参照してください。

## E.3 設定の切り戻し

アダプタの時刻同期の設定を元の OS 時刻同期に戻したい場合は、設定変更時に作成した設定ファイルのバックアップファイルを使用します。

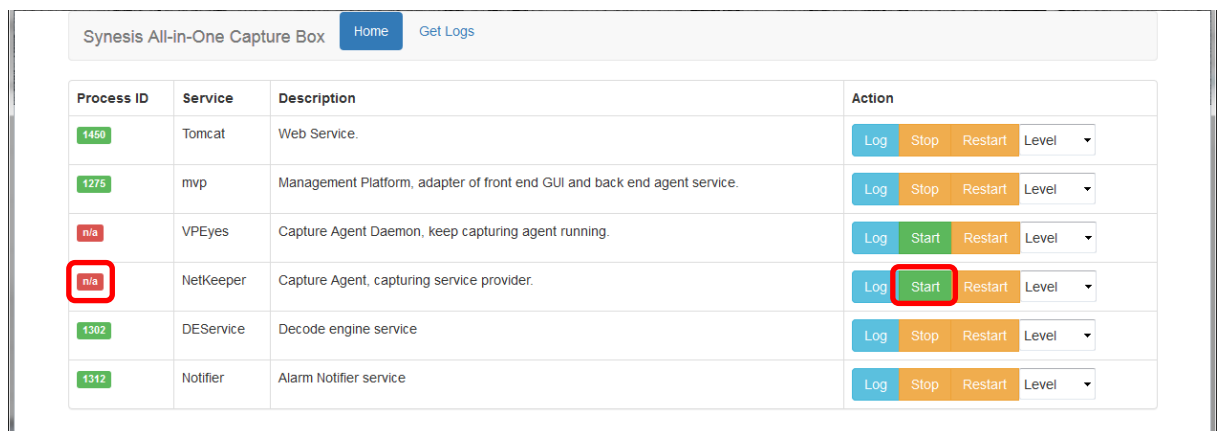
操作は設定時と同様、TeraTerm を使用して SSH で操作を行ってください。

1. ブラウザを起動し、“http://[Synesis IP]:3000” から下図の Synesis 管理画面にアクセスし、NetKeeper サービスの「Stop」ボタンをクリックしてください。



Process ID	Service	Description	Action
1450	Tomcat	Web Service.	Log Stop Restart Level ▾
1275	mvp	Management Platform, adapter of front end GUI and back end agent service.	Log Stop Restart Level ▾
1322	VPEyes	Capture Agent Daemon, keep capturing agent running.	Log Stop Restart Level ▾
1414	NetKeeper	Capture Agent, capturing service provider.	Log Stop Restart Level ▾
1302	DEService	Decode engine service	Log Stop Restart Level ▾
1312	Notifier	Alarm Notifier service	Log Stop Restart Level ▾

2. Netkeeper の Process ID が“n/a”に、「Stop」ボタンが緑の「Start」ボタンに変わったことを確認してください。



Process ID	Service	Description	Action
1450	Tomcat	Web Service.	Log Stop Restart Level ▾
1275	mvp	Management Platform, adapter of front end GUI and back end agent service.	Log Stop Restart Level ▾
n/a	VPEyes	Capture Agent Daemon, keep capturing agent running.	Log Start Restart Level ▾
n/a	NetKeeper	Capture Agent, capturing service provider.	Log Start Restart Level ▾
1302	DEService	Decode engine service	Log Stop Restart Level ▾
1312	Notifier	Alarm Notifier service	Log Stop Restart Level ▾

3. TeraTerm を起動し、SSH でログインしてください。
4. PPS 時刻同期用 pps\_os が実行中であれば、停止させてください。
5. 以下のコマンドでバックアップした設定ファイルをリストアします。

```
$ sudo mv /opt/napatech3/config/ntservice.ini.org /opt/napatech3/config/ntservice.ini
```

6. 以下のコマンドでアダプタの設定を反映させます。

```
$ sudo /opt/napatech3/bin/ntstop.sh
Stopping NTService (this may take a while)
NTService stopped [Done]
$ sudo /opt/napatech3/bin/ntstart.sh
Starting NTService (this may take a while) [Done]
```

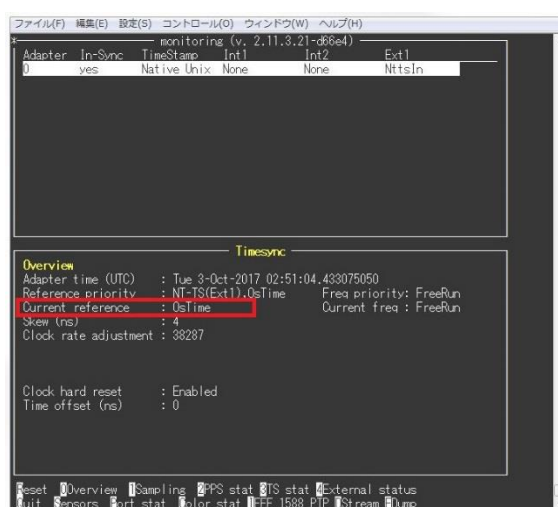
7. アダプタの時刻同期の設定が OS 時刻同期に戻っていることを確認します。

下記コマンドを実行してください。

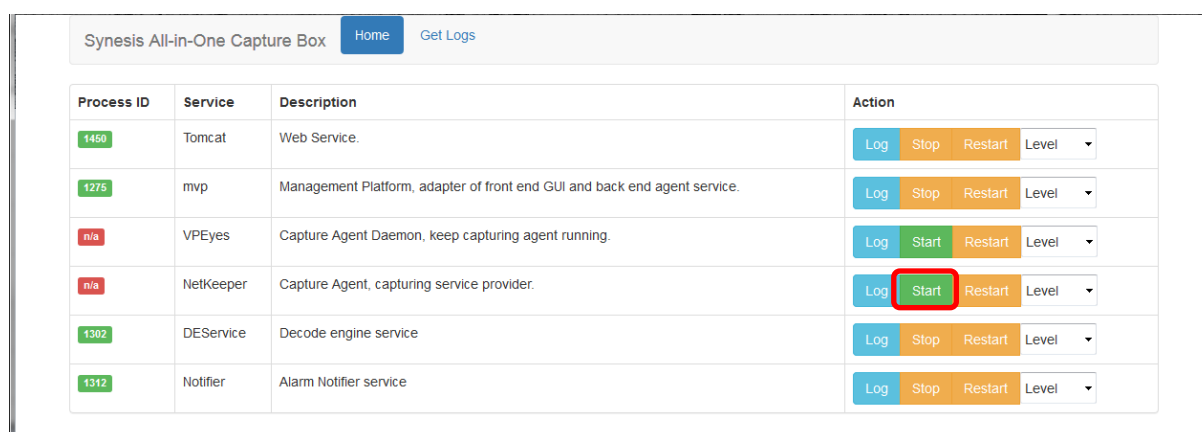
```
$ sudo /opt/napatech3/bin/monitoring
```

8. アダプタの設定確認ツールが起動します。[Shift]+x で画面を切り替えてください。

9. Current reference が "OsTime" になっていることを確認します。



10. 下記 Synesis 管理画面にアクセスし、NetKeeper の「Start」ボタンをクリックします。



11. 必要に応じて、OS と NTP サーバとの同期を再開させます。

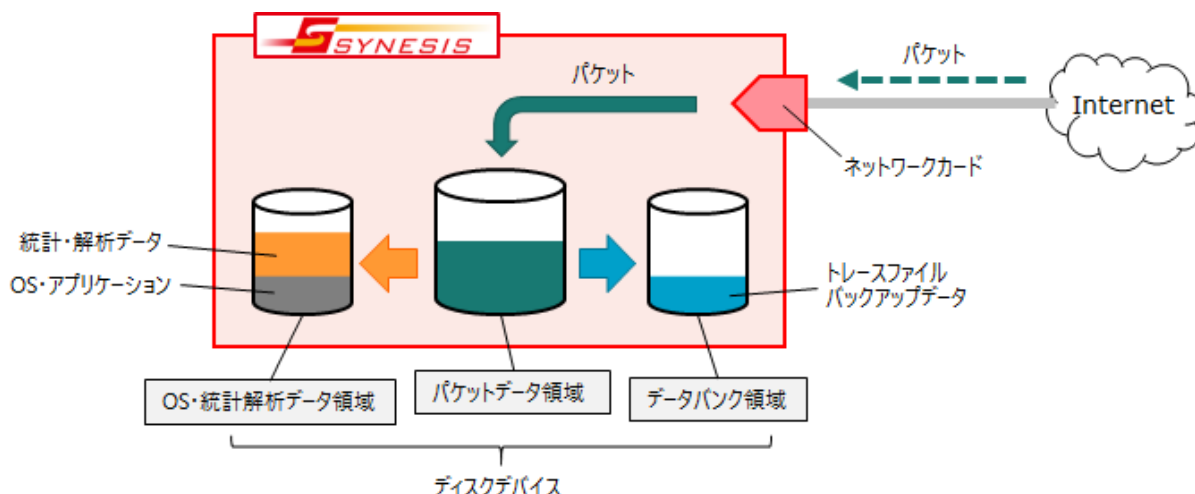
詳細は **12.4 時刻同期**を参照してください。



## Appendix F Synesis のディスク構成

### F.1 概要

Synesis 内部のディスクデバイスは 3 つの領域に分かれています。それぞれの名称は「パケットデータ領域」、「OS・統計解析データ領域」、「データバンク領域」です。



### F.2 パケットデータ領域

この領域には、下記のデータが保存されます。

- ネットワークカードでキャプチャしたパケット
- パケットデータのインデックス情報

実際のファイルパスは /pvc/data/packetdbN/ (N = 1, 2, ...) です。

パケットデータ領域の全容量および使用量は、**5.3.2.8 ストレージ情報** で確認できます。

### F.3 OS・統計解析データ領域

この領域には、下記のデータが保存されます。

- 出荷時にインストールされた OS およびアプリケーションデータ
- キャプチャしたパケットの DLC 統計データ、および APM/NPM 解析・マイクロバースト解析データ

Synesis を継続して使用すると統計・解析データの容量が増加し、動作に影響を与える場合があります。それを防ぐため、出荷時にはデータベースのエイジアウト機能が有効になっています。

詳細は **12.12 解析** の **[データベースのエイジアウトを有効にする]** を参照してください。

## F.4 データバンク領域

ユーザが作成したデータを保存する領域です。下記の機能で作成されたデータが保存されます。

- トレース保存で保存先フォルダにビルトインフォルダを指定したトレースファイル
- トレースファイル タブ の「トレースバンカー」にアップロードされたトレースファイル
- 自動保存で作成されたトレースファイル(変更可能※)
- バックアップ機能で作成されるバックアップデータ
- 統計のエクスポートで作成した CSV ファイル
- レポート作成機能で作成されたレポートファイル

実際のファイルパスは /pvc/data/databank です。

データバンク領域の全容量および使用量は、**5.3.4 トレースファイル** タブ の **[ディスク容量情報]** で確認できます。

## Appendix G 使用するポートの一覧

---

Synesis では下記のポートを使用します。

ポート番号	説明
<b>22</b>	Synesis に SSH で接続する際に使用します
<b>1311</b>	Open Manage Server Administrator で使用します。このポートは、Synesis Distributed のみ使用します。Synesis Portable では使用しません。
<b>2002</b>	WinPcap remote packet capture daemon
<b>3000</b>	Synesis Admin Management Page
<b>3389</b>	リモートデスクトップで使用します。
<b>5432</b>	PostgreSQL データベースへのアクセスに使用します
<b>5433 ~ 5435</b>	バックアップの作成、および外部データソースの有効化において、PostgreSQL データベースへのアクセスに使用します
<b>8080</b>	Synesis の Web アプリケーションで使用します
<b>9010</b>	Synesis のプロセス間通信で使用します (thrift)
<b>9012</b>	Synesis のエージェントプロセスを監視する用途で使用します (VPEyes)
<b>9013 ~ 9014</b>	バックアップの作成、および外部データソースの有効化において、エージェントプロセスを監視する用途で使用します (VPEyes)
<b>9050 ~ 9059</b>	Decode サービスの通信で使用します
<b>9090</b>	Synesis のプロセス間通信で使用します (mvp)
<b>9999</b>	Remote monitoring JVM で使用します。

## Appendix H モデルによる違い

モデルによって異なる点は下表の通りです。

表 H-1 モデル別機能対応表

モデル	SYS-2G-EP SYS-2G-ER	SYS-4G-STP SYS-4G-STR	SYS-4G-HPP SYS-4G-HPR SYS-10G-CP SYS-10G-R SYS-20G-CP SYS-20G-R SYS-20G-HPR SYS-20G-HPP SYS-40G-HPR SYS-40G-HPP	SYS-8G2-HPR SYS-80G2-HPR	SYS-100G-HPP SYS-100G-HPR
キャプチャフィルタ	×	×	○	○	○
PTP/1PPS	×	×	○	×	×
エラーフィルタ (保存フィルタ)	×	○	○	○	×
CRC〜ラント	×	○	○	○	○
ジャバー・オーバーサイズ	×	9018byte	9018byte	9018byte	9018byte
キャプチャ可能な 最大パケット長(byte)	14440byte	10000byte	10000byte	10000byte	10000byte
スライス	64〜	32〜	32〜	32〜	32〜
リンクステータス	非対応(灰色)	緑／赤	緑／赤	緑／赤	緑／赤

表 H-2 推奨されるダッシュボードのグラフ数

モデル	SYS-2G-EP SYS-4G-STP SYS-4G-HPP SYS-10G-CP SYS-20G-HPP SYS-100G-HPP	SYS-2G-ER SYS-4G-STR SYS-4G-HPR SYS-20G-CP SYS-40G-HPP	SYS-8G2-HPR SYS-10G-R SYS-20G-R SYS-20G-HPR SYS-40G-HPR SYS-100G-HPR	SYS-80G2-HPR
ダッシュボードのグラフ数	4		12	

表 H-3 ポート図 具体的なポートやチャネルの位置は次章のポート図を参照ください

Synesis Distributed(1U 版)	SYS-2G-ER	SYS-4G-STR	SYS-4G-HPR	
Synesis Distributed(2U 版)	SYS-8G2-HPR SYS-20G-HPR	SYS-10G-R SYS-40G-HPR	SYS-20G-R SYS-80G2-HPR	SYS-100G-HPR
Synesis Portable-1	SYS-2G-EP	SYS-4G-STP	SYS-4G-HPP	SYS-10G-CP
Synesis Portable- 2	SYS-20G-CP			
Synesis Portable- 3	SYS-20G-HPP	SYS-40G-HPP		
Synesis Portable-4	SYS-80G-HPP	SYS-100G-HPP		

## Appendix I 各モデルのポートとチャネルの配置

Synesis はモデルによって各ポートとチャネルの位置が異なります。

どのポート図を参照するかは前章 **Appendix H モデルによる違い**の表 H-3 を参照してください。





### I.1 Synesis Distributed(1U 版)ポート図

ラックマウントタイプ 1U 版の Synesis の各ポートの位置は下図の通りです。



<b>D</b>	VGA(アナログ RGB)端子です。 VGA モニタ(同梱されていません)を接続してください。
<b>K</b>	USB 端子です。
<b>R</b>	管理用イーサネットポートです。 Synesis をリモート操作・管理する場合は、これらのイーサネットポートの 1 つを 管理用ネットワークへ接続してください。
<b>C</b>	アダプタ(キャプチャカード)の入力端子です。 これらのポートとモニタ、キャプチャしたいネットワークを接続してください。 ※各チャネルの位置は下の表を参照してください。
<b>P</b>	AC 電源ケーブルを接続してください。 電源への入力は 100-240 V AC (オート・レンジング)、50/60 Hz です

各モデルのチャネルの位置は以下の通りです。

チャネル位置	対象モデル
 	SYS-2G-ER
	SYS-4G-STR
	SYS-4G-HPR

## I.2 Synesis Distributed (2U版)ポート図

ラックマウントタイプ 2U版の Synesis の各ポートの位置は下図の通りです。

[メインユニット]



[拡張ストレージ]



※拡張ストレージは S/N ラベルの末尾で区別します。拡張ストレージ 2 = S/N ラベルの末尾が "-2"

<b>D</b>	VGA(アナログ RGB)端子です。 VGA モニタ(同梱されていません)を接続してください。
<b>K</b>	USB 端子です。
<b>R</b>	管理用イーサネットポートです。 Synesis をリモート操作・管理する場合は、これらのイーサネットポートの 1 つを管理用ネットワークへ接続してください。
<b>C</b>	アダプタ(キャプチャカード)の入力端子です。 これらのポートとモニタ、キャプチャしたいネットワークを接続してください。 ※各チャンネルの位置は下の表を参照してください。
<b>P</b>	AC 電源ケーブルを接続してください。 電源への入力 は 100-240 V AC (オート・レンジング)、50/60 Hz です
<b>Slot1,2,3,4</b>	拡張ストレージがある(SYS-100G-HPR 以外の)場合は、メインユニットの Slot1 の Port0 と拡張ストレージの Port1 を SAS ケーブルで接続してください。 SYS-100G-HPR の場合は、メインユニットの Slot1~4 の Port0 を、Slot の番号と一致した番号の拡張ストレージ 1~4*の Port1 に、メインユニットの Slot1~4 の Port1 を拡張ストレージ 1~4 の Port2 に接続してください。

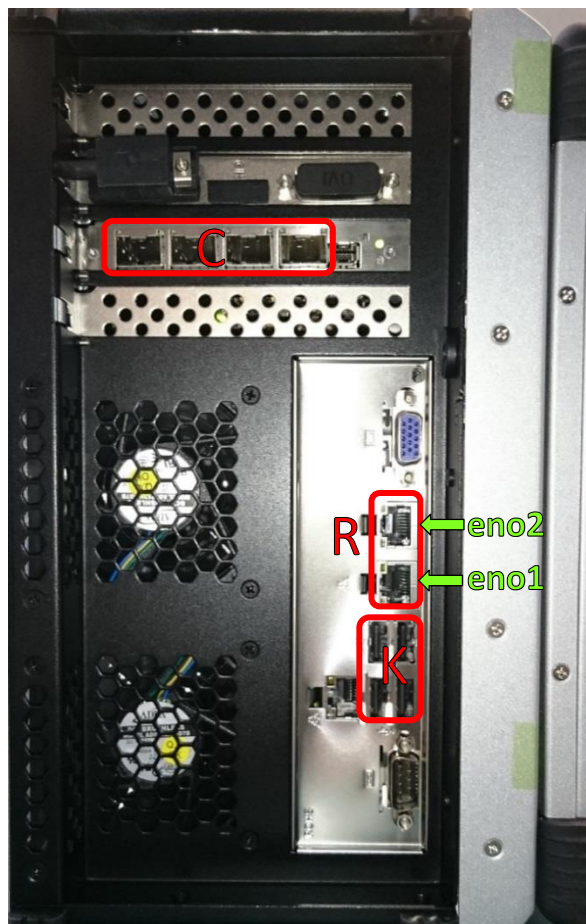
各モデルのチャンネルの位置は以下の通りです。

チャンネル位置	対象モデル
	SYS-10G-R, SYS-20G-HPR
	SYS-100G-HPR
	SYS-10G-R2, SYS-20G-R, SYS-40G-HPR
	SYS-8G2-HPR, SYS-80G2-HPR

## I.3 Synesis Portable-1

ポータブルタイプ、SYS-2G-EP と SYS-4G-STP, SYS-4G-HPP, SYS-10G-CP のポート図になります。

AC 電源ケーブルの接続箇所が本体の逆に付いています。



注意：AC 電源ケーブルの  
接続箇所は反対側の  
側面にあります。

<b>K</b>	USB 端子です。
<b>R</b>	管理用イーサネットポートです。 Synesis をリモート操作・管理する場合は、これらのイーサネットポートの 1 つを 管理用ネットワークへ接続してください。
<b>C</b>	アダプタ(キャプチャカード)の入力端子です。 これらのポートとモニタ、キャプチャしたいネットワークを接続してください。 ※各チャンネルの位置は下の表を参照してください。

各モデルのチャンネル位置は以下の通りです。

チャンネル位置	対象モデル
∴ [D] [C] [B] [A] ∴ □	SYS-2G-EP
[A] [B] [C] [D] ∴	SYS-4G-STP
[A] [B] [C] [D] □ ∴	SYS-4G-HPP
[A] [B] □ □ □ ∴	SYS-10G-CP



I.4 Synesis Portable-2

ポータブルタイプ、SYS-20G-CP のポート図になります。  
AC 電源ケーブルの接続箇所が本体の逆に付いています。



注意 : AC 電源ケーブルの  
接続箇所は反対側の  
側面にあります。

K	USB 端子です。
R	管理用イーサネットポートです。 Synesis をリモート操作・管理する場合は、これらのイーサネットポートの 1 つを 管理用ネットワークへ接続してください。
C	アダプタ(キャプチャカード)の入力端子です。 これらのポートとモニタ、キャプチャしたいネットワークを接続してくださ い。 ※各チャンネルの位置は下の表を参照してください。

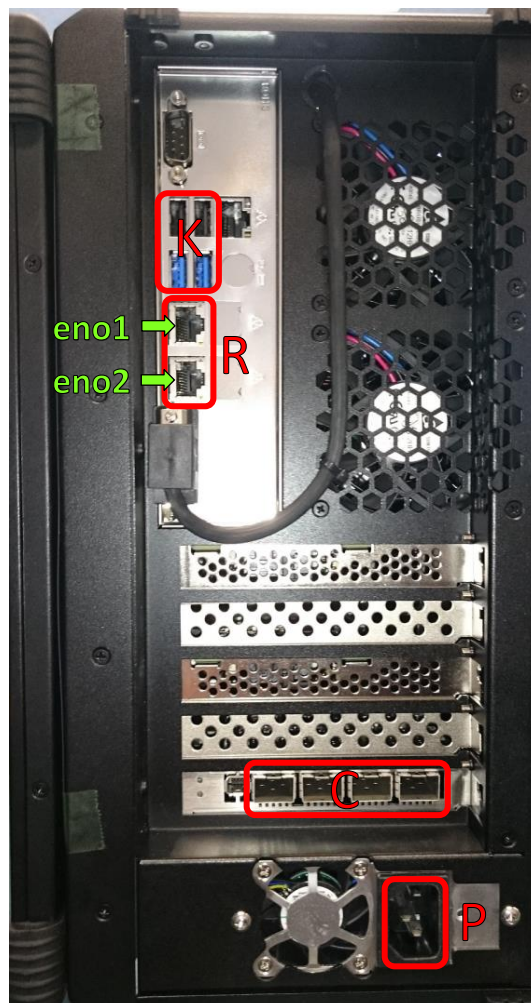
チャンネル位置は以下の通りです。

チャンネル位置	対象モデル
<div><div>A</div><div>B</div><div>C</div><div>D</div><div></div><div></div></div>	SYS-20G-CP



## I.5 Synesis Portable-3

ポータブルタイプ、SYS-20G-HPP と SYS-40G-HPP のポート図になります。



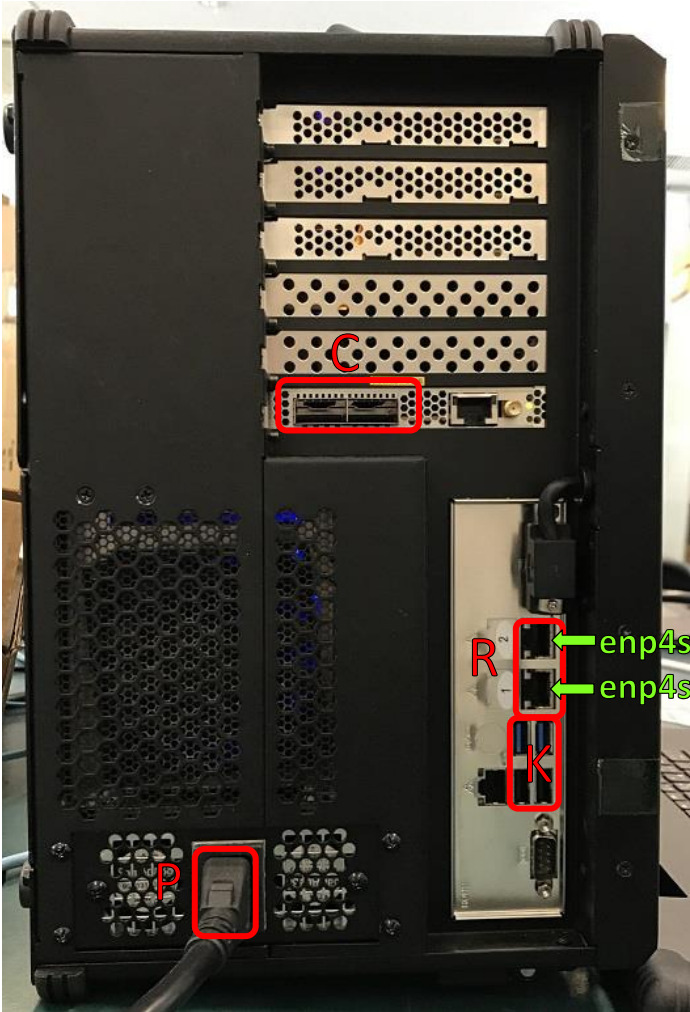
<b>K</b>	USB 端子です。
<b>R</b>	管理用イーサネットポートです。 Synesis をリモート操作・管理する場合は、これらのイーサネットポートの 1 つを管理用ネットワークへ接続してください。
<b>C</b>	アダプタ(キャプチャカード)の入力端子です。 これらのポートとモニタ、キャプチャしたいネットワークを接続してください。 ※各チャンネルの位置は下の表を参照してください。
<b>P</b>	AC 電源ケーブルを接続してください。 電源への入力 は 100-240 V AC (オート・レンジング)、50/60 Hz です

チャンネル位置は以下の通りです。

チャンネル位置	対象モデル
 <div style="display: inline-block; border: 1px solid black; padding: 2px 10px; margin: 0 5px;">B</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px; margin: 0 5px;">A</div>	SYS-20G-HPP
 <div style="display: inline-block; border: 1px solid black; padding: 2px 10px; margin: 0 5px;">D</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px; margin: 0 5px;">C</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px; margin: 0 5px;">B</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px; margin: 0 5px;">A</div>	SYS-40G-HPP

I.6 Synesis Portable-4

ポータブルタイプ、SYS-80G-HPP と SYS-100G-HPP のポート図になります。



K	USB 端子です。
R	管理用イーサネットポートです。 Synesis をリモート操作・管理する場合は、これらのイーサネットポートの 1 つを管理用ネットワークへ接続してください。
C	アダプタ(キャプチャカード)の入力端子です。 これらのポートとモニタ、キャプチャしたいネットワークを接続してください。 ※各チャンネルの位置は下の表を参照してください。
P	AC 電源ケーブルを接続してください。 電源への入力 は 100-240 V AC (オート・レンジング)、50/60 Hz です

チャンネル位置は以下の通りです。

チャンネル位置	対象モデル
<div><div>A</div><div>B</div></div> <div></div>	SYS-80G-HPP, SYS-100G-HPP

## Appendix J RESTful API

---

Synesis は、各種機能を組み合わせて利用できる利便性の高いインターフェースを提供しています。現在は、エージェントリストの取得、接続のリストの取得、フィルタリストの取得、キャプチャしたレコードの取得、レコードの状態の取得、レコードのロック、レコードの削除、キャプチャの開始、キャプチャの停止、ユーザ認証、トレースの保存、フィルタの保存が提供されています。詳細は RESRful API 資料をご覧ください。

---

**東陽テクニカ**  
**Synesis 取扱説明書**

Copyright © 2015 TOYO Corporation All Rights Reserved.

---