東陽テクニカ

SYNESIS

取扱説明書

2021/04/08

A010-1799-90

Rev. 6.0.5.1

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
Rev.K	2018/02/06	Synesis 3.7
Rev.L	2020/04/06	SYNESIS 5.0
Rev.M	2020/08/04	SYNESIS 5.5
Rev.N	2021/02/10	SYNESIS 6.0
Rev.6.0.5.1	2021/04/08	SYNESIS 6.0.5、細かい点を修正

安全上の注意

警告

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された時点で、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実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い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 および PacketReplayer(パケットリプレイヤー)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)

https://www.synesis.tech/

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 技術部 SYNESIS サポートグループ

TEL : 03-3279-0771(代表)　03-3245-1107(直通)

FAX : 03-3246-0645

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

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

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. はじめに 1
1.1. 表記規則および略号 1
1.2. SYNESIS の機能 1
2. SYNESIS の構造 4
2.1. SYNESIS について 4
2.2. エージェントのプロセス管理 5
2.3. SYNESIS のディスク領域 6
2.3.1. パケットデータ領域 6
2.3.2. OS・統計解析データ領域 7
2.3.3. データバンク領域 7
2.4. 使用するポートの一覧 8
2.4.1. 外部との通信で使用するポート 8
2.4.2. ループバック通信で使用するポート 9
2.4.3. Distributed モデルの iDRAC との通信に使用するポート 9
2.5. Web アプリケーションのセッション管理 9
2.6. 画面構成 12
2.6.1. メインメニュー 13
2.6.2. ツールバーメニュー 14
2.6.3. エージェント・ペインとワークスペース 15
2.6.4. 一覧表示の項目の表示設定 16
2.6.5. グラフ画面での期間指定 17
2.6.6. ダイアログの必須項目 18
2.6.7. 構成の項目編集 19
2.7. アドレス帳の設定 20

3. 起動・終了・接続方法 21
3.1. SYNESIS の初期設定 21
3.2. SYNESIS の起動 21
3.3. SYNESIS の終了 23
3.4. 接続方法 24
3.4.1. SYNESIS の IP アドレスの確認方法 24
3.4.2. Web ブラウザ接続 24
3.4.3. リモートデスクトップ接続 25
3.4.4. SSH 接続 27
4. キャプチャの開始・停止 28
4.1. キャプチャの開始・停止手順 28
4.2. キャプチャを開始する前に設定する項目 30
4.3. キャプチャ全般に関する制限 30
4.4. キャプチャオプション 31
4.4.1. 共通 オプション 32
4.4.2. キャプチャフィルタ オプション 36
4.4.3. ロックトリガオプション 37
4.4.4. 自動保存オプション 38
4.4.5. チャネル設定 41
4.4.6. 通知設定 42
4.5. レコードのよるキャプチャデータの管理 43
4.5.1. レコード一覧 43
4.5.2. レコードからの操作 44
4.5.3. レコードの分割 45
4.6. キャプチャのステータス 48
4.6.1. キャプチャの設定情報 48
4.6.2. キャプチャの統計情報 50
4.6.3. 統計情報のトレンドグラフ 51
5. トレースの保存操作 52
5.1. トレースの保存画面 52
5.2. タイムレンジの設定と自動入力 53
5.3. 保存フィルタの適用 54
5.4. トレースの保存先 55

5.4.1. ビルドインファイル.....56
5.4.2. カスタムファイル.....57
5.4.3. トレースバンカー.....57
5.5. トレースファイルの操作 58
5.6. 各画面での機能差異 59
5.7. トレースの保存全般の制限事項..... 59
5.8. トレースファイルのサイズ..... 60
6. フィルタ機能 61
6.1. キャプチャフィルタの概要..... 61
6.2. キャプチャフィルタの項目..... 63
6.2.1. MAC アドレス 63
6.2.2. VLAN 63
6.2.3. イーサタイプ 64
6.2.4. IP フロー 65
6.2.5. フロー 66
6.2.6. アプリケーション.....67
6.2.7. パターン 68
6.3. キャプチャフィルタ時のトンネルオプション 69
6.3.1. アウターヘッダ 69
6.3.2. インナーヘッダ 70
6.3.3. 全てのヘッダ 70
6.3.4. トンネルオプションの制限.....71
6.4. 保存フィルタの概要 71
6.4.1. 保存フィルタの作成・管理.....72
6.4.2. 保存フィルタの詳細設定.....74
6.5. 保存フィルタの項目 75
6.5.1. チャネル 77
6.5.2. エラー 77
6.5.3. パケットサイズ 78
6.5.4. MAC アドレス 78
6.5.5. VLAN 79
6.5.6. L2 イーサタイプ 79
6.5.7. L3 プロトコル.....80
6.5.8. フロー 81
6.5.9. TCP フラグ.....82

6.5.10. TCP ウィンドウサイズ 82
6.5.11. アプリケーション 83
6.5.12. パターン 84
6.5.13. VoIP 85
6.6. フィルタ共通の定義 86
6.6.1. 「パターン」と「マスク」の指定方法 86
7. デコード機能 87
7.1. リアルタイムデコード 87
7.2. トレースファイルからのデコード 88
7.3. デコード画面の構成 88
7.3.1. パケット一覧 89
7.3.2. パケット詳細 90
7.3.3. バイト列 90
7.3.4. 検索機能 90
7.3.5. 表示フィルタ 91
7.3.6. エキスパート情報 92
7.3.7. トレースの保存 93
7.3.8. Lua プラグインの適用 93
8. 統計情報 94
8.1. レコード全体のトレンド表示 94
8.1.1. チャネルの合計値のトレンドグラフ 95
8.1.2. チャネルごとの統計値 95
8.1.3. チャネルごとのトレンドグラフ 96
8.1.4. 期間を指定しての拡大表示 97
8.1.5. トレンド表示からのトレースの保存 97
8.2. 統計のエクスポート 98
8.2.1. 統計値の CSV ファイルの作成手順 98
8.2.2. 統計のエクスポートに関する制限事項 100
8.3. 統計値の定義 101
9. ロック機能 103
9.1. 手動ロック 103
9.1.1. レコード単位のロック設定 104
9.1.2. 期間指定のロック設定 104
9.2. 自動ロック 106

9.2.1. 時間トリガ 107
9.2.2. SNMP トラップトリガ 107
9.3. ロックタブの構成 108
9.3.1. レコードのロック解除 108
9.3.2. トレースの保存 108
9.3.3. ロック名の変更 108
10. 解析機能 109
10.1. 解析機能の概要 109
10.1.1. 解析を実行するタイミング 110
10.1.2. 解析前に必要な設定項目 110
10.1.3. 解析実行手順 110
10.2. APM/NPM 解析 111
10.2.1. APM/NPM の画面構成 112
10.2.2. APM/NPM の期間指定 112
10.2.3. APM/NPM 解析の検索項目と KPI 114
10.2.4. APM 解析のフローテーブル 116
10.2.5. NPM 解析でのフローテーブル 117
10.2.6. APM/NPM 解析の制限事項 118
10.3. APM/NPM に関する KPI の定義 119
10.3.1. サーバの規則(APM/NPM 共通) 119
10.3.2. TopN 表示の規則(APM/NPM 共通) 119
10.3.3. APM の KPI 119
10.3.4. NPM の KPI 121
10.4. マイクロバースト解析 122
10.4.1. マイクロバーストの閾値の検出方法 122
10.4.2. マイクロバーストのリアルタイム検出 123
10.4.3. マイクロバーストの画面構成 124
10.4.4. マイクロバーストの期間指定 126
10.4.5. マイクロバーストの再解析 127
10.4.6. マイクロバーストの外部通知 128
10.4.7. マイクロバースト解析に必要なディスク容量 128
10.4.8. マイクロバースト解析に関する制限事項 128
10.5. 解析に関する設定項目と仕様 129
10.5.1. 解析共通 129
10.5.2. APM/NPM の事前設定 130

10.5.3. マイクロバーストの閾値設定 141
11. ダッシュボード 143
11.1. ダッシュボードの作成・管理 143
11.2. 新規グラフの追加と設定 145
11.2.1. 選択可能なグラフ種別 145
11.2.2. グラフの追加手順 146
11.2.1. グラフの設定変更 147
11.2.2. 新規グラフの設定項目 148
11.3. 画面の操作方法 149
11.3.1. 時間範囲の選択 149
11.3.2. グラフの拡大表示 149
11.3.3. 各チャネルデータの表示/非表示の切替え 150
11.3.4. 配置可能なグラフ数 150
11.4. ダッシュボードのグラフに関する制限事項 150
12. レポート 151
12.1. レポートテンプレート 152
12.1.1. レポートテンプレートの作成・管理 152
12.1.2. 選択可能なグラフの種類 154
12.1.3. 新規グラフの設定項目 154
12.1.4. レポートロゴの変更 156
12.1.5. レポートテンプレートのエクスポートとインポート 156
12.2. レポートプラン 157
12.2.1. レポートプランの作成・管理 157
12.2.2. 周期レポートと周期レポート 159
12.2.3. 統計情報レポートの CSV ファイルで出力 160
12.3. レポートリスト 161
12.3.1. 作成されたレポートの管理 161
12.3.2. レポートの保存場所 162
12.4. サンプルレポート 162
12.4.1. デイリー・レポート例 164
12.4.2. マンスリー・レポート例 164
12.5. レポートに関する制限事項 165
13. MFA(マルチフロー解析) 166
13.1. MFA 機能の概要 166

13.1.1. プロファイルの作成・管理 167
13.1.2. ラダービュータブ 172
13.1.3. ラダービューからの操作 173
13.1.4. 統計タブ 175
13.1.5. データソースと制限 176
13.2. フロービュー 177
13.2.1. アプリケーション・ツリー 178
13.2.2. フローリスト 178
13.2.3. フロービューの操作 179
13.3. MFA ビュー 181
13.3.1. MFA ビューの作成手順 181
13.3.2. MFA のラダービュー表示と解析手法 182
13.4. パケットロス解析 183
13.4.1. パケットロス解析の作成手順 184
13.4.2. パケットロス・テーブル 184
13.5. MFA に関する設定項目と仕様 185
13.5.1. MFA の表示設定 185
13.5.2. 自動時刻同期の仕様 186
13.5.3. MFA に関する KPI の定義 187
14. アラート機能と通知 188
14.1. アラート検出手順 188
14.1.1. 閾値の設定 189
14.1.2. アラート一覧 190
14.2. アラートの画面構成 191
14.2.1. アラートの期間指定 192
14.2.2. 検索条件 193
14.2.3. アラート一覧 194
14.3. 通知 194
14.3.1. 通知先の設定 195
14.3.2. 通知グループの設定 197
14.3.3. 通知設定の確認 199
15. ユーザと認証 200
15.1. ユーザの登録・管理 200
15.2. ユーザの機能制限 202

15.3. デフォルトユーザの扱い 203
15.4. 外部認証.....203
15.4.1. 外部認証に関する制限事項.....205
16. 時刻同期.....206
16.1. NTP サーバとの時刻同期.....206
16.2. PPS＋NTP 時刻同期.....207
16.2.1. PPS＋NTP 時刻同期の設定手順.....207
16.2.2. PPS＋NTP 時刻同期の際の注意点.....211
16.3. PTP 時刻同期の設定手順.....211
16.3.1. PTP 時刻同期の設定手順.....212
16.3.2. PTP 時刻同期の設定切り戻し.....217
16.4. 複数のキャプチャアダプタを使用する場合の時刻同期.....219
17. 管理ツール.....220
17.1. 設定のバックアップ・リストア.....220
17.1.1. 設定のバックアップ作成とダウンロード.....220
17.1.2. 設定のリストア.....221
17.1.3. バックアップファイルのアップロード.....221
17.1.4. バックアップファイルの削除.....222
17.1.5. バックアップ対象一覧.....222
17.1.6. バックアップ・リストアに関する制限.....223
17.2. SYNESIS の初期化.....224
17.2.1. 初期化対象一覧.....225
17.2.2. 初期化に関する既知の不具合.....226
18. 構成.....227
Appendix A 用語集.....229

1.はじめに

本書は、SYNESIS の機能の概要、基本的な操作を説明しています。SYNESIS を導入、使用する前にお読みください。

SYNESIS は、高速・大容量のトラフィックを取りこぼしなく連続してキャプチャし、長期間パケットを保存できる製品です。保存されたパケットは、簡単な操作で抽出、解析が行えます。

1.1. 表記規則および略号

本書で使用する表記規則は下記の通りです。

表記	説明
[メニュー名]	操作画面上に表示されるメニュー名またはボタン名を意味します。
<ボタン名>	キーボード上のキーを意味します。
「設定項目」	操作画面上の設定項目を意味します。
>	画面遷移を意味します。

なお、記号は特に断りがない限り、原則半角で表現します。

1.2. SYNESIS の機能

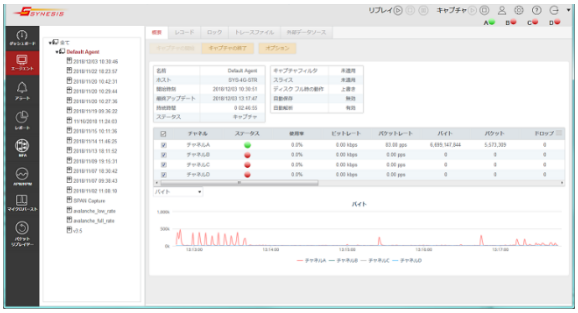
SYNESIS の持つ主な機能は、以下の通りです。

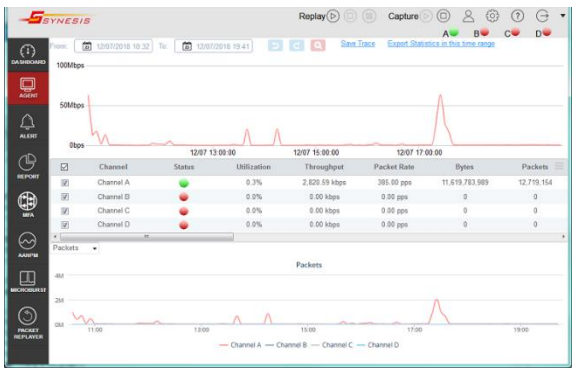
- パケットキャプチャ機能

イーサネットを流れるパケットをキャプチャし、ディスク内に保存します。

キャプチャの開始と停止は、ボタンをクリックするだけで簡単に操作することができます。

詳細は、**キャプチャの開始・停止**の章を参照してください。





- トレースファイルの保存機能

レコードから、必要な部分だけを抽出したトレースファイルを作成することができます。

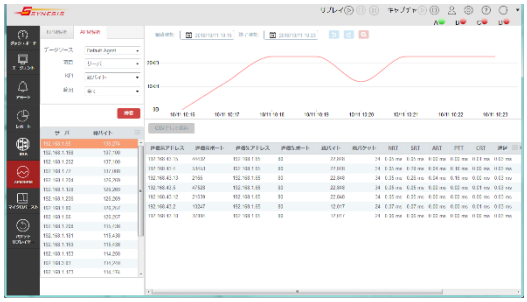
作成したトレースファイルはブラウザからのダウンロードが可能です。

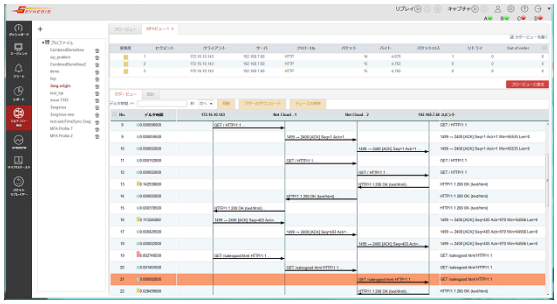
詳細は、**トレースの保存操作**の章を参照してください。

- 解析機能

キャプチャした大量なパケットから通信の動向を把握することができます。解析画面から、フロー、期間を確認し、目的のパケットを簡単に取り出すことが可能です。

詳細は、**解析機能**の章を参照してください。





- MFA 機能

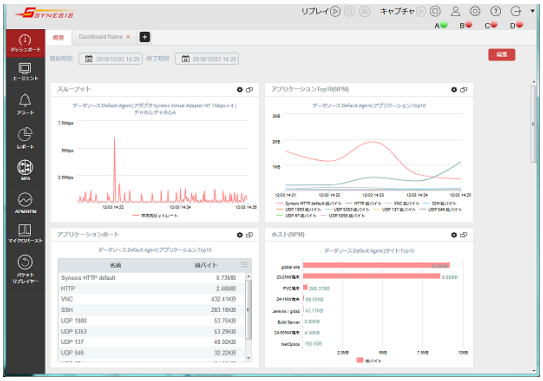
キャプチャデータごとにキャプチャポイントを定義し、フローを抽出して図示することができます。キャプチャしたデータをクライアントとサーバに分類し、フローごとの挙動がパケット単位で確認できます。

詳細は、**MFA(マルチフロー解析)**の章を参照してください。

- ダッシュボード

キャプチャしたデータを現在の時刻から遡った期間で、複数のグラフを 1 画面に表示します。表示可能な期間は、5 分、30 分、1 時間、8 時間、24 時間から選択できます。

詳細は、**ダッシュボード**を参照してください。



- レポート作成機能

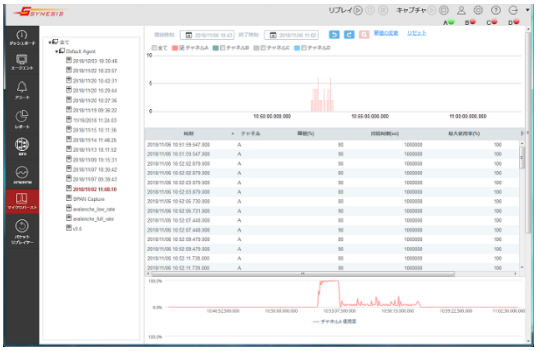
キャプチャしたパケットの解析結果から、レポートを作成することができます。レポートに記載する項目やグラフは、用意されたオブジェクトの中から選択できます。

詳細は、**レポート**の章を参照してください。

- アラート機能

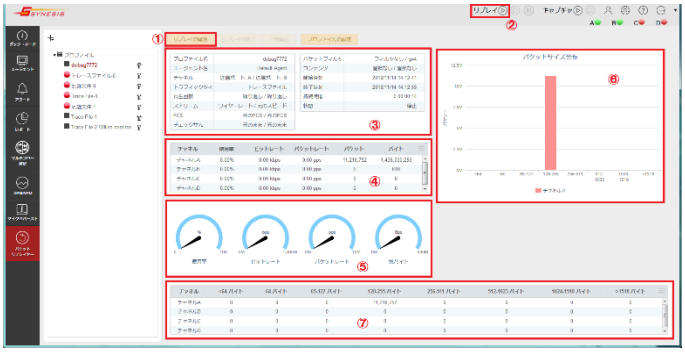
応答遅延やマイクロバーストの発生など、異常が疑われるトラフィックを検知することが可能です。アラートから関連するパケットのみの抽出ができます。アラートは、外部へ通知することが可能です。

詳細は、**アラート機能と通知**の章を参照してください。



- パケットのリプレイ機能

キャプチャしたトラフィックをリプレイすることが可能です。
本機能は、「パケットリプレイヤーオプション」が必要です。
詳細は、パケットリプレイヤーのマニュアルを参照ください。



- リモート操作機能

リモートから SYNESIS へ操作する場合は、ローカル同様 Web ブラウザを使用します。リモートデスクトップでの接続も可能です。一部設定は、SSH 接続で行います。リモートでもローカルと同様の操作が行えます。
詳細は、**3.4. 接続方法** を参照してください。

2.SYNESIS の構造

SYNESIS の構造について説明します。

2.1.　SYNESIS について

構成メニュー>「SYNESIS について」では、SYNESIS の情報が表示されます。

図 1：「構成」メニュー>「SYNESIS について」

以下の情報が確認可能です。

- 製品名
- 製品構成（コントロールユニット、ストレージユニット、キャプチャモジュール）
- シリアルナンバー
- バージョン
- バージョントレース
- チャネル位置
- 外観

2.2.　エージェントのプロセス管理

[エージェント]メニュー>「全て」をクリックすると、右側のワークスペースに利用可能なエージェントの情報が表示されます。

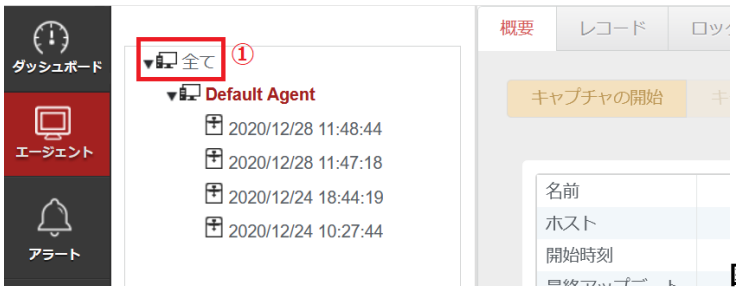


図 2：エージェント・ペイン

図 3：全てのエージェント画面

プロセスのリスタートを行う場合は、対象の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(図 3②)をクリックします。 全てのエージェントをする対象とする場合は、先頭行のチェックボックス(図 3③)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。

画面左上の検索テキストボックスにするエージェントの名前を入力すると部分一致するエージェントのみが表示されます。

確認できるエージェントの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。変更できません。
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	現在のキャプチャのステータスです。 キャプチャ中は「キャプチャ」、停止中は「停止」と表示されます。キャプチャを開始・停止する手順はキャプチャの開始・停止 を参照してください。
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	

2.3. SYNESIS のディスク領域

SYNESIS 内部のディスク領域は 3 つに分かれています。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。

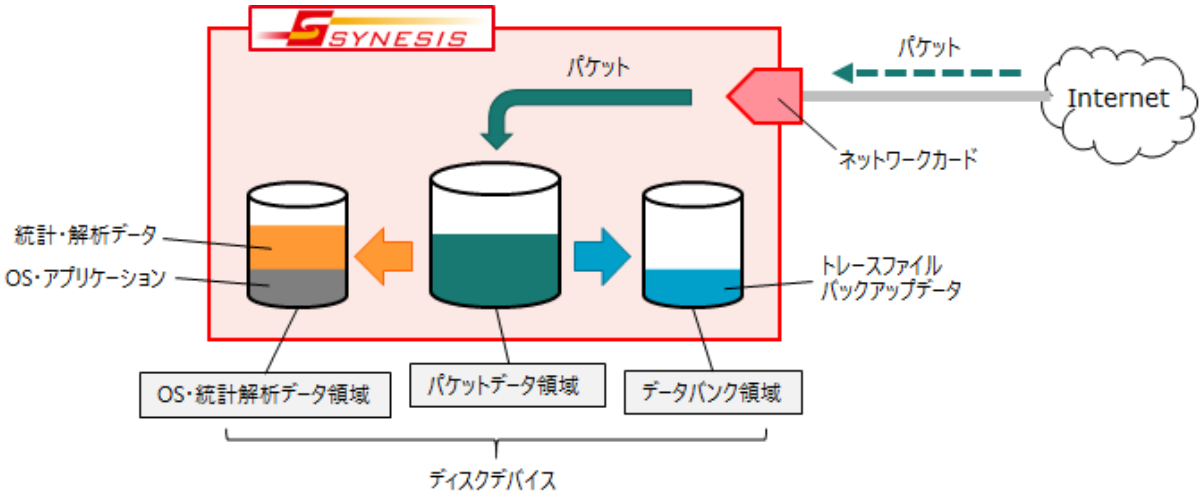


図 4:SYNESIS のディスク領域

2.3.1. 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。

- 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、[エージェント]メニュー>[レコード]タブ>[ストレージ情報]ボタンをクリックすることで確認できます。

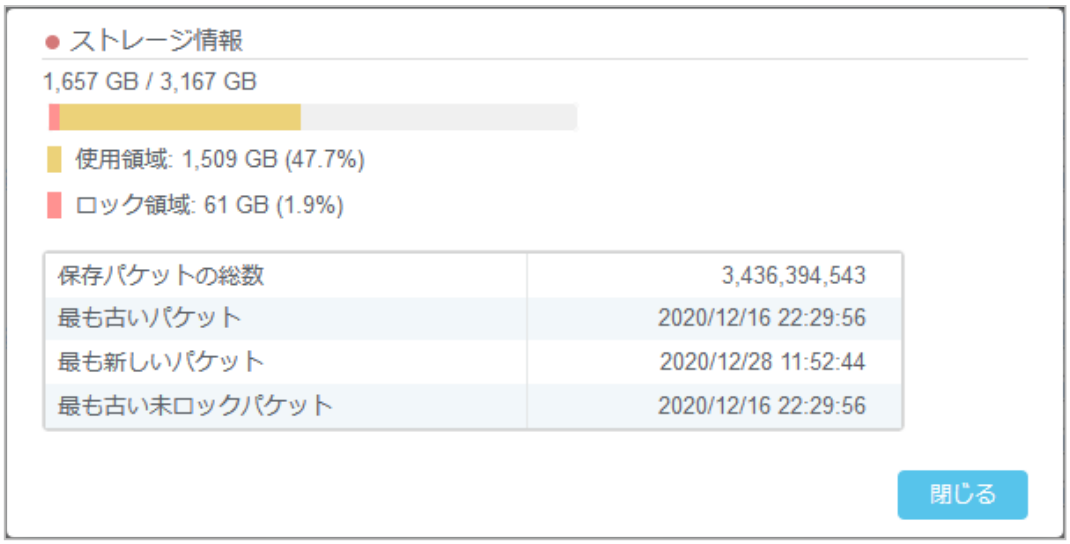


図 5：ストレージ情報

ストレージ情報画面で確認できる情報は、以下の通りです。

項目	説明
全体に占める空き容量	「空き容量(GB) / パケットデータ領域の全容量(GB)」で表示されます。
使用領域	使用境域のサイズが GB 単位で表示されます。 また、その使用領域がパケットデータ領域の全容量に対して占める割合がパーセンテージで表示されます。
ロック領域	ロック境域のサイズが GB 単位で表示されます。 また、そのロック領域がパケットデータ領域の全容量に対して占める割合がパーセンテージで表示されます。
保存パケットの総数	パケットデータ領域に保存されているパケットの総数です。
最も古いパケット	パケットデータ領域に保存されている中で、最も古いパケットの保存日時です。
最も新しいパケット	パケットデータ領域に保存されている中で、最も新しいパケットの保存日時です。
最も古い未ロックパケット	パケットデータ領域に保存されている中の、ロックされていない最も古いパケットの保存日時です。

ロックされているデータがある場合、最も古いパケットの保存時刻が実際にロックを開始した時刻と異なる場合があります。ただし、ユーザの指定した時刻は含まれていますので、ロックしたデータのパケットが上書きされることはありません。

2.3.2. 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 MFA 解析・APM/NPM 解析・マイクロバースト解析データ

キャプチャを継続すると統計・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、**10.5.1. 解析共通**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。

2.3.3. データバンク領域

この領域には、下記の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**ビルドインファイル**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(デフォルト設定)で作成されたトレースファイル
- 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**・メニュー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、トレースファイル・タブの **ビルドインファイル**・タブに表示されている「ディスク容量情報」で確認できます。

図 6：トレースファイル・タブ

「ディスク容量情報」の帯グラフが「データバンク領域」の使用状況です。

「使用領域(GB) / データバンク領域の全容量(GB)」で表示されています。

2.4. 使用するポートの一覧

SYNESIS で使用しているポートは、以下の通りです。

2.4.1. 外部との通信で使用するポート

外部との通信は、管理ポート(eno1～eno4)を介して以下のポートを使用します。

記載のないポートは、初期設定では SYNESIS 上の Firewall にて遮断されています。

ポートの開閉は管理ポート(eno1～eno4)に対してのみ可能です。

ポート番号	ポート開閉※	説明
22	**不可**	リモートから SSH で接続する際に使用します。
80	**可能**	SYNESIS の Web アプリケーションで使用します。 ただし、"https://～"(ポート番号 443)へ強制的にリダイレクトされます。
443	**不可**	SYNESIS の Web アプリケーションで使用します。
1311	**可能**	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。
3389	**可能**	リモートデスクトップで使用します。

2.4.2. ループバック通信で使用するポート

ループバック (内部) 通信として、以下のポートを使用します。

ポート番号	説明
3000	SYNESIS Management Console で使用します。
5432	PostgreSQL データベースへのアクセスに使用します。
5433 ～ 5435	バックアップを作成する際に、PostgreSQL データベースへのアクセスに使用します。
8080	SYNESIS の Web アプリケーションで使用します
8443	AA 解析のサービスで使用します。AA 解析対応モデルでのみ使用します。
9010	SYNESIS のプロセス間通信(thrift)で使用します。
9012	SYNESIS のエージェントプロセスの監視 (VPEyes)で使用します。
9013 ～ 9014	バックアップを作成する際に、エージェントプロセスの監視 (VPEyes)で使用します。
9050 ～ 9059	Decode サービスの通信で使用します。
9090	SYNESIS のプロセス間通信(mvp)で使用します。
9999	Remote monitoring JVM で使用します。

2.4.3. Distributed モデルの iDRAC との通信に使用するポート

iDRAC との通信として、以下のポートを使用します。(Distoributed モデルのみ)

ポート番号	説明
22	リモートから SSH で iDRAC に接続する際に使用します。
80	iDRAC の Web アプリケーションで使用します。 ただし、"https://～"(ポート番号 443)へ強制的にリダイレクトされます。
443	iDRAC の Web アプリケーションで使用します。
5900	iDRAC の仮想コンソールで使用します。

2.5. Web アプリケーションのセッション管理

SYNESIS GUI の Web アプリケーションのアクセスは、下記の通り管理しています。

項目	説明	初期値
セッション継続時間	無操作の状態でセッションを継続できる時間です。 無操作のままこの時間が経過すると、自動的にセッションが切断されます。 設定変更により本機能を無効化することもできます。	30 分

ユーザ数上限	同時にサインインできるユーザ数です。	3 ユーザ
セッション数上限	同時に接続可能なセッション数です。 この値は SYNESIS のサインイン画面に表示されます。	3 セッション

サインイン後、無操作のまま 30 分を経過すると自動的にサインアウトし、以下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" の部分をクリックすると、再度ログインが可能です。

図 7：サインアウト画面

セッション継続時間、ユーザ数上限、セッション数上限は、設定ファイルで変更が可能です。以下に手順を示します。

1) TeraTerm またはコンソールから Terminal を起動します。以下は TeraTerm から操作する場合の例になります。

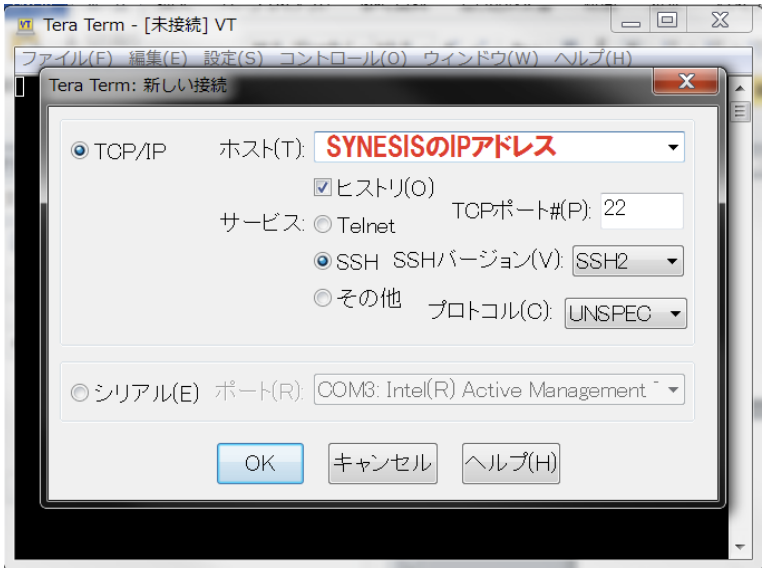


図 8：TeraTerm 起動画面

2) 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ます。

3) OS のユーザ名とパスワードの入力を求められますので、OS のユーザ名とパスワードを入力します。SYNESIS に SSH で接続されます。

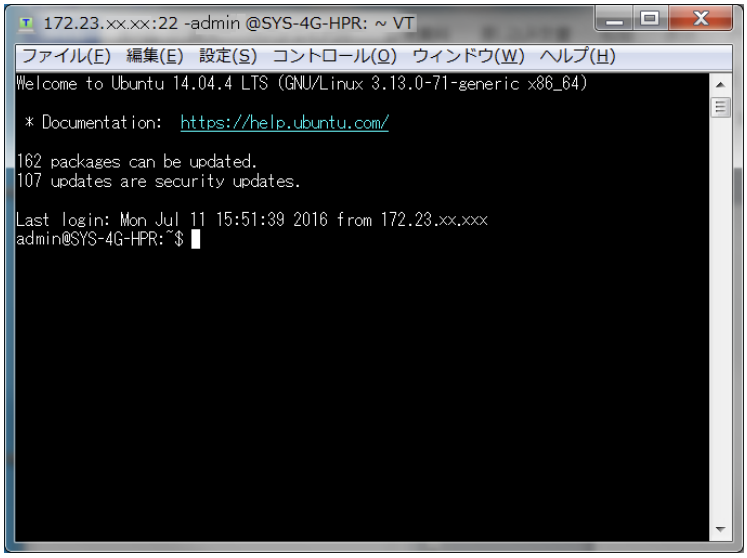


図 9：SSH 通信画面

4) 設定ファイルを開きます。

```
$ sudo vi /var/lib/tomcat/webapps/ROOT/WEB-INF/classes/common.properties
```

5) 必要に応じて下記のパラメータを変更します。

セッションの切断を無効化する場合は autologout.time を 0 にしてください。

```
autologout.time = 30 ：セッション継続時間 （分）
usercount.limitation = 3 ：ユーザ数上限
sessioncount.limitation = 3 ：セッション数上限
```

6) 設定ファイルを上書き保存します。

7) ブラウザを起動し、"https://[SYNESIS IP]/mgmt/" から SYNESIS 管理画面にアクセスします。管理画面のユーザ名とパスワードの入力を求められますので、 ユーザ名とパスワードを入力します。

8) Web アプリケーションを再起動して設定を有効化します。

Tomcat サービスの[Restart]ボタンをクリックします。

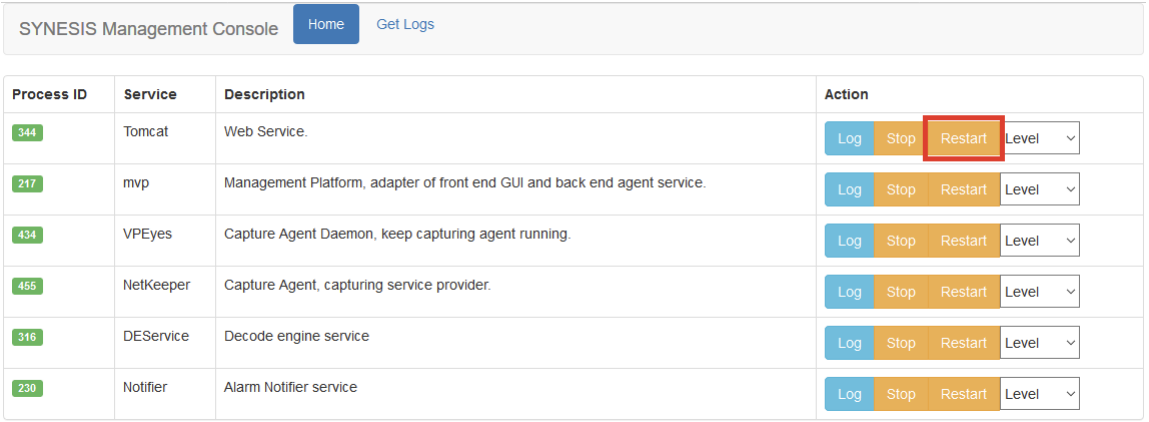


図 10：SYNESIS 管理画面

以上の手順で設定が反映されます。

2.6. 画面構成

SYNESIS の画面構成は、以下の通りです。

図 11：SYNESIS の画面構成

画面の左側には、**メインメニュー**(上図①)が配置されています。各機能の画面の切り替えの際に使用します。

画面の上部には、**ツールバーメニュー** (上図②)が配置されています。使用頻度の高いアイコンと現在のチャネルのステータスが表示されています。

画面の中央は、各メニューのワークスペースとなり、実際に操作や解析が行える部分です。

2.6.1. メインメニュー

画面左端に表示されるメインメニューのアイコンから、各種操作、解析メニューにアクセスできます。 メインメニューの種類と機能は以下の通りです。

メインメニューの種類と機能

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 **11. ダッシュボード**を確認してください。
	エージェント	キャプチャの開始・停止、トレースファイルの保存が行えます。 詳細は **4. キャプチャの開始・停止**を確確認してください。
	アラート	キャプチャ時に検知された、異常が起きたと疑われる時刻を検索・閲覧できます。 アラート機能を利用するためには、キャプチャを開始する前に検知基準となる閾値を設定する必要があります。 詳細は、**14. アラート機能と通知**を確認してください。
	レポート	統計情報や解析結果から、定型のレポートを作成することができます。 詳細は **12. レポート**を確認してください。
	MFA	キャプチャデータごとにキャプチャポイントを定義し、フローを抽出してラダー表示をすることができます。 詳細は **13. MFA(マルチフロー解析)**を参照してください。
	APM/NPM	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 **10.2. APM/NPM 解析**を確認してください。
	マイクロバースト	瞬間的にトラフィックが集中するマイクロバーストの発生状況を確認できます。 詳細は **10.4. マイクロバースト解析**を確認してください。
	パケットリプレイヤー	本機能は、「パケットリプレイヤーオプション」が必要です。 詳細は、パケットリプレイヤーのマニュアルを参照してください。
	AA 解析	プレビュー版での提供です。 詳細は、AA 機能のマニュアルを参照してください。

2.6.2. ツールバーメニュー

SYNESIS 画面上部のツールバーには使用頻度の高い操作用のアイコンが表示されています。

ツールバーの下にはチャンネルごとのリンク状態が表示されています。

ツールバーメニューの種類と機能

表示		メニュー名	動作
リプレイ		リプレイの開始	パケットの再生を開始します。 前回再生したプロファイルの条件で再生が実行されます。
		リプレイの停止	実行中のパケットの再生を停止します。
		パケット再生の一時停止	実行中のパケットの再生を一時停止します。 再度、再生ボタンをクリックすると、一時停止していたところから再生が再開されます。
キャプチャ		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。
		キャプチャの停止	パケットキャプチャを停止します。
		アクティブユーザプロファイル	サインイン中のユーザの登録情報が変更できます。 表示名やパスワードの変更がこちらから行えます。
		構成	「構成」メニュー画面にアクセスします。 詳細は **18. 構成**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、サイン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します。 ボタンをクリックすると、この表で説明されているアイコンがリストで表示されます。 表示するするアイコンの左端のチェックボックスにチェックすると、チェックされたアイコンがツールバー上に表示されます。 非表示する場合は、チェックボックスからチェックを外し、ます。
チャネル	●	リンクアップ	Rx 信号がリンクアップしています。
	●	リンクダウン	Rx 信号がリンクダウンしています。
	●	unknown	未対応のモデルです。

リプレイ機能については、パケットリプレイヤーマニュアルを参照してください。

2.6.3. エージェント・ペインとワークスペース

画面の中央は、各メニューのワークスペースとなり、実際に操作や解析が行える部分です。

ワークスペースはメインメニューやツールバーメニューの選択によって表示が変わります。

メニューにより、ワークスペース画面の左側に別枠のウィンドウ(下図赤枠)が表示されます。このウィンドウはペインと呼ばれ、ワークスペースで操作するデータやファイルを選択するための画面です。

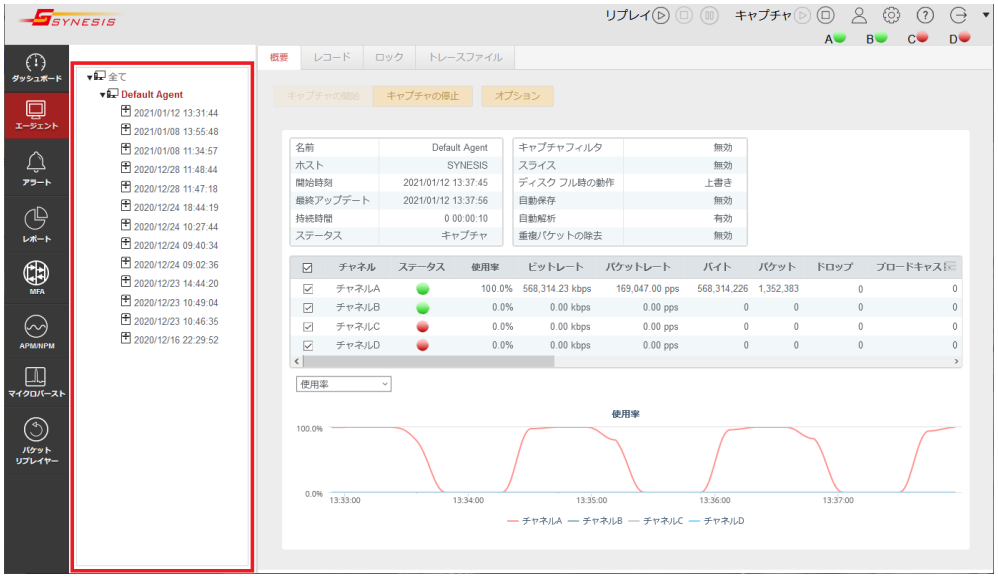


図 12：エージェント・ペインとワークスペース

一部のメニューでは、画面左側に表示されるエージェント・ペインを非表示にし、ワークスペースを拡大表示させることが可能です。

表示・非表示の切り替えは、hide ボタン⊖(左下図①)と、 show ボタン⊕(右下図②)で行います。

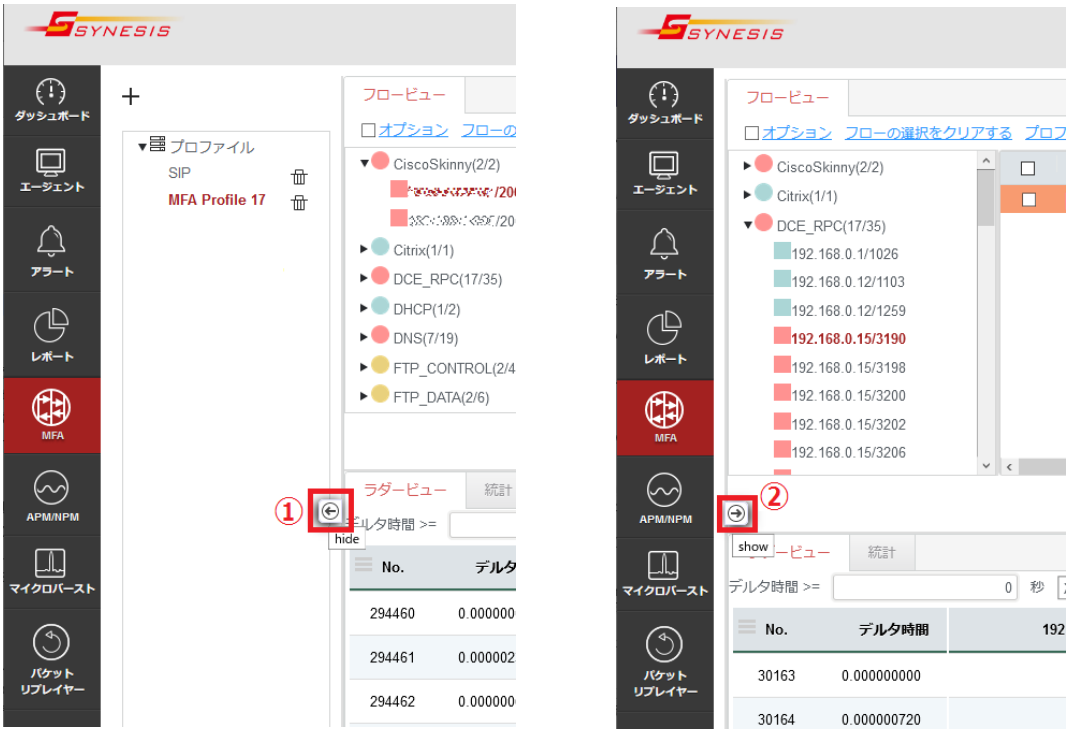


図 13：hide ボタン・show ボタン

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。

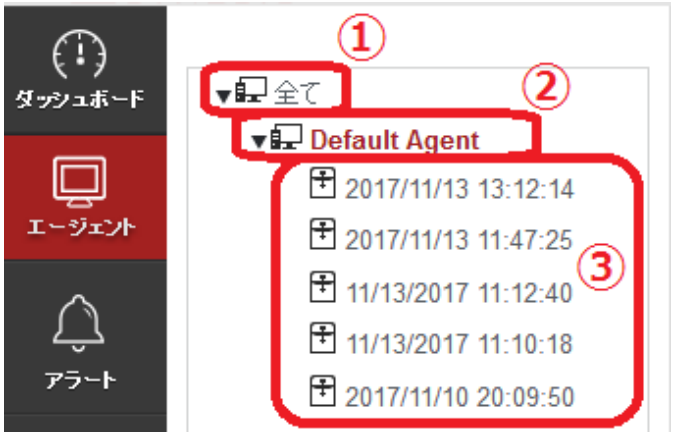


図 14：エージェント・ペイン

「全て」ノード(上図①)をクリックすると、右側に「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②)をクリックすると、「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③)をクリックすると、「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、トレースの保存の操作などが行えます。

2.6.4. 一覧表示の項目の表示設定

一覧表示の項目名欄の右端に表示されている表示項目 アイコンで項目の表示/非表示を切り替えることができます。

表示項目 アイコンをクリックすると、現在表示されている項目がチェックされています。項目を選択し、クリックすると非表示/非表示が切り替わります。

図 15：一覧表示の項目の表示設定

2.6.5.　グラフ画面での期間指定

エージェント、アラート、APM/NPM、マイクロバースト機能のワークスペースの画面の上部には、グラフ画面と時刻を指定する操作用のアイコンやリンクメニューが配置されています。

グラフ画面と下部にあるテーブルは、連動しており、グラフ画面上の期間を指定すると、テーブルの表示もその期間で表示されます。

時間範囲を指定する場合は、トレンドグラフ上をドラッグもしくはカレンダー表示で指定します。

- トレンドグラフ上で指定する場合

画面中央上部の拡大アイコンをクリックすると、指定した時刻範囲でグラフが拡大表示されます。

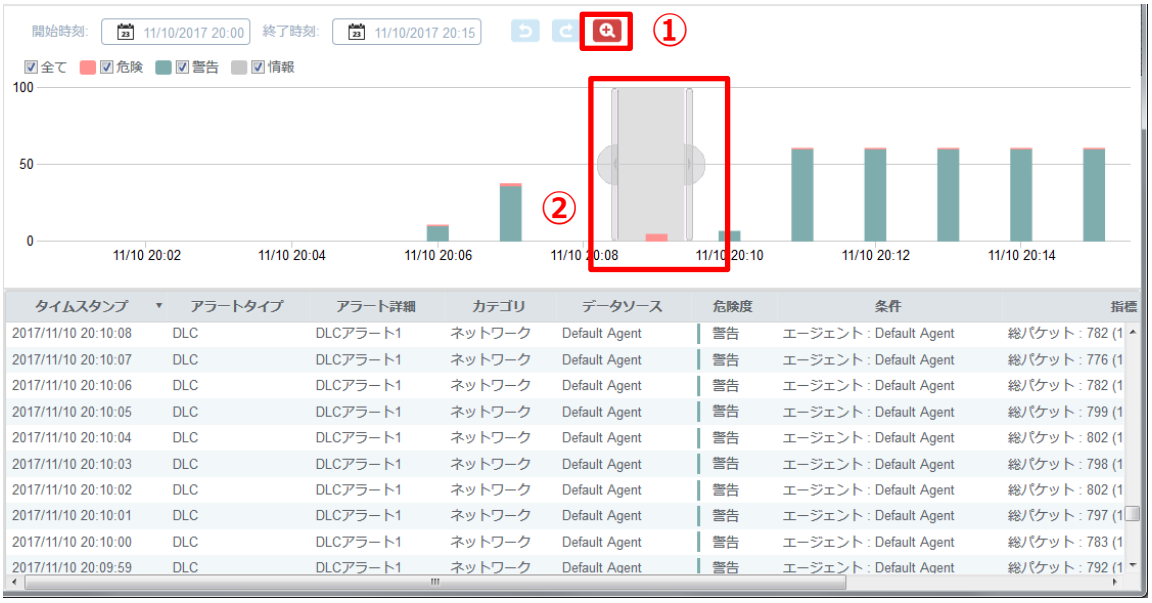


図 16：拡大表示範囲指定

拡大する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)をクリックすると、グラフが選択した時間範囲で拡大表示されます(下図 17)。

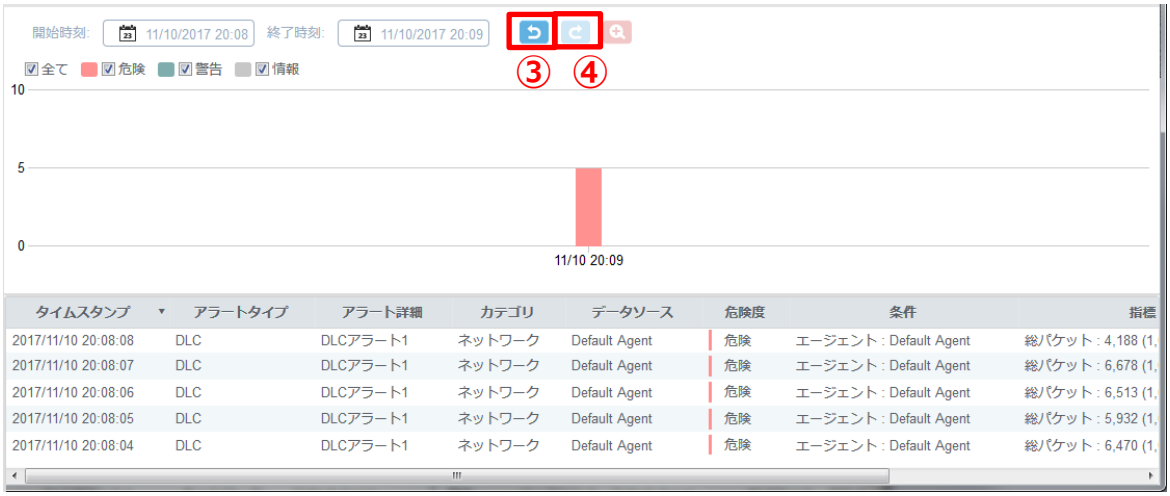


図 17：指定範囲拡大表示

このとき、テーブルの情報は、指定した時間範囲のデータに更新されます。

元に戻す アイコン(上図③)をクリックすると、直前に行った操作が取り消されます。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」操作がキャンセルされます。

● カレンダー表示で指定する場合

開始時刻と終了時刻で任意に期間を設定することが可能です、

カレンダーアイコンをクリックすると、下図の期間指定画面が表示されます。

図 18:期間指定画面

時間範囲を指定し、[適用]ボタンをクリックします。

カレンダー表示は、画面により仕様が異なりますので、各機能の章で制限を確認ください。

2.6.6. ダイアログの必須項目

操作中に入力や確認を求めるダイアログが表示されることがあります。

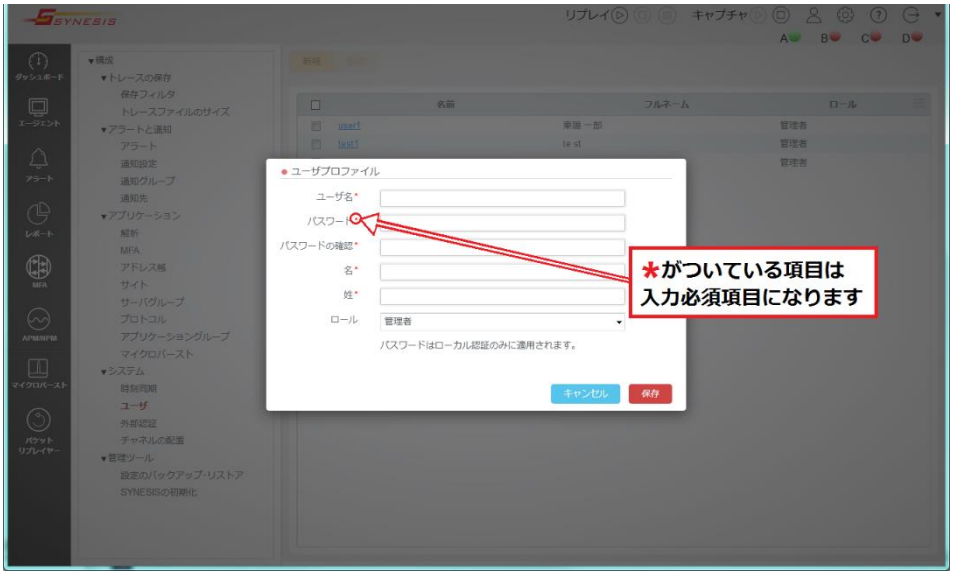


図 19：ダイアログ表示

*がついている項目は、入力必須項目です。

ダイアログが表示されたら各項目に値を入力し、[保存]ボタンや[適用]ボタンをクリックします。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、内容は保存されずにダイアログが閉じられます。

2.6.7. 構成の項目編集

編集ボタンが配置されている画面の編集を行う場合は、左上の[編集]ボタンをクリックします。

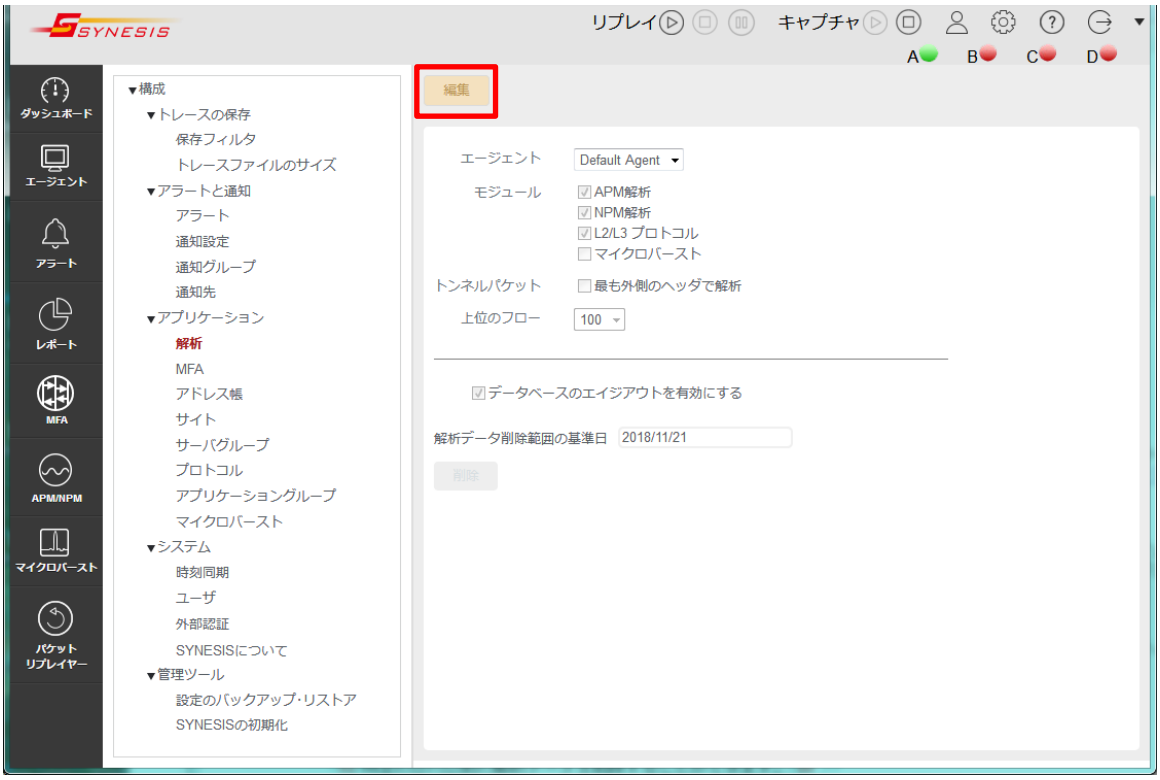


図 20：「構成」メニューの編集ボタン

以下のように各項目が編集可能になります。

図 21：設定編集画面

各項目の設定が完了したら[保存]ボタンをクリックします。

2.7. アドレス帳の設定

構成メニュー>「アドレス帳」では、IP アドレスを名前で登録できます。

アドレス帳で登録した名前は、以下の画面で適用されます。

適用する画面	機能
ダッシュボード	解析を実行する前の設定で適用
レポート	
APM/NPM	
MFA	マージ前の設定で適用
デコード	デコード前の設定で適用
AA 解析	AA 解析前の設定で適用

なお、アラート画面では、アドレス帳の設定は適用されません。

新規に IP アドレスを登録する場合は、「構成」メニュー>「アドレス帳」の上部にある[新規] ボタンをクリックします。

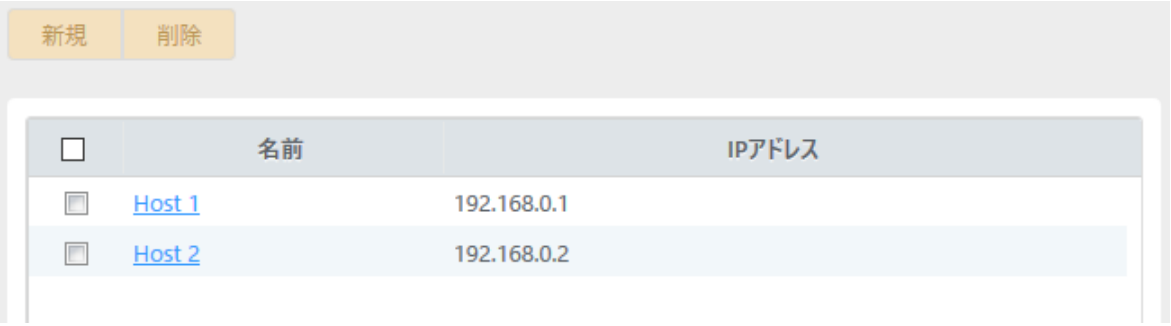


図 22 :「構成」メニュー>「アドレス帳」

以下の「アドレス帳」ダイアログが表示されます。

図 23 :「アドレス帳」ダイアログ

「名前」欄に変換する名前を、「IPv4 もしくは IPv6 アドレス」欄に IP アドレスを入力します。<保存>ボタンをクリックすると、入力した情報が一覧に追加されます。

登録されているアドレスを変更する場合は、名前の部分をクリックします。「アドレス帳」ダイアログが表示され、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する場合は、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ます。該当するアドレスが削除されます。

3.起動・終了・接続方法

SYNESIS の起動・終了・接続方法について説明します。

SYNESIS の操作および閲覧は、Web ブラウザから行います。

SYNESIS の電源を投入して OS にログイン後、Web ブラウザを起動します。リモート PC から Web ブラウザを用いる場合は、OS のログインは必要ありません。

なお、SYNESIS はソフトウェアおよびライセンスがすべてインストールされた状態で出荷されていますので、 設置後、SYNESIS の電源を投入するだけで利用できます。

3.1. SYNESIS の初期設定

OS と SYNESIS GUI の初期設定でのユーザ名とパスワードは、以下の通りです。

ソフトウェア	初期設定	
	ユーザ名	パスワード
OS (Ubuntu)	synesis	admin
SYNESIS GUI (Web ブラウザ)	admin	synesis1

SYNESIS のユーザ名パスワードの変更方法は **15.1.ユーザの登録・管理**を参照してください。

OS のユーザ名とパスワードの変更方法は、管理マニュアルの “4. 初期設定の変更”を参照してください。

3.2. SYNESIS の起動

SYNESIS の起動手順は、以下の通りです。

1) SYNESIS 本体の電源ボタンを押し、電源を ON にします。

拡張ストレージユニットが付属しているモデルは、コントロールユニットより先に拡張ストレージユニットの電源を ON にします。拡張ストレージユニットの電源を ON にすると、ディスクドライブのフロントパネル上にある緑色 LED の点滅が始まります。 点滅が終わり、点灯状態になるまで待ち、その後、コントロールユニットの電源を ON にします。

2) 以下のログイン画面が表示されますので、OS のユーザ名とパスワードを入力し、<Enter>キーを押下します。

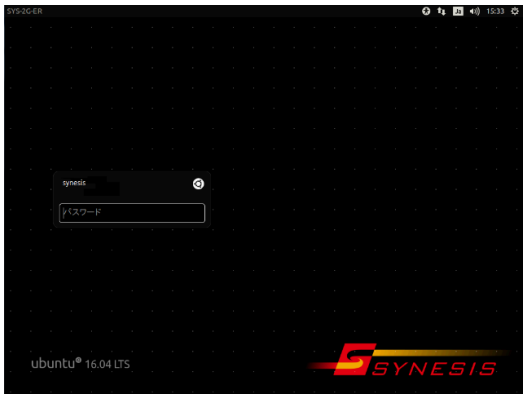


図 24 : OS サインイン画面

3) 以下のデスクトップ画面が表示されます。画面左上の アイコンをクリックし、 Web ブラウザ(Firefox)を起動します。

図 25：デスクトップ画面

4) 以下のサインイン画面が表示されます。ユーザ名とパスワードを入力し、[サインイン]ボタンをクリックします。

図 26：SYNESIS サインイン画面

サインイン後、無操作のまま 30 分を経過すると自動的にサインアウトし、以下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、再度ログインを実施します。

図 27：自動サインアウト画面

3.3. SYNESIS の終了

SYNESIS を終了するには、本体のデスクトップ画面から直接停止させる方法とリモート操作によって停止させる方法があります。それぞれの場合の停止手順は以下の通りです。

- デスクトップ画面から行う場合

1) デスクトップ画面右上の ボタンをクリックします。

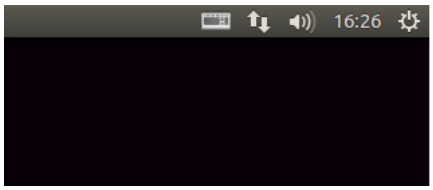


図 28：ツールバー・メニュー

2) 画面右上に以下のメニューが表示されますので、 **[シャットダウン...]**をクリックします。

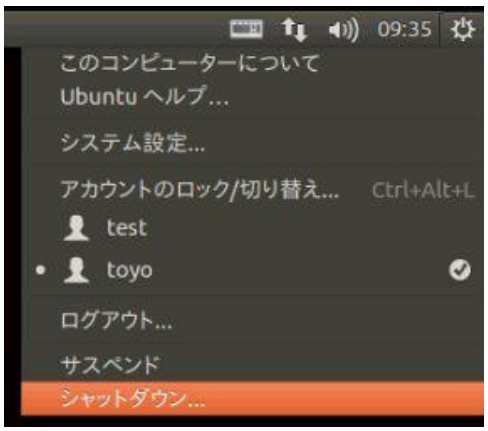


図 29：メニュー

3) 以下のダイアログが表示されますので、**[シャットダウン]**をクリックします。

図 30：シャットダウン選択

- SSH または Terminal から終了する場合

1) SSH で接続し、以下のコマンドを入力します。

```
$sudo shutdown -h now
```

拡張ストレージユニットが付属しているモデルは、コントロールユニットの電源ボタンが消えたことを確認してから、拡張ストレージユニット正面の電源ボタンを押して拡張ストレージユニットの電源を落とします。

3.4. 接続方法

リモートからの接続方法は、以下 3 つの方法があります。

- Web ブラウザ接続
- リモートデスクトップ接続
- SSH 接続

3.4.1. SYNESIS の IP アドレスの確認方法

リモートからの操作は、IP アドレスの入力が必要です。SYNESIS の IP アドレスは、以下の手順で確認できます。

1) SYNESIS のデスクトップの左上に位置する検索 アイコンをクリックします。

2) 検索ウィンドウに「Terminal」と入力し、検索結果で表示されるターミナルアイコンをクリックして、ターミナル・ウィンドウを開きます。

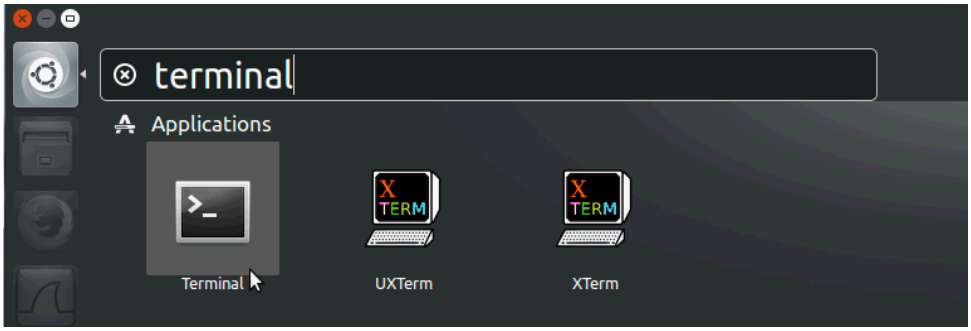


図 31：OS 検索画面

3) 下記コマンドを実行し、接続されている管理ポートの IP アドレスを確認してください。

```
$ ifconfig
```

3.4.2. Web ブラウザ接続

リモート PC から Web ブラウザを用いて SYNESIS をリモート操作することが可能です。

リモート PC の推奨環境は下記の通りです。

推奨 OS　　：Windows10

推奨ブラウザ　：Firefox

Web ブラウザを起動し、アドレスバーに以下のアドレスを入力します。

https://<SYNESIS の IP アドレス>

接続が成功した場合、ローカルでの接続同様に SYNESIS のサインイン画面が表示されます。ユーザ名とパスワードを入力し、[サインイン]ボタンをクリックします。

3.4.3. リモートデスクトップ接続

Windows のリモートデスクトップ機能で接続する手順は、以下の通りです。

1) [Windows のスタートボタン]>[リモートデスクトップ接続]を開きます。

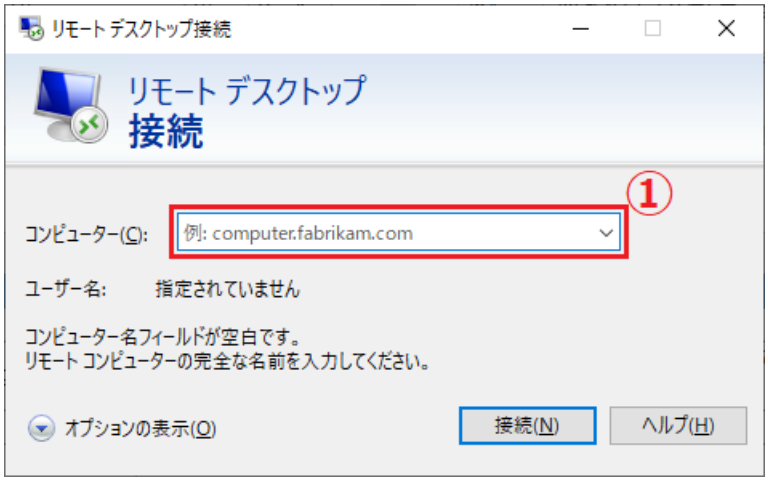


図 32：リモートデスクトップ起動画面

2) 「コンピュータ(C)」 の欄(上図①)に SYNESIS の IP アドレスを入力します。

3) [オプションの表示]をクリックし、エクスペリエンスタブ(下図②)を選択します。[接続品質の自動検出]より、「LAN (10 Mbps 以上)」以外 (下図③)を選択します。

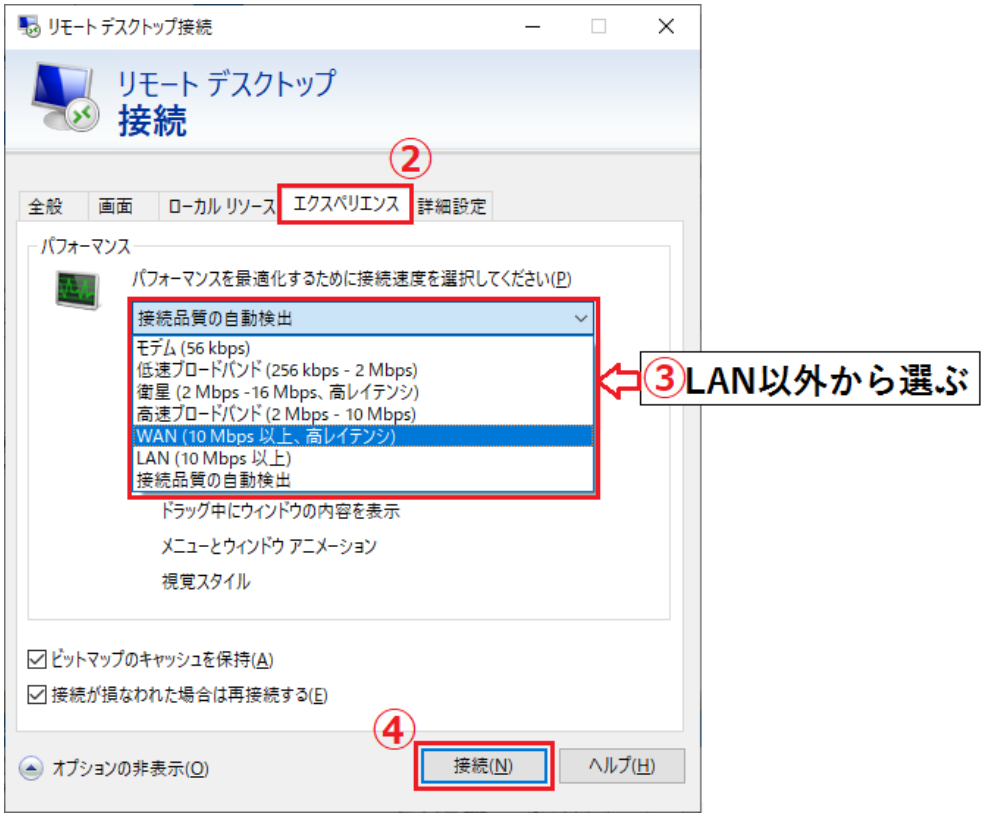


図 33：リモートデスクトップ設定画面

4) [接続]ボタン(上図④)をクリックします。接続に成功すると、次ページのログイン画面(図 34)が表示されます。

5) SYNESIS の 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ます。

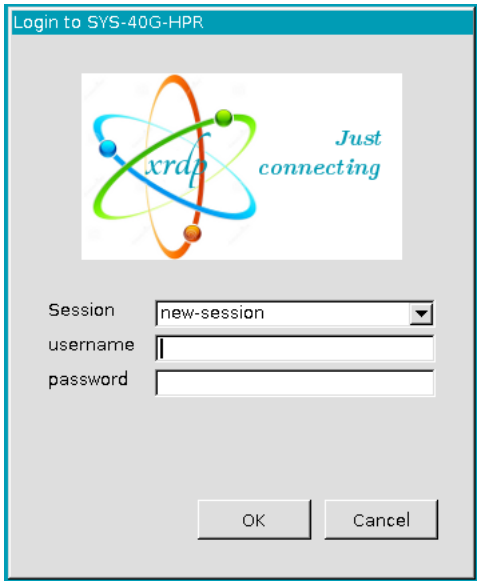


図 34:リモートログイン画面

6) 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。

図 35：OS デスクトップ画面

7) ログアウトする場合は、メニューバー>[システム]>—[<ユーザ名>のログアウト･･･]を選択します。

図 36：リモートデスクトップ接続のログアウト

リモートデスクトップからシャットダウンや再起動は行わないでください。

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。

3.4.4. SSH 接続

一部の設定は SSH で接続を行います。SSH で接続する場合の手順は、以下の通りです。

1) ターミナルソフトまたはコンソールから Terminal を起動します。以下は、TeraTerm から操作する場合の例です。

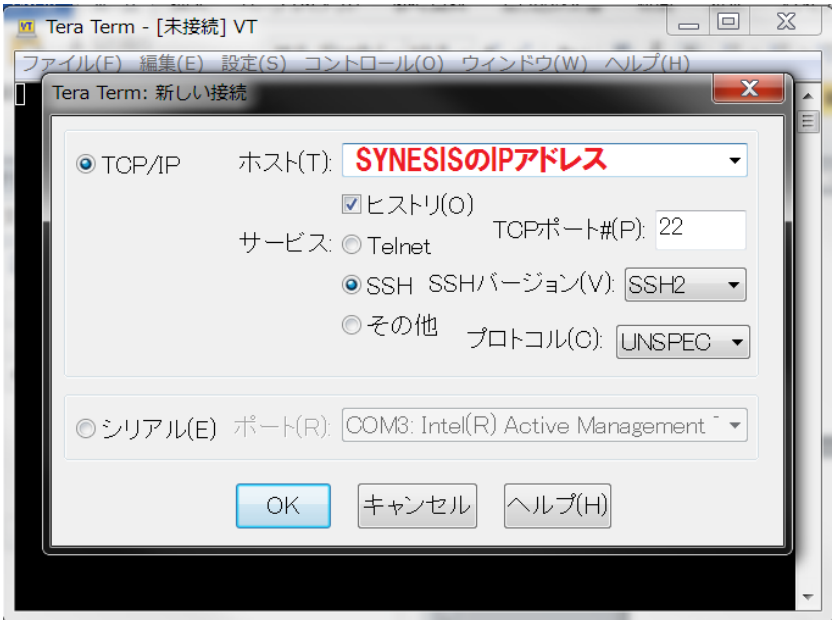


図 37 : TeraTerm 起動画面

2) 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ます。

3) OS のユーザ名とパスワードの入力を求められますので入力します。SYNESIS に SSH で接続されます。

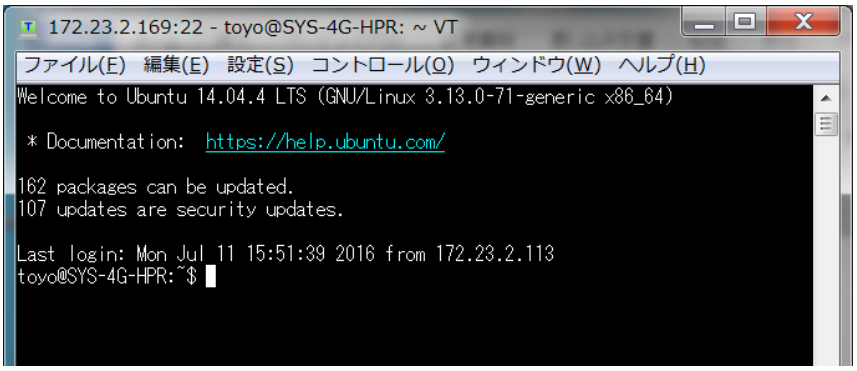


図 38 : SSH 接続画面

4.キャプチャの開始・停止

キャプチャの開始・停止の操作について説明します。

キャプチャの開始・停止の操作、その時点でのキャプチャ状況の確認は、[エージェント]メニューから行います。

図 39：エージェント・メニュー画面

4.1. キャプチャの開始・停止手順

キャプチャの開始・停止は、以下の手順で行います。

- キャプチャの開始

1) キャプチャの開始ボタン(下図①)をクリックします。

図 40：[キャプチャの開始]ボタン

2) 以下の「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(下図③)をクリックします。

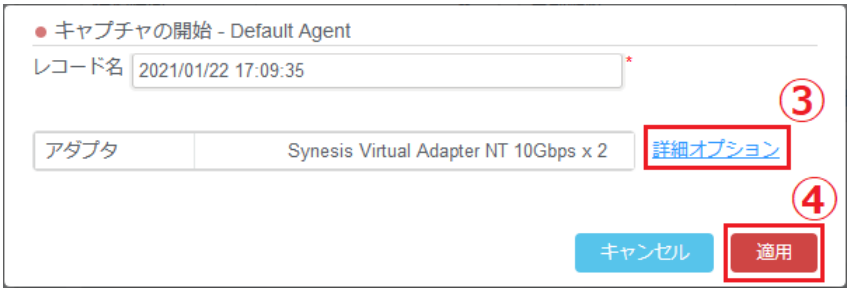


図 41：キャプチャの開始ダイアログ

3) キャプチャの設定は、キャプチャオプションで設定します。この設定は、キャプチャを停止するまで変更できません。設定後、[適用]ボタンをクリックして、「キャプチャの開始」ダイアログに戻ります。

4) レコード名を変更する必要があれば、書き換えます。[適用]ボタン(上図④)をクリックし、キャプチャを開始します。

ツールバーのキャプチャ ボタン(前頁図 40②)でもキャプチャの開始が可能です。 ボタンをクリックすると同様に「キャプチャの開始」ダイアログが表示され、[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。

- キャプチャの停止

[キャプチャの停止]ボタン(下図⑤)、またはツールバーのキャプチャ停止 ボタン(下図⑥)をクリックします。

図 42：[キャプチャの停止]ボタン

指定したキャプチャオプションの設定は保存され、次回以降のキャプチャに自動的に適用されます。

4.2. キャプチャを開始する前に設定する項目

いくつかの設定項目は、キャプチャ中の設定変更、およびキャプチャ後の設定反映に制限があります。キャプチャを開始する前に必要な設定を行ってください。

設定箇所	項目	説明
キャプチャオプション	すべての設定項目	キャプチャ前に設定が必要です。 キャプチャ中に設定の編集はできません。 また終了したレコードに対して設定の反映はできません。
構成	アラートの有効・無効 アラートの条件	キャプチャ前に設定が必要です。 キャプチャ中に設定を編集できますが、実行中のキャプチャに対しては反映されません。 次回のキャプチャから反映されます。
	アラートの通知先グループ 通知グループの定義 通知先の定義	変更した設定はキャプチャ中でもただちに反映されます。
	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	自動解析が有効になっている場合は、キャプチャ前に設定が必要です。手動で解析を行う場合は、解析前に設定が必要です。 解析の実施後に新しい設定の反映はできません。

4.3. キャプチャ全般に関する制限

- SYNESIS のキャプチャ性能は、キャプチャ以外の機能および操作を一切実施しない状態でのみ保証されます。
- キャプチャ中のレコードの名称を変更しても、キャプチャ終了時に変更前の名称に戻ります。
- キャプチャ開始後 2 秒間はパケット数などの統計情報がカウントされません。

4.4. キャプチャオプション

キャプチャオプションタブは、キャプチャに関する設定です。

概要タブの[オプション]ボタン、または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」リンクをクリックすると、以下の[キャプチャオプション]ダイアログが表示されます。

図 43：キャプチャオプション画面

各項目を設定した上で[適用]ボタンをクリックします。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]は、以下の６画面で構成されています。

- 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

4.4.1. 共通 オプション

適用するアダプタ選択などの基本的なキャプチャ設定を行います。

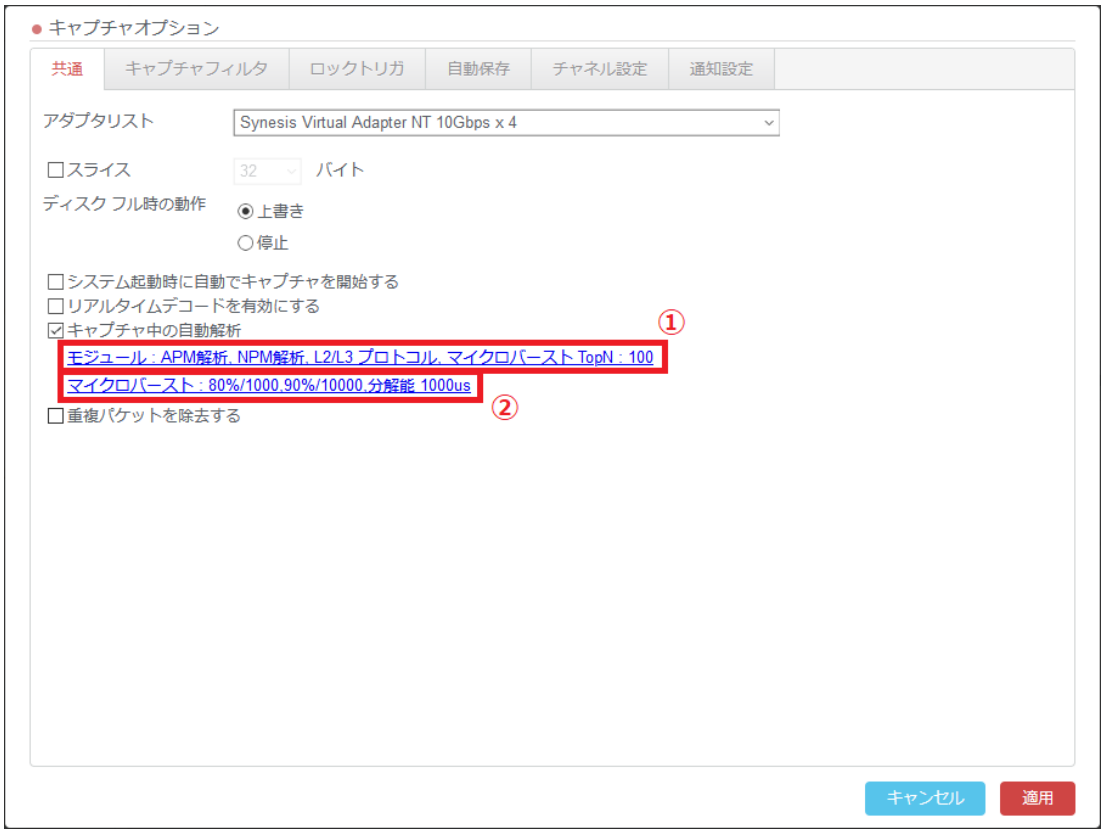


図 44：共通オプション画面

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	適用するアダプタ(キャプチャカード)を選択します。アダプタが複数搭載されている場合は、選択可能なアダプタがすべて表示されます。
スライス	スライスの設定を行います。 チェックボックスにチェックをした場合、スライスが有効になり、各フレームの先頭から選択したバイト数までが保存されます。 無効の場合は、フレーム全体が保存されます。 設定可能なバイト数やキャプチャ可能な最大バイト数はモデルにより異なります。詳細は、SYNESISの諸元一覧を参照ください。
ディスクフル時の動作	パケットデータ領域に空き容量がなくなった場合の動作を指定します。 ● 上書き：最も古いデータから上書きし、キャプチャを停止しません。 ● 停止：ディスクが満杯になった時点でキャプチャを停止します。既にディスクフルの状態でキャプチャを開始した場合は、パケットストアが新しく開始したキャプチャのパケットで一杯になった時点でキャプチャが停止します。この時、パケットストアに残っていた、それ以前のキャプチャのパケットはディスクに書き込まれます。 SYNESIS のディスク構成の詳細は、**2.3. SYNESIS のディスク領域**を確認してください。

システム起動時に自動でキャプチャを開始する	チェックした場合、次回以降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	チェックを入れた場合、キャプチャ中にリアルタイムデコードを行います。リアルタイムデコードのサンプリング周期は 1 秒に 1 パケットです。詳細は、**7.1. リアルタイムデコード** を参照してください。
キャプチャ中の自動解析	チェックを入れた場合、キャプチャ中の自動解析が有効になります。 詳細は、**10. 解析機能** を参照してください。
解析モジュールと上位のフロー数の指定 **(リンク/図 43①)**	適用されている解析の設定項目が表示されます。 キャプチャ中の自動解析を有効にすると、解析モジュールと上位フロー数(前頁図 44①)の設定が行えます。 表示はその時点での設定です。変更する場合は、リンクをクリックします。 詳細は、**10. 解析機能** を参照してください。
アラート閾値設定 **(リンク/図 43②)**	モジュールでマイクロバーストを選択した場合、マイクロバーストのリンク(前頁図 44②)のリンクが有効になります。マイクロバースト解析の閾値と分解能が設定できます。 表示はその時点での設定値です。変更する場合は、リンクをクリックします。 詳細は、**10.4. マイクロバースト解析**を参照してください。
重複パケットを除去する	チェックした場合、重複パケット除去機能が有効になります。 100usec 以内に受信したすべてのチャネルからのパケットで、MAC ヘッダから FCS を除くデータまでが一致したパケットを重複パケットと判断し、2 つ目以降のパケットは保存しません。 一部未対応のモデルは、グレイアウトされ選択することができません。 対応モデルは、諸元一覧を確認してください。

4.4.1.1 ディスクフル時の動作=停止 の制限事項

- ディスクフル時の動作を停止にした場合、自動でキャプチャが停止する直前の数秒間ドロップカウントが上昇します。この現象は、ディスクがフルになった後に届いたパケットがカウントされているもので、SYNESIS がパケットのキャプチャに失敗したことを示すものではありません。
- ディスクフル時の動作を停止にしてキャプチャを開始した場合、ディスクがフルになった後もキャプチャステータスが更新されません。画面をリフレッシュするとステータスが停止になります。

4.4.1.2 解析モジュールと上位のフロー数の指定

キャプチャ中の自動解析を有効にすると、解析モジュールと上位フロー数の設定が行えます。表示はその時点で設定です。変更する場合は、リンクをクリックします。

以下の[解析モジュールと上位のフロー数]ダイアログが表示されます。

図 45：「解析モジュールと上位のフロー数」ダイアログ

設定が完了したら[適用]ボタンをクリックします。

設定項目は、以下の通りです。

項目	説明
モジュール	有効にする解析モジュール選択します。選択可能なモジュールは以下の通りです。 ● APM 解析 ● NPM 解析 ● L2/L3 プロトコル ● マイクロバースト 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。
トンネル	APM、NPM、L2/L3 プロトコル及び ARP 解析は、インナーヘッダで行われます。対応しているトンネルプロトコルの種類は、4.3.1.3 インナーヘッダで解析できるトンネルプロトコルの種類を参照ください。 アウターヘッダで解析を行う場合は、「最も外側のヘッダで解析」にチェックを入れます。
上位のフロー	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。

4.4.1.3 インナーヘッダで解析できるトンネルプロトコルの種類

以下のトンネルプロトコルが使われている場合、APM、NPM、L2/L3 プロトコル及び ARP 解析は、インナーヘッダで行われます。

アウターヘッダで解析を行う場合は、「最も外側のヘッダで解析」にチェックを入れます。

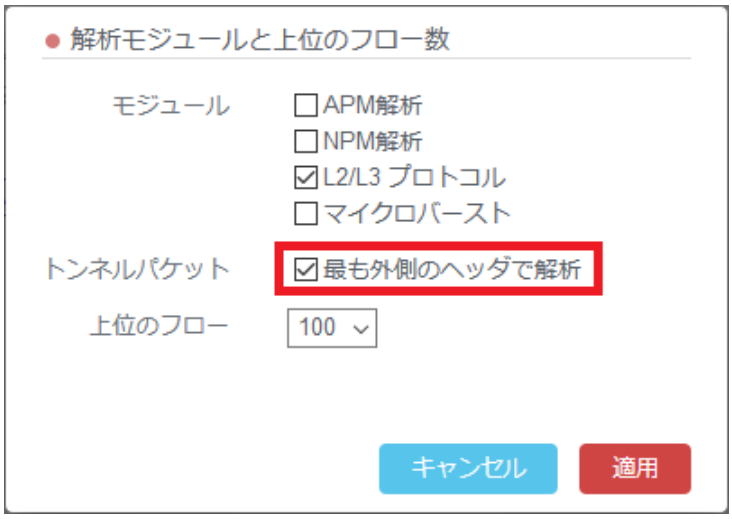


図 46:「最も外側のヘッダで解析」を選択

VLAN, MPLS, IPinIP は二重以上の階層的なタギングに対応しています。

インナーで解析可能なトンネルプロトコル	種類
EoE	Version 2 (イーサタイプ 0xa100) Version 3 (イーサタイプ 0xb100)
VLAN	IEEE 802.1Q (イーサタイプ 0x8100) IEEE 802.1ad (イーサタイプ 0x88a8, 0x9100, 0x9200, 0x9300) IEEE 802.1ah(PBB) (イーサタイプ 0x88e7)
MPLS	MPLS ユニキャスト (イーサタイプ 0x8847) MPLS マルチキャスト (イーサタイプ 0x8848) MPLS in IP (IP プロトコル番号 137) MPLS in UDP (UDP ポート 6635) MPLS Pseudowire MPLS over GRE
GRE	NVGRE GRE in UDP
GTP	GTP User Plane (UDP/TCP ポート 2152)
PPPoE	PPPoE (イーサタイプ 0x8864)
L2TP	L2TP (IP プロトコル番号 115)
EtherIP	EtherIP (IP プロトコル番号 97)
IPinIP	IPinIP (IP プロトコル番号 4)
VXLAN	VXLAN (UDP ポート 4789)

4.4.1.4 マイクロバースト解析のアラート閾値設定

モジュールでマイクロバーストを選択した場合、マイクロバーストのリンク(図 44②)のリンクが有効になります。マイクロバースト解析の閾値と分解能が設定できます。

表示はその時点での設定値です。変更する場合は、リンクをクリックします。

図 47：アラート閾値設定画面

設定が完了したら[適用]ボタンをクリックします。

詳細は、**10.4.1. マイクロバーストの閾値の検出方法**を参照してください。

4.4.2. キャプチャフィルタ オプション

キャプチャフィルタは、キャプチャ時に必要なパケットのみをディスクに保存するためのフィルタです。フィルタでキャプチャ対象外となったパケットは、ディスクに保存されません。

設定は、キャプチャを開始する前に行います。

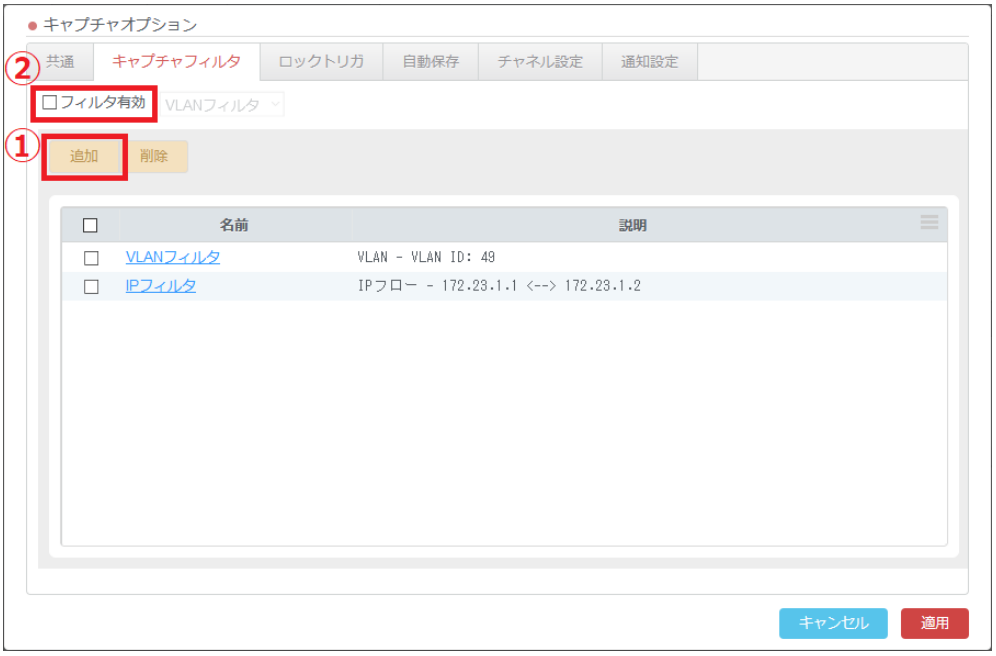


図 48：キャプチャフィルタオプション画面

なお、モデルによってはキャプチャフィルタは使用できません。未対応モデルでは、「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。

使用可能なモデルかどうかは、諸元一覧を参照ください。

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 オプション」タブで[追加]ボタン(前頁図 48①)をクリックします。

以下の「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登録できます。

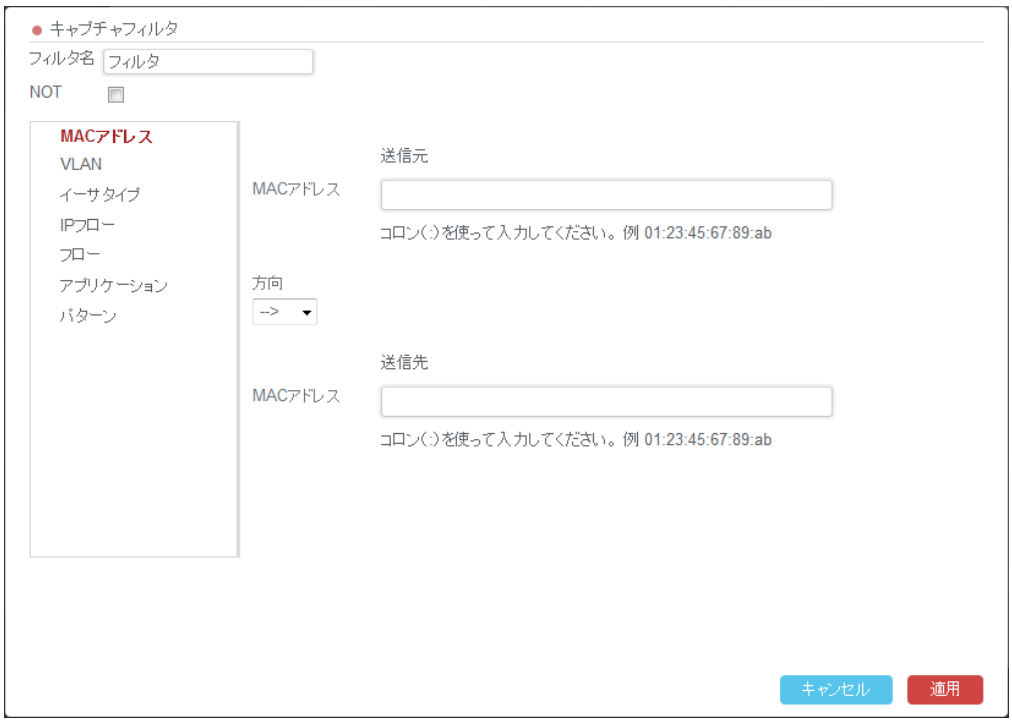


図 49 :「キャプチャフィルタ」ダイアログ

キャプチャフィルタを適用するためには、「フィルタ有効」のチェックボックス(前頁図 48②)にチェックを入れ、登録されているキャプチャフィルタ名を選択します。

キャプチャ時に適用できるフィルタは、ひとつのみです。複数のフィルタ項目を組み合わせて適用することはできません。

登録済みのキャプチャフィルタを削除する場合は、該当するフィルタの左端のチェックボックスにチェックを入れ、 画面左上の[削除]ボタンをクリックします。選択したキャプチャフィルタが削除されます。

登録済みのキャプチャフィルタをまとめて削除する場合は、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ます。

キャプチャフィルタリスト上にある登録済みの保存フィルタがまとめて削除されます。

詳細は、**6.1. キャプチャフィルタの概要** と **6.2. キャプチャフィルタの項目**を参照してください。

4.4.3. ロックトリガオプション

ロックトリガは、キャプチャ中にパケットが上書きされないように予め上書き禁止の設定を行う機能です。

詳細は、**9.2. 自動ロック** を参照ください。

4.4.4. 自動保存オプション

自動保存は、キャプチャしながら自動的にトレースファイルの作成、保存を自動的に行う機能です。

自動保存の有効/無効は、上部の「自動保存機能を有効にする」のチェックボックスで設定します。有効すると自動保存に必要な条件の設定が入力できます。

図 50：自動保存設定画面

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	保存するトレースファイル形式を指定します。 指定できるファイル形式は、pcap, pcap(ナノ秒), pcapng です。
分割ファイルサイズ	ファイルサイズを指定します。設定できる最大値は「構成」メニューの「トレースのサイズ」から設定できます。 詳細は **5.8. トレースファイルのサイズ**を参照してください。
最大ファイル数	保存するトレースファイルの上限数を指定します。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。 “0” を入力した場合はファイル数が無制限となります。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た場合、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	チェックを入れるとオートローテーション機能が有効になります。 オートローテーション機能は、トレースファイルの保存先の空き容量が少なくなってきた際に、 古いファイルから順に自動的に削除して、自動保存を続ける機能です。 詳細は **4.4.4.2. オートローテーション**オートローテーション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する場合、フィルタ名を選択します。 詳細は、**フィルタ機能**の章を参照してください。
スライス	パケットのスライスサイズを指定します。
保存先フォルダ	トレースファイルの保存先を指定します。 SYNESIS のディスク領域を指定する際には、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	保存先フォルダを指定します。
セカンダリを有効にする※	チェックを入れると、書き込み先にセカンダリフォルダを設定できます。プライマリフォルダへの保存に失敗した場合、セカンダリフォルダへ保存します。
セカンダリ	セカンダリの保存先フォルダを指定します
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の動作を選択します。 「保存先フォルダをプライマリに戻す」または「セカンダリのまま保存を継続する」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通知することができます。

詳細は、**4.4.6. 通知設定**を参照してください。

4.4.4.1 自動保存ファイルの保存先フォルダ構成

自動保存のフォルダ構成は以下の通りです。

[yyyymmdd]のフォルダの下に[HH]のフォルダが作成されます。

トレースファイル名は、HHMMSS+id となります。id は、0~9999 までの数字が自動的に割り当てられます。

```
[指定したフォルダ]
├[yyyymmdd]
│   ├[HH]
│   │   ├[HHMMSS.id.pcapng]
│   │   ├[HHMMSS.id.pcapng]
│   │   ├[HHMMSS.id.pcapng]
:   :   :
```

4.4.4.2 オートローテーション

オートローテーション機能は、保存先の空き容量が少なくなってしまった際に、古いファイルを削除して、自動保存を続ける機能です。

保存されている中で最も古いファイルから順に削除されていきます。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ファイルの削除を行います。

削除が実行されるトリガとして「期間」「サイズ」「パーティション」が指定できます。

項目	説明
期間	設定できる範囲は、1～365 日です。 新しい日付フォルダを作成する際に、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。その数が設定した期間に達していた場合、保存されている中で最も古い日付フォルダが削除されます。
サイズ	指定可能なサイズは、50 GB ～10240 GB です。 ファイルを保存する際、保存先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、保存されている中で最も古い時間フォルダが削除されます。
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パーティションの空き容量が、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が削除されます。

4.4.4.3 自動保存の性能

自動保存の性能には以下の制約があります。

- キャプチャレートが平均 1Gbps である必要があります。このレートを超えた場合、(1)キャプチャによるパケットの保存、および(2)トレースファイル作成のためのパケットの読み出し の 2 つの処理でディスクアクセスが競合し、SYNESIS の安定動作に影響が出る可能性があります。
- 保存先ディスクへの通信速度および書き込み速度は、平均キャプチャレートの 3 倍は必要です。例えばキャプチャレートが 1Gbps であれば、保存先への書き込み性能が 3Gbps は必要です。これは、トレースファイル作成が数秒から数十秒ごとに行われるため、保存先ディスクへの書き込み性能がピーク時でキャプチャレートの 3 倍程度は必要となるためです。
- 保存先ディスクは、SYNESIS 内部のディスクでないことが望ましいです。Databank を含む SYNESIS 内部のディスクに保存した場合、(1)キャプチャによるパケットの保存、(2)トレースファイル作成のためのパケットの読み出し、(3)トレースファイルの書き込み の 3 つの処理が競合するためです。

4.4.4.4 自動保存の制限事項

- 自動保存で作成した pcapng ファイルの Interface ID は、チャネルに関わらず 0 となります。
- 自動保存を有効にして、かつ時刻トリガによるロックを有効にしてキャプチャを行うと、ロックが設定時刻より遅れて作成される場合があります。
- 自動保存機能の保存先としてネットワークマウントを行っているディレクトリを指定する場合には、マウント時に適切にタイムアウトを設定する必要があります。
- 自動保存機能は、キャプチャ停止の直前 10 秒間のパケットは保存されません。
- 自動保存を有効にした場合、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。
- 自動保存機能の保存フィルタで、VoIP フィルタは適用できません。

4.4.5. チャネル設定

本画面では、チャネルごとにキャプチャの有効・無効、および使用率の計算基準となるラインスピードが指定できます。

図 51：チャネル設定画面

4.4.5.1 キャプチャ有効・無効の指定

キャプチャの対象とするチャネルをキャプチャ前に指定することができます。これにより、物理的な配線を変更せずに、所望のチャネルのみでキャプチャを行うことができます。

「チャネル設定を手動で変更する」にチェックを入れ、キャプチャの対象とするチャネルのみチェックを入れます。次回のキャプチャから、チェックを外したチャネルは無効化されます。

無効化されたチャネルは以下のように動作します。

- 無効にしたチャネルで受信したパケットは、パケットストアに保存されません。
- 無効にしたチャネルの DLC 統計値は、すべて 0 となります。
- 無効にしたチャネルに対して、リンクステータスの通知およびドロップの通知は行われません。
- キャプチャ中のリンクステータス表示は、灰色になります。

チャネル	ステータス	使用率	ビットレート	パケットレート	バイト	パケット	ドロップ	ブロードキャス
チャネルA		100.0%	568,314.23 kbps	169,047.00 pps	568,314,226	1,352,383	0	0
チャネルB		0.0%	0.00 kbps	0.00 pps	0	0	0	0
チャネルC		0.0%	0.00 kbps	0.00 pps	0	0	0	0
チャネルD		0.0%	0.00 kbps	0.00 pps	0	0	0	0

図 52：キャプチャ中のリンクステータス表示

- 画面右上のリンクステータス表示は、チャネルの有効・無効に関わらず、リンクアップまたはリンクダウンの状態が表示されます。

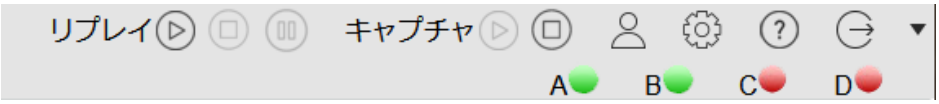


図 53：ツールバーのリンクステータス表示

4.4.5.2 ラインスピードの指定

ラインスピードは、統計値の使用率、およびマイクロバーストの使用率の計算の際 100%の基準として使用される値です。

「チャネル設定を手動で変更する」にチェックを入れると、ラインスピードが手動で設定できます。

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。

項目	説明
状態	各チャ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手動で設定できます。 単位は Kb, Mb, Gb から選択できます。

4.4.6. 通知設定

通知を行うイベントを指定できます。

図 54：通知設定画面

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行います。 自動保存機能についての詳細は **4.4.4. 自動保存オプション**を参照ください。
リンクステータス	各チャネルのリンクステータスが変化した際に通知を行います。 リンクステータスの変化とは、リンクアップ状態からリンクダウンした場合または、リンクダウン状態からリンクアップした場合を指します。
ドロップ	キャプチャ中にパケットがディスクに書き込めず、パケットドロップが発生した際に通知を行います。

「有効」にチェックを入れると、「通知グループ」を指定もしくは新規作成ができます。

「通知グループ」の登録方法は、**14.3.2. 通知グループの設定**を参照してください。

4.5. レコードによるキャプチャデータの管理

SYNESIS では、キャプチャの開始から停止までをひとつのレコードとして取り扱います。キャプチャしたデータの管理は、レコード単位で行います。

[レコード]タブでは、レコードに関連する操作を行います。

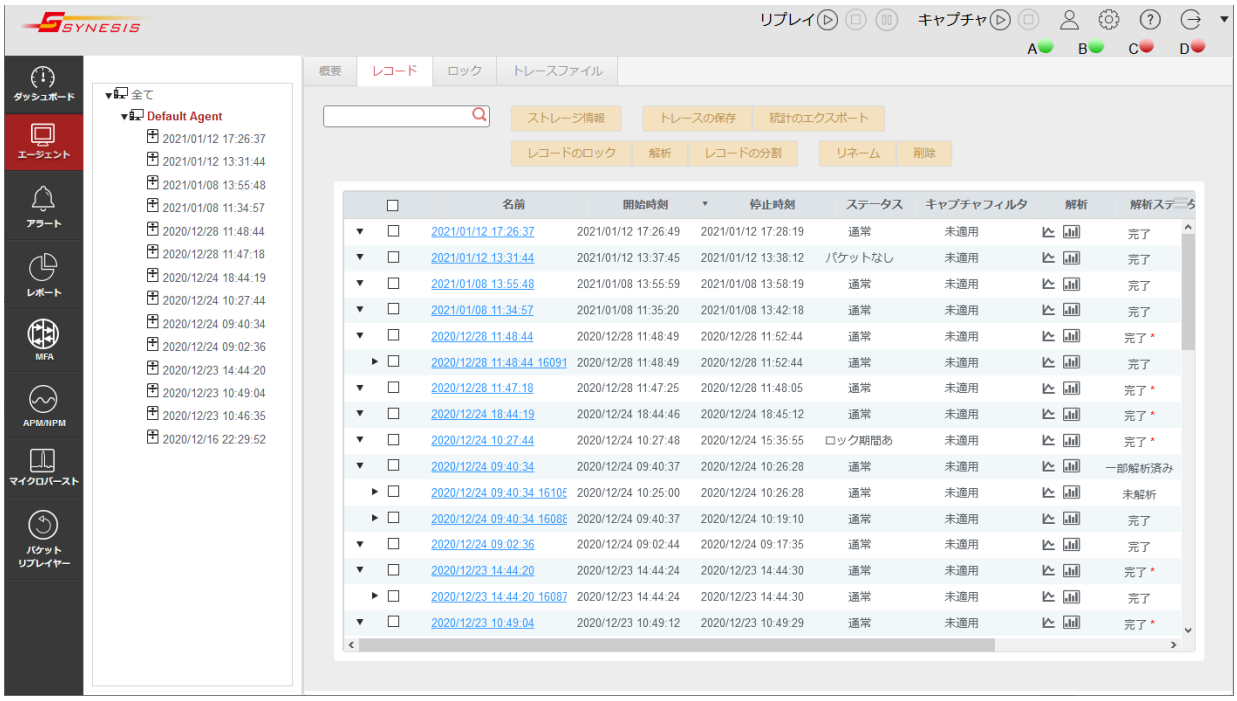


図 55 :「レコード」タブ画面

4.5.1. レコード一覧

[レコード]タブで確認できる情報は、以下の通りです。

項目	説明	
名前	レコードの名前です。キャプチャを開始する際レコード名を指定した場合は、指定した名前が表示されます。 名前の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。	
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。	
	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。
	上書き済み	レコード期間内にキャプチャしたパケットが全て上書きされた場合に表示されます。
	パケットなし	レコード期間内にパケットが全く保存されなかった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の条件が表示されます。 キャプチャフィルタが適用されていない場合は「未適用」と表示されます。
解析	レコードの開始時刻、停止時刻を指定した状態で、各解析メニューに移動します。 ：APM/NPM 解析 ：マイクロバースト解析
解析ステータス	解析ステータスが表示されます。 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	統計値の CSV ファイルが作成済みの場合、「ダウンロード」と表示されます。 「ダウンロード」のリンクをクリックすると統計値の CSV ファイルをダウンロードすることができます。 詳細は **8.2. 統計のエクスポート** を参照してください。

4.5.2. レコードからの操作

[レコード]タブの上部のボタンから、各レコードに対し操作が可能です。

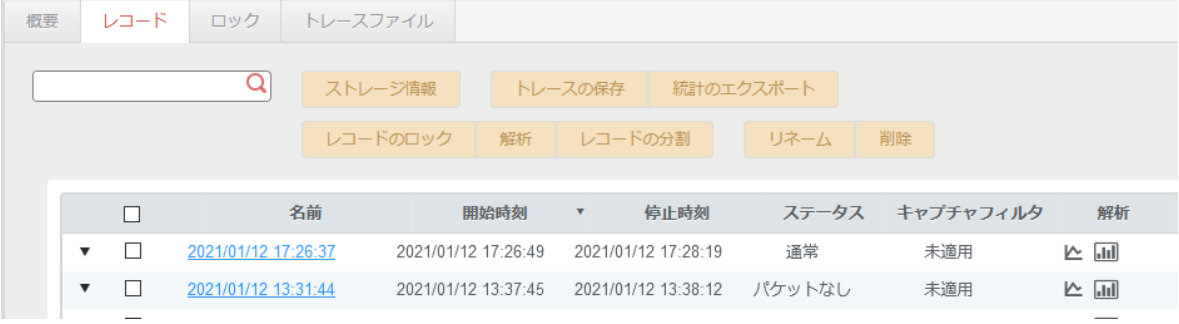


図 56：レコード・タブ上部のボタン

ボタン	説明
ストレージ情報	キャプチャされたパケットが保存されている 「パケットデータ領域」の使用状況が確認できます。 詳細は、**SYNESIS の構造**の章を参照してください。
トレースの保存	レコードからトレースファイルに保存することができます。 該当するレコードにチェックを入れ、[トレースの保存]ボタンをクリックします。 詳細は、**5. トレースの保存操作**を参照してください。
統計のエクスポート	レコード単位で統計のエクスポートができます。 該当するレコードにチェックを入れ、[統計のエクスポート]ボタンをクリックします。 詳細は、**統計情報**の章を参照してください。
レコードのロック	レコード単位でロックを設定できます。 該当するレコードにチェックを入れ、[レコードのロック]ボタンをクリックします。 詳細は、**ロック機能**の章を参照してください。
解析	レコード単位で解析を実施します。 該当するレコードにチェックを入れ、[解析]ボタンをクリックします。 詳細は、**10. 解析機能**を参照ください。

分割	レコードの一部を分割します。 該当するレコードにチェックを入れ、[分割]ボタンをクリックします。 詳細は、**レコードの分割**の節を参照してください。
リネーム	レコード名の名前を変更することができます。 該当のするレコードのチェックボックスにチェックを入れ、 [リネーム] ボタンをクリックすると、「レコードの編集」画面が表示されます。 「名前」に任意の名前を入力し、[適用]ボタンをクリックすると、レコードの名前が変更されます
削除	レコードを削除できます。 該当するレコードにチェックを入れ、[削除]ボタンをクリックします。 全てのキャプチャレコードを削除する場合は、リストの一番上のチェックボックスにチェックを入れると、 全てのレコードが対象となります。

4.5.3. レコードの分割

レコードの一部を分割し、分割したレコードに対して操作を行うことが可能です。

分割することにより、以下のような利点があります。

- トレースの保存、統計のエクスポート、解析の実行時間の短縮
- ２度目以降の時間指定が省略可能

分割したレコードに対して、分割前のレコードと同等な操作が行えます。

可能な操作は以下の通りです。

- トレースの保存
- 統計のエクスポート
- レコードのロック
- 解析
- リネーム
- 削除
- キャプチャレコード・ワークスペースの表示

4.5.3.1 **レコードの分割手順**

レコードの分割手順は、以下の通りです。

1) 該当するレコードのチェックボックスにチェックを入れ、[レコードの分割]ボタンをクリックします。

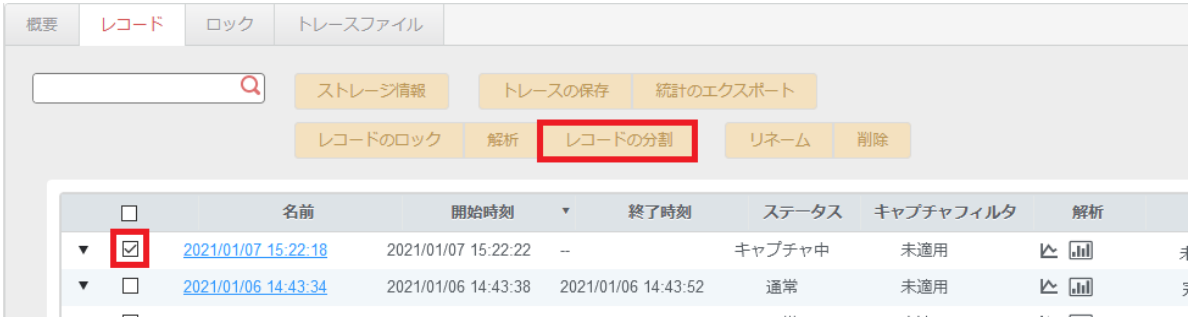


図 57：レコードの分割

2)　「レコードの分割」画面が表示されます。分割レコード名と分割する期間の指定を行います。
「期間」の指定で選択できる設定は「開始/終了」と「センタースパン」です。

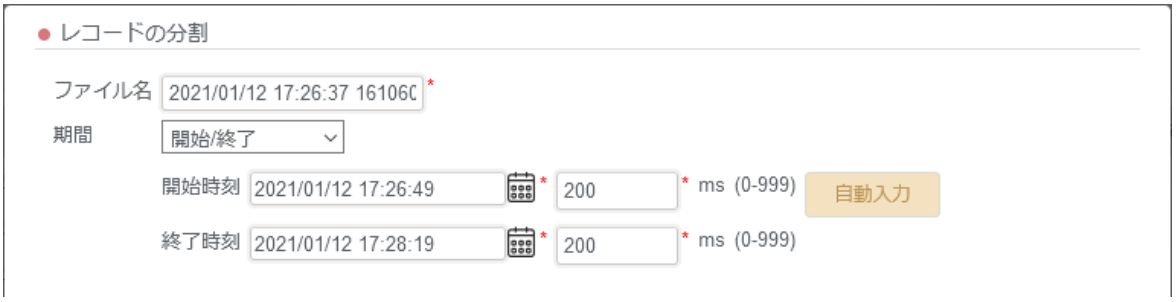


図 58：レコードの分割-「開始/終了」設定

「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(時間/分/秒/ミリ秒)を指定します。

[自動入力]ボタンをクリックすると、選択内容に応じて開始時刻・終了時刻が自動設定されます。

選択可能な時間範囲は、以下の通りです。

30 分、 1 時間、12 時間、24 時間、48 時間、72 時間、前日 24 時間

3)　元のレコードの下に作成された分割レコードが表示されます。

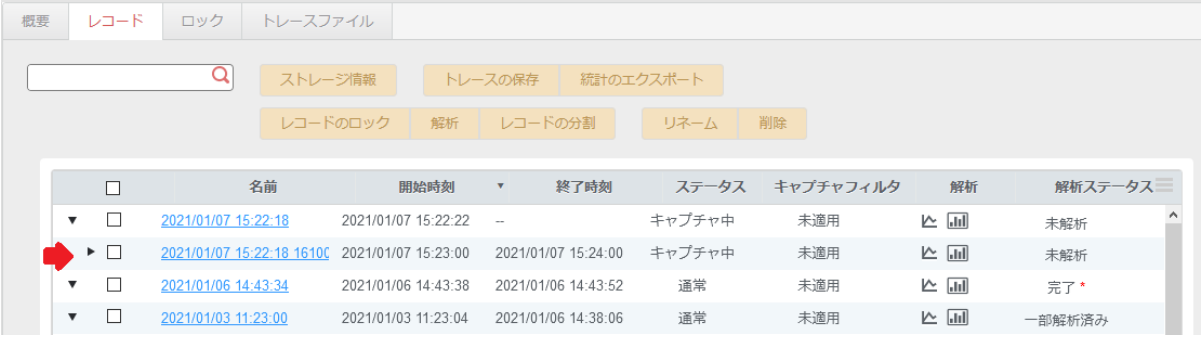
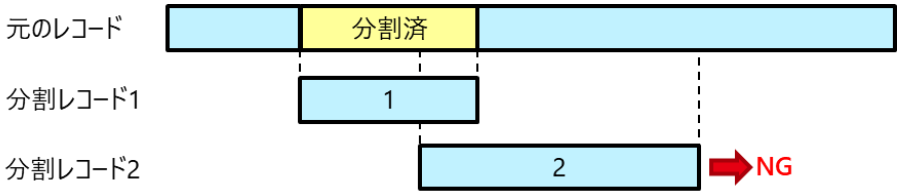


図 59：分割レコードの表示

4.5.3.2 **分割レコードの作成に関する仕様**

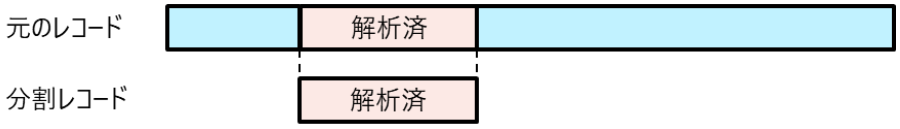
- リアルタイム解析を実施していない場合は、キャプチャ中のレコードも、分割が可能です。
- 分割レコードは、レコード全体で 10 個まで作成可能です。
- 作成済の分割レコードと時間範囲が重複するような分割レコードは、作成できません。下記は分割レコード 1 が作成済の例ですが、分割レコード 2 は時間範囲が重複するため作成できません。



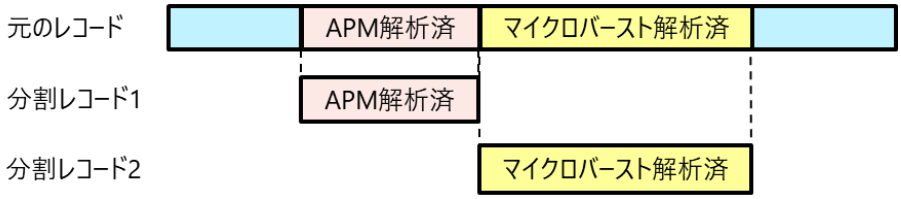
- 分割レコードをさらに分割することはできません。

4.5.3.3 **分割レコードの解析に関する仕様**

- レコードの分割が可能なのは、未解析のレコードに限られます。リアルタイム解析中のレコードと、ポスト解析済のレコードは、分割できません。
- 分割レコードを解析した場合、元のレコードの同じ時間範囲も解析された状態となります。



- 分割レコードが解析済の場合、元のレコードもその時間範囲の割合に応じて、一部解析済みとなります。
- 元のレコード全体が解析された場合は、「解析ステータス」の項目に"*(アスタリスク)"が付きます。
- APM/NPM 解析で参照されるホスト、サーバ、サーバグループは、元のレコードに紐づく各分割レコード間で共通設定が用いられます。最初に分割レコードを解析した時点の設定が、その後の分割レコードの解析でも用いられます。
- 元のレコードに紐づく各分割レコードに対して、異なる解析モジュールを適用したポスト解析が可能です。例えば 1 つの分割レコードに対して APM/NPM 解析、別の分割レコードに対してマイクロバースト解析を適用することができます。



- APM 解析はスリーウェイハンドシェイクが確立した通信を対象としています。そのため、スリーウェイハンドシェイクパケットが分割レコードの範囲外にある場合、それ以降の通信が解析対象となりません。
- キャプチャ中に、別のキャプチャ済みのレコードをポスト解析できるようになる訳ではありません。

4.5.3.4 **分割レコードの削除に関する仕様**

- 解析済の分割レコードは、削除できません。
- 分割前のレコードを削除すると、それに紐づくすべての分割レコードが同時に削除されます。

4.6. キャプチャのステータス

[エージェント]メニュー>[概要]タブは、キャプチャの開始・停止操作の他にキャプチャのステータスが確認できます。

図 60：[概要]タブ画面

画面上部のテーブルには、その時点で実行中のキャプチャに関する情報が表示されます。

キャプチャ中は、中央のテーブルにはチャネルごとの統計情報が、テーブルの下には統計情報のトレンドグラフが表示されます。

キャプチャが停止状態では、統計情報と統計情報のトレンドグラフは表示されません。

4.6.1. キャプチャの設定情報

画面上部のテーブルには、その時点で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	無効
ホスト	SYNESIS	スライス	無効
開始時刻	2020/01/31 16:54:07	ディスク フル時の動作	上書き
最終アップデート	2020/01/31 16:54:48	自動保存	プライマリ
持続時間	0 00:00:41	自動解析	有効
ステータス	キャプチャ	重複パケットの除去	無効

図 61：キャプチャの設定情報

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。変更できません。
ホスト	ホスト名です。
開始時刻	実行中のキャプチャを開始した時刻です。 キャプチャが停止中の場合は「--」と表示されます。
最終アップデート	統計情報の最終アップデート時刻です。 キャプチャが停止中の場合は「--」と表示されます。
持続時間	キャプチャを開始してからの経過時間です。 キャプチャが停止中の場合は「--」と表示されます。
ステータス	その時点でのキャプチャステータスです。 キャプチャ実行中は「キャプチャ」、停止中は「停止」と表示されます。
キャプチャフィルタ	実行中のキャプチャに適用されている、キャプチャフィルタの設定です。 キャプチャフィルタが適用されている場合はフィルタ名が表示され、適用されていない場合は「無効」と表示されます。
スライス	実行中のキャプチャに適用されている、スライスの設定です。 スライスが適用されている場合は設定のバイト数が表示され、適用されていない場合は「無効」と表示されます。
ディスクフル時の動作	実行中のキャプチャに適用されている、ディスクフル時のキャプチャ動作の設定です。表示されるステータスは以下の通りです。 ➢ 上書き：最も古いデータから上書きしキャプチャを停止しません。 ➢ 停止：ディスクが満杯になった時点でキャプチャを停止します。
自動保存	実行中のキャプチャに適用されている、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。 ➢ 無効：自動保存設定が無効です。 ➢ プライマリ：プライマリに指定したフォルダに自動保存しています。 ➢ セカンダリ：セカンダリに指定したフォルダに自動保存しています。 ➢ 失敗：自動保存に失敗し、自動保存していません。
自動解析	実行中のキャプチャに適用されている、自動解析の設定です。 キャプチャ中の自動解析が有効となっている場合は「有効」、無効となっている場合は「無効」と表示されます。
重複パケット除去	実行中のキャプチャに適用されている、重複パケット除去の設定です。 重複パケット除去機能が有効になっている場合は「有効」、無効になっている場合は「無効」と表示されます。

4.6.2. キャプチャの統計情報

中央のテーブルにはチャネルごとのキャプチャの統計情報が表示されます。

キャプチャ中は、統計情報を 5 秒ごとに更新します。

☑	チャネル	ステータス	使用率	ビットレート	パケットレート	バイト
☑	チャネルA		0.8%	513.82 kbps	175.00 pps	44,789,325,595
☑	チャネルB		0.3%	134.49 kbps	93.00 pps	11,723,292,574
☑	チャネルC		2.0%	1,238.05 kbps	308.00 pps	107,919,231,811
☑	チャネルD		0.0%	0.00 kbps	0.00 pps	0

図 62：キャプチャの統計情報テーブル

表示される情報は、以下の通りです。

- チャネル
- ステータス
- 使用率
- ビットレート
- パケットレート
- バイト
- パケット
- ドロップ
- ブロードキャスト
- マルチキャスト
- ユニキャスト
- CRC
- フラグメント
- ジャバー
- オーバーサイズ
- ラント
- アダプタ

フラグメントとラントの統計はモデルにより対応していません。未対応の場合、統計値は「N/A」と表示されます。対応モデルは諸元一覧を参照してください。

各項目の定義は、**8.3. 統計値の定義**を参照ください。

4.6.3. 統計情報のトレンドグラフ

画面下のグラフはチャネルごとの統計情報に基づくトレンドグラフです。横軸は、直近の５分間を１秒ごとにプロットします。

グラフ上にカーソルを合わせると、詳細な時刻と値が表示されます。

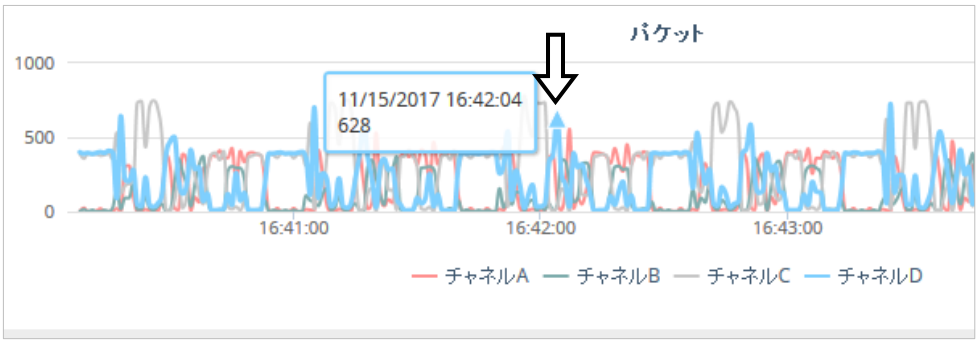


図 63：統計情報のトレンドグラフ

グラフ左上のリストボックスで表示するデータを指定します。選択可能な統計情報の項目は以下の通りです。

- 使用率
- ビットレート
- バイト
- パケット
- ドロップ
- ブロードキャスト
- マルチキャスト
- ユニキャスト
- CRC
- フラグメント
- ジャバー
- オーバーサイズ
- ラント
- アダプタ

フラグメントとラントの統計はモデルにより対応していません。未対応の場合、統計値は「N/A」と表示されます。対応モデルは諸元一覧を参照してください。

各項目の定義は、**8.3. 統計値の定義**を参照ください。

5.トレースの保存操作

トレースファイル保存の仕様と操作について説明します。

5.1. トレースの保存画面

トレースの保存画面は、以下の通りです。

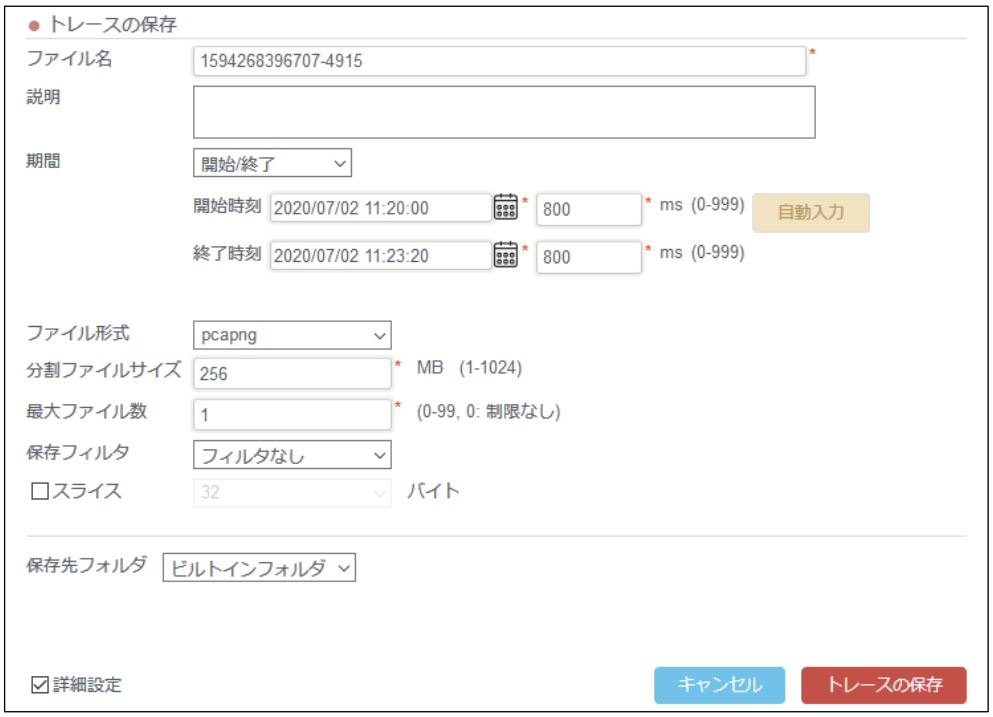


図 64：トレースの保存画面

設定項目は、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	トレースファイルの説明です。任意のコメントを入力できます。
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(時間/分/秒/ミリ秒)を指定します。
自動入力	クリックすると、選択内容に応じて開始時刻・終了時刻が自動設定されます。 選択可能な時間範囲は、以下の通りです。 30 分、 1 時間、12 時間、24 時間、48 時間、72 時間、前日 24 時間 詳細は、**5.2. タイムレンジの設定と自動入力**を参照してください。
ファイル形式	トレースファイルの形式です。 pcap、pcap (ナノ秒)、pcapng から選択できます。

「詳細設定」にチェックを入れると、下記の項目が設定可能になります。

項目	説明
分割ファイルサイズ(MB)	トレースファイルを分割するサイズの設定です。 トレースファイルが指定するサイズを超えた場合に、自動的にこのサイズに分割されます。
最大ファイル数(0-99, 0=無制限)	分割される最大ファイル数を設定します。 “0”を指定した場合は、無制限となります。
保存フィルタ	保存の際に適用するフィルタの設定です。 詳細は、**5.3. 保存フィルタの適用**を参照ください。
スライス	保存の際に適用するスライスの設定です。 スライスは、各フレームの先頭からの設定のバイト数までフレームサイズを切り詰める機能です。 32,64,128,256,512,1024 バイトで指定が可能です。
保存先フォルダ	トレースファイルの保存先の設定です。 「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、任意のフォルダを指定できます。 カスタムフォルダを選択した場合、ブラウザからのダウンロードとデコードが行えません。

5.2. タイムレンジの設定と自動入力

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。

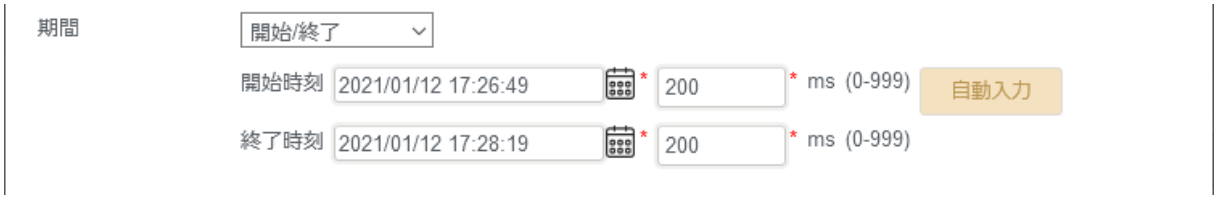


図 65 :「期間」の設定項目

初期状態では、下記の時間範囲が表示されます。

条件	開始時刻	終了時刻
キャプチャを停止したレコード	レコードの開始時刻	レコードの終了時刻
キャプチャ中のレコード	レコードの開始時刻	現在時刻
上記以外	表示中の時間範囲	

[レコード]タブまたはキャプチャレコード・ワークスペースからのトレース保存では、開始/終了モードで「自動入力」が可能です。[自動入力]ボタンをクリックすると、選択内容に応じて開始時刻・終了時刻が自動設定されます。終了時刻を手動で変更してからの「自動入力」も可能です。

「自動入力」で設定される開始時刻・終了時刻は以下の通りです。

項目	説明
30 分 1 時間 12 時間 24 時間 48 時間 72 時間	開始時刻: 現在表示中の終了時刻より選択した時間だけ前の時刻 終了時刻: 現在表示中の終了時刻
前日 24 時間	開始時刻: 現在表示中の終了時刻より 1 日前の 00:00:00.000 終了時刻: 現在表示中の終了時刻と同日の 00:00:00.000
リセット	開始時刻・終了時刻とも初期状態に戻ります

ただし、上記のいずれの場合においても、時間範囲内のパケットが上書きされている場合は、最も古いパケットの時刻が開始時刻になります。

5.3. 保存フィルタの適用

保存フィルタは、トレースファイルに保存する際、目的のパケットだけを保存するためのフィルタです。

構成メニューの保存フィルタで管理されており、「詳細設定」にチェックを入れると保存フィルタが指定できるようになります。

適用する保存フィルタを指定する場合は、「保存フィルタ」のドロップダウンリストをクリックします。下図のように保存フィルタの一覧が表示されます。

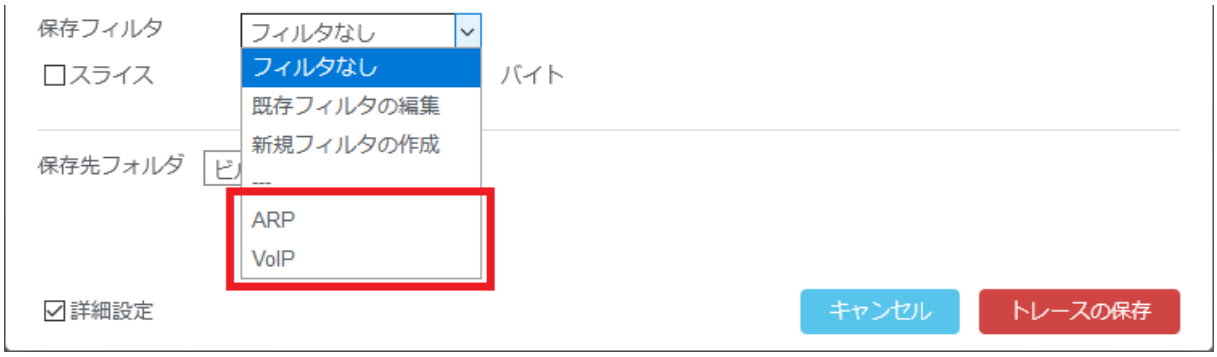


図 66:保存フィルタのドロップダウンリスト

適用する保存フィルタが定義済みであれば、リストの中(上図赤枠)からその保存フィルタを選択します。

選択した保存フィルタするキャンセルする場合は、「フィルタなし」を選択します。

管理者ロールで操作を行っている場合は、保存フィルタを追加・編集・削除することができます。

詳細は、**6.4. 保存フィルタの概要**を参照してください。

5.4. トレースの保存先

[トレースの保存]ボタンをクリックすると、画面は自動的に指定した保存先フォルダのタブに切り替わります。

図 67：トレースファイル保存の進行状況

ビルトインファイル・タブ画面の一覧には、新しいトレースファイルの行が追加され、ファイル保存の進行状況が表示されます。作成を途中で停止する場合は、ボタンをクリックします。トレースファイルの作成が中止され、中止されたところまでのトレースファイルが作成されます。

図 68：トレースフィアル・タブ

トレースの保存先は、以下の３つです。

- [**ビルドインファイル**]タブ：所定のフォルダに保存されているトレースファイルの一覧
- [**カスタムファイル**]タブ　：任意のフォルダに保存されたトレースファイルの一覧
- [**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の一覧

詳細は、それぞれのリンク先を参照してください。

5.4.1. ビルドインファイル

SYNESIS 内の規定のフォルダ内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。

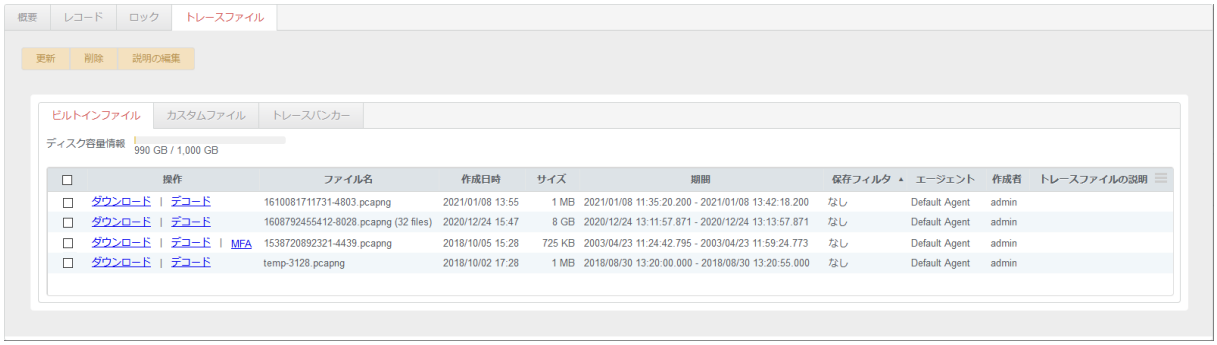


図 69：ビルトインファイル・タブ

一覧表の上に表示されている「ディスク容量情報」の帯グラフは、SYNESIS 内でユーザが作成したファイル保存する 「データバンク領域」の使用状況です。

「使用領域(GB) / データバンク領域の全容量(GB)」で表示されています。

一覧表で確認できる情報は以下の通りです。

項目	説明
操作	リンクから各操作が実施できます。 ・「ダウンロード」：トレースファイルのダウンロード ・「デコード」：新たに[デコード]タブが追加され、デコードを表示 ・「MFA」：MFA のフロー解析画面を表示 トレースファイル作成中はファイル保存の進行状態とキャンセル ボタンが表示されます。保存が完了すると「ダウンロード」と「デコード」のリンク表示に変わります。 「AA 解析(プレビュー版)」がインストールされている場合には、AA 解析へのリンクが表示されます。「AA 解析を実行」リンクをクリックすると、AA 解析が実行されます。解析が完了すると「AA 解析結果を表示」に変わり、リンクをクリックすると AA 解析結果が表示されます。 詳細は、AA 機能のマニュアルを参照してください。
ファイル名	トレースファイル名です。
作成日時	トレースファイルが作成された時刻です。
サイズ	トレースファイルのサイズです。
期間	トレースファイル保存時に指定した期間です。
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。 保存フィルタが適用されていない場合は、「なし」と表示されます。
エージェント	トレースファイルを作成した SYNESIS の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 SYNESIS のアカウントです。
トレースファイルの説明	トレースファイルの保存時に指定したトレースファイルの説明文です。 トレースファイルの保存後に編集することが可能です。

5.4.2. カスタムファイル

ユーザが定義した任意の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。

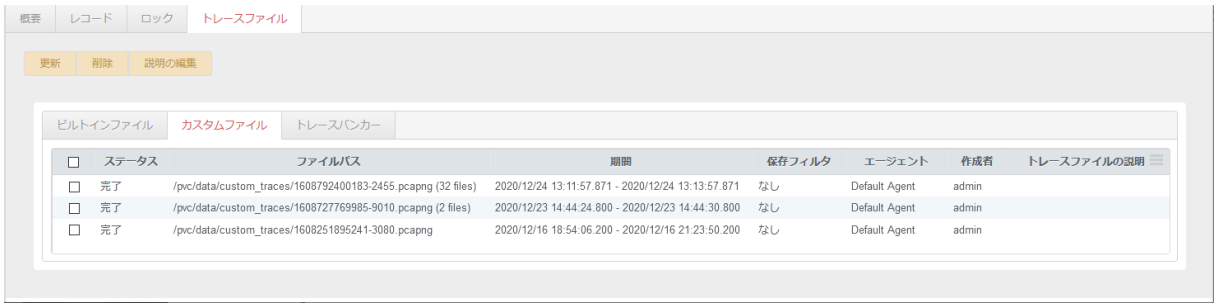


図 70：カスタムファイル・タブ

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、完了すると「完了」と表示されます。
ファイルパス	保存されたトレースファイルのファイルパスが表示されます。
期間	トレースファイル保存時に指定した期間です。
保存フィルタ	トレースファイルの保存時に適用された保存フィルタ名です。 保存フィルタが適用されない場合は、「なし」と表示されます。
エージェント	トレースファイルを作成した SYNESIS の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 SYNESIS のアカウントです。
トレースファイルの説明	トレースファイルの保存時に指定したトレースファイルの説明文です。 トレースファイルの保存後に編集することが可能です。

保存不可能なディレクトリを指定した場合でもエラーは表示されず一覧に追加されます。その場合は、実際にトレースファイルは保存されていません。

5.4.3. トレースバンカー

アップロードしたトレースファイルが一覧で表示されます。

この画面から、トレースファイルをアップロードすることが可能です。現在のユーザ以外がアップロードしたトレースファイルも閲覧できます。

トレースバンカー・タブは、管理者権限を持ったユーザのみ表示されます。

図 71：トレースバンカー・タブ

確認できる情報は、以下の通りです。

項目	説明
名前	アップロードしたトレースファイルの名前です。 「デコード」のリンクをクリックすると、トレースファイルのパケットがデコードされて表示されます。 デコード機能の詳細は **7. デコード機能** を参照してください。
サイズ	トレースファイルのサイズです。
更新日時	トレースファイルがアップロードされた時刻です。

SYNESIS に外部のトレースファイルをアップロードする場合は、[アップロード]ボタンをクリックします。「アップロード」ダイアログが表示されます。

図 72：アップロード・ダイアログ

[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ます。

指定したファイルがアップロードされ、一覧に追加されます。

5.5. トレースファイルの操作

[トレースファイル]タブの上部のボタンより、各種操作が可能です。

ボタン名	説明
更新	トレースファイルの保存先の一覧を更新します。 ただし、[カスタムフォルダ]タブは更新されません。
削除	トレースファイルを削除します。 該当のトレースファイルにチェックを入れ、[削除]ボタンをクリックします。 全てのトレースファイルを削除する場合は、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。
説明の編集	トレースファイル保存時に設定した「トレースファイルの説明」を編集します。 該当の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ます。

5.6. 各画面での機能差異

トレースの保存機能は、以下の画面から適用することが可能です。

画面	制限
[エージェント]メニュー>[レコード]タブ>各レコード	なし
[エージェント]メニュー>[ロック]タブ>各レコード	
[エージェント]メニュー>[デコード]タブ	
[エージェント]メニュー>[エージェント]ペイン> 各レコード>トレンドグラフ	
[アラート]メニュー>各アラート	なし
[MFA]メニュー>[フロービュー]タブ	分割ファイルサイズ、ファイル数、スライス、保存フィルタの指定不可
[MFA]メニュー>[MFA]タブ	
[MFA]メニュー>[パケットロス]タブ	
[APM/NPM]>[APM]タブ>各フロー	保存フィルタの指定不可
[APM/NPM]>[NPM]タブ>各フロー	
[マイクロバースト]メニュー>各マイクロバーストアラート	なし

- MFA からトレースを保存する場合、分割ファイルサイズ、ファイル数、スライス、保存フィルタの指定はできません。 「現在のフィルタを適用する」のチェックボックスが表示され、チェックを入れると選択中のフローのみ、チェックを外すとデータソース全体が保存されます。
- APM/NPM からトレースを保存する場合、任意の保存フィルタは指定できません。選択中のフローでフィルタが自動的に設定されます。

5.7. トレースの保存全般の制限事項

- 最大ファイル数を 2 以上としてトレースの保存を開始し、保存先の容量が一杯になった場合は、作成済のファイルもダウンロードできません。
- アラート、APM/NPM、マイクロバースト画面からトレースファイルの保存をした場合、pcapng ファイルの Interface ID の値は、チャネルに関わらず 0 となります。
- サイズの大きいトレースファイル (概ね 10GB 以上) を保存した後、最初にトレースファイルへのアクセスを行うタイミングで、応答時間が 1～2 分必要となります。この事象は 1 つのトレースファイルにつき 1 回のみ発生します。

5.8. トレースファイルのサイズ

「構成」メニュー>「トレースファイルのサイズ」では、トレースファイル作成時のファイルサイズの上限を指定します。

トレースファイルは、ここで指定されたサイズ以下のファイルに分割されて保存されます。

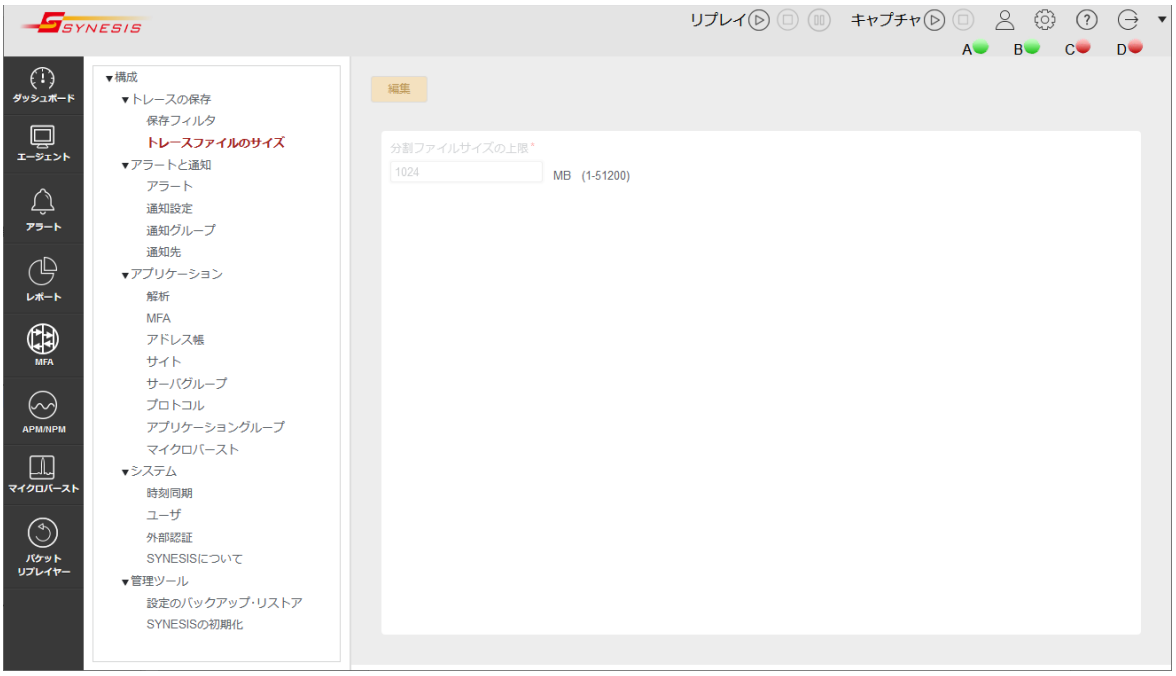


図 73：トレースファイルのサイズ画面

上限値を変更するする場合は[編集]ボタンをクリックします。

「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。

図 74：「トレースファイルのサイズ」編集画面

希望するファイルサイズの上限値を MB 単位で入力し、[保存]ボタンをクリックします。GUI 上で指定できる値は、1MB～51200MB です。

6.フィルタ機能

フィルタの種類、適用方法、定義について、説明します。

フィルタは、以下 2 種類があります。

種類	用途
キャプチャフィルタ	キャプチャ時に目的のパケットだけを保存するために設定をするフィルタです。 キャプチャ時に適用できるフィルタ項目は、ひとつのみです。
保存フィルタ	目的のパケットだけを保存する、または表示するために設定するフィルタです。保存フィルタの機能は、適用する画面により異なります。 フィルタ項目を AND/OR/NOT で組み合わせることにより、複雑な条件を設定することが可能です。

キャプチャフィルタの概要と**保存フィルタの概要**では、設定項目や制限が異なります。

詳細は、該当の節を確認してください。

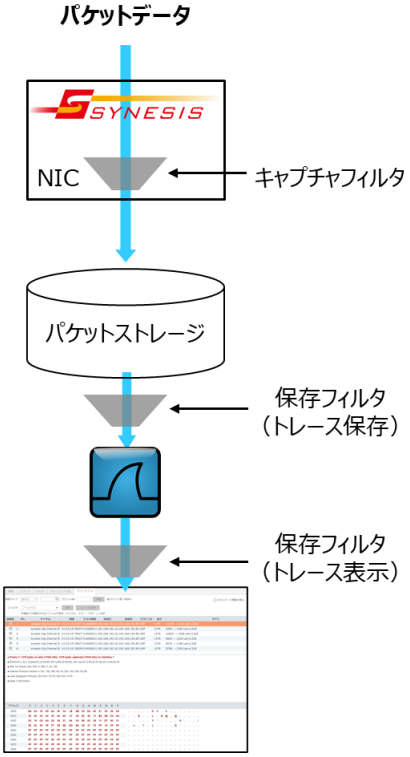


図 75：パケットキャプチャ時のフィルタ適用イメージ

6.1. キャプチャフィルタの概要

キャプチャフィルタは、キャプチャ時にフィルタを設定し、必要なパケットのみをディスクに保存するためのフィルタです。設定は、キャプチャを開始する前に行います。

フィルタでキャプチャ対象外となったパケットは、ディスクに保存されません。

なお、モデルによってはキャプチャフィルタは使用できません。未対応モデルでは、「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。

使用可能なモデルかどうかは、諸元一覧を参照ください。

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ます。

以下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登録できます。

図 76：キャプチャフィルタダイアログ

各項目入力後、[保存]ボタンをクリックします。新しいフィルタが登録されます。

登録済みのフィルタを編集している場合に[保存]ボタンをクリックすると、変更されたフィルタ条件で保存し直されます。

[名前を付けて保存]ボタンをクリックすると、元のフィルタの設定は変更せず、 編集したフィルタ条件が新しい名前で、別のフィルタとして登録されます。

キャプチャ時に適用できるフィルタ項目は、ひとつのみです。複数のフィルタ項目を組み合わせて適用することはできません。

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です。	
NOT	チェックを入れると、論理演算子「NOT」が適用され、「指定したフィルタ条件に当てはまらないもの」がフィルタされます。	
フィルタ項目	フィルタ項目です。選択可能なフィルタ項目は、以下の通りです。 キャプチャ時に適用できるフィルタ項目は、ひとつのみです。	
	MAC アドレス	送信元/送信先の MAC アドレスでフィルタします。
	VLAN	VLAN ID でフィルタします。

	イーサタイプ	イーサタイプでフィルタします。
	IP フロー	IP アドレスでフィルタします。
	フロー	IP アドレスと TCP/UDP ポート番号の組み合わせでフィルタします。
	アプリケーション	アプリケーションでフィルタします。
	パターン	指定したパターンでフィルタします。

フィルタの種類によってフィルタの定義方法が異なります。

6.2. キャプチャフィルタの項目

キャプチャフィルタの項目について説明します。

6.2.1. MAC アドレス

MAC アドレスでフィルタします。

図 77： MAC アドレスフィルタ設定画面

項目	説明
MAC アドレス	送信元と送信先の MAC アドレスを入力します。 6 バイトの 16 進数を 1 バイトずつコロン(:)で区切った形で入力します。 空欄の場合は全ての MAC アドレスが対象になります。
方向	パケットの方向を指定します。 「<-->」、「-->」、「<--」、から選択します。

6.2.2. VLAN

VLAN ID でフィルタします。

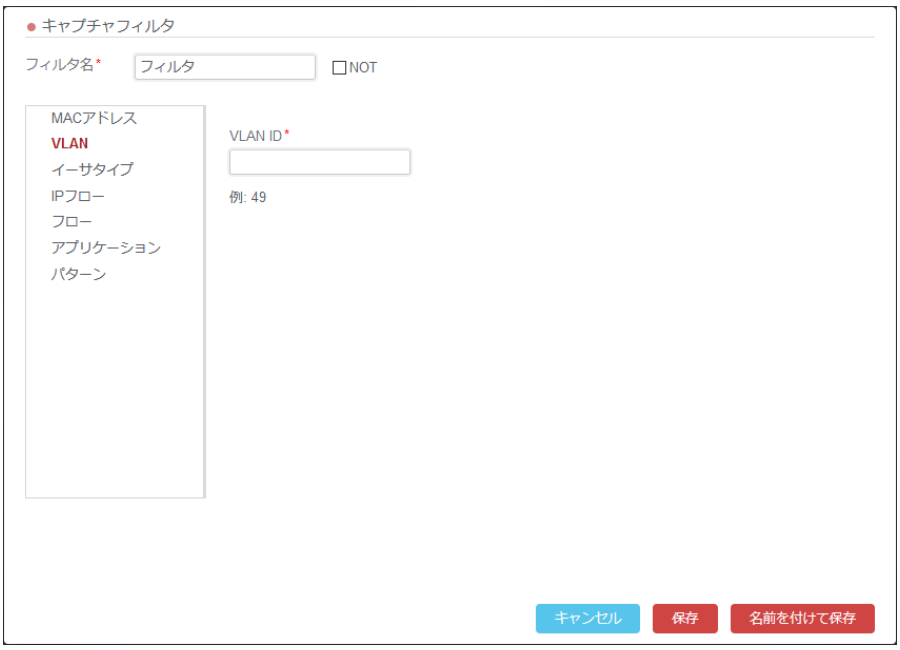


図 78 : VLAN フィルタ設定画面

項目	説明
VLAN	VLAN ID を入力します。0 以上 4095 以下の値で入力してください。 VLAN が多段で構成されている場合、指定した VLAN ID がどこに含まれていても、合致したものをフィルタします。 ただし、VLAN 構成が 4 段以上で構成されている場合は、イーサヘッダよりの 3 段までがフィルタの対象となります。 VLAN ヘッダは、以下に対応しています。 ➢ IEEE 802.1Q (イーサタイプ 0x8100)

6.2.3. イーサタイプ

イーサタイプでフィルタします。

図 79 : イーサタイプフィルタ設定画面

項目	説明
イーサタイプ	イーサタイプを 16 進数で入力します。

6.2.4. IP フロー

IP アドレスでフィルタします。

図 80 : IP フローフィルタ設定画面

項目	説明
IP アドレス	IPv4、IPv6 アドレスを指定します。 複数のアドレスを指定する場合は、";(半角セミコロン)"で区切ります。 IPv4 アドレスと IPv6 アドレスを組み合わせて指定することが可能です。 例) 172.23.1.1; 172.23.1.2 172.23.1.1; 2001:088::8:800:0:1 IP アドレスは、CIDR 形式で指定可能です。 例) 192.168.1.0/24" 2001:DB8:0:0:8:800::/96 CIDR 形式で指定した場合、IP アドレスは複数指定できません。 空欄の場合は、「Any」となり全ての IP アドレスが対象になります。
方向	パケットの方向を指定します。 「<-->」、「-->」、「<--」から選択できます。
トンネルオプション	指定した IP がカプセル化されている場合、対象ヘッダを指定します。 アウターヘッダ、インナーヘッダ、両方から選択できます。詳細は、**6.3 キャプチャフィルタ時のトンネルオプション**を参照してください。

6.2.5. フロー

フローでフィルタします。

IP アドレスと TCP/UDP ポート番号の組み合わせで指定します。

図 81：フローフィルタ設定画面

項目	説明
TCP/UDP	「TCP」または「UDP」を選択します。
IP アドレス	IPv4、IPv6 アドレスを指定します。 複数のアドレスを指定する場合は、";(半角セミコロン)"で区切ります。 IPv4 アドレスと IPv6 アドレスを組み合わせて指定することが可能です。 例)　172.23.1.1; 172.23.1.2 172.23.1.1; 2001:088::8:800:0:1 IP アドレスは、CIDR 形式で指定可能です。 例)　192.168.1.0/24" 2001:DB8:0:0:8:800::/96 CIDR 形式で指定した場合、IP アドレスは複数指定できません。 空欄の場合は、「Any」となり全ての IP アドレスが対象になります。
ポート	送信元/送信先の TCP/UDP ポートの番号を 1 以上 65535 以下の数値で入力してください。複数のポートを指定する場合は ";(半角)" で区切ってポート番号を入力してください。 ポート番号を範囲で指定する場合は、間を "- (ハイフン)" でつないで入力してください。範囲を複数指定することはできません。 空欄の場合は全てのポート番号が対象になります。
方向	どちらが送信元になるか、パケットの方向を指定します。 「<-->」、「-->」、「<--」から選択できます。
トンネルオプション	アウターヘッダとインナーヘッダのどちらでフィルタするかを指定します。 両方を指定することも可能です。詳細は、**6.3 キャプチャフィルタ時のトンネルオプション**を参照してください。

6.2.6. アプリケーション

アプリケーションでフィルタします。

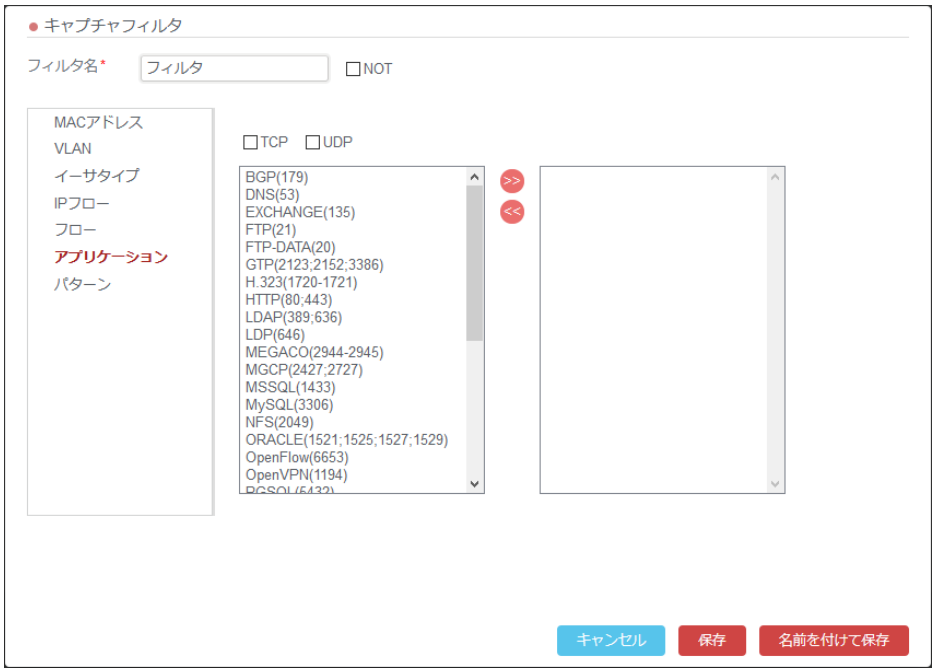


図 82：アプリケーションフィルタ設定画面

TCP/UDP の条件およびアプリケーションリストの条件を両方満たしたパケットがフィルタされます。

項目	説明
TCP/UDP	フィルタ対象とするプロトコルにチェックを入れます。
アプリケーションリスト	右側の欄(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がフィルタとして適用されます。 左側の欄には SYNESIS 内で定義済の L4 ポート番号がリストアップされています。このリストの中の適用するアプリケーションを選択し、 >> アイコンをクリックします。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。 フィルタに設定するアプリケーションがない場合は、構成メニューのプロトコルの項目でアプリケーション(L4 ポート番号)の定義を追加します。 右側のリストから外すには、該当のアプリケーションを選択し、 << アイコンをクリックします。

6.2.7. パターン

指定されたオフセットの位置にあるデータパターンでフィルタします。

図 83：パターンフィルタ設定画面

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」か「OR」で選択可能です。

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。

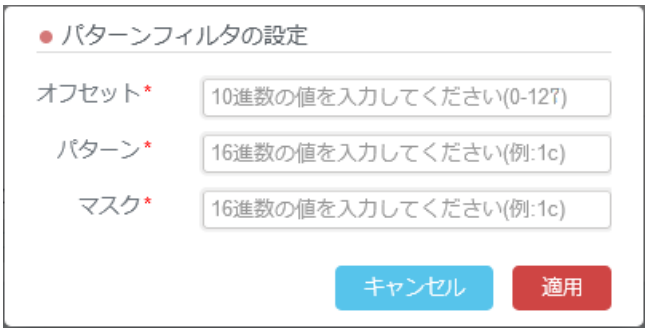


図 84：個々のパターンフィルタの設定画面

項目	説明
オフセット	パターンの一致を判定する開始位置を 10 進数のバイトで指定します。 0 以上 127 以下の数値で入力してください。
パターン	フィルタするパターンです。16 進数で指定します。
マスク	フィルタに適用される「マスク」のパターンを 16 進数で指定します。

「パターン」と「マスク」の指定方法の具体例は、**6.6. フィルタ共通の定義**を参照ください。

6.3. キャプチャフィルタ時のトンネルオプション

IP フローおよびフローフィルタを設定する場合、フィルタ対象をアウターヘッダとインナーヘッダのどちらで行うか指定できます。設定画面のトンネルオプションのリンクをクリックして設定します。

アウターヘッダ、インナーヘッダを識別できるトンネルプロトコルは、以下のとおりです。

プロトコル	種類
GRE v0	GRE Protocol Typefield 0x0800
GTPv0-U GTPv1-U	GTPMessage Type field 0xFF.
IPinIP	IPv4-in-IPv4 IPv4-in-IPv6
EtherIP	

- アウターヘッダ：トンネルプロトコルのアウターヘッダおよびトンネルプロトコル以外の IP フロー/フローが対象
- インナーヘッダ：トンネルプロトコルのインナーヘッダの IP フロー/フローが対象
- 全てのヘッダ：トンネルプロトコルのアウターヘッダとインナーヘッダおよびトンネルプロトコル以外の IP フロー/フローが対象

ラジオボタンで設定を選択すると、フィルタ対象となる設定がハイライトされます。選択後[適用]ボタンをクリックすると、選択が保存され元のフィルタ登録画面に戻ります。

6.3.1. アウターヘッダ

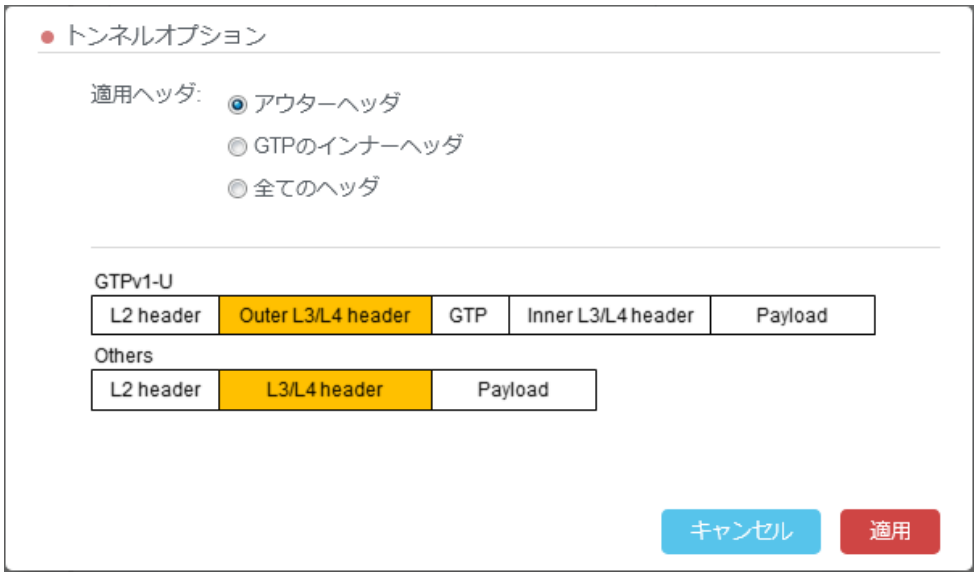


図 85：トンネルオプション・アウターヘッダー

なお、IP フローフィルタでは「L4 header」でのフィルタは対象外です。

「アウターヘッダ」を選択すると、トンネルプロトコルの「Outer L3/L4 header」とトンネルプロトコル以外の「L3/L4 header」でのフィルタが有効になります。

6.3.2. インナーヘッダ

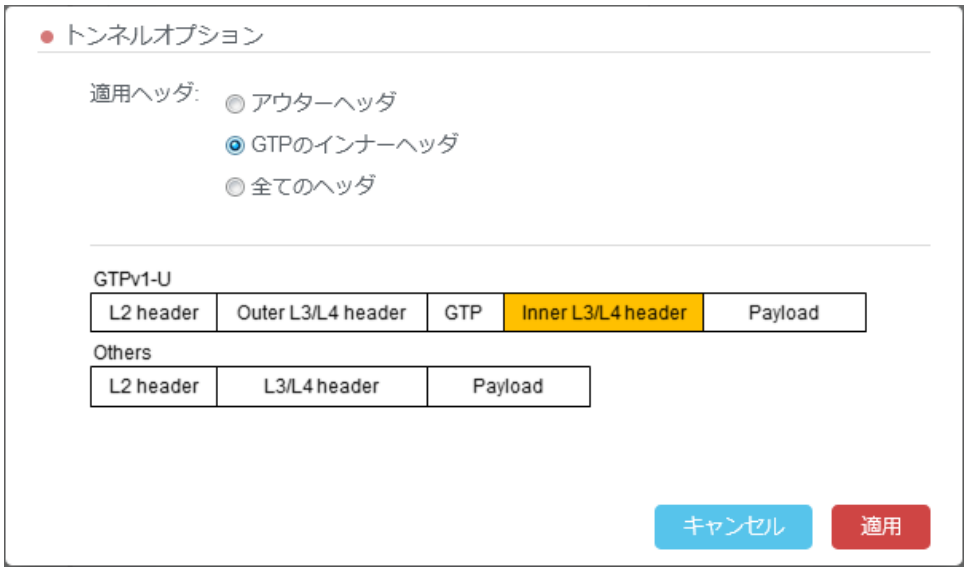


図 86：トンネルオプション・インナーヘッダ

「GTP のインナーヘッダ」を選択すると、トンネルプロトコルの「Inner L3/L4 header」でのフィルタが有効になります。

6.3.3. 全てのヘッダ

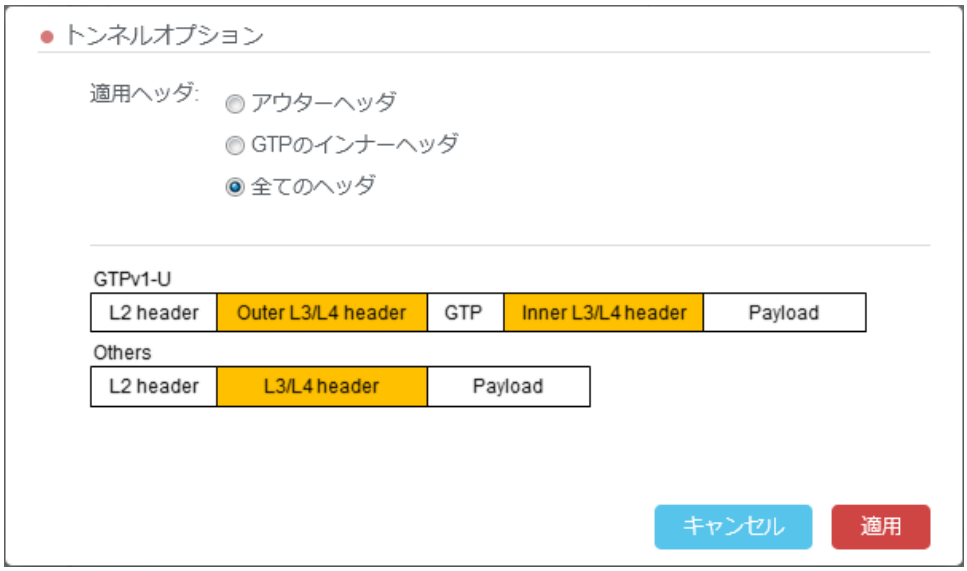


図 87：トンネルオプション・全てのヘッダ

「全てのヘッダ」を選択すると、トンネルプロトコルの「Outer L3/L4 header」と「Inner L3/L4 header」、トンネルプロトコル以外の「L3/L4 header」でのフィルタが有効になります。

なお、「全てのヘッダ」を指定した場合、「アウターヘッダ」や「インナーヘッダ」を指定したよりも、 IP フローフィルタやフローフィルタで指定できる IP アドレス数やポート数が少なくなる場合があります。

6.3.4. トンネルオプションの制限

- フローフィルタおよび IP フローフィルタのトンネルオプションに「すべてのヘッダ」を選択した場合、以下のパケットに対してフィルタが適用されません。
  - アウターヘッダとインナーヘッダの L3 プロトコルがともに IPv4 で、アウターヘッダにフィルタ条件がマッチするパケット
  - アウターヘッダとインナーヘッダの L3 プロトコルがともに IPv6 で、アウターヘッダにフィルタ条件がマッチするパケット
- IP フローフィルタおよびフローフィルタにおいて、一方のアドレス+ポートの範囲が他方を包含する指定をした場合、そのフィルタを保存できない場合があります。 また設定を保存できたとしても、キャプチャに適用した際に意図通りにフィルタできない場合があります。
  - IP フローフィルタの設定不可例(IP アドレス 1 が IP アドレス 2 を包含する)：

    IP アドレス 1 - 10.1.0.0/16

    IP アドレス 2 - 10.1.1.0/24
  - フローフィルタの設定不可例(IP アドレス 1+ポート 1 が IP アドレス 2+ポート 2 を包含する)：

    IP アドレス 1 - 10.1.0.0/16, ポート 1 - なし(Any)

    IP アドレス 2 - 10.1.1.0/24, ポート 2 – 100

6.4. 保存フィルタの概要

保存フィルタは、目的のパケットだけを保存する、または表示するために設定するフィルタです。保存フィルタの機能は、適用する画面により異なります。

適用する画面	機能
[エージェント]メニュー>[レコード]タブ>各レコード>[トレースの保存]ボタン	トレースの保存を実行する際に、条件に合致するパケットのみを保存します。
[エージェント]メニュー>[ロック]タブ>各レコード>[トレースの保存]ボタン	
[エージェント]メニュー>[エージェント]ペイン>各レコード>トレンドグラフ>[トレースの保存]ボタン	
[アラート]メニュー>各アラート>[トレースの保存]ボタン	
[APM/NPM]>[APM]タブ>各フロー>[トレースの保存]ボタン	
[APM/NPM]>[NPM]タブ>各フロー>[トレースの保存]ボタン	
[マイクロバースト]メニュー>各マイクロバーストアラート>[トレースの保存]ボタン	
[エージェント]メニュー>[デコード]タブ	デコードを表示する際に、条件に合致するパケットのみを表示します。
[MFA]メニュー>[MFA プロファイル]画面	MFA のマージを実行する際に、条件に合致するパケットのみをマージします。

[パケットリプレイヤー]メニュー>[プロファイル]画面>パケットフィルタ	パケットリプレイヤーのマニュアルを参照ください。
[パケットリプレイヤー]メニュー>[プロファイル]画面>置換フィルタ	

6.4.1. 保存フィルタの作成・管理

保存フィルタは、以下の手順で作成できます。

- 保存フィルタの作成

1) [保存フィルタ]画面を開きます。画面は、以下の操作で開くことが可能です。
   - [構成]メニュー>「保存フィルタ」>画面左上の[新規]ボタンをクリック
   - 各適用する画面から「保存フィルタ」のドロップダウンリスト>「既存フィルタの編集」>画面左上の[新規]ボタンをクリック
   - 適用する各画面から「保存フィルタ」のドロップダウンリスト>「新規フィルタの作成」選択

図 88：保存フィルタのドロップダウンリスト

下図の保存フィルタ登録画面が表示され、新しく保存フィルタを登録することができます。

図 89：保存フィルタ登録画面

2) 必要な項目を入力します。「名前」欄に登録するフィルタの名前を入力します。

「モード」でフィルタ項目を選択します。モードは、以下の通りです。

- 通常：単独のフィルタ条件で登録
- 詳細設定：複数のフィルタ条件を組み合わせて登録

3) 「なし」と書かれた「フィルタ項目」欄の編集 アイコンをクリックすると、下図のフィルタ項目画面が表示され、フィルタの種類や適用範囲など、個別のフィルタ条件を設定・登録できます。

図 90：フィルタ項目画面

設定可能なフィルタの種類は、**6.5. 保存フィルタの項目**を参照ください。

- 保存フィルタの編集

登録済みの保存フィルタの登録内容を変更する場合は、フィルタの「名前」欄のリンク部分をクリックします。 下図の保存フィルタ登録画面が表示されます。

図 91：保存フィルタ登録内容編集画面

フィルタ条件を変更する場合は、フィルタ条件が記載されている「フィルタ項目」欄右上の編集アイコンをクリックします。「フィルタ項目」画面が表示され、フィルタの種類や適用範囲を編集できるようになります。

登録内容を変更した状態で、[保存]ボタンをクリックすると、変更内容が保存されます。

[名前を付けて保存]ボタンをクリックすると、元のフィルタの設定は変更せず、 編集したフィルタ条件に名前を付けて、別のフィルタとして登録されます。

- 保存フィルタの削除

登録済みの保存フィルタを削除する場合は、該当するフィルタの左端のチェックボックスにチェックを入れ、 画面左上の[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。

登録済みの保存フィルタをまとめて削除する場合は、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ます。

保存フィルタリスト上にある登録済みの保存フィルタがまとめて削除されます。

6.4.2. 保存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、より複雑な条件を作成できます。

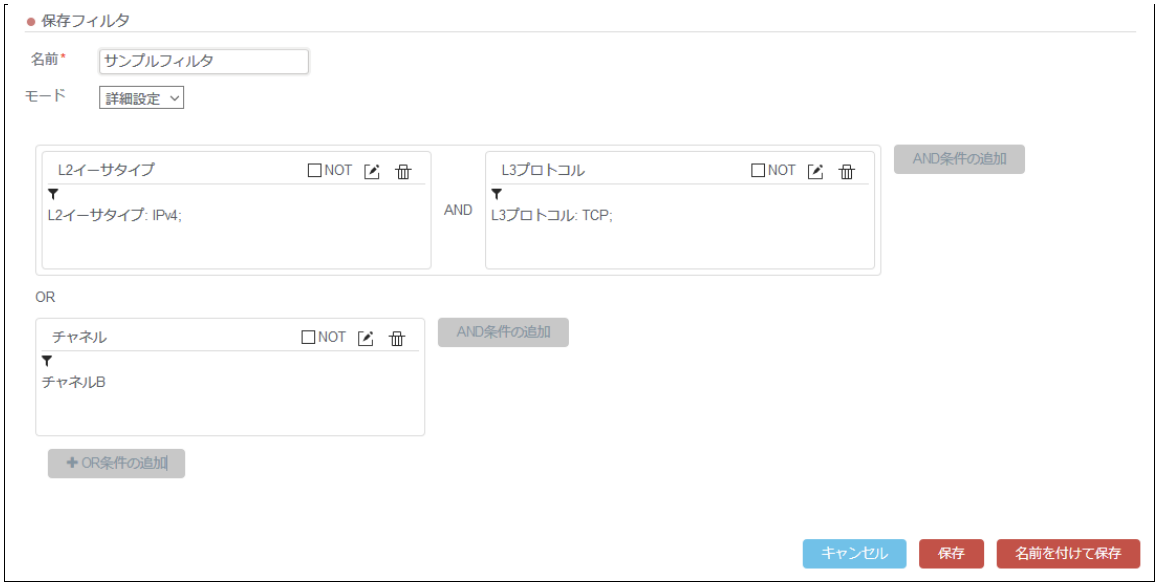


図 92：保存フィルタの詳細設定画面

横方向に並べた条件が AND で結合され、縦方向に並べた条件が OR で結合されます。条件の否定は「NOT」のチェックボックスで設定します。

既存フィルタの右側または下にある「AND 条件の追加」または「＋OR 条件の追加」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。

6.5. 保存フィルタの項目

保存フィルタの項目について説明します。

「構成」メニュー>「保存フィルタ」では、保存フィルタの設定・管理を行います。保存フィルタは、パケットを絞り込む際に設定するフィルタです。キャプチャフィルタ以外のフィルタ設定は、すべてこの「保存フィルタ」で行います。

キャプチャ時に適用されるキャプチャフィルタは、**6.1. キャプチャフィルタの概要**を参照してください。

図 93 :「構成」メニュー>「保存フィルタ」

構成メニューの「保存フィルタ」では、登録済みの「保存フィルタ」が一覧で表示されます。

保存フィルタの種類や適用範囲を指定するためには、保存フィルタ新規登録時や 編集時に表示される以下の保存フィルタ登録画面で、フィルタ項目欄の編集 アイコンをクリックします。

図 94 :「保存フィルタ」登録画面

下図の「フィルタ項目」ダイアログが表示されます。

図 95 :「フィルタ項目」ダイアログ

必要な設定を行った上で[適用]ボタンをクリックすると、設定したフィルタ条件が「フィルタ項目」として保存され、フィルタ項目欄に追加されます。

設定可能なフィルタの項目は、以下の通りです。

- チャネル
- 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
- VoIP

6.5.1. チャネル

チャネルでフィルタします。

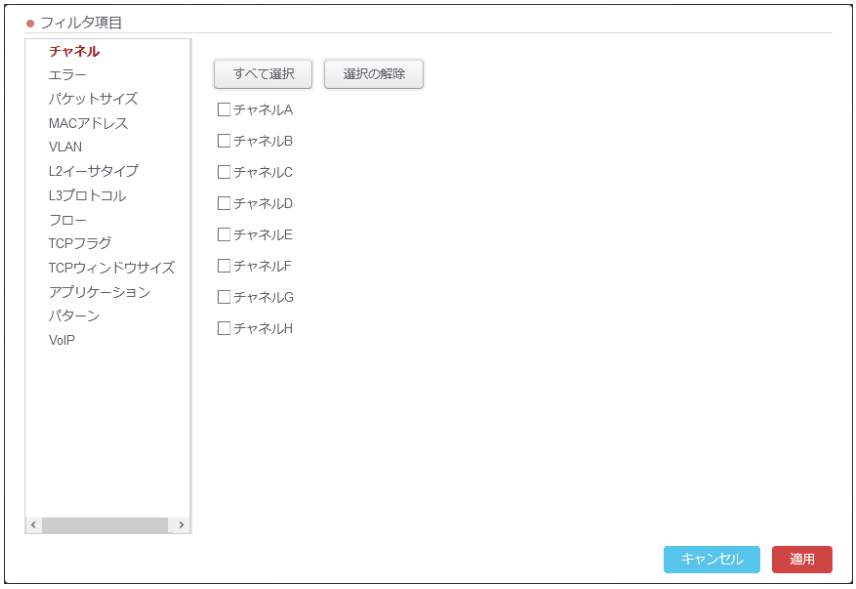


図 96：チャネルフィルタ設定画面

項目	説明
[すべてを選択]ボタン	クリックすると、すべてのチャネルにチェックされた状態になります。
[選択の解除]ボタン	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。
チャネル	チェックを入れたチャネルでキャプチャしたパケットがフィルタ対象です。 複数にチェックを入れた場合は、OR 条件で適用されます。

6.5.2. エラー

L2 エラーでフィルタします。

図 97：エラーフィルタ設定画面

項目	説明
L2 エラー	対象となる L2 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。 チェックを入れたエラーパケットがフィルタされます。複数チェックを入れた場合は OR 条件で適用されます。

V4.0 以前の一部モデルではエラーフィルタが適用できません。 詳細は、諸元一覧を確認してください。

6.5.3. パケットサイズ

パケットサイズでフィルタします。

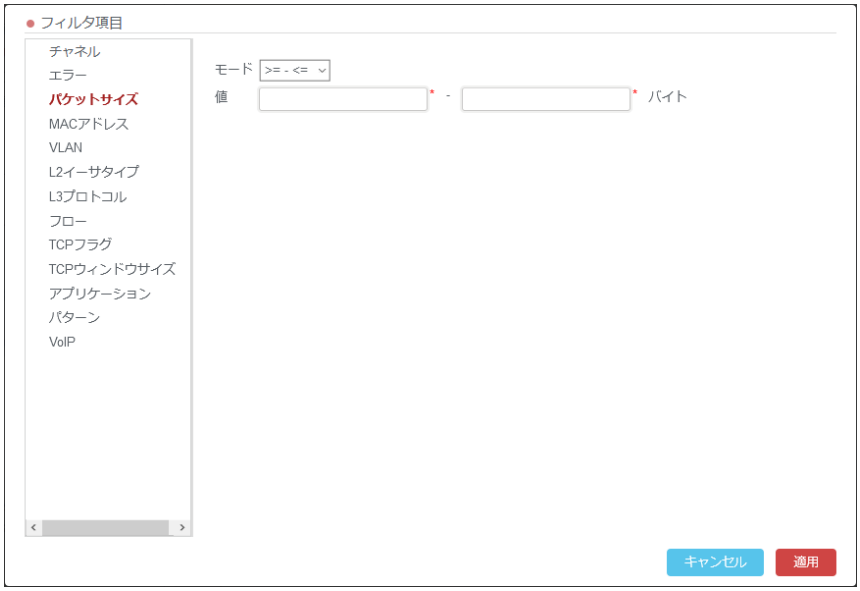


図 98：パケットサイズフィルタ設定画面

項目	説明
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	境界値をバイト単位で入力します。

6.5.4. MAC アドレス

送信元/送信先の MAC アドレスでフィルタします。

図 99：MAC アドレスフィルタ設定画面

項目	説明
MAC アドレス	送信元と送信先の MAC アドレスを入力します。 6 バイトの 16 進数を 1 バイトずつコロン(:)で区切った形で入力します。 空欄の場合は全ての MAC アドレスが対象になります。
方向の選択	どパケットの方向を指定します。 「-->」、「<--」、「<-->」、から選択します。

6.5.5. VLAN

VLAN ID でフィルタします。

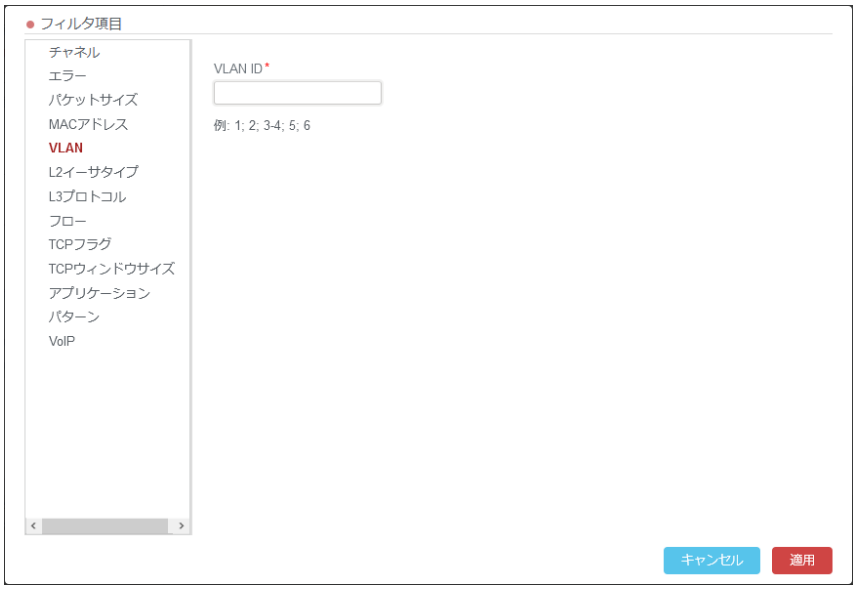


図 100：VLAN フィルタ設定画面

項目	説明
VLAN	VLAN ID を入力します。 0 以上 4095 以下の値で入力してください。 VLAN が多段で構成されている場合、指定した VLAN ID がどこに含まれていても、合致したものをフィルタします。 VLAN ヘッダは、以下に対応しています。 ➢ IEEE 802.1Q (イーサタイプ 0x8100) ➢ IEEE 802.1ad (イーサタイプ 0x88a8, 0x9100, 0x9200, 0x9300) ➢ IEEE 802.1ah(PBB) (イーサタイプ 0x88e7)

6.5.6. L2 イーサタイプ

イーサタイプでフィルタします。

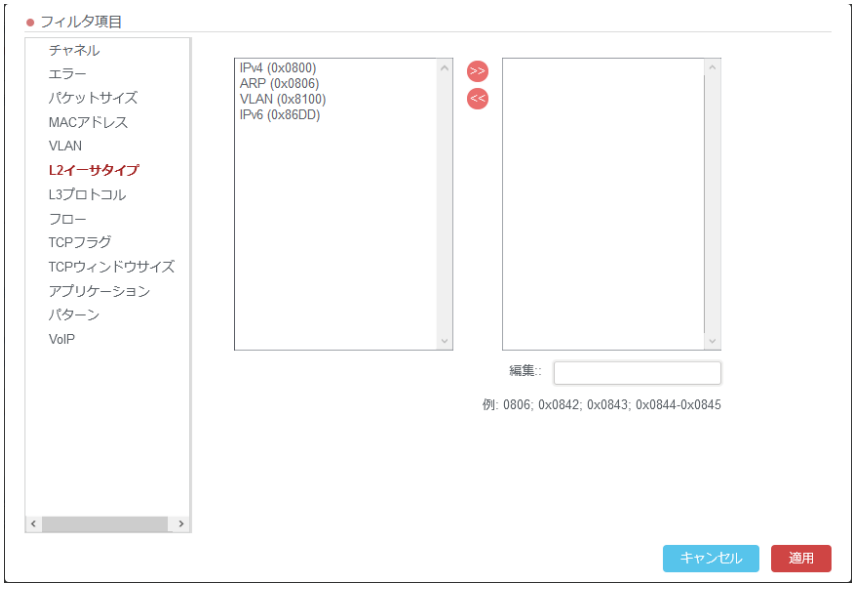


図 101：L2 イーサタイプフィルタ設定画面

項目	説明
L2イーサタイプリスト	右側の欄(デフォルトでは空欄)にリストアップされたイーサタイプがフィルタとして適用されます。 左側の欄には SYNESIS 内で定義済のイーサタイプがリストアップされています。このリストの中の適用するイーサタイプを選んで >> アイコンをクリックします。 選んだイーサタイプが右側のリストに追加されます。 する定義済以外のイーサタイプをリストに定義する場合は、構成メニューのプロトコルの項目で L2 イーサタイプの定義を追加します。 右側のリストから外すには、する該当の L2 イーサタイプを選択し << アイコンをクリックします。
編集	定義せずにイーサタイプを指定する場合は、16 進数で値を入力します。

6.5.7. L3 プロトコル

プロトコル番号でフィルタします。

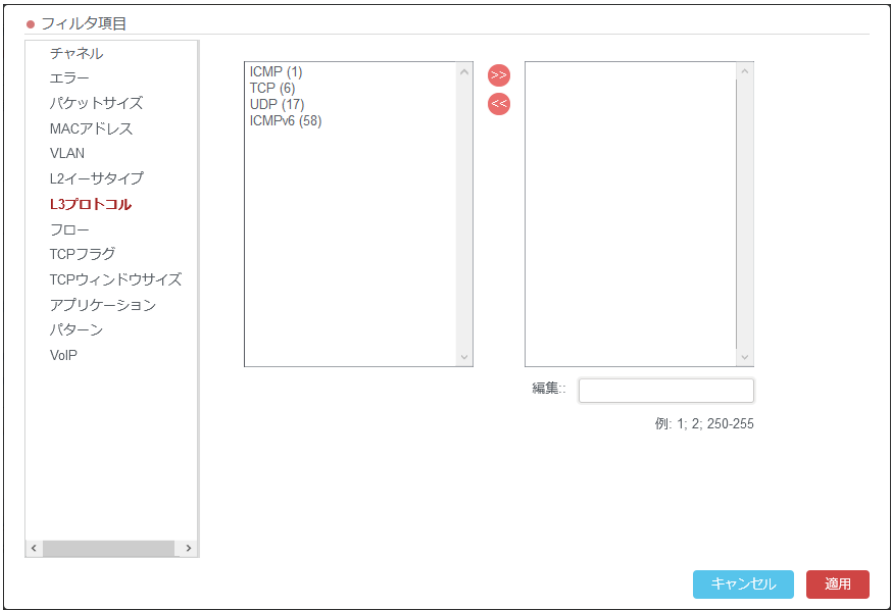


図 102：L3 プロトコルフィルタ設定画面

項目	説明
L3プロトコルリスト	右側の欄(デフォルトでは空欄)にリストアップされた L3 プロトコルがフィルタとして適用されます。 左側の欄には SYNESIS 内で定義済の L3 プロトコルがリストアップされています。このリストの中の適用する L3 プロトコルを選択し、 >> アイコンをクリックします。選んだ L3 プロトコルが右側のリストに追加されます。 定義済以外のプロトコル番号をリストに追加するには、構成メニューのプロトコルの項目で L3 プロトコルの定義を追加します。 右側のリストから外すには、該当する L3 プロトコルを選択し、 << アイコンをクリックします。
編集	定義をせずにプロトコル番号を指定する場合は、10 進数で値を入力します。

6.5.8. フロー

IP アドレスとポート番号の組み合わせでフィルタします。

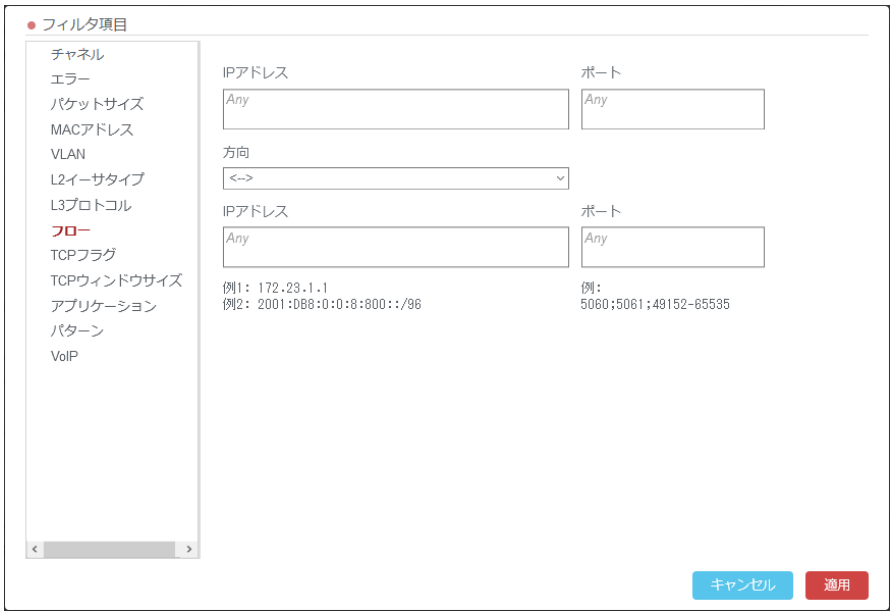


図 103：フローフィルタ設定画面

項目	説明
IP アドレス	IPv4 または IPv6 アドレスを入力します。 CIDR 表記でアドレスブロックを入力することも可能です。 （例：192.168.1.0/24, 2001:1111:2222:3333:: /64 等） 空欄の場合は、全ての IP アドレスが対象になります。
方向	パケットの方向を指定します。 「<-->」、「-->」、「<--」から選択してください。
ポート	TCP/UDP ポートの番号を 1 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"セミコロン(;)"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"-(ハイフン)"でつないでください。 空欄の場合は全てのポート番号が対象になり、TCP/UDP 以外のパケットも対象となります。

6.5.9. TCP フラグ

TCP コントロールフラグでフィルタします。

図 104：TCP フラグフィルタ設定画面

項目	説明
フラグ	チェックボックスにチェックの入った TCP コントロールフラグでフィルタされます。 指定可能な項目は「UGR」、「ACK」、「PSH」、「RST」、「SYN」、「FIN」の 6 種類です。 複数チェックを入れた場合は、OR 条件で適用されます。

6.5.10. TCP ウィンドウサイズ

TCP ウィンドウサイズでフィルタします。

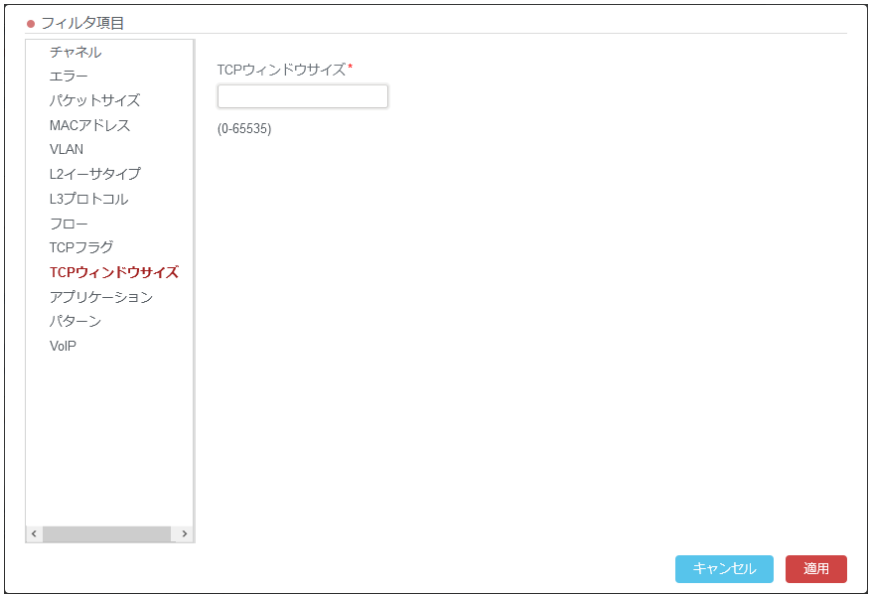


図 105：TCP ウィンドウサイズフィルタ設定画面

項目	説明
TCP ウィンドウサイズ	TCP ウィンドウサイズの値を入力します。 0 以上 65535 以下の数値で入力してください。

6.5.11. アプリケーション

アプリケーションでフィルタします。

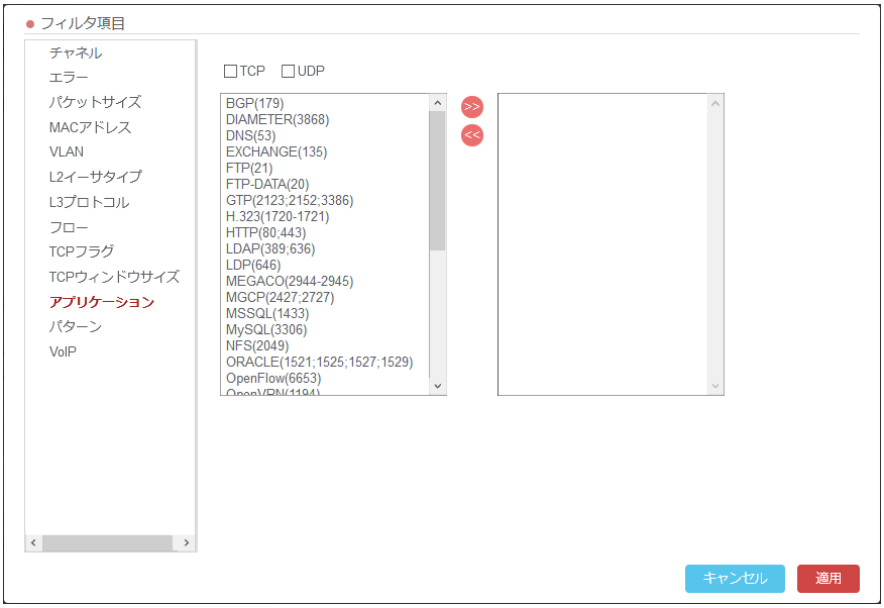


図 106：アプリケーションフィルタ設定画面

項目	説明
TCP/UDP	フィルタ対象とする L4 プロトコルを選択します。
アプリケーション	右側の欄にリストアップされたアプリケーションがフィルタとして適用されます。 左側の欄には SYNESIS 内で定義済の L4 ポート番号がリストアップされています。適用するアプリケーションを選択し、 >> アイコンをクリックします。 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。 アプリケーションを定義する場合は、構成メニューの プロトコルの項目でアプリケーション(L4 ポート番号)の定義を追加します。 右側のリストから外すには、該当するアプリケーションを選択し、 << アイコンをクリックします。

6.5.12. パターン

指定されたオフセットの位置にあるデータパターンでフィルタします。

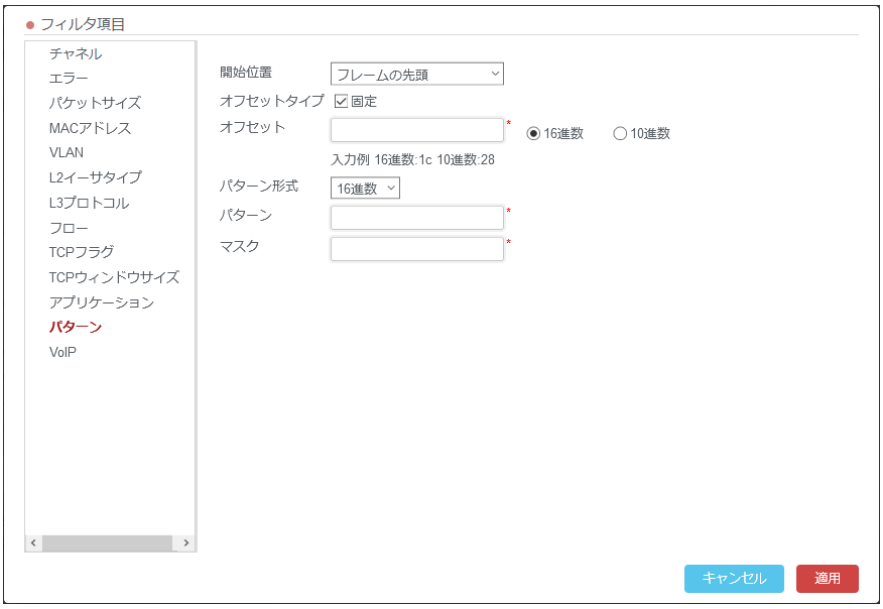


図 107：パターンフィルタの設定画面

設定項目の詳細は、以下の通りです。

項目	説明	
開始場所	パターンの一致を判定する位置を指定する際、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。	
	フレームの先頭	フレームの先頭を起点とします。
	IP ヘッダ	IP ヘッダの先頭を起点とします。
	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(L4 ヘッダの終端)を起点とします。
オフセットタイプ	「固定」にチェックを入れると、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	「開始場所」で指定された位置を起点として、パターンの一致を判定する位置をバイトで指定します。「16 進数」または「10 進数」で選択することができます。	
パターン形式	パターン文字列の表示形式を指定します。 「ASCII」 または 「16 進数」 で選択することができます。	
パターン	パターンを「ASCII」または「16 進数」で指定します。	
マスク	「マスク」のパターンを 16 進数で指定します。 パターン形式が「16 進数」の場合のみ有効で、「ASCII」を指定した場合は選択できません。	

「パターン」と「マスク」の指定方法の具体例は、**6.6. フィルタ共通の定義** を参照ください。

6.5.13. VoIP

SIP、 RTP、RTCP パケットを、設定された発信番号と着信番号でフィルタします。

図 108 : VoIP フィルタの設定画面

項目		説明
発番号/着番号	**国番号**	電話番号の国番号を入力します。 初期値として日本の国番号[+81]が入力されています。
	電話番号	発番号と着番号の電話番号を入力します。電話番号は数字のみ入力可能です。 電話番号を範囲指定する場合は、電話番号の間を"ハイフン(-)"でつなぎます。 （例: "0352687941-0352687990"） 複数の電話番号を指定する場合は、電話番号を"セミコロン(;)"で区切ります。 （例: "0352687941;0352687990;0352688565"） 番号の一部を"*"や"?"で、任意の数字に置き換えることも可能です。 "*"は 1 文字以上の任意の数字にマッチします。番号の先頭または末尾にのみ指定することができます。（例: "090370658*", "*4253"） "?"は任意の 1 文字にマッチします。（例: "09037?6586"） 空欄の場合は全ての電話番号が対象になります。
ENUM/DNS パケットをフィルタする		チェックを入れると、ENUM/DNS パケットをフィルタリングします。 ENUM/DNS パケットと判断されるのは、以下を OR 条件で満たす TCP パケットです。 ●UDP または TCP パケットであり、送信元または送信先のポート番号が、「L4 ポート番号」に登録されている DNS のポート番号と一致 ●IP アドレスが ENUM サーバ (AppWars.lua ファイルに記載) と一致
Diameter パケットをフィルタする		チェックを入れると、Diameter パケットをフィルタリングします。 Diameter パケットと判断されるのは、以下の条件を満たす TCP パケットです。 ●「L4 ポート番号」に登録されている Diameter のポート番号またはポート範囲と、送信元ポートまたは送信先ポートの少なくとも片方が一致

VoIP フィルタの詳細仕様は、SYNESIS の VoIPFilter マニュアルを参照ください。

6.6. フィルタ共通の定義

キャプチャフィルタと保存フィルタ共通の定義について説明します。

6.6.1. 「パターン」と「マスク」の指定方法

「マスク」を 2 進数で表示したときに "1" になる桁のビットが「パターン」と一致するものがフィルタされます。 「マスク」を 2 進数で表示したとき "0" の桁は "don't care" です。
以下に具体的な指定例を挙げました。

例１：バイトパターン”８７”をフィルタする

フィルタするバイトパターン”８７”を「パターン」に入力します。
「マスク」のビットが全て "1" となる 16 進数をパターンの長さと同じ長さで入力します。
指定されたオフセットの位置にあるバイトパターンでフィルタされます。

	16 進数	2 進数
パターン	８７	１０００　０１１１
マスク	ＦＦ	１１１１　１１１１
フィルタ結果	８７	１０００　０１１１

例２：最下位ビットが"1"のパターンをフィルタする

フィルタするビットパターンを 16 進数で「パターン」に入力します。その際、”don’t care”となるビット位置の値は“0”と”1”のどちらで指定しても構いません。以下は、”０”で指定した場合の例です。パターンは、オクテット単位で指定します。

2 進数で「マスク」の最下位のみ "1" で他のビットが“0”となる 16 進数”０１”を入力します。

指定されたオフセットの位置にある最下位ビット”１”のパケットでフィルタされます。

	16 進数	2 進数
パターン	０１	００００　０００１
マスク	０１	００００　０００１
フィルタ結果	—	ｘｘｘｘ　ｘｘｘ１

7.デコード機能

パケットのデコードする機能について説明します。

デコードの表示は、以下２つの方法があります。

- リアルタイムデコード
- トレースからのデコード

7.1. リアルタイムデコード

キャプチャ開始前にキャプチャオプションの**共通 オプション**で リアルタイムデコード機能を有効にすると、１秒間に１パケットのサンプリング周期で自動的にデコードが実行され、その結果が[リアルタイムデコード]タブに表示されます。

「パケット一覧」(下図①)にはキャプチャされたパケットが時刻順に表示されます。

１秒ごとに画面は更新され、キャプチャされた最新のパケットが一番下に追加されていきます。

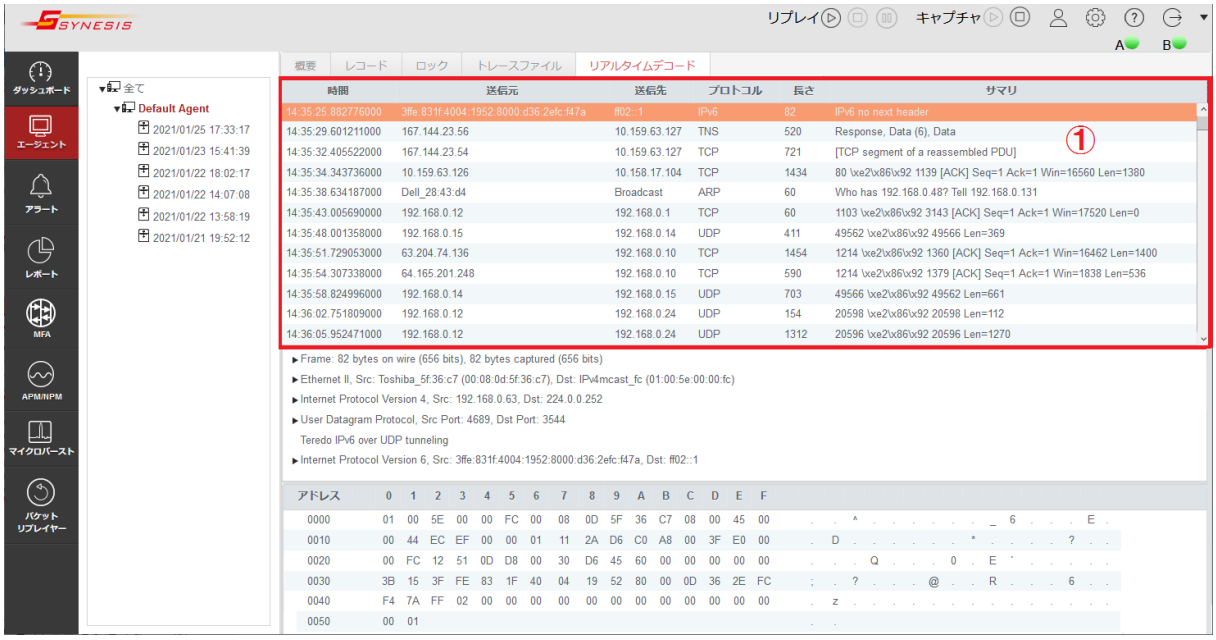


図 109：リアルタイムデコード

[リアルタイムデコード]タブは、リアルタイムデコード機能が有効になっている場合、キャプチャ開始時に自動的に追加されます。

リアルタイムデコードでは、検索、フィルタ、エキスパート情報の表示、トレースの保存機能は利用できません。

[リアルタイムデコード]タブは、キャプチャを停止した時点で自動的に閉じられます。

7.2. トレースファイルからのデコード

トレースファイルに含まれている各パケットに対して、デコードを行います。

以下の画面から実施可能です。

- [エージェント]メニュー>[トレースファイル]タブ>[ビルトインファイル]タブ>「デコード」リンク
- [エージェント]メニュー>[トレースファイル]タブ>[トレースバンカー]タブ>「デコード」リンク
- [MFA]メニュー>[フロービュー]タブ>フローを選択>ラダー上をクリック
- [MFA]メニュー>[MFA ビュー]タブ>ラダー上をクリック
- [MFA]メニュー>[パケットロス]タブ>フローを選択>ラダー上をクリック

7.3. デコード画面の構成

デコード画面は、キャプチャされたパケットが時刻順に表示される「パケット一覧」(下図①)と、ヘッダやレイヤ情報が表示される「パケット詳細」(下図②)、16 進数と ASCII でパケットの中身が表示される「バイト列」 (下図③)の 3 つのペインで構成されます。

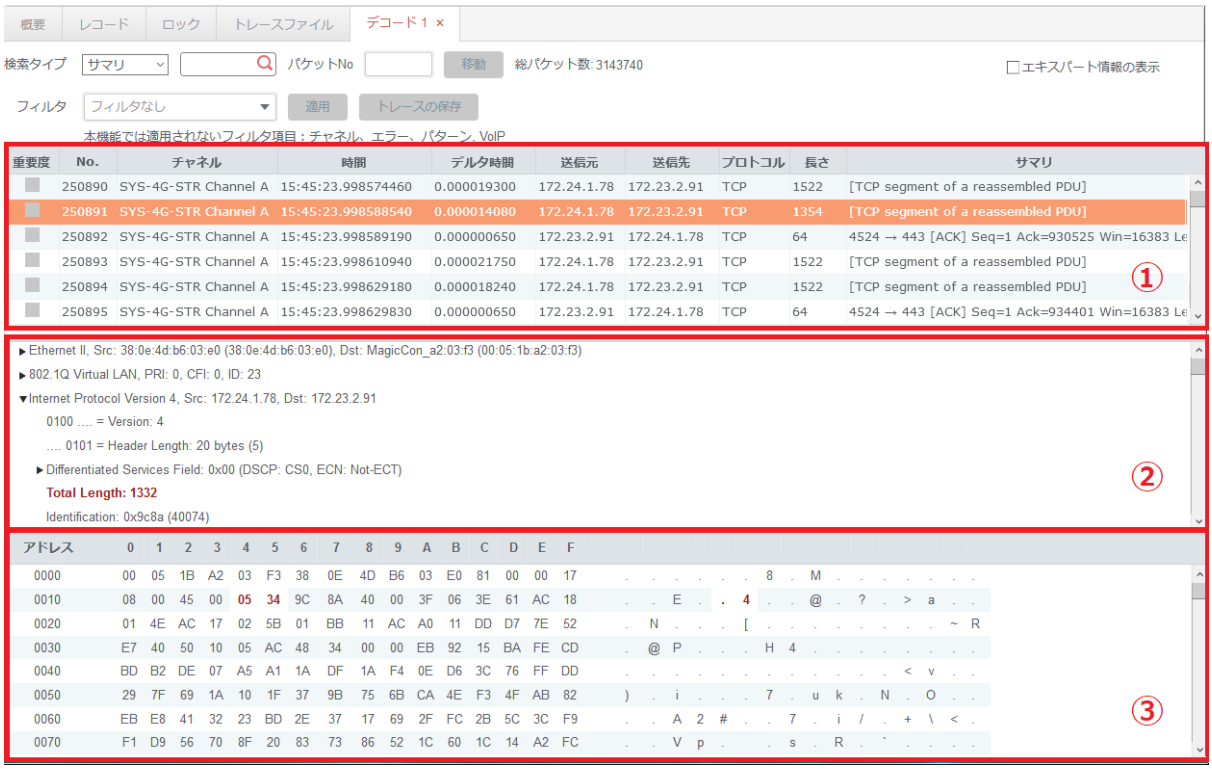


図 110 : デコード画面

3つのペインは互いに連動し、フレームに含まれるプロトコル層を表示します。

「パケット一覧」ペインには、キャプチャされたパケットが各行に列記され、送信元アドレス、送信先アドレス、最上位層プロトコル、プロトコル情報などの概要が表示されます。

「パケット詳細」 ペインには、「パケット一覧」 ペインで選択したパケットの各層が表示されます。これらの層を段階的に開くと、翻訳されたパケット内のさまざまなフィールドを表示できます。

「バイト列」 ペインには、「パケット一覧」 ペインで選択したパケットの 16 進数翻訳と ASCII 翻訳の両方が表示されます。「バイト列」ペインのハイライト表示は、「パケット詳細」ペインでどのプロトコル層が選択されるかに応じて更新されます。16 進数翻訳がどのプロトコル層に対応しているかを正確に把握することができます。

トレースファイルからデコードを行った場合、タブにカーソルを合わせると、デコードしているファイルのファイル名が表示されます。

画面右上の「エキスパート情報の表示」にチェックマークを入れると、「エキスパート情報」が表示されます。エキスパート情報は、パケットの昇順で 1,000 個まで表示されます。

7.3.1. パケット一覧

「パケット一覧」ペインには、キャプチャされたフレームが各行に列記され、送信元アドレス、送信先アドレス、最上位プロトコル、プロトコル情報などの概要が時刻順に表示されます。

重要度	No.	チャネル	時間	デルタ時間	送信元	送信先	プロトコル	長さ	サマリ
	250890	SYS-4G-STR Channel A	15:45:23.998574460	0.000019300	172.24.1.78	172.23.2.91	TCP	1522	[TCP segment of a reassembled PDU]
	250891	SYS-4G-STR Channel A	15:45:23.998588540	0.000014080	172.24.1.78	172.23.2.91	TCP	1354	[TCP segment of a reassembled PDU]
	250892	SYS-4G-STR Channel A	15:45:23.998589190	0.000000650	172.23.2.91	172.24.1.78	TCP	64	4524 → 443 [ACK] Seq=1 Ack=930525 Win=16383 Le
	250893	SYS-4G-STR Channel A	15:45:23.998610940	0.000021750	172.24.1.78	172.23.2.91	TCP	1522	[TCP segment of a reassembled PDU]
	250894	SYS-4G-STR Channel A	15:45:23.998629180	0.000018240	172.24.1.78	172.23.2.91	TCP	1522	[TCP segment of a reassembled PDU]
	250895	SYS-4G-STR Channel A	15:45:23.998629830	0.000000650	172.23.2.91	172.24.1.78	TCP	64	4524 → 443 [ACK] Seq=1 Ack=934401 Win=16383 Le

図 111：パケット一覧

パケット一覧で確認できる項目は、以下の通りです。

項目	説明
重要度	確認されたエラーの重要度です。 詳細は **7.3.6 エキスパート情報**を参照してください。
No	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。 表示フィルタが適用された場合も、この番号は変わりません。
チャネル	キャプチャしたチャネル名の情報です。
時間	そのパケットがキャプチャされた時刻です。
デルタ時間	１つ前のパケットとの時間の差分です。
送信元	パケットの送信元アドレスです。
送信先	パケットの送信先アドレスです。
プロトコル	最上位プロトコルです。
長さ	パケットの長さです。
サマリ	パケット内容の要約です。

7.3.2. パケット詳細

「パケット詳細」では「パケット一覧」で選択したフレーム(前頁図④)のヘッダ情報が表示されます。

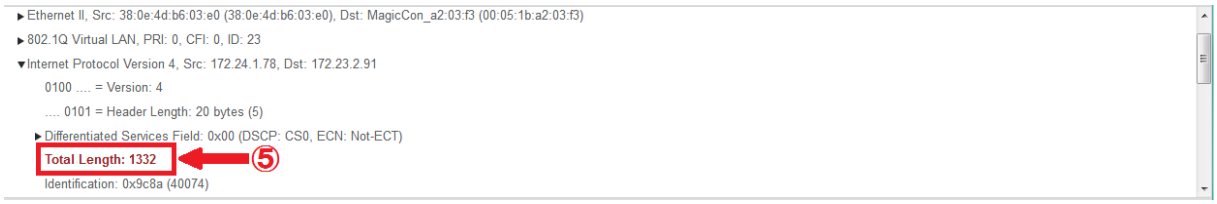


図 112：パケット詳細

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。

7.3.3. バイト列

「バイト列」ペインには、「パケット一覧」ペインで選択したパケット(前頁図④)の中身が 16 進数と ASCII で表示されます。

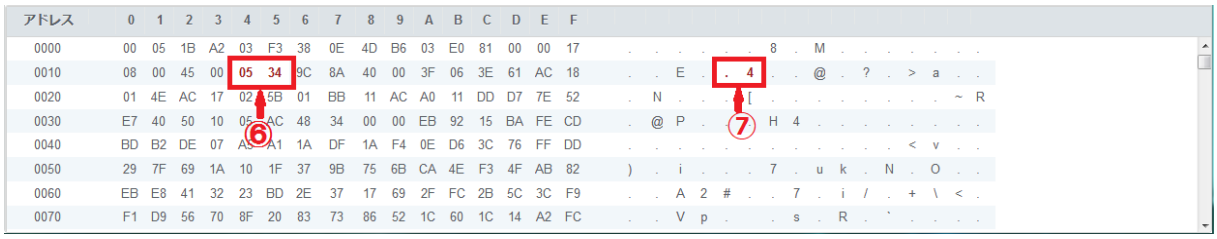


図 113：バイト列

「パケット詳細」でフィールドを選択すると、該当するフィールド部分の 16 進数(上図⑥)と ASCII(上図⑦)がフォーカスされます。

7.3.4. 検索機能

デコードに表示されているパケットは、文字列またはパケット No で検索することが可能です。

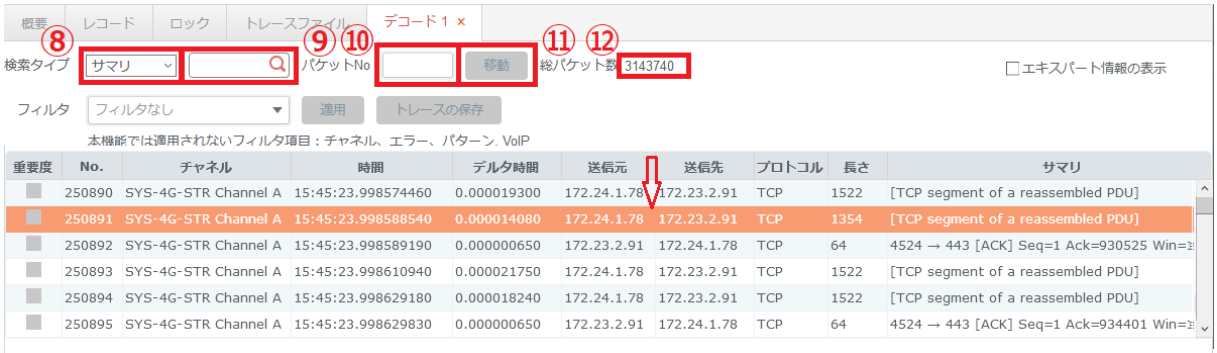


図 114：検索機能

- 文字列の検索

各ペインに含まれる文字列で検索を行うには、検索タイプ(上図⑧)で検索対象を選択し、検索する文字列をテキストボックス(上図⑨)に入力して、「検索」アイコンをクリックしてすると、指定された値の検索が実行されます。

検索は、パケット一覧で選択されているパケット以降で、「検索」アイコンをクリックするごとに条件が一致したパケットを時刻の昇順にフォーカスします。

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	パケット一覧の「サマリ」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 パターンを検索します。 2 バイト以上のパターンを検索する場合、1 バイトごとにスペースを入れる必要があります。
(ASCII)パケットデータ部	パケットデータの ASCII を検索します。

- パケット No 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、時刻の昇順に並べた場合の通し番号です。

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(前頁図 114⑩)に検索対象のパケット No を入力し、「移動」ボタン(前頁図 114⑪)をクリックします。

パケット一覧上のフォーカス(前頁図オレンジ部)が、指定した「パケット No」の行に移動します。

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（前頁図 114⑫)です。

7.3.5. 表示フィルタ

表示されているパケットを絞り込むことができます。

表示フィルタは、保存フィルタと共通で定義されます。

フィルタのテキストボックスの▼アイコン(下図⑬)をクリックすると、設定済みの保存フィルタ定義(下図⑭)が表示されます。

図 115：デコードの表示フィルタ

適用する保存フィルタ定義を選択し、[適用]ボタン(上図⑮)をクリックすると、条件に一致するパケットのみが表示されます。

下記のフィルタは、表示フィルタではサポートしていません。

- **チャネル**
- **エラー**
- **パターン**
- **VoIP**

また、TCP フラグフィルタで複数にチェックを入れた場合、デコードでは AND 条件として適用されます。

選択した保存フィルタするキャンセルする場合は、「フィルタなし」を選択します。

管理者ロールで操作を行っている場合は、保存フィルタを追加・編集することができます。

詳細は、**6.4. 保存フィルタの概要** の章を参照ください。

7.3.6. エキスパート情報

デコード画面右上の「エキスパート情報の表示」にチェックを入れると、エラー情報がリストアップされた「エキスパート情報」画面(下図⑦)が表示されます。

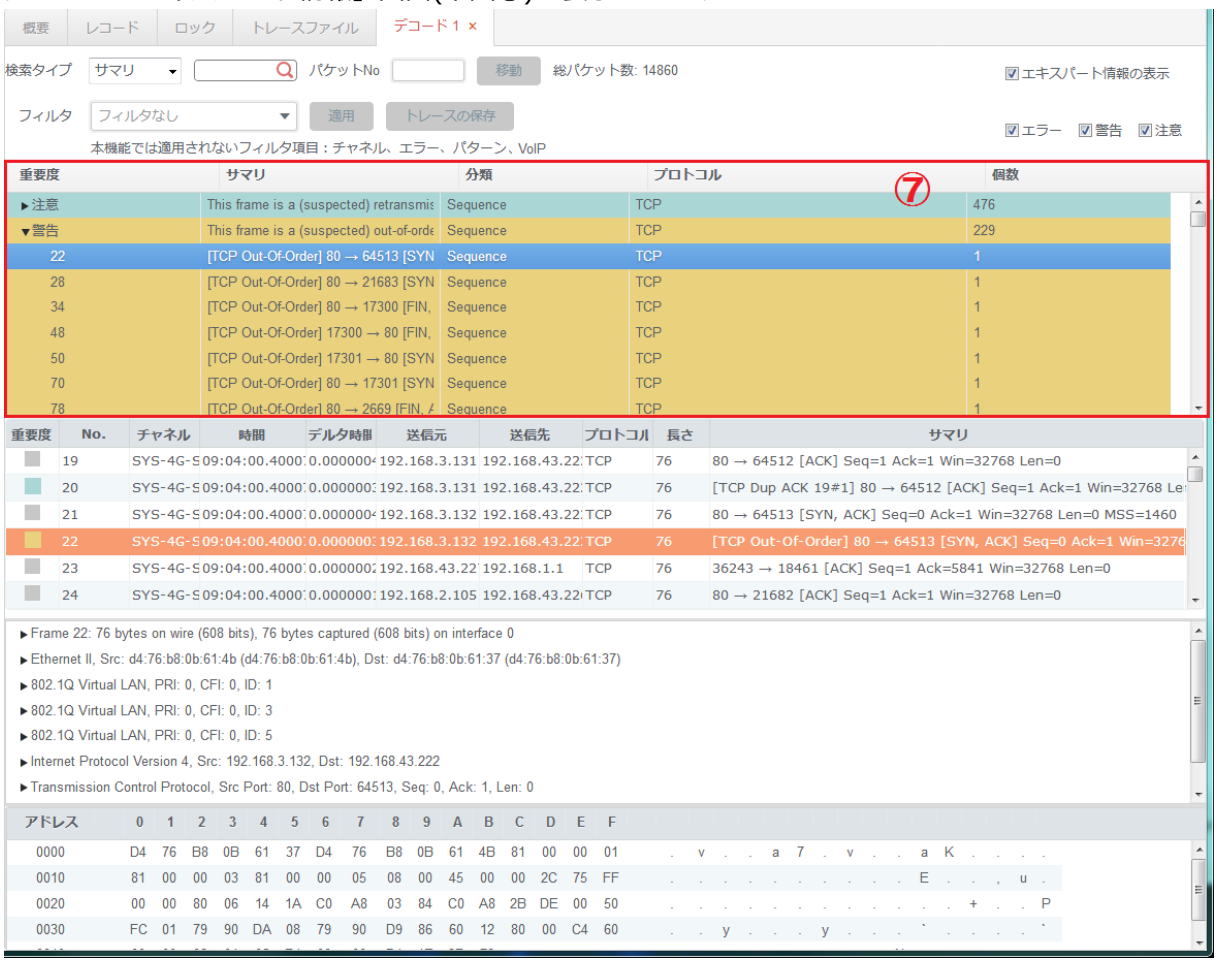


図 116：エキスパート情報

「エキスパート情報」は、重要度によって「エラー」「警告」「注意」に分類されます。

画面右上の「エラー」「警告」「注意」のチェックボックスで、チェックの入ったものだけが「エキスパート情報」に表示されます。

エキスパート情報で確認できる項目は、以下の通りです。

項目	説明
重要度	重要度によって「エラー」「警告」「注意」に分類されます。 「重要度」のノード▶をクリックすると、 その警告に含まれるパケットの情報が個別に表示されます。 パケットを個別に表示した際には、この欄には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が表示されます。
サマリ	確認されたエラーの概要です。
分類	確認されたエラーの種類です。
プロトコル	通信プロトコルです。 そのパケットの最上位のレイヤが表示されます。
個数	重要度ごとのエラー数です。

7.3.7. トレースの保存

[トレース保存]ボタンをクリックすると、現在表示されているパケットをトレースファイルに保存します。

詳細は **5. トレースの保存操作** を参照してください。

7.3.8. Lua プラグインの適用

SYNESIS にインストールされている Wireshark および tshark に対して、任意の Lua プラグインを適用することが可能です。画面上のデコード機能の結果もプラグインが適用された状態で表示されます。

Lua プラグインを有効にした場合は、リアルタイムデコード、トレースファイルからのデコードの両方に適用されます。

適用手順は、以下の通りです。

1) 適用する Lua ファイルを /etc/pvc/wireshark/plugins/ ディレクトリ内に配置します。
2) ブラウザで "https://[SYNESIS IP]/mgmt/" にアクセスし SYNESIS 管理画面を開きます。
   管理画面のユーザ名とパスワードの入力を求められますので、ユーザ名とパスワードを入力します。
3) デコードエンジンを再起動してプラグインを有効化します。
   管理画面内で下から 2 番目にある DEService の "Restart" をクリックします。

8.統計情報

統計情報の画面構成、仕様について説明します。

キャプチャ中は、パケットと同時に 1 秒ごとの統計情報を保存します。

統計情報は、以下の用途で使用します。

- 統計情報のトレンド表示からのトレースの保存操作
- 統計情報の CSV ファイルの作成

統計情報のトレンド表示は、以下の画面よりアクセスが可能です。

- レコード全体のトレンド表示
  - [エージェント]メニュー>各レコードを選択
  - [エージェント]メニュー>[レコード]タブ>各レコードの「名前」をクリック
  - [エージェント]メニュー>[レコード]タブ>各分割レコードの「名前」をクリック
- キャプチャ中のトレンド表示
  - [エージェント]メニュー>[概要]タブ

レコード全体のトレンド表示の操作方法は、次項の **8.1. レコード全体のトレンド表示**を、キャプチャ中のトレンド表示は、**4.6. キャプチャのステータス** を参照してください。

8.1. レコード全体のトレンド表示

統計情報のレコード全体のトレンド表示は、以下のような構成となっています。

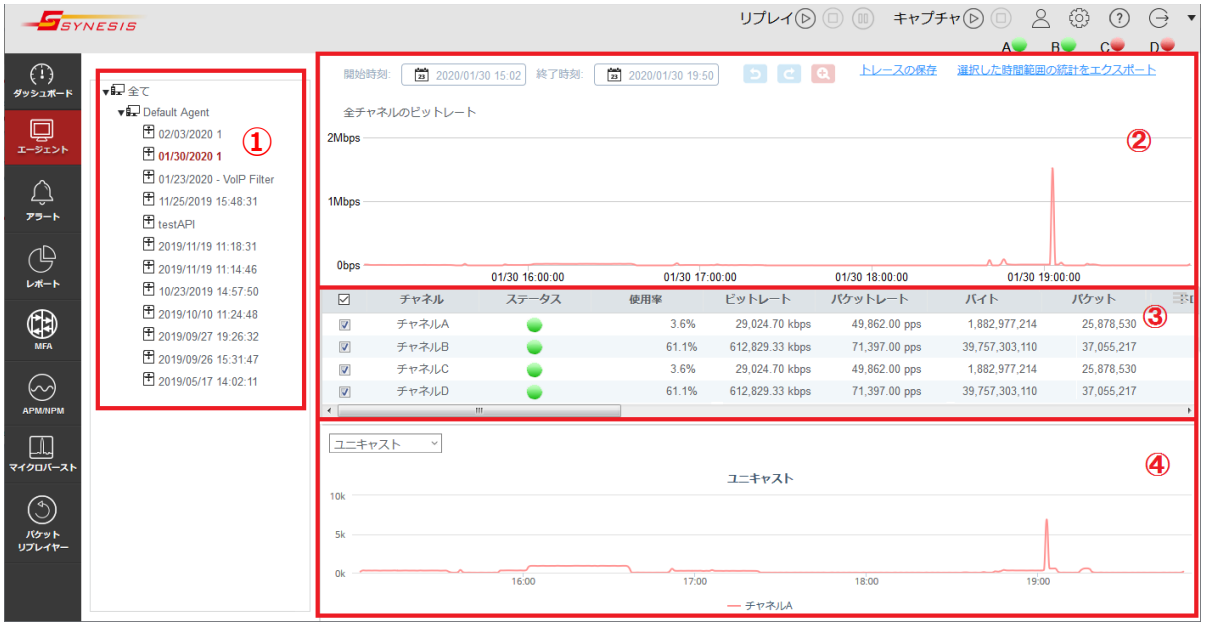


図 117：レコード全体のトレンド表示

選択したレコード(上図①)の情報が、画面の右側に表示されます。

表示される情報は、全チャネルのビットレートの合計値のトレンドグラフ(上図②)、チャネルごとの統計値のテーブル(上図③)、 チャネルごとのトレンドグラフ(上図④)です。

8.1.1. チャ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、全チャネルの合計のビットレートがトレンドグラフとして表示されます。

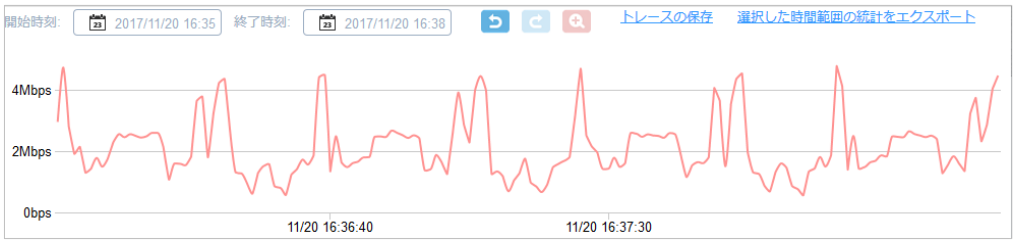


図 118：チャネルの合計値のトレンドグラフ

8.1.2. チャネルごとの統計値

キャプチャレコード・ワークスペースの 2 段目にはチャネルごとのキャプチャの統計情報が表示されます。

チャネル	ステータス	使用率	ビットレート	パケットレート	バイト	パケット	ドロップ	ブロードキャスト	マルチキャスト	ユニキャスト	CRC	フラグメント	ジャバー	オーバーサイズ	ラント	アダプタ
チャネルA		79.4%	780,370.28 kbps	89,907.00 pps	38,433,236,530	35,423,656	0	0	0	35,423,656	0	0	0	0	0	Synesis Virtual Adapter NT 10Gbps x 4
チャネルB		5.2%	42,577.55 kbps	62,789.00 pps	2,096,944,569	24,739,197	0	0	0	24,739,197	0	0	0	0	0	Synesis Virtual Adapter NT 10Gbps x 4
チャネルC		0.0%	0.00 kbps	0.00 pps	0	0	0	0	0	0	0	0	0	0	0	Synesis Virtual Adapter NT 10Gbps x 4
チャネルD		0.0%	0.00 kbps	0.00 pps	0	0	0	0	0	0	0	0	0	0	0	Synesis Virtual Adapter NT 10Gbps x 4

図 119：統計情報のテーブル

テーブルに記載される項目は、以下の通りです。

- チャネル
- ステータス
- 使用率
- ビットレート
- パケットレート
- バイト
- パケット
- ドロップ
- ブロードキャスト
- マルチキャスト
- ユニキャスト
- CRC
- フラグメント
- ジャバー
- オーバーサイズ
- ラント
- アダプタ

エラーパケットの内、フラグメントとラントはモデルによっては統計が取れません。その場合の統計値は「N/A」と表示されます。

対応モデルは諸元一覧をご確認ください。

詳細は、**8.3. 統計値の定義** をご参照ください。

8.1.3. チャネルごとのトレンドグラフ

画面の一番下に表示されているのは、チャネルごとのトレンドグラフです。

グラフ左上のドロップダウン・リスト(下図⑤)で、どの項目のグラフを表示するかを選択することができます。

グラフ下部に表示されたチャネル名(下図⑥)などの要素をクリックすると、チャ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。

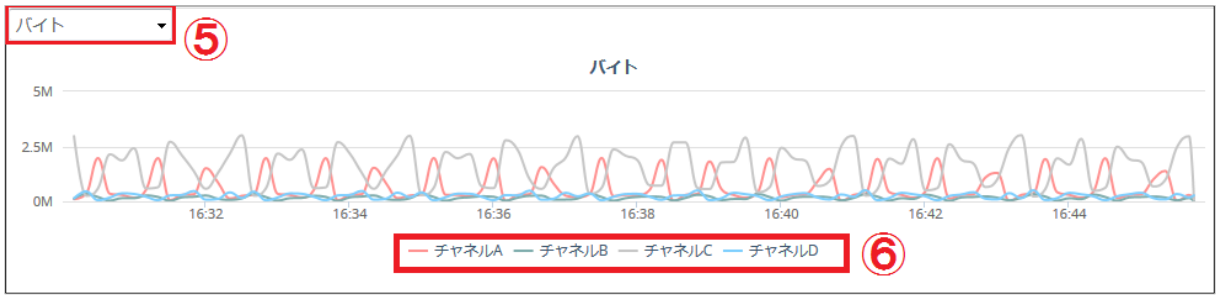


図 120：チャネルごとのトレンドグラフ

選択可能な項目は、以下の通りです。

- 使用率
- ビットレート
- バイト
- パケット
- ドロップ
- ブロードキャスト
- マルチキャスト
- ユニキャスト
- CRC
- フラグメント
- ジャバー
- オーバーサイズ

エラーパケットの内、フラグメントとラントはモデルによっては統計が取れません。その場合の統計値は「N/A」と表示されます。

対応モデルは諸元一覧をご確認ください。

詳細は、**8.3. 統計値の定義**をご参照ください。

8.1.4.　期間を指定しての拡大表示

表示する期間を指定する場合は、トレンドグラフ上をドラッグもしくはカレンダー表示で行います。

「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」は、グラフで指定した期間のデータが対象となります。

画面の操作方法は、**2.6.5. グラフ画面での期間指定** を参照ください。

それぞれの機能は、以下の通りです。

項目	説明
開始時刻 **/終了時刻**	選択されたレコードの開始時刻と終了時刻です。 開始時刻と終了時刻で時間範囲を指定し、拡大表示させることが可能です。 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。 キャプチャ中の場合は、最新の更新時刻が終了時間になります。 表示を更新するする場合は、ブラウザを更新してください。
拡大	レコードの期間の一部をドラッグで選択し、拡大表示させることができます。 詳細は、**2.6.5. グラフ画面での期間指定** を参照してください。
元に戻す **やり直す**	元に戻す」アイコン をクリックすると、直前に行った操作が取り消されます。「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」操作がキャンセルされます。
トレースの保存	表示されている時間範囲のパケットをトレースファイルに保存します。 詳細は **5. トレースの保存操作** を参照してください。
選択した時間範囲の統計をエクスポート	表示されている時間範囲の統計値の CSV ファイルが作成されます。 詳細は統計値の CSV ファイルの作成手順を参照してください。

8.1.5.　トレンド表示からのトレースの保存

時間範囲を指定して、レコードの全体または一部をトレースファイルとして保存できます。 ツールバーの下にある「トレースの保存」リンク(下図赤枠)をクリックします。

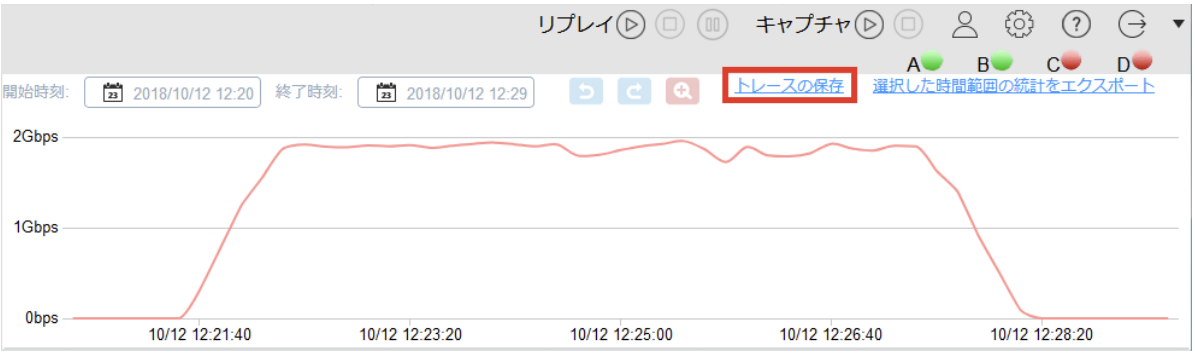


図 121：トレンド表示

本画面からトレースの保存を実施した場合は、グラフで表示されている時間範囲が、トレース保存時の開始時刻・終了時刻に反映されます。

トレース保存画面における操作方法は、**5. トレースの保存操作** を参照ください。

8.2. 統計のエクスポート

統計値は、CSV ファイルとして作成、ブラウザからダウンロードが可能です。

以下の画面から行えます。

- [エージェント]メニュー>[レコード]タブ>各レコードまたは各分割レコード
- [エージェント]メニュー>エージェント・ペイン>各レコード
- [レポート]メニュー>[レポートプラン]タブ> レポートテンプレートで「Statistics」を選択

8.2.1. 統計値の CSV ファイルの作成手順

統計値の CSV ファイルの作成は、画面により作成手順や仕様が異なります。

CSV ファイルに含まれる統計値の項目については **8.3. 統計値の定義**を参照してください。

- [レコード]タブからの作成手順

1) 該当のレコードまたは分割レコードにチェックを入れ(下図①)、画面上部の[統計のエクスポート]ボタン(下図②)をクリックします。レコードの開始時刻から停止時刻までの CSV ファイルが作成されます。

図 122 :「統計のエクスポート」ボタン

2) ファイルの作成が完了したら、レコード一覧の「統計データ」欄の表示が「未エクスポート」から「ダウンロード」(下図③)に変わります。

図 123 : 統計データの「ダウンロード」リンク

3) 「ダウンロード」リンクをクリックすると、ダウンロードダイアログが表示され、ダウンロードが可能になります。

レコードを削除すると、統計値の CSV ファイルも同時に削除されます。

● エージェント・ペインからの作成手順

1) ツールバーの下にある「選択した時間範囲の統計をエクスポート」のリンク(下図赤枠)をクリックします。

図 124 :「選択した時間範囲の統計をエクスポート」リンク

2) 下図の「統計のエクスポート」ダイアログが表示されます。期間を指定します。

図 125 :「統計のエクスポート」ダイアログ

テキストボックスに入力するか、時刻指定の アイコンをクリックして行います。

期間の初期値は、以下の通りです。

条件	開始時刻	終了時刻
拡大表示を行っているレコード	拡大表示の開始時刻	拡大表示の終了時刻
キャプチャを停止したレコード	レコードの開始時刻	レコードの終了時刻
キャプチャ中のレコード	レコードの開始時刻	現在時刻

3) [エクスポート]ボタンをクリックします。

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。

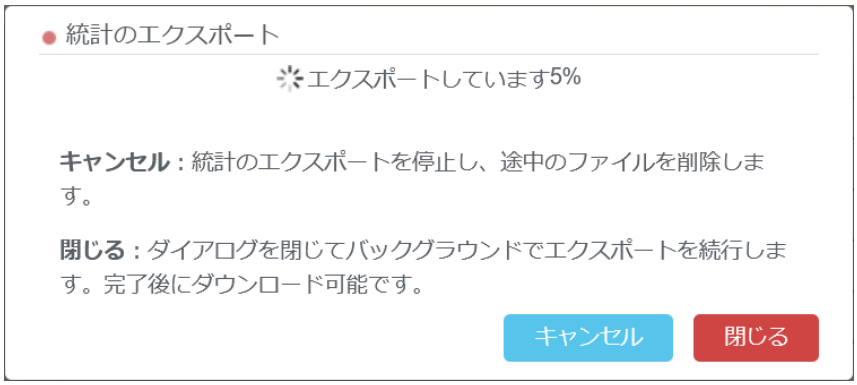


図 126 :「統計のエクスポート」ダイアログ

[閉じる]をクリックすると操作画面に戻りますが、統計値の CSV ファイルの作成はバックグラウンドで続行されます。

[キャンセル]をクリックすると、エクスポートが中止され、作成途中のファイルも破棄されます。

4) 統計値の CSV ファイルが完成すると、ダイアログの表示が「ダウンロード」に変わります。「ダウンロード」リンクをクリックすると、ダウンロードダイアログが表示され、ダウンロードが可能になります。

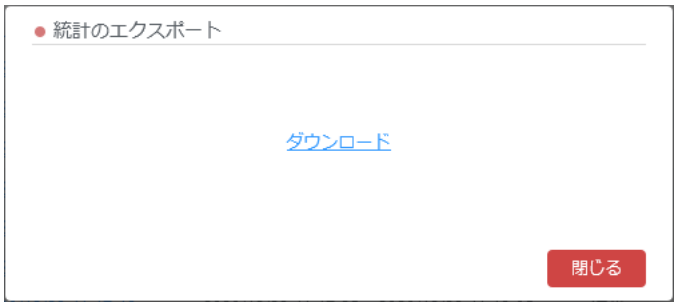


図 127 :「ダウンロード」リンク表示

5) [閉じる]をクリックして「統計のエクスポート」ダイアログを閉じると、作成した統計値の CSV ファイルはダウンロードできなくなります。

作成した統計値の CSV ファイルは、SYNESIS 内に保存されません。そのため、「統計のエクスポート」ダイアログを閉じると、CSV ファイルはダウンロードできなくなります。誤ってダイアログを閉じてしまった場合には、再度時間範囲を指定して、統計値の CSV ファイルを作成してください。

統計値をエクスポートする期間として、レコードの開始時刻と停止時刻を指定した場合のみ、作成した CSV ファイルは、SYNESIS 内に保存されます。保存された CSV ファイルは [レコード]タブ>各レコードよりダウンロードが可能です。

- レポートプランからの作成手順

「レポート」メニューから、定期的に統計情報の CSV ファイルを出力させることが可能です。
詳細は、**レポート**の **12.2.3. 統計情報レポートの CSV ファイルで出力** を参照してください。

8.2.2. 統計のエクスポートに関する制限事項

- 統計のエクスポート機能で、ユニキャストパケットの総和が実際と合わない場合があります。この現象はブロードキャストパケットおよびマルチキャストパケットのみキャプチャされ、ユニキャストパケットがキャプチャされない場合に発生します。
- 各チャネルのリンク状況を確認できるモデルで、キャプチャ開始直後の統計情報のステータスが "unknown"と表示されることがあります。

8.3. 統計値の定義

キャプチャの統計値の定義は、以下の通りです。

表示・保存される項目は、画面により異なりますので、詳細は各章の記載を参照してください。

項目	説明
タイムスタンプ	各項目はタイムスタンプの 1 秒前からタイムスタンプまでの統計値です。表示形式は yyyy/mm/dd hh:mm:ss です。 例えば、00 時 00 分 00 秒のデータは、23 時 59 分 59 秒以降から 00 時 00 分 00 秒になる直前までの 1 秒間の統計値になります。
チャネル	キャプチャ可能なチャネル情報です。
ステータス	Rx のリンクアップ状態を示します。 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。 対応モデルかどうかは、諸元一覧を参照してください。
使用率	回線使用率を%で示した値です。 以下の例は、ラインスピードを 1Gbps として計算しています。 $$\text{使用率}(t) = \frac{\{\text{パケットレート}(t) * (8+12)\} * 8 + \{\text{ビットレート}(t)\}}{10^9}$$ 上記の計算式では、8 はプリアンブル、12 はフレーム間の最小ギャップを意味します。 ラインスピードは任意の値に変更可能です。
ビットレート	1 秒間に受信したビット数です。 以下の計算式で算出しています。 $$\text{ビットレート}(t) = \frac{\{\text{バイト}(t) - \text{バイト}(t-\Delta t)\} * 8}{\Delta t}$$
パケットレート	1 秒間に受信したパケット数です。 以下の式で算出しています。 $$\text{パケットレート}(t) = \frac{\{\text{パケット}(t) - \text{パケット}(t-\Delta t)\}}{\Delta t}$$
バイト	バイト数です。 バイト数には、イーサネットヘッダの 4 バイトの FCS が含まれます。
パケット	パケット(フレーム)数です。
ドロップ	ディスク書き込みにディスク書き込み時にドロップしたフレーム数です。

ブロードキャスト	L2 エラーを含まないブロードキャストフレーム数です。 送信先 MAC アドレスが FF:FF:FF:FF:FF:FF のフレームの場合、ブロードキャストと判定します。
マルチキャスト	L2 エラーを含まないマルチキャストフレーム数です。 送信先 MAC アドレスの最初のバイトの最下位ビットは 1 で、このバイトの残りのビットはすべて 0 の場合、マルチキャストと判定します。
ユニキャスト	L2 エラーを含まないユニキャストフレーム数です。ブロードキャスト、マルチキャスト以外のフレーム数です。
CRC	CRC エラーのフレーム数です。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 エラーを伴う 64 バイト未満のフレーム数です。
ジャバー	CRC エラーを伴う 9019 バイト以上のフレーム数です。 10,000 バイトにスライスされたフレームも含まれます。
オーバーサイズ	CRC エラーを伴わない 9019 バイト以上フレーム数です。
ラント	CRC エラーを伴わない 64 バイト未満のフレーム数です。
アダプタ	キャプチャ時に選択されたアダプタです。

キャプチャフィルタ、パケット重複除去機能で保存対象外となったフレームも統計値の値に含みます。

10,001 バイト以上のフレームは、10,000 バイトにスライスされます。

表中の L2 エラーは、CRC、フラグメント、ジャバー、オーバーサイズ及びラントを指します。

フラグメントとラントの統計はモデルにより対応していません。未対応の場合、統計値は「N/A」と表示されます。

対応モデルは、諸元一覧を参照してください。

9.ロック機能

ロック機能は、キャプチャしたパケットが上書きまたは削除されないよう保護することです。ロックは、レコード単位、または期間を指定して設定することが可能です。

ロックは、以下２つのタイミングで設定が可能です。

1. キャプチャオプションのロックトリガで設定する自動ロック
2. [レコード]タブ、[ロック]タブで設定する手動ロック

ロックは、パケットデータ領域全体の 80%まで設定することができます。ロック領域が 80%を超過すると、自動、手動ともにロックは設定できません。

不要となったロックは、手動で解除することが可能です。ロックを解除することにより、ロック可能な領域を増やすことができます。

ロック機能の種類による違いや設定方法について説明します。

9.1. 手動ロック

手動ロックは、既にキャプチャされたパケットにロックを設定する機能です。新たなキャプチャ開始によりパケットが上書きされないよう、保護することができます。

[レコード]タブ、または[ロック]タブからレコード単位または期間を指定して、ロックを設定できます。

ロックされたレコードは、レコードリストの「ステータス」欄が「ロック期間あり」に変わります。**ロックタブの構成**にも情報が追加されます。

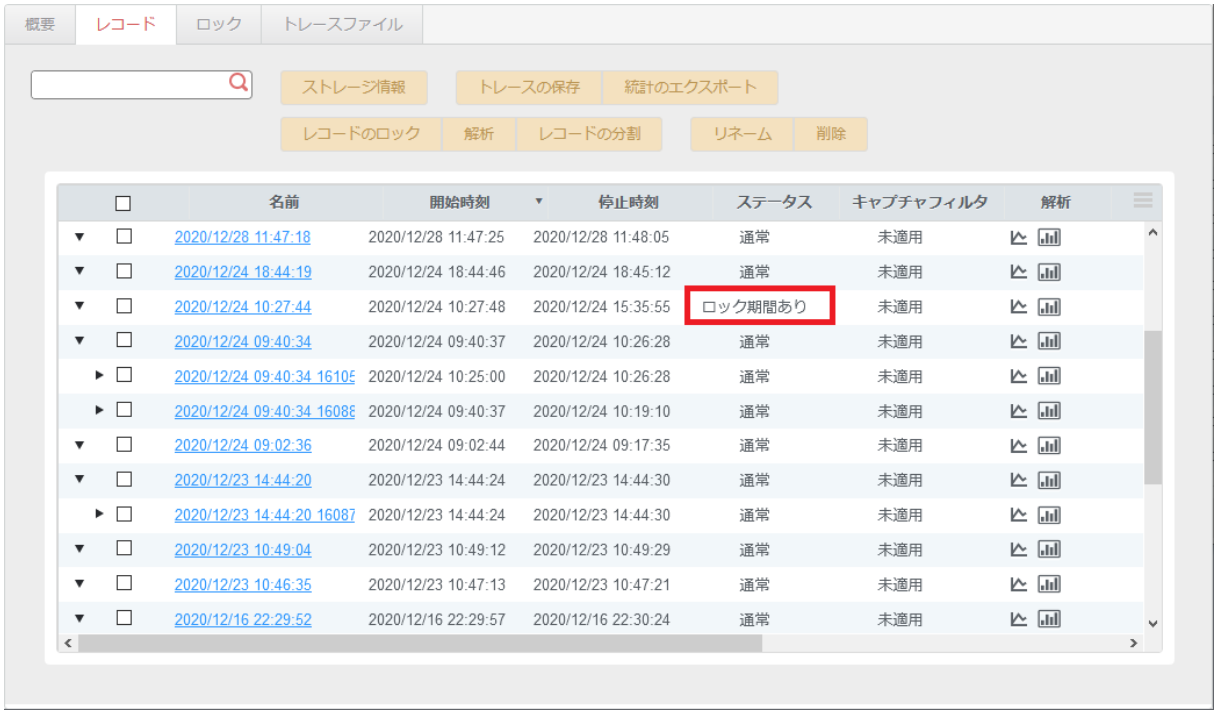


図 128：ロック期間あり

9.1.1. レコード単位のロック設定

レコード全体をロックする場合は、[エージェント]メニュー>[レコード]タブより、該当のレコードにチェックを付け(下図①)、「レコードのロック」ボタン(下図②)をクリックします。

キャプチャが停止しているレコードは、レコード全体がロックされます。

キャプチャ中のレコードは、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刻までの期間でロックされます。

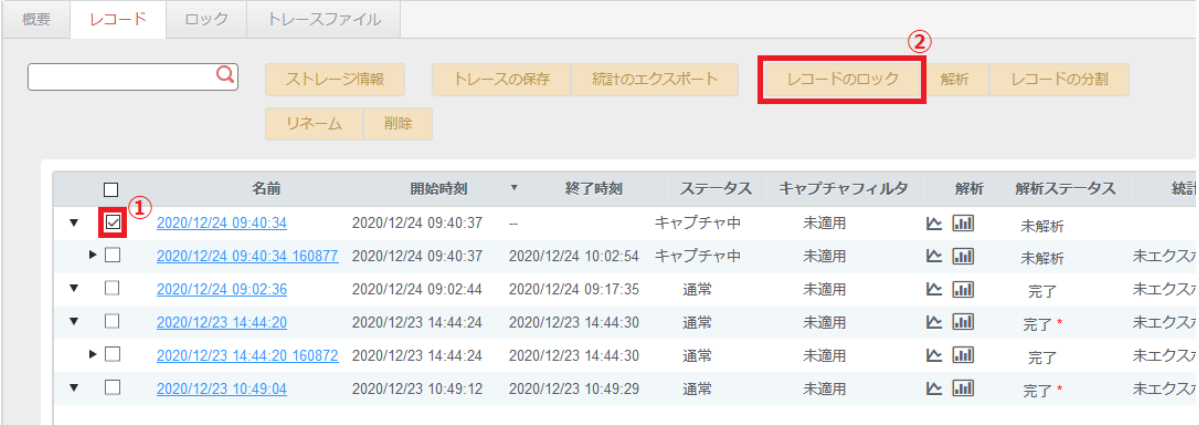


図 129：レコード単位のロック設定

9.1.2. 期間指定のロック設定

期間指定のロックを設定する場合は、[エージェント]メニュー>[ロック]タブ>[新規]ボタンをクリックします。

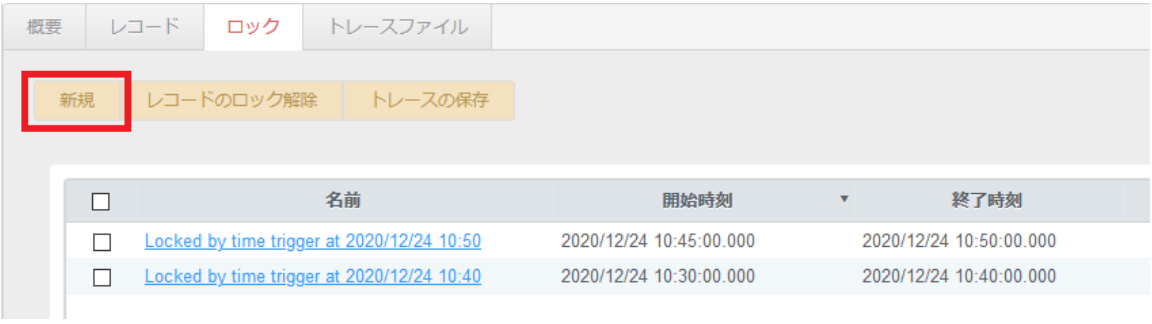


図 130：ロックタブの新規ボタン

以下の「新規」ウィンドウが表示されます。

図 131：ロック設定の新規ウィンドウ

「名前」と「ロック期間」を指定して、[適用]ボタンをクリックします。
指定した期間でロックが設定され、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	ロックの名前です。
ロック期間	ロックする期間です。 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」は開始時刻と終了時刻で指定します。 「センタースパン」は期間の中央の時刻を指定して、その前後の期間(時/分/秒/ミリ秒)で指定します。

「センタースパン」を選択すると、以下のような画面が表示されます。

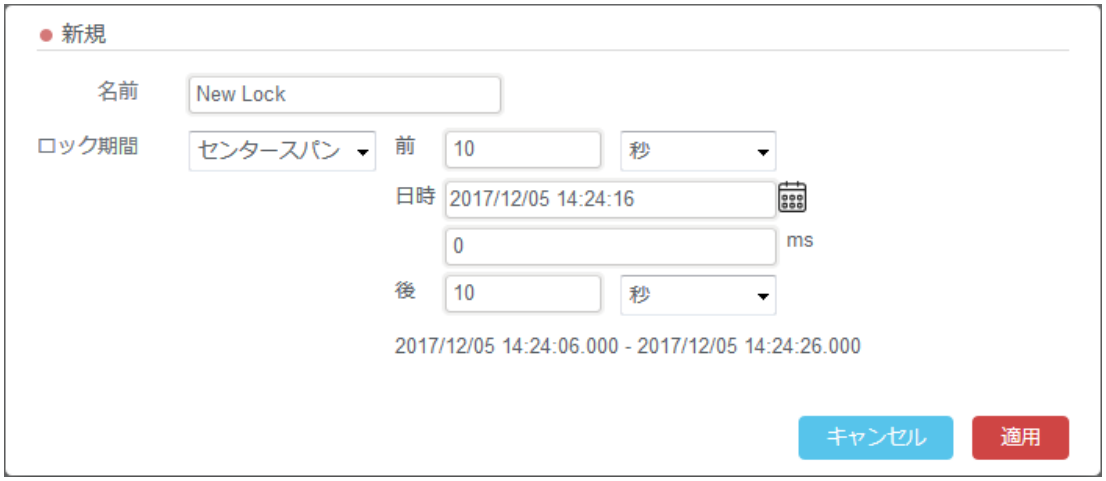


図 132：「センタースパン」モード

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

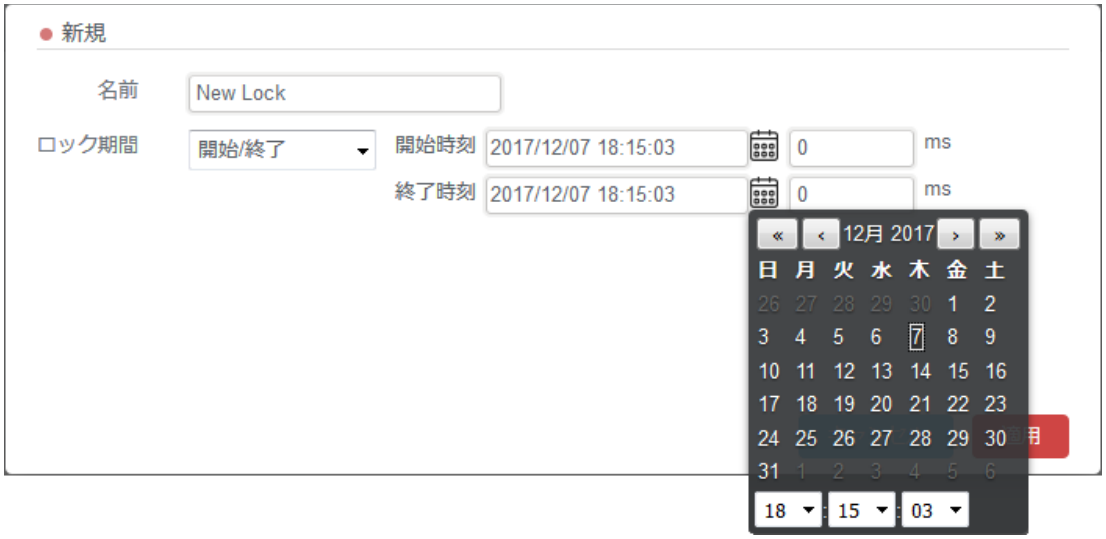


図 133：期間指定のカレンダー表示

カレンダーで日付を指定し、下の時計で時間を指定します。
ミリ秒単位でロック期間を指定する場合は、ミリ秒の部分を手入力します。

9.2. 自動ロック

自動ロックは、キャプチャ中にパケットが上書きされないように予め上書き禁止の設定を行う機能です。自動ロックは、キャプチャオプションのロックトリガで設定します。

ロックトリガを有効にしてキャプチャを開始すると、指定された条件のパケットは、自動的にロックされ、重要なパケットを保護することができます。

図 134：ロックトリガオプション画面

ロックトリガの有効/無効は、上部の「ロックトリガを有効にする」のチェックボックスで設定します。有効にすると、トリガ設定条件を入力できます。

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をロックします。
SNMP トラップトリガ	設定条件に合致した 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します。

9.2.1. 時間トリガ

時間トリガを有効にするためには、トリガボックスに条件を作成します。

時間トリガの条件を作成する場合は、+アイコンをクリックします。

以下の「期間の設定」画面が表示されますので、開始と終了の時間を入力します。

図 135：「期間の設定」画面

登録済の時間トリガの条件を編集する場合は、該当する条件のリンク部分をクリックして定義を編集します。

時間トリガの条件を削除する場合は、該当の条件のチェックボックスにチェックを入れ、 アイコンをクリックします。

リピートトリガ： チェックを入れた場合、時間トリガの条件が毎回有効になります。
チェックが外れている場合は、時間トリガは 1 回に限り有効となります。複数の時間トリガが設定されている場合は、それぞれの設定において 1 回に限り有効となります。

9.2.2. SNMP トラップトリガ

SNMP トラップトリガの有効/無効は、「SNMP トラップトリガを有効にする」のチェックボックスで設定します。

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。SYNESIS で利用しているポートは指定しないでください。 指定されたポートは、SYNESIS の Firewall にて通信を許可する必要があります。 設定方法については、管理者マニュアルをご覧ください。
ロック開始時間	SNMP トラップを受信してから遡ってロック期間が開始するまでの秒数を指定します。
ロック終了時間	SNMP トラップを受信してからロック期間が終了するまでの秒数を指定します。

9.3. ロックタブの構成

ロックタブでは、キャプチャデータのロック状況を確認できます。

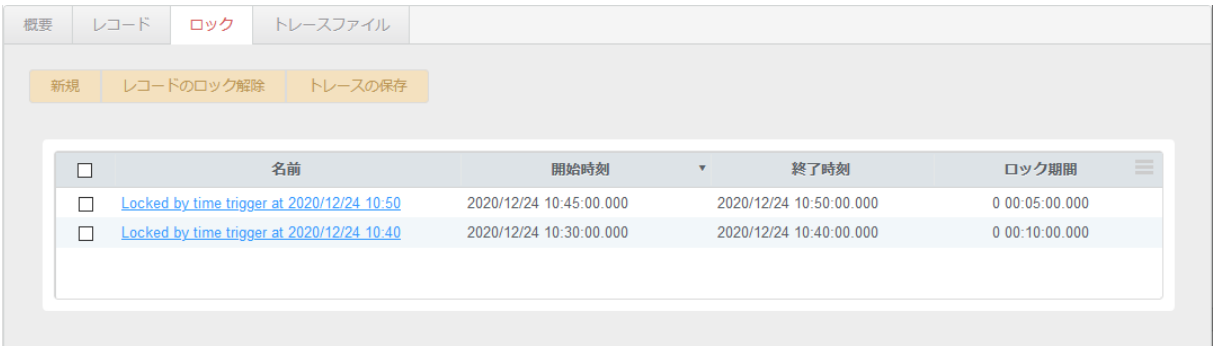


図 136：ロックタブ

ロックの作成・解除や、ロック期間のキャプチャデータをトレースファイルに保存することが可能です。

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	ロックされたレコードの名前です。
開始時刻	ロックの開始時刻です。
終了時刻	ロックの終了時刻です。
ロック期間	ロックの開始時刻から終了時刻までの期間です。

9.3.1. レコードのロック解除

ロックを解除する場合は、該当するロック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ます。

選択したキャプチャデータのロックが解除されます。

9.3.2. トレースの保存

ロックされているデータのトレースファイルに保存することができます。

該当するロック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ます。「トレース保存」ダイアログが表示され、その期間のキャプチャデータをトレースファイルに保存することができます。

詳細は **5. トレースの保存操作** を参照してください。

9.3.3. ロック名の変更

ロック名は変更することができます。

ロック名を変更する場合は、該当のロックの「名前」をクリックします。

テキストボックスが表示され、ロック名を変更することができます。

10.解析機能

解析機能は、キャプチャした大量なパケットから通信の動向を把握することができる機能です。解析ジュールごとの機能、解析の実行方法について、説明します。

10.1.解析機能の概要

キャプチャされたパケットの「解析」を実行することにより、キャプチャしたパケットをデータベースにエクスポートします。それにより、通信イベントの閲覧や関連するパケットの抽出が可能になります。

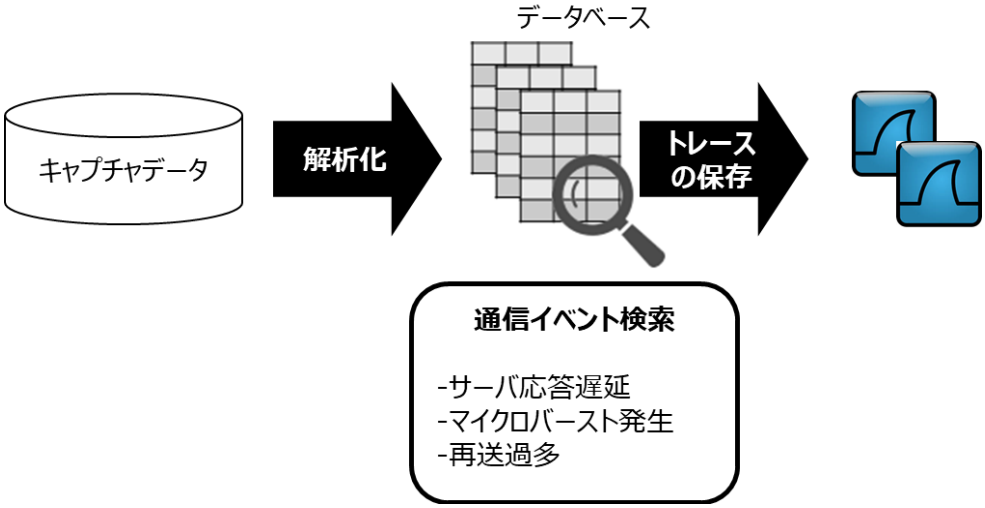


図 137：解析とデータの抽出

解析対象データソースは、レコードに対してのみで、トレースファイルからは実行できません。

解析できるモジュール、機能、確認できる画面は、以下の通りです。

解析モジュール	機能	画面
APM 解析	TCP フローごとにコネクションの各段階で要している時間を表示します。フローのどの段階にボトルネックがあるかを確認できます。	・ダッシュボード ・アラート ・レポート ・APM/NPM
NPM 解析	TCP/UDP フローの IP ペアをホスト単位で KPI を表示します。双方向通信であるフローをそれぞれの方向に対しての通信量とフローの通信状況を把握することができます。	
L2/L3 プロトコル	イーサタイプ、プロトコル番号ごとのパケット数、バイト数を確認できます。	・ダッシュボード ・アラート ・レポート
マイクロバースト	瞬間的にトラフィックが集中するマイクロバーストの発生状況を検出できます。	・マイクロバースト
ARP	ARP パケットの大量発生を検出することができます。	・アラート

ダッシュボード、**アラート機能と通知**、**レポート**の機能は各章を参照ください。

10.1.1. 解析を実行するタイミング

解析を実行するタイミングは、以下２通りあります。

- リアルタイム解析：過去１分間のキャプチャ中のパケットをデータベースにエクスポート
- ポスト解析　　：キャプチャが完了したレコードを手動でデータベースにエクスポート

リアルタイム解析は、キャプチャを開始する前に設定を行う必要があります。

ポスト解析は、解析を実行する前に設定を行う必要があります。

ポスト解析は、対象となるレコードのキャプチャが完了していても、キャプチャ中は解析を実行できません。解析を実行するためには、キャプチャを停止する必要があります。

10.1.2. 解析前に必要な設定項目

モジュール別に以下の通解析を実行する前に必要な設定項目は、以下の通りです。

モジュール	事前に必要な設定項目
共通	[構成]メニュー>「解析」
APM/NPM	[構成]メニュー>「サイト」 [構成]メニュー>「サーバグループ」 [構成]メニュー>「プロトコル」 [構成]メニュー>「アプリケーショングループ」 [構成]メニュー>「プロトコル」
L2/L3 プロトコル	[構成]メニュー>「プロトコル」
マイクロバースト	[構成]メニュー>「マイクロバースト」

詳細は、解析に関する設定項目と仕様を参照ください。

10.1.3. 解析実行手順

- リアルタイム解析

キャプチャを開始する前に、解析に関する設定項目を完了する必要があります。

「キャプチャの開始」ダイアログの[詳細オプション]リンクをクリックし、「キャプチャの自動解析」の項目にチェックをします。

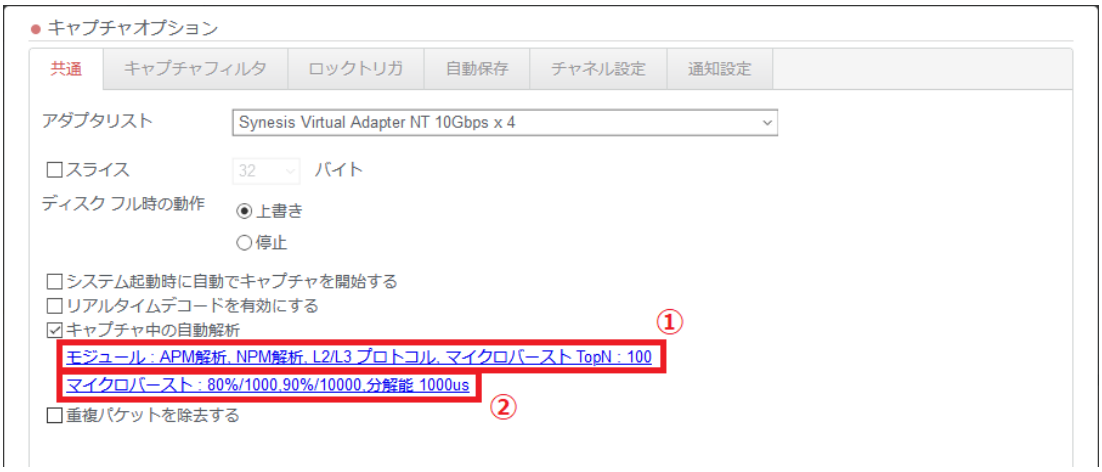


図 138：キャプチャの自動解析

「オプション」ボタンをクリックしても、同様の操作が行えます。

「キャプチャの自動解析」の項目の下には、その時点で選択されているモジュールが表示されます。「マイクロバースト」を有効にした場合、マイクロバーストのリンク(前頁図②)が表示され、設定されている閾値が確認できます。

内容を変更する場合は、モジュール表示のリンク(前頁図①)をクリックします。

設定画面が開かれますので、設定が完了したら、[適用]ボタンをクリックし設定を保存します。

その後、キャプチャを開始すると、リアルタイム解析が実施されます。

詳細は、**4.4.1. 共通 オプション** を参照してください。

- ポスト解析

解析を実行する前に、解析前に必要な設定項目を行う必要があります。

[エージェント]メニュー>[レコード]タブ>該当するレコードにチェックを入れ(下図①)、[解析]ボタン(下図②)をクリックします。解析のステータスが「完了」と表示されたら、解析は完了です。

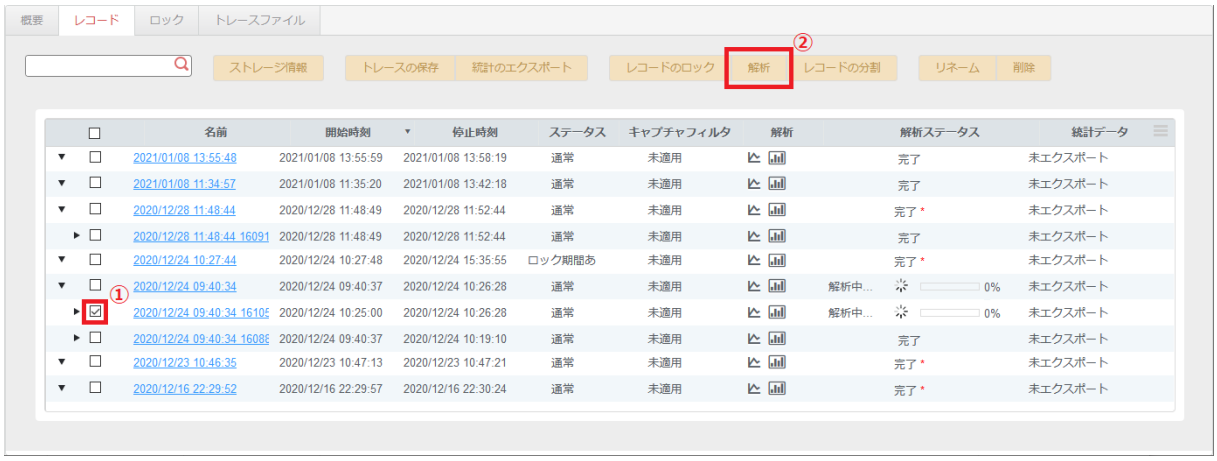


図 139：ポスト解析の実行

解析を実行するためには、キャプチャを停止する必要があります。

10.2. APM/NPM 解析

APM/NPM 解析は、キャプチャしたデータをフローという単位で KPI を表示します。フローとは、IP アドレスおよび TCP/UDP ポート番号の送受信ペアを指します。

APM/NPM の解析結果は、[APM/NPM]メニューより閲覧できます。

APM/NPM 解析は、以下の特長をもちます。

- APM 解析

TCP フローごとにコネクションの各段階で要している時間を表示します。フローのどの段階にボトルネックがあるかを確認できます。フローのリスト表示は、送信元をクライアントとし、送信先をサーバとして扱います。

- NPM 解析

双方向通信であるフローを、それぞれの方向(ホスト 1、ホスト 2)に対しての通信量とフローの通信状況を把握することができます。

10.2.1.　APM/NPM の画面構成

[APM/NPM]メニュー>左上の「開始時刻」「終了時刻」で表示されている期間のフロー情報が、ワークスペース上に表示されます。

検索実行後の画面構成は、以下の通りです。

- ペイン (左側)：項目の TOPN が KPI 順に選択した範囲で表示
- ワークスペース(右側)：ペインで選択されている項目のトレンドグラフ(下図①)とフローテーブル(下図②)が表示

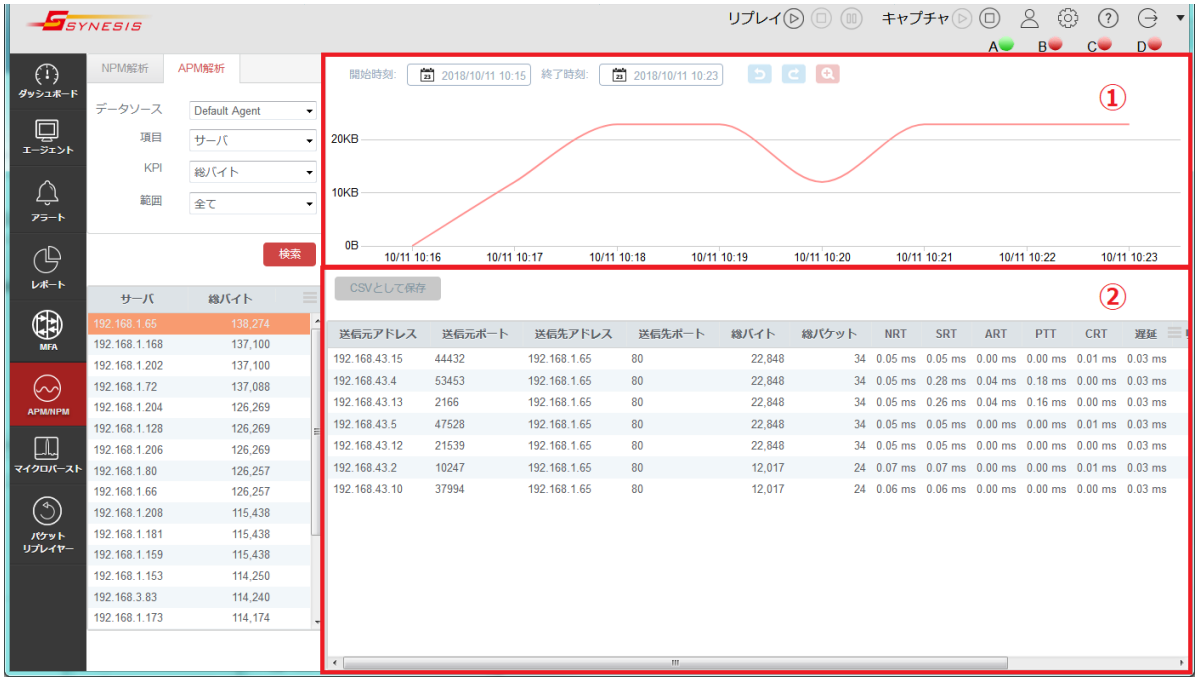


図 140：APM/NPM の画面構成

トレンドグラフ(上図①)には、指定した KPI により異なりますが、KPI の合計値または平均値が表示されます。

フローテーブル(上図②)にはフローごとの KPI が表示されます。

トレンドグラフの線上にカーソルを合わせると、その時点の KPI の値が表示されます。

10.2.2.　APM/NPM の期間指定

APM/NPM の解析結果は、上部に表示されている「開始時間」から「終了時間」までの情報です。

表示期間の指定、変更は、以下の 3 通りの方法があります。

1. [APM/NPM]メニュー>画面上部の「開始時刻」「終了時刻」のカレンダーアイコンで指定
   トレンドグラフ上部の「開始時間/終了時間」をクリックすると、以下の「期間」ダイアログが表示されます。

図 141：期間指定ダイアログ

ダイアログボックス左側のボタンから、表示する時間の範囲を一括で指定できます。選択できる時間は 30 分、1 時間、8 時間で、直近から遡った期間を指定します。

任意の期間を表示する場合は、「カスタム」を選択します。

2. [APM/NPM]メニュー>トレンドグラフから指定

[拡大]ボタン(下図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フロー情報も指定範囲の情報になります。

グラフ上でドラッグして時間範囲を指定し、画面中央上部の拡大アイコンをクリックします。

指定した時刻範囲でグラフが拡大表示されます。

図 142：拡大表示する時間範囲の指定

詳細は、**2.6.5. グラフ画面での期間指定** を参照してください。

3. [エージェント]メニュー>[レコード]タブ>該当レコードの解析 アイコンから指定

アイコンをクリックすると、以下の通り時刻を指定した状態で各解析メニューに移動します。

条件	**開始時刻**	**終了時刻**
キャプチャを停止したレコード	レコードの開始時刻	レコードの終了時刻
キャプチャ中のレコード	レコードの開始時刻	現在時刻

10.2.3. APM/NPM 解析の検索項目と KPI

左側の[APM 解析][NPM 解析]タブで右側のワークスペースに表示するフローと順序を指定します。

表示する項目と項目に関連した KPI、項目の表示する範囲を選択し、[検索]ボタン(下図①)をクリックします。左下のリスト(下図②)に項目で指定した KPI の結果が表示されます。

図 143：APM 解析の検索項目指定画面

リストを選択すると(下図③)、右側のワークスペースに関連するフローが表示されます(下図④)。

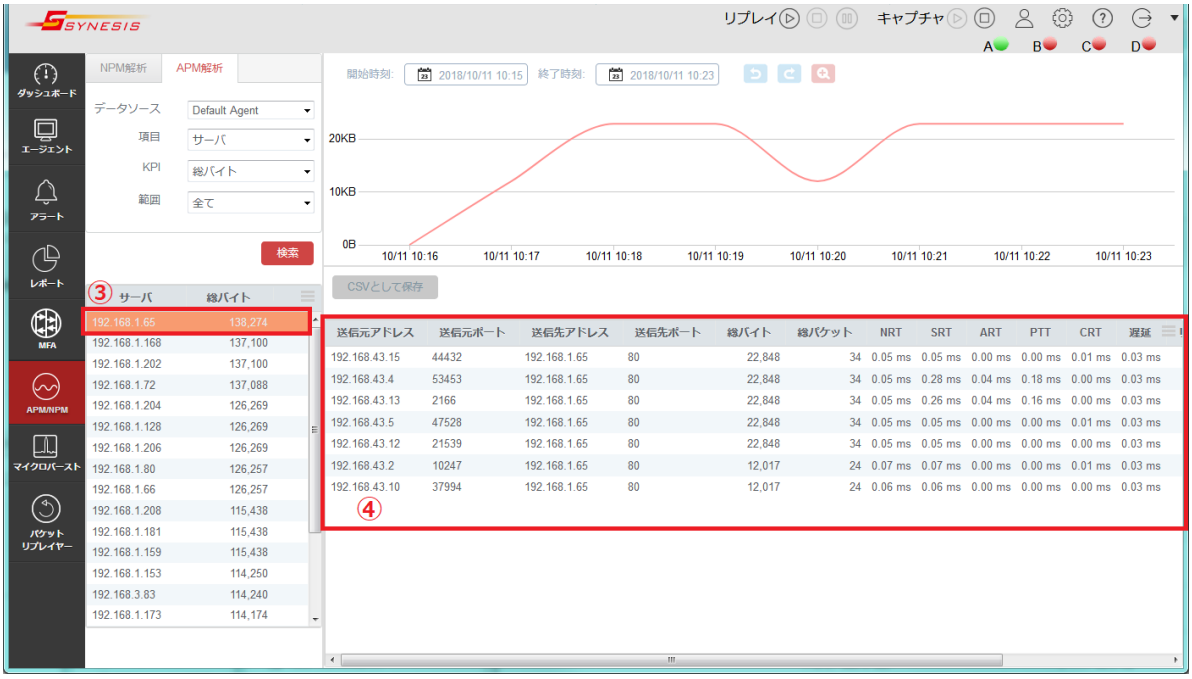


図 144：APM 解析の検索結果の表示

表示期間を更新した際には、左側のリストは更新されません。更新するためには[検索]ボタンをクリックし、都度、リストを更新する必要があります。

APM/NPM 解析の設定条件は、以下の通りです。

項目	説明	
データソース	選択できる項目は、「Default Agent」のみです。	
項目	選択された項目でデータを分類します。 選択可能な項目は以下の通りです。	
	サイト	「サイト」は、構成メニューの サイトの項目で登録されたネットワークグループです。 IP アドレスをサブネットごとにグループ化して登録できます。 サイトで登録された IP がクライアントの IP アドレスに含まれる場合に登録されたサイトに分類されます。
	サーバ	サーバの IP アドレスです。 フロー中のサーバの IP アドレスが表示されます。
	サーバグループ	「サーバグループ」は、構成メニューの サーバグループの項目で登録されたサーバのグループです。 複数のサーバをひとつのグループとして登録することができます。 サーバの IP アドレスがサーバグループに含まれる場合に分類されます。
	アプリケーション	アプリケーションは、構成メニューのプロトコル項目で登録された L4 ポート番号で登録されたアプリケーションです。 サーバのポートが登録されたプロトコルに含まれる場合に分類されます。
	アプリケーショングループ	「アプリケーショングループ」は、構成メニューのプロトコル項目で登録された L4 ポート番号で登録されたアプリケーショングループです。 サーバのポートが登録されたアプリケーショングループに含まれる場合に分類されます。
	アプリケーションホスト	「アプリケーショングホスト」は、IP アドレスと構成メニューのプロトコル項目で登録された L4 ポート番号で登録されたアプリケーションの組み合わせで分類されます。
KPI	フローを表示する際、ソートをする KPI です。指定した KPI で TopN をフローテーブルに表示します。トレンドグラフには、指定した KPI により異なりますが、KPI の合計値または平均値が表示されます。	
範囲	「項目」で「サイト」を選択すると、選択項目として 「プロトコル」で登録したアプリケーションのリストが表示されます。 「項目」で「サイト」以外を選択すると、 サイトで登録したネットワーク拠点が選択項目として表示されます。	

一部の設定は、検索を適用するために解析を実行する前に設定をしておく必要があります。

検索項目	事前設定	画面
サイト	[構成]メニュー>サイト	APM, NPM
サーバ	なし	APM, NPM
サーバグループ	[構成]メニュー>サーバグループ	APM, NPM
アプリケーション	[構成]メニュー>プロトコル	APM, NPM

アプリケーショングループ	[構成]メニュー>アプリケーショングループ	APM, NPM
アプリケーションホスト	[構成]メニュー>プロトコル	NPM

10.2.4. APM 解析のフローテーブル

クライアントとサーバを判断し、フローを表示します。判断の仕方は、**10.3.1. サーバの規則 (APM/NPM 共通)** を参照ください。

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
192.168.43.15	44432	192.168.1.65	80	22,848	34	0.05 ms	0.05 ms	0.00 ms	0.00 ms	0.01 ms	0.03 ms	12	トレースの保存
192.168.43.4	53453	192.168.1.65	80	22,848	34	0.05 ms	0.28 ms	0.04 ms	0.18 ms	0.00 ms	0.03 ms	12	トレースの保存
192.168.43.13	2166	192.168.1.65	80	22,848	34	0.05 ms	0.26 ms	0.04 ms	0.16 ms	0.00 ms	0.03 ms	12	トレースの保存
192.168.43.5	47528	192.168.1.65	80	22,848	34	0.05 ms	0.05 ms	0.00 ms	0.00 ms	0.01 ms	0.03 ms	12	トレースの保存
192.168.43.12	21539	192.168.1.65	80	22,848	34	0.05 ms	0.05 ms	0.00 ms	0.00 ms	0.00 ms	0.03 ms	12	トレースの保存
192.168.43.2	10247	192.168.1.65	80	12,017	24	0.07 ms	0.07 ms	0.00 ms	0.00 ms	0.01 ms	0.03 ms	3	トレースの保存
192.168.43.10	37994	192.168.1.65	80	12,017	24	0.06 ms	0.06 ms	0.00 ms	0.00 ms	0.00 ms	0.03 ms	3	トレースの保存

図 145 : APM のフローテーブル

[トレースの保存]リンクから、各フローのトレースファイルが保存できます。

詳細は、**5. トレースの保存操作** を参照してください。

フローテーブルの左上に表示される[CSV として保存]ボタンをクリックすると、フローテーブルに表示されているフロー情報を CSV ファイルで保存することができます。

フローテーブルで表示される KPI は、以下の通りです。

- 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

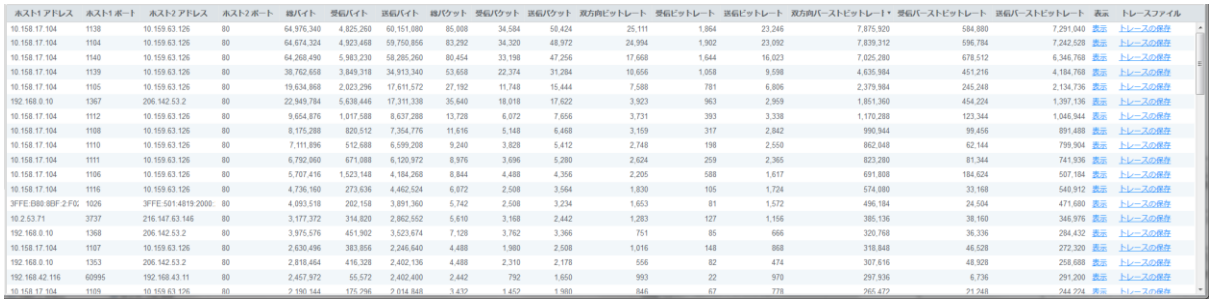
各 KPI のサンプリング周期は 1 分です。

詳細は、**10.3.3. APM の KPI** を参照ください。

10.2.5.　NPM 解析でのフローテーブル

APM 同様、クライアントとサーバを判断し、フローを表示します。判断の仕方は、**10.3.1. サーバの規則(APM/NPM 共通)** を参照してください。

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	1138	10.159.63.126	80	64,976,340	4,825,260	60,151,080	85,008	34,584	50,424	25,111	1,864	23,246	7,875,920	584,880	7,291,040	表示	トレースの保存
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	7,839,312	596,784	7,242,528	表示	トレースの保存
10.158.17.104	1140	10.159.63.126	80	64,268,490	5,983,230	58,285,260	80,454	33,198	47,256	17,668	1,644	16,023	7,025,280	678,512	6,346,768	表示	トレースの保存
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	表示	トレースの保存
10.158.17.104	1105	10.159.63.126	80	19,634,868	2,023,296	17,611,572	27,192	11,748	15,444	7,588	781	6,806	2,379,984	245,248	2,134,736	表示	トレースの保存
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	表示	トレースの保存
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	393	3,338	1,170,288	123,344	1,046,944	表示	トレースの保存
10.158.17.104	1108	10.159.63.126	80	8,175,288	820,512	7,354,776	11,616	5,148	6,468	3,159	317	2,842	990,944	99,456	891,488	表示	トレースの保存
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	表示	トレースの保存
10.158.17.104	1111	10.159.63.126	80	6,792,060	671,088	6,120,972	8,976	3,696	5,280	2,624	259	2,365	823,280	81,344	741,936	表示	トレースの保存
10.158.17.104	1106	10.159.63.126	80	5,707,416	1,523,148	4,184,268	8,844	4,488	4,356	2,205	588	1,617	691,808	184,624	507,184	表示	トレースの保存
10.158.17.104	1116	10.159.63.126	80	4,736,160	273,636	4,462,524	6,672	2,508	3,564	1,830	105	1,724	574,080	33,168	540,912	表示	トレースの保存
3FFE:B80:8BF:2:F0(	1026	3FFE:501:4819:2000:	80	4,093,518	202,158	3,891,360	5,742	2,508	3,234	1,653	81	1,572	496,184	24,504	471,680	表示	トレースの保存
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	表示	トレースの保存
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	表示	トレースの保存
10.158.17.104	1107	10.159.63.126	80	2,630,496	383,856	2,246,640	4,488	1,980	2,508	1,016	148	868	318,848	46,528	272,320	表示	トレースの保存
192.168.0.10	1353	206.142.53.2	80	2,818,464	416,328	2,402,136	4,488	2,310	2,178	556	82	474	307,616	48,928	258,688	表示	トレースの保存
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	970	297,936	6,736	291,200	表示	トレースの保存
10.158.17.104	1109	10.159.63.126	80	2,190,144	175,296	2,014,848	3,432	1,452	1,980	846	67	778	265,472	21,248	244,224	表示	トレースの保存

図 146：NPM のフローテーブル

[トレースの保存]リンクから、各フローのトレースファイルが保存できます。

詳細は、**5. トレースの保存操作** を参照してください。

[表示]リンクから、トレンドグラフを拡大表示することができます。

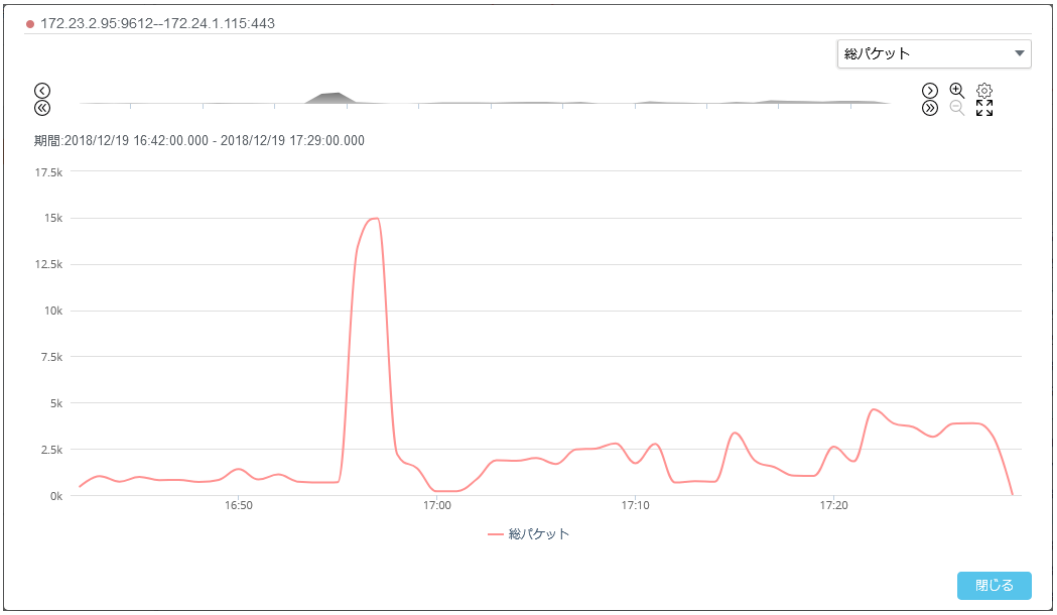


図 147：トレンドグラフの拡大表示

画面右上のリストボックスからグラフに表示させる KPI を選択できます。

「閉じる」ボタンをクリックすると、元の操作画面に戻ります。

フローテーブルの左上に表示される[CSV として保存]ボタンをクリックすると、フローテーブルに表示されているフロー情報を CSV ファイルで保存することができます。

フローテーブルに表示される KPI は、以下の通りです。

- 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

各 KPI のサンプリング周期は 1 分です。
詳細は、**10.3.4. NPM の KPI** を参照ください。

10.2.6. APM/NPM 解析の制限事項

- APM/NPM での解析結果の表示されたデータをソートした場合、 全データからソートは行われません。「構成->解析->上位のフロー」で設定された数のデータがあらかじめ取得され、その中でのみソートが行われます。
- キャプチャ期間が 5 分未満のレコードでは、APM 解析の結果が検出できないことがあります。APM 解析を行う場合には 5 分以上キャプチャしたレコードで行ってください。
- 直近のデータの解析結果は、キャプチャの停止を行う、または次のパケットがキャプチャされるまで、 APM/NPM 画面で閲覧できません。
- APM 解析はスリーウェイ(3way)ハンドシェイクが確立した通信を対象としています。そのため、スリーウェイハンドシェイクパケットが解析で指定した期間の範囲外にある場合、フローは解析対象となりません。

10.3. APM/NPM に関する KPI の定義

解析で使用される KPI の定義について説明します。

10.3.1. サーバの規則(APM/NPM 共通)

APM/NPM の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。

10.3.2. TopN 表示の規則(APM/NPM 共通)

各 KPI のサンプリング周期は 1 分です。

SYNESIS 内部のメモリには 4,000,000 フロー(IP アドレスとポートのペア)が保持されています。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。

フローは、25 秒以上非アクティブとなった場合、もしくは FIN/ RESET パケット後 2 秒経過した場合に終了となり、以降のパケットを同一のフローとして扱いません。

フローが終了したタイミングでそのフローはメモリ上から消去されます。

10.3.3. APM の KPI

TCP フローごとにコネクションの各段階で要している時間を表示します。フローのどの段階にボトルネックがあるかを確認できます。スリーウェイハンドシェイクが確立した TCP のフローのみ APM 解析を行います。

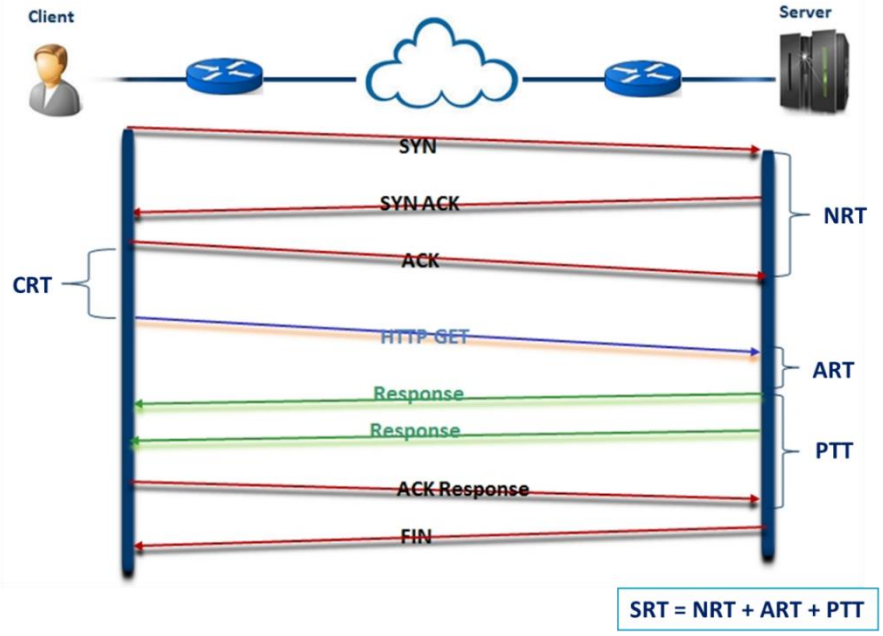


図 148：スリーウェイハンドシェイクが確立した通信と各 KPI

項目	詳細
送信元アドレス	クライアントの IP アドレスです。
送信元ポート	クライアントのポート番号です。
送信先アドレス	サーバの IP アドレスです。
送信先ポート	サーバのポート番号です。
総バイト	バイト数です。
総パケット	総パケット数です。
NRT	ネットワーク往復遅延時間(Network Round-trip Time)です。 スリーウェイハンドシェイクが確立した時間です。
CRT	クライアント応答時間(Client Response Time)です。 スリーウェイハンドシェイク確立後、クライアントがサーバへリクエストを開始するまでにかかる時間になります。 [スリーウェイハンドシェイク後クライアントから送信された最初のパケットのタイムスタンプ]-[スリーウェイハンドシェイクの最後のパケットのタイムスタンプ]で計算されます。
ART	アプリケーション応答時間(Application Response Time)です。 サーバがクライアントリクエストへの応答に要した時間になります。 [リクエストに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	ペイロード転送時間(Payload Transfer Time)です。 サーバが実際のデータの転送に要した時間になります。 [データに対応する応答のタイムスタンプ]-[サーバのデータパケットのタイムスタンプ]で計算されます。
SRT	サーバ応答時間(Server Response Time)です。 サーバ側で発生した応答時間の合計です。 NRT＋ART＋PTT で計算されます。
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。 NRT の 1/2 の値で計算されます。
リトライ	TCP の再送パケット数です。 リトライの判定は、MFA の KPI と同様です。詳細は、**13.5.3. MFA に関する KPI の定義** の中の、**13.5.3.2. フローごとの KPI** を参照ください。

10.3.4. NPM の KPI

TCP/UDP フローの IP ペアをホスト単位で KPI を表示します。双方向通信であるフローのそれぞれの方向に対して通信量とフローの通信状況を把握することができます。

項目	説明
ホスト 1 アドレス	クライアントの IP アドレスです。
ホスト 1 ポート	クライアントのポート番号です。
ホスト 2 アドレス	サーバの IP アドレスです。
ホスト 2 ポート	サーバのポート番号です。
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	期間中のビットレートの平均です。単位は bps です。 ビットレートは 1 分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。単位は bps です。 例えば、期間を 10 分に指定した場合、1 分ごとのビットレート値が 10 個存在します。10 個のビットレート値の最大値がバーストビットレートです。

各 KPI のサンプリング周期は 1 分です。

フローの送受信の方向は、「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 1 からホスト 2 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。

10.4. マイクロバースト解析

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するマイクロバーストの発生状況を検出できます。

マイクロバースト解析結果は、[マイクロバースト]メニューより確認します。

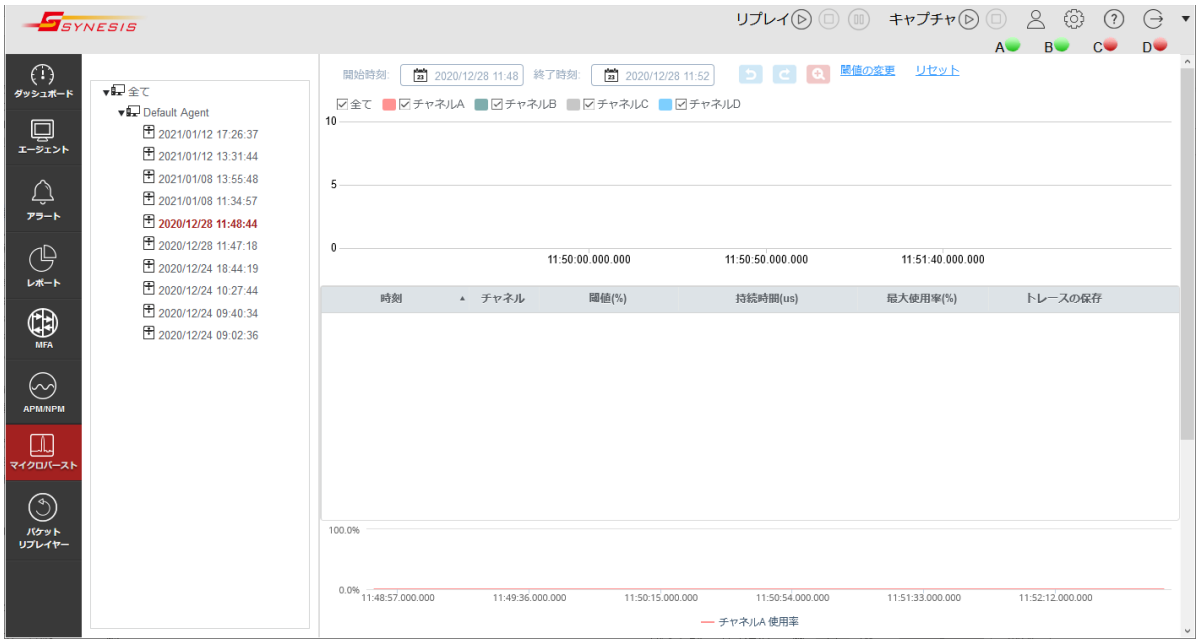


図 149 :「マイクロバースト」メニュー画面

10.4.1. マイクロバーストの閾値の検出方法

マイクロバーストを検知するには、あらかじめ閾値を設定する必要があります。閾値の設定方法は、**10.5.3. マイクロバーストの閾値設定** を参照ください。

閾値は、「使用率」と「持続時間」のふたつの項目で設定します。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。

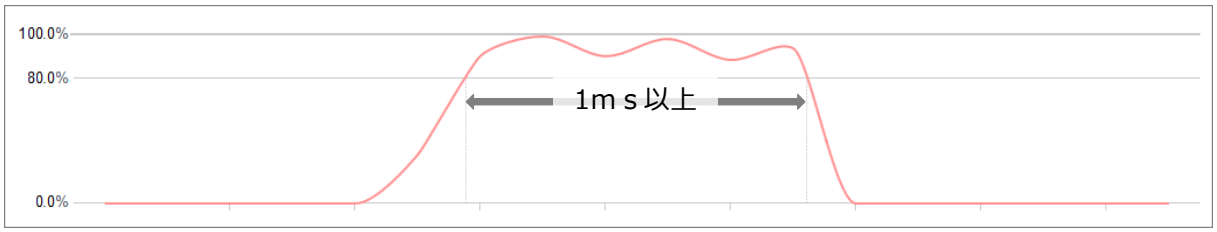


図 150 : 使用率が閾値を超える時間が、指定した持続時間を超えて続いた場合

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、 1 ms 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。

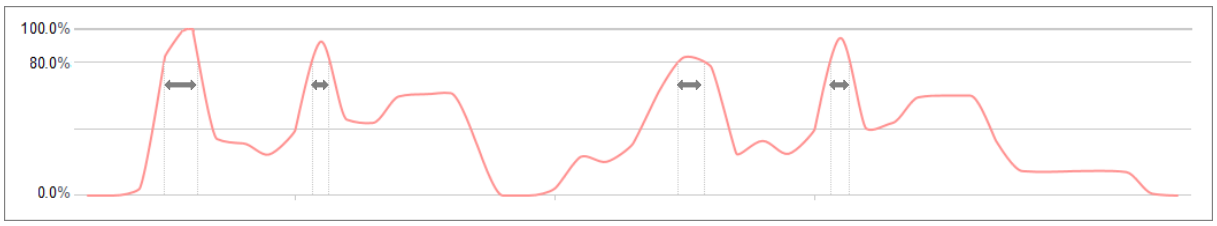


図 151：使用率が閾値を超える時間が短い場合

実際の解析過程では、レコードを指定された「分解能」で区切ります。区切られた分解能で使用率を計算し、その使用率が指定した閾値を超えていないかを確認します。

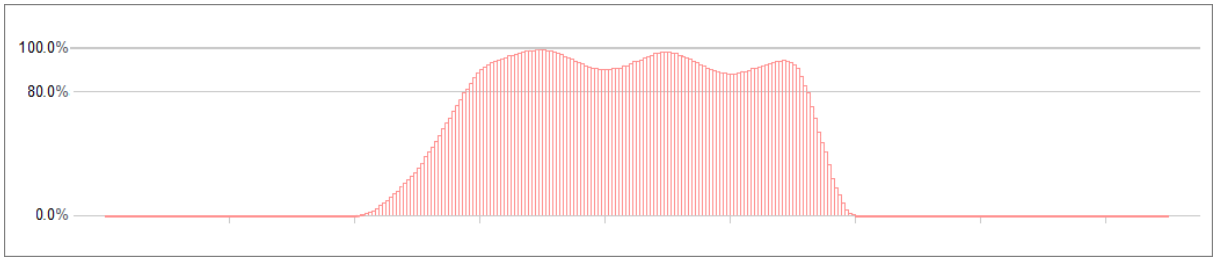


図 152：指定された分解能で区切られたレコード

「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、分解能で区切られた使用率が閾値を超えた時点から、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」で計算され、「持続時間」の閾値も「分解能」と「連続発生数」で指定されます。

10.4.2. マイクロバーストのリアルタイム検出

リアルタイムにマイクロバーストの発生を検出する場合は、キャプチャ開始前に閾値を設定した上で、自動解析を有効にします。

手順は、以下の通りです。**4.4.1. 共通 オプション**もあわせて参照ください。

1) 構成メニューのマイクロバーストで閾値を設定します。なお、キャプチャ開始後は、閾値を変更できません。
2) キャプチャオプションの共通タブで、「キャプチャ中の自動解析」にチェックを入れ、自動解析を有効にします。
3) 解析モジュールのリストに「マイクロバースト」を追加します。

解析結果を更新する場合は、キーボードの＜F5＞キーをクリックし、ブラウザを更新します。終了時刻が更新され、最新の解析結果が表示されます。

通知先を設定することで、通知を行うことが可能です。詳細は、**10.4.6. マイクロバーストの外部通知** を参照してください。

10.4.3. マイクロバーストの画面構成

マイクロバーストの解析結果は、[マイクロバースト]メニューから確認します。

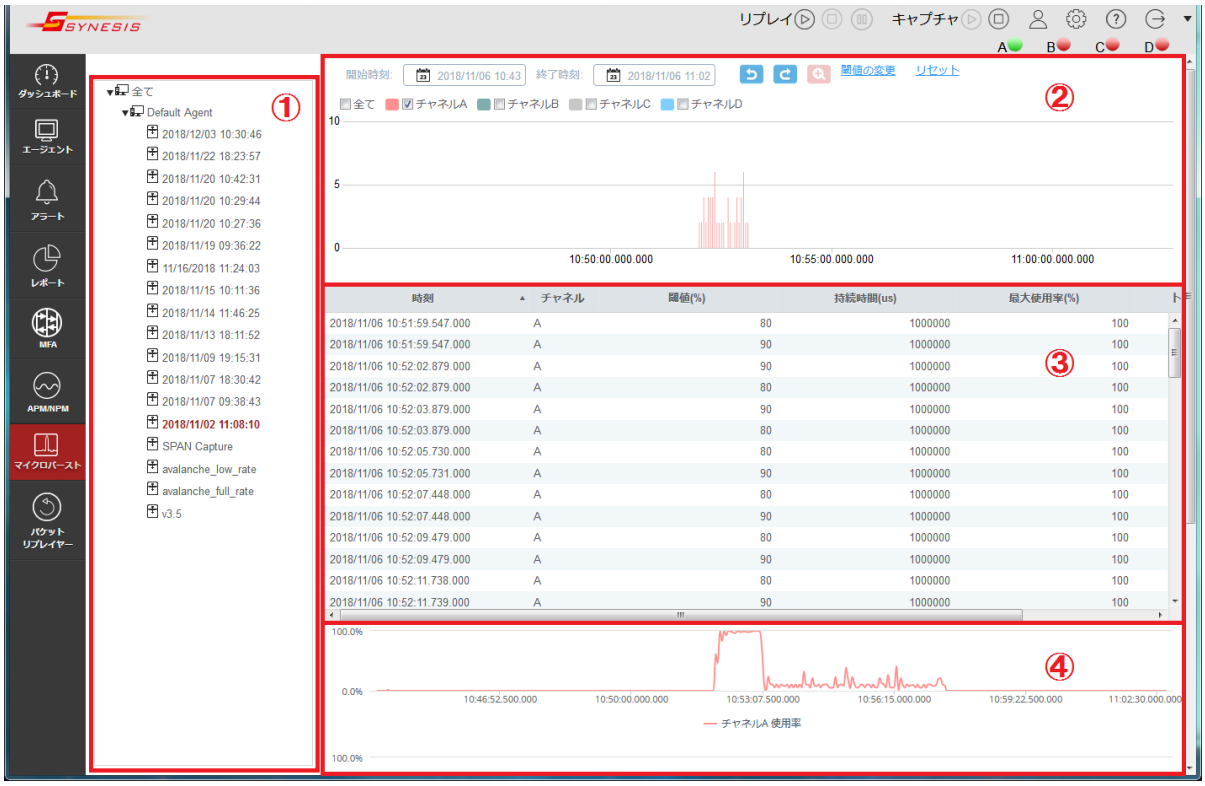


図 153：マイクロバーストの画面構成

画面は、４つの画面で構成されています。

- エージェント・ペイン (上図①)

レコードの一覧です。選択されたレコードの解析結果が右側のワークスペースに表示されます。レコードが未解析な場合は、結果が表示されません。

- アラートグラフ (上図②)

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 (上図③)

検索期間中、使用率の大きい順にトップ 500 のアラート一覧です。

アラートテーブルに表示される情報は、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。
チャネル	マイクロバーストが検知されたチャネルです。
閾値(%)	検知基準として参照されたアラート閾値の回線使用率(%)です。 実際に検知されたマイクロバーストの最大使用率ではありません。

持続時間(μs)	検知基準として参照されたアラート閾値の持続時間(μs)です。 実際に検知されたマイクロバーストの持続時間ではありません。
最大使用率(%)	マイクロバーストの中で検知された最大の使用率(%)です。
トレースの保存	アラートが発生した期間のデータをトレースファイルに保存できます。 詳細は **5. トレースの保存操作** を参照してください。

- 使用率グラフ (上図④)

チャネルごとの使用率のグラフです。

マイクロバースト・ワークスペース画面の上部には、表示期間と閾値の変更ができるメニューやアイコンが表示されています。

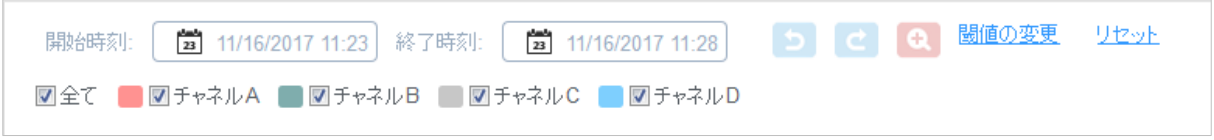


図 154 :「マイクロバースト」ワークスペース上部のメニュー

それぞれの機能は、以下の通りです。

項目/表示	説明
開始時刻 **/終了時刻**	表示するデータの開始時刻と終了時刻を指定できます。 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。 表示を更新する場合は、キーボードの<F5>キーをクリックしてブラウザを更新します。
ボタン	グラフ上の期間を指定して拡大表示させることができます。 詳細は、**2.6.5. グラフ画面での期間指定** を参照してください。
元に戻す **やり直す**	「 元に戻す」アイコンをクリックすると、直前に行った操作が取り消されます。 「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」操作がキャンセルされます。
閾値の変更	閾値を変更してデータを再解析することができます。 詳細は **10.4.5. マイクロバーストの再解析** を参照してください。
リセット	再解析したデータをリセットして、最初の設定に表示を戻します。 詳細は、**10.5.3. マイクロバーストの閾値設定** を参照してください。
全て **/各チャネル**	表示するデータのチャネル選択できます。 チェックが入ったチャネルのデータのみが表示されます。

10.4.4. マイクロバーストの期間指定

マイクロバーストの解析結果は、上部に表示されている「開始時間」から「終了時間」までの情報です。

表示期間の指定、変更は、以下の４通りの方法があります。

1. ［マイクロバースト]メニュー>画面上部の「開始時刻」「終了時刻」のカレンダーアイコンで指定
   トレンドグラフ上部の「開始時間/終了時間」をクリックすると、以下の「期間」ダイアログが表示されます。

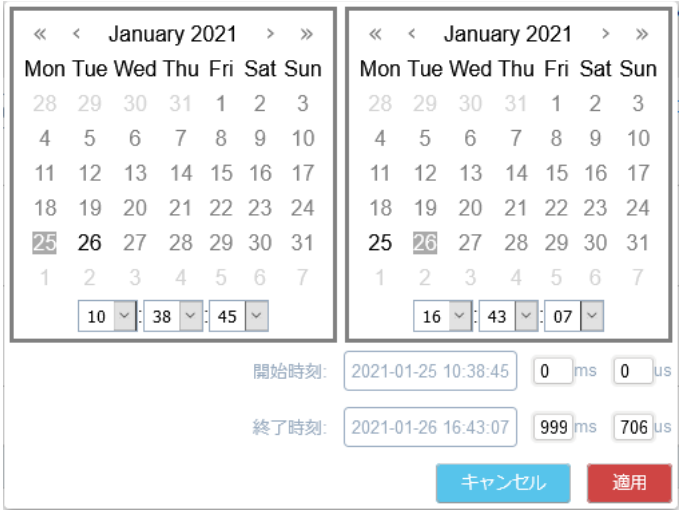


図 155：期間指定ダイアログ

2. ［マイクロバースト]メニュー>トレンドグラフから指定
   トレンドグラフ上でドラッグして時間範囲を指定します。(下図①)
   画面中央上部の「拡大」アイコン（下図②）をクリックすると、指定した時刻範囲が拡大表示されます。アラートテーブルに表示されるフロー情報も指定範囲の情報になります。

図 156：トレンドグラフ上での拡大範囲指定

詳細は、**2.6.5. グラフ画面での期間指定** を参照してください。

3.　[エージェント]メニュー>[レコード]タブ>該当レコードの「マイクロバースト」アイコンから指定

アイコンをクリックすると、以下の通り時刻を指定した状態で各解析メニューに移動します。

[レコード]タブからの時刻指定	**開始時刻**	**終了時刻**
キャプチャを停止したレコード	レコードの開始時刻	レコードの終了時刻
キャプチャ中のレコード	レコードの開始時刻	現在時刻

4.　「マイクロバースト」メニュー>エージェント・ペイン>各レコードで指定

レコードを選択してクリックすると、以下の通り時刻が指定された状態で各解析メニューに移動します。

エージェント・ペインからの時刻指定	**開始時刻**	**終了時刻**
キャプチャを停止したレコード	レコードの開始時刻	レコードの終了時刻
キャプチャ中のレコード	レコードの開始時刻	現在時刻

10.4.5. マイクロバーストの再解析

解析済のマイクロバースト結果に対して、閾値を変更して再度解析を行うことができます。

再解析を行う場合は、画面上部の「閾値の変更」のリンクをクリックします。 以下の「再解析」設定画面が表示されます。

図 157：マイクロバースト「再解析」ダイアログ

各項目を設定して、[適用]ボタンをクリックすると、設定した新しい閾値で再解析が実行されます。一度に再解析できる期間は最大 120 分です。

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 120 分まで指定できます。
閾値 1 **閾値 2**	２つの閾値を設定できます。 チェックしたアラート閾値のみ設定が有効となり、アラートの対象となります。 閾値は、「使用率」と「連続発生数」の 2 つで指定します。
使用率	回線使用率を 1 以上 100 以下の値で入力します。ここで指定した回線使用率を超えるトラフィックが指定した「持続時間」(「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して検知されます。
連続発生数	回線使用率を連続して超えた期間を「持続時間」とした場合、「連続発生数」は「持続時間」÷「分解能」となります。 1 以上 70000 以下の値で入力します。
分解能	使用率の計算に使用される分解能です。閾値 1 ・閾値 2 で共通の設定であり、別々の分解能では指定できません。 1000 us または 100 us から選択します。

ここで設定する閾値と「構成」メニュー>「マイクロバースト」で設定する閾値は、独立して管理されています。値を変更しても互いに影響しません。

10.4.6. マイクロバーストの外部通知

通知設定が有効な場合は、アラートが発生したことを外部に通知することができます。 外部通知は自動解析のアラートに対してのみ行われます。ポスト解析では通知されません。

外部通知は 1 分間隔で行われます。1 分間に複数のアラートが発生した場合は 1 回に集約して通知されます。

通知を行う場合は、キャプチャを開始する前に[構成]メニュー>「マイクロバースト」より通知先を設定します。

詳細は、**10.5.3. マイクロバーストの閾値設定** と **14.3. 通知** を参照してください。

10.4.7. マイクロバースト解析に必要なディスク容量

マイクロバースト解析では、再解析に必要な中間ファイルを保存するため、ディスク容量を大量に消費します。1 日あたり、1 チャネルあたりおよそ 1.2GB です。

全くトラフィックが流れていないチャネル、リンクダウンしているチャネル、キャプチャを無効にしたチャネルに対しても、この割合でディスク容量が消費されます。

10.4.8. マイクロバースト解析に関する制限事項

- 検出したマイクロバーストのアラームは、最大 500 個までしかテーブルに表示できません。
- マイクロバースト解析はチャネル A～D に対してのみ実行できます。 5 ポート以上存在するモデルでは、チャネル E 以降のデータはマイクロバースト解析できません。

10.5.　解析に関する設定項目と仕様

解析に関する設定項目と仕様について説明します。

10.5.1.　解析共通

解析機能共通の設定は、 [構成]メニュー>「解析」より行います。

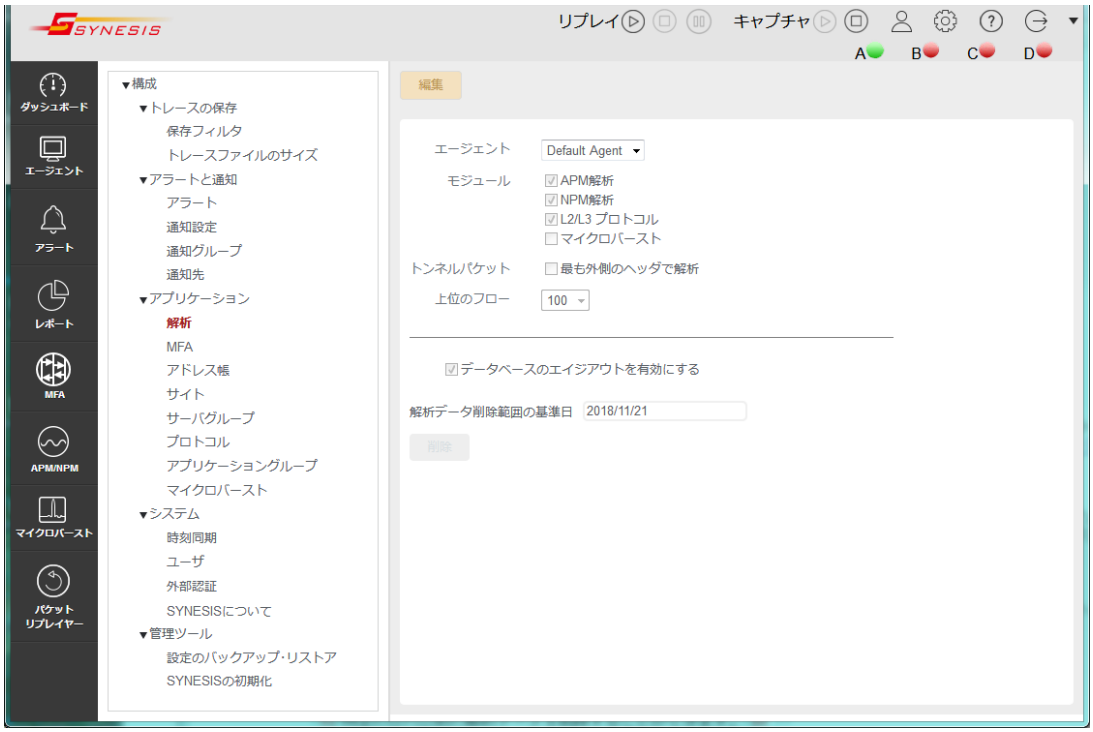


図 158 :「解析」メニュー画面

編集する場合は、画面左上の[編集]ボタンをクリックし、編集画面にて設定項目を編集します。

各項目の設定が完了したら[保存]ボタンをクリックし、確認画面に戻ります。

設定項目は、以下の通りです。

項目	説明	
エージェント	選択できる項目は、「Default Agent」のみです。	
モジュール	解析モジュールを選択します 下記の内の 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 解析の詳細は、**14.1.2. アラート一覧** を参照してください。	
	APM 解析	APM 解析を有効にします。
	NPM 解析	NPM 解析を有効にします。
	L2/L3 プロトコル	L2/L3 プロトコル解析を有効にします。ダッシュボード機能で有効になります。
	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。

トンネルパケット	APM/NPM 解析、L2/L3 プロトコル解析、ARP 解析はインナーヘッダで行われます。「最も外側のヘッダで解析」をチェックすると、アウターヘッダで解析が行われます。
上位のフロー	グラフに表示する上位の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 4,000,000 フロー(IP アドレスとポートのペア)が保持されています。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。 フローが終了したタイミングでそのフローはメモリ上から消去されます。
データベースのエイジアウトを有効にする	解析済のデータを自動的に削除させることができます。削除対象は、ARP を除く APM、NPM、L2/L3 プロトコル、マイクロバーストの各データです。 エイジアウトが有効な状態での動作は、下記の通りです。 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。 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。 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。 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。
解析データの削除	解析データを削除することができます。 削除対象は、APM、NPM、L2/L3 プロトコル、マイクロバーストの各データです。 ARP 解析のデータは削除されません。 解析データを削除する場合は、画面左上の[編集]ボタンをクリックします。[削除]ボタンが有効になります。 「解析データ削除範囲の基準日」欄で日付を指定して、[削除]ボタンをクリックします。指定した日付より過去のデータが削除され、指定した日付以降のデータのみ残ります。

10.5.2. APM/NPM の事前設定

APM/NPM 解析は、「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」を事前に設定することにより、状況に合わせたデータの分類が可能となります。

- 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

10.5.2.1 サイトの設定・管理

サイトの設定は、「構成」メニュー>「サイト」で行います。

解析画面では、サイトで登録された IP アドレスがクライアントに含まれる場合に分類されます。 登録された「サイト」の情報は、一覧表に表示されます。

図 159 :「構成」メニュー>「サイト」

サイトの新規登録、削除、編集する手順は以下の通りです。

- サイトの新規登録

[新規]ボタンをクリックします。

下図のサイト登録ダイアログが表示されます。

図 160 :「サイト」登録ダイアログ

登録項目は、以下の通りです。

項目	説明
名前	サイトの名前です。
説明	サイトの説明です。
範囲	サイトの IP アドレスの範囲です。 IP アドレス形式または CIDR 形式で入力します。 複数のアドレスを登録する場合は、セミコロン(;)で区切ってアドレスを列記します。 （例:192.168.2.3/24;192.168.9.7） 同一定義内でアドレス範囲が重複する場合は、設定ができません。 定義済のサイトとアドレス範囲が重複する場合は、設定ができません。

各項目入力後、[保存]ボタンをクリックします。入力したサイトの情報がリストに追加されます。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。

- サイトの削除

登録済みのサイトを削除する場合は、該当の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ます。 選択したサイトが削除されます。

登録済みのサイトをすべて削除する場合は、項目名欄のチェックボックスにチェックを入れます。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。

- サイトの編集

登録済みのサイトを編集する場合は、「名前」のリンクをクリックします。登録ダイアログが表示され、登録内容を編集できます。

入力内容を保存する場合は、[保存]ボタンをクリックします。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。

10.5.2.2 サーバ グループの設定・管理

「構成」メニュー>「サーバグループ」では、サーバをグループ化するサーバグループの登録・管理を行います。

解析画面では、サイトで登録された IP がサーバに含まれる場合に分類されます。登録された「サーバグループ」の情報は一覧表に表示されます。

図 161 :「構成」メニュー>「サーバグループ」

サーバグループの新規登録、削除、編集する手順は以下の通りです。

- サーバグループの新規登録

新規にサーバグループを登録する場合は、[新規]ボタンをクリックします。

下図のサーバグループ登録ダイアログが表示されます。

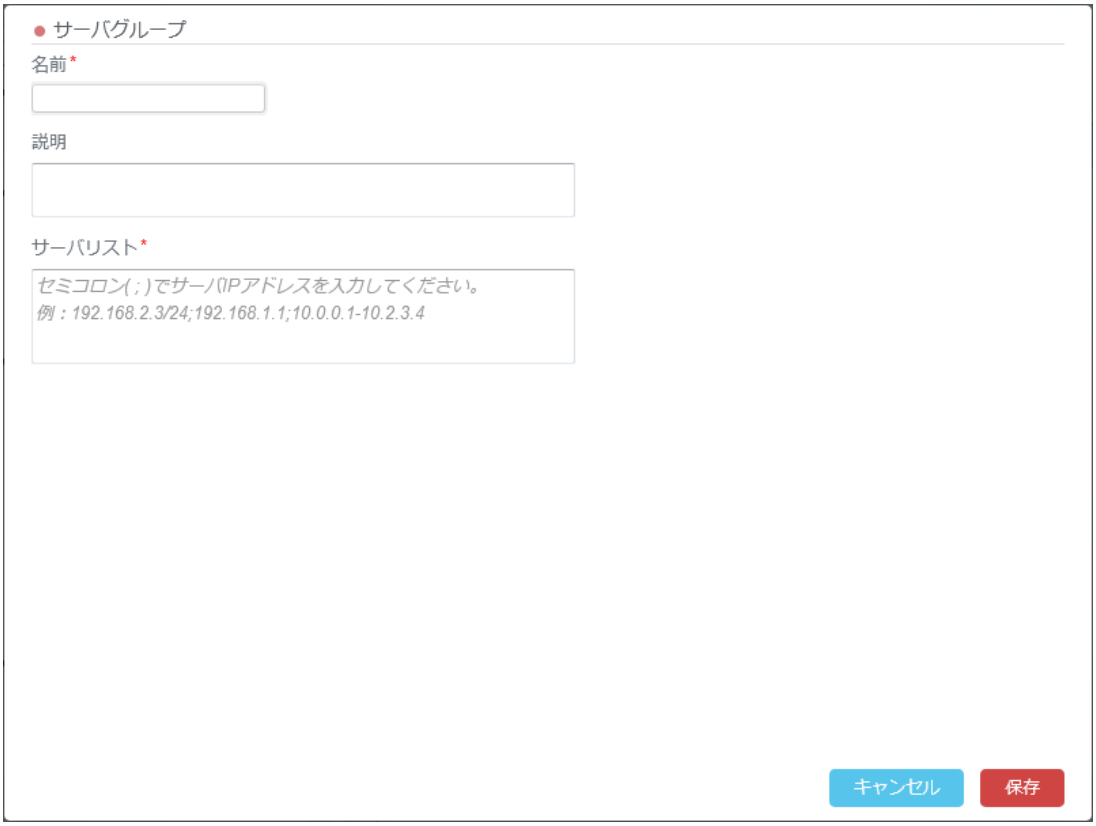


図 162：「サーバグループ」登録ダイアログ

登録項目は、以下の通りです。

項目	説明
サーバグループ名	サーバグループの名前です。
サーバグループの説明	サーバグループの説明です。
サーバリスト	サーバの IP アドレスの範囲です。 IP アドレス形式または CIDR 形式で入力します。複数のアドレスを登録する場合は、セミコロン(;)で区切ってアドレスを列記します。 （例:192.168.2.3/24;192.168.9.7） 同一定義内でアドレス範囲が重複する場合は、設定ができません。 定義済のサーバグループとアドレス範囲が重複する場合は、設定ができません。

各項目入力後、[保存]ボタンをクリックします。入力したサーバグループの情報がリストに追加されます。

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。

- サーバグループの削除

登録済みのサーバグループを削除する場合は、該当のサーバグループ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ます。 選択したサーバグループが削除されます。

登録済みのサーバグループをすべて削除する場合は、項目名欄のチェックボックスにチェックを入れます。 すべてのサーバグループが選択された状態になり、すべてのサーバグループが削除されます。

- サーバグループの編集

登録済みのサーバグループを編集する場合は、「名前」のリンクをクリックします。登録ダイアログが表示され、登録内容を編集できます。

入力内容を保存する場合は、[保存]ボタンをクリックします。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。

10.5.2.3 プロトコルの設定・管理

「構成」メニューの「プロトコル」では、L2/L3/L4 の各プロトコルの登録・管理を行います。
登録済みのプロトコルは一覧表で表示されます。

図 163 :「構成」メニュー >「プロトコル」

登録できるプロトコルは、「

L2 イーサタイプ」と「**L3 プロトコル**」と「**L4 ポート番号**」の 3 種類です。

登録したプロトコルは、以下の画面で使用します。

- ダッシュボード
- レポート
- APM/NPM
- MFA
- 保存フィルタ

「全て」の タブ (上図)では、登録済みの L2/L3/L4 プロトコルが全て表示されます。

L2 イーサタイプと L3 プロトコルと L4 ポート番号では 各レイヤでの登録済みのプロトコルが一覧表で表示され、プロトコルの登録・削除・編集が行えます。

詳細は、それぞれの章を参照してください。
プロトコルの新規登録、削除、編集する手順は以下の通りです。

- プロトコルの新規登録

新規にプロトコルを登録する場合は、該当するレイヤタブ上の[新規]ボタンをクリックします。
プロトコル登録ダイアログが表示されます。
登録項目は、各レイヤの設定項目を参照ください。

- プロトコルの削除

登録済みのプロトコルを削除する場合は、該当のするプロトコルのチェックボックスにチェックを入れて、画面左上の削除ボタンをクリックします。 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。

- プロトコルの編集

登録済みのプロトコルを編集する場合は、「名前」のリンクをクリックします。登録ダイアログが表示され、登録内容を編集できます。
入力内容を保存する場合は、[保存]ボタンをクリックします。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。

10.5.2.3.1.**登録済プロトコルの一覧**

「全て」のタブには登録済みの L2、L3、L4 プロトコルが全て表示されます。
「全て」のタブは閲覧のみです。登録と編集は各レイヤのタブ画面から行ってください。

項目	**説明**
名前	プロトコルの名前です。
説明	プロトコルの説明です。
値	プロトコルの値です。 レイヤごとに登録する値は異なります。 ● L2:イーサタイプ (16 進数) ● L3:プロトコル番号 (10 進数) ● L4:ポート番号 (10 進数)
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 ポート番号

10.5.2.3.2.**L2 イーサタイプ**

「L2 イーサタイプ」タブではイーサタイプを登録・管理できます。

図 164 :「L2 イーサタイプ」タブ

下図が、「L2 イーサタイプ」登録ダイアログです。

図 165 :「L2 イーサタイプ」登録ダイアログ

設定項目は、以下の通りです。

項目	説明
名前	イーサタイプの名前です。
説明	イーサタイプの説明です。
イーサタイプ	イーサタイプを 16 進数で入力します。 数値は 0001 以上 FFFF 以下、半角で入力してください。

10.5.2.3.3.L3 プロトコル

「L3 プロトコル」タブではプロトコル番号を登録・管理できます。

図 166 :「L3 プロトコル」タブ

下図が「L3 プロトコル」登録ダイアログです。

図 167 :「L3 プロトコル」登録ダイアログ

設定項目は、以下の通りです。

項目	説明
名前	プロトコル番号の名前です。
説明	プロトコル番号の説明です。
プロトコル番号	プロトコル番号を 10 進数で入力します。 1 以上 255 以下の数値で入力してください。 43,44,51,60 は登録できません。

10.5.2.3.4.L4 ポート番号

「L4 ポート番号」タブでは TCP/UDP のポートを登録・管理できます。

図 168 :「L4 ポート番号」タブ

下図が「L4 ポート番号」登録ダイアログです。

図 169 :「L4 ポート番号」登録ダイアログ

設定項目は、以下の通りです。

項目	説明
名前	ポート番号の名前です。
説明	ポート番号の説明です。
ポート範囲	ポート番号を 10 進数で入力します。 範囲で指定する場合は、 "- (半角ハイフン)"でつなぎ、ポート範囲同士は "; (半角セミコロン)"で区切って入力してください。 （例：3500-3511;8300;9810-9816）

10.5.2.4 アプリケーショングループ

構成メニュー>「アプリケーショングループ」では、アプリケーションプロトコルをグループ化するアプリケーショングループの管理・登録を行います。

L4 ポート番号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、「アプリケーショングループ」として登録することができます。

解析の画面では、サーバのポートが登録されたアプリケーショングループに含まれる場合に分類されます。

登録された「アプリケーショングループ」の情報は一覧表で表示されます。

図 170 :「アプリケーショングループ」画面

サーバグループの新規登録、削除、編集する手順は以下の通りです。

- アプリケーショングループの新規登録

アプリケーショングループの登録を追加する場合は、[新規]ボタンをクリックします。

下図のアプリケーショングループ登録ダイアログが表示されます。

図 171 :「アプリケーショングループ」登録ダイアログ

登録項目は、以下の通りです。

項目	説明
名前	アプリケーショングループの名前です。
説明	アプリケーショングループの説明です。
アプリケーションプロトコルリスト	左側の欄には SYNESIS 内で定義済の L4 ポート番号がリストアップされています。このリストの中の適用するプロトコルを選択し、 >> アイコンをクリックします。選択したプロトコルが右側のリストに追加されます。 リストに設定するプロトコルがない場合は、構成メニューのプロトコルの項目でプロトコルの定義を追加します。 右側のリストから外す場合は、該当するプロトコルを選択し、 << アイコンをクリックします。

各項目入力後、[保存]ボタンをクリックします。入力したアプリケーショングループの情報がリストに追加されます。

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。

- アプリケーショングループの削除

登録済みのアプリケーショングループを削除する場合は、削除するアプリケーショングループ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ます。選択したアプリケーショングループが削除されます。

登録済みのアプリケーショングループをすべて削除するする場合は、項目名欄のチェックボックスにチェックを入れます。 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、すべてのアプリケーショングループが削除されます。

- アプリケーショングループの編集

登録済みのアプリケーショングループを編集する場合は、「名前」のリンクをクリックします。登録ダイアログが表示され、登録内容を編集できます。

入力内容を保存する場合は[保存]ボタンをクリックします。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。

10.5.3. マイクロバーストの閾値設定

構成メニュー>「マイクロバースト」では、マイクロバースト発生の判断基準となる閾値の設定を行います。指定された閾値を超えるトラフィックが検知されると、マイクロバースト発生と判断されます。

図 172 :「構成」メニュー >「マイクロバースト」

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ます。マイクロバースト検知とこれら閾値の関係は **10.4.1. マイクロバーストの閾値の検出方法** を参照してください。

マイクロバーストのアラート閾値を変更する場合は、[編集]ボタンをクリックします。各項目が編集可能になります。

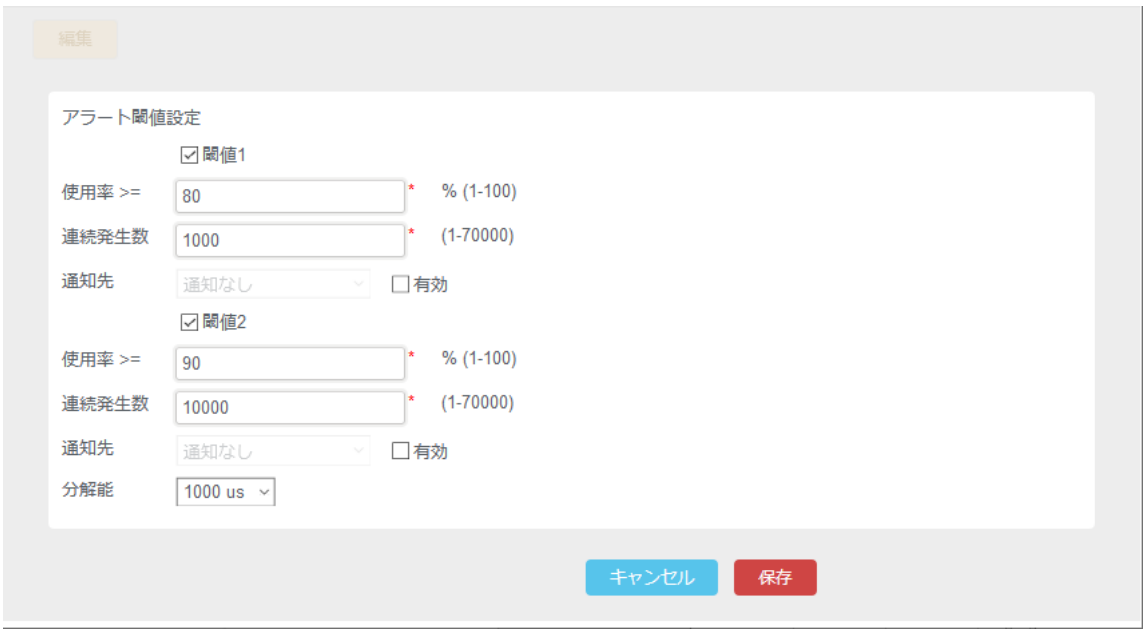


図 173 :「マイクロバースト」閾値設定画面

設定項目は、以下の通りです。

項目	説明
閾値１ 閾値２	２つの閾値を設定できます。 チェックしたアラート閾値のみ設定が有効となり、アラートの対象となります。 閾値は、「使用率」と「連続発生数」の２つで指定します。
使用率	回線使用率を１以上 100 以下の値で入力します。ここで指定した回線使用率を超えるトラフィックが指定した「持続時間」(「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して検知されます。
連続発生数	回線使用率を連続して超えた期間を「持続時間」とした場合、「連続発生数」は「持続時間」÷「分解能」となります。１以上 70000 以下の値で入力します。
通知先	閾値を超えた際に外部に通知をする設定を行います。 チェックボックスにチェックを入れると通知が有効になり、通知先の設定が行えます。 外部通知はリアルタイム解析のアラートに対してのみ行われます。ポスト解析では通知されません。 外部通知は 1 分間隔で行われます。1 分間に複数のアラートが発生した場合は 1 回に集約して通知されます。 通知先は登録した通知グループから選択します。 通知グループの登録方法は **14.3.2. 通知グループの設定** を参照してください。
分解能	使用率の計算に使用される分解能です。閾値１・閾値２で共通の設定であり、別々の分解能では指定できません。 1000 us または 100 us から選択します。

ここで設定する閾値と再解析のための閾値は、独立して管理されています。値を変更しても互いに影響しません。

マイクロバーストの再解析の詳細は **10.4.5. マイクロバーストの再解析** を参照してください。

11.ダッシュボード

ダッシュボード表示は、キャプチャしたデータを現在の時刻から遡った期間で、複数のグラフを 1 画面に表示します。表示可能な期間は、5 分、30 分、1 時間、8 時間、24 時間から選択できます。

ダッシュボードは、[ダッシュボード]メニューより確認できます。

ユーザごとにダッシュボードは、作成されます。他のアカウントで作成したダッシュボードは表示されません。

ダッシュボードの作成手順、グラフ種類、期間の指定について、説明します。

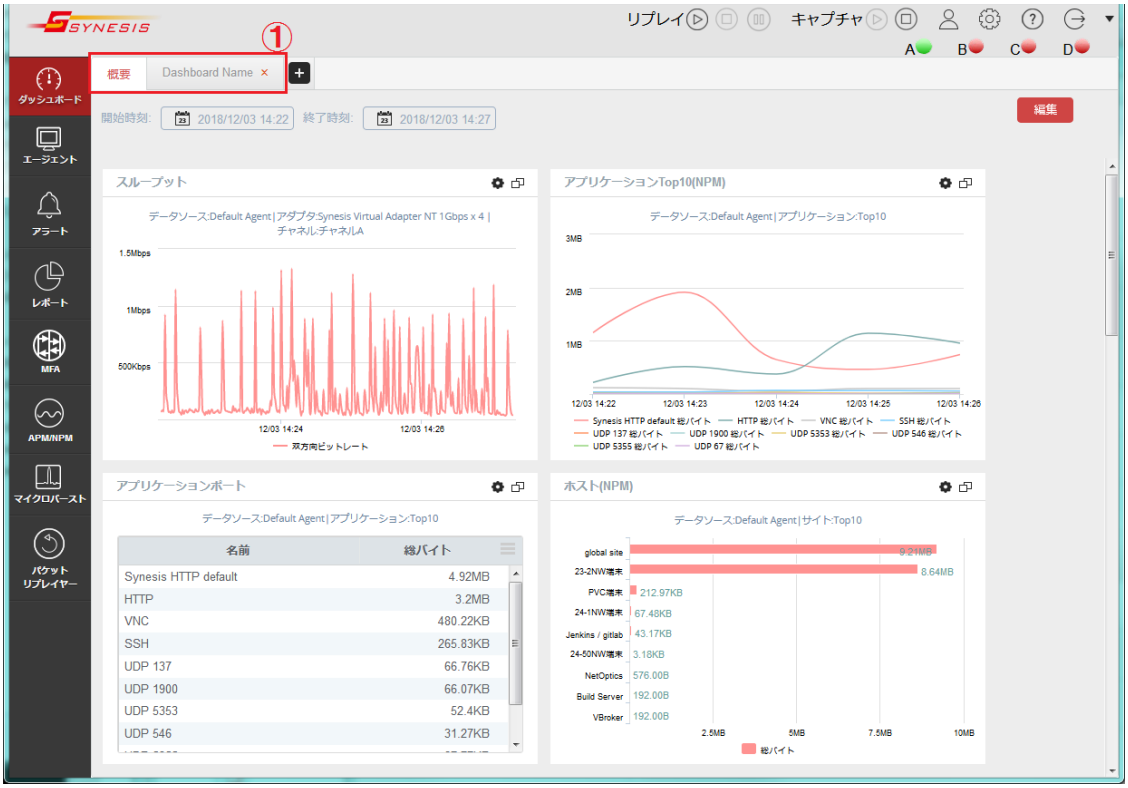


図 174：ダッシュボード

11.1. ダッシュボードの作成・管理

ダッシュボードの追加・削除は、編集モードかどうかにかかわらず実行できます。

手順は、以下の通りです。

- ダッシュボードの新規作成

1) ダッシュボードを新規に追加する場合は、[ダッシュボード]タブ>タブリスト右端にある ＋ ボタンをクリックします。

図 175：ダッシュボード・タブリスト

2)　下図の「新規ダッシュボード」ダイアログが表示されます。

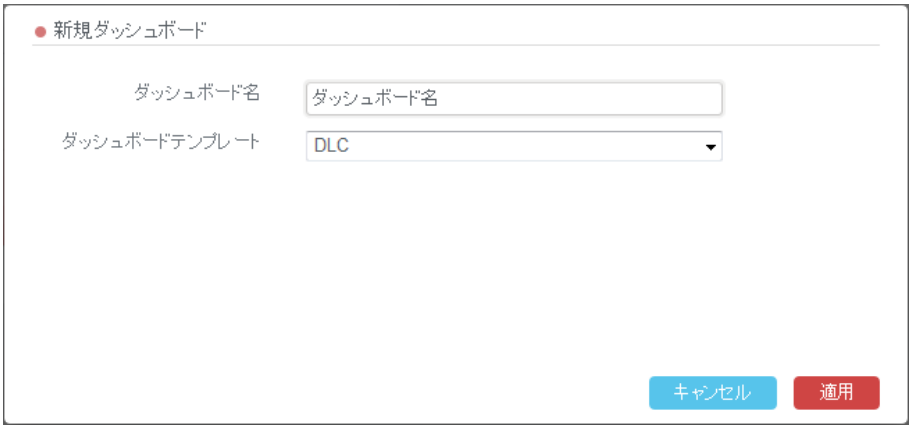


図 176：新規ダッシュボード・ダイアログ

「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、「ダッシュボードテンプレート」欄でテンプレートを選択します。

テンプレートは、「DLC」と「Top Site」の 2 種類のテンプレートを選択できます。

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

3)　[適用]ボタンをクリックします。 新しくダッシュボードが追加され、右側に指定した名前のタブが追加されます。

- ダッシュボードの削除

ダッシュボードを削除する場合は、該当のダッシュボード・タブの×ボタンをクリックします。 ×ボタンのない概要タブはデフォルトで作成されているタブであり削除できません

- 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する場合は、編集モードで表示される[リネーム]ボタンをクリックします。 下図の「ダッシュボードのリネーム」ダイアログが表示されます。

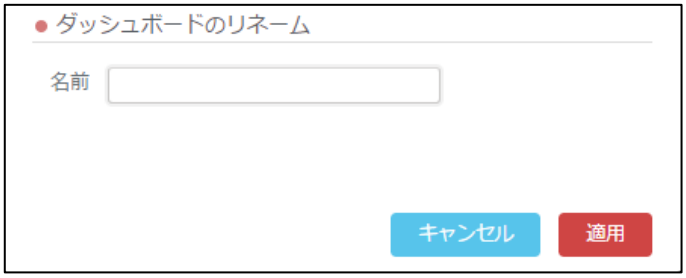


図 177：ダッシュボードのリネーム・ダイアログ

「名前」欄に新しい名前を入力し、[適用]ボタンをクリックします。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。

[保存]ボタンをクリックすると、元のダッシュボード画面に戻ります。

11.2. 新規グラフの追加と設定

ダッシュボードに追加できるグラフ種別と手順について、説明します。

11.2.1. 選択可能なグラフ種別

選択可能なグラフの種類は下記の通りです。

一部のグラフは、解析実行後データが反映されます。

リアルタイムでダッシュボードを確認する場合は、リアルタイム解析を有効にする必要があります。

有効手順は、キャプチャオプションの節を参照してください。

L2/L3 モジュール、APM 解析モジュール、NPM 解析モジュールの詳細は、解析の章を参照してください。

アドオン	サブリスト	グラフ種別	データの反映
DLC	–	折れ線グラフ	キャプチャ開始後
	イーサタイプ	表	L2/L3 プロトコルモジュール解析後
Net	IP プロトコル	表	L2/L3 プロトコルモジュール解析後
APM	Top N	棒グラフ 円グラフ 比較表 表	APM 解析モジュール解析後
	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	
NPM	Top N	棒グラフ 円グラフ 比較表 表	NPM 解析モジュール解析後
	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	

11.2.2. グラフの追加手順

1) グラフを追加するためにダッシュボードを編集モードに切り替えます。
ダッシュボード画面右上の[編集]ボタンをクリックし、編集モードにします。

2) 解析方法(アドオン)とグラフ種別を選択します。
画面左上のメニューでデータの解析方法(アドオン)を選択します。
グラフ種別のサブリスト(下図)が表示されますので、グラフ種別を選択します。

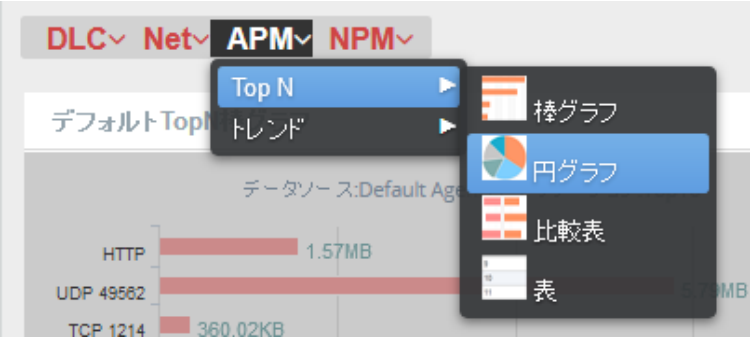


図 178：グラフ種別リスト

3) 表示データを指定します。
新規グラフ追加用画面で各項目を入力、選択します。

図 179：新規グラフ追加用画面

選択されたグラフ種別により設定項目は変わり、表示されるダイアログも異なります。 各設定項目の詳細は、**11.2.2. 新規グラフの設定項目**を参照してください。

項目入力後、[保存]ボタンをクリックすると、ダッシュボード上にグラフが追加されます。

追加したグラフの設定を変更する場合は、グラフの右上の ⚙ アイコンをクリックします。 詳細は、**11.2.1. グラフの設定変更** を参照してください。

削除する場合は、編集モードでグラフの右上の 🗑 アイコンをクリックします。

11.2.1. グラフの設定変更

編集モードでなくても、データソースや集計間隔の変更は可能です。

集計間隔を変更するする場合は、グラフ右上の⚙アイコンをクリックします。下図の「セットアップ構成」ダイアログが表示されます。

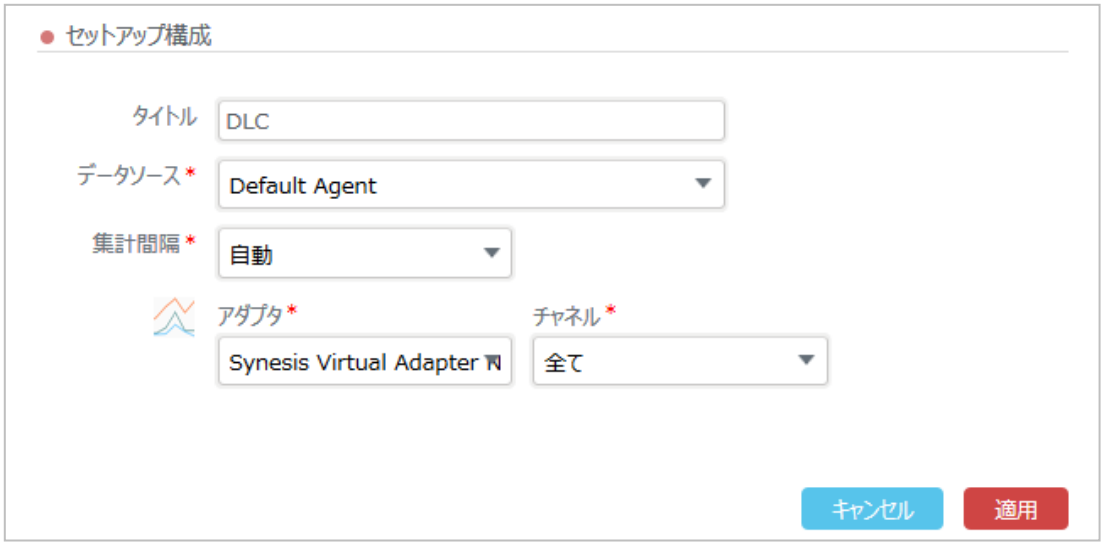


図 180 :「セットアップ構成」ダイアログ

各項目を変更した上で[適用]ボタンをクリックすると、グラフの設定が変更されます。

なお、グラフの種類や表示するデータの種類(アドオン)は変更できませんので、その場合は、グラフを削除して再度作成します。

変更可能な項目は、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。
データソース	選択できる項目は、「Default Agent」のみです。
集計間隔	時系列グラフの集計間隔です。以下が選択可能な値です。 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	現在選択されているアダプタ(キャプチャカード)です。 SYNESIS に組み込まれている選択可能なアダプタが表示されます。
チャネル	現在選択されているチャネルです。 選択可能なチャネルが表示されます。 任意のチャネル、または全てのチャネルが選択できます。

11.2.2. 新規グラフの設定項目

設定項目は、以下の通りです。グラフの種類によって表示される項目は異なります。

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	グラフデータの解析方法です。グラフ種別選択時に指定します。
タイプ	データの抽出方法です。 選択可能な項目はサイト、サーバ、サーバグループ、 アプリケーション、アプリケーショングループの 5 種類です。
範囲	「タイプ」で指定した条件によって抽出されたデータを、「範囲」で指定した項目でさらにフィルタします。 「タイプ」でアプリケーションを選択した時はサイトに、 サイトを選択した場合にはアプリケーションに固定されます。 その他の「タイプ」を指定した場合には表示されません。
インデックス	グラフに表示する KPI です。 左側のリストは利用可能な KPI で、右側のリストが実際にグラフに表示される KPI です。 左側のリストで 1 つ以上の KPI を選択し、 >> アイコンをクリックすると、選択したデータが右側のリストに移動します。 右側のリストから削除する場合は、右側のリストで削除する KPI を選択し、 << アイコンをクリックするとデータが左側のリストに移動します。
上限を固定する	有効にした場合、プロットされた KPI の上限を設定できます。 実際のプロット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。 チェックボックスで有効・無効を切り替えることができます。
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、桁数の表示(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 までです。 ただし、単位を「sec」にした場合の最大値は 100,000 になります。

11.3. 画面の操作方法

ダッシュボード画面の操作方法について、説明します。

11.3.1. 時間範囲の選択

ダッシュボード画面は、現在の時刻から指定した期間の通信状況や統計情報が表示されます。

画面左上の「開始時刻」または「終了時刻」の部分をクリックすると、下図のダイアログが表示されます。

図 181：表示時間選択ダイアログ

希望の表示期間を選択してクリックします。

選択可能な表示期間は 5 分、30 分、1 時間、8 時間、24 時間です。

11.3.2. グラフの拡大表示

ダッシュボード上に表示されている各グラフの右上には「 新しいウィンドウで開く」アイコンと、グラフや表の設定が変更できる「プロファイルの設定」アイコンが配置されています。

アイコンをクリックすると、 下図のようにグラフが別ウィンドウで拡大表示されます。

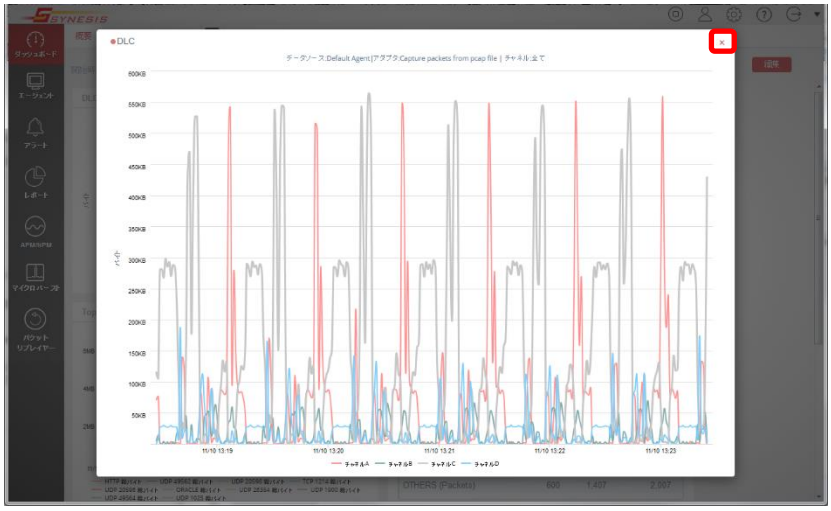


図 182：別ウィンドウで拡大表示

グラフ右上の×ボタンをクリックすると拡大表示中のウィンドウが閉じられます。

アイコンをクリックするとグラフの設定画面が表示されます。

詳細は **11.2.1. グラフの設定変更** を参照してください。

11.3.3.　各チャネルデータの表示/非表示の切替え

グラフ下部に表示された項目（下図②）をクリックすることで、対象となるデータの表示/非表示を切り替えることができます。

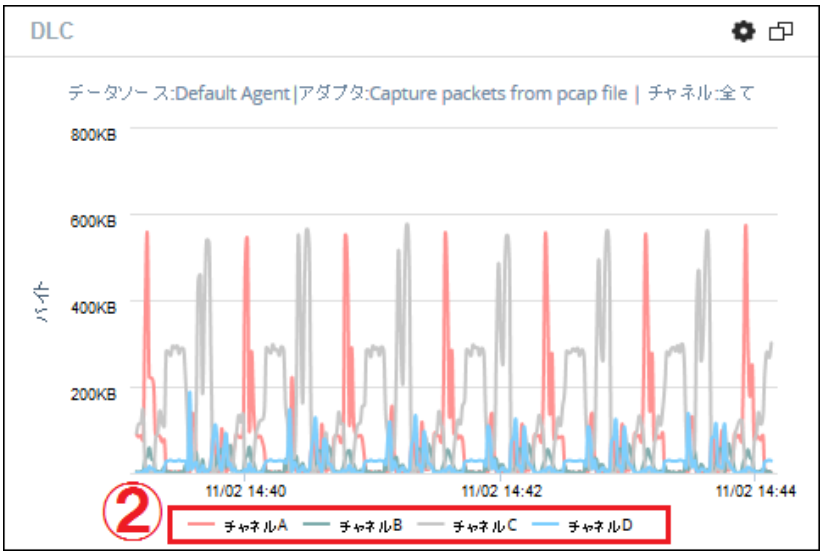


図 183：チャネルの表示/非表示選択

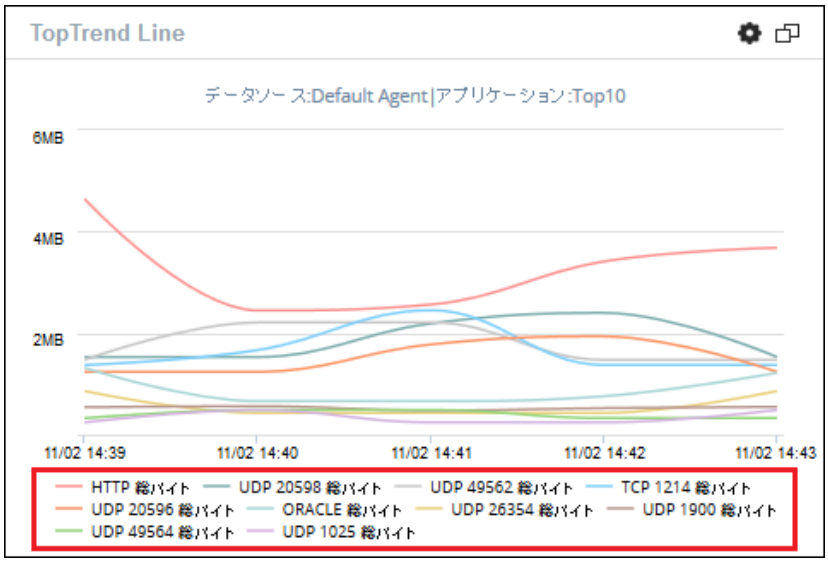


図 184：データの表示/非表示選択

11.3.4.　配置可能なグラフ数

１ページのダッシュボード上に大量のグラフを追加すると、動作が極端に遅くなるなどの問題を引き起こす可能性があります。

その問題を回避するため、モデルごとに配置可能なグラフの数の推奨値が提示されています。 推奨値を超えるグラフを作成する場合は、新規にダッシュボードを追加しグラフを追加してください。

ご使用モデルでのグラフ数の推奨値は SYNESIS の諸元一覧を参照してください。

11.4. ダッシュボードのグラフに関する制限事項

- ダッシュボード画面のトレンドグラフで、集計のタイミングによっては右端のプロットが 0 になる場合があります。

12.レポート

レポートは、キャプチャしたデータをレポート形式で表示する機能です。

レポートは、[レポート]メニューより確認できます。

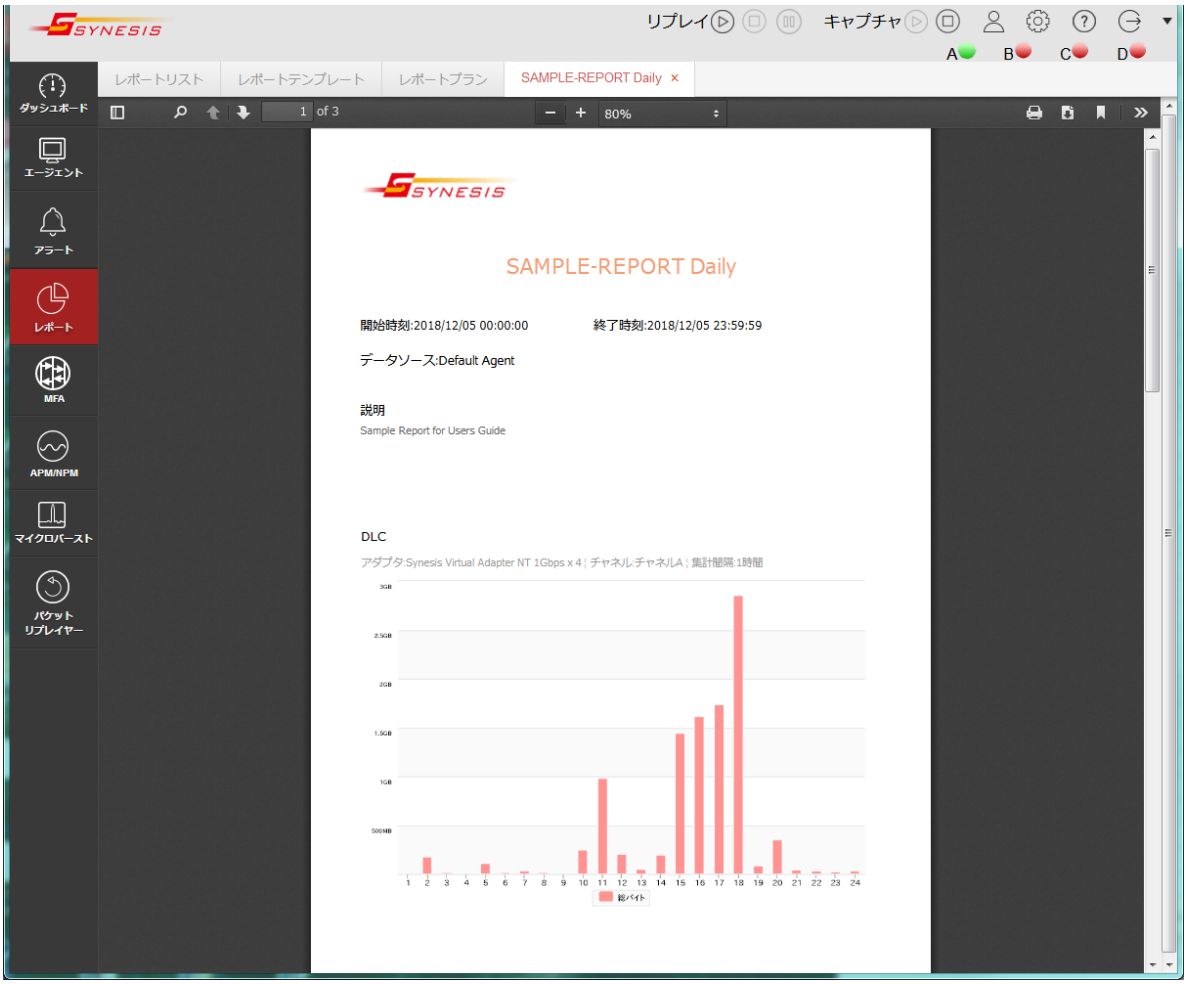


図 185 :「レポート」メニュー画面

レポートの作成手順、グラフ種類について説明します。

レポートの作成までの流れは、以下の通りです。

1. [レポートテンプレート]タブで必要なレポートのテンプレートを作成
2. [レポートプラン]タブでテンプレートをどのように反映するかを設定
3. [レポートリスト]タブで作成されたレポートの一覧

12.1. レポートテンプレート

レポートテンプレートでは、レポートに記載するグラフや表の種類や、レイアウトを設定できます。レポートテンプレートの作成・管理は[レポート]メニュー>[レポートテンプレート]タブで行います。

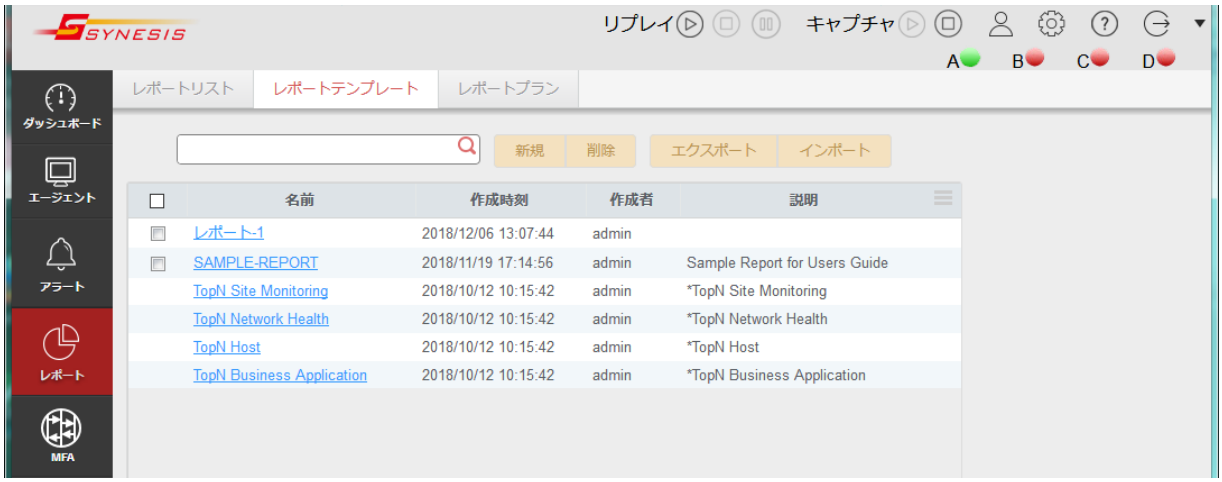


図 186 :「レポートテンプレート」画面

作成済のレポートテンプレートは、一覧で表示されます。

確認できる情報は各テンプレートの「名前」、「作成時刻」、「作成者」、「説明」です。

12.1.1. レポートテンプレートの作成・管理

- レポートテンプレートの作成

[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。

図 187 :「新規テンプレート」画面

画面左のグラフ・ペインからレポートに記載するグラフを選んでクリックし、レポートの空白部分までドラッグします。ドロップした位置にドラッグしたグラフが配置されます。

[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。

編集可能な項目と操作手順は、以下の通りです。

項目	説明
グラフの種類	レポートに記載するグラフの種類を選択できます。 左側のグラフ・ペインから記載するグラフをクリックして選び、レポート上にドラッグ＆ドロップします。 選択可能なグラフの種類や設定方法は、**12.1.2. 選択可能なグラフの種類** を参照してください。 グラフ追加後にグラフの位置を入れ替えることは可能です。
グラフの設定	グラフや表に記載するデータを指定することができます。 レポート上にグラフを配置すると、グラフの設定ダイアログが表示されます。 詳細は、**12.1.3. 新規グラフの設定項目** を参照してください。
レポートタイトル	レポートのタイトルや、その下の説明文を編集することが可能です。 「レポート-#(数字)」と書かれた部分をクリックすると、レポートタイトルが編集できます。「説明を入力してください」と書かれた部分をクリックすると、説明文を編集できます。
レポートロゴ	ロゴ画像を挿入することができます。 詳細は、**12.1.4. レポートロゴの変更** を参照してください。

- レポートテンプレートの検索

レポートテンプレートを検索することが可能です。

検索フィールドにマッチする文字列を入力し、 アイコンを クリックします。入力した文字列と名前の一部が一致するレポートテンプレートがリストアップされます。

- レポートテンプレートの削除

レポートテンプレートを削除する場合は、該当するレポートテンプレートにチェックを入れ、[削除]ボタンをクリックします。削除の確認メッセージが表示されますので、「はい」ボタンをクリックすると、チェックを付けたレポートテンプレートが削除されます。

全てのレポートテンプレートを削除する場合は、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ます。

チェックボックスが表示されていないレポートテンプレートはデフォルトで登録されているテンプレートのため削除できません。

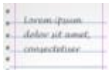
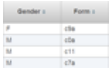
また、レポートプランで使用されているレポートテンプレートも削除できません。使用中のテンプレートを削除する場合は、そのテンプレートを使用しているレポートプランを全て削除した上で、削除作業を行ってください。

- レポートテンプレートの編集

登録済みのレポートテンプレートを編集する場合は、該当するレポートテンプレートの「名前」リンクをクリックします。「テンプレートの表示」画面が表示され、編集が可能になります。

12.1.2.　選択可能なグラフの種類

選択できるレポートの要素は以下の通りです。

アイコン	項目	アドオン
	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

グラフのアイコンをドラッグ＆ドロップしてレポート上に配置すると、グラフの設定ダイアログが表示されます。設定ダイアログで、グラフに記載するデータを設定することができます。

詳細は、次項の **新規グラフの設定項目** を参照してください。

12.1.3.　新規グラフの設定項目

レポート上に新しいグラフを配置すると、以下のようなグラフの設定ダイアログが表示されます。

図 188：グラフ設定ダイアログ

グラフの種類によって設定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	グラフの解析方法です。
タイプ	ドロップダウンリストから、データの抽出方法を指定します。 選択可能な項目はサイト、サーバ、サーバ グループ、アプリケーション、アプリケーショングループの 5 種類です。
範囲	「タイプ」で指定した条件によって抽出されたデータを、「範囲」で指定した項目でさらに絞り込みます。 「タイプ」でアプリケーションを選択した時はサイトに、 サイトを選択した場合にはアプリケーションに固定されます。 その他の「タイプ」を指定した場合には、表示されません。
インデックス	グラフに表示する KPI です。グラフや表の種類によっては複数選択可能です。 左側のリストは利用可能な KPI で、右側のリストが実際にグラフに表示される KPI です。 左側のリストで 1 つ以上の KPI を選択し、>> アイコンをクリックすると、選択したデータが右側のリストに移動します。 右側のリストから削除する場合は、右側のリストで削除する KPI を選択して、<< アイコンをクリックすると、データが左側のリストに移動します。
上限を固定する	有効にした場合、プロットされた KPI の上限を設定できます。 実際のプロット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。 チェックボックスで有効・無効を切り替えることができます。
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、桁数の表示(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 までです。 ただし、単位を「sec」にした場合の最大値は 100,000 になります。

12.1.4. 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 をクリックすると、下図のロゴ設定ダイアログが表示されます。

図 189：「ロゴの設定」画面

[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ます。[アップロード]ボタンをクリックすると、画面中央に選んだ画像が表示されます。

[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は、選択した画像になります。

ロゴに指定する画像のサイズは、50 x 200 ピクセル以下にしてください。

12.1.5. レポートテンプレートのエクスポートとインポート

- レポートテンプレートのエクスポート

レポートテンプレートはエクスポートすることができ、別筐体の SYNESIS で利用することが可能です。

レポートテンプレートのエクスポート手順は、以下の通りです。

1) エクスポートする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ます。
2) 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ます。 「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指定したフォルダに保存されます。

- レポートテンプレートのインポート

別筐体の SYNESIS で作成されたレポートテンプレートをインポートすることができます。

レポートテンプレートのインポート手順は、以下の通りです。

1) [インポート]ボタンをクリックし、作成済のレポートテンプレートを指定します。
2) [アップロード]ボタンをクリックすると、指定したレポートテンプレートが追加されます。

12.2. レポートプラン

レポートプランでは、レポートテンプレートにデータをどのように反映させるかを設定します。

レポートプランの作成・管理は、[レポート]メニュー>[レポートプラン]タブで行います。

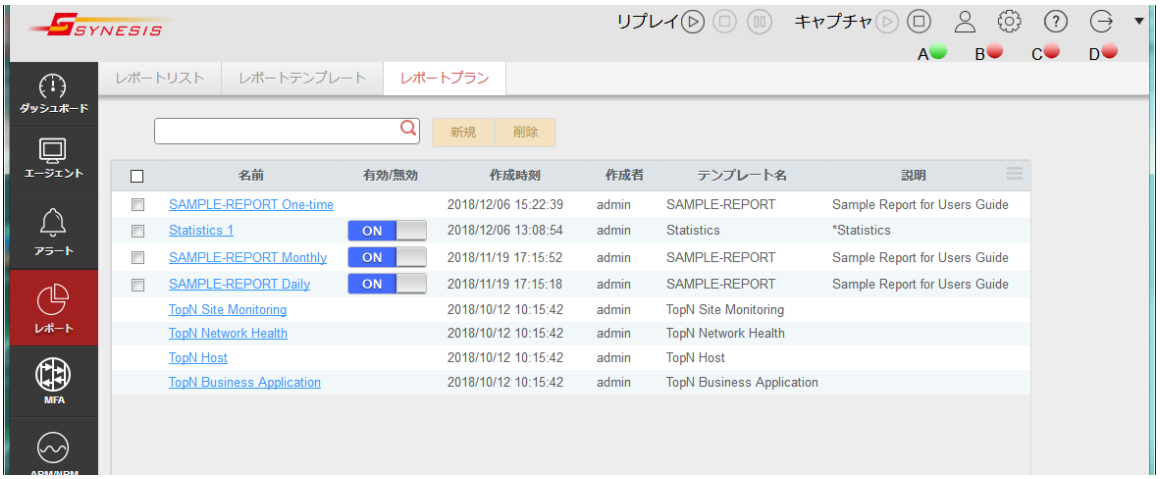


図 190 : [レポートプラン]タブ

12.2.1. レポートプランの作成・管理

- レポートプランの作成

新しいレポートプランを作成する場合は、[新規]ボタンをクリックします。

下図の「新規プランの作成」画面が表示されます。

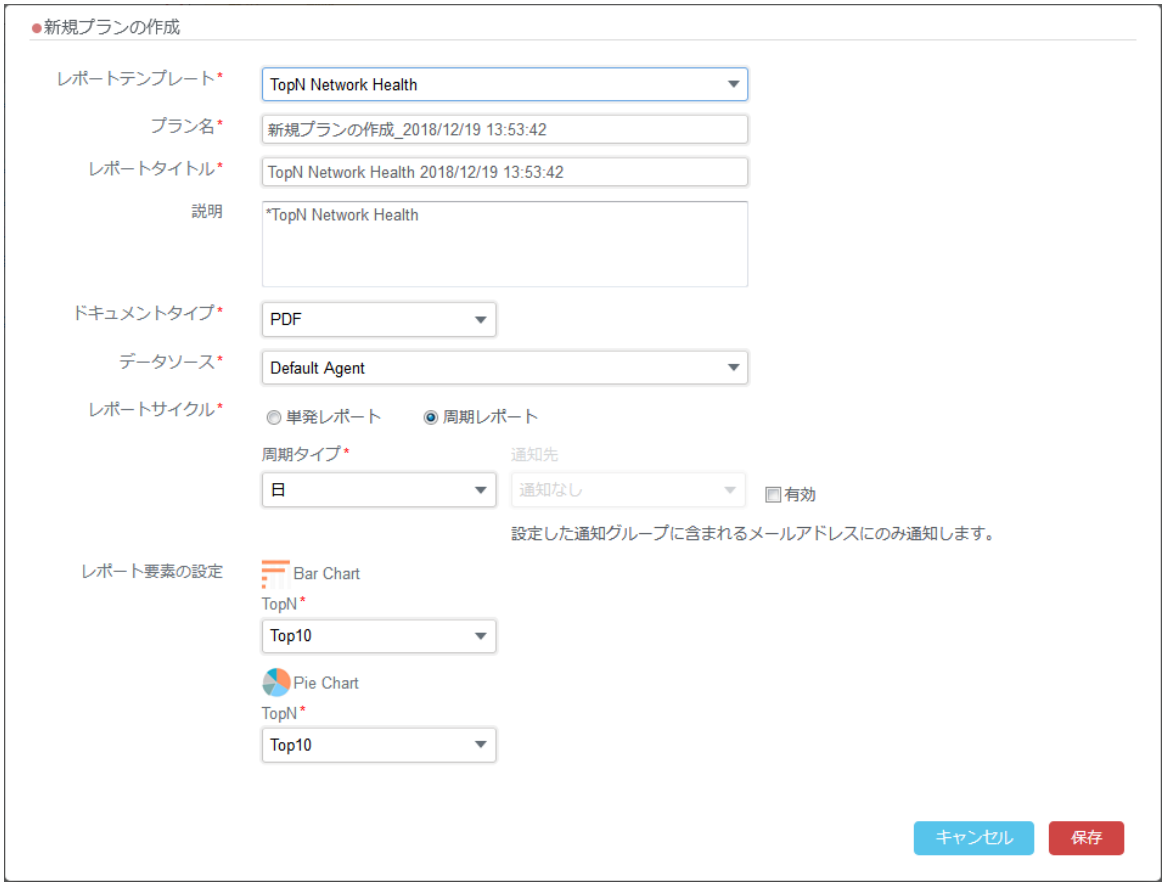


図 191 :「新規プランの作成」画面

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」を選択した場合は、[保存]ボタンをクリックした際に作成したレポートが表示されます。

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です。 作成済のレポートプランを選択します。 統計情報を CSV ファイルで出力する場合は、「Statistics」を選択します。
プラン名	レポートプランの名前です。
レポートタイトル	レポートのタイトルです。
説明	レポートプランリストの「説明」欄に表示される説明です。
ドキュメントタイプ	作成されるレポートのファイル形式です。 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」を選択した場合、CSV ファイルになります。
データソース	選択できる項目は、「Default Agent」のみです。
レポートサイクル	レポートが作成されるタイミングです。 単発レポートまた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、単発レポートの設定と周期レポートの設定を参照してください。
集計間隔	トレンドグラフや統計情報のデータの集計間隔を設定します。 指定したレポート・テンプレート(「Statistics」以外)にトレンドグラフがない場合は、この「集計間隔」の項目は表示されません。 なお、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、単発レポートの設定と周期レポートの設定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設定を行います。

- レポートプランの検索

レポートプランを名前で検索可能です。

検索フィールドにマッチする文字列を入力し、 アイコンを クリックします。入力した文字列と名前の一部が一致するレポートプランがリストアップされます。

- レポートプランの削除

レポートプランを削除する場合は、該当するレポートプランにチェックを入れ、[削除]ボタンをクリックします。削除の確認メッセージが表示されます。「はい」をクリックすると、チェックを付けたレポートプランが削除されます。

全てのレポートプランを削除する場合は、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ます。

チェックボックスが表示されていないレポートプランは、デフォルトで登録されているプランのため削除できません。

● レポートプランの編集

登録済みのレポートプランを編集する場合は、該当のレポートプランの「名前」リンクをクリックします。「プランの表示」画面が表示されます。「レポートテンプレート」以外の項目が変更可能です。

12.2.2. 単発レポートと周期レポート

レポートサイクルでは、「単発レポート」か「周期レポート」が選択できます。

● 単発レポート

キャプチャしたデータからレポートを作成する場合は、「レポートサイクル」の項目で「単発レポート」を選択し、データの時間範囲を指定します。

図 192：単発レポート指定画面

設定項目の詳細は、以下の通りです。

項目	説明
開始時刻	レポートの開始時刻です。 手入力またはカレンダーアイコンから指定します。
終了時刻	レポートの終了時刻です。 手入力またはカレンダーアイコンから指定します。
集計間隔	データの集計間隔を指定します。 選択できる集計間隔は、以下の通りです。 自動、5 分、30 分、1 時間、2 時間、8 時間、1 日、1 週間、1 ヶ月 開始時刻と終了時刻の範囲内のデータが、指定した集計間隔で集計されます。 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。

● 周期レポート

指定した周期ごとに自動的にレポートを作成する場合は、「レポートサイクル」の項目で「周期レポート」を選択し、「周期タイプ」を指定します。

図 193：周期レポート指定画面

設定項目は、以下の通りです。

項目	説明
周期タイプ	レポートを作成する周期を指定します。 選択可能な周期タイプと、レポートが生成されるタイミングは以下の通りです。 「日」：毎日午前 2:00 「週」：毎週日曜日の午前 2:00 「月」：毎月 1 日の午前 2:00 「年」：毎年 1 月 1 日の午前 2:00
集計間隔	トレンドグラフのデータの集計間隔を指定します。 周期タイプにより、選択可能な集計間隔は異なります。 周期タイプ【日】：自動、5 分、30 分、1 時間 周期タイプ【週】：自動、30 分、1 時間、1 日 周期タイプ【月】：自動、2 時間、8 時間、1 日 周期タイプ【年】：自動、1 日、1 週間、1 ヶ月 指定したレポートテンプレートにトレンドグラフがない場合は、「集計間隔」の項目は表示されません。
通知先	周期レポートが自動作成された際に、指定した「通知グループ」の 「通知先」宛に通知メールが送信されます。 通知は E-mail のみで Trap と Syslog には通知されません。 「通知先」の登録方法は **14.3.1. 通知先の設定** と **14.3.2. 通知グループの設定** を参照してください。
有効	チェックボックスにチェックを入れると、「通知先」が有効になります。 「通知先」の設定は、**14.3. 通知** を参照ください。

周期レポートプランは、レポートプラン一覧の「有効/無効」欄にステータスを表す ON/OFF アイコンが表示されています。

-

：無効状態。自動的にレポートは作成されません。
-

：有効状態。自動的にレポートが作成されます。

有効/無効はクリックで切り替えられます。

12.2.3. 統計情報レポートの CSV ファイルで出力

バイトやパケット数などの統計情報を自動的に CSV ファイルで出力させることが可能です。統計情報を CSV で出力させる場合は、レポートテンプレートの項目で「Statistics」を指定します。

この CSV ファイルを作成する際に選択できるレポート種別は、「周期レポート」のみです。

任意の期間で統計情報の CSV ファイルを作成する場合は、エージェント・ワークスペースの[レコード]タブより作成する必要があります。

詳細は、**8.2. 統計のエクスポート**を参照してください。

12.3. レポートリスト

[レポート]メニュー>[レポートリスト]タブでは、SYNESIS 内に保存されたレポートの閲覧・検索・削除が行えます。

図 194：レポートリスト画面

保存されたレポートは、一覧で表示されます。保存したレポートを閲覧する場合は、レポートの名前のリンク部分をクリックします。

レポート一覧で確認できる情報は、以下の通りです。

項目	説明
名前	レポートの名前です。
レポートサイクル	レポート種別です。
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	レポートのドキュメントタイプです。
作成者	レポートの作成者です。レポートテンプレートを作成したユーザが作成者になります。

12.3.1. 作成されたレポートの管理

- レポートの検索

保存されたレポートの名前で検索可能です。

検索フィールドにマッチする文字列を入力し、 アイコンを クリックします。入力した文字列と名前の一部が一致するレポートプランがリストアップされます。

- レポートの削除

レポート削除する場合は、該当のレポートにチェックを入れ、[削除]ボタンをクリックします。削除の確認メッセージが表示されます。「はい」をクリックすると、チェックを付けたレポートプランが削除されます。

全てのレポートプランを削除する場合は、「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ます。

12.3.2. 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/

このフォルダは SYNESIS 内でユーザが作成したデータが保存される**データバンク領域**にあります。

詳細は、**2.3.3. データバンク領域**を参照してください。

12.4. サンプルレポート

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・設定方法は **12.1. レポートテンプレート** を参照してください。

[レポート例]

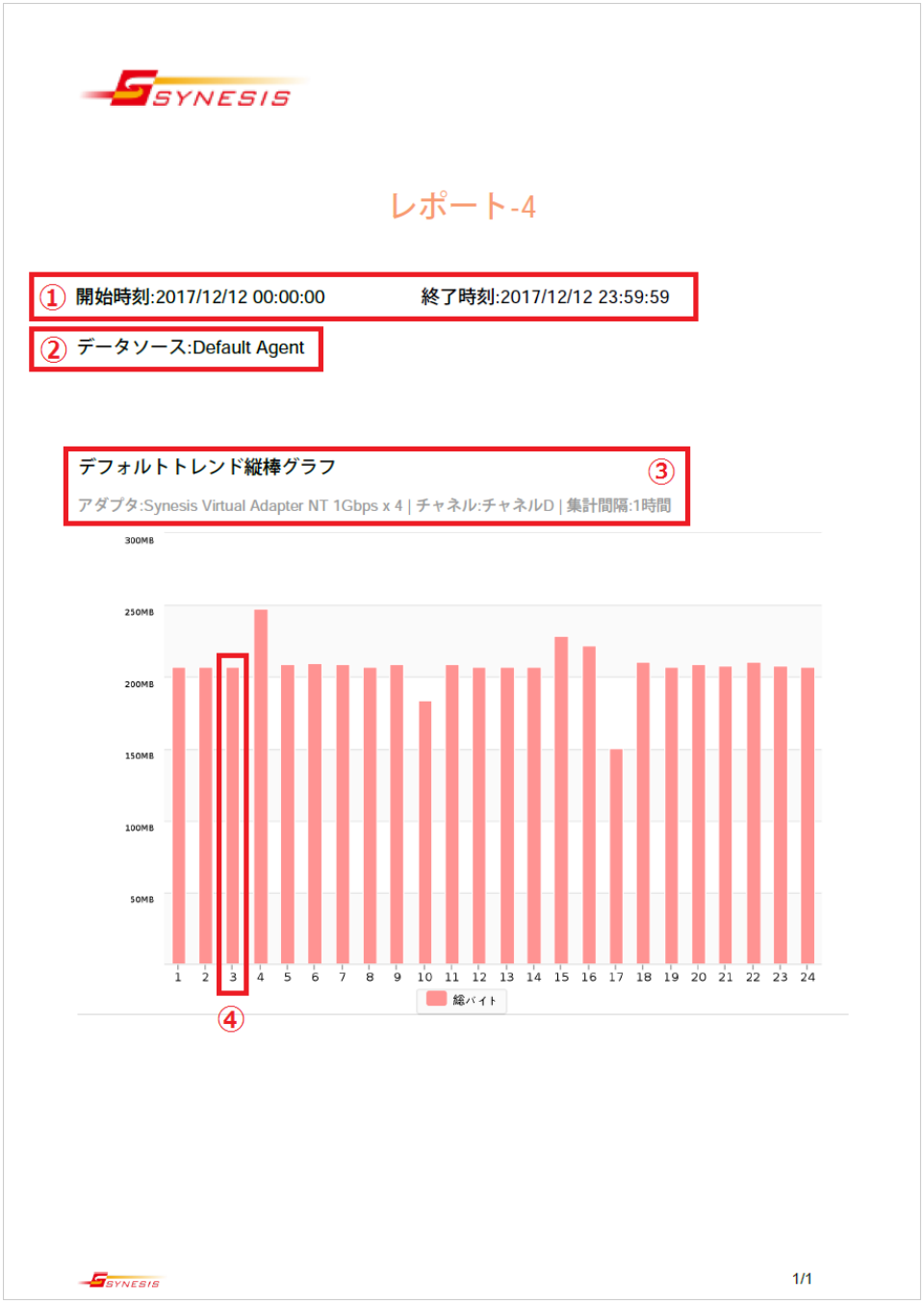


図 195：レポート例

例として、下記の項目がレポートに記載されます。

レポート要素		説明
①	**開始時刻と終了時刻**	解析したキャプチャデータの期間が、開始時刻と終了時刻として yyyy/mm/dd hh:mm:ss の形式で記載されます。
②	**データソース**	レポートのデータをキャプチャした SYNESIS のエージェント名で、「Default Agent」と記載されます。
③	**各グラフや表の情報**	そのグラフや表の種類、アダプタ、チャネル、集計間隔が記載されます。

④	**集計間隔と集計期間**	横軸に時間が設定されているグラフでは、指定した集計間隔で期間を区切ってデータの集計が行われます。 集計される期間は、データラベルに表示される時刻より集計間隔で指定された期間だけ前の時刻から、その時刻になる直前までです。 例えば、集計間隔 1 時間のグラフでは、02:00:00～02:59:59 のデータが 3:00 の位置にプロットされます。

12.4.1. デイリー・レポート例

「レポートプラン」作成時にレポートサイクル「周期レポート」を選択し、周期タイプ「日」を選択すると、 毎日午前 2：00 に前日の 00：00：00 から 23：59：59 までの集計結果をまとめた以下のようなデイリー・レポートが作成されます。

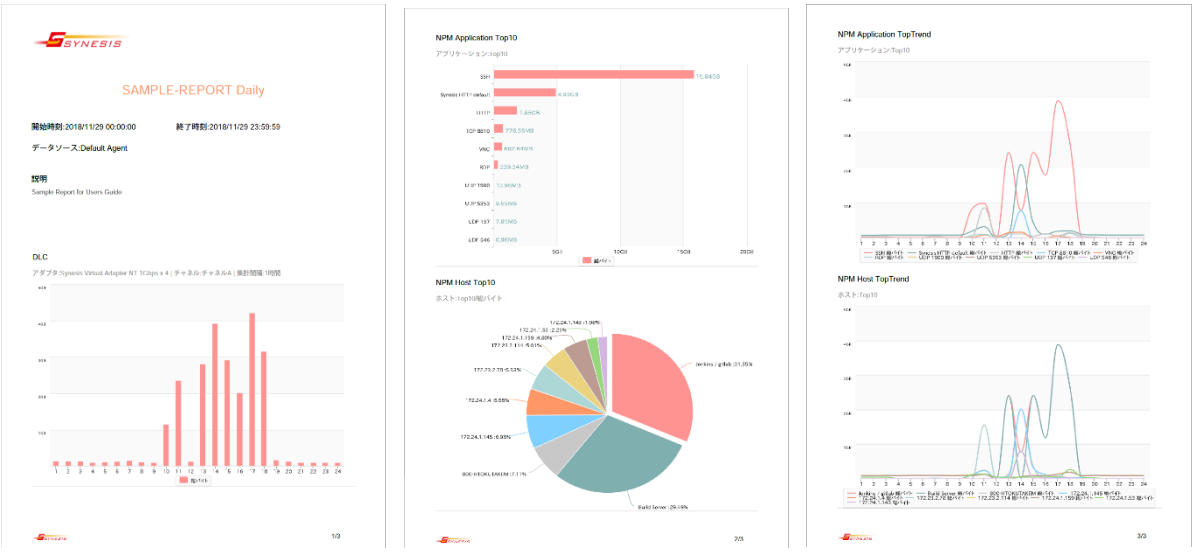


図 196：デイリー・レポート例

12.4.2. マンスリー・レポート例

「レポートプラン」作成時にレポートサイクル「周期レポート」を選択し、周期タイプ「月」を選択すると、 毎月 1 日午前 2：00 に前月の 1 日 00：00：00 から前月末日の 23：59：59 までの集計結果をまとめた以下のような マンスリー・レポートが作成されます。

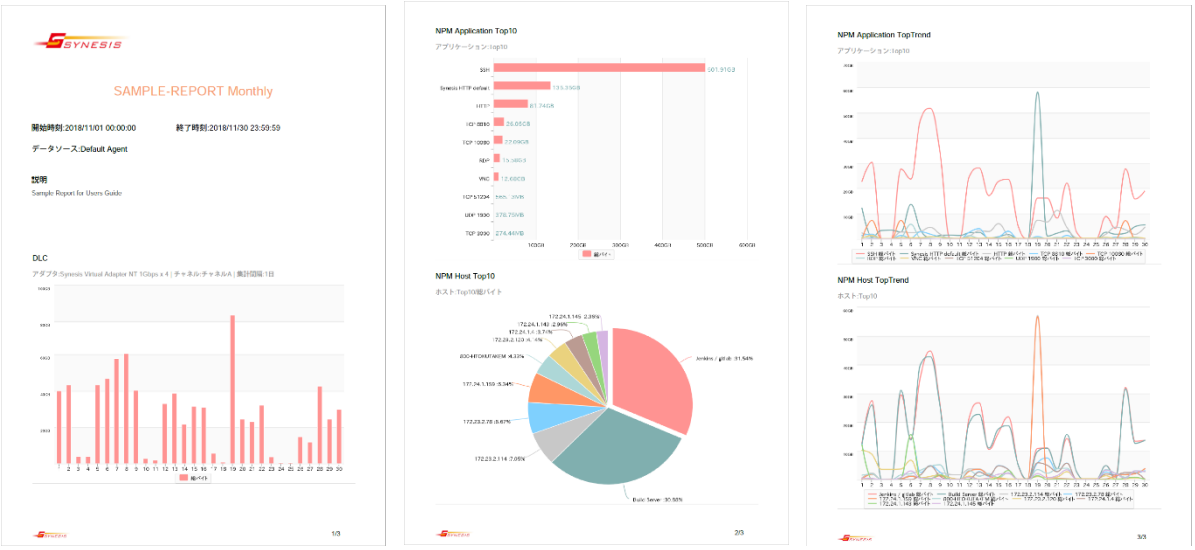


図 197：マンスリー・レポート例

12.5. レポートに関する制限事項

- 周期レポートおよび単発レポートで、集計間隔が 1 ヶ月のグラフは、正しく描画されない場合があります。
- 周期レポート機能でトレンドグラフを生成すると、時間範囲の最終時刻を X 軸の値としてプロットします。例えば集計間隔 1 日のグラフで、1/1 0:00 から 1/2 0:00 のデータ点は、横軸が 1/2 の位置にプロットされます。

13. MFA(マルチフロー解析)

MFA(マルチフロー解析/Multi Flow Analysis)は、キャプチャデータごとにキャプチャポイントを定義し、フローを抽出して図示する機能です。

フローとは、IP アドレスおよび TCP/UDP ポート番号の送受信ペアをさします。MFA では、フローをクライアントとサーバに分類し、フローごとの挙動がパケット単位で確認できます。

MFA では、フローはラダー図(下図①)で表示され、視覚的なトラブルシューティングが行えます。

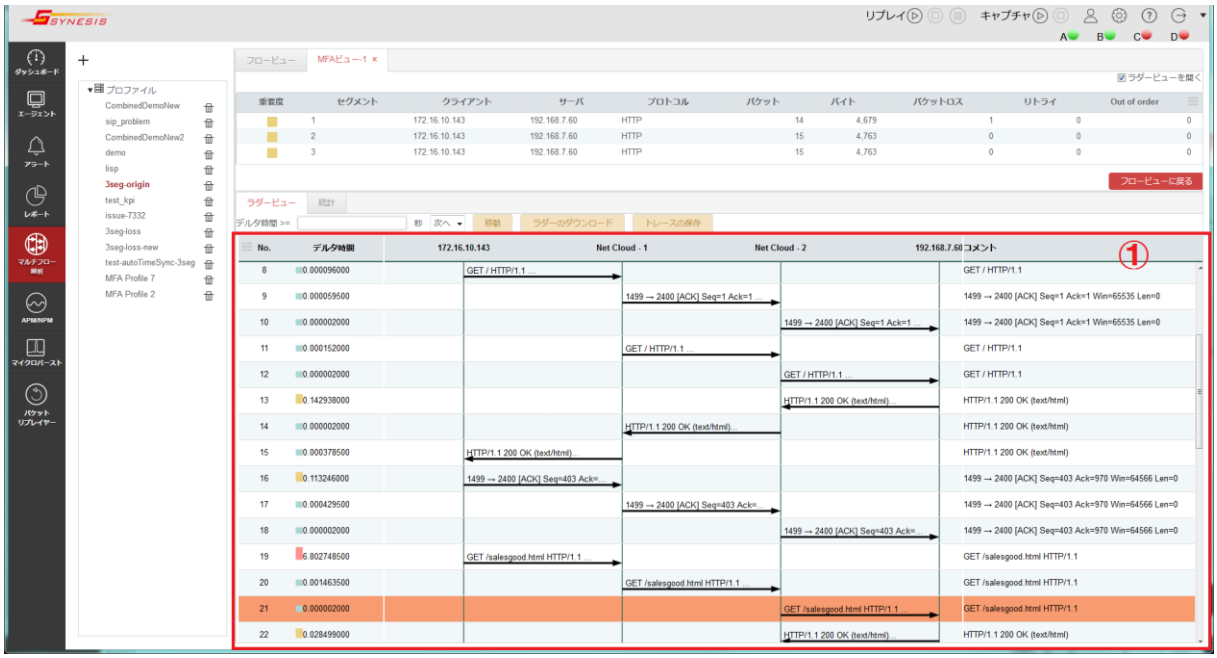


図 198 : [MFA]メニュー画面

MFA の表示方法、定義、手順について説明します。

13.1. MFA 機能の概要

MFA の作成、結果の閲覧は、[MFA]メニューから行います。

- MFA 機能の表示

MFA には、以下 3 つの表示があります。

1. フロービュー

マージされたデータソースに含まれる通信をプロトコル、サーバごとに分類して、フロー単位で表示します。

表示されたフローの中から、MFA ビューやパケットロス解析を行うためのフローを選択します。

詳細は、**13.2. フロービュー** を参照してください。

2. MFA ビュー

フロービューで選択されたフローを、まとめてひとつのラダー図で表示します。

詳細は、**13.3. MFA ビュー** を参照してください。

3.　パケットロス解析の表示

複数のセグメント同一フローについて、セグメントごとにパケット数を比較し、パケットロスを検出します。

詳細は、**13.4. パケットロス解析** を参照してください。

- マージ可能なデータソース

MFA で各種表示を行うためには、データソースをマージすることが必要です。

表示可能なデータソースは、以下の通りです。

  - ビルトインファイル、カスタムファイル、トレースバンカーに保存されているトレースファイル
  - SYNESIS でキャプチャされたレコード

データソースの制限については、**13.1.5. データソースと制限** を参照ください。

- MFA の各種画面から可能な操作

MFA の各種画面から可能な操作は、以下の通りです。

  - ラダー図の表示、図のダウンロード(JPEG、PNG、TXT 形式)
  - 関連するパケットのデコード表示
  - 関連するパケットのトレースの保存
  - パケットロス・テーブル結果の CSV ファイルの作成、ダウンロード

ラダー図の仕様については、**13.1.2. ラダービュータブ** を参照ください。

13.1.1.　プロファイルの作成・管理

MFA で各種表示を行うためには、表示するデータソースの選択や各種条件を設定したプロファイルを作成する必要があります。作成したプロファイルをマージすることにより、データソースに含まれる通信をプロトコル、サーバごとのフローに分類します。

プロファイルの作成手順は、以下の通りです。

- プロファイルの作成

1)　プロファイル・ペイン左上に表示されている[追加] ＋アイコンをクリックします。

図 199：プロファイル追加アイコン

2) 以下の「MFA プロファイル」ダイアログが表示されます。[追加]ボタン(下図①)をクリックします。

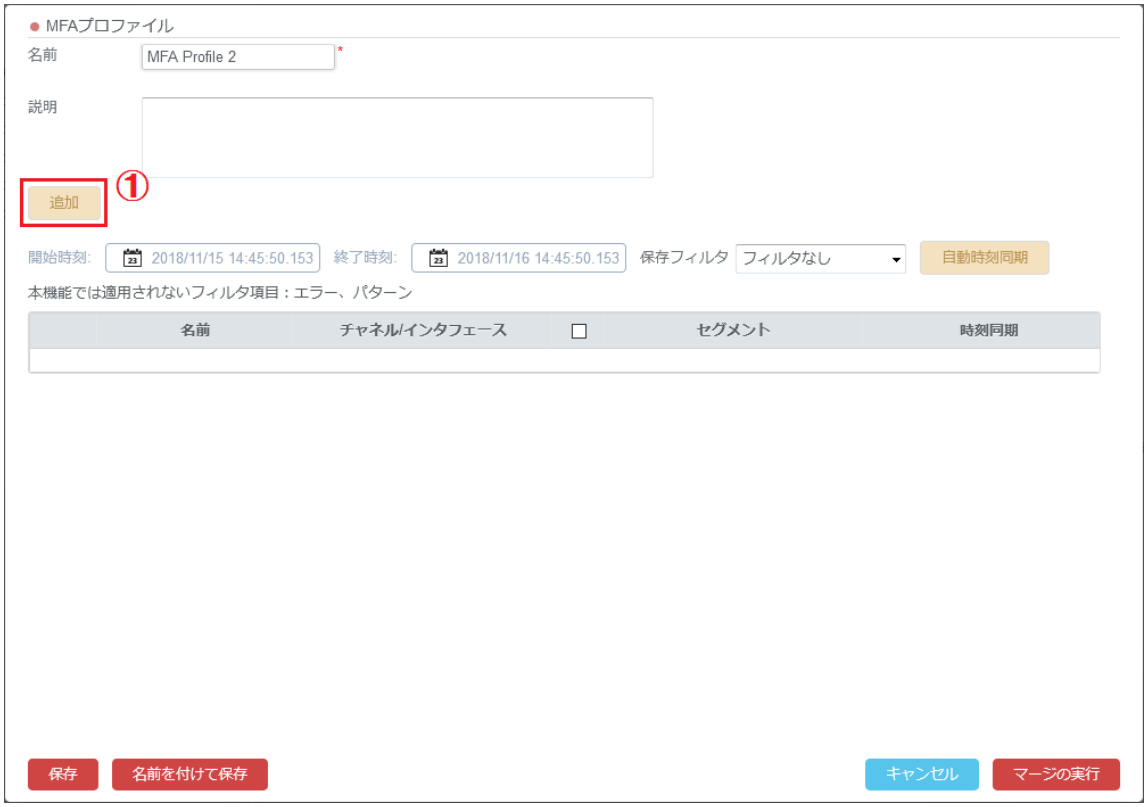


図 200：MFA プロファイル・ダイアログ

3) 選択可能なトレースファイルとキャプチャレコードが表示されます(下図②)。リストの中からデータソースを選択し、「選択する」リンクをクリックします。

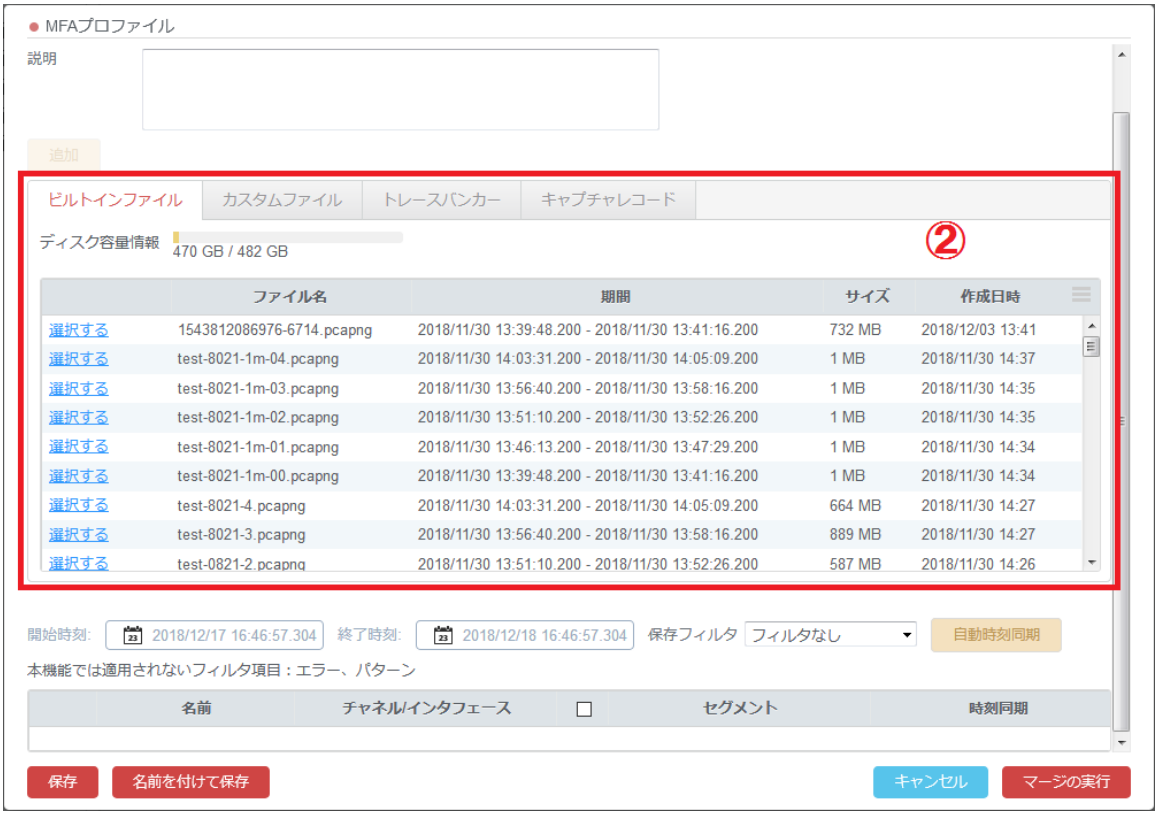


図 201：選択可能なトレースファイル

4) 選択したファイルがダイアログの下部にあるデータソースリストに追加され、「選択する」リンクの表示が「選択中」に変わります。

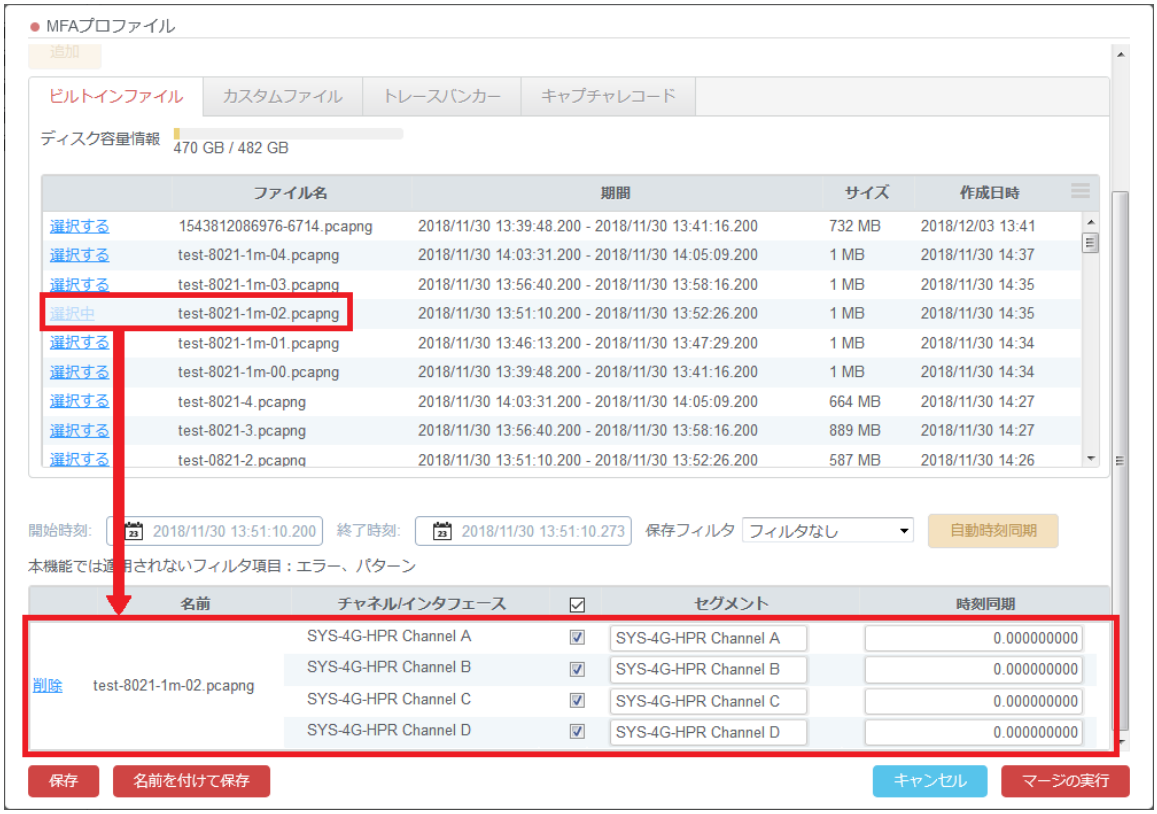


図 202：フロー選択中

データソースリストに追加したファイルを削除する場合は、該当するファイルの「削除」リンクをクリックします。

MFA プロファイルの設定は、以下の通りです。

項目	説明
名前	プロファイルの名前です。
説明	プロファイルの説明です。
[追加]ボタン	クリックすると、データソースとして選択可能なトレースファイル、レコードのリストが表示されます。
開始時刻	マージの実行を行う開始時間です。 初期設定では、データソースに含まれる最も古いパケットの時刻が設定されます。時刻同期が行われている場合は、調整後の時刻が表示されます。 手入力で変更することが可能です。
終了時刻	マージの実行を行う終了時間です。 初期設定では、データソースに含まれる最も新しいパケットの時刻が設定されます。時刻同期が行われている場合は、調整後の時刻が表示されます。 手入力で変更することが可能です。

<table>
<tr><td colspan="2">保存フィルタ</td><td>データソース全体に対する保存フィルタです。
設定した場合、マージの段階でこのフィルタが適用されます。
この画面のフィルタでは、エラーフィルタとパターンフィルタは適用できません。
また、SIP と RTP が異なったチャネルでキャプチャされた場合は、VoIP フィルタが適用できません。
詳細は、6.4. 保存フィルタの概要を参照してください。</td></tr>
<tr><td colspan="2">自動時刻同期</td><td>ボタンをクリックすると、異なるセグメント間にある共通のフローの データを時刻同期させるための補正値が計算されます。
詳細は、13.5.2. 自動時刻同期の仕様 を参照ください。</td></tr>
<tr><td rowspan="4">データソースリスト</td><td>名前</td><td>データソースとして選択されたトレースファイルやレコードの名前です。</td></tr>
<tr><td>チャネル / インターフェイス</td><td>データのチャネル情報やインターフェイス情報が表示されます。
初期設定では、以下の値が設定されます。
● インターフェイス名がサポートされているトレースファイル：インターフェイス名
● インターフェイス名がサポートされていないトレースファイル：N/A
● レコード：SYNESIS のホスト名 ＋ チャネル情</td></tr>
<tr><td>セグメント</td><td>MFA を解析する際に使用するセグメント名です。
キャプチャポイントが同じチャネルには同じセグメント名を入力してください。
チェックの付いたチャネル/インターフェイスでマージが実行されます。</td></tr>
<tr><td>時刻同期</td><td>時刻同期させるための補正値です。
「自動時刻同期」ボタンをクリックすると、自動的に計算され、計算結果が入力されます。
手入力でも可能です。</td></tr>
</table>

データソースの指定が完了したら、[保存]ボタンをクリックします。 作成したプロファイルが保存され、プロファイル・ペインに作成したプロファイルが追加されます。

[マージの実行]ボタンをクリックすると、データソースの解析が実行され、プロファイルは自動的に保存されます。

詳細は **13.2. フロービュー** を参照してください。

● プロファイルの削除

登録済みのプロファイルを削除する場合は、プロファイル・ペインより、該当のプロファイルの右側にあるごみ箱アイコンをクリックします。確認ダイアログが表示され、「はい」をクリックするとプロファイルが削除されます。

● プロファイルの編集

作成済みのプロファイルを編集する場合は、プロファイル・ペインより、 該当のプロファイルを選択してクリックします。

新規作成同様、「MFA プロファイル」画面が表示され、編集が可能になります。

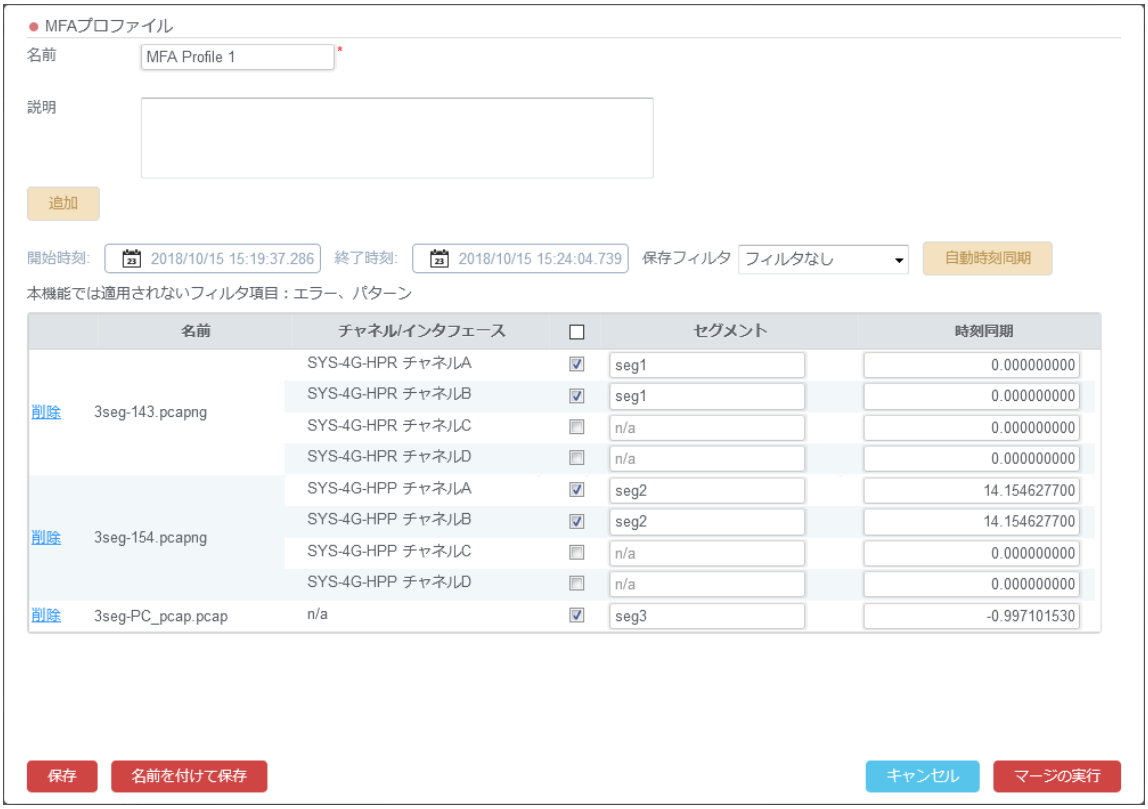


図 203：MFA プロファイル編集画面

編集が完了したら、[保存]ボタンをクリックします。プロファイル名を含め、変更した内容が保存されます。

[名前を付けて保存」ボタンをクリックすると、編集したプロファイルが新しいプロファイルとして保存され、 プロファイル・ペインにプロファイルが追加されます。

[マージの実行]ボタンをクリックすると、データソースの解析が実行され、プロファイルは自動的に保存されます。

13.1.2. ラダービュータブ

MFA の各種表示のフローを画面上部で選択した場合、関連するラダー図が[ラダービュー]タブに表示されます。

ラダー図とは、通信シーケンス図の一種で、IP 通信間での方向、および通信の内容が 1 パケットごとに表示さます。

矢印が通信の方向を表し、矢印の上にプロトコルのペイロード情報が表示されます。

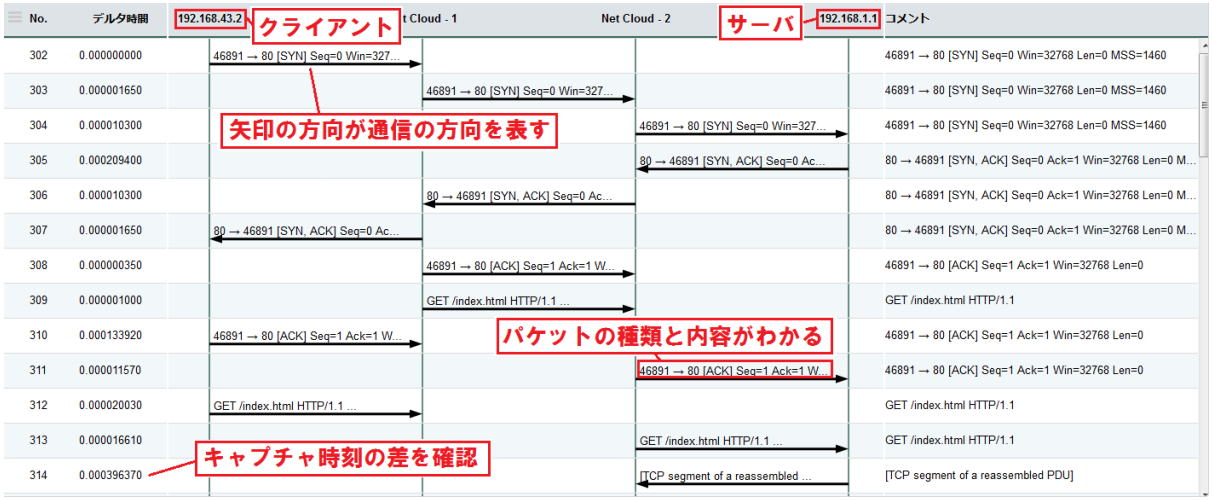


図 204 : ラダービュー

通信に異常が確認されたパケットは、矢印が色付きで表示されます。

異常と判別されたパケットの個数とフレーム番号は、統計タブで確認できます。

No.の右は、時刻表示で「相対時間」「デルタ時間」「絶対時間」の 3 種類を表示することができます。

表示可能な項目は、以下の通りです。

項目	説明
No.	マージされたデータ全体のフレーム番号です。 マージされた全パケットを、時刻の昇順で並べた通し番号となります。 時刻同期が行われている場合は、調整後の時刻で並べられた通し番号になります。
相対時間	対象フローまたは選択されたフローの初めのパケットがキャプチャされてからの経過時間を表示します。
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。 構成メニューの MFA で指定したデルタ時間を超えた場合、 指定に合わせて「エラー■」「警告■」 「注意■」の色が表示されます。
絶対時間	そのパケットがキャプチャされた時刻を表示します。 時刻同期が行われている場合は、調整後の時刻が表示されます。
長さ	パケットの長さです。

13.1.3. ラダービューからの操作

ラダービューから実行できる機能について説明します。

13.1.3.1 デルタ時間からパケットを検索

デルタ時間からパケットの検索が可能です。

ラダー図の左上の「デルタ時間> =」欄(下図赤枠)にデルタ時間を入力します。

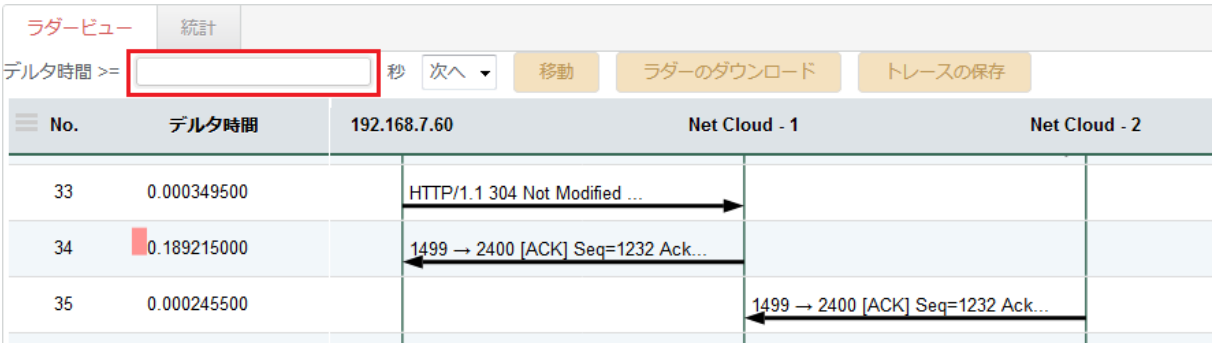


図 205：デルタ時間での検索

「デルタ時間」欄の右側に表示されているドロップダウン・ボックスで、検索を実施する方向を指定し[移動]ボタンをクリックすると、指定された順にデルタ時間以上経過したパケットを検索することができます。

「次へ」：現在ラダー上で選択されているパケットより下方向、時刻の昇順に検索をします。

「前へ」：現在ラダー上で選択されているパケットより上方向、時刻の降順に検索をします。

13.1.3.2 ラダーのダウンロード

表示されているラダー図の内容を、テキストまたは画像（jpeg, png)ファイルでダウンロードすることができます。

ラダー図のファイルをダウンロードする場合は、[ラダーのダウンロード]ボタンをクリックします。以下のような「ラダーのダウンロード」画面が表示されます。

図 206：ラダーのダウンロード

必要に応じて、ラダー図に表示させる項目や、ラダーの数を指定します。

指定後、[ダウンロード]ボタンをクリックすると、ラダー図を指定したファイル形式でダウンロードできます。

TXT を選択した場合は、以下のようなテキストファイルになります。

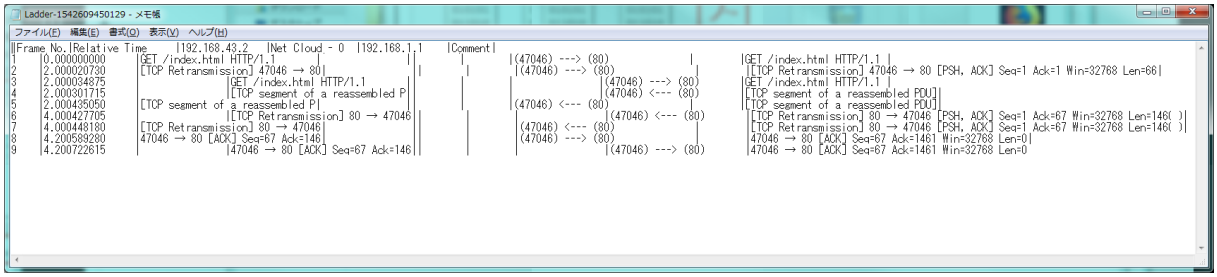


図 207：テキストタイプのラダー図

13.1.3.3 トレースの保存

表示されているフローをトレースファイルに保存できます。時刻同期を行っている場合は、調整された時刻となります。

「現在のフィルタを適用する」のチェックを外した場合はマージしたデータソース全体が保存されます。

MFA 画面からトレースの保存を行う場合は、任意の保存フィルタを指定することはできません。

また、分割ファイルサイズ、ファイル数、スライスの設定もできません。

詳細は、**5. トレースの保存操作** を参照してください。

13.1.3.4 デコードビュー

ラダー図をクリックすると、[デコード]タブが追加され、関連するパケットのデコード結果が表示されます。

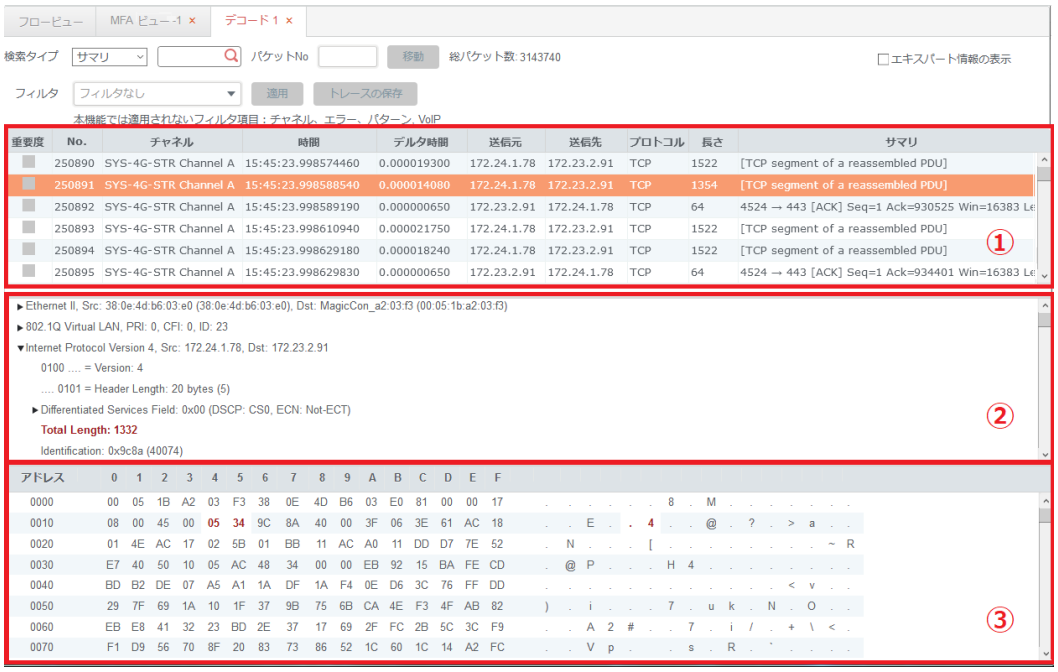


図 208：デコードビュー

「パケット一覧(上図①)」は、ラダー上でクリックしたパケットが選択された状態で移動します。表示される項目と機能の詳細は、**7. デコード機能** を参照してください。

13.1.4. 統計タブ

[ラダービュー]タブの隣には、[統計]タブが表示されます。選択されたフローのセグメントごとの統計値が記載されたフローテーブルと、「エキスパート情報」が表示されます。

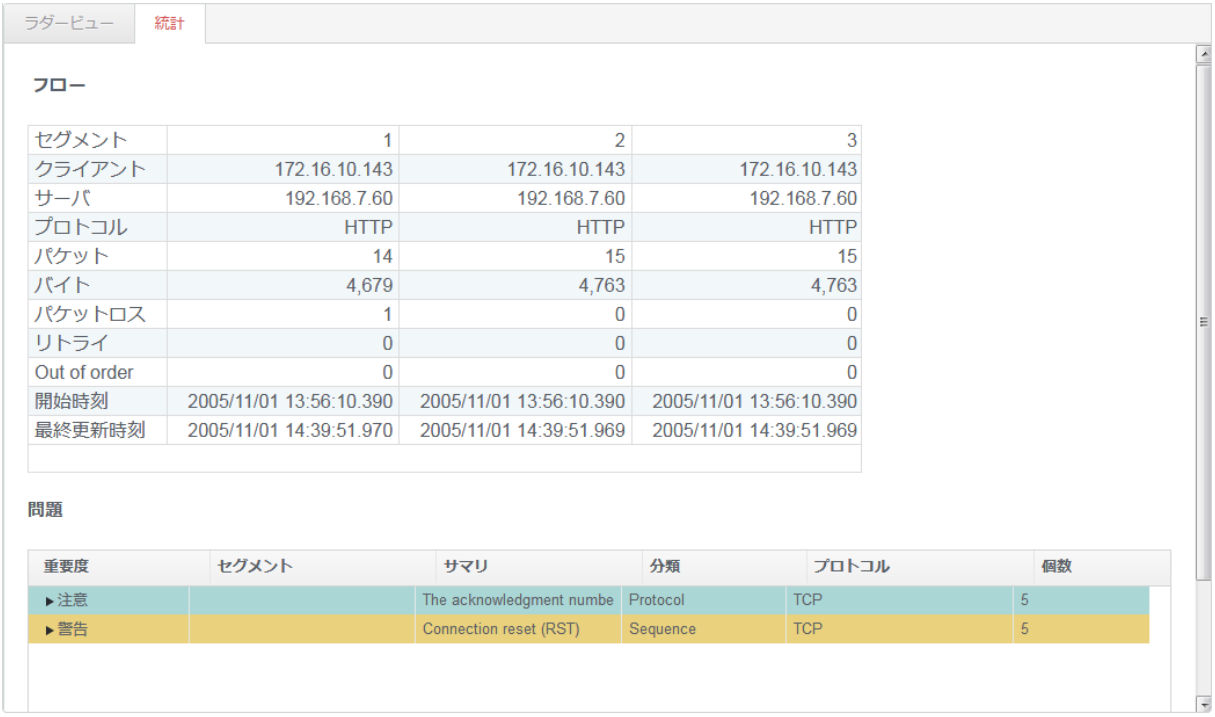


図 209：統計タブ

フローテーブルに表示される項目は以下の通りです。

項目	説明
セグメント	セグメント名です。
クライアント	クライアントの IP アドレスです。
サーバ	サーバの IP アドレスです。
プロトコル	最上位の通信プロトコルです。
パケット	パケットの数です。
バイト	パケットのバイト数です。
パケットロス	そのセグメントで消失したパケットの数です。 同一のフローの、他のセグメントでのパケット数と比較して計算されます。 フロービューで表示されるフロー一覧ではこの項目は表示されません。
リトライ	TCP の再送と判別されたパケット数です。
アウトオブオーダー	TCP の順序不正(アウトオブオーダー)と判別されたパケット数です。
開始時刻	フロー関連するパケットの中で、一最も古いパケットの時刻です。時刻同期が行われている場合は、調整後の時刻が表示されます。
最終更新時刻	フロー関連するパケットの中で、最も新しいパケットの時刻です。 時刻同期が行われている場合は、調整後の時刻が表示されます。

フローテーブルの下には、「エキスパート情報」が表示されます。

重要度	セグメント	サマリ	分類	プロトコル	個数
▼注意		The acknowledgment numbe	Protocol	TCP	5
44	1	2400 → 1499 [RST] Seq=22	Protocol	TCP	1
37	2	1499 → 2400 [RST] Seq=12	Protocol	TCP	1
43	2	2400 → 1499 [RST] Seq=22	Protocol	TCP	1
38	3	1499 → 2400 [RST] Seq=12	Protocol	TCP	1
42	3	2400 → 1499 [RST] Seq=22	Protocol	TCP	1
▼警告		Connection reset (RST)	Sequence	TCP	5
44	1	2400 → 1499 [RST] Seq=22	Sequence	TCP	1
37	2	1499 → 2400 [RST] Seq=12	Sequence	TCP	1

図 210：エキスパート情報

「エキスパート情報」には、異常と判別されたパケットの情報が表示されます。

エキスパート情報は、パケットの昇順で 1,000 個まで表示されます。

表示される項目は、以下の通りです。

項目	説明
重要度	確認されたエラーは、重要度によって「エラー■」「警告■」「注意■」に分類されます。「重要度」の右の▶をクリックすると、エラーごとに含まれるパケットの情報が展開されます。
セグメント	「重要度」を展開した際、該当するパケットのセグメント名が表示されます。
サマリ	「重要度」を展開した際、該当するパケットのサマリが表示されます。
分類	エラーの分類です。
プロトコル	エラーが確認された通信プロトコルです。
個数	「重要度」のエラーが確認されたパケットの総数です。 「重要度」を展開した際は、パケットごとの個数が表示されます。

13.1.5. データソースと制限

MFA で表示できるデータソースは、以下です。

- ビルトインファイル、カスタムファイル、トレースバンカーにあるトレースファイル
- SYNESIS でキャプチャしたレコード

データソースをマージした際には、以下の制限があります。

項目	制限
最大データソース	1 セグメントにつき 512MB マージ後の最大は 4GB
ラダー表示する IP ペア	マルチセグメント：1 フローで 8 セグメントまで表示 マルチティア：8 フロー(8 ティア)まで表示 マルチセグメント＋マルチティア：マルチセグメントの共通フローはひとつまで、ラダーの橋桁(IP 表示、Net-Cloud の下に表示される縦線)は 9 本まで
ラダーの段数	1,000
サーバ数	1,000
フロー数	10,000

ラダーの段数、サーバ数、フロー数は、[構成]メニュー>「MFA」で変更できます。

詳細は、**13.5.1. MFA の表示設定** を参照ください。

13.2. フロービュー

プロファイルでデータソースの選択、設定を行ったあと、[マージ]ボタンをクリックすると、データソースに含まれる通信をプロトコル、サーバごとのに分類しフロー単位で表示します。

フロービューは、また表示されたフローから、MFA ビューやパケットロス解析を行うためのフローの選択を行う画面でもあります。

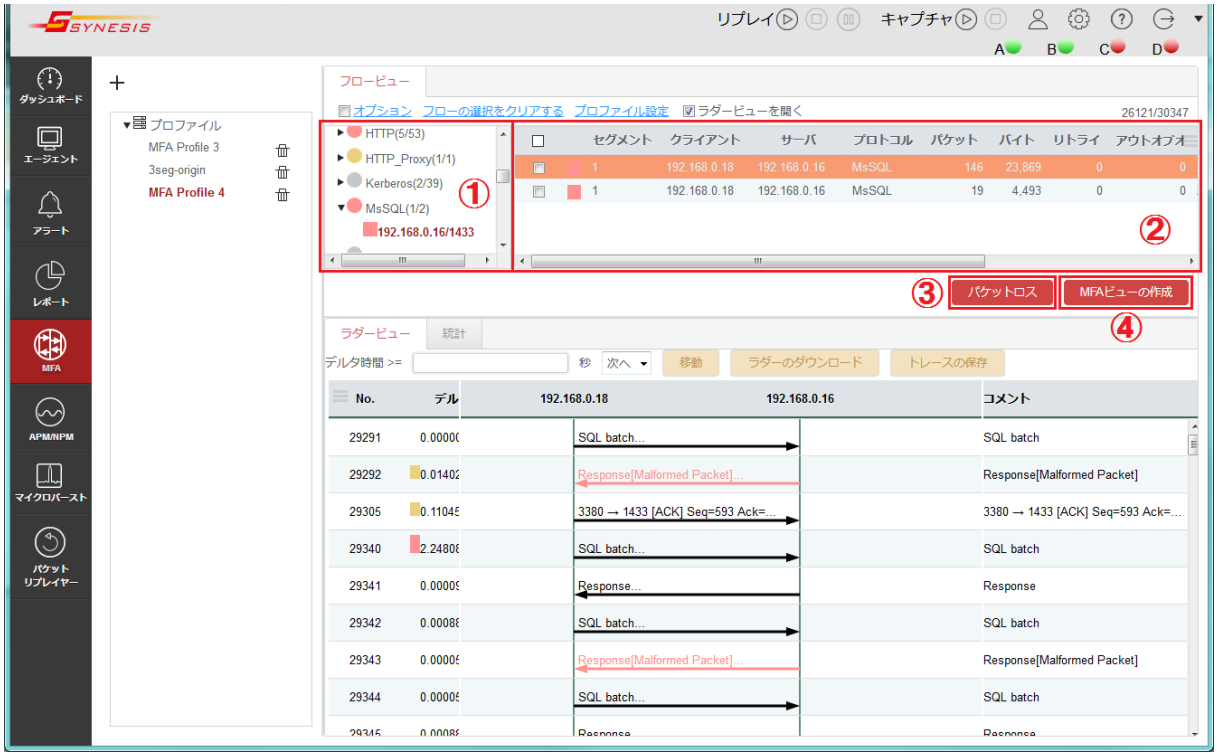


図 211：フロービュー

アプリケーション・ツリー(上図①)にプロトコルがリストアップされます。

プロトコルを選択すると、そのプロトコルのフローリスト(上図②)が表示されます。フローリストの左側にあるチェックボックスは、MFA ビューやパケットロス解析を行う際に選択します。

パケットロス解析を行う場合は、[パケットロス]ボタン(上図③)をクリックします。

その際、フローを選択した場合は、選択したフローのみでパケットロス解析を行います。フローの選択を行わなかった場合は、全フローが対象になります。

MFA ビューの作成を行う場合は、フローを選択し、[MFA ビューの作成]ボタン(上図④) をクリックします。

パケットロス解析の詳細は、**13.4. パケットロス解析** を参照してください。

MFA ビューの作成の詳細は、**13.3. MFA ビュー** を参照してください。

13.2.1. アプリケーション・ツリー

アプリケーション・ツリーにはデータソース内で確認された サーバがプロトコル別に表示されています。

プロトコル表示の右側は、サーバリストに表示されるサーバ数とフロー数が表示されます。

プロトコルの左にあるノード ▶をクリックすると、 そのプロトコルで通信しているサーバとポート番号表示されます。

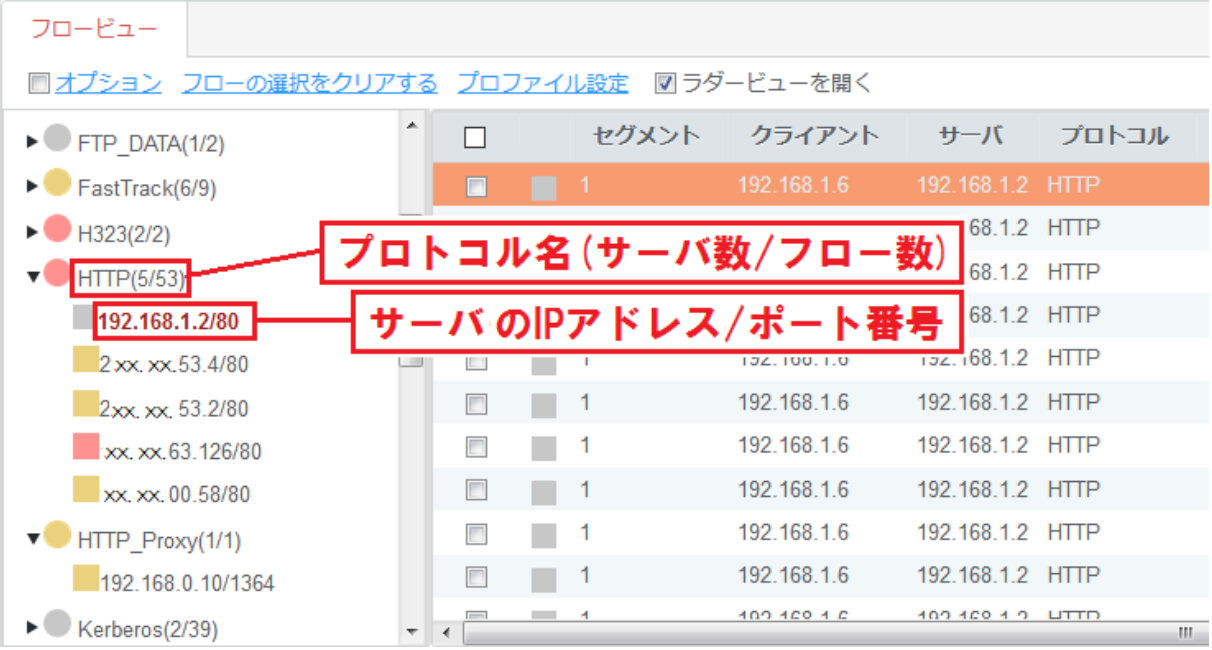


図 212：アプリケーション・ツリー

アプリケーション・ツリーから、プロトコルを選択してクリックすると、そのプロトコルの通信を行っている全フローがフローリストに表示されます。

アプリケーション・ツリーから、プロトコルで展開されたサーバを選択してクリックすると、選択したプロトコルのサーバのフローがフローリストに表示されます。

「オプション」を適用すると、表示するプロトコルやサーバを絞り込むことができます。

詳細は、**13.2.3. フロービューの操作** を参照してください。

13.2.2. フローリスト

フローリストは、アプリケーション・ツリーで選択した項目に含まれるフローが表示されます。

図 213：フローリスト

フローリストに表示される情報は、以下の通りです。

項目	説明
セグメント	セグメント名です。
クライアント	クライアントの IP アドレスです。
サーバ	サーバの IP アドレスです。
プロトコル	通信プロトコルです。
パケット	パケット数です。
バイト	バイト数です。
リトライ	TCP の再送と判別されたパケット数です。
アウトオブオーダー	TCP の順序不正(Out-of-Order)と判別されたパケット数です。
開始時刻	フローに含まれる最も古いパケットの時刻が設定されます。時刻同期を行った場合は、調整後の時刻が表示されます。
最終更新時刻	フローに含まれる最も新しいパケットの時刻が設定されます。時刻同期を行った場合は、調整後の時刻が表示されます。

13.2.3. フロービューの操作

画面上部には、フロービュー画面での実施できる操作が表示されています。

- オプション

フロービューに表示するフローをする絞り込む場合に使用します。

「オプション」リンクをクリックします。以下の「オプション」画面が表示されます。

図 214：フロービューのオプション画面

IP アドレス、アプリケーション、ポート番号のうちの 1 つ以上を指定します。フローを追加する場合は、[フローの追加]ボタンをクリックします。すべての設定が完了したら、[適用]ボタンをクリックします。

[適用]ボタンをクリックすると、オプションのチェックボックスにチェックが自動的につき、オプションが適用された状態となります。「オプション」のチェックを外すと、全フローが表示されます。

なお、フローを選択した状態で「オプション」を適用し非表示にした場合、フローの選択は解除されます。

設定項目は、以下の通りです。

項目	説明
セグメント	絞り込む対象のセグメントを選択します。 プロファイルのデータリストで登録したセグメント名が表示されます。
IPv4/IPv6	IP アドレスの種別を選択します。 「IPv4」と「IPv6」の選択が可能です。
IP アドレス	絞り込むフローの IP アドレスを入力します。 空欄の場合は、Any として扱われます。
アプリケーション	絞り込むフローのプロトコルを入力します。 「Any」を選択した場合は、すべてのプロトコルのフローが対象となります。
ポート	アプリケーション」でプロトコルを指定した場合、構成メニューのプロトコルで定義済のポート番号が表示されます。 「Any」を選択した場合、手動でポート番号が設定可能です。

- フローの選択をクリアする

「フローの選択をクリアする」リンクをクリックすると、フローの選択が一括でクリアされます。

- プロファイル設定

「プロファイル設定」リンクをクリックすると、現在のプロファイルの設定ダイアログが表示されます。プロファイルを編集後、[マージの実行]ボタンをクリックすると、編集した内容でマージと解析が実行されます。

[保存]ボタンをクリックすると、編集した内容が保存され、MFA の初期画面に戻ります。

[名前を付けて保存]ボタンをクリックすると、編集した新しい名前のプロファイルが作成され、MFA の初期画面に戻ります。

[キャンセル]ボタンをクリックすると、元のフロービュー画面に戻ります。

- ラダービューを開く

「ラダービューを開く」にチェックを入れると、 フローリストで選択されたフロー(フローリストのオレンジ部)のラダー図が表示されます。

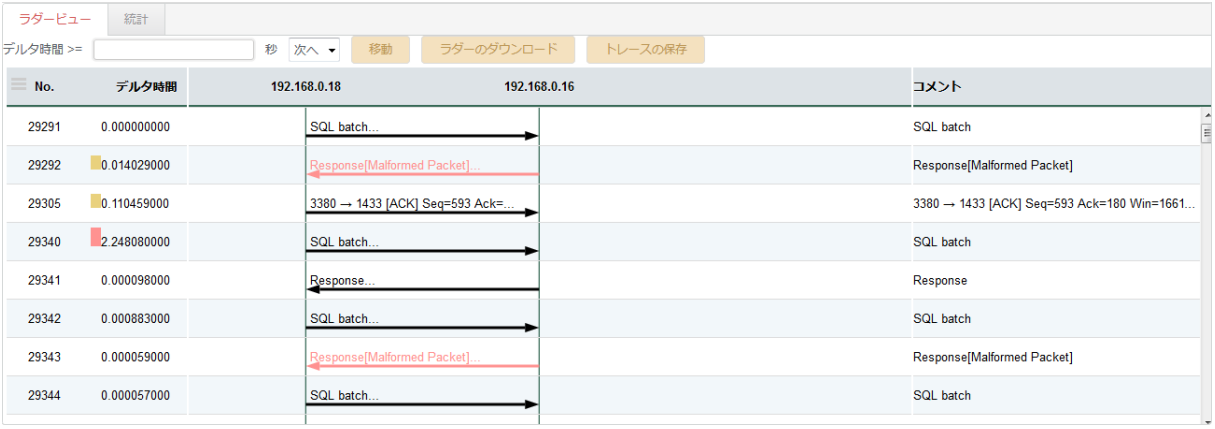


図 215 : ラダービュー

13.3. MFA ビュー

MFA ビューでは、フロービューで選択した複数のフローでひとつのラダー図が表示されます。

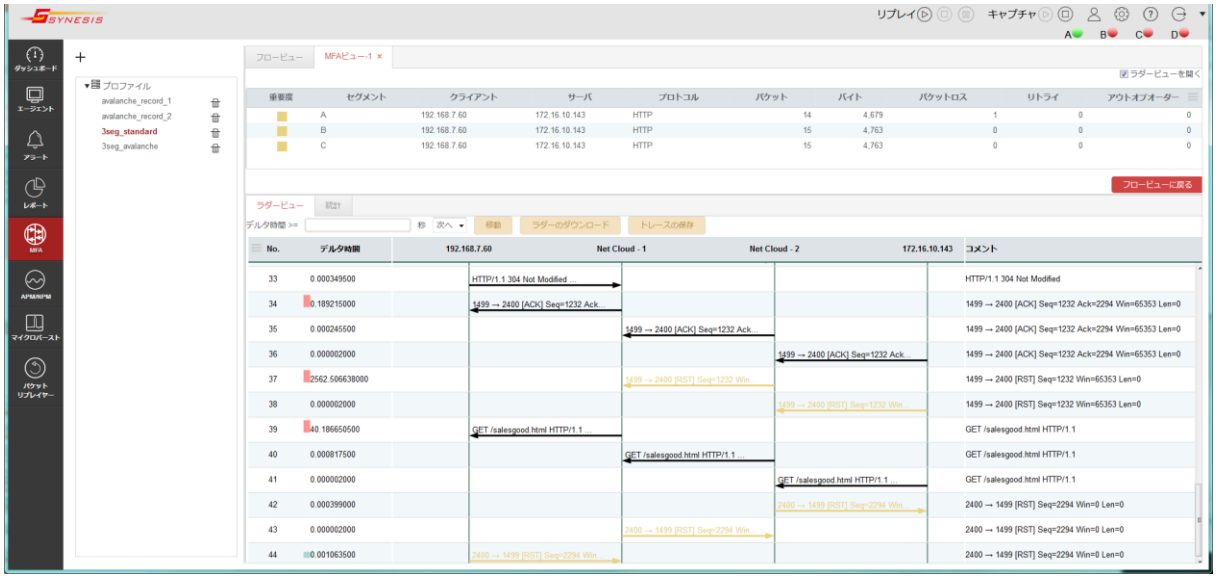


図 216：MFA ビュー

MFA ビューで選択できるフローの数は、制限があります。詳細は、**13.5.1. MFA の表示設定** を参照してください。

13.3.1. MFA ビューの作成手順

MFA を作成する手順は、以下の通りです。

1) [フロービュー]タブでまとめてラダー表示するフローを選択します。フローの左側にあるチェックボックス(下図①)にチェックを入れて、[MFA ビューの作成]ボタン(下図②)をクリックします。

図 217：フロー選択

2) 「確認」画面で、チェックしたフローを確認します。
その際、不要なフローはチェックを外すことができます。
必要なフローが表示されていなければ、[キャンセル]ボタンをクリックし、[フロービュー]タブに戻り、再度選択します。
問題なければ、[作成]ボタンをクリックします。

図 218：「確認」画面

3) [MFA ビュー]タブが開き、[フロービュー]タブで選択したフローがまとめてラダー表示されます。

[MFA ビュー]タブは、最大８個まで開くことが可能です。[MFA ビュー]タブの×をクリックすると、タブは削除されます。

フローリストの下の[フロービューに戻る]ボタンをクリックすると、 該当の MFA ビューを作成した時に選択されていたフローが選択された状態のフロービューに戻ります。[フロービュー]タブをクリックすると、最後に設定されていた状態のフロービューが表示されます。

13.3.2. MFA のラダービュー表示と解析手法

MFA でラダー図を作成することにより、以下のような解析を行うことができます。

- マルチセグメント解析：複数のセグメント間にまたがる同一のフローに着目する解析
- マルチティア解析 :複数のフローに着目する解析

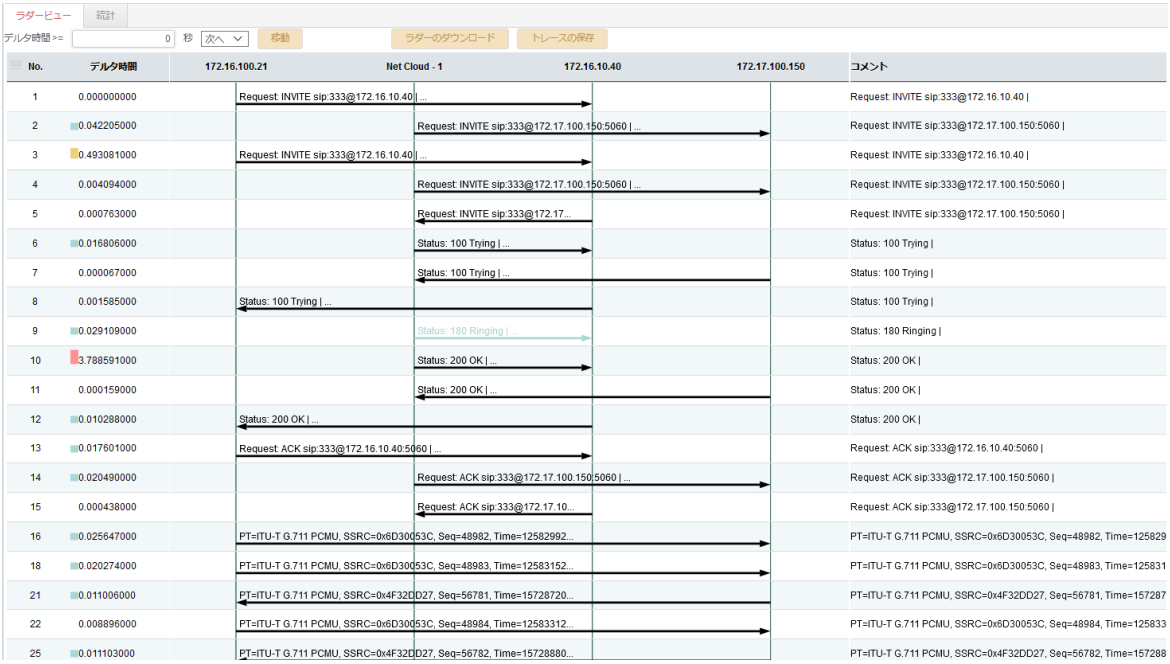


図 219：ラダービュー表示

同一フローが異なるセグメントに存在する場合、クライアントとサーバの間に「Net Cloud」を挿入し、異なるセグメントのフローであることを表します。同一フローの判断は、送信元と送信先の IP アドレスおよびポート番号で行います。VLAN ID が異なっていても、送信元と送信先の IP アドレスおよびポート番号が同一の場合は、同一フローとみなします。

マルチセグメント解析を行う場合は、データソースをマージする際、セグメント名を意識する必要があります。

マルチティア解析は、セグメント名を意識する必要はありません。

13.4. パケットロス解析

同一フローが異なるセグメントでキャプチャされた場合、フローごとにパケット数、パケットロス数のセグメントの比較ができます。各セグメントのフローの発生状況の確認やパケットロスが起きたセグメントの特定が行えます。

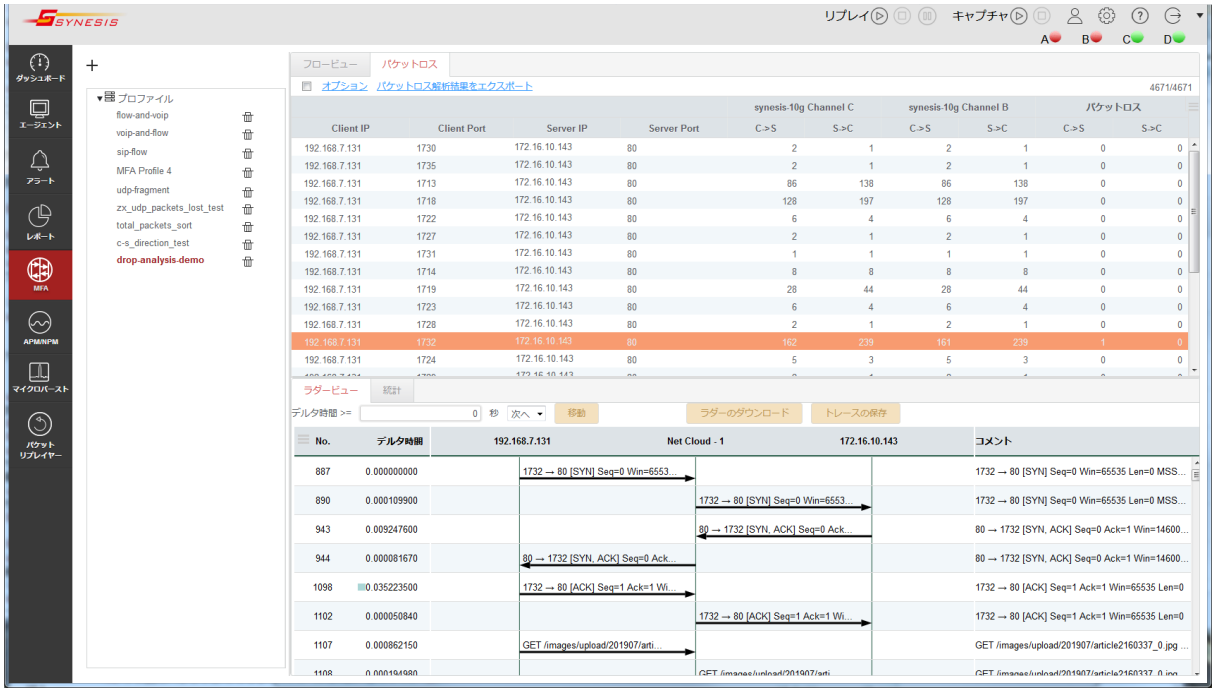


図 220 : パケットロス解析画面

フロービューでフローを選択し、「パケットロス解析」をクリックした場合、パケットロスタブが表示されます。

画面上部のパケットロス・テーブルには、フローごとに各セグメントで確認されたパケット数とパケットロスの発生数が表示されます。

画面上部のパケットロス・テーブルでフローを選択すると、 画面下部に関連するフローのラダー図と統計値のテーブルが表示されます。

13.4.1. パケットロス解析の作成手順

[フロービュー]タブでパケットロス解析するフローを選択し、[パケットロス]ボタンをクリックします。

その際、パケットロス表示するフローの条件は、以下の通りです。

- フローの左側にあるチェックボックスにチェックを入れて選択した場合

選択したフローがパケットロス解析をする対象となります。

- フローの選択を行わなかった場合

フロービューの全フローが対象となります。

13.4.2. パケットロス・テーブル

パケットロス・テーブルでは、フローごとに各セグメントで確認されたパケット数をセグメントごとに方向別に表示します。

パケットロス数の算出方法は、最大パケット数から最小パケット数を引いた値です。

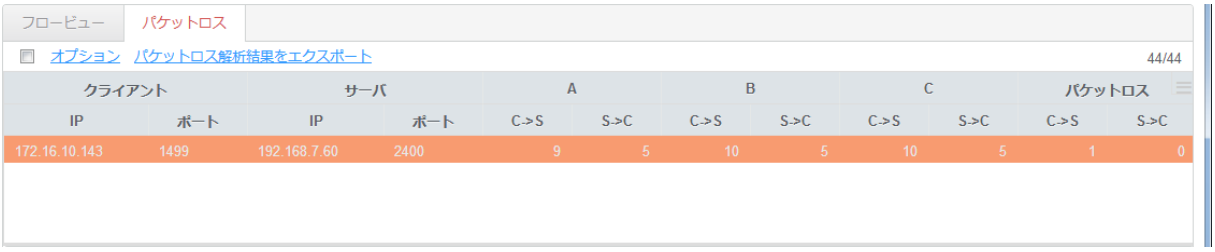


図 221：パケットロス・テーブル

パケットロス・テーブルに表示される項目は、以下の通りです。

項目	説明	
クライアント	IP	クライアントの IP アドレスです。
	ポート	クライアントのポート番号です。
サーバ	IP	サーバの IP アドレスです。
	ポート	サーバのポート番号です。
セグメント名	マージする際に設定したセグメントごとに情報が表示されます。	
	C->S	クライアント(C)からサーバ(S)の方向のパケット数です。
	S->C	サーバ(S)からクライアント(C)の方向のパケット数です。
パケットロス	パケットロス数が、通信の方向別に表示されます。 パケットロス数は、各セグメントのパケット数の最大値から最小値を引いた数値です。	
	C->S	クライアント(C)からサーバ(S)の方向のパケットロス数です。 最大パケット数から最小パケット数を引いた値です。
	S->C	サーバ(S)からクライアント(C)の方向のパケットロス数です。 最大パケット数から最小パケット数を引いた値です。

13.5. MFA に関する設定項目と仕様

MFA に関する設定項目と仕様について説明します。

13.5.1. MFA の表示設定

構成メニュー>「MFA」では、MFA(マルチフロー解析)で警告表示させるデルタ時間や、 ラダー図に表示するラダー数などの上限値を指定できます。

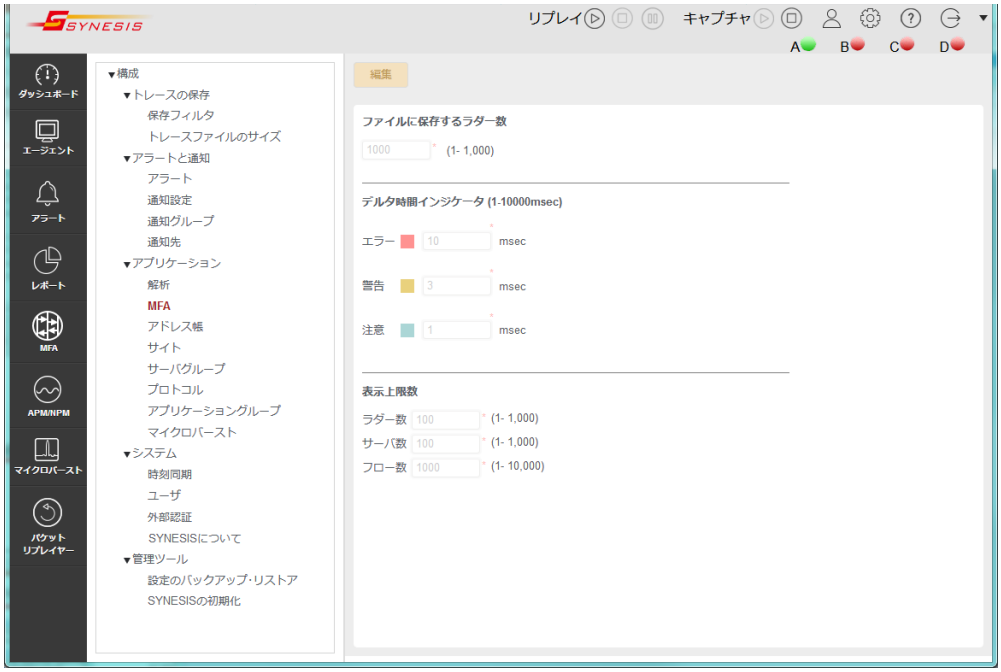


図 222 :「構成」メニュー>「MFA」

設定を変更する場合は、画面左上の[編集]ボタンをクリックします。

以下のように各項目が編集可能になります。

図 223 : MFA 表示設定編集画面

編集後、[保存]ボタンをクリックします。

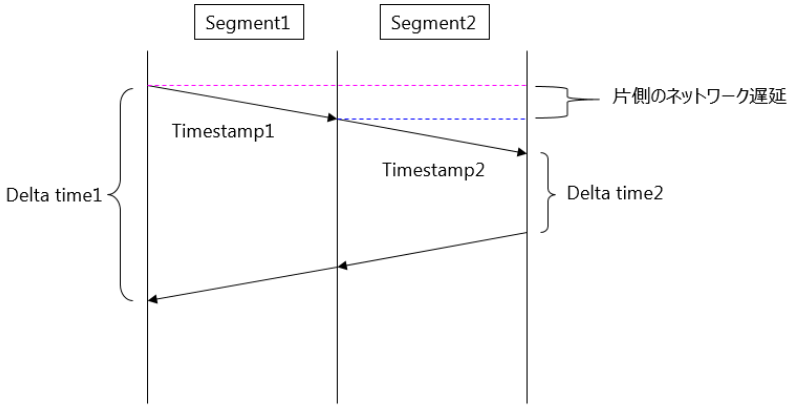
設定項目は、以下の通りです。

項目		説明
ファイルに保存するラダー数		作成したラダー図を保存する際に、ファイルに保存するラダー数の上限を指定します。
デルタ時間インジケータ	**エラー**	インジケータを表示するデルタ時間の間隔を msec 単位で指定します。1 以上 10,000 以下の数値を入力してください。 数値の大きさは、エラー>警告>注意の順で入力する必要があります。
	警告	
	注意	
表示上限数	**ラダー数**	表示するラダー数の上限を指定します。 1 以上 1,000 以下の数値を入力します。
	サーバ数	ラダー図に表示するサーバ数の上限を指定します。 1 以上 1,000 以下の数値を入力します。
	フロー数	フローリストに表示するフロー数の上限を指定します。 1 以上 10,000 以下の数値を入力しします。

13.5.2. 自動時刻同期の仕様

自動時刻同期は、各セグメント間のデータソースの時刻を自動的に調整します。複数のデータソースにチェックをし、それぞれのチャネル/インターフェイス名が異なる場合、このデータは別の装置でキャプチャされたと判断し、TCP 通信のターンから時刻を計算します。

フローに複数の TCP ターンが含まれている場合、フローのはじめから 20 ターンまでの各ネットワーク遅延を計算し、最小値をオフセット時間の計算に採用します。



$$\text{片側のネットワーク遅延} = \frac{\text{Delta time1} - \text{Delta time2}}{2}$$

$$\text{オフセット時間} = (\text{Timestamp1-Timestamp2}) + \text{片側のネットワーク遅延}$$

図 224：遅延とオフセットの計算

MFA プロファイルの一番上のデータソース(一番初めに追加したデータソース)を基準としてオフセット時間を計算します。

自動時刻同期ボタンで調整した場合のみ、開始時間/終了時間の調整もあわせて行います。

データソースに複数のフローが含まれている場合は、最も古い共通のフローで計算をします。

<自動時刻同期ができない場合>

・異なるチャネル/インターフェイス名に共通の通信が含まれていない場合

・共通の通信に TCP が含まれていない場合

・共通の通信にシーケンス番号とその応答番号が含まれていない、片側のみのフローの場合

13.5.3. MFA に関する KPI の定義

13.5.3.1 サーバの規則

1. 送信先 MAC アドレスがブロードキャストまたはマルチキャストアドレスの場合、送信元 IP アドレスをサーバとみなします。
2. 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。
3. nDPI の結果に基づきサーバを判定します。
4. 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。
5. 送信元と送信先のポート番号が同じ場合、最初のパケットの送信先をサーバとみなします。

13.5.3.2 フローごとの KPI

リトライとアウトオブオーダーの値は、TCP ヘッダ上のシーケンス番号をもとに KPI を算出します。

UDP 通信の場合は、リトライとアウトオブオーダーの値は、“0”となります。

判定は、以下の通りです。

- リトライ

ひとつ前のパケットと比較し、現在のシーケンス番号のほうが小さい値の場合、そのパケットを「リトライ」と判定します。リトライは、スリーウェイハンドシェイク以降から FIN パケットの直前までのデータのパケットで判定します。

ネットワークでは、ふたつの場合が想定されます。

1) 一部のパケットが消失している場合

2) 同じシーケンス番号のパケットが 2 回以上送信されている場合

- アウトオブオーダー

ひとつ前のパケットと比較し、現在のシーケンス番号が期待するシーケンス番号よりも大きい値の場合、そのパケットを「アウトオブオーダー」と判定します。

14.アラート機能と通知

アラート機能と通知について、説明します。

- アラート機能

アラート機能とは、キャプチャしたデータから閾値を超過したパケットをアラートとして検出することです。

アラートとして検出できる閾値の種類は、以下の４つです。

- DLC
- ARP
- NPM
- APM

ARP、NPM、APM のアラート検出は、該当のモジュールを有効にした上で予め解析を行う必要があります。また、通知を行うためには、リアルタイム解析を行う必要があります。

解析の手順は、**解析機能**の章を参照ください。

アラートは、[アラート]メニューで確認できます。

- 通知

通知とは、イベントが発生した際に Email、Syslog、SNMP Trap による外部通知を行うことです。

イベントとは、以下を指します。

- アラート機能でアラートが検出された場合
- マイクロバースト機能で閾値の超過が検出された場合
- リンクステータス、ドロップ、自動保存で、事象が検出された場合
- 定期レポートの送付（E-mail のみ）

通知は、キャプチャ中のみ行われます。

14.1. アラート検出手順

[アラート]メニューにアラートとして検出するための条件は、以下の通りです。

アラート種類	データの反映
DLC	閾値を設定後、キャプチャしたデータに対して反映
ARP	閾値を設定後、解析したデータに対して反映
NPM	
APM	

アラート機能をご利用の場合には、必ずキャプチャ開始前に構成メニューのアラート項目で検知基準となるアラートの閾値を設定し、アラートを有効にしてください。

設定手順は、以下の通りです。

1) キャプチャ開始もしくは解析実行前に、異常発生の検知基準となる閾値を設定します。
   詳細は、**14.1.1. 閾値の設定** を参照ください。

2) リアルタイムに通知を行う場合は、以下の設定を行います。

- 通知先
- 通知グループ

詳細は、**14.3. 通知** を参照ください。

3) 2)で設定した項目の確認を行います。

詳細は、**14.3.3. 通知設定の確認** を参照ください。

14.1.1. 閾値の設定

キャプチャ開始もしくは解析実行前に、異常発生の検知基準となる閾値を設定します。

構成メニュー>「アラート」では、設定済みの全てのアラート設定が表示されます。

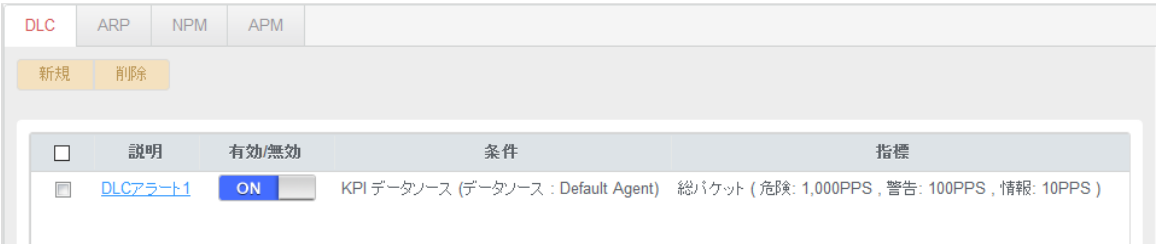


図 225 : アラートメニュー

有効/無効のアイコンをクリックすると、有効/無効が切り替わります。

検出対象となるのは、有効となっているアラートのみです。

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ます。複数のチェックを入れた場合は、OR 条件で判定されます。

図 226 : APM アラート設定画面

アラート設定を削除する場合は、該当するアラート設定の左側のチェックボックスにチェックを付けます。[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。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付けると、すべてのアラートが対象となります。

14.1.2. アラート一覧

アラート設定可能な項目は、以下の通りです。

カテゴリ	項目	説明
DLC	総パケット	総パケットの数で閾値を設定します。 データ対象：全チャネル合計 サンプリング周期：1 秒
	双方向 ビットレート	ビットレートで閾値を設定します。 データ対象：全チャネル合計 サンプリング周期：1 秒
ARP	ARP	解析モジュールを 1 つでも有効にした場合、自動的に解析されます。 解析された ARP パケットの数で閾値を設定します。閾値の設定は、同一送信元 MAC アドレスでの ARP の個数です。 データ対象：解析済みデータ サンプリング周期：1 分
NPM	総パケット	NPM で解析された各フローの総パケット数で閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	双方向 ビットレート	NPM で解析された各フローのビットレートで閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	受信パケット	NPM で解析された各フローの受信パケット数で閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	受信 ビットレート	NPM で解析された各フローの受信ビットレートで閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	送信パケット	NPM で解析された各フローの送信パケットで閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
	送信 ビットレート	NPM で解析された送信ビットレートで閾値を設定します。 データ対象：NPM で解析された各フロー サンプリング周期：1 分
APM	ART	APM で解析された各フローの ART で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	PTT	APM で解析された各フローの PTT で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	NRT	APM で解析された各フローの NRT で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分

	SRT	APM で解析された各フローの SRT で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	CRT	APM で解析された各フローの CRT で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	遅延	APM で解析された各フローの遅延で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分
	リトライ	APM で解析された各フローのリトライ A で閾値を設定します。 データ対象：APM で解析された各フロー サンプリング周期：1 分

各 KPI の仕様は、**10.3. APM/NPM に関する KPI の定義** を参照ください。

14.2. アラートの画面構成

アラートの結果は、[アラート]メニューから確認します。

[アラート]メニュー>「開始時刻」「終了時刻」で表示されている期間のフロー情報がワークスペース上に表示されます。

検索実行後の画面構成は、以下の通りです。

- ペイン (左側)：アラート条件の検索画面
- ワークスペース(右側)：ペインで選択されている項目のアラートグラフとアラート一覧が表示

アラートグラフ上で、表示させたい危険度のラベル 危険 警告 情報 にチェックを入れます。危険度ごとに表示/非表示を切り替えることができます。

アラート情報の一覧には、指定されている期間の情報が表示されます。

図 227：アラートメニュー画面

14.2.1. アラートの期間指定

アラートの結果は、上部に表示されている「開始時間」から「終了時間」までの情報です。

表示期間の指定、変更は、以下の 2 通りの方法があります。

1. [アラート]メニュー>画面上部の「開始時刻」「終了時刻」のカレンダーアイコンで指定

   トレンドグラフ上部の「開始時間」「終了時間」をクリックすると、以下の「期間」ダイアログが表示されます。

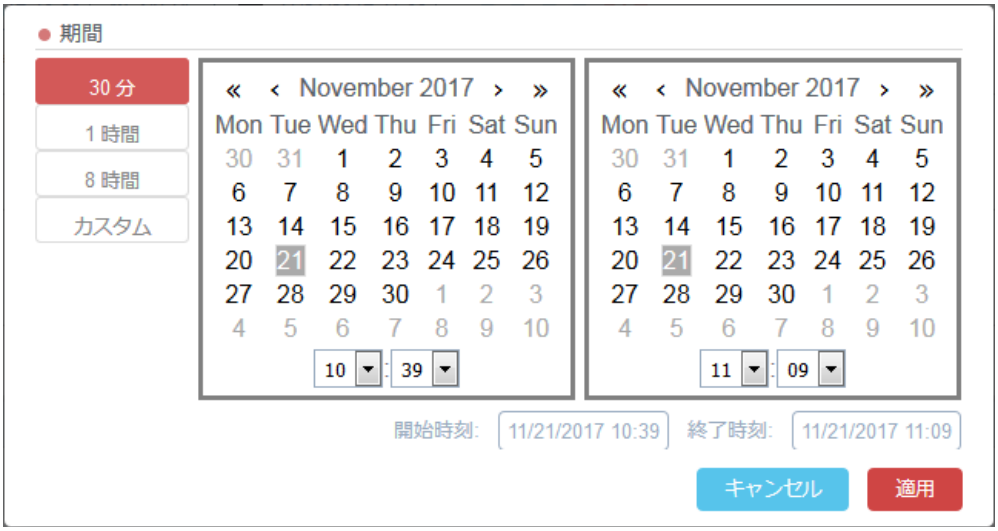


図 228：期間ダイアログ

ダイアログボックス左側のボタンから、表示する時間の範囲を一括で指定できます。選択できる時間は 30 分、1 時間、8 時間で、直近から遡った期間を指定します。

任意の期間を表示する場合は、「カスタム」を選択し表示されるカレンダーで指定します。

2. [アラート]メニュー>ヒストグラムから指定

   選択した時間範囲で拡大表示されると、アラート一覧に表示される情報も指定範囲の情報になります。

   グラフ上でドラッグして時間範囲を指定し、画面中央上部の拡大アイコンをクリックします。

   指定した時刻範囲でグラフが拡大表示されます。

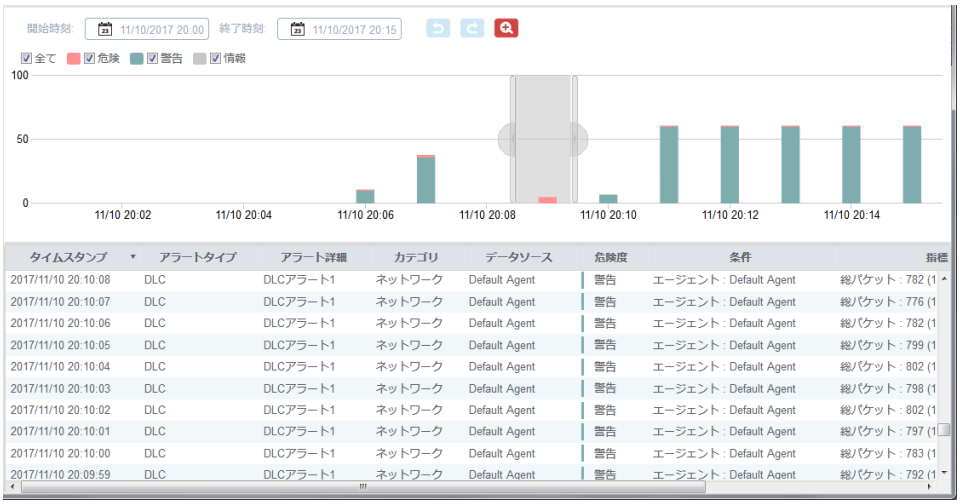


図 229：拡大時刻範囲選択

詳細は、**2.6.5. グラフ画面での期間指定** を参照してください。

14.2.2. 検索条件

検索ペインで検索条件を指定し、「検索」ボタンをクリックします。

検索条件は、アラートタイプにより異なります。

項目	説明
アラートタイプ	検索するアラートタイプです。 選択可能な項目は「Any」「DLC」「ARP」「NPM」「APM」です。 「Any」を指定すると、全てのアラートタイプが表示されます。
サイト	「サイト」は、構成メニューの サイトの項目で登録されたネットワークグループです。IP アドレスをサブネットごとにグループ化して登録することができます。 「Any」を指定すると、登録にかかわらずすべてが表示されます。 「global site」を指定すると、登録したサイトに含まれないアラートが表示されます。
アプリケーション	「アプリケーション」は、構成メニューのプロトコル項目で登録された L4 ポート番号で登録されたアプリケーションです。 「Any」を指定すると、登録にかかわらずすべてが表示されます。
サーバグループ	「サーバグループ」は、構成メニューの サーバグループの項目で登録されたサーバのグループです。「Any」を指定すると、登録にかかわらずすべてが表示されます。 「「global server group」を指定すると、 登録したサーバ グループに含まれない通信がアラートに表示されます。
アプリケーショングループ	「アプリケーショングループ」は、構成メニューのプロトコル項目で登録された L4 ポート番号で登録されたアプリケーショングループです。「Any」を指定すると、登録にかかわらずすべてが表示されます。
データソース	エージェントを指定します。 「Default Agent」のみ選択可能です。「Any」を選択した場合も、結果は「Default Agent」と同じです。

サイト、プロトコル、サーバ グループ、アプリケーショングループの詳細と登録方法は、APM/NPM の事前設定を参照ください。

14.2.3. アラート一覧

一覧で確認できる情報は、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。 yyyy/mm/dd hh:mm:ss の形式で記載されます。
アラートタイプ	検出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。 「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。 危険度は 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、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	トレースファイルの保存操作に使用するリンクです。 詳細は **5. トレースの保存操作** を参照してください。 アラートからトレースを保存する場合、該当のアラートの情報を含む 2 分間の全パケットが保存されます。

14.3. 通知

通知とは、イベントがあがった際に Email、Syslog、SNMP Trap による外部通知を行うことです。イベントとは、以下を指します。

- アラート機能でアラートが検出された場合
- マイクロバースト機能で閾値の超過が検出された場合
- キャプチャオプションのリンクステータス、ドロップ、自動保存で、事象が検出された場合
- 定期レポートの送付（E-mail のみ）

通知は、キャプチャ中のみ行われます。

アラート機能で通知を行うためには、リアルタイム解析をする必要があります。

自動保存、リンクステータス、ドロップの詳細は、通知設定を参照ください。

マイクロバーストの詳細は、マイクロバーストの外部通知を参照してください。

通知を行うためには、通知先、通知グループの設定が必要です。

14.3.1. 通知先の設定

リアルタイムで通知を行う通知先を[構成]メニュー>「通知先」で設定します。

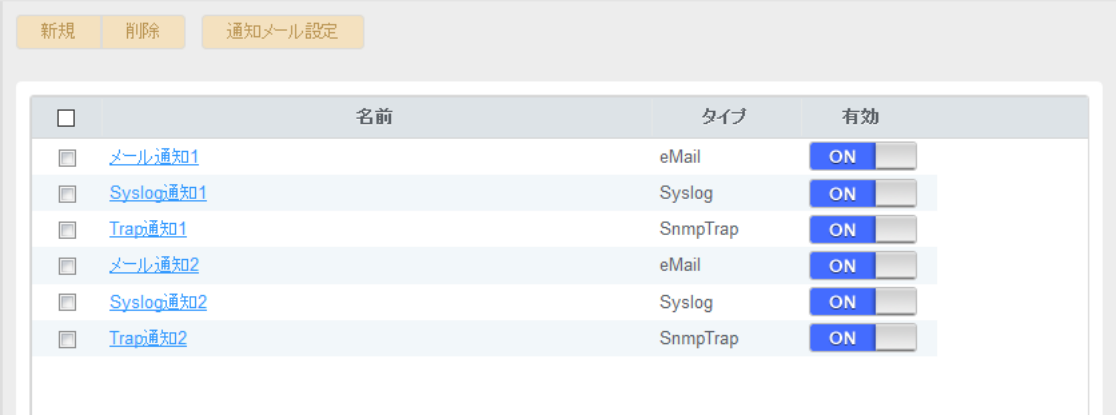


図 230：[構成]メニュー>「通知先」

「通知先」として登録可能な通知方法は、 Email, Syslog, Trap です。

登録した「通知先」をまとめて「通知グループ」を作成します。アラート発生や周期レポート作成などのイベント発生や、 キャプチャオプションの通知設定の各項目の通知先は、「通知グループ」で指定する必要があります。

詳細は、「通知グループ」を参照してください。

項目		説明
名前		登録されている「通知先」の名前です。
タイプ		登録されている「通知先」の通知方法です。 Email, Syslog, Trap のいずれかです。
有効	OFF	無効状態です。有効になっている通知設定で通知先に指定されていても、通知は送信されません。
	ON	有効状態です。イベント発生の通知が送信されます。

アイコン ON ／ OFF をクリックすると「通知先」の有効/無効化が切り替えられます。

新規に通知先を設定する場合は、[新規]ボタンをクリックします。

下図の通知先登録ダイアログが表示されます。

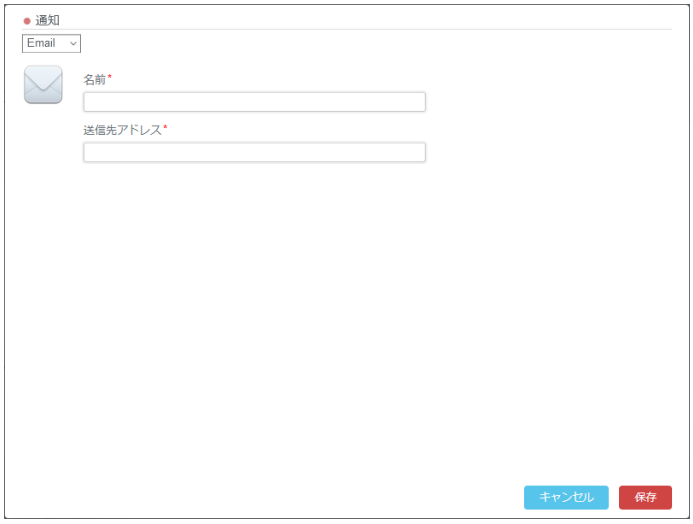


図 231：通知先登録ダイアログ

通知手段として Email, Syslog, SNMP 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ます。 登録した通知先がリストに追加されます。

新規登録された「通知先」はデフォルトで有効に設定されます。

通知手段として使用するプロトコルは、初期設定では Firewall で遮断しています。利用する場合は、使用するポートの通信を許可してください。

詳細は、Administrator Guide を参照してください。

無効にする場合は、一覧画面でアイコンをクリックして無効に設定してください。

通知設定が有効になっていても、無効に設定されている「通知先」には通知は送信されません。

- Email

項目	説明
名前	登録する「通知先」の名前です。
送信先アドレス	送信先の電子メールアドレスです。

通知手段として、Email を使用する場合は、メールサーバの設定が必要です。

画面上部にある「通知メール設定」ボタンをクリックします。下図の通知メール設定画面が表示されます。

図 232：通知メール設定画面

必要な項目に入力を行い、[保存]ボタンをクリックします。

- Syslog

項目	説明
名前	登録する「通知先」の名前です。
サーバ	Syslog サーバの IP アドレスです。
UDP プロトコル	Syslog サーバの UDP ポート番号です。
危険度	通知する Syslog の危険度を指定してください。選択可能な項目は以下の通りです。 Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug

- Trap

項目	説明
名前	登録する「通知先」の名前です。
通知先 IP アドレス	SNMP マネージャの IP アドレスです。
ポート	SNMP マネージャのポート番号です。
バージョン	SNMP のバージョンです。 選択可能なバージョンは、1 または 2c です。
コミュニティ	SNMP のコミュニティ名です。

14.3.2. 通知グループの設定

アラートごとの通知の設定は、通知グループを作成する必要があります。

通知グループは、[構成]メニュー>「通知グループ」で設定・管理します。

本画面で作成した通知グループは、下記の機能で使用できます。

- キャプチャオプションの通知
  - 自動保存
  - リンクステータス
  - パケットドロップ
- DLC, ARP, NPM, ARP のアラート
- 周期レポートの送付先(E-mail のみ)
- マイクロバーストのアラート

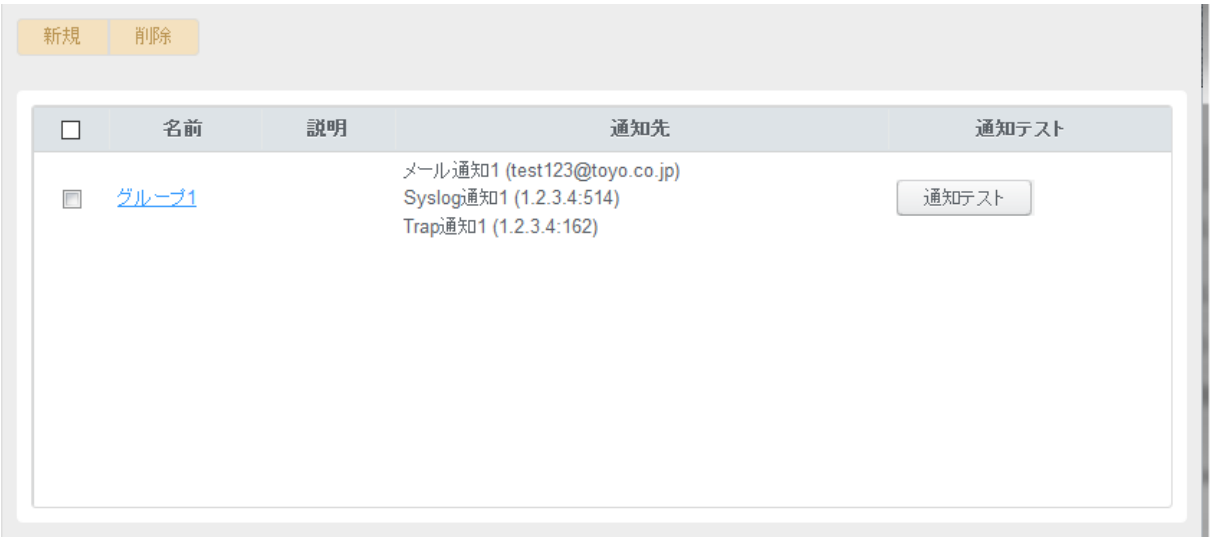


図 233：[構成]メニュー>「通知グループ」

新しく通知グループを登録する場合は画面左上の[新規]ボタンをクリックします。

下図の通知グループ登録画面が表示されます。

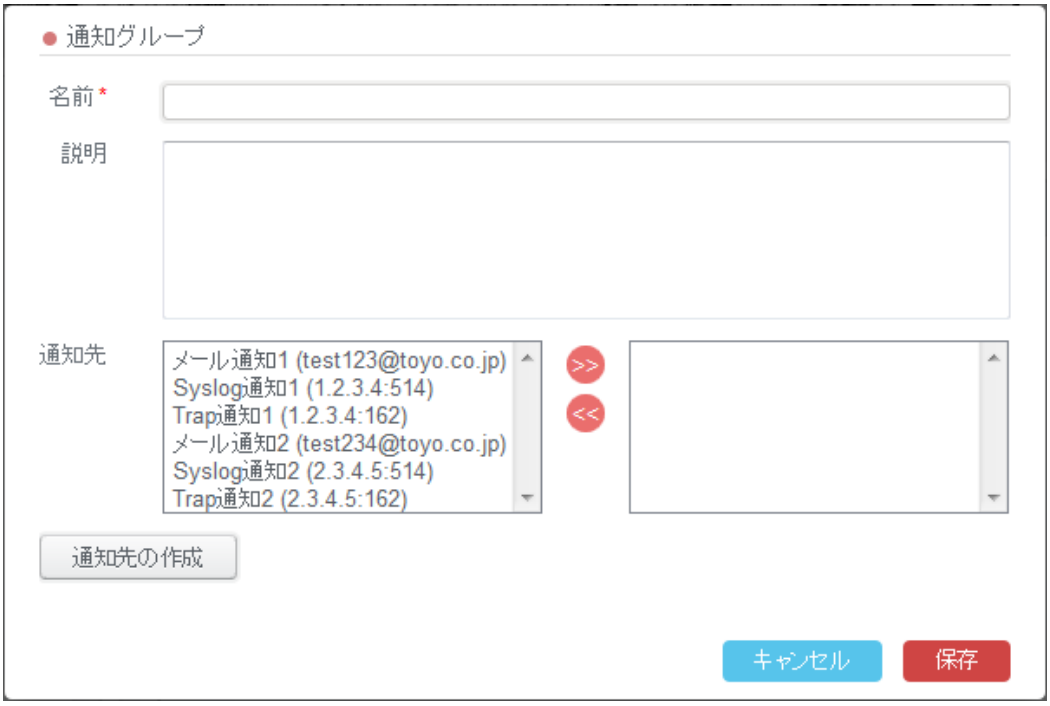


図 234：通知グループ設定画面

設定項目は、以下の通りです。

項目	説明
名前	通知グループの名前です。
説明	通知グループの説明です。
通知先	右側の欄(ディフォルトでは空欄)にリストアップされた通知先が通知グループに登録されます。左側の欄には SYNESIS 内で登録済の通知先がリストアップされます。 左側のリストからする通知先を選択し、 >> アイコンをクリックします。選択した通知先が右側のリストに追加されます。 通知先を定義する場合はする、「通知先の作成」ボタンをクリックして、通知先を追加します。 右側のリストから外す場合は、する該当の通知先を選択し、 << アイコンをクリックします。

「通知グループ」登録後に「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ます。 SYNESIS から正しく通知が送信された場合に、ステータスが「成功」となります。ただし、通知テストの「成功」はあくまでも送信の成功であり、受信の成功ではありません。

14.3.3. 通知設定の確認

[構成]メニュー>「通知設定」では、登録済みのアラートに対する通知グループと通知先の設定が一覧で確認できます。有効/無効の設定もこの画面から行います。

図 235：通知設定メニュー画面

各項目の詳細は、以下の通りです

項目		説明
名前		通知設定が登録されているイベントの名前が表示されます。 アラート設定やレポートプランの名前や、 キャプチャオプションの通知設定の各項目名 「Auto Backup」「Link Status」「Packet Drop」が表示されます。
有効	OFF	通知が無効な状態です。
	ON	通知が有効な状態です。
通知グループ		指定した「通知グループ」です。
通知先		指定した「通知グループ」に登録されている「通知先」がリストアップされています。 個々の「通知先」の名前と実際の連絡先が確認できます。

15.ユーザと認証

SYNESIS にログインをするユーザと認証について説明します。

ユーザは、[構成]メニュー>「ユーザ」で登録・管理を行います。

認証は、ローカルまたは外部で行います。外部認証は、RADIUS に対応しています。

図 236：[構成]メニュー>「ユーザ」

「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。

表示される情報は「名前」、「フルネーム」、「ロール」です。

「ロール」には以下 2 種類が存在します。

- 管理者：すべての機能を利用可能
- ユーザ：一部の機能に制限

15.1. ユーザの登録・管理

ユーザの登録の手順は、以下の通りです。

- ユーザの新規登録

ユーザを新規登録する場合は、ユーザリストの左上の[新規]ボタンをクリックします。

下記のユーザプロファイルダイアログが表示されます。

図 237 :「ユーザプロファイル」ダイアログ

[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。

設定項目は、以下の通りです。

項目	機能制限
ユーザ名	登録するユーザのユーザ ID を入力します。 半角、全角文字が使用可能です。 詳細は、ユーザ名・パスワードの使用可能文字を参照してください。
パスワード	登録するユーザのパスワードを入力します。ユーザ名とパスワードが一致した場合、サインインが可能となります。 半角、全角文字が使用可能です。 詳細は、ユーザ名・パスワードの使用可能文字を参照してください。
パスワードの確認	確認のため「パスワード」を再度入力します。
名	ユーザの名(ファーストネーム)を入力します。
姓	ユーザの姓(ラストネーム)を入力します。
ロール	登録するユーザのロールを選択します。 選択可能な項目は、「管理者」と「ユーザ」です。 各ロールが許可されている操作の詳細は、**ユーザの機能制限**を参照してください。

ユーザ名、パスワードには半角、全角文字が使用可能です。入力制限は以下の通りです。

ユーザ名・パスワードの使用可能文字

項目		入力制限
ユーザ名	**文字数**	50 文字(50 バイト)以下
	文字列	下記の特殊文字は利用できません。 ! # $ % & = ~ ^ | ¥ ` @ + * , ? (半角) ！ ＃ ＄ ％ ＆ ＝ ～ ＾ ｀ ｜ ￥ ‘ ＠ ＋ ＊ 、 。 ？ (全角)
パスワード	**文字数**	30 文字(30 バイト)以下
	文字列	下記の特殊文字は利用できません。 ! # $ % & = ~ ^ | ¥ ` @ + * , ? (半角) ！ ＃ ＄ ％ ＆ ＝ ～ ＾ ｀ ｜ ￥ ‘ ＠ ＋ ＊ 、 。 ？ (全角)

- ユーザの編集

登録済みのユーザの登録情報を編集する場合は、一覧表の名前のリンク部分をクリックします。ユーザプロファイ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。

- ユーザの削除

ユーザを削除する場合は、する該当の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ます。

すべての登録ユーザを削除する場合は、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ます。

15.2. ユーザの機能制限

「管理者」は、SYNESIS の全ての機能が利用可能なユーザです。「ユーザ」は、機能が一部制限されているユーザです。

以下が「ユーザ」権限で許可されていない操作です。

項目	機能制限
管理者	なし
ユーザ	・キャプチャを開始/停止できない。 ・パケットリプレイヤーの再生/一時停止/停止ができない。 ・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 ・キャプチャレコードを削除できない。 ・キャプチャレコードのロックの設定・解除が行えない。 ・統計値の CSV ファイルを作成できない。 ・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 ・ユーザの新規登録・管理が行えない。 ・解析用の保存フィルタの新規作成・編集が行えない。 ・キャプチャレコードの外部書き出しが行えない。 ・外部からのトレースファイルの読込み・参照が行えない。 ・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。 ・MFA のプロファイルの作成・削除・設定変更が行えない。 ・パケットリプレイヤーのプロファイルの作成・削除・設定変更が行えない。

15.3.　デフォルトユーザの扱い

デフォルトユーザとして、以下のユーザが登録されています。

- ユーザ名：admin
- パスワード：synesis1 (初期設定)
- ロール：管理者

このユーザは一覧に表示されず、削除およびロール変更はできません。

パスワードは、admin でサインインの上、画面右上のアクティブユーザプロファイル ボタンをクリックして変更を行います。

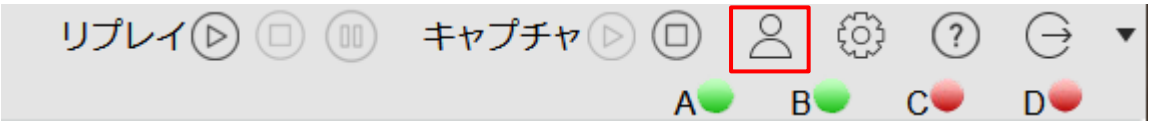


図 238：アクティブユーザプロファイルボタン

15.4.　外部認証

ユーザの認証をローカルではなく外部認証で行うことが可能です。

[構成]メニュー>「外部認証」で、ユーザ認証として外部認証サーバを設定します。

外部認証として対応しているプロトコルは、RADIUS です。

外部認証サーバを利用する際には、外部認証サーバに登録されているユーザと SYNESIS の「ユーザ」を一致させる必要があります。指定された外部認証サーバを利用している他のシステムと共通のパスワードで SYNESIS にサインインできるようになります。

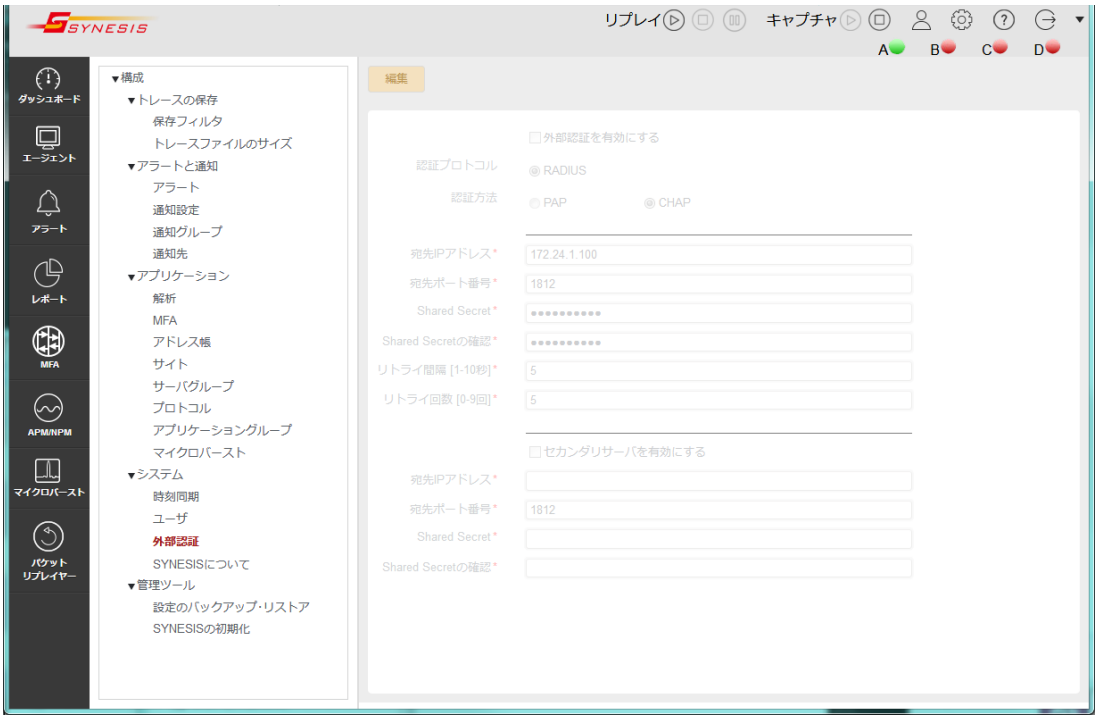


図 239：[構成]メニュー>「外部認証」

外部認証の登録・変更を行う場合は、[編集]ボタンをクリックし、「外部認証を有効にする」にチェ

ックします。 以下のように各設定項目が有効になります。

図 240：外部認証編集画面

各項目入力後、[保存]ボタンをクリックします。

設定項目は、以下の通りです。

項目	機能制限
外部認証を有効にする	チェックを入れると、外部認証の各設定項目が入力可能になります。
認証プロトコル	選択可能な認証プロトコルは「RADIUS」です。
認証方法	接続の際に使用される認証方法を指定します。 「PAP」「CHAP」から選択します。
認証サーバ IP アドレス	認証サーバの IP アドレスを入力します。 IPv4 アドレスのみ有効です。
宛先ポート番号	認証サーバの宛先ポート番号を 入力します。 1 以上 65535 以下の整数で入力してください。
Shared Secret	外部認証サーバの Shared Secret(32 文字以下)を入力します。
Shared Secret の確認	再度外部認証サーバの Shared Secret(32 文字以下)を入力します。
リトライ間隔	通信に失敗した場合のリトライ間隔を秒数で指定します。 1 以上 10 以下の整数で入力してください。
リトライ回数	最初の通信に失敗した後で、何度リトライするかを指定します。 0 以上 9 以下の整数で入力してください。
セカンダリサーバを有効にする	セカンダリサーバを指定する場合は、チェックボックスにチェックを入れてください。
宛先 IP アドレス	セカンダリサーバの IP アドレスを入力してください。

宛先ポート番号	セカンダリサーバの宛先ポート番号を 1 以上 65535 以下の整数で入力してください。
Shared Secret	セカンダリサーバの Shared Secret(32 文字以下)を入力してください。
Shared Secret の確認	再度、セカンダリサーバの Shared Secret(32 文字以下)を入力してください。

外部認証を有効にすると、SYNESIS のサインイン画面に「ローカル認証モード」のチェックボックスが表示されます。

図 241：ローカル認証モードのサインイン画面

部認証サーバやそのサーバ間との通信に問題が発生した場合は、「ローカル認証モード」にチェックをします。ローカルでサインインすることが可能になります。

15.4.1. 外部認証に関する制限事項

- RADIUS による外部認証が有効な状態であっても、RESTful API はローカルユーザで認証されます。
- SYNESIS で作成したユーザは、RADIUS から LDAP への連携はサポートしていません。

16. 時刻同期

時刻同期について説明します。

SYNESIS は、以下の手段で時刻同期が可能です。

- NTP
- PPS＋NTP
- PTP

PPS＋NTP、PTP 同期は、モデルにより対応していません。詳細は、SYNESIS の諸元一覧を参照してください。

NTP サーバとの接続は、マネージメントポートを使用します。

PPS および PTP のインターフェイスとの接続は、キャプチャアダプタ上の接続端子または別売りの変換コネクタを使用します。接続端子およびリンク速度はキャプチャアダプタにより異なります。詳細は、以下の通りです。

キャプチャアダプタ	PPS 同期	PTP 同期
SYxC-100G2N1-HP SYxC-100G2N2-HP	SMA 端子を使用します	専用のイーサネットポートを使用します 10/100/1000BASE-T に対応しています
上記以外のアダプタ	変換コネクタ TSA-PTP-RJ45/SMA を使用します PTP 同期は 10/100BASE-T のみ対応しています。	

16.1. NTP サーバとの時刻同期

複数の NTP(Network Time Protocol)サーバに問い合わせを行い、OS の時刻を正確に調整します。

NTP サーバとの接続は、マネージメントポートを使用します。

[構成]メニュー>「時刻同期」で、時刻同期先の NTP サーバを指定します。

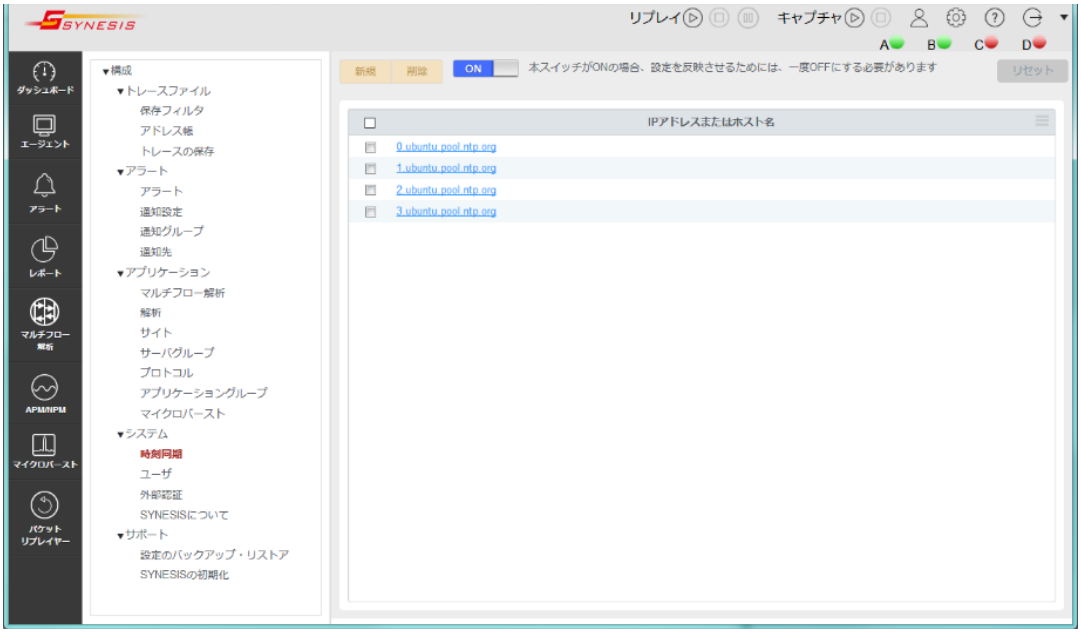


図 242：[構成]メニュー>「時刻同期」

初期設定では、４つの ubuntuNTP サーバが登録されています。

変更する場合は、NTP サーバのリンクをクリックします。「時刻同期」ダイアログが表示されます。

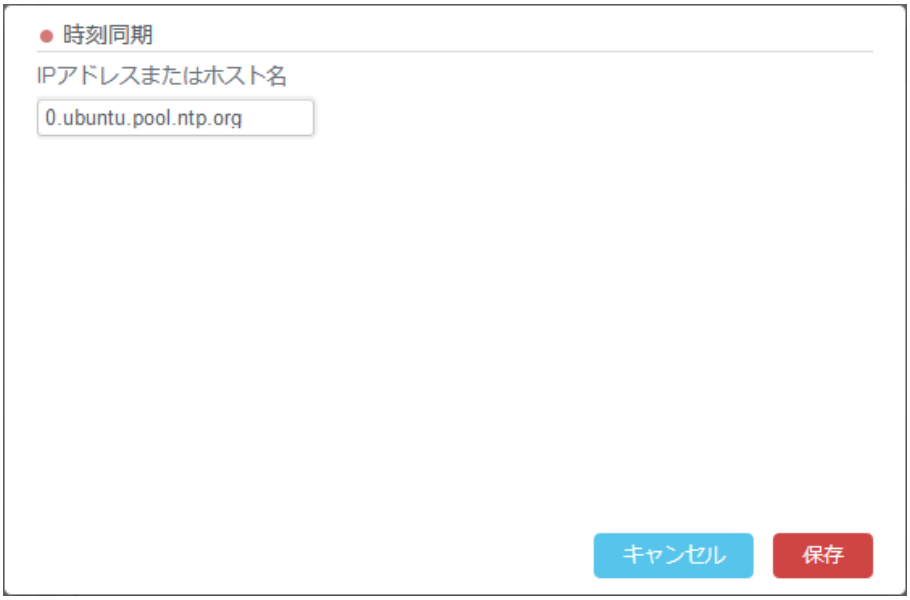


図 243：時刻同期ダイアログ

NTP サーバを新規登録する場合は、[新規]ボタンをクリックします。

登録済みの NTP サーバを削除する場合は、該当する 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ます。選択した NTP サーバが一覧から削除されます。

登録が完了したら、画面左上のスイッチをクリックして、ON に切り替えます。 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]ボタンをクリックすると NTP サーバリストが初期設定に戻り、時刻同期が停止します。

16.2. PPS＋NTP 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。

PPS＋NTP 時刻同期により、NTP 以上の精度で時刻同期が可能です。

PPS インターフェイスとの接続は、キャプチャアダプタ上の SMA 接続端子または別売りの変換コネクタを使用します。

NTP サーバとの接続は、マネージメントポートを使用します。

16.2.1. PPS＋NTP 時刻同期の設定手順

設定手順は、以下の通りです。

1. SMA 端子または変換コネクタから PPS 信号を入力します。複数のアダプタを搭載したモデルでは、アダプタ 0 に PPS 信号を入力します。
2. NTP サーバの設定を確認します。「構成」 メニューの「時刻同期」を選択します。

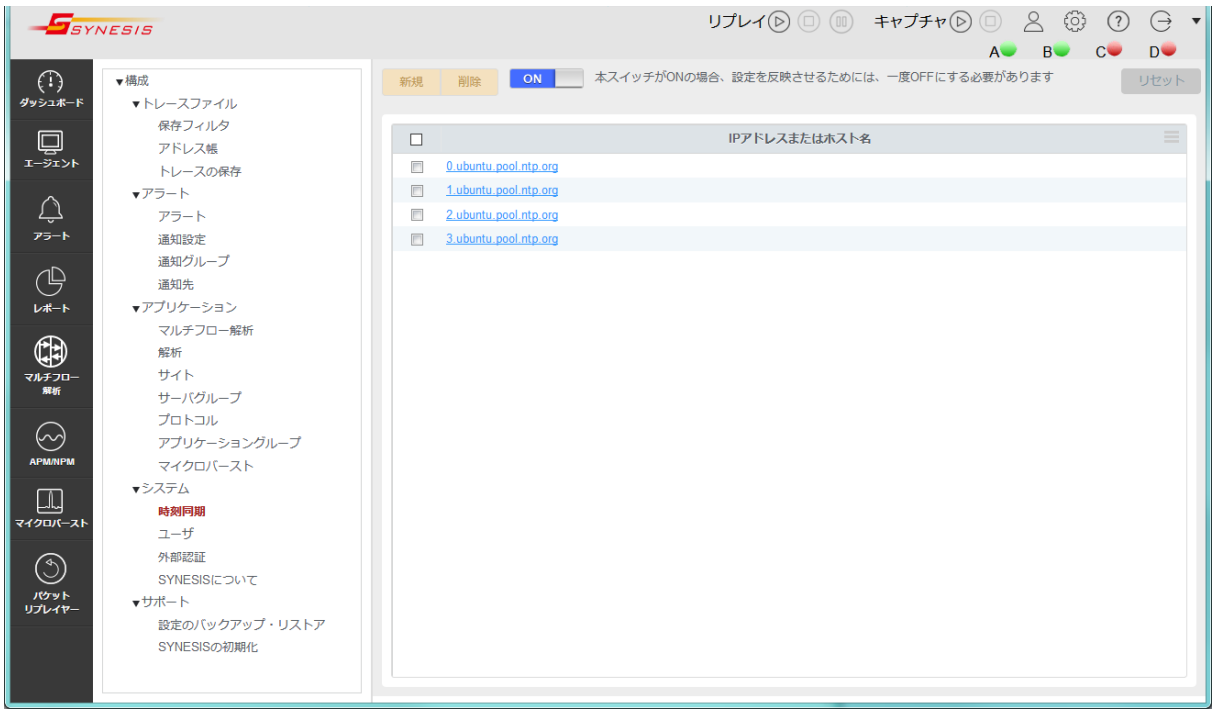


図 244：[構成]メニュー>「時刻同期」

3. PPS 時刻同期は、NTP で時刻同期した OS の時刻と PPS 信号を共に使用するため、NTP サーバの設定が必要となります。

   NTP サーバを設定した上で、画面左上の ON/OFF ボタンが ON になっていることを確認します。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。

4. TeraTerm またはコンソールから Terminal を起動します。

   以下は TeraTerm から操作する場合の例になります。

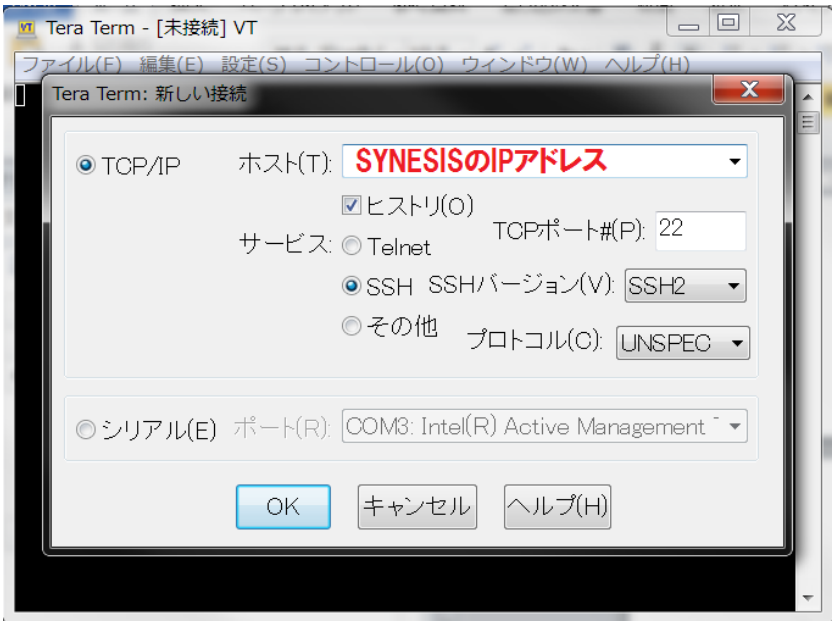


図 245：TeraTerm 起動画面

5. 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ます。

6. OS のユーザ名とパスワードの入力を求められますので、OS のユーザ名とパスワードを入力してます。SYNESIS に SSH で接続されます。

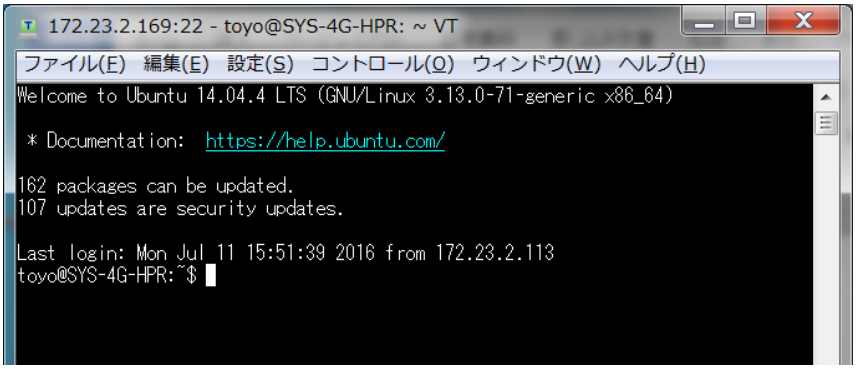


図 246：SSH 接続画面

7. ブラウザを起動し、"https://[SYNESIS IP]/mgmt/" から SYNESIS Management Console にアクセスします。

   管理画面のユーザ名とパスワードの入力を求められますので、ユーザ名とパスワードを入力します。

8. NetKeeper サービスの[Stop]ボタンをクリックします。

   NetKeeper を停止すると、実行中のキャプチャは停止します。

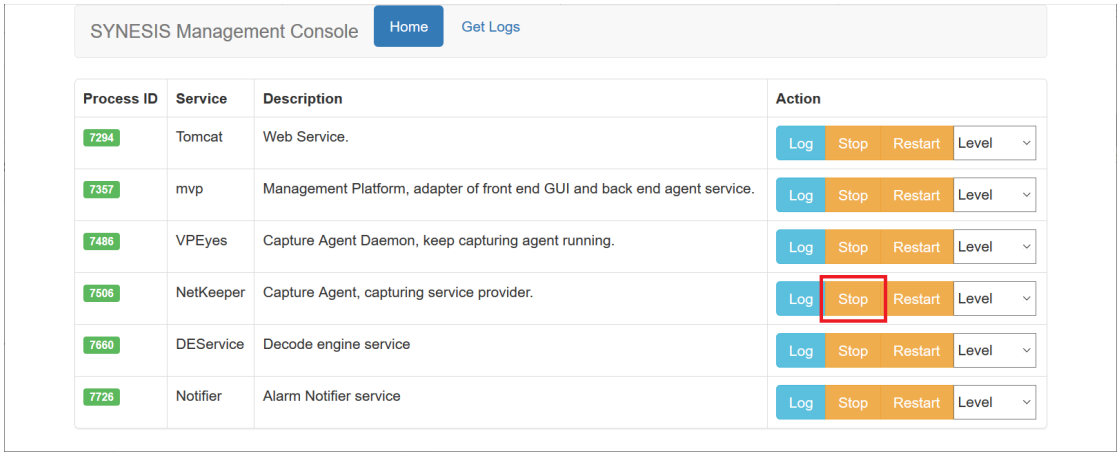


図 247：SYNESIS 管理画面

9. 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ます。 NetKeeper が停止すると、VPEyes プロセスも同時に停止します。

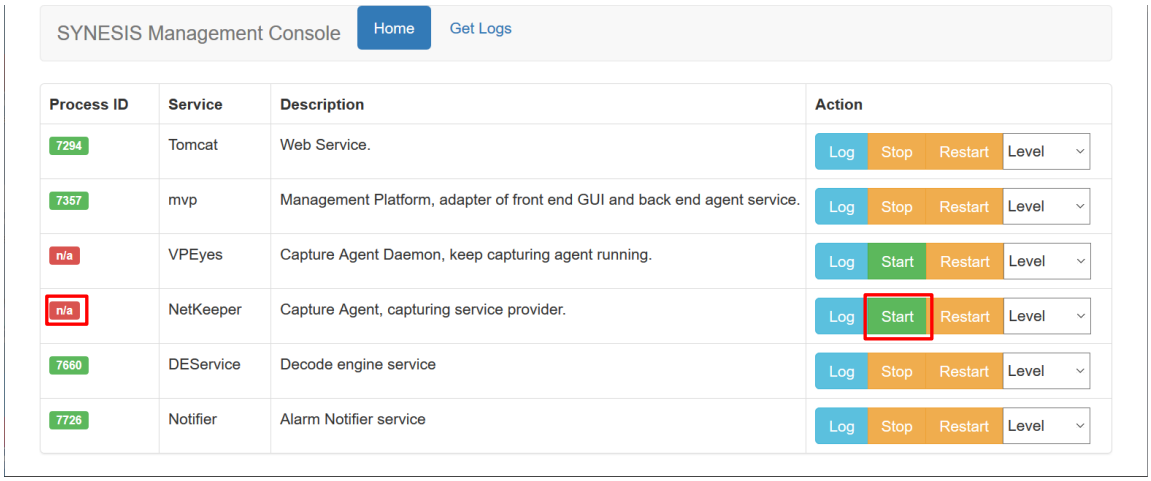


図 248：SYNESIS 管理画面-Netkeeper 停止時

10. 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 またはコンソール上の Terminal で下記のコマンドを実行します。

```
$ sudo cp /opt/napatech3/config/ntservice.ini /opt/napatech3/config/ntservice.ini.org
```

11. アダプタの設定ファイルを開きます。

```
$ sudo vi /opt/napatech3/config/ntservice.ini
```

12. 設定ファイルの [TimeSyncConnectorExt1] の項目を [PpsIn] に変更します。

【変更前】

```
TimeSyncConnectorExt1 = NttsIn          # None - NttsIn* - PpsIn - NttsOut - PpsOut
- RepeatInt1 - RepeatInt2
```

【変更後】

```
TimeSyncConnectorExt1 = PpsIn           # None - NttsIn* - PpsIn - NttsOut - PpsOut
 - RepeatInt1 - RepeatInt2
```

アダプタが 2 枚以上の場合は、[Adapter0]と[Adapter1]の設定箇所があります。
[Adapter0]に対してのみ変更を行ってください。

13. 下記の 2 つ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。

① サービス停止

```
$ sudo /opt/napatech3/bin/ntstop.sh
```

以下のメッセージが表示されます。

```
Stopping NTService (this may take a while)
NTService stopped                                   [Done]
```

② サービス開始

```
$ sudo /opt/napatech3/bin/ntstart.sh
```

以下のメッセージが表示されます。

```
Starting NTService (this may take a while)          [Done]
```

14. SYNESIS Management Console にアクセスし、NetKeeper サービスの[Start]ボタンをクリックします。

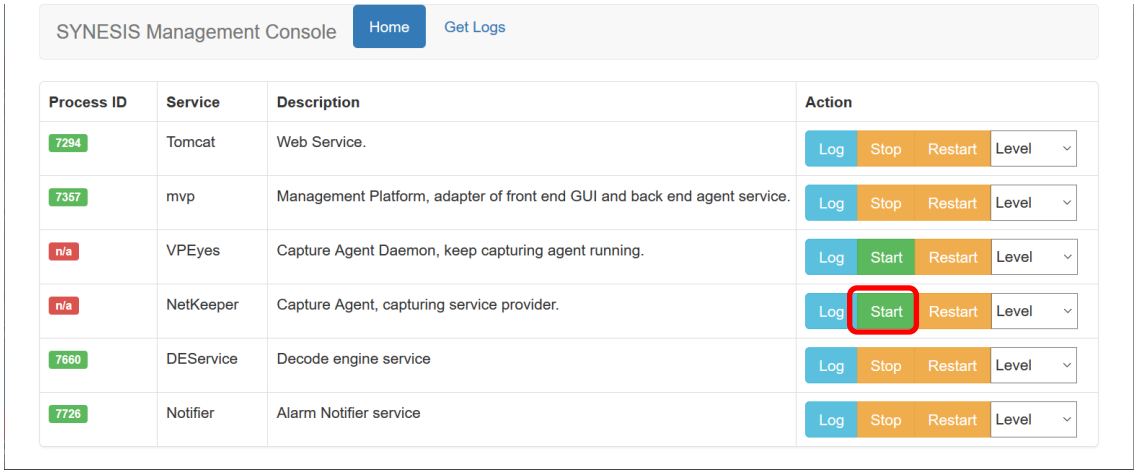


図 249：Netkeeper の Start ボタン

15. 下記コマンドを実行し、OS から取得した時刻を PPS 信号で補正するようにします。

```
$ sudo /usr/local/synesis/synesis_tools/PPS/pps_os_toyo
```

以下のメッセージが表示されます。

```
PPS signal found on adapter 0
0: PPS not in SYNC: UTC Time : Thu 20-Apr-2017 05:19:18.000171290   ClockSkew   :
      171298 nano seconds
:       171298 nano seconds
```

”ClockSkew”が 0 nano seconds 付近に落ち着くまで待ちます。

```
PPS signal found on adapter 0
0: PPS in SYNC:     UTC Time : Thu 20-Apr-2017 05:22:06.000000000   ClockSkew
:            0 nano seconds
```

16. 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、キャプチャの開始・停止の章を参照してください。
17. <Ctrl+C>キーを押下し、/opt/napatech3/bin/pps_os コマンドを終了させると同期は停止します。

16.2.2. PPS＋NTP 時刻同期の際の注意点

- 前述の手順 15）を実行すると、PPS の同期が始まります。
  以下の場合は、PPS の同期が外れますので、再度手順 15）から開始をする必要があります。
  - <Ctrl+C>キーを押下した場合
  - 電源を落とした場合
- キャプチャ中に前述の手順 15）を行った場合、キャプチャは停止します。
- PPS の同期を行った状態で同期ケーブルを抜いた場合は、再度同期をする際に<Ctrl+C>キーで一旦同期を停止したあと、再度手順 15)を行ってください。この作業を行わないで時刻同期を続けた場合、同期までに時間がかかる可能性があります。

16.3. PTP 時刻同期の設定手順

PTP(Precision Time Protcol)時刻同期は、利用環境を LAN に制限することで高精度な時刻同期を行うことが可能な同期方式です。

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 1μs(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。

PTP サーバとの接続は、キャプチャアダプタ上のイーサネットポートまたは別売りの変換コネクタを使用します。

対応プロトコルは、以下の通りです。

プロファイル	プロファイル ID
Default	00-1B-19-00-01-00
Telecom (G.8265.1)	00-19-A7-00-01-00
Telecom (G.8275.1)	00-19-A7-01-02-00

16.3.1. PTP 時刻同期の設定手順

設定手順は、以下の通りです。

1. アダプタのイーサネットポートまたは変換コネクタに PTP 信号を入力します。複数のアダプタを搭載したモデルでは、アダプタ 0 に PPS 信号を入力します。
2. NTP サーバの設定を確認します。「構成」 メニューの「時刻同期」を選択します。

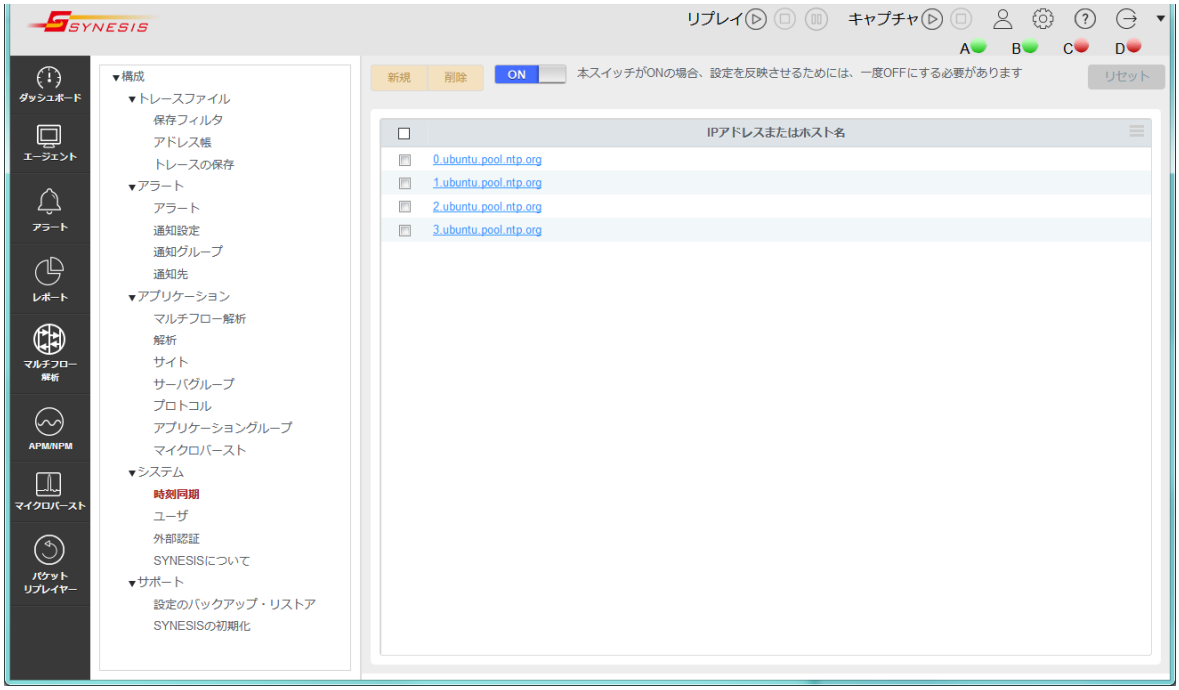


図 250：[構成]メニュー>「時刻同期」

3. 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ます。ON になっていた場合はボタンをクリックして、OFF に切替えます。
4. TeraTerm またはコンソールから Terminal を起動します。
   以下は TeraTerm から操作する場合の例になります。

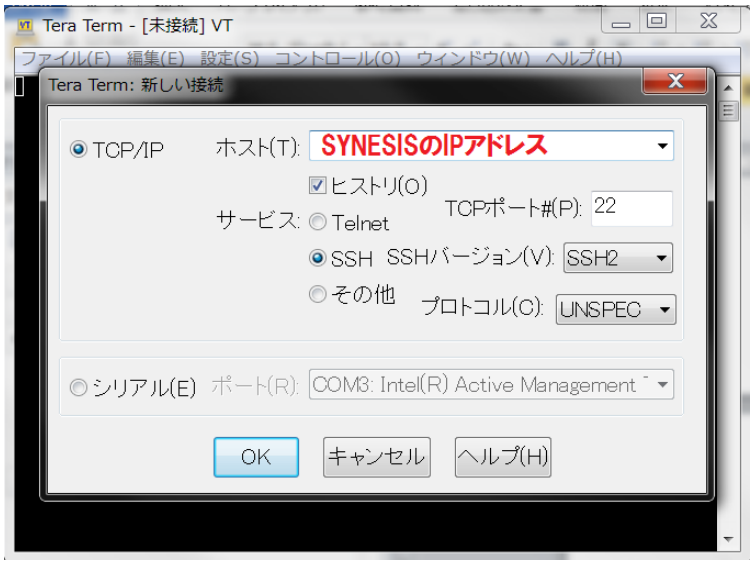


図 251：TeraTerm 起動画面

5. 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ます。
6. OS のユーザ名とパスワードの入力を求められますので、OS のユーザ名とパスワードを入力します。SYNESIS に SSH で接続されます。

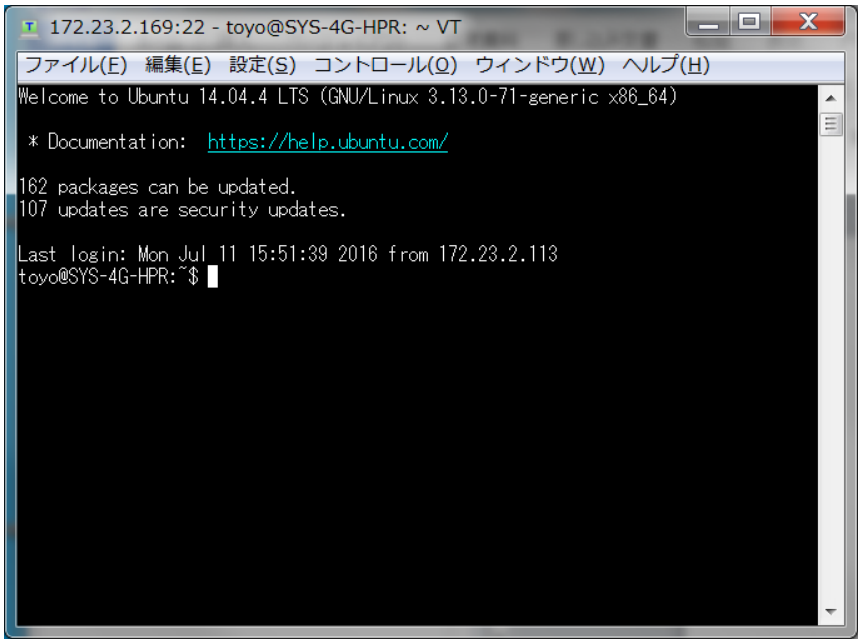


図 252 : SSH 接続画面

7. ブラウザを起動し、"https://[SYNESIS IP]/mgmt/" から SYNESIS Management Console にアクセスします。
   管理画面のユーザ名とパスワードの入力を求められますので、ユーザ名とパスワードを入力します。
8. NetKeeper サービスの[Stop]ボタンをクリックします。
   NetKeeper を停止すると、実行中のキャプチャは停止します。

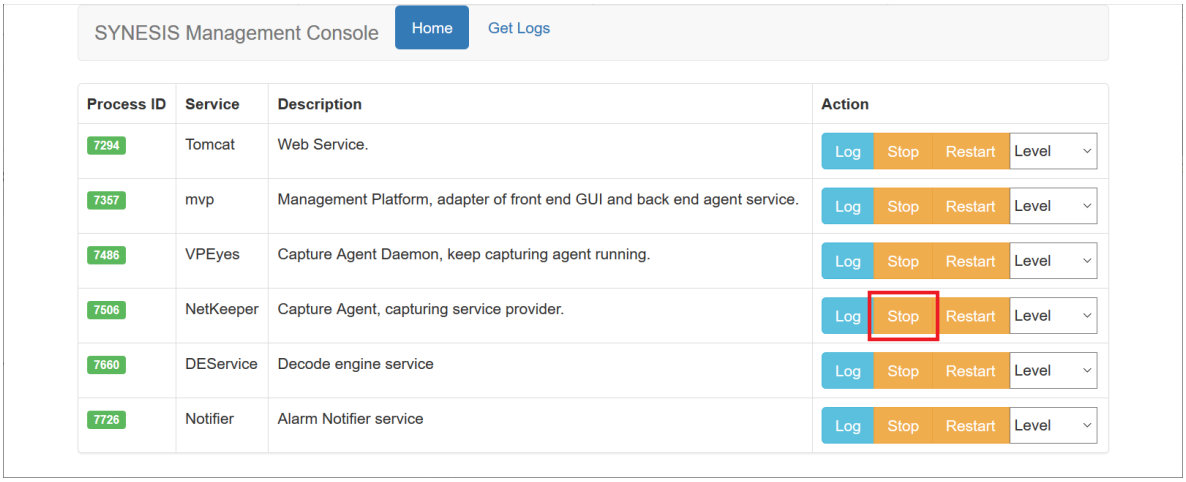


図 253 : SYNESIS 管理画面

9. 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ます。 NetKeeper が停止すると、VPEyes プロセスも同時に停止します。

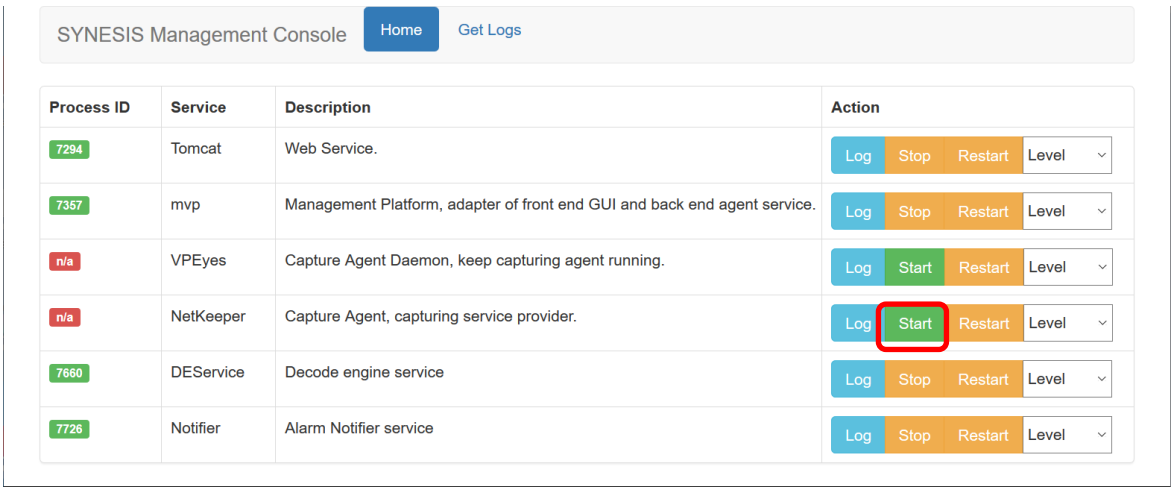


図 254：Netkeeper の Start ボタン

10. 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 またはコンソール上の Terminal で下記のコマンドを実行します。

```
$ sudo cp /opt/napatech3/config/ntservice.ini /opt/napatech3/config/ntservice.ini.org
```

11. 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
```

    アダプタが 2 枚以上の場合は、[Adapter0]と[Adapter1]の設定箇所があります。

    [Adapter0]に対してのみ変更を行ってください。

12. [TimeSyncReferencePriority] の項目を [PTP, FreeRun] に変更します。

    【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
```

13. 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、[PtpIpAddr]、[PtNetMask]、[PtpGw]に実際に使用する固定 IP アドレスを入力します。

    【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
```

14. 使用する PTP Profile に合わせた設定を反映させます。

【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(G.8265.1)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。

Telecom (G.8275.1)のプロファイルを適用する場合は、東陽テクニカまでお問い合わせください。

15. SYNESIS の OS の時刻を PTP 同期したアダプタの時刻に同期させます。

[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 - a
dapter-2 - adapter-3 - adapter-4 - adapter-5 - adapter-6 - adapter-7
```

【変更後】

```
[System]
TimeSyncOsTimeReference = adapter-0     # None* - adapter-0 - adapter-1 - ad
apter-2 - adapter-3 - adapter-4 - adapter-5 - adapter-6 - adapter-7
```

16. 下記の２つ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。

③　サービス停止

```
$ sudo /opt/napatech3/bin/ntstop.sh
```

以下のメッセージが表示されます。

```
Stopping NTService (this may take a while)
NTService stopped                                    [Done]
```

④　サービス開始

```
$ sudo /opt/napatech3/bin/ntstart.sh
```

以下のメッセージが表示されます。

```
Starting NTService (this may take a while)          [Done]
```

17. 時刻同期が正常になされていることを確認します。下記コマンドを実行します。

```
$ sudo /opt/napatech3/bin/monitoring
```

18. アダプタの使用状況を確認するためのツールが起動します。

<Shift+x>キーで画面を切り替えてください。

19. Current reference が ”PTP” になっていれば成功です。

アダプタが複数ある場合には、Adapter 0 のみ Current reference が ”PTP”になります。

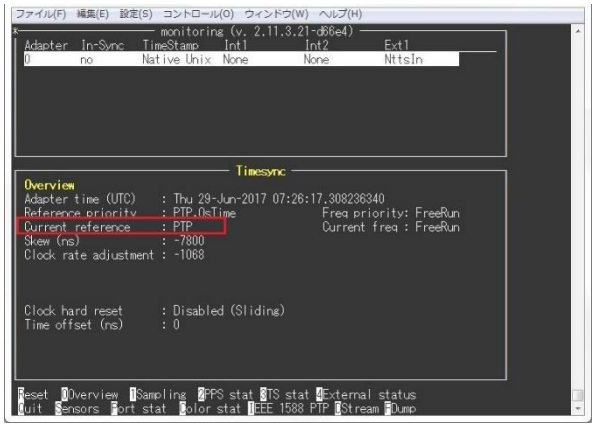


図 255：モニタリングツール

20. 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ます。

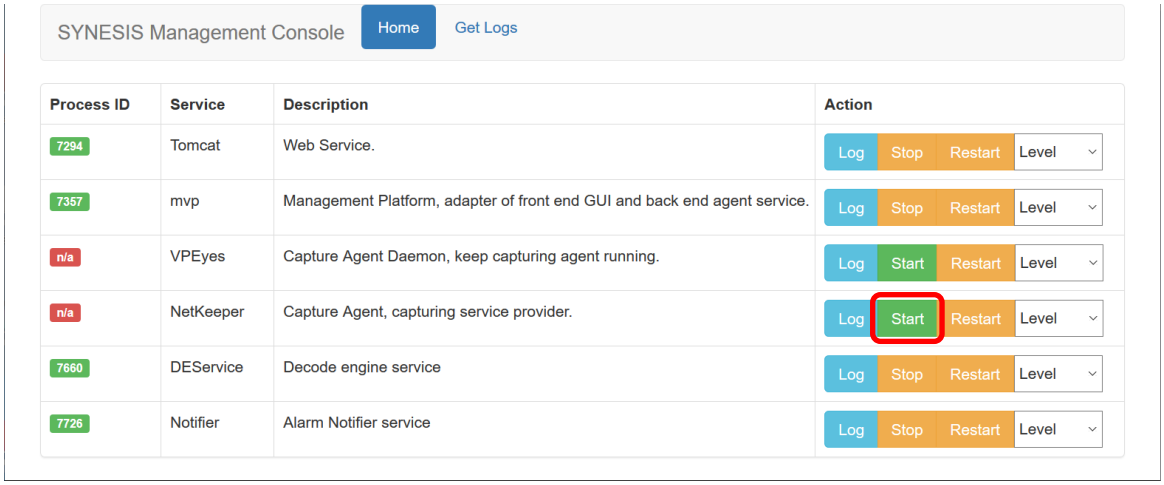


図 256：Netkeeper の Start ボタン

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、**4.1. キャプチャの開始**を参照してください。

この設定を行った後は、SYNESIS を再起動した場合も PTP 時刻同期の設定が適用されます。

設定前に戻す場合は **16.3.2. PTP 時刻同期の設定切り戻し** の手順を実行してください。

16.3.2. PTP 時刻同期の設定切り戻し

アダプタの時刻同期の設定を元の OS 時刻同期に戻す場合は、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。

1. ブラウザを起動して、"https://[SYNESIS IP]/mgmt/" から SYNESIS Management Console にアクセスし、 NetKeeper サービスの[Stop]ボタンをクリックします。

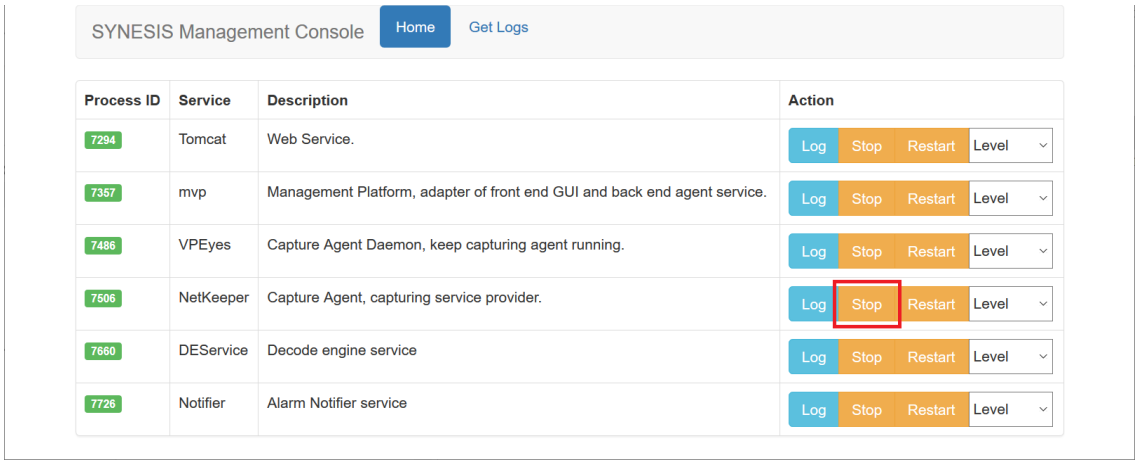


図 257 : SYNESIS の管理画面

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ます。

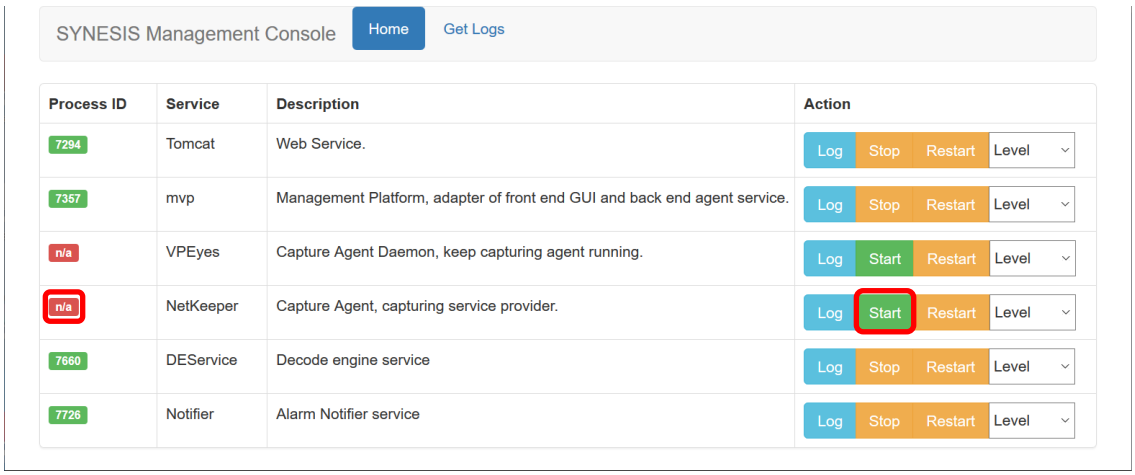


図 258 : Netkeeper の Start ボタン

3. SSH またはコンソールでログインします。
4. PPS 時刻同期用 pps_os が実行中であれば、停止させます。PTP 時刻同期を使用していた場合には不要です。
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ます。

```
$ sudo /opt/napatech3/bin/monitoring
```

8. アダプタの使用状況を確認するための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。

   アダプタが複数ある場合には、Adapter 0 のみ Current reference が " OsTime"になります。

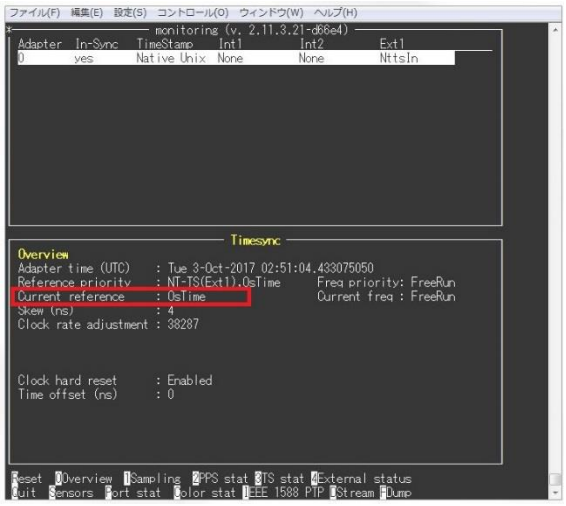


図 259：モニタリングツール

10. 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。

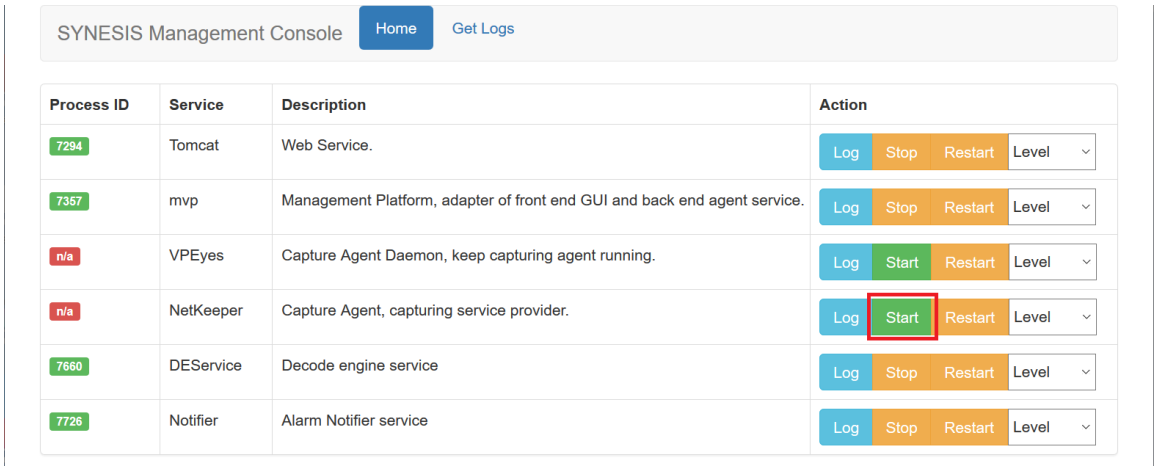


図 260：Netkeeper の Start ボタン

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 **16.1. NTP サーバとの時刻同期** を参照してください。

16.4. 複数のキャプチャアダプタを使用する場合の時刻同期

出荷時のバージョンが V5.0 以降の SYNESIS では、アダプタ間の時刻同期ケーブルが取り付けられています。キャプチャアダプタ #0 が OS 時刻と同期し、キャプチャアダプタ #1 が #0 と同期しています。

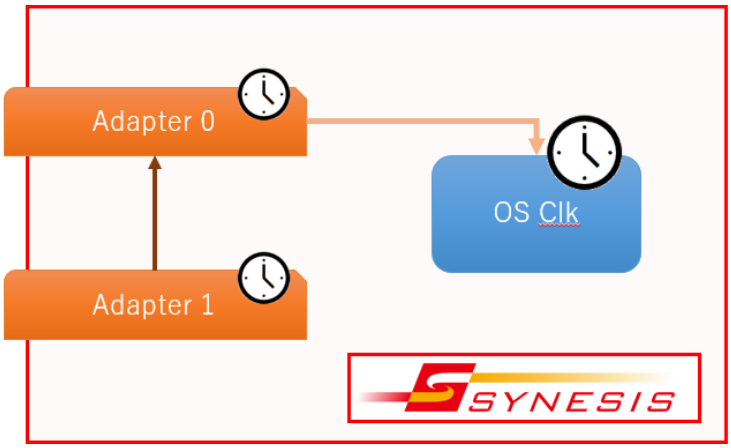


図 261：キャプチャアダプタ間の時刻同期

PPS 時刻同期、PTP 時刻同期を行う場合は、キャプチャアダプタ #0 を外部信号と同期させてください。

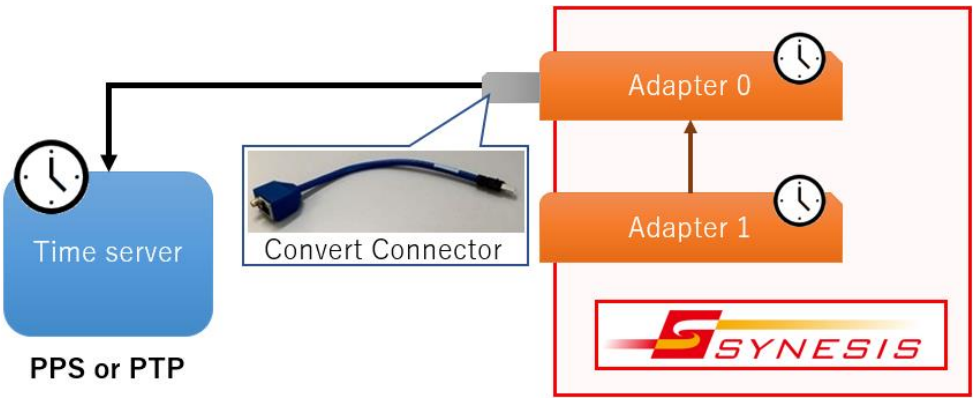


図 262：PPS 時刻同期・PTP 時刻同期

出荷時のバージョンが V4.5 以前の SYNESIS では、キャプチャアダプタ #0, #1 がそれぞれ OS 時刻と同期しています。

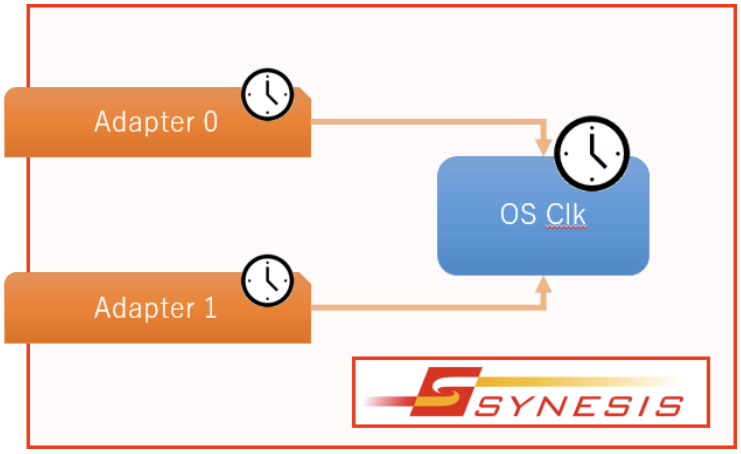


図 263：V4.5 以前の時刻同期

SYNESIS に取り付けられたアダプタ番号については、**SYNESIS について**の画面内で確認できます。

17.管理ツール

SYNESIS の管理ツールについて説明します。

17.1.　設定のバックアップ・リストア

[構成]メニュー>「設定のバックアップ・リストア」は、SYNESIS の設定のバックアップ・リストアを管理します。

バックアップファイルできる設定は、「構成」メニューで設定した項目です。

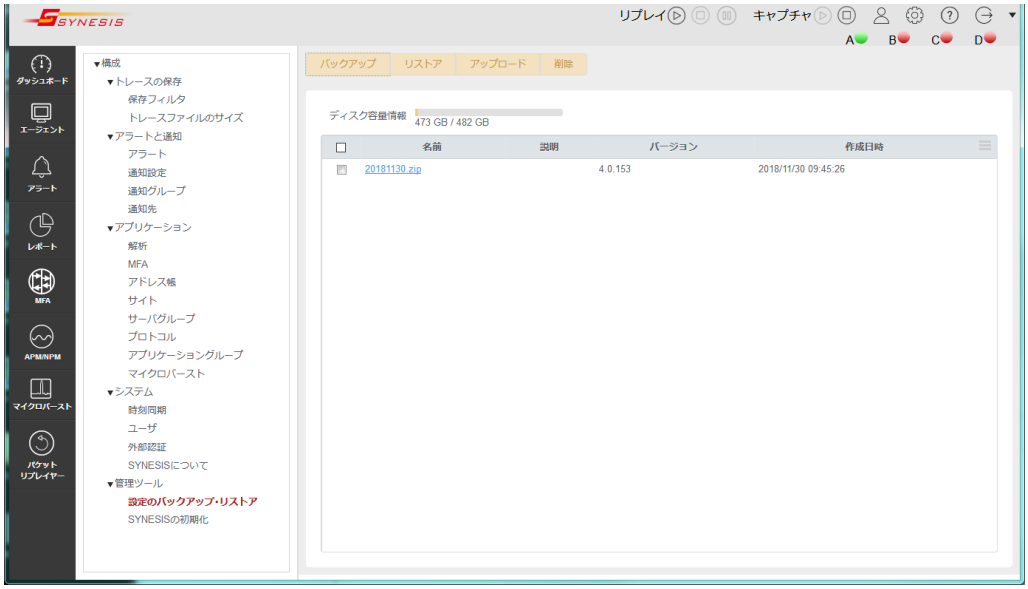


図 264：[構成]メニュー>「設定のバックアップ・リストア」

17.1.1.　設定のバックアップ作成とダウンロード

バックアップファイルを作成する場合は、[バックアップ]ボタンをクリックします。以下の「バックアップ」ダイアログが表示されます。

図 265：バックアップ・ダイアログ

ファイル名と OS(Ubuntu)のユーザ名、パスワードを入力して[適用]ボタンをクリックします。 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。

作成したバックアップファイルをダウンロードする場合は、該当するバックアップファイルの「名前」のリンクをクリックします。

以下の「バックアップファイルの編集・ダウンロード」ダイアログが表示されます。

図 266 : バックアップファイルの編集・ダウンロート・ダイアログ

「ダウンロード」ボタンをクリックすると、ローカルディスクに保存できます。

SYNESIS を初期化すると、SYNESIS に保存されていたバックアップファイルは削除されます。初期化を行った後でもう一度初期化前の設定に戻す場合は、初期化を実行する前にバックアップファイルを外部ストレージに退避する必要があります。

17.1.2. 設定のリストア

設定のバックアップファイルをリストアすることで、SYNESIS をバックアップファイル作成時の設定に戻すことができます。

適用する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入れ、画面左上の「リストア」ボタンをクリックします。

ユーザ名とパスワードの入力を求められますので、バックアップファイルを作成した際に入力した OS(Ubuntu)のユーザ名とパスワードを入力します。 バックアップファイルに保存した設定が読み込まれ、SYNESIS の設定ファイルの各項目が上書きされます。

リストア実施後は、SYNESIS の再起動が必要です。外部ストレージにバックアップした設定は、一度 SYNESIS 上にアップロードの上、リストアをする必要があります。

17.1.3. バックアップファイルのアップロード

「アップロード」ボタンをクリックすると、以下の「アップロード」ダイアログが表示されます。

図 267：バックアップファイルのアップロード・ダイアログ

[参照]で外部ストレージに保存したバックアップファイルを選択します。

[アップロード]ボタンをクリックすると、外部から読み込まれたバックアップファイルが一覧に追加されます。

17.1.4. 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する場合は、該当する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ます。

選択したバックアップファイルが削除されます。

保存されているバックアップファイルをすべて削除する場合は、一番上の項目名欄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ます。

全てのバックアップファイルのチェックボックスにチェックが付けられ、全てのバックアップファイルが削除されます。

17.1.5. バックアップ対象一覧

設定のバックアップで取得する設定対象の一覧です。

トレースファイル及びレコードなどのデータファイルはバックアップ対象外です。

メニュー名	タブ・設定項目		
ダッシュボード	概要(default)		
	追加ダッシュボード		
エージェント	概要	キャプチャオプション	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
			チャネル設定
			通知設定
	レポートリスト		

レポート	レポート―テンプレート
	レポートプラン
MFA	プロファイル
マイクロバースト	閾値
パケット リプレイヤー	プロファイル
構成	**保存フィルタ**
	トレースファイルのサイズ
	アラート
	通知設定
	通知グループ
	通知先
	解析
	MFA
	アドレス帳
	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
	時刻同期
	ユーザ
	外部認証
	設定のバックアップ・リストア

マルチフロー解析やパケットリプレイヤーのプロファイルは保存されますが、 プロファイルがデータソースとして指定しているトレースファイルやレコードはバックアップでは保存されません。

17.1.6. バックアップ・リストアに関する制限

リストアできる条件は、下記の条件を全て満たすバックアップファイルに限ります。

- コントロールユニット、外部ストレージ、キャプチャモジュールが同一の構成
- メジャーバージョンが同一

条件を満たしていれば、異なる筐体で作成されたバックアップファイルを使ってリストアすることが可能です。

メジャーバージョンとは、V6.x.y の数字 x が一致するものであり、y は一致していなくても構いません。

17.2. SYNESIS の初期化

[構成]メニューの「SYNESIS の初期化」では、SYNESIS の初期化を実行します。

図 268：[構成]メニュー>「SYNESIS の初期化」

初期化を実行する場合は、[データの初期化]ボタンをクリックします。確認のため、下図の警告メッセージが表示されます。

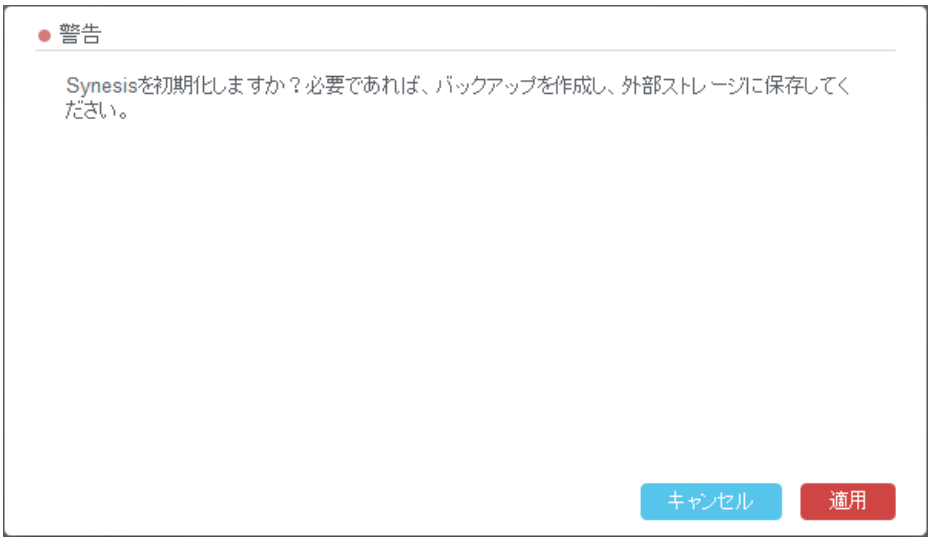


図 269：初期化メッセージ

[適用]ボタンをクリックすると、初期化が開始されます。

トレースファイルや統計情報などのデータが消去され、ユーザ設定が初期化されます。

初期化される項目は、**17.2.1. 初期化対象一覧** を参照してください。

なお、初期化したとしても既にキャプチャしたパケットは SYNESIS のディスクに残りますが、読みだすことは不可能です。

17.2.1. 初期化対象一覧

以下の各設定項目が初期化され、保存されているデータも削除されます。

メニュー名	タブ・設定項目		
ダッシュボード	概要(デフォルトタブ)		
	追加ダッシュボード		
エージェント	概要	キャプチャオプション	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
			チャネル設定
			通知設定
	レコード		
	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
レポート	レポートリスト		
	レポート―テンプレート		
	レポート―プラン		
MFA	プロファイル		
マイクロバースト	閾値		
パケットリプレイヤー	プロファイル		
構成	保存フィルタ		
	トレースファイルのサイズ		
	アラート		
	通知設定		
	通知グループ		
	通知先		
	解析		
	MFA		
	アドレス帳		
	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		
	時刻同期		
	ユーザ		
	外部認証		
	設定のバックアップ・リストア		

カスタムファイルの保存先に ”/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。

17.2.2.　初期化に関する既知の不具合

- 初期化機能を出荷後はじめて実行した場合に失敗することがあります。その場合は、再度初期化を実行すると正常に完了できます。

18. 構成

ツールバー上の構成 ボタンをクリックすると、 画面左に「構成」内の設定メニューがツリー形式で表示されます。

利用する構成メニューをクリックすると、その設定項目のページに移動します。

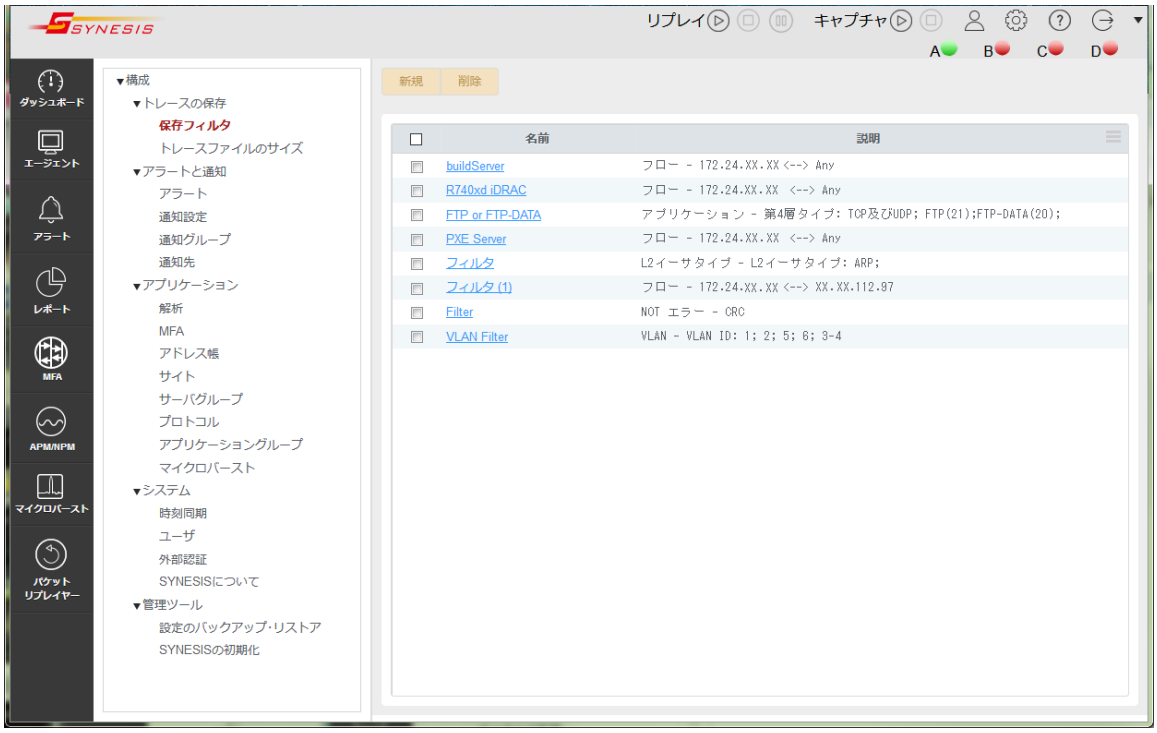


図 270：[構成]メニュー画面

利用可能なメニューの種類と機能は、以下の通りです。

メニュー名	概要
保存フィルタの概要	キャプチャフィルタ以外のフィルタ設定の登録・管理
トレースファイルのサイズ	トレースの保存時のファイルサイズの設定
アラート機能と通知	アラート発生条件の登録・管理
通知設定	設定されている通知設定の一覧
通知グループの設定	通知グループの登録・管理
通知先の設定	通知グループに登録できる連絡先の登録・管理
解析	解析モジュールの選択と解析データの自動削除設定
MFA の表示設定	マルチフロー解析の画面上での設定
アドレス帳の設定	IP アドレスを名前に変換する設定
サイトの設定・管理	サイトの設定
サーバ グループの設定・管理	サーバグループの設定
プロトコルの設定・管理	L2/L3/L4 プロトコルの設定

アプリケーショングループ	アプリケーショングループの設定
マイクロバーストの閾値設定	マイクロバーストの閾値設定
時刻同期	時刻同期させる NTP サーバの登録・管理
ユーザの登録・管理	ユーザの登録・管理
外部認証	RADIUS による外部認証の登録設定
SYNESIS について	使用中の SYNESIS のセットアップ構成の確認
設定のバックアップ・リストア	設定のバックアップ・リストアの管理・実行
SYNESIS の初期化	SYNESIS の初期化の実行

詳細は、各機能の章を参照してください。

Appendix A 用語集

SYNESIS で使用される用語の説明です。

用語	説明
APM 解析	TCP フローごとにコネクションの各段階で要している時間を表示します。フローのどの段階にボトルネックがあるかを確認できます。
DLC	データリンク層(Data Link Control)の略です。 キャプチャしたパケットの統計値情報をまとめて指す場合に使用します。
KPI	Key Performance Indicators の略で、性能や能力を評価するための指標です。機能ごとに KPI はいくつか存在します。
NPM 解析	TCP/UDP フローの IP ペアをホスト単位で KPI を表示します。双方向通信であるフローをそれぞれの方向に対しての通信量とフローの通信状況を把握することができます。
アラート	キャプチャしたデータから閾値を超過したパケットをアラートとして検出することです。 アラートは、[アラート]メニューで確認できます。
エージェント	パケットキャプチャを実行するプロセス、トレース保存や解析などパケットを利用するプロセス、およびそれらが制御するハードウェアの総称です。
解析機能	キャプチャした大量なパケットをインデックス化して、通信の動向を把握することができる機能の一種です。解析機能は、目的別に以下ふたつの機能があります。 ● APM/NPM 解析 ● マイクロバースト解析 解析画面から、フロー、期間を確認し、目的のパケットを簡単に取り出すことが可能です。
スライス	各フレームの先頭からの設定のバイト数までフレームサイズを切り詰める機能です。キャプチャ時、トレースの保存時に適用することが可能です。
通知	イベントがあがった際に Email、Syslog、SNMP Trap による外部通知を行うことです。 イベントとは、以下を指します。 ➢ アラート機能でアラートが検出された場合 ➢ マイクロバースト機能で閾値の超過が検出された場合 ➢ キャプチャオプションのリンクステータス、ドロップ、自動保存で、事象が検出された場合 ➢ 定期レポートの送付（E-mail のみ） 通知は、キャプチャ中のみ行われます。
フロー	IP アドレスおよび TCP/UDP ポート番号の送受信ペアを指します。 APM 解析、MFA は、フロー単位で KPI を計算します。

	APM 解析、MFA、各種フィルタのフローのポート番号は、TCP、UDP のみ対応しています。
マイクロバースト解析	通常 1 秒単位以上で計算される使用率を最小 100μs 単位で計算し、バーストトラフィックが発生した時間を検出します。1 秒では平準化されて検出されない瞬間的なバースト現象を捉えることが可能です。
ラインスピード	回線が単位時間あたりに受信できる最大ビットレートの状態を指します。 統計値及びマイクロバーストの使用率の計算は、ラインスピードを基準に計算されます。
レコード	キャプチャデータを管理する単位です。キャプチャの開始から停止までをひとつのレコードとして取り扱います。
ロック	キャプチャしたパケットが上書きまたは削除されないよう保護することです。ロックは、レコード単位、または期間を指定して設定することが可能です。

東陽テクニカ
SYNESIS 取扱説明書

Copyright © 2015 TOYO Corporation All Rights Reserved.