ClearSight Analyzer 7.0.7

ユーザガイド



文書バージョン1.00

重要 - お読みください
エンドユーザソフトウェアライセンス契約書 (「契約書」)

本契約は、お客様と ClearSight Networks, Inc. (以下、「ClearSight」) との間で法的拘束力を持ち、このコンピュータにインストールしようとする ClearSight ソフトウェア製品 (以下、「ソフトウェア」) の使用に関するものです。本契約において、「お客様」という用語を個々のエンドユーザおよびその組織に対して同等に適用します。本ソフトウェアに関して、お客様の組織が個別の書面によるエンドユーザソフトウェアライセンス契約書を所有していない限り、常に本ソフトウェアの使用は以下の事項に従うものとします。

ライセンスの許諾

ClearSight では、本ソフトウェアのコピーを 1 つだけ、1 台のコンピュータ上での使用するライセンスが供与されます。「使用」とは、本ソフトウェアの、格納、読み込み、インストール、実行、または表示を意味します。本ソフトウェアを変更したり、本ソフトウェアのライセンスまたは制御機能を無効にすることはできません。本ソフトウェアで「同時使用」をライセンスされている場合、本ソフトウェアを共有のサーバーにインストールすることはできますが、認可されたユーザの最大数を超えて、本ソフトウェアを同時に使用することはできません。本契約の締結により、お客様が法的年齢にあることを ClearSight に対して認証したものとします。

所有権

本ソフトウェアは、ClearSight またはサードパーティの供給元が所有し、著作権を持ちます。本ソフトウェア使用のライセンスは、本ソフトウェアの権利または所有権を授与するものではなく、本ソフトウェアの権利を販売するものでもありません。本契約書に対する違反が発生した場合、ClearSight のサードパーティの供給元は権利を保護します。

コピーと改造

保管を目的とする場合、またはコピーや改造が承認された本ソフトウェアの使用で不可欠な手順の場合に限って、本ソフトウェアのコピーまたは改造が許可されます。元のソフトウェアにおけるすべての著作権通知を、コピーまたは改造されたすべてのソフトウェア上で再生する必要があります。内外の掲示板または同様のシステムに本ソフトウェアをコピーすることはできません。ClearSight の事前の書面による許可なしで、印刷物または文書をコピーすることはできません。

逆アセンブル、逆コンパイル、または暗号化解除の禁止

お客様は、本ソフトウェアのマシン実行可能なオブジェクトコードに限り、使用を認可されています。いかなる方法においても本ソフトウェアあるいはその一部を逆アセンブルまたは逆コンパイルすることは禁止されます。本ソフトウェアの操作に不可欠な場合を除いて、暗号化解除は禁止されます。お客様が第三者による本ソフトウェアの逆アセンブル、逆コンパイル、または暗号化解除の試みを知り得た場合、お客様は、そのような行為に関して所有するすべての情報を、ClearSight にただちに提供することに同意するものとします。

不正使用の禁止

お客様は、本ソフトウェアの不正使用または不正行為を促す使用を禁止されています。お客様の責任において、本ソフトウェアに適用される地域、州、地方、連邦のすべての法律に同意し従うものとします。ClearSight は、本ソフトウェアの使用における不正または不法行為に対していかなる責任または義務を負いません。お客様は、本ソフトウェアの不正使用の結果、ClearSight に対して発生したすべての請求、訴訟、弁護費用、訴訟費用を ClearSight に保証することに同意するものとします。

譲渡

本ソフトウェア使用のライセンスは、本ライセンスを第三者に法的譲渡すると同時に、自動的に解除されます。譲渡の際は、一切のコピーおよび関連文書を含む、本ソフトウェアを譲渡先に提供する必要があります。譲渡先は、これらのライセンス条項を譲渡の条件として許諾する必要があります。

契約解除

ClearSight は、これらのライセンス条項の違反に対する通知後、ただちにお客様のライセンスを解除できます。お客様は、契約解除時に、一切のコピー、改造品、およびいかなる構成部分も含む、本ソフトウェアをただちに破棄する必要があります。

輸出規制

お客様は、本ソフトウェア、または準拠法や規格に違反した一切のコピーまたは改造品を輸出することは禁止されています。

米国政府の制限規定

本ソフトウェアおよび文書は、全面的に自己負担により開発され、「商業用コンピュータソフトウェア」または「制限付きコンピュータソフトウェア」として提供されます。本ソフトウェアおよび文書は、DFARS 252.227-7013 (1988 年 10 月)、DFARS 252.211-7015 (1991 年 5 月)、または DFARS 252.227-7014 (1995 年 6 月) で定義された「商業用コンピュータソフトウェア」、FAR 2.101 (a) で定義された「商業品目」、または FAR 52.227-19 (1987 年 6 月) (または同等機関の規制や契約条項) で定義されて「制限付きコンピュータソフトウェア」として提供されます。米国政府のユーザは、該当する FAR または DFARS の条項、または製品の ClearSight 標準ソフトウェア契約書により本ソフトウェアと文書に対して提供される権利のみを所有します。

ClearSight ソフトウェア保証

1. ClearSight ソフトウェアは、無保証で、または口述書面、明示的暗黙的かどうかの状態にかかわらず、「現状のまま」お客様に提供されます。ClearSight は、暗黙の保証、市販性、品質の満足、無謬性や割り込まれない操作、または特定の目的への適合性について一切保証しません。

2. ClearSight は、正常なインストールおよび使用の場合に、製造上の不良のないメディアですべてのソフトウェアが提供されることを保証します。本ソフトウェアの操作開始日から 30 日以内に、このような不良を ClearSight に通知した場合、ClearSight は無償で不良メディアを交換します。

3. この保証書にリストされた補償は、お客様に特定のものであり、本契約書のもとに行われた請求に対して排他的に補償するものです。欠陥の可視不可視に関わらず ClearSight の過失、疑わしい破損や不良などの原因により発生したお客様の組織への損失と損害に対する ClearSight の責任は、いかなる場合においても、損失や破損が申し立てられた特定のソフトウェア製品のライセンス単位価格、あるいは ClearSight の選択による不良品や破損品の修理または交換を越えるものではありません。過失の請求の場合など、いかなる場合においても、データの損失、または (利益の損失を含む) 直接的、偶発的、間接的などの損害に対して、それが契約、不正、その他に基づくものであっても、ClearSight は一切責任を負わないものとします。本契約は、米カリフォルニア州で関係者により締結されたものとみなされ、米カリフォルニア州法に準拠します。

警告

本製品の一部のパーツは、モニタ対象のネットワークアプリケーションの特性を表示するために「アプリケーションコンテンツビューア」を使用しています。これらのビューアは、エンドユーザのビューアと同じ方法でアプリケーションデータを表示するように設計されているため、表示アプリケーションと同じ理論的なすべての脆弱性を呈示する傾向が高くなります。このため、ウイルスに感染したアプリケーションコンテンツビューアがアナライザデバイスを同様に感染させる危険性があります。当社は、さまざまな対策を施して、このような状況の回避に努めていますが、エンドユーザの見聞を表示するというコンテンツビューアの目的を考えれば、理論的にはこのような状況が成立することになります。代わりとなる手段を講じてアナライザデバイス上のウイルス感染を識別および防止し、誤ってウイルスに感染することのないようにしてください。

サードパーティソフトウェア 謝辞および著作権表示

ClearSight Networks Inc. は、ClearSight 製品の開発に使用されるか、ClearSight 製品の中に組み込まれるか、または Clearsight 製品で配布される様々なサードパーティソフトウェア製品の使用を許可されています。

含まれるライセンスの詳細は、以下 URL を参照ください。

http://www.clearsightnet.com/eula/third_party/CSA.html

商標

Wireshark は Gerald Combs の登録商標です。

下記は ClearSight Networks, Inc. の商標です :

ClearSight Networks™ VQFactor™ VRFactor™

文書改訂履歴

改訂	該当箇所	内容
1.00 （2009年 10月23日）		初回リリース

目次

このガイドについて 15
スタンドアロン機能および分散機能について 16
このガイドの対象者 16
このガイドの構成 17
このガイドで使用する規則 19
このガイドで使用する注意表記 20
カスタマサービス 20
その他の部門 20

第 1 章 ClearSight のインストール 23
ClearSight のシステム要件 24
ClearSight をインストールする前に 32
ClearSight Analyzer のインストール 32
Windows XP でのインストール 32
Windows Vista でのインストール 34
ClearSight Distributed のインストール 36
Windows XP でのインストール 36
Windows Vista でのインストール 39
ClearSight Analyzer のアンインストール 42
ClearSight Distributed のアンインストール 43

第 2 章 ClearSight Analyzer のネットワークへの接続 45
アナライザ接続の基本 46
ハブの接続 47
タップの接続 49
ポートミラーリングの使用 52
ClearSight Distributed エージェントの接続 55
2 枚のインターフェイスカードによるエージェントの設定 56
2 枚のインターフェイスカードの使用例 57
まとめ 58

第 3 章 ClearSight Analyzer の概要 59
ClearSight の機能 60
Light バージョンについて 61
ネットワークアダプタサポートの制限 61
Vista サポートの制限 61
ClearSight Analyzer Light で制限された機能 61
試用版ライセンス 64
CSA 7.0.7 の新機能 65
利用可能なモデル 65
ClearSight スタンドアロンの基本設定 65
スタンドアロン Analyzer の [ユーザリスト] の設定 66
ClearSight Analyzer スタンドアロンの起動 71
ClearSight ユーザインターフェイス 73
ClearSight ツールバー 75
ClearSight の使用方法 77
リアルタイムモニタ 79
パケットのキャプチャ 80
ポストキャプチャアナリシス (キャプチャ後の解析) 80

第 4 章 ClearSight Distributed の使用 83
ClearSight Distributed システムについて 84
ClearSight Distributed の通信について 86
ClearSight Distributed の基本 86
エージェントの [ユーザリスト] の設定 87
エージェントマネージャの使用 91
エージェントマネージャでの Distributed エージェントの管理 93
アラートマネージャの使用 102

その他の CSD 固有の機能 108
Secure Socket Layer (SSL) オプション 108
Windows セキュリティマネージャオプション 109

第 5 章 ClearSight を使用したネットワークのモニタ 111
リアルタイムモニタ画面の操作 112
表示するアプリケーションの選択 113
ClearSight ワークスペースの概要とナビゲーション 114
ClearSight のネットワークモデル 119
アプリケーション層のモニタ 121
アプリケーションモニタについて 121
アプリケーションモニタ詳細画面の表示 122
アプリケーションモニタ詳細画面の操作 122
アプリケーションモニタ詳細画面 133
Citrix 詳細画面 134
DNS 詳細画面 135
FTP 詳細画面 136
Telnet 詳細画面 138
HTTP 詳細画面 140
POP 詳細画面 142
SMTP 詳細画面 144
MS SQL 詳細画面 146
Oracle 詳細画面 149
Exchange 詳細画面 151
MSN 詳細画面 153
VoIP 詳細画面 154
RTP 詳細画面 161
RTSP 詳細画面 163
IPTV 詳細画面 164
Kerberos 詳細画面 166
ISAKMP 詳細画面 167
SMB 詳細画面 168
Generic 詳細画面 169
ネットワーク層のモニタ 170
[概要] タブ (ネットワーク層) 171
[コネクション] タブ (ネットワーク層) 172
[ホスト] タブ (ネットワーク層) 177

[チャート] タブ (ネットワーク層) 179
[マルチキャスト] タブ (ネットワーク層) 180
物理層のモニタ 183
[概要] タブ (物理層) 184
[VLAN] タブ (物理層) 185
[サブネット] タブ (物理層) 186
[ノード] タブ (物理層) 187
[チャート] タブ (物理層) 188
ClearSight Analyzer の設定 190
[共通]>[プロトコル設定] 191
[共通]>[モニタ設定] 192
モニタオプション 195
CSV 設定 198
プロトコルフォーシング [共通]>[プロトコルフォーシング] オプション . 199
問題のしきい値 201
問題のアクション 201
翻訳 201
VoIP E- モデル 202
VoIP コーデック 202
レポートの設定 202
ヒストリレポートのデータベース設定 202
WEP キー 203
[アドレス帳] タブ 203
[フィルタ] タブ 203
ウィンドウスタイルの変更 204

第 6 章 ClearSight を使用したデータのキャプチャ 205
キャプチャについて 206
キャプチャワークスペース 207
[統計] タブ 210
[設定] タブ 211
[バッファサイズ] の設定 214
[バッファフル時のアクション] の指定 214
[スライスサイズ] の設定 215
[自動保存] パラメータの設定 216
キャプチャオプションの設定 217
[トリガ] タブ 219

実行中のキャプチャの観察 223

第 7 章 ポストキャプチャアナリシス 225
ポストキャプチャアナリシスについて 225
ポストキャプチャアナリシス画面の使用 227
[ClearSight] タブと [翻訳] タブの間のスマートナビゲーション 230
ポストキャプチャ画面における自動フィルタの使用 235
[翻訳] タブの使用 235
[翻訳] タブのペイン 237
[翻訳] タブにおけるフレームの検索 241
Ethernet OAM フレームの翻訳 242
3G-324M フレームの翻訳 244
[翻訳] タブの設定オプション 246
[翻訳] > [全般] オプション 246
[翻訳] > [設定] オプション 251
[翻訳] > [表示] オプション 253
[翻訳] > [プロトコルフォーシング] オプション 256
IPsec 翻訳オプション 259
トレースファイルの使用 261

第 8 章 複数セグメント解析 263
複数セグメント解析 264
マージしたトレースファイルの作成 264
VoIP 結合フローの表示 266
ラダービューの操作 267
その他の結合フローの表示 268
ラダービューの操作 270
自動結合フィルタの使用 271
[複数 - ティア] タブの使用 275
[NAT] タブの使用 276
手動によるフローの結合 276
複数セグメントのリアルタイム
モニタ 278

第 9 章 フィルタの使用 279
フィルタについて 279
自動フィルタと定義済みフィルタ 279

リアルタイムまたはポストアナリシスでのフィルタの使用 280
パケットベースのフィルタとフローベースのフィルタ 281
自動フィルタの使用 282
自動キャプチャフィルタ 282
自動表示フィルタ 283
定義済みフィルタの使用 284
アプリケーション層フィルタの設定 287
DNS フィルタの設定 288
FTP フィルタの設定 290
HTTP フィルタの設定 292
POP フィルタの設定 294
SMTP フィルタの設定 296
MSN フィルタの設定 298
[Voice-H.323] フィルタの設定 299
[Voice-SIP] フィルタの設定 301
[Voice-Skinny] フィルタの設定 303
[Voice-MGCP] フィルタの設定 305
[Voice-Megaco] フィルタの設定 307
ISAKMP フィルタの設定 309
Kerberos フィルタの設定 310
RTSP フィルタの設定 312
IPTV フィルタの設定 314
SMB フィルタの設定 315
フローフィルタの設定 316
パターンフィルタの設定 317
IP サブネットフィルタの設定 318
プロトコルフィルタの設定 319
MAC アドレスフィルタの設定 325
物理層フィルタの設定 326
フィルタリスト 328

第 10 章 アラートの操作 329
アラートについて 330
アラート表示の操作 330
アラート表示の [事象] タブの情報 332
アラート表示の [問題] タブの情報 333
重要度とアクションの定義 334

重要度の定義 334
アクションの定義 335
問題レポートスレッショルドの設定 344
DNS しきい値の設定 345
FTP しきい値の設定 346
Telnet しきい値の設定 348
Citrix しきい値の設定 348
HTTP しきい値の設定 349
POP しきい値の設定 351
SMTP しきい値の設定 353
MSN しきい値の設定 354
H.323 しきい値の設定 355
SIP しきい値の設定 357
Skinny しきい値の設定 358
MGCP しきい値の設定 359
Megaco しきい値の設定 360
RTP しきい値の設定 361
RTSP しきい値の設定 363
IPTV しきい値の設定 365
ISAKMP しきい値の設定 366
Kerberos しきい値の設定 366
SMB しきい値の設定 367
IP しきい値の設定 368
IPv6 しきい値の設定 370
DLC しきい値の設定 371

第 11 章 アドレス帳の使用 373
アドレス帳について 373
アドレス帳の使用 374
アドレス帳の自動生成 375

第 12 章 レポートの使用 377
レポートについて 378
Windows XP でのレポートの生成 379
レポートワークスペース 379
アプリケーションレポートの使用 382
DNS レポート 383

FTP レポート 384
Telnet レポート 385
HTTP レポート 386
POP レポート 387
SMTP レポート 387
MS SQL サーバーレポート 388
Oracle SQL サーバーレポート 389
VoIP レポート 390
IPTV ビデオ品質レポート 392
Kerberos レポート 392
ISAKMP レポート 393
Exchange レポート 393
MSN レポート 394
SMB レポート 394
RTSP レポート 395
ネットワークレポートの使用 396
[ネットワーク概要] レポート 396
[コネクション] レポート 396
[IP 会話情報] レポート 396
[IP ホスト] レポート 397
[アプリケーション分布] レポート 397
[IP プロトコル分布] レポート 397
[IP 応答時間分布] レポート 397
DLC レポートの使用 398
[DLC 概要] レポート 398
[ノード] レポート 398
[VLAN] レポート 398
[使用率分布] レポート 399
ユーザ定義レポートの作成 399
ヒストリレポーターの使用 401
データ蓄積の制御 403
ヒストリレポートの作成 404
VoIP コールログの作成 407
コールブラウザの使用 408

第 13 章 パケットジェネレータの使用 409
パケットジェネレータオプション 409

ClearSight パケットジェネレータ機能 410
パケットジェネレータの使用 411
統計テーブル 412
トラフィックグラフ 413
[トラフィック制御] ボタン 413
[パケットを送信] ダイアログボックス 414
[バッファを送信] ダイアログボックス 419
プロファイルリスト 423

第 14 章 ClearSight Apex へのリンク 425
ClearSight Apex の機能 425
リンクの場所 426

第 15 章 ClearSight Networks へのエラーレポートの送信 429
エラーレポート機能の基本操作 429

付録 A 特殊なネットワークカードの設定 433
ギガビット XD イーサネットカードの設定 434
[モード] オプション 435
[物理コネクション] オプション 436
10 ギガビットイーサネットカードの設定 437
[モード] オプション 438
[キャプチャモード] オプション 439

索引 441

このガイドについて

このガイドでは、ClearSight® Analyzer ソフトウェアのインストール、接続、および操作方法を説明します。ClearSight Analyzer ソフトウェアは、ネットワークをモニタして、次の操作のための情報を提供します。

- ClearSight Analyzer の直感的なアプリケーションモニタインターフェイスを使った、一般的なアプリケーションに対する IP ベースのフローのモニタ。
- 見合った帯域幅の受信を確認するサービスレベルアグリーメントのモニタ。
- ClearSight Analyzer の強力なアラート検出機能を使った、リアルタイムでのネットワーク障害の検出と解決。
- 将来のネットワークの計画を支援するさまざまなレポートの生成。
- 従来のネットワークプロトコルの解析。

注意：このガイドでは、ClearSight Analyzer ソフトウェアを略して「ClearSight」と表記します。

スタンドアロン機能および分散機能について

このガイドでは、スタンドアロン設定と分散設定の ClearSight Analyzer について説明します。このガイドで説明されている一部の例外を除いて、ClearSight Analyser のスタンドアロン設定で使用可能な機能は、接続された ClearSight Distributed エージェントで使用可能な機能と同じです。大きな違いは、ClearSight Distributed エージェントに接続した場合、ローカル PC ではなく、エージェントビューアでコマンドを実行したり、ClearSight 画面を表示したりすることです。

第 4 章「ClearSight Distributed の使用」では、エージェントビューアからエージェントに接続する方法や、システム全体の警告レポートを設定する方法などを含め、ClearSight Distributed システムについて詳しく説明します。残りの章では、ClearSight の機能を使用して、Distributed エージェントに接続後のネットワークをモニタおよび解析する方法について説明します。

注意：CSD は CSA バージョン 7.0.7 でサポートされていません。

このガイドの対象者

このガイドは、ユーザがネットワークの基本概念を理解し、16 進コードの画面を探索する必要がないネットワークの管理とトラブルシュートを支援するツールの準備ができていることを前提としています。ClearSight はネットワークトラブルシュートの初心者にとって簡単なツールであるだけでなく、上級ネットワーク管理者にとっても十分に洗練された強力なツールです。

このガイドの構成

第 1 章、ClearSight のインストール	最小システム要件を満たす PC 上に ClearSight Analyzer ソフトウェアをインストールする方法を説明します。
第 2 章、ClearSight Analyzer のネットワークへの接続	ClearSight をネットワークに接続してネットワークのモニタと解析での効果を最大にする方法について説明します。
第 3 章、ClearSight Analyzer の概要	ClearSight Analyzer、その機能、およびネットワークのトラブルシュートの支援について説明します。
第 4 章、ClearSight Distributed の使用	Distributed バージョンの ClearSight Analyzer について説明します。ClearSight Distributed を使用すると、中央の ClearSight エージェントビューアからリモート環境の ClearSight エージェントに接続できます。これによって、中央のエージェントビューアから分散ネットワーク環境の全体的なモニタ情報と解析情報を受け取ることができます。
第 5 章、ClearSight を使用したネットワークのモニタ	ClearSight のリアルタイムネットワークモニタ表示を使った、ネットワークの把握とトラブルシュートの方法について説明します。また、ClearSight のネットワークモデルとアプリケーションモニタ全般についても説明します。
第 6 章、ClearSight を使用したデータのキャプチャ	ClearSight を使用してネットワークからデータをキャプチャする方法を説明します。また、キャプチャ設定のオプションと表示も含まれます。
第 7 章、ポストキャプチャアナリシス	ClearSight の強力なポストキャプチャアナリシス機能を使ってネットワークデータを解釈、理解、およびトラブルシュートする方法を説明します。

第 8 章、複数セグメント解析	トレースファイルのマージ方法や、結合フローの作成と解釈の方法の説明を含め、ClearSight の複数セグメント解析機能の使用方法を説明します。
第 9 章、フィルタの使用	自動と定義済みのフィルタ、キャプチャと表示のフィルタ、パケットベースとフローベースのフィルタの説明など、ClearSight のフィルタ機能の使用方法を説明します。
第 10 章、アラートの操作	重要度を定義する方法、アクションを重要度に関連付ける方法、および問題検出のスレッショルドを設定する方法など、ClearSight のアラートログの操作方法を説明します。
第 11 章、アドレス帳の使用	ClearSight のアドレス帳機能を使って、ClearSight の [翻訳] タブで IP アドレスに代わって使用される名前を割り当てる方法を説明します。
第 12 章、レポートの使用	ClearSight のレポート機能を使って、異なった種類のネットワークデータでさまざまな種類のレポートを表示する方法を説明します。
第 13 章、パケットジェネレータの使用	ClearSight の統合パケットジェネレータの使用方法を説明します。
第 14 章、ClearSight Apex へのリンク	エキスパートナレッジベースへのアクセスを提供する ClearSight Apex 製品にリンクする方法を説明します。
第 15 章、ClearSight Networks へのエラーレポートの送信	故障が発生した場合に ClearSight Networks にエラーレポートを送信する方法を説明します。
付録 A、特殊なネットワークカードの設定	別売りの 10/100 全二重イーサネットアダプタと Gigabit イーサネットアダプタをネットワークに接続する方法とこれらのアダプタの特定オプションを設定する方法を説明します。

このガイドで使用する規則

このガイドでは、次の表記規則を使用します。

ボールド体

ボールド体は、ClearSight ユーザインターフェイスのメニュー、ボタン、およびフィールドの名前に使用します。

例 : ClearSight ツールバーの **[モニタ]** ボタンをクリックします。

ボールド イタリック

ボールドイタリックフォントは、ユーザ定義の変数を表します。

例 : ***yymmdd*** 形式で日付を入力します。

>

右の山括弧は、メニューの連続する選択を分割するために使用します。

例 : **[ファイル] > [保存]** コマンドを選択します。

< >

山括弧は括弧で囲まれたアイテムがコンピュータのキーボード上のキーの名前であることを示しています。

例 : Windows のキーボードショートカットは <CTRL - C> です。



ClearSight Application Flow Analyzer に対応していることを表します。



ClearSight Analyzer Light に対応していることを表します。



ClearSight Distributed に対応していることを表します。

このガイドで使用する注意表記

このガイドでは、次の注意表記を使用します。次に進む前にこれらを注意してお読みください。

警告： 「警告」は、データファイル、プログラムファイル、またはハードウェアデバイスの破損の発生を避けるために知る必要がある情報であることを示します。

注記： 「注記」は、ClearSight Analyzer の使用に関する重要な情報であることを示します。

重要： 「重要」は、一般的な情報に注意を向けるために使用します。

ヒント： 「ヒント」は、実行可能なその他の処理を示します。

カスタマサービス

製品に関する質問、ライセンスに関する質問、またはその他の問題については、表 i の（株）東陽テクニカ ClearSight サポート担当までお問い合わせください。営業時間は、月曜～金曜日の、9:30 AM ～ 5:30 PM です。

表 i: （株）東陽テクニカ ClearSight サポート担当連絡先情報

Fax	03-3246-0645
電子メール	clearsight-support@ict.toyo.co.jp
Web	http://www.toyo.co.jp/clearsight

その他の部門

東陽テクニカでの他の ClearSight 担当部門への連絡方法を表 ii に示します。

表 ii: その他の ClearSight 担当部門

■ ClearSight アナライザの機能、構成、価格に関する総合的なお問い合わせ

株式会社東陽テクニカ　情報通信システム営業部

TEL.03-3279-0771

FAX.03-3246-0645

E-mail:clearsight@ict.toyo.co.jp

■ 関西地区における ClearSight の販売／サポートに関するお問い合わせ

株式会社東陽テクニカ　大阪支店　エレクトロニクス営業部

TEL.06-6399-9771

FAX.06-6399-9781

E-mail:mino@toyo.co.jp

■ ClearSight トレーニングセミナー／ ClearSight Academy に関するお問い合わせ

株式会社東陽テクニカ　情報通信システム営業部

TEL.03-3279-0771

FAX.03-3246-0645

第 1 章

ClearSight のインストール

この章は、次の項目で構成されています。

- 「ClearSight のシステム要件」
- 「ClearSight をインストールする前に」
- 「ClearSight Analyzer のインストール」
- 「ClearSight Distributed のインストール」
- 「ClearSight Analyzer のアンインストール」
- 「ClearSight Distributed のアンインストール」

ClearSight のシステム要件



ClearSight は強力なネットワーク解析ツールです。最適なパフォーマンスを得るには強力なシステムが必要になることに注意してください。ここでは、以下の最小システム要件を示します。

- 「ClearSight スタンドアロンのシステム要件」
- 「ClearSight エージェントマネージャおよびエージェントのシステム要件」
- 「ClearSight エージェントマネージャのみのシステム要件」
- 「ClearSight Distributed エージェントのみのシステム要件」

ClearSight スタンドアロンのシステム要件

表 1-1 および表 1-2 は、ClearSight Analyzer の最小システム要件を示しています。

表 1-1: ClearSight スタンドアロンの最小システム要件 (Windows XP)

項目	最小要件
コンピュータ	ソフトウェアのインストール用 CD ドライブを持つ、業界標準のコンピュータシステム (ラップトップまたはデスクトップ)
プロセッサ	Pentium 4 1.0 GHz 以上相当 (2 GHz 以上を推奨)
RAM	512 MB 以上 (1 GB を推奨)
ハードディスクの空き容量	250 MB。これ以外に、保存されたトレースファイルを格納する容量が必要になります。個々のトレースファイルは、最大で 1GB 程度になりますが、256MB よりも大きなトレースファイルを開くことは推奨できません。
オペレーティングシステム	Microsoft Windows XP Home Edition SP2。 ファイアウォールを無効にしてください。 Microsoft Windows XP Professional SP2。 ファイアウォールを無効にしてください。

表 1-1: ClearSight スタンドアロンの最小システム要件 (Windows XP)

項目	最小要件
モニタ	解像度 1024x768 の XGA カラーモニタ
ネットワーク アダプタ	NDIS 互換のネットワークデバイスドライバを持ったネットワーク接続

表 1-2: ClearSight スタンドアロンの最小システム要件 (Windows Vista)

項目	最小要件
コンピュータ	オーディオ出力およびソフトウェアのインストール用 DVD ドライブを持つ、業界標準のコンピュータシステム (ラップトップまたはデスクトップ)
プロセッサ	Pentium 4 1.0 GHz 以上相当 (2 GHz 以上を推奨)
RAM	2 GB 以上
ハードディスクの空き容量	15 GB 以上 (全容量 40 GB 以上)
オペレーティングシステム	Windows Vista 32 ビット版 SP1 または SP2
モニタ	解像度 1024x768 の XGA カラーモニタ。DirectX 9 対応のグラフィックカード推奨
ネットワーク アダプタ	ネットワークデバイスドライバを通じたネットワーク接続（リモートエージェントへのアクセス用）

ClearSight エージェントマネージャおよびエージェントのシステム要件

表 1-3 および表 1-4 は、エージェントマネージャおよびエージェントを同じ PC にインストールする場合の ClearSight Distributed の最小システム要件を示しています。

表 1-3: ClearSight Distributed の最小システム要件 ー エージェントマネージャおよびエージェントを同じ PC にインストールする場合（Windows XP）

項目	最小要件
コンピュータ	ソフトウェアのインストール用に CD ドライブが付いている業界標準のコンピュータシステム (ラップトップまたはデスクトップ)
プロセッサ	Pentium 4 1.0 GHz 以上相当 (2 GHz 以上を推奨)
RAM	512MB 以上 (1 GB を推奨)
ハードディスクの空き容量	250 MB。これ以外に、保存されたトレースファイルを格納する容量が必要になります。個々のトレースファイルは、最大で 1GB 程度になりますが、256MB よりも大きなトレースファイルを開くことは推奨できません。
オペレーティングシステム	Microsoft Windows XP Home Edition SP2。 ファイアウォールを無効にしてください。 Microsoft Windows XP Professional SP2。 ファイアウォールを無効にしてください。
モニタ	解像度 800x600、16 色表示の VGA カラーモニタ。 解像度 1024x768、256 色表示を推奨
ネットワークアダプタ	NDIS 互換のネットワークデバイスドライバを使用したネットワーク接続
インターネットブラウザ	Microsoft Internet Explorer 6.0 以降

表 1-4: エージェントマネージャおよびエージェントを同じ PC にインストールする場合の ClearSight Distributed の最小システム要件 (Windows Vista)

項目	最小要件
コンピュータ	オーディオ出力およびソフトウェアのインストール用 DVD ドライブを持つ、業界標準のコンピュータシステム (ラップトップまたはデスクトップ)
プロセッサ	Pentium 4 1.0 GHz 以上相当 (2 GHz 以上を推奨)
RAM	2 GB 以上
ハードディスクの空き容量	15 GB 以上 (全容量 40 GB 以上)
オペレーティングシステム	Windows Vista 32 ビット版 SP1 または SP2
モニタ	解像度 1024x768 の XGA カラーモニタ。DirectX 9 対応のグラフィックカード推奨
ネットワークアダプタ	NDIS 互換のネットワークデバイスドライバを持ったネットワーク接続
インターネットブラウザ	Microsoft Internet Explorer 6.0 以降

ClearSight エージェントマネージャのみのシステム要件

表 1-5 および表 1-6 は、エージェントマネージャのみを PC にインストールする場合の ClearSight Distributed の最小システム要件を示しています。

表 1-5: ClearSight Distributed の最小システム要件 ― エージェントマネージャのみを PC にインストールする場合（Windows Vista より前のバージョン）

項目	最小要件
コンピュータ	ソフトウェアのインストール用に CD ドライブが付いている業界標準のコンピュータシステム (ラップトップまたはデスクトップ)
プロセッサ	Pentium 4 1.0 GHz 以上相当 (2 GHz 以上を推奨)
RAM	512 MB 以上 (1 GB を推奨)
ハードディスクの空き容量	250 MB。これ以外に、保存されたトレースファイルを格納する容量が必要になります。個々のトレースファイルは、最大で 1GB 程度になりますが、256MB よりも大きなトレースファイルを開くことは推奨できません。
オペレーティングシステム	Microsoft Windows XP Home Edition SP2。 ファイアウォールを無効にしてください。 Microsoft Windows XP Professional SP2。 ファイアウォールを無効にしてください。
モニタ	解像度 800x600、16 色表示の VGA カラーモニタ。 解像度 1024x768、256 色表示を推奨
ネットワークアダプタ	ネットワークデバイスドライバを通じたネットワーク接続（リモートエージェントへのアクセス用）
インターネットブラウザ	Microsoft Internet Explorer 6.0 以降

表 1-6: ClearSight Distributed の最小システム要件 ー エージェントマネージャのみを PC にインストールする場合（Windows Vista）

項目	最小要件
コンピュータ	オーディオ出力およびソフトウェアのインストール用 DVD ドライブを持つ、業界標準のコンピュータシステム (ラップトップまたはデスクトップ)
プロセッサ	Pentium 4 1.0 GHz 以上相当 (2 GHz 以上を推奨)
RAM	2 GB 以上
ハードディスクの空き容量	15 GB 以上 (全容量 40 GB 以上)
オペレーティングシステム	Windows Vista 32 ビット版 SP1 または SP2
モニタ	解像度 1024x768 の XGA カラーモニタ。DirectX 9 対応のグラフィックカード推奨
ネットワークアダプタ	ネットワークデバイスドライバを通じたネットワーク接続（リモートエージェントへのアクセス用）
インターネットブラウザ	Microsoft Internet Explorer 6.0 以降

ClearSight Distributed エージェントのみのシステム要件

表 1-7 および表 1-8 は、エージェントのみが PC にインストールされている場合の ClearSight Distributed の最小システム要件を示しています。

表 1-7: エージェントのみインストールする場合の ClearSight の最小システム要件 (Windows XP)

項目	最小要件
コンピュータ	ソフトウェアのインストール用に CD ドライブが付いている業界標準のコンピュータシステム (ラップトップまたはデスクトップ)
プロセッサ	Pentium 4 1.0 GHz 以上相当 (2 GHz 以上を推奨)
RAM	512 MB 以上 (1 GB を推奨)
ハードディスクの空き容量	250 MB。これ以外に、保存されたトレースファイルを格納する容量が必要になります。個々のトレースファイルは、最大で 1GB 程度になりますが、256MB よりも大きなトレースファイルを開くことは推奨できません。
オペレーティングシステム	Microsoft Windows XP Home Edition SP2。 ファイアウォールを無効にしてください。 Microsoft Windows XP Professional SP2。 ファイアウォールを無効にしてください。
ネットワークアダプタ	ネットワークデバイスドライバを通じたネットワーク接続（リモートエージェントへのアクセス用）
インターネットブラウザ	Microsoft Internet Explorer 6.0 以降

表 1-8: エージェントのみインストールする場合の ClearSight の最小システム要件 (Windows Vista)

項目	最小要件
コンピュータ	オーディオ出力およびソフトウェアのインストール用 DVD ドライブを持つ、業界標準のコンピュータシステム (ラップトップまたはデスクトップ)
プロセッサ	Pentium 4 1.0 GHz 以上相当 (2 GHz 以上を推奨)
RAM	2 GB 以上
ハードディスクの空き容量	15 GB 以上 (全容量 40 GB 以上)
オペレーティングシステム	Windows Vista 32 ビット版 SP1 または SP2
ネットワークアダプタ	ネットワークデバイスドライバを通じたネットワーク接続（リモートエージェントへのアクセス用）
インターネットブラウザ	Microsoft Internet Explorer 6.0 以降

ClearSight をインストールする前に



ClearSight をインストールする前に、次の項目を確認します。

- 対象システムが 24 ページの「ClearSight のシステム要件」にリストされた最小システム要件を満たしていること。
- アプリケーション CD にインストールファイルが含まれていること。または、ClearSight Networks の Web サイトからインストールファイルをダウンロードしていること。
- 旧バージョンの ClearSight Analyzer がインストールされている場合は、新バージョンをインストール前に、自動的に旧バージョンはアンインストールされます。ダイアログボックスが表示され、旧バージョンのアンインストールを案内します。

ClearSight Analyzer のインストール

ClearSight Analyzer スタンドアロンを WindowsXP または Windows Vista にインストールする方法を以下に記述します。

Windows XP でのインストール

スタンドアロンバージョンの ClearSight Analyzer を Windows XP にインストールするには、次の手順に従います。

1. ClearSight 製品 CD を対象 PC の CD-ROM ドライブに挿入します。
2. InstallShield ウィザードが自動的に起動しない場合 (またはソフトウェアをダウンロードした場合) は、インストールプログラムの場所に移動し、そこからプログラムを実行します。
3. ウィザードの指示に従って、ClearSight Analyzer ソフトウェアをインストールします。インストールの間、次の操作が必要です。
   a. エンドユーザソフトウェアライセンス契約書の条件に同意する。
   b. 顧客情報を入力する。
   c. ClearSight Analyzer ソフトウェアのインストールディレクトリを指定する。

注記 : ClearSight では、デフォルトのインストールディレクトリを使用することをお勧めします。

4. リストされたディレクトリが正しいことを確認し、**[インストール]** をクリックします。
5. インストールが完了したら、**[終了]** をクリックして InstallShield ウィザードを終了します。
6. システムを再起動するかどうかを確認するメッセージが表示されたら、**[いいえ]** をクリックします。
7. 次の画面では、2 枚目の CD を挿入するように要求されます。Third Party Decode Engine CD を挿入します。
8. InstallShield ウィザードが自動的に起動しない場合 (またはソフトウェアをダウンロードした場合) は、インストールプログラムの場所に移動し、そこからプログラムを実行します。
9. ウィザードの指示に従って、Third Party Decode Engine をインストールします。インストールの間、次の操作が必要です。
   a. ソフトウェアライセンス契約書の条件に同意する。
   b. Third Party Decode Engine ソフトウェアのインストールディレクトリを指定する。

      注記 : ClearSight では、デフォルトのインストールディレクトリを使用することをお勧めします。
10. リストされたディレクトリが正しいことを確認し、**[インストール]** をクリックします。
11. インストールが完了したら、**[完了]** をクリックして InstallShield ウィザードを終了します。
12. コンピュータを手動で再起動します。
13. [スタート] メニューから ClearSight Analyzer ソフトウェアを起動します **([スタート] メニュー > [すべてのプログラム] > [ClearSight] > [ClearSight Analyzer])**。

Windows Vista でのインストール

スタンドアロンバージョンの ClearSight Analyzer を Windows Vista にインストールするには、次の手順に従います。

1. ClearSight 製品 CD を対象 PC の DVD-ROM ドライブに挿入します。
2. InstallShield ウィザードが自動的に起動しない場合 (またはソフトウェアをダウンロードした場合) は、インストールプログラムの場所に移動し、そこからプログラムを実行します。
3. Administrator アカウントでログインしている場合にはステップ 5 に進みます。
4. Administrator アカウント以外の管理者権限を持つユーザアカウントでログインしている場合は、**[ユーザアカウント制御]** ダイアログボックスが表示されます。“ 認識できないプログラムがこのコンピュータへのアクセスを要求しています “ というメッセージが **[ユーザアカウント制御]** ダイアログボックスに表示されますので、**[許可]** をクリックします。
5. ウィザードの指示に従って、ClearSight Analyzer ソフトウェアをインストールします。インストールの間、次の操作が必要です。
   a. エンドユーザソフトウェアライセンス契約書の条件に同意する。
   b. 顧客情報を入力する。
   c. ClearSight Analyzer ソフトウェアのインストールディレクトリを指定する。

      注記 : ClearSight では、デフォルトのインストールディレクトリを使用することをお勧めします。
6. リストされたディレクトリが正しいことを確認し、**[インストール]** をクリックします。
7. インストールが完了したら、**[終了]** をクリックして InstallShield ウィザードを終了します。
8. システムを再起動するかどうかを確認するメッセージが表示されたら、**[いいえ]** をクリックします。
9. 次の画面では、2 枚目の CD を挿入するように要求されます。Third Party Decode Engine CD を挿入します。

10. InstallShield ウィザードが自動的に起動しない場合 (またはソフトウェアをダウンロードした場合) は、インストールプログラムの場所に移動し、そこからプログラムを実行します。
11. Administrator アカウントでログインしている場合にはステップ 13 に進みます。
12. Administrator アカウント以外の管理者権限を持つユーザアカウントでログインしている場合は、**[ユーザアカウント制御]** ダイアログボックスが表示されます。“ 認識できないプログラムがこのコンピュータへのアクセスを要求しています “ というメッセージが **[ユーザアカウント制御]** ダイアログボックスに表示されますので、**[許可]** をクリックします。
13. ウィザードの指示に従って、Third Party Decode Engine をインストールします。インストールの間、次の操作が必要です。
    a. ソフトウェアライセンス契約書の条件に同意する。
    b. Third Party Decode Engine ソフトウェアのインストールディレクトリを指定する。

       注記 : ClearSight では、デフォルトのインストールディレクトリ を使用することをお勧めします。
14. リストされたディレクトリが正しいことを確認し、**[インストール]** をクリックします。
15. インストールが完了したら、**[完了]** をクリックして InstallShield ウィザードを終了します。
16. コンピュータを手動で再起動します。
17. [スタート] メニューから ClearSight Analyzer ソフトウェアを起動します **([スタート] メニュー > [すべてのプログラム] > [ClearSight] > [ClearSight Analyzer])**。
18. Administrator アカウント以外の管理者権限を持つユーザアカウントでログインしている場合は、**[ユーザアカウント制御]** ダイアログボックスが表示されます。“ 認識できないプログラムがこのコンピュータへのアクセスを要求しています “ というメッセージが **[ユーザアカウント制御]** ダイアログボックスに表示されますので、**[許可]** をクリックします。

ClearSight Distributed のインストール

ClearSight Distributed のインストール方法は、ClearSight Analyzer 製品の場合とほぼ同じです。ただし、ClearSight Distributed には、次のインストールオプションがあります。

- エージェントマネージャとエージェント
- エージェントマネージャのみ
- エージェントのみ

エージェントマネージャのみをインストールする場合、ClearSight Analyzer のスタンドアロンバージョンをインストールする場合とは異なり、エージェントの「ローカル」のモニタおよび解析インターフェイスはありません。エージェントマネージャのみをインストールする場合は、リモートエージェントを使用してモニタと解析のみを実行できます。

同様に、エージェントのみをインストールする場合、その PC からエージェントを管理することはできません。インストールされる ClearSight Distributed エージェントは、別の PC にインストールされたエージェントマネージャによって管理できます。

同じ PC にエージェントマネージャとエージェントをインストールすることもできます。この場合は、ローカルのエージェントマネージャのみを使用してローカルエージェントとリモートエージェント両方を管理できます。

Windows XP でのインストール

ClearSight Distributed を Windows XP にインストールするには、次の手順に従います。

1. 製品 CD を対象 PC の CD-ROM ドライブに挿入します。
2. InstallShield ウィザードが自動的に起動しない場合 (またはソフトウェアをダウンロードした場合) は、インストールプログラムの場所に移動し、そこからプログラムを実行します。
3. ウィザードの指示に従って、ClearSight Distributed ソフトウェアをインストールします。インストールの間、次の操作が必要です。
   a. エンドユーザソフトウェアライセンス契約書の条件に同意する。

b. 顧客情報を入力する。

c. ClearSight Distributed ソフトウェアのインストールディレクトリを指定する。

注記 : ClearSight では、デフォルトのインストールディレクトリを使用することをお勧めします。

d. インストールする ClearSight Distributed コンポーネントを選択する (図 1-1 を参照)。

注記 : 最初にインストールしたシステムを、異なるシステムとして再構成する場合は、まず初めに最初にインストールしたシステムをアンインストールする必要があります。アンインストール後、システムが再起動してから、インストールを開始してください。

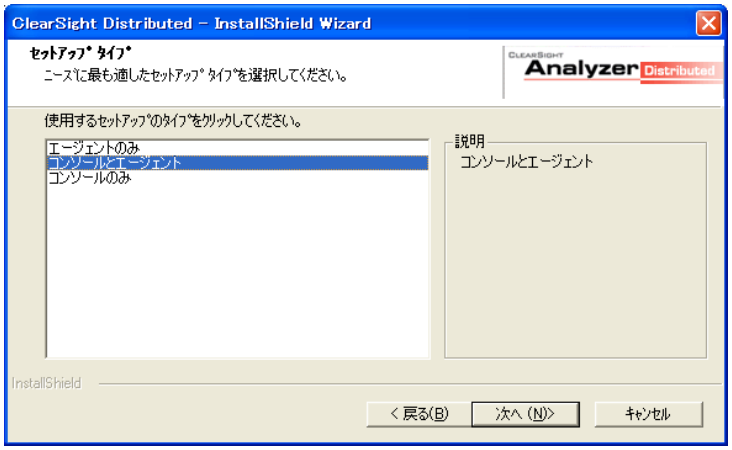


図 1-1: インストールする ClearSight Distributed コンポーネントの選択

4. リストされたディレクトリが正しいことを確認し、**[インストール]** をクリックします。

5. インストールが完了したら、**[終了]** をクリックして InstallShield ウィザードを終了します。

6. システムを再起動するかどうかを確認するメッセージが表示されたら、Third Party Decode Engine をインストールする場合は **[いいえ]** をクリックし、それ以外の場合は **[はい]** をクリックします。

7. Third Party Decode Engine をインストールする場合は、インストールプログラムの場所に移動し、そこからプログラムを実行します。
8. ウィザードの指示に従って、Third Party Decode Engine をインストールします。インストールの間、次の操作が必要です。
   a. ソフトウェアライセンス契約書の条件に同意する。
   b. Third Party Decode Engine ソフトウェアのインストールディレクトリを指定する。

      注記 : ClearSight では、デフォルトのインストールディレクトリ を使用することをお勧めします。
9. リストされたディレクトリが正しいことを確認し、**[インストール]** をクリックします。
10. インストールが完了したら、**[完了]** をクリックして InstallShield ウィザードを終了します。
11. コンピュータを手動で再起動します。
12. この PC にマネージャがインストールされている場合は、**[スタート]** メニュー (**[スタート]** > **[すべてのプログラム]** > **[ClearSight Distributed]** > **[ClearSight Distributed Agent Manager]**) から、ClearSight Distributed エージェントマネージャソフトウェアを起動します。

    ClearSight Distributed エージェントマネージャは、複数の ClearSight Distributed エージェントに接続する「ホームベース」として使用します。Distributed エージェントに接続したら、スタンドアロンバージョンの場合と同様に、標準的な ClearSight Analyzer 機能を使用します。

Windows Vista でのインストール

ClearSight Distributed を Windows Vista にインストールするには、次の手順に従います。

1. 製品 CD を対象 PC の CD-ROM ドライブに挿入します。
2. InstallShield ウィザードが自動的に起動しない場合 (またはソフトウェアをダウンロードした場合) は、インストールプログラムの場所に移動し、そこからプログラムを実行します。
3. Administrator アカウントでログインしている場合にはステップ 5 に進みます。
4. Administrator アカウント以外の管理者権限を持つユーザアカウントでログインしている場合は、**[ユーザアカウント制御]** ダイアログボックスが表示されます。“ 認識できないプログラムがこのコンピュータへのアクセスを要求しています “ というメッセージが **[ユーザアカウント制御]** ダイアログボックスに表示されますので、**[許可]** をクリックします。
5. ウィザードの指示に従って、ClearSight Distributed ソフトウェアをインストールします。インストールの間、次の操作が必要です。
   a. エンドユーザソフトウェアライセンス契約書の条件に同意する。
   b. 顧客情報を入力する。
   c. ClearSight Distributed ソフトウェアのインストールディレクトリを指定する。

      注記 : ClearSight では、デフォルトのインストールディレクトリを使用することをお勧めします。
   d. インストールする ClearSight Distributed コンポーネントを選択する (図 1-2 を参照)。

      注記 : 最初にインストールしたシステムを、異なるシステムとして再構成する場合は、まず初めに最初にインストールしたシステムをアンインストールする必要があります。アンインストール後、システムが再起動してから、インストールを開始してください。

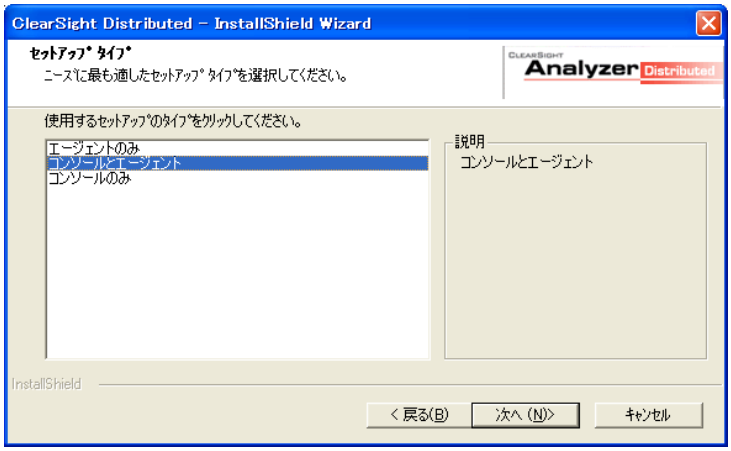


図 1-2: インストールする ClearSight Distributed コンポーネントの選択

6. リストされたディレクトリが正しいことを確認し、**[インストール]** をクリックします。
7. インストールが完了したら、**[終了]** をクリックして InstallShield ウィザードを終了します。
8. システムを再起動するかどうかを確認するメッセージが表示されたら、Third Party Decode Engine をインストールする場合は **[いいえ]** をクリックし、それ以外の場合は **[はい]** をクリックします。
9. Third Party Decode Engine をインストールする場合は、インストールプログラムの場所に移動し、そこからプログラムを実行します。
10. Administrator アカウントでログインしている場合にはステップ 12 に進みます。
11. Administrator アカウント以外の管理者権限を持つユーザアカウントでログインしている場合は、**[ユーザアカウント制御]** ダイアログボックスが表示されます。“ 認識できないプログラムがこのコンピュータへのアクセスを要求しています “ というメッセージが **[ユーザアカウント制御]** ダイアログボックスに表示されますので、**[許可]** をクリックします。
12. ウィザードの指示に従って、Third Party Decode Engine をインストールします。インストールの間、次の操作が必要です。
    a. ソフトウェアライセンス契約書の条件に同意する。

b. Third Party Decode Engine ソフトウェアのインストールディレクトリを指定する。

注記：ClearSight では、デフォルトのインストールディレクトリを使用することをお勧めします。

13. リストされたディレクトリが正しいことを確認し、**[インストール]** をクリックします。
14. インストールが完了したら、**[完了]** をクリックして InstallShield ウィザードを終了します。
15. コンピュータを手動で再起動します。
16. この PC にマネージャがインストールされている場合は、[スタート] メニュー (**[スタート]** > **[すべてのプログラム]** > **[ClearSight Distributed]** > **[ClearSight Distributed Agent Manager]**) から、ClearSight Distributed エージェントマネージャソフトウェアを起動します。
17. Vista に Administrator としてログインしている場合は、プログラムが起動します。Administrator アカウント以外の管理者権限を持つユーザアカウントで Vista にログインしている場合は、[ユーザアカウント制御] ダイアログボックスが表示されます。“認識できないプログラムがこのコンピュータへのアクセスを要求しています”というメッセージが [ユーザアカウント制御] ダイアログボックスに表示されますので、**[許可]** をクリックします。

    ClearSight Distributed エージェントマネージャは、複数の ClearSight Distributed エージェントに接続する「ホームベース」として使用します。Distributed エージェントに接続したら、スタンドアロンバージョンの場合と同様に、標準の ClearSight Analyzer 機能を使用できます。

ClearSight Analyzer のアンインストール



ClearSight Analyzer をアンインストールする手順

1. **[スタート] > [すべてのプログラム] > [ClearSight] > [ClearSight Analyzer をアンインストール]** を選択します。
2. Windows Vista では、[ユーザアカウント制御] ダイアログボックスが表示されます。**[許可]** をクリックしてください
3. 画面の指示に従って、ClearSight をアンインストールします。

   注記 : アンインストール時に、インストール以降に変更したファイルを削除するオプションがあります。変更したファイルはそのまま残しても何の影響もありません。しかし、空き容量を増やす場合には、それらの削除を選択できます。
4. コンピュータを再起動します。アンインストール処理は、コンピュータを再起動するまでは完了しません。

   注記 : ClearSight を再インストールするときは、その前にコンピュータを再起動する必要があります。

Third Party Decode Engine をアンインストールする手順

1. **[スタート] > [すべてのプログラム] > [Third Party Decode Engine x.x.x] > [Third Party Decode Engine をアンインストール]** を選択します。
2. Windows Vista では、[ユーザアカウント制御] ダイアログボックスが表示されます。**[許可]** をクリックしてください
3. 画面の指示に従って、Third Party Decode Engine をアンインストールします。
4. コンピュータを再起動します。アンインストールの手順は、コンピュータを再起動するまでは完了しません。

   注記 : Third Party Decode Engine を再インストールするときは、その前にコンピュータを再起動する必要があります。

ClearSight Distributed のアンインストール

ClearSight Distributed をアンインストールする手順

1. **[スタート] > [すべてのプログラム] > [ClearSight Distributed] > [アンインストール]** を選択します。
2. 画面の指示に従って、ClearSight をアンインストールします。

   注記 : インストールの方法によっては、インストール以降に変更したファイルをアンインストール時に削除するオプションもあります。変更したファイルはそのまま残しても影響はありません。空き容量を増やす場合には、それらのファイルを削除します。
3. コンピュータを再起動します。アンインストールの処理は、コンピュータを再起動するまでは完了しません。

   注記 : ClearSight を再インストールするときは、その前にコンピュータを再起動する必要があります。

Third Party Decode Engine をアンインストールする手順

1. **[スタート] > [すべてのプログラム] > [Third Party Decode Engine x.x.x] > [Third Party Decode Engine をアンインストール]** を選択します。
2. Windows Vista では、[ユーザアカウント制御] ダイアログボックスが表示されます。**[許可]** をクリックしてください
3. 画面の指示に従って、Third Party Decode Engine をアンインストールします。
4. コンピュータを再起動します。アンインストールの手順は、コンピュータを再起動するまでは完了しません。

   注記 : Third Party Decode Engine を再インストールするときは、その前にコンピュータを再起動する必要があります。

第 2 章

ClearSight Analyzer のネットワークへの接続

この章では、ClearSight をネットワークに接続してネットワークのモニタと解析での効果を最大にする方法について説明します。ClearSight では、観測されるネットワークデータのみ解析が可能です。この章では、ClearSight をネットワークに接続する方法について解説します。この章は、次の項目で構成されています。

- アナライザ接続の基本
- 次の典型的な接続シナリオ、およびその長所と短所
  - ハブ
  - タップ
  - ポートミラーリング
- ClearSight Distributed エージェントを接続する際の注意点

アナライザ接続の基本

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

効果的にネットワークをモニタしたり解析したりする基本は、アナライザをネットワーク上のどこに接続するかということにあります。つまりデータの可視性を最大限にするように接続することが必要です。数年前、ほとんどのネットワークは、ネットワークハブなどの共有のメディアを大量に使用していました。共有のメディア環境では、ネットワークセグメント上の各ステーションはすべてのパケットを監視し、それが自分に宛てられたものかどうかを確認します。個々のステーションは、自分に宛てられたフレームを単純にコピーして、他のフレームは流れるままにします。このため、アナライザを単純にプロミスキャスモードで接続すれば、セグメント上のすべてのフレームを解析用のキャプチャバッファにコピーでき、容易にネットワーク解析を行うことが可能でした。

時が経つにつれて、ネットワークスイッチが普及し、アナライザの接続はより複雑になりました。ハブとは異なり、ネットワークスイッチは、送信先アドレスが実際に存在するポートだけにパケットを転送します。この結果、ハブを使っていたときよりも、ネットワークの帯域幅をより効果的に使用できるようになりましたが、同時にネットワークのモニタと解析は、より困難になりました。ハブのオープンポートにアナライザを接続すると、デバイス上を流れるすべてのトラフィックを表示できるのに対して、オープンスイッチポートにアナライザを接続すると、ブロードキャストとマルチキャストのパケットのみが表示されます。

次のように、スイッチを使用したネットワークで可視性を向上するための一般的な方法がいくつかあります。

- モニタするセグメントごとにハブを接続 (47 ページ)
- モニタするセグメントごとにタップを接続 (49 ページ)
- スイッチ上のポートミラーリングを設定 (52 ページ)

以下のセクションでは、これらの方法の長所と短所をそれぞれ説明します。

ハブの接続

ClearSight Application Flow Analyzer ClearSight Analyzer Light

最も簡単に低価格な方法で、スイッチを使用したネットワークの可視性を向上させるには、2 つのデバイス間にハブを接続します。ハブが受信する各パケットは、デバイス上のすべてのポートに複製されるため、ClearSight をハブのオープンポートに接続することで、2 つのデバイス間のすべてのデータフローを監視できます。

図 2-1 は、ハブを使用してネットワークのモニタと解析を行う方法の一例を示しています。この例では、**スイッチ A** と**スイッチ B** の両方でスイッチポートと接続されたデバイスの間にハブが接続されています。**スイッチ A** と WAN のクラウドの間に配置されたオープンポートに接続することによって、ClearSight はスイッチポートと WAN の間のすべてのトラフィックを監視できます。

長所と短所

ハブには、費用対効果がよく、接続しやすいという長所があります。ただし、ハブがすべてのネットワークに適しているわけではありません。例えば、全二重リンク上へのハブの接続は、リンクを半二重に制限するため、応答時間が遅くなりスループットが減少します。

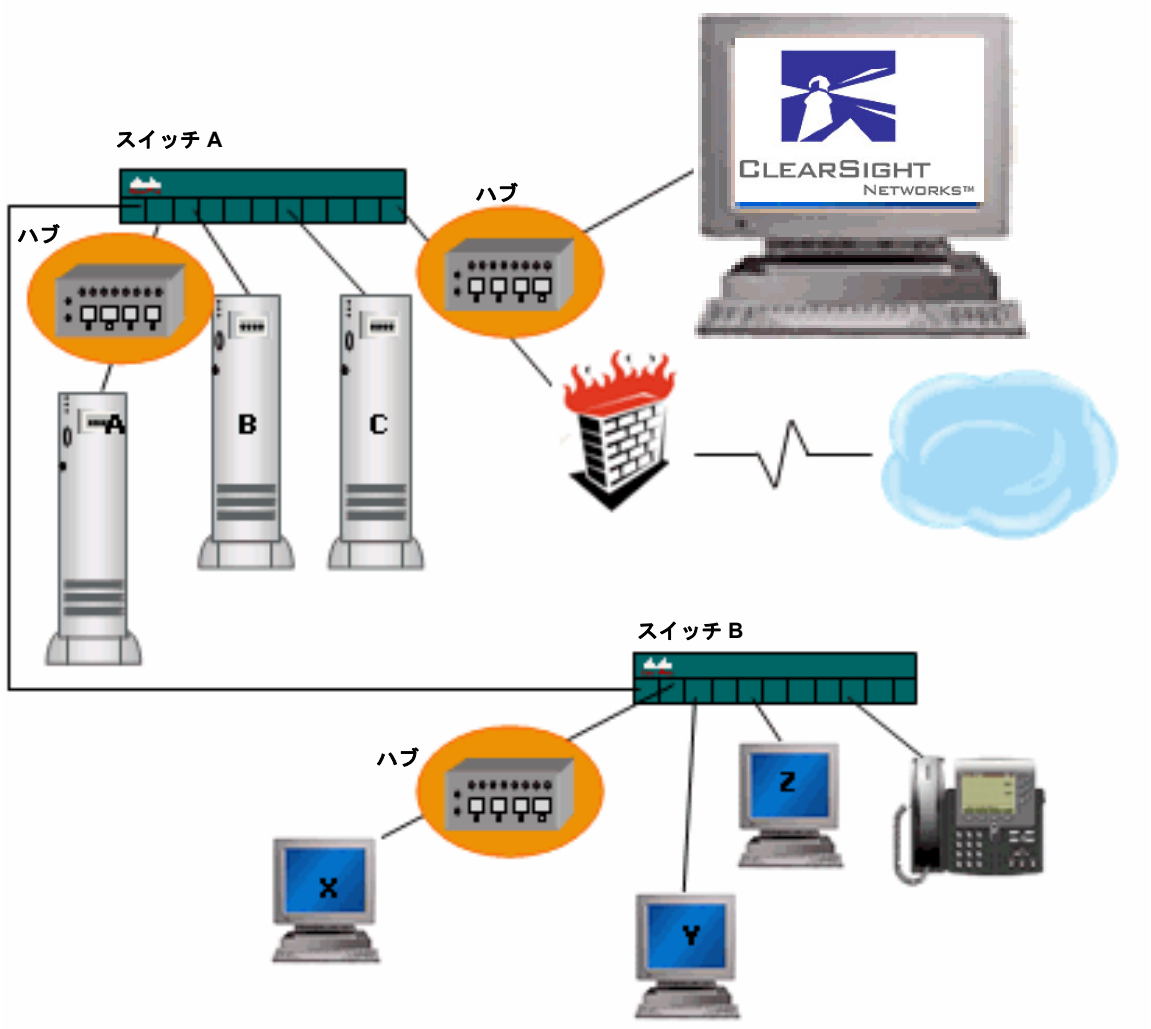


図 2-1: ハブの挿入

タップの接続

ClearSight Application Flow Analyzer

ClearSight は、タップを使用してネットワークに接続することが可能です。ネットワークタップは、ネットワーク上に配置され、1 つ以上のモニタポートへ回線を流れるデータをコピーする受信デバイスです。ネットワークタップは、カッパーや光ファイバなどさまざまなネットワークメディアで使用できます。多くのネットワークは、すでに配置されたタップを使用して設計され、特定のネットワークセグメントに容易にアクセス可能にします。

図 2-2 は、タップを使用してネットワークのモニタと解析を行う方法の一例を示しています。この例では、**スイッチ A** と**スイッチ B** の間のタップは、全二重リンクの両側をそれぞれ ClearSight Analyzer が接続されている個別のモニタポートに分割します。

注記 : 別売りの ClearSight 10/100 全二重イーサネットアダプタを所有している場合、単一の ClearSight Analyzer を使用して、図 2-2 に示すように接続を構築することもできます。詳細は、434 ページの「ギガビット XD イーサネットカードの設定」を参照してください。

長所と短所

タップは、次のような点でハブよりも優れています。

- ハブとは異なり、ネットワークタップは全二重リンクの整合性を維持して、モニタと解析用にそれぞれリンクの両側を分割します。
- ネットワークタップはパッシブデバイスであるため、リンクをダウンさせることなく常にタップをネットワークに設置しておき、必要に応じて ClearSight を接続することができます。

ネットワークタップにも短所があります。以下はその例です。

- ネットワークタップを挿入することにより、ネットワークに潜在的な障害点が追加されます。タップに障害が発生すると、共にリンクも切断されます。
- ネットワークのすべてのトラフィックを監視するには、全二重ネットワークセグメントごとにタップを挿入する必要があり、これには費用がかかります。

- 全二重リンクに接続すると、タップは、リンクの両側 (DTE と DCE) をそれぞれ、モニタポートへ分割します。リンクの両側をモニタするには、2 つの ClearSight Analyzer (リンクの両側に 1 つずつ。図 2-2 を参照)、または 10/100 全二重イーサネットカードを使用するバージョンの ClearSight Analyzer (Application Flow Analyzer) のいずれかが必要になります。このカードには、リンクの両側を同時にモニタする機能があります。

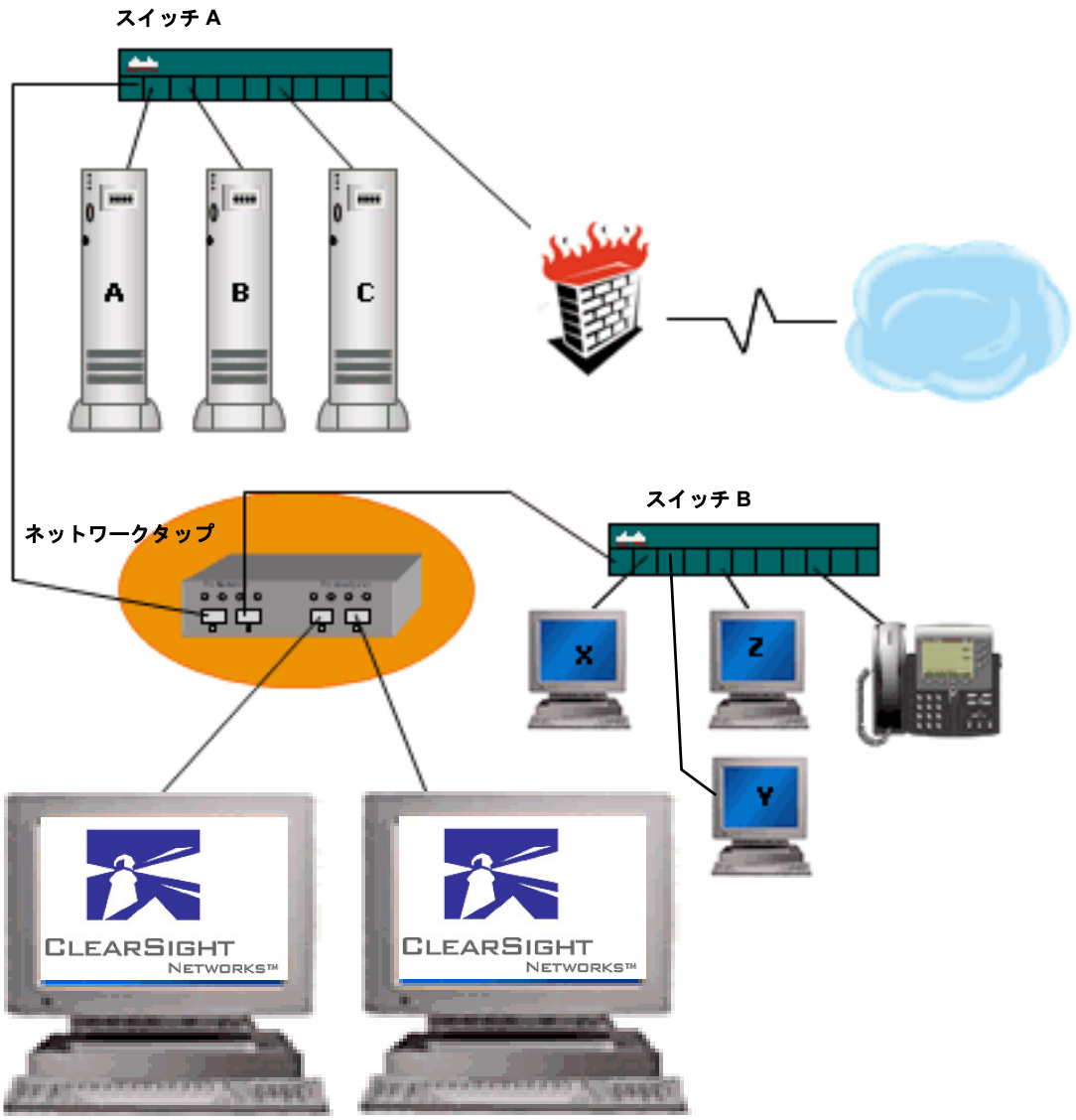

スイッチ A
A
B
C
スイッチ B
ネットワークタップ
X
Z
Y
CLEARSIGHT
NETWORKS™
CLEARSIGHT
NETWORKS™

図 2-2: タップの挿入

ポートミラーリングの使用

ClearSight Application Flow Analyzer　ClearSight Analyzer Light

多くのスイッチは、ネットワークモニタを可能にするポートミラーリングをサポートしています。ポートミラーリングによって、スイッチ上にある 1 つ以上のモニタポートに流れるトラフィックを、指定されたモニタポート (「ミラーポート」または「スパンポート」とも呼ばれる) にコピーできます。ClearSight をこのモニタポートに接続して、コピーされたトラフィックを監視することができます。

図 2-3 は、ポートミラーリングを使用してネットワークのモニタと解析を行う方法の一例を示しています。この例は、次のようになっています。

- **スイッチ A** では、**スイッチ B** とのスイッチ間のリンクで送受信されるトラフィックが、**スイッチ A** のモニタポートにミラーリングされています。ClearSight は、モニタポートに接続されています。
- **スイッチ B** では、**ワークステーション X**、**Y**、および **Z** のポートで送受信されるトラフィックが、**スイッチ B** のモニタポートにミラーリングされています。ClearSight は、モニタポートに接続されています。

長所と短所

ポートミラーリングは、次のような点でハブやネットワークタップよりも優れています。

- ポートミラーリングにより、単一のポートではなく、複数のポートからのトラフィックをモニタまたはキャプチャすることが可能です。大部分の実装では、特定の VLAN のすべてのトラフィックをモニタポートにコピーでき、問題のある構成をすばやく解析できます。
- ポートミラーリングでは、ハードウェアをインストールする必要がありません。

ポートミラーリングにも短所があります。以下はその例です。

- すべてのスイッチがポートミラーリングをサポートしているわけではありません。
- 異なったスイッチではポートミラーリングの実装が異なり、スイッチ上でのポートミラーリングの構成方法を理解する必要があります。
- 間違って使用すると、ポートミラーリングはネットワークループを引き起こす可能性があります。
- ポートミラーリングは、スイッチのプロセッサとメモリバッファに負担をかけます。極端な場合には、ポートミラーリングは、スイッチが再起動するほど、スイッチプロセッサに負荷がかかる可能性があります。
- ポートをミラーリングすればするほど、スイッチは、モニタポートにデータを送信する前に、より多くのデータをバッファする必要があります。これは、コマンドと応答の待機時間を測定する際に、デルタ時間の正確性に影響します。また、スイッチはモニタポートに送信する前にパケットをドロップしてしまう可能性があり、その結果アナライザで間違ったエラーメッセージを表示してしまう場合があります。

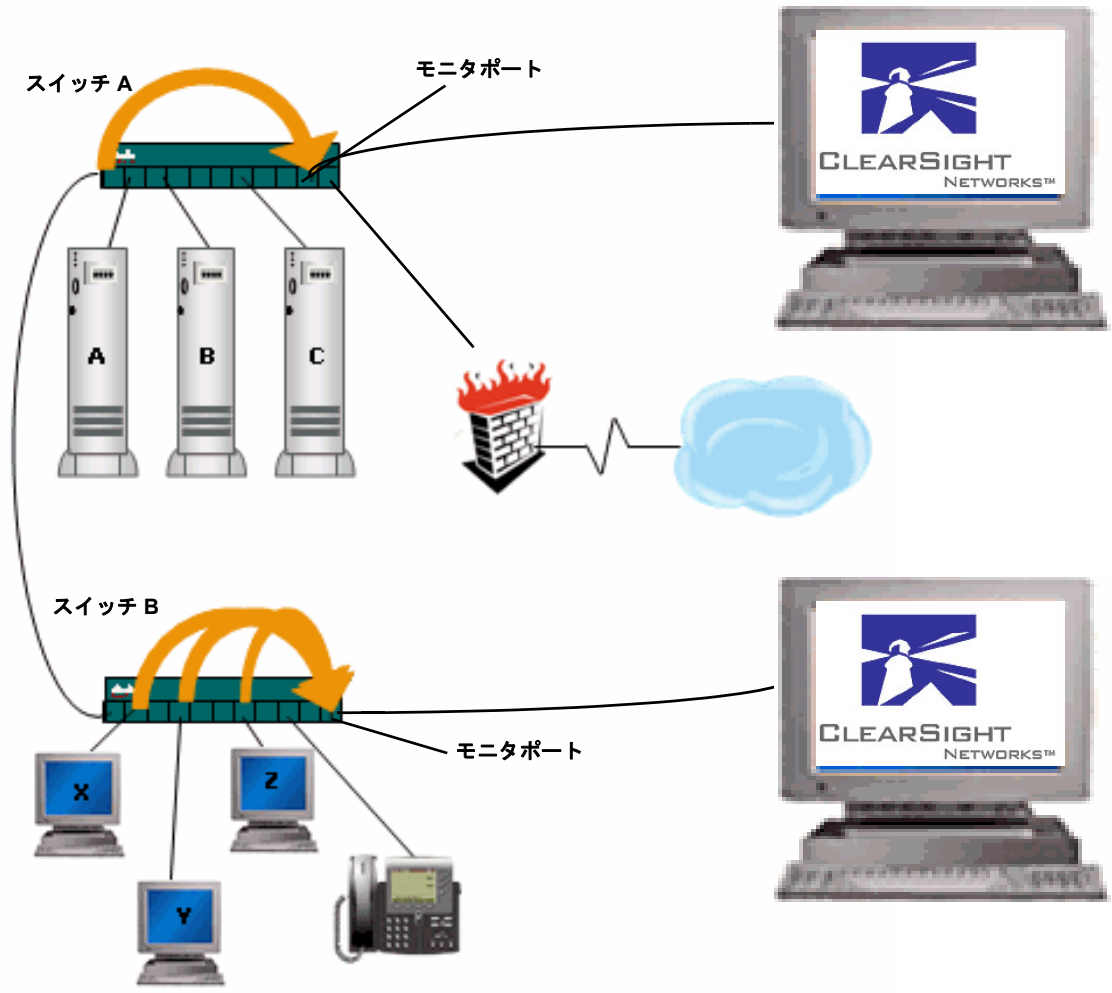


図 2-3: ポートミラーリングの使用

ClearSight Distributed エージェントの接続

ClearSight Distributed エージェントをネットワークに接続する場合、エージェントビューアとエージェントの通信と、ネットワークのモニタに同じインターフェイスカードを使用できます。ただし、ClearSight Distributed エージェントの PC に複数のネットワークインターフェイスカードがインストールされている場合は、カードを次のように使用できます。

- エージェントビューアとエージェントとの通信用に、エージェント用に 1 枚目のカード (通信カード) を使用する。
- 実際のネットワークモニタリング用に 2 枚目のカード (モニタカード) を使用する。

この実装には、次のような利点があります。

- モニタおよび解析のパフォーマンスが向上します。エージェントビューアとエージェントの通信にモニタカードを使用しない場合は、そのリソースが解放され、モニタと解析のパフォーマンスが向上します。
- ネットワークに問題が発生しても、ネットワークモニタ機能が維持されます。通信カードとモニタカードを別のネットワークセグメントに接続すると、モニタカードが接続されているネットワークセグメントに問題が発生したとき (つまり、ClearSight の機能が最も必要とされるとき) も、エージェントビューアとエージェントの間の通信を保持できます。

図 2-4 には、2 枚のネットワークインターフェイスカードを使用した Distributed エージェントのインストール例を示します。

この例では、エージェントビューアは通信カードを使用し、LAN セグメント 1 を介して ClearSight Distributed エージェントと通信しています。一方、Distributed エージェントはモニタカードを使用し、LAN セグメント 2 をモニタしています。これによって、LAN セグメント 2 に問題が発生しても、エージェントマネージャはエージェントと通信できます。

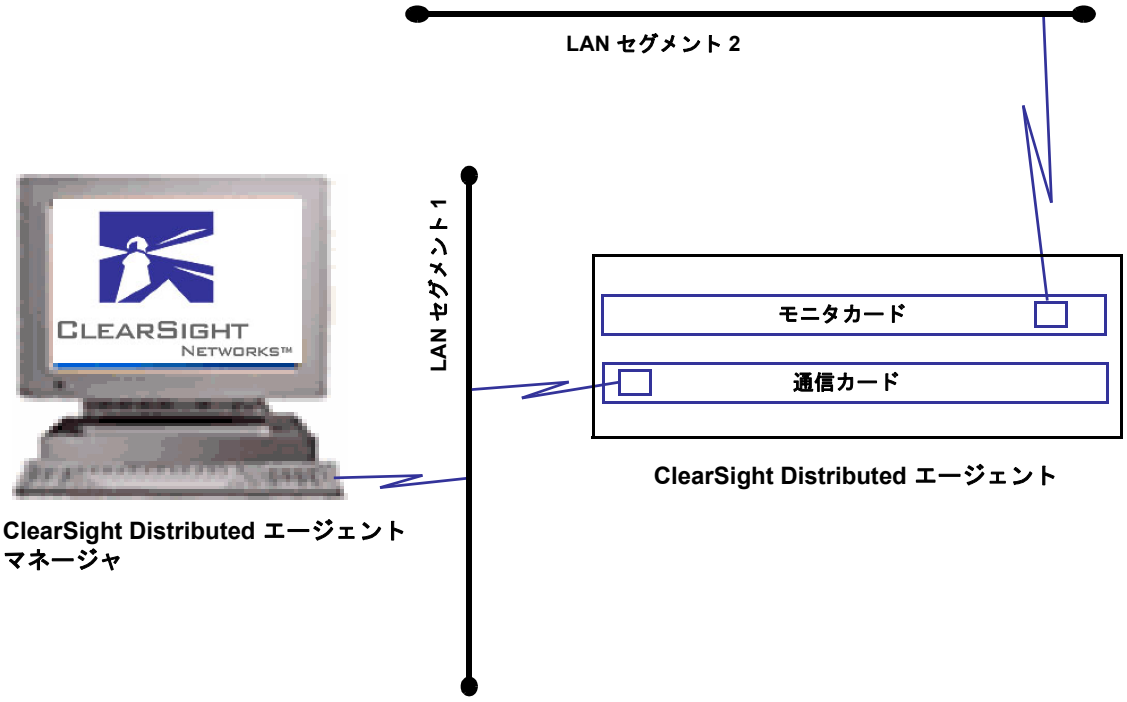


図 2-4: Distributed エージェントで 2 枚の NIC を使用した場合

2 枚のインターフェイスカードによるエージェントの設定

図 2-4 で示したとおり、エージェントで 2 枚のインターフェイスカードを使用するための設定は比較的簡単です。

- エージェントを [エージェントリスト] に追加するときに、[エージェントの追加] ダイアログボックスの **[ホスト名]** フィールドを、通信先エージェントのアダプタの IP アドレスに設定します。

- [アダプタを開く] ダイアログボックス (図 2-5) が表示されたら、エージェントビューアとエージェントの通信に使用するアダプタとは別の、モニタ用アダプタを選択します。

注記 : エージェントを [エージェントリスト] に追加する方法、[アダプタを開く] ダイアログボックスの使用方法、その他の ClearSight Distributed の概念については、第 4 章の「ClearSight Distributed の使用」で説明します。



図 2-5: [アダプタを開く] ダイアログボックス

2 枚のインターフェイスカードの使用例

図 2-5 では、標準的な ClearSight Networks ループバックアダプタのほかに、4 つのアダプタがリストされています。ここでは、**ClearSight Fast Ethernet Adapter #2** アダプタに IP アドレス **192.168.1.100** が割り当てられており、**ClearSight Fast Ethernet Adapter** に IP アドレス **192.168.5.100** が割り当てられているとします。この例では、次の作業が可能です。

- **[ホスト名]** フィールドの IP アドレス **192.168.1.100** を使用して、エージェントを [エージェントリスト] に追加する。つまり、通信カードとして **ClearSight Fast Ethernet Adapter #2** アダプタを使用します。
- エージェントに接続し、[アダプタを開く] リストで **ClearSight Fast Ethernet Adapter** を選択する。つまり、モニタカードとして **ClearSight Fast Ethernet Adapter** を使用します。

まとめ



ClearSight をネットワークに接続するには、効果的なモニタと解析に必要な、ネットワークのデザインとデータを考慮に入れる必要があります。一般的に、次のように言えます。

- ハブは、迅速で簡単な費用対効果のよいソリューションに最も有効です。
- タップは、全二重リンクの両側を同時にモニタする際に有効です。また、ネットワークの実装の初めから、ネットワークのデザインに盛り込むこともできます。
- ポートミラーリングは、複数のスイッチポート、または単一の VLAN からのデータを監視する際に、最も有効です。
- ClearSight Distributed エージェントを接続する場合は、2 枚のカード (通信カードとモニタカード) を使用するほうが有利なことがあります。また、モニタ中のセグメントにネットワーク障害が発生してもネットワーク通信を維持できるように、2 枚のカードを別のネットワークセグメントに接続するのもよい方法です。

第 3 章

ClearSight Analyzer の概要

ClearSight Analyzer ソフトウェアは、ネットワークモニタ、パケットキャプチャ、プロトコル翻訳などの従来のネットワークアナライザの機能と、ネットワーク上の障害を発生に応じて表示する強力なリアルタイムアプリケーションモニタ機能が一つになった強力なネットワーク管理ツールです。

この章では、以下の項目について説明します。

- ClearSight の機能
- CSA 7.0.7 の新機能
- 利用可能なモデル
- ClearSight スタンドアロンの基本設定
- スタンドアロン Analyzer の [ユーザリスト] の設定
- ClearSight Analyzer スタンドアロンの起動
- ClearSight ユーザインターフェイス
- ClearSight の使用方法

※この章には、一部 ClearSight Analyzer Light には、適用されない内容が含まれています。それぞれの機能の詳細な適用状況については、第 5 章 (111 ページ) 以降をご参照ください。

スタンドアロン機能および分散機能について

この章で述べる機能は、スタンドアロン設定で使用しても、ClearSight Distributed エージェントに接続して使用しても同じです。主な違いは、次のとおりです。

- ClearSight Distributed エージェントに接続して作業する場合は、ローカル PC ではなく、エージェントビューアでコマンドの実行や ClearSight 画面の表示を行います。ClearSight Distributed の詳細な使用方法に関しては、第 4 章「ClearSight Distributed の使用」を参照してください。

注意 : CSD は CSA バージョン 7.0.7 でサポートされていません。

ClearSight の機能



ClearSight Analyzer ソフトウェアは、接続されたネットワークセグメントに流れるデータのモニタと解析をします。ClearSight は、ネットワークに流れるさまざまな IP フローやそこで実行しているアプリケーションの情報を取得して、ネットワーク状況の理解に役立つさまざまな統計、チャート、およびグラフを提供します。ClearSight では、以下の主要な機能が提供されます。

- 次の一般的な IP ベースのネットワークアプリケーションに重点を置いたリアルタイムアプリケーションモニタ
  - WWW (HTTP)
  - 電子メール (SMTP、POP、および MS-Exchange)
  - データベース (MS SQL および Oracle)
  - Voice-over-IP (H.323、SIP、Skinny、MGCP、および Megaco)
  - ストリーミングメディア (RTP、RTSP)
  - セキュリティ (Kerberos および ISAKMP)
  - その他の一般的なネットワークアプリケーション (DNS、FTP、Telnet、Citrix)
- さまざまなネットワークの問題に対するリアルタイムの問題検出と通知
- パケットキャプチャとプロトコル翻訳

- アプリケーションモニタの拡張機能を使用し、ユーザに表示されたアプリケーションフローと同じフローを再現する強力なポストキャプチャアナリシス。例えば、Web トランザクションの再現、電子メールの表示、さらに ClearSight PC のスピーカ上で VoIP 会話の再生が可能です。
- 強力なフィルタ機能
- ネットワークのベースライニング、メンテナンス、および将来の拡張計画を行うのに適した各種のカスタマイズ可能なレポート

Light バージョンについて

ClearSight Analyzer Light は機能限定の CSA 低価格版を必要とするユーザ向けに開発されました。

ClearSight Analyzer Light は CSA をベースにいくつかの機能を制限したものとなっていますが、このガイドの大部分は、完全な機能を持つ ClearSight Analyzer についての記述になっています。そこでこのセクションでは、通常の CSA と CSA Light との違いについて記述します。

ネットワークアダプタサポートの制限

ClearSight Analyzer Light は半二重 10/100/ 1000 イーサネットアダプタのみをサポートします。全二重イーサネットアダプタ、ギガビット SC-1 カードアダプタ , ギガビット XD カードアダプタ , または 10 ギガビットアダプタはサポートしません。

Vista サポートの制限

Windows Vista 上で ClearSight Analyzer Light を実行する場合、ユーザは ClearSight を管理者として実行する必要があります。

ClearSight Analyzer Light で制限された機能

以下では CSA Light で制限された機能について記述します。

ユーザ設定

ユーザ設定 (66 ページ参照) は無効になります。

モニタ機能の制限

- アプリケーションレイヤに関する全ての情報は表示されません。
- ネットワークレイヤでは、トランスポートレイヤのみの表示に制限されます。
- ネットワークレイヤでは、マルチキャストタブは表示されません。
- 物理層レイヤでは、サブネットタブは表示されません。
- リアルタイム翻訳機能は無効になります。

アラート機能の制限

- アプリケーションレイヤの事象および問題は表示されません。
- 事象と問題のフィルタは無効になります。

レポート機能の制限

- アプリケーションレイヤのレポートは表示されません。ユーザ定義レポートの設定においてもアプリケーションレイヤレポートは選択できません。
- ヒストリタブは表示されません。
- コールブラウザタブは表示されません。

パケットジェネレータ

パケットジェネレータは無効になります。また送信ボタンは表示されません。

キャプチャ機能の制限

- キャプチャ中 ClearSight ビューを有効にした場合、アプリケーションレイヤは表示されません。

- 設定タブでは、キャプチャの優先度オプションは無効になります。
- トリガタブでは、アプリケーションレイヤのアラームトリガは設定できません。IP および DLC アラームでのトリガのみ設定できます。
- 事象と問題タブでは、フィルタは無効になります。
- アプリケーションレイヤの事象と問題は無効になります。

設定の制限

[設定] ボタン ->[設定] タブから、以下のオプションは削除されます :

- 共通 > モニタ設定
- 共通 > モニタオプション > アプリケーション
- 共通 > CSV 設定 > 設定 > RTP フロー
- 共通 > プロトコルフォーシング
- 問題 > スレッショルド > 問題 : アプリケーションに関連したスレッショルドはすべて削除されます。IP と DLC のみ設定できます。
- 翻訳 > 設定
- 翻訳 > プロトコルフォーシング
- VoIP、レポート、WEP

フィルタ設定機能の制限

設定 > フィルタタブで新規フィルタを作成する際、新規フィルタダイアログボックスでアプリケーションレイヤフィルタは表示されません。フロー、パターン、IP サブネット、プロトコル、MAC アドレスおよび物理層フィルタのみ有効になります。

その他の機能制限

EtherOAM 翻訳、WiMax および Spirent Integration はサポートされません。

メニュー項目の削除

メニューバーから以下の項目が削除されます :

- ファイル > マージ
- ファイル > ログオフして終了
- ツール

試用版ライセンス

ClearSight Analyzer Light の試用版ライセンス期限は 5 日間に設定されています。ClearSight Analyzer Light 試用版から正規版へアップグレードするには、試用版を一度アンインストールした後、正規版を再度インストールする必要があります。

CSA 7.0.7 の新機能

CSA 7.0.7 では、以前の CSA 7.0.6 から、主に以下のような新機能が追加されました。

- **3G-324M 再生** — AMR または MPEG4 コーデックを使用している 3G-324M フローのメディアコンテンツを再生できます。
- **Wireshark バージョン 1.2.2 サポート** — Wireshark バージョン 1.2.2 をサポートします。247 ページの「[トレースファイルを開くときの動作]」を参照して下さい。

利用可能なモデル

表 3-1 は、CSA 7.0.7 の利用可能なモデルです。

表 3-1: ClearSight アナライザ 7.0.7 のモデル

プラットフォーム	モデル	OS
汎用 PC	CSA と汎用の NIC	Windows XP SP2, Vista SP1/SP2
Dolch	CSA と 1 ギガビット XD アダプタ (SUS)	Windows XP SP2
	CSA と 10 ギガビット NT20 アダプタ (SUS)	

注意 : CSD は CSA バージョン 7.0.7 でサポートされていません。

ClearSight スタンドアロンの基本設定

※以下は ClearSight Analyzer Light では必要ありません。

ClearSight スタンドアロンをインストールする場合、次の設定をします。

1. ClearSight Analyzer の [ユーザリスト] を設定する。[ユーザリスト] には、このプログラムの操作を許可されたすべてのユーザが含まれます。
2. ClearSight スタンドアロン Analyzer を起動する。

これらの項目について、以下に説明します。

スタンドアロン Analyzer の [ユーザリスト] の設定

※以下は ClearSight Analyzer Light では必要ありません。

セキュリティ上の理由から、すべての ClearSight Analyzer は、このアナライザを操作可能なユーザのリストを保持します。ユーザが、有効なユーザ名とパスワードなしにログインしようとすると、アナライザは接続を拒否します。

重要：ClearSight Analyzer スタンドアロンは、次のデフォルトのユーザ名とパスワードでインストールされます。

ユーザ名　　Admin

パスワード　＜空白＞(パスワードなし)

[ユーザリスト] の管理

次の手順で示すように、ユーザ設定ユーティリティを使用して ClearSight の [ユーザリスト] を管理します。

ClearSight Analyzer の [ユーザリスト] の設定手順

1. **[スタート]** > **[すべてのプログラム]** > **[ClearSight]** > **[ユーザ設定]** を選択して、ユーザ設定ユーティリティを起動します。[ユーザ設定ログイン] ダイアログボックス (図 3-1) が表示されます。
2. デフォルトのユーザ名 **Admin** を入力して、**[OK]** をクリックします。

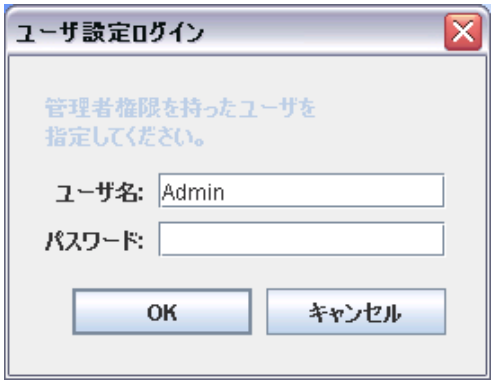


図 3-1: [ユーザ設定ログイン] ダイアログボックス

[ClearSight ユーザ設定] ダイアログボックス (図 3-2) が表示されます。初期状態では、このウィンドウにはログインした管理者 (Admin) だけが表示されます。この管理者は、[ClearSight ユーザ設定] ダイアログボックス内の対応するボタンを使用して、このリストでユーザの追加、編集、削除を行うことができます。

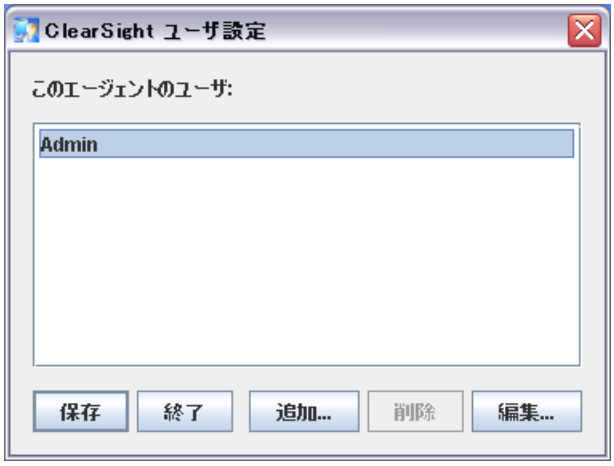


図 3-2: 初期状態の [ClearSight ユーザ設定] ダイアログボックス

3. Admin 自体を削除することはできません。ユーザが Admin である場合は、新しいパスワードを設定することをお勧めします。新しいパスワードを設定するには、**[編集]** ボタンをクリックします。[ユーザの編集] ダイアログボックス (図 3-3) が表示されます。新しいパスワードを入力して (2 回)、**[OK]** をクリックし

ます。新しいパスワードは直ちに有効になり、[ClearSight ユーザ設定] ダイアログボックス (図 3-2) が再び表示されます。

注記：[権限] ボタンの機能については、後ほど説明します。

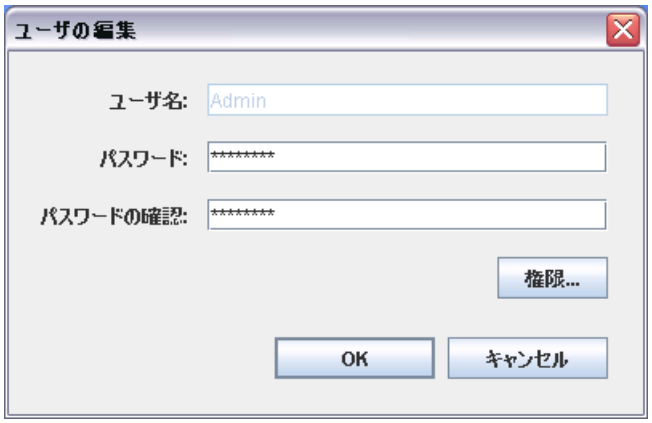


図 3-3: Admin の [ユーザの編集] ダイアログボックス

4. [ユーザリスト] に他のユーザを追加できます。その場合は、**[追加]** ボタンをクリックします。[ユーザの追加] ダイアログボックスが開き、新しいユーザのユーザ名とパスワードの入力 (2 回) を要求されます。たとえば、ユーザ David を追加すると、[ユーザの追加] ダイアログボックスは 図 3-4 のようになります。



図 3-4: David の [ユーザの追加] ダイアログボックス

重要：[ユーザリスト] に追加したユーザ名とパスワードの組み合わせを覚えておいてください。これらの許可されたユーザに対して同一のユーザ名とパスワードを指定する必要があります。

5. 新しいユーザのユーザ名とパスワードを設定するほかに、そのユーザの「権限」を設定できます。**[権限]** ボタンをクリックします。[ユーザ権限：David] ダイアログボックス (図 3-5) が表示されます。

   設定できる権限は、以下の 3 種類です。

   - **[管理者ユーザ権限]** ― この権限では、ユーザは次のことを行うことができます。
     - 他のユーザの作成、編集、削除。
     - [設定] ページ上の設定の変更。

     注記：Admin を削除したり、Admin の権限を無効にできるユーザはありません。ただし、**[管理者ユーザ権限]** が有効になっているユーザは、Admin のパスワードを変更できます。
   - **[アプリケーションコンテンツ閲覧権限]** ― この権限では、ユーザはアプリケーションの内容 (VoIP 会話や電子メールなど) を表示できます。

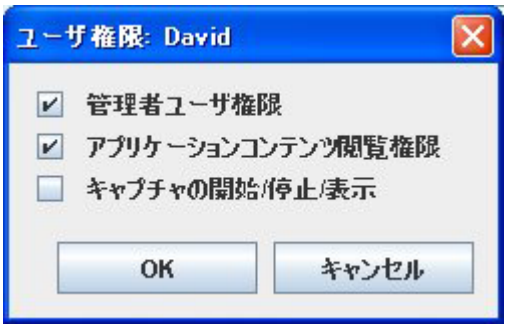


図 3-5: **[ユーザ権限：David] ダイアログボックス**

6. このユーザに設定する権限を選択したら、**[OK]** をクリックします。[ユーザの追加] ダイアログボックスが再び表示されます。もう一度 **[OK]** をクリックします。[ClearSight ユーザ設定] ダイアログボックスに戻り、図 3-6 のように新しいユーザがリストに表示されます。

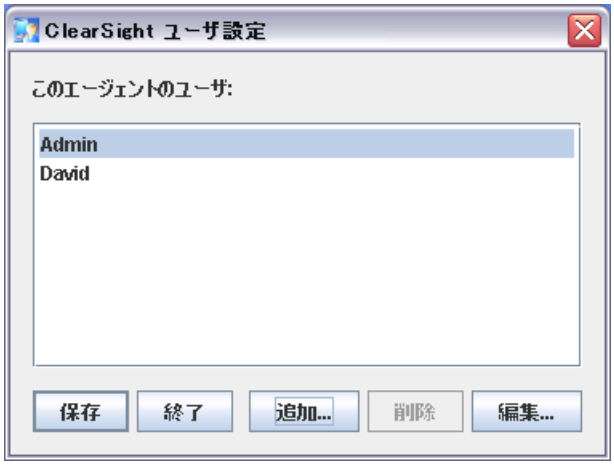


図 3-6: David が追加された [ユーザリスト]

7. ユーザをリストに追加したら、**[保存]** ボタンをクリックして変更を保存します。

   ほとんどの変更は、直ちに有効になります。ただし、現在ログイン中のユーザを削除した場合は、そのユーザのすべてのアクティブなセッションは終了してしまいます。

ClearSight Analyzer スタンドアロンの起動

※ ClearSight Analyzer Light では以下の [ClearSight ログイン] ダイアログボックスは表示されません。

1. **[スタート] > [すべてのプログラム] > [ClearSight] > [ClearSight Analyzer]** を選択して、ClearSight Analyzer スタンドアロンを起動します。[ClearSight ログイン] ダイアログボックス (図 3-7) が表示されます。



図 3-7: [ClearSight ログイン] ダイアログボックス

2. 有効なユーザ名とパスワードを入力して、**[OK]** をクリックします。
3. ClearSight Analyzer を最初に起動したときは [アダプタを開く] ダイアログボックス (図 3-8) が表示されます。

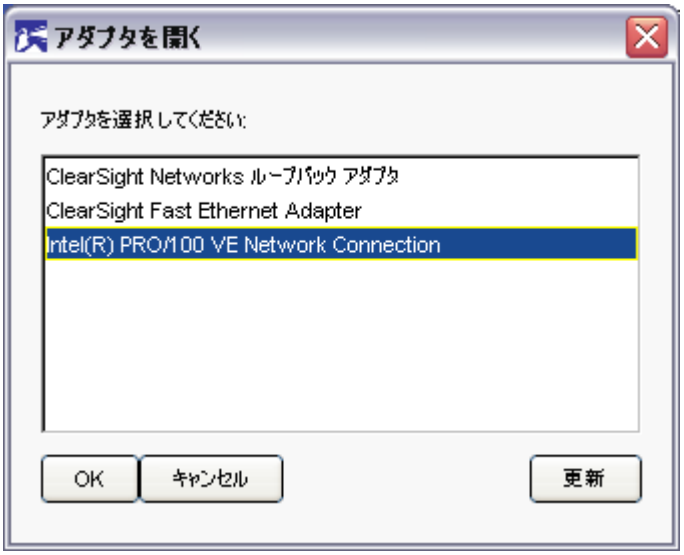


図 3-8: [アダプタを開く] ダイアログボックス

4. 使用するネットワークアダプタを選択し、**[OK]** をクリックします。
5. ClearSight ユーザインターフェイス (図 3-9) が表示されます。

ClearSight ユーザインターフェイス

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

図 3-9 に示すように、ClearSight のユーザインターフェイスには、いくつかの主要なコンポーネントがあります。

- ツールバーにより、リアルタイムモニタ、アラートログ、レポートなど、ClearSight の主要機能に簡単にアクセスできます。75 ページの「ClearSight ツールバー」では、ツールバーにある各ボタンの詳細を説明します。
- メインワークスペースでは、ツールバーで選択されている機能に応じて、表示が変更されます。ClearSight を最初に開始したときは、[モニタ] 機能が選択され、そのボタンがツールバーでハイライト表示されます。それに応じて、ワークスペースには、リアルタイムモニタインターフェイスが表示されます。
- メニューでは、トレースファイルのオープンや保存、選択されているアダプタの変更、モニタのカウンタのリセット、キャプチャの開始および停止、オンラインヘルプファイルへのアクセスなど、その他のコマンドを利用できます。一般的に、ツールバーのボタンを使って、最も多く使用する機能にアクセスします。メニューを使って、その他の補足的な機能にアクセスします。

これらの主要機能に加えて、ClearSight では、タイトルバーとキャプションバーに次のような情報が表示されます。

- タイトルバーには、ClearSight がモニタしているアダプタが表示されます。
- キャプションバー (表示画面の下部にあるバー) には、次の情報が表示されます。
  - 現在進行中のモニタセッションの時間 (**実行時間**)。
  - ClearSight がモニタ統計の収集を開始した日時 (**開始時刻**)。
  - ClearSight が監視しているネットワークトラフィックの量を即時に示すリアルタイムの**ネットワークアクティビティ**の LED。
  - **ギガビットリンクステータス**の LED (ギガビットイーサネットカードを選択していた場合に限る)。赤色はリンクが機能停止中であることを、緑色はリンクが稼働中でアクティブであることを示す。

ClearSight のメニュー、**[ファイル]**、**[キャプチャ]**、**[モニタ]**、**[ヘルプ]** では、トレースファイルのオープンおよび保存、アダプタの切り替え、キャプチャの開始および停止、モニタ統計のリセット、Trace Route の実行、オンラインヘルプファイルへのアクセスなどを行うことができます。

ClearSight のツールバーにより、最も一般的に使用される機能とオプションにアクセスできます。ClearSight を最初に開始したときは、**[モニタ]** 機能が選択されています。そのカウンタがツールバーでハイライト表示されます。



メインワークスペースでは、ツールバーで選択されている機能のインターフェイスが表示されます。この例では、リアルタイムの **[モニタ]** 機能が選択されています。それに応じて、[アプリケーションモニタ] の [ダッシュボード] が表示され、ネットワーク上で実行しているアプリケーション全体の状態、およびネットワーク層の接続とその物理統計の概略が提供されます。表示されている特定のカウンタをクリックして、ここから詳細を表示できます。

通常、表示されているカウンタをクリックして、ClearSight ユーザインターフェイスをナビゲートします。表示されている特定のカウンタがクリック可能な場合、マウスカーソルが指さしに変わって、カウンタをクリックすると詳しい統計と解析が表示できます。

図 3-9: ClearSight ユーザインターフェイス

ClearSight ツールバー

図 3-10 は、ClearSight ツールバーを示しています。ツールバーにより、最も一般的に使用される ClearSight の機能に簡単にアクセスできます。

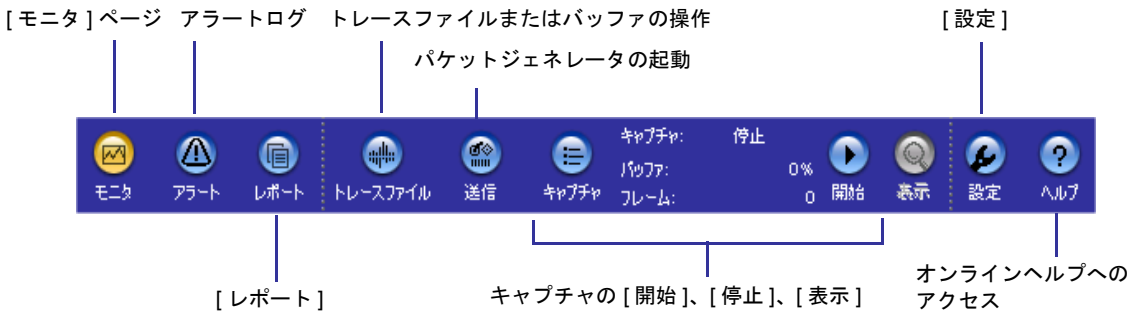


図 3-10: ClearSight ツールバー

図 3-10 で示すように、ClearSight ツールバーには、次のボタンがあります。

[モニタ] このボタンをクリックすると、リアルタイムモニタインターフェイスが表示されます。リアルタイムモニタについては、第 5 章「ClearSight を使用したネットワークのモニタ」で説明します。

[アラート] このボタンをクリックすると、アラートログが表示されます。アラートログの操作については、第 10 章「アラートの操作」で説明します。

[レポート] このボタンをクリックすると、モニタが収集したデータのレポートが表示されます。レポートについては、第 12 章「レポートの使用」で説明します。

[トレースファイル]	このボタンをクリックして、ポストキャプチャアナリシスのページで保存されたトレースファイルを操作します。トレースファイルとバッファのポストキャプチャアナリシスについては、第 7 章「ポストキャプチャアナリシス」で説明します。
[送信]	このボタンをクリックして、組み込みのパケットジェネレータを起動します (パケットジェネレータが搭載されている場合)。パケットジェネレータについては、第 13 章「パケットジェネレータの使用」で説明します。
[キャプチャ]	このボタンをクリックして、キャプチャセッションを設定します。データのキャプチャについては、第 6 章「ClearSight を使用したデータのキャプチャ」で説明します。
[開始 / 停止]	このボタンをクリックして、キャプチャセッションを開始および停止します。データのキャプチャについては、第 6 章「ClearSight を使用したデータのキャプチャ」で説明します。
[表示]	このボタンをクリックして、キャプチャバッファに現存するデータのポストキャプチャアナリシスを実行します。ポストキャプチャアナリシスについては、第 7 章「ポストキャプチャアナリシス」で説明します。
[設定]	このボタンをクリックして、フィルタ (第 9 章「フィルタの使用」)、アラート (第 10 章「アラートの操作」)、アドレス帳 (第 11 章「アドレス帳の使用」) などの ClearSight 構成オプションを操作するページにアクセスします。
[ヘルプ]	このボタンをクリックして、ClearSight のオンラインヘルプシステムにアクセスします。

ClearSight の使用方法

ClearSight Application Flow Analyzer　ClearSignt Distributed

特定のネットワークに特化した方法で ClearSight を使用することもできますが、どの方法でも次のフェーズの一部が使用されます。

- リアルタイムモニタ
- パケットのキャプチャ
- ポストキャプチャアナリシス (キャプチャ後の解析)

図 3-12 は、これらのフェーズを示しています。さらに、以下の項では、ClearSight を使用してネットワークをモニタ、管理、トラブルシューティングする手法の一例を説明します。

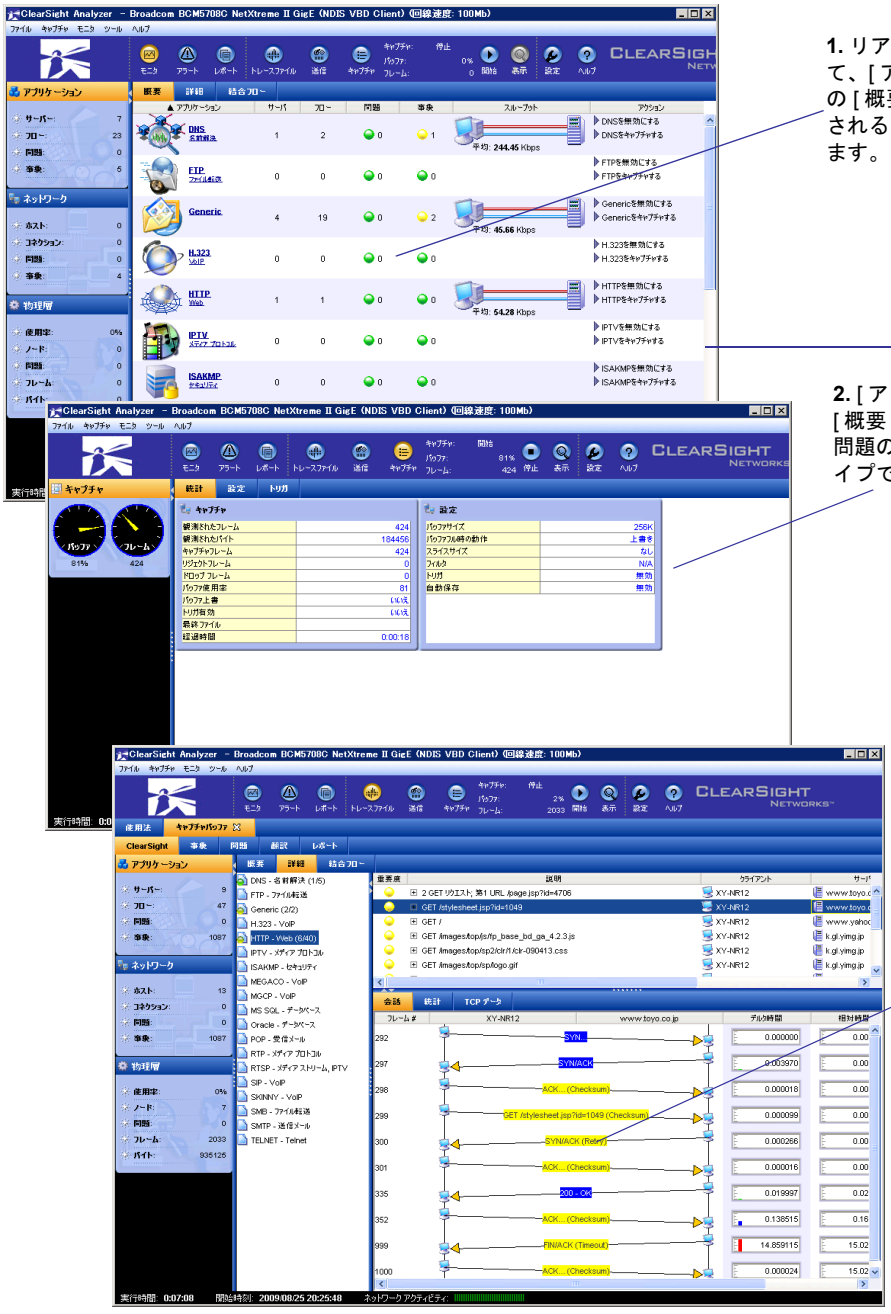


図 3-11: ClearSight を使用したネットワーク解析 - 手法の一例

リアルタイムモニタ

ClearSight は、アプリケーションが開始されるとすぐにネットワークのモニタを開始し、ネットワーク層の接続とネットワーク上のアプリケーションのフローに関連する統計と情報の表示を更新します。アプリケーションのフローとは、Web サーバーの **Get** または **Post**、電子メールメッセージの送受信、ドメイン名の解決、電話の呼び出しなどの特定の機能を実行するパケットのセットです。トランザクションの性質に従って、フローは最小 5 パケット、最大 200 パケットで構成されます。

モニタ中には、ClearSight はデータをキャプチャバッファに保存しません。その代わり、ClearSight は統計を収集しネットワーク上の問題と事象を警告します。それによって、より正確な表示が必要なときにキャプチャを開始できます。

リアルタイムモニタ表示の使用

リアルタイムモニタ中は、[アプリケーションモニタ] の [概要] にある **[問題]** と **[事象]** のカウンタに注意します。これらのカウンタが増加し始め黄色、オレンジ色、または赤色に変化した場合、該当するアプリケーションフローまたはネットワーク層の接続に問題が起きている可能性が示されています。この状況で、問題のあるアプリケーションに重点を置いたキャプチャを開始できます。

[ネットワーク] 層の **[チャート]** タブと **[ホスト]** タブにも注意する必要があります。これらのタブでは、ネットワーク上の大部分の帯域幅を消費しているプロトコルの概要がただちに表示され、原因となっているホストが示されます。ネットワークの問題は、帯域幅を集中的に使用するストリーミングメディアアプリケーション (SIP コールなど) または Web アクセスの悪用が原因となることがよくあります。ClearSight は、対処できるように問題となるユーザを直接示します。

パケットのキャプチャ

ClearSight のリアルタイムアプリケーションモニタがネットワーク上の潜在的な事象を警告した後、キャプチャを開始して、問題の背後にあるデータをクローズアップできます。キャプチャ中には、ClearSight はリアルタイムモニタ中に表示する統計と同じ統計を表示します。ただし、キャプチャ中にアナライザは、後で解析するためにキャプチャしたパケットをキャプチャバッファに格納します。このバッファの大きさ、フレームのスライスサイズ、バッファが一杯になったときに ClearSight が対処する方法を指定できます。

さらに、フィルタを設定して、必要なフレームのみのキャプチャに集中できます。例えば、単一の問題のあるアプリケーションタイプのキャプチャに集中するように、[アプリケーションモニタ] の [概要] でフィルタを直接設定できます。このようにして、問題を解決する必要があるフレームのみをキャプチャして、必要のないフレームでバッファが一杯になることを避けることができます。

ポストキャプチャアナリシス (キャプチャ後の解析)

キャプチャの後、ClearSight は、キャプチャバッファのパケットを解析する強力な機能を提供します。これにより、フレーム上に表示された問題をすばやく正確にゼロにします。

リアルタイムモニタと同じ画面、[アプリケーションモニタ] の [概要] で開始します。[アプリケーションモニタ] の [概要] のグラフィカルユーザインターフェイスにより、潜在的なボトルネック、問題、および事象に迅速にアクセスできます。**[問題]** と **[事象]** の列にある黄色または赤色のカウンタを確認します。これらのカウンタをクリックして、問題のあるフローまたは接続の詳細な統計を表示します。それに対して、ClearSight はクライアントとサーバー間での要求と返答のやりとりを再構築し、それをネットワークラダー図 (図 3-12) で視覚的に表示します。

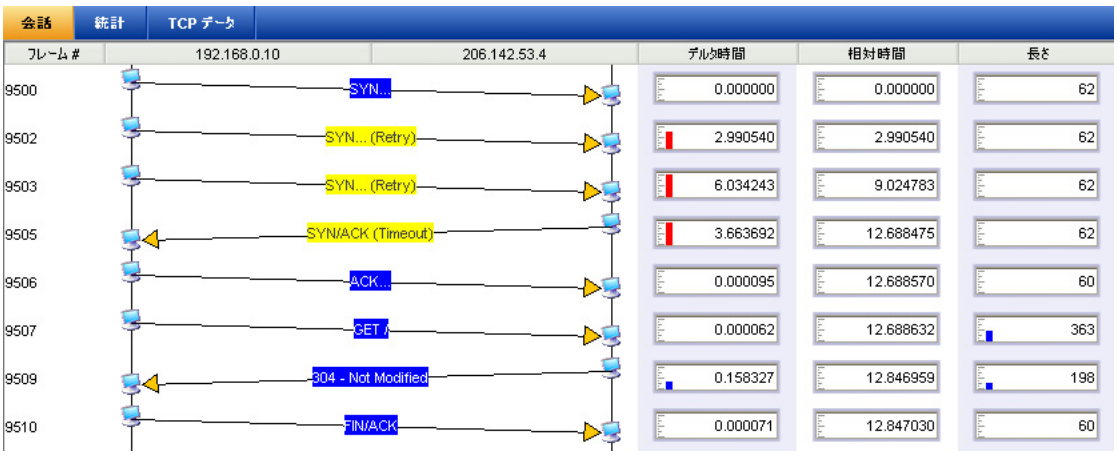


図 3-12: ネットワークラダー図

この図では、問題を表示している要求と応答が、問題の重要度に従って、黄色または赤色のいずれかで表示されます。たとえば、図 3-12 は HTTP サーバーへの GET 要求を再送する必要があったことを示しています。ここで、問題のある要求または応答をクリックして、選択したフロー内の問題のあるフレームに対する翻訳画面を直接表示することもできます。このように、問題のあるフレームを表示し、フレームを含んだフローに限定してフィルタされた翻訳画面を直接表示して、ClearSight は選択した問題のあるフレームでプロトコル解析を実行します。

フローを構成する要求と応答の交換を再構築するネットワークラダー図の他に、ClearSight のキャプチャ解析の詳細表示には、問題のあるフローがユーザにどのように表示されるかを示すアプリケーション固有の機能もあります。例えば、以下のことが可能です。

- PC スピーカで VoIP 会話を再生する。
- 問題のある HTTP 要求を ClearSight インターフェイス内で再試行する。
- ユーザに表示されたとおりに電子メールを表示する。
- ユーザが作成したとおりにデータベース要求を表示する。
- Telnet ターミナルに表示されたとおりに Telnet セッションを表示する。

利用可能な機能は、解析するアプリケーションフローのタイプによって異なります。アプリケーションタイプごとに利用可能な機能については、第 5 章「ClearSight を使用したネットワークのモニタ」で説明します。

第 4 章

ClearSight Distributed の使用

この章では、ClearSight Distributed システムの概要、主なコンポーネント、および Distributed バージョン固有の ClearSight 機能の使用方法について説明します。この章は次の項目で構成されています。

- 「ClearSight Distributed システムについて」
- 「ClearSight Distributed の基本」
- 「エージェントの [ユーザリスト] の設定」
- 「エージェントマネージャの使用」
- 「その他の CSD 固有の機能」

ClearSight Distributed システムについて

ClearSight Distributed システムは、1 つまたは複数の **ClearSight Distributed エージェント**に接続してそれを制御する、**ClearSight Distributed エージェントマネージャ**で構成されています。

- **ClearSight Distributed エージェントマネージャ**は、ClearSight Distributed システム内のエージェントを管理します。**エージェントマネージャ**ウィンドウでは、複数のエージェントに接続し、接続したエージェントごとに **ClearSight エージェントビューア**ウィンドウを開くことができます。さらに**エージェントマネージャ**は、アラートマネージャでアラームの**集中管理機能**を提供します。
- **ClearSight Distributed エージェント**は、接続先のローカルネットワークセグメントのモニタおよび解析を行います。解析結果は画面の更新と同時に ClearSight エージェントビューアに送信されます。

  Distributed エージェントマネージャから Distributed エージェントに接続すると、キーボードでコマンドを入力してトラフィックを解析しているかのように Distributed エージェントとの対話が可能になります。これによって、スタンドアロンバージョンの ClearSight で利用可能なリアルタイムのアプリケーションのモニタおよび解析機能を、遠隔地からすべて利用することができます。
- ClearSight Distributed エージェントを接続して作業する場合は、コマンドを入力して、エージェントのローカル PC ではなく、エージェントビューアで ClearSight 画面を表示します。

図 4-1 は、ClearSight Distributed システムを簡単に示しています。

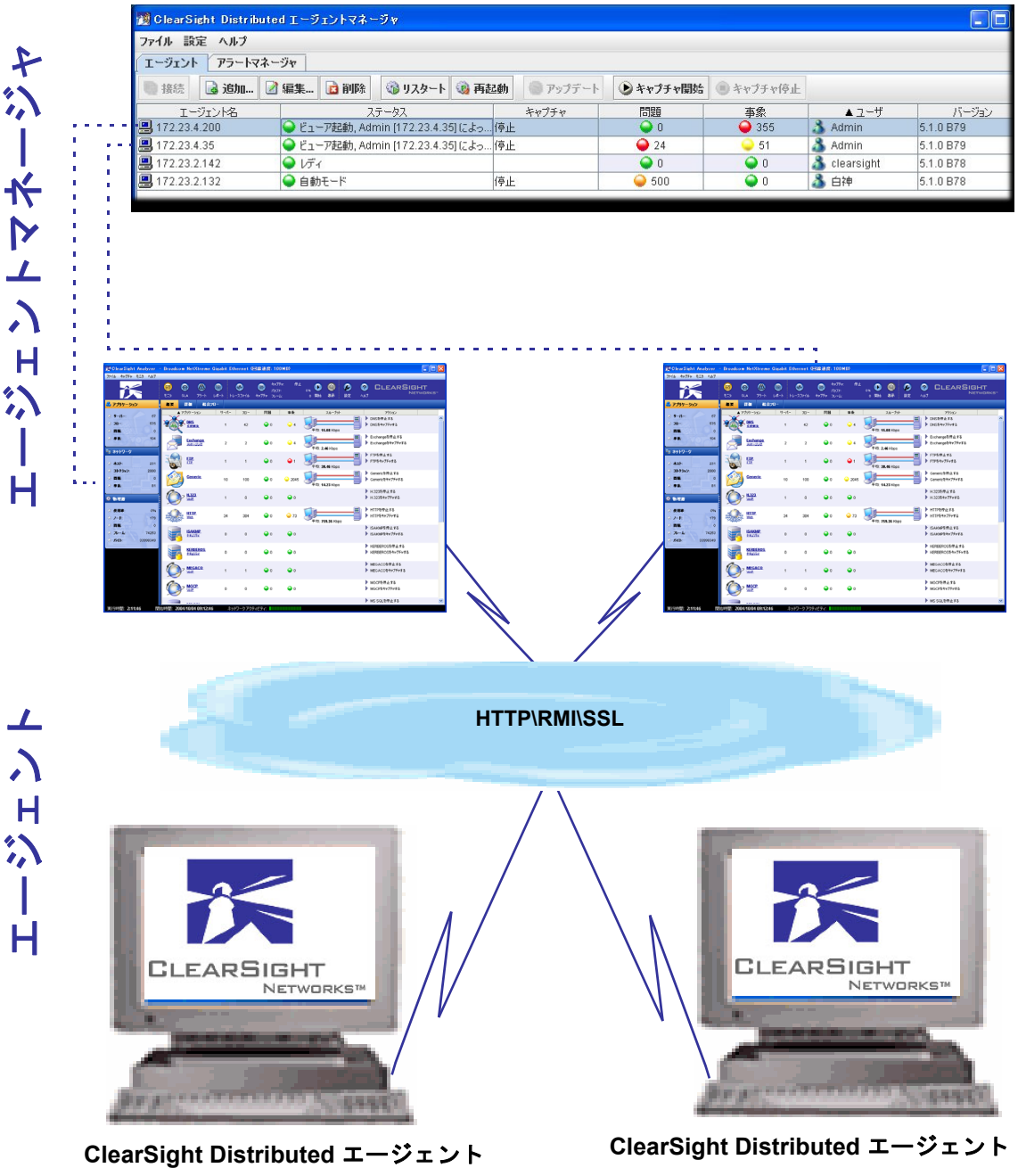


図 4-1: ClearSight Distributed システム

ClearSight Distributed の通信について

ClearSight Distributed エージェントソフトウェアのインストール中に、次の処理がセットアッププログラムによって自動的に行われます。

- **ClearSight カーネル**を、エージェント PC で使用可能なすべてのネットワークインターフェイスカードに**バインドします**。ClearSight カーネルを使用すると、エージェントはネットワークからのモニタおよびキャプチャを行うことができます。
- **ClearSight Server サービスをインストール**し、システム起動時に自動的に開始されるように設定します。ClearSight Server サービスは、エージェントビューアからの接続を待ちます。接続に成功すると、エージェントは、ネットワークのモニタおよび解析データを送り、エージェントビューアで表示を開始します。

図 4-1 に示されているように、ClearSight エージェントビューアは HTTP および Java RMI を使用して ClearSight Distributed エージェントと通信します。オプションで、SSL を介した HTTP および Java RMI を使用して、データの安全な転送を行うこともできます。

ClearSight Distributed の基本

ClearSight Distributed エージェントマネージャと、少なくとも 1 つの Distributed エージェントをインストールすると、次のことが可能です。

1. Distributed エージェントの [ユーザリスト] を設定する。[ユーザリスト] には、エージェントビューアからエージェントへの接続を許可されたすべてのユーザが含まれます。
2. ClearSight Distributed エージェントマネージャを起動し、エージェントをエージェントマネージャの [エージェントリスト] に追加する。
3. エージェントマネージャの **[エージェント]** タブからエージェントに接続する。
4. **[アラートマネージャ]** タブで、システム全体の問題レポートの設定と管理を行う。

これらの項目について、以下に説明します。

エージェントの [ユーザリスト] の設定

セキュリティ上の理由から、すべての ClearSight Distributed エージェントは、エージェントに接続可能なユーザのリストを保持します。エージェントビューアのユーザが、有効なユーザ名とパスワードなしにログインしようとすると、エージェントは接続を拒否します。

重要 : ClearSight Distributed エージェントは、次のデフォルトのユーザ名とパスワードでインストールされます。

ユーザ名 :	**Admin**
パスワード :	**< 空白 >(パスワードなし)**

エージェントの [ユーザリスト] の管理

次の手順で示すように、ユーザ設定ユーティリティを使用して ClearSight Distributed エージェントの [ユーザリスト] を管理します。

Distributed エージェントの [ユーザリスト] の設定手順

1. エージェントがインストールされているコンピュータで、**[スタート]** > **[すべてのプログラム]** > **[ClearSight Distributed]** > **[ユーザ設定]** を選択して、そのエージェントのユーザ設定ユーティリティを起動します。[ユーザ設定ログイン] ダイアログボックス (図 4-2) が表示されます。
2. デフォルトのユーザ名 **Admin** を入力して、**[OK]** をクリックします。

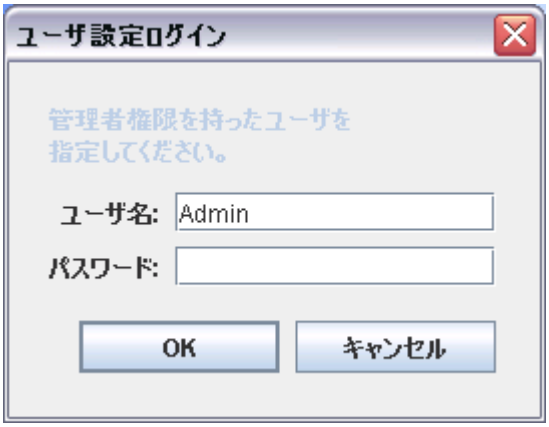


図 4-2: [ユーザ設定ログイン] ダイアログボックス

ClearSight ユーザ設定ユーティリティ (図 4-3) が表示されます。初期状態では、このウィンドウにはログインした管理者 (Admin) だけが表示されます。この管理者は、[ClearSight ユーザ設定] ダイアログボックス内の対応するボタンを使用して、このリストでユーザの追加、編集、または削除を行うことができます。

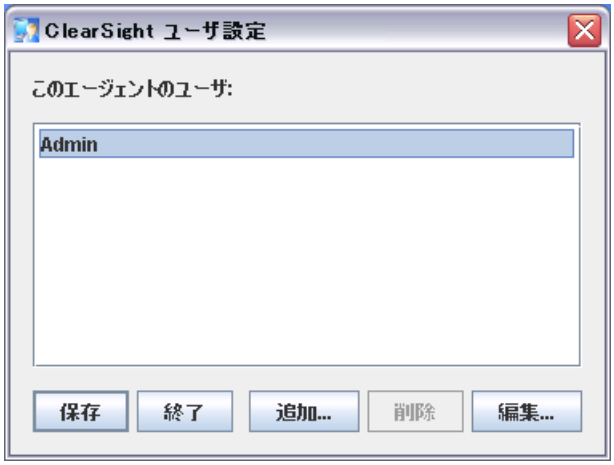


図 4-3: 初期状態のユーザ設定ユーティリティ

3. Admin 自体を削除することはできません。ユーザが Admin である場合は、新しいパスワードを設定することをお勧めします。新しいパスワードを設定するには、**[編集]** ボタンをクリックします。[ユーザの編集] ダイアログボックス (図 4-4) が表示されます。新しいパスワードを入力して (2 回)、**[OK]** をクリックします。新しいパスワードは直ちに有効になります。各エージェントに接続すると、[ClearSight ユーザ設定] ダイアログボックス (図 4-3) が表示されます。

   注記 : [権限] ボタンの機能については、のちほど説明します。

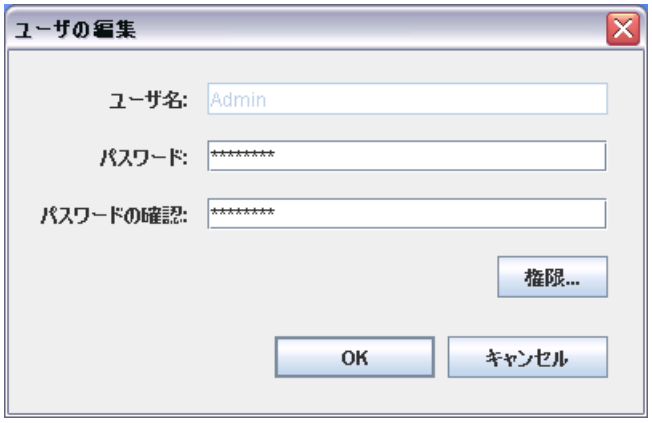


図 4-4: Admin の [ユーザの編集] ダイアログボックス

4. [ユーザリスト] に他のユーザを追加できます。その場合は、**[追加]** ボタンをクリックします。[ユーザの追加] ダイアログボックスが開き、新しいユーザのユーザ名とパスワードの入力 (2 回) を要求されます。たとえば、ユーザ David を追加すると、[ユーザの追加] ダイアログボックスは 図 4-5 のようになります。

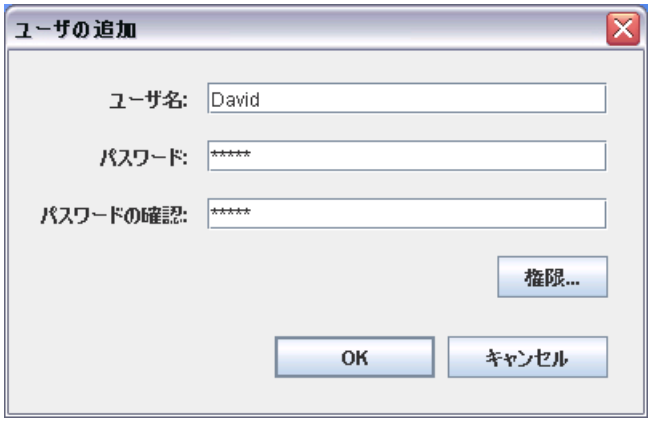


図 4-5: David の [ユーザの追加] ダイアログボックス

重要 : [ユーザリスト] に追加したユーザ名とパスワードを覚えておいてください。ClearSight Distributed エージェントマネージャで、エージェントを [エージェントリスト] に追加するときに、有効なユーザ名とパスワードを指定する必要があります。

5. 新しいユーザのユーザ名とパスワードを設定するほかに、そのユーザの「権限」を設定できます。**[権限]** ボタンをクリックします。[ユーザ権限 : David] ダイアログボックス (図 4-6) が表示されます。

   設定できる権限は、以下の 2 種類です。

   - **[管理者ユーザ権限]**。この権限では、ユーザは次のことを行うことができます。
     - 他のユーザの作成、編集、削除。
     - アダプタの切り替え、エージェントの再起動。
     - **[設定]** ページ上の設定の変更。
     - 自動モード以外のモードにする。

     注記 : Admin を削除したり、Admin の権限を無効にできるユーザはありません。ただし、**[管理者ユーザ権限]** が有効になっているユーザは、Admin のパスワードを変更できます。
   - **[アプリケーションコンテンツ閲覧権限]**。この権限では、ユーザはアプリケーションの内容 (VoIP 会話や電子メールなど) を表示できます。
   - **[キャプチャの開始 / 停止 / 表示]**。この権限では、ユーザはこのエージェント上でキャプチャの開始、停止、および表示を行うことができます。

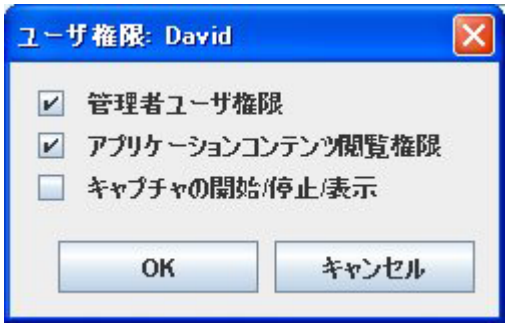


図 4-6: **[ユーザ権限 : David] ダイアログボックス**

6. このユーザに設定する権限を選択したら、**[OK]** をクリックします。[ユーザの追加] ダイアログボックスが再び表示されます。もう一度 **[OK]** をクリックします。[ClearSight ユーザ設定] ダイアログボックスに戻り、図 4-7 のように新しいユーザがリストに表示されます。

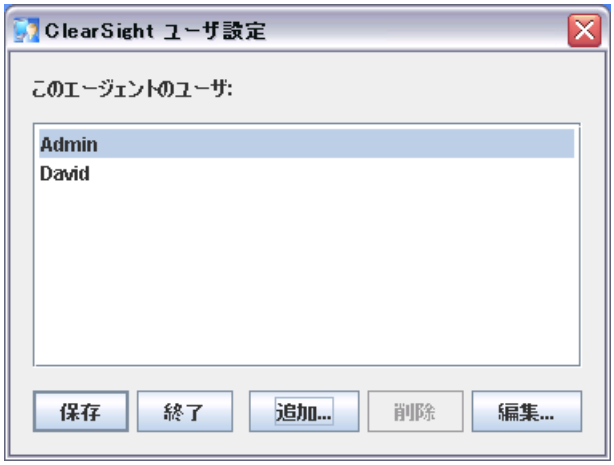


図 4-7: David が追加された [ユーザリスト]

7. ユーザをリストに追加したら、**[保存]** ボタンをクリックして変更を保存します。

   ほとんどの変更は、直ちに有効になります。ただし、現在ログイン中のユーザを削除した場合は、そのユーザは現在アクティブになっているセッションを終了します。

エージェントマネージャの使用

エージェントマネージャを「ホームベース」として使用すると、次のことが可能になります。

- **[エージェント]** タブで、ClearSight Distributed エージェントを管理する (93 ページ)。
- ClearSight Distributed エージェントに接続する (97 ページ)。
- **[アラートマネージャ]** タブで、ClearSight Distributed エージェントによって検出された問題を管理する (102 ページ)。
- あるエージェントの設定データを別のエージェント (複数可) にコピーする (105 ページ)。

[スタート]>[すべてのプログラム]>[ClearSight Distributed]>[ClearSight Distributed Agent Manager] を選択して、ClearSight Distributed エージェントマネージャを起動します。エージェントマネージャウィンドウ（図 4-8）が表示されます。

[エージェントリスト] には、エージェントマネージャに追加した各 Distributed エージェントが表示されます。各エージェントのリストには、**エージェント名**、**ステータス**、**キャプチャ**ステータス、検出された**問題**と**事象**、そのエージェントに接続するように設定されたユーザ、そのエージェントにインストールされているソフトウェアのバージョンが表示されます。

リスト内のエントリをダブルクリックするか、エージェントを選択して [接続] ボタンをクリックすると、エージェントに接続できます。接続に成功すると ClearSight ウィンドウが表示され、キーボードで操作しているかのように Distributed エージェントを使用できるようになります。



[アラートマネージャ] タブをクリックすると、Distributed エージェントからこのエージェントマネージャにレポートされた問題をまとめてログに表示できます。問題のレポートおよび管理を集中的に効率よく行うには、このエージェントマネージャに問題を送信するように各エージェントを設定する必要があります

図 4-8: エージェントモニタ

エージェントマネージャでの Distributed エージェントの管理

エージェントマネージャの **[エージェント]** タブ ([エージェントリスト] とも呼ぶ) で ClearSight Distributed エージェントを管理します。図 4-8 で示されているように、[エージェントリスト] には、エージェントマネージャに追加した ClearSight Distributed エージェントが表示されます。ここから、コマンドバーのボタンをクリックして、次の操作を行います。

- Distributed エージェントの**追加**、**編集**、および**削除**
- Distributed エージェントへの**接続**
- 1 つまたは複数のエージェントのエージェントサービスの**再起動**
- 1 つまたは複数のエージェントがインストールされているコンピュータの**アップデート**
- エージェントのソフトウェアの**アップデート**
- 1 つのエージェントでのキャプチャの開始および停止、または複数のエージェントでのキャプチャの同時**開始**および**停止**

これらの操作について、以下に説明します。

[エージェントリスト] へのエージェントの追加

エージェントマネージャの **[追加]** ボタンをクリックして、エージェントを [エージェントリスト] に追加します。[エージェントの追加] ダイアログボックス (図 4-9) が表示されます。

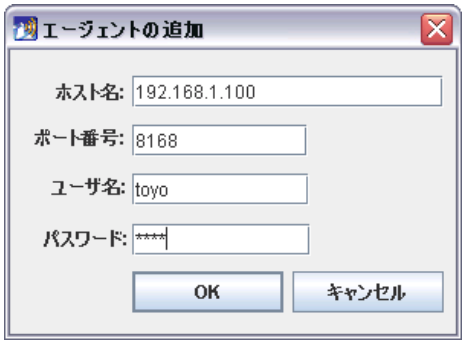


図 4-9: [エージェントの追加] ダイアログボックス

[エージェントの追加] ダイアログボックスのフィールドを次のように設定します。

[ホスト名] Distributed エージェントの解決可能なホスト名または IP アドレスのどちらかを入力します。

注記 : ClearSight Distributed エージェントマネージャは、ここで指定したホスト名または IP アドレスを使用してこの Distributed エージェントに接続します。2 枚のインターフェイスカード (エージェントビューアの通信用とネットワークのモニタおよび解析用) を備えた Distributed エージェントを追加する場合、エージェントビューアの通信に使用するカードのアドレスをここに入力します。この設定の詳細については、55 ページの「ClearSight Distributed エージェントの接続」を参照してください。

[ポート] Distributed エージェントの接続のデフォルトポートは 8168 です。通常は、テクニカルサポートに指示された場合を除いて、この設定を変更する必要はありません。

[ユーザ名] この Distributed エージェントへの接続に使用するユーザ名を入力します。

[パスワード] この Distributed エージェントへの接続に使用するパスワードを入力します。

重要 : ここで指定した **[ユーザ名]** と **[パスワード]** は、エージェントの [ユーザリスト] のユーザ名とパスワードと一致している必要があります。エージェントの [ユーザリスト] にユーザを追加する方法については、87 ページの「エージェントの [ユーザリスト] の設定」を参照してください。

[エージェントの追加] ダイアログボックスのフィールドに値を入力したら、**[OK]** をクリックして エージェントをリストに追加します。

エージェントを [エージェントリスト] に追加後に起こること

[エージェントの追加] ダイアログボックスで **[OK]** をクリックして、エージェントを [エージェントリスト] に追加すると、ClearSight Distributed エージェントマネージャは、ステータスを判定するためにそのエージェントに接続しようとします。この接続の試行は完全なものではありません。ただし、ClearSight Distributed エージェントマネージャによって次のことが確認されます。

- エージェントのマシンで ClearSight サービスが動作していること。
- ほかのユーザが、エージェントビューアからエージェントにログインしているかどうか。
- Distributed エージェント上の ClearSight ソフトウェアのバージョン。

この情報は、エージェントごとに [エージェントリスト] でレポートされます (図 4-8 と表 4-1 を参照)。

[エージェントリスト] のエージェントのフィールド

表 4-1 は、[エージェントリスト] で各エージェントについて表示されるフィールドの一覧と説明を示しています。

表 4-1: [エージェントリスト] のエージェントのフィールド

フィールド	説明
[エージェント名]	このエージェントのホスト名または IP アドレス。
[ステータス]	このエージェントの最新ステータス。以下の情報を含むさまざまなメッセージがレポートされます。 • このエージェントが起動、実行され、接続の準備ができているかどうか。 • ほかのユーザがエージェントに接続しているかどうかと、接続している場合はその接続のユーザ名。 • このエージェントが自動モードであるのかレディモードであるのか (キャプチャを開始するためにはこれらのモードであることが必要)。 • このエージェントに通信エラーが発生しているかどうか。

表 4-1: [エージェントリスト] のエージェントのフィールド

フィールド	説明
[キャプチャ]	このエージェントの現在のキャプチャステータス。値は、[開始中]、[開始]、[開始に失敗しました。]、[停止中]、[停止]、[停止に失敗しました。] のいずれかです。この列が空白の場合もあります (キャプチャが実行されておらず、エージェントがその他の手段で接続されていない場合)。
[問題]	このエージェントの現在の問題の数と、最大の問題重要度。このフィールドは問題の数のみでソートできます。最大重要度ではソートできません。
[事象]	このエージェントの現在の事象の数と、最大の事象重要度。このフィールドは事象の数のみでソートできます。最大重要度ではソートできません。
[ユーザ]	このエージェントの接続用に設定されたユーザ名。
[バージョン]	このエージェントにインストールされた ClearSight ソフトウェアのバージョン。

注記：エージェントマネージャは、ClearSight Distributed エージェントに加え、Network Time Machine（NTM）エージェントビューアウィンドウを介して NTM エージェントの接続と制御も実行できます。このような NTM エージェントが [エージェントリスト] に表示された場合、これらのエージェントは **[ステータス]** フィールドの「**(NTM)**」、**[バージョン]** フィールドの「**NTM**」によって識別できます。

[エージェントリスト] 上のエージェントの編集

[エージェントリスト] 上のエージェントの情報を編集するには、目的のエージェントを選択して、**[編集]** ボタンをクリックします。これにより、[エージェントの編集] ダイアログボックスが表示されます。このダイアログ ボックスは、タイトルバーに「エージェントの編集」と表示される以外は、[エージェントの追加] ダイアログボックス (図 4-9) とまったく同じです。必要な変更を行って、**[OK]** をクリックします。

[エージェントリスト] からのエージェントの削除

[エージェントリスト] から 1 つまたは複数のエージェントを削除するには、目的のエージェントを選択して、**[削除]** ボタンをクリックします。

[エージェントリスト] 上のエージェントへの接続

Distributed エージェントを [エージェントリスト] に接続したら、以下のいずれかの方法でそこに接続できます。

- [エージェントリスト] のエントリをダブルクリックする。
- リスト内のエージェントを選択して **[接続]** ボタンをクリックする。

どちらの場合も、ClearSight は [エージェントリスト] で指定した IP アドレスまたはホスト名に接続しようとします。接続に成功すると、[アダプタを開く] ダイアログボックス (図 4-10) が表示されます。

注記 : 接続しようとしている Distributed エージェントに、別のユーザがすでに接続している場合は、現在のセッションを引き継ぐかどうかを確認するメッセージが表示されます。**[はい]** をクリックすると、もう一方のユーザの接続は切断され、こちら側がエージェントを制御できるようになります。

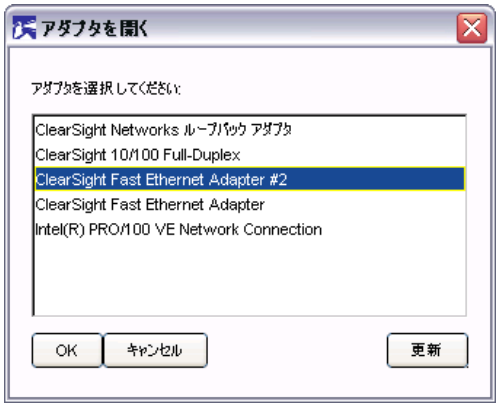


図 4-10: [アダプタを開く] ダイアログボックス

[アダプタを開く] ダイアログボックスでは、そのエージェントでモニタするアダプタを選択できます。ダイアログボックスには、ClearSight カーネルがバインドされたエージェントのネットワークインターフェイスカードがリストされています。デフォルトでは、エージェントソフトウェアがインストールされたときにエージェントの PC にインストールされたすべてのネットワークインターフェイスカードがここに含まれます。

ClearSight でモニタするアダプタを選択し、**[OK]** をクリックして続行します。ClearSight エージェントビューアウィンドウが表示され、スタンドアロンバー ジョンの場合と同様に、標準的な ClearSight Analyzer 機能を使用できるようになります。

接続したエージェントの切断

ClearSight エージェントビューアウィンドウを閉じるか、**[ファイル] > [終了]** コマンドと選択して、接続したエージェントを切断します。接続したエージェントを切断すると、図 4-11 に示すダイアログボックスが表示されます。

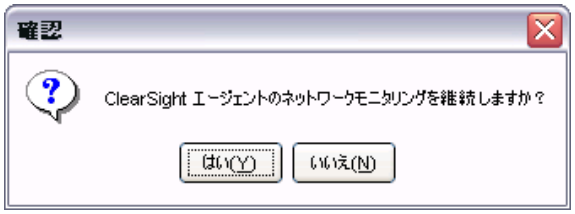


図 4-11: エージェントセッションの切断

このダイアログボックスでは、エージェントでネットワークのモニタを継続するよう選択できます。

- **[はい]** をクリックすると、ネットワークのモニタが継続され、カウンタと統計情報が更新されます。さらに、検出された問題が、エージェントで設定されているエージェントマネージャのアラートマネージャに通知されます。Distributed エージェントマネージャから再びエージェントに接続すると、ClearSight のディスプレイに表示された統計情報は、新しい接続の開始時からではなくモニタの最初からの情報が有効になっています。
- **[いいえ]** をクリックすると、エージェントはネットワークのモニタを停止し、Distributed エージェントマネージャから新しい接続が開始されるまで待機します。

[エージェントリスト] 上のエージェントの再起動

[エージェントリスト] のエントリを選択して、**[再起動]** ボタンをクリックすると、Distributed エージェントを再起動できます。

エージェント上のソフトウェアのアップデート

この機能によって、エージェントマネージャはエージェント上のソフトウェアをリモートで最新のバージョンにアップデートすることができます。

必要なファイルがあらかじめエージェントマネージャのコンピュータに存在している必要があります。リモートアップデートを開始するには、[エージェントリスト] で目的のエージェントを選択し、**[アップデート]** ボタンをクリックします。

注記 : エージェント上のソフトウェアのバージョンが、エージェントマネージャのコンピュータ上で使用可能な最新のバージョンより前のバージョンでないかぎり、**[アップデート]** ボタンはグレー表示されます (機能が使用不可になっている)。

キャプチャの開始と停止

[キャプチャ開始] ボタンおよび **[キャプチャ停止]** ボタンを使用して、1 つのエージェント上でキャプチャを開始および停止したり、複数のエージェント上でキャプチャを同時に開始および停止できます。

複数のエージェント上でキャプチャを開始または停止する場合は、Ctrl キーを押しながらクリックしてエージェントを選択します。

キャプチャを開始するように選択するエージェントは、自動モードまたはレディモードでなければなりません。モードは、エージェントマネージャの **[ステータス]** 列に表示されます。キャプチャを開始するには、ビューアに接続されているエージェントを事前に切断する必要があります。アクティブなビューアを自動モードにするには、ビューアウィンドウを閉じて、[確認] ダイアログ ボックス (98 ページの図 4-11) で [はい] をクリックします。エージェントは

前回の接続時に選択されていたネットワークアダプタを使用した自動モードになります。

注記 : 管理者ユーザ権限がないユーザが終了するときは自動モードになります。**[確認]** ダイアログボックスは表示されません。

エージェントが適切な状態 (自動モードまたはレディモード) で、設定されているユーザにキャプチャ権限がある場合 (90 ページの図 4-6 を参照)、**[キャプチャ開始]** ボタンを押すと、現在選択されているすべてのエージェントでキャプチャ処理が自動的に開始されます。

[キャプチャ] ステータス列の値は変化して、エージェントのキャプチャステータスを示します。この機能や他の方法を使用してキャプチャを開始すると、値は **[開始]** に切り替わります。

[キャプチャ停止] ボタンを使用すると、キャプチャが開始されていた 1 つまたは複数のエージェント上のキャプチャを停止することができます。この場合も、正常に停止するには、設定されているユーザにキャプチャ権限があり、エージェントのキャプチャステータスが **[開始]** である必要があります。

注記 : 次のような特殊な状況の場合エージェントはキャプチャを開始できません。

- エージェントの新規インストール後、まだエージェントビューアで接続していない場合。この場合、キャプチャに使用するネットワークアダプタが選択されていないためキャプチャが実行できません。
- エージェントビューアや別のエージェントマネージャによって既にキャプチャが実行されている場合、または自動モードでキャプチャが実行されている場合。
- エージェントが再起動中の場合。

エージェントのキャプチャバッファをトレースファイルに保存

キャプチャが正常に終了し、エージェントのキャプチャバッファに一つ以上のパケットが含まれている場合、**[キャプチャ]** ステータス列の表示は **[停止（バッファ保持）]** となり、**[キャプチャ転送]** ボタンが有効になります。**[キャプチャ転送]** ボタンをクリックすると、**[エージェントからのトレースファイルを保存]** ダイアログボックスが表示されます。(図 4-12).

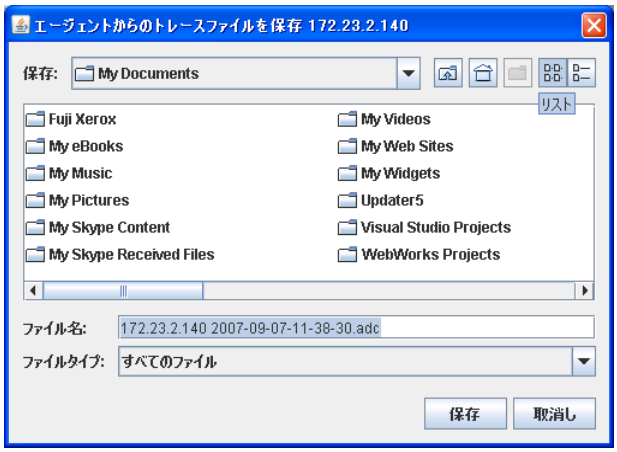


図 4-12: エージェントからのトレースファイルを保存ダイアログボックス

保存場所およびファイル名を指定して **[保存]** ボタンをクリックするとトレースファイルがエージェントから転送されて保存されます。転送の状態はエージェントマネージャの **[ステータス]** 列で確認することができます。

アラートマネージャの使用

エージェントマネージャの **[アラートマネージャ]** タブ (図 4-13) では、Distributed エージェントからレポートされた問題がまとめてログ表示されます。これらの問題は、Distributed エージェントで検出されたネットワークエラーです。

エージェントから アラートマネージャにレポートされた問題を集中的に効率よく管理するための主な設定の手順は、次のとおりです。

- 問題生成機能を有効にし、**[設定]** ボタン > **[設定]** タブ >**[問題]** > **[スレッショルド]** ページでエージェントでの問題のしきい値と重要度を設定する。問題のしきい値と重要度の設定については、第 10 章「アラートの操作」を参照してください。
- 各 Distributed エージェントの **[設定]** ボタン > **[設定]** タブ > **[問題]** > **[アラートマネージャ]** で、エージェントマネージャを問題レポートの送信先に指定する。エージェントマネージャを問題レポートの送信先に指定すると、エージェントで有効にされたすべての問題がそのエージェントマネージャにレポートされ、**[アラートマネージャ]** タブにリストされます。詳細については、104 ページの「問題をレポートするためのエージェントの設定」を参照してください。

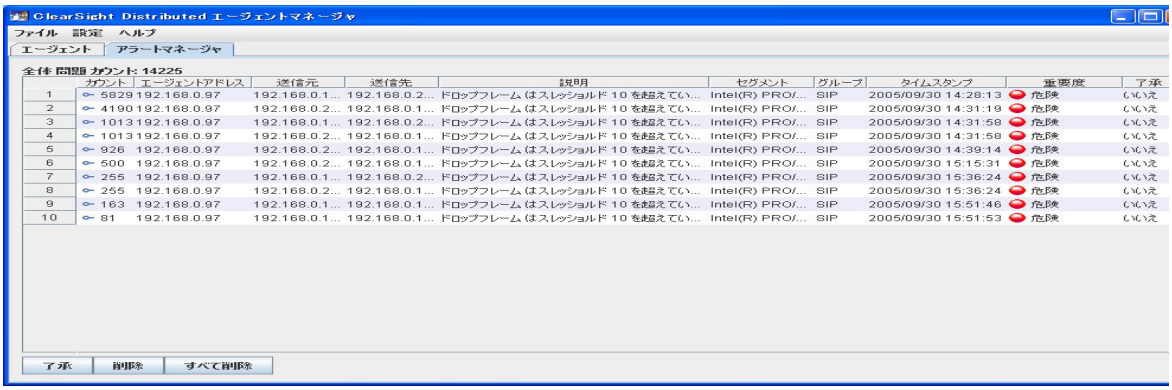


図 4-13: [アラートマネージャ] タブ

アラートマネージャのフィールド

[アラートマネージャ] タブでは、ClearSight Distributed エージェントによってレポートされた問題が次のフィールドにリスト表示されます。

[カウント]	グループ化された類似タイプの問題の数
[エージェントアドレス]	この問題をレポートする Distributed エージェントの IP アドレス。
[送信元]	この問題の送信元ステーションの IP アドレス
[送信先]	この問題の送信先ステーションの IP アドレス
[説明]	問題についての簡単な説明。
[セグメント]	問題が検出されたネットワークセグメント
[グループ]	問題のあるアプリケーション。
[タイムスタンプ]	問題が検出された時間。
[重要度]	問題の重要度を示す色付けされたアイコン。
[了承]	この問題が了承されているかどうか。すでに対処済みの問題を選択し、**[了承]** ボタンをクリックすると、その問題を了承できます。これにより、アラートマネージャをすばやくソートして、まだ対処していない問題のみを表示できます。

[アラートマネージャ] タブを統計のパラメータタイプごとにソートするには、対応する列見出しをクリックします。列見出しをもう一度クリックすると、逆順にソートされます。現在ソートされている統計の列見出しには、三角形のアイコンが表示されます。

問題を了承するには **[了承]** ボタンを使用し、問題を画面から削除するには **[削除]** ボタンを使用します。**[すべて削除]** ボタンをクリックすると、すべての問題が画面から削除されます。

[ファイル] メニューから **[名前をつけて問題を保存]** を選択して、[問題] リストを CSV ファイルに保存することができます。

問題をレポートするためのエージェントの設定

Distributed エージェントから問題をアラートマネージャに送信するように設定するには、**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[アラートマネージャ]** オプションをクリックします (図 4-14)。次に、以下の情報を指定します。

[送信先ホスト] このエージェントからの問題のレポート送信先となるホスト名または IP アドレス。ClearSight Distributed エージェントマネージャまたは標準 SNMP トラップサーバを指定します。

[コミュニティ] SNMP コミュニティ文字列 (SNMP トラップサーバに送信する場合)。

[セグメント] このエージェントからレポートされた問題についてアラートマネージャの [セグメント] フィールドに表示するネットワークセグメントの名前。このボックスを空白にすると、問題をレポートするアダプタカードの名前がエージェントから送信されます。

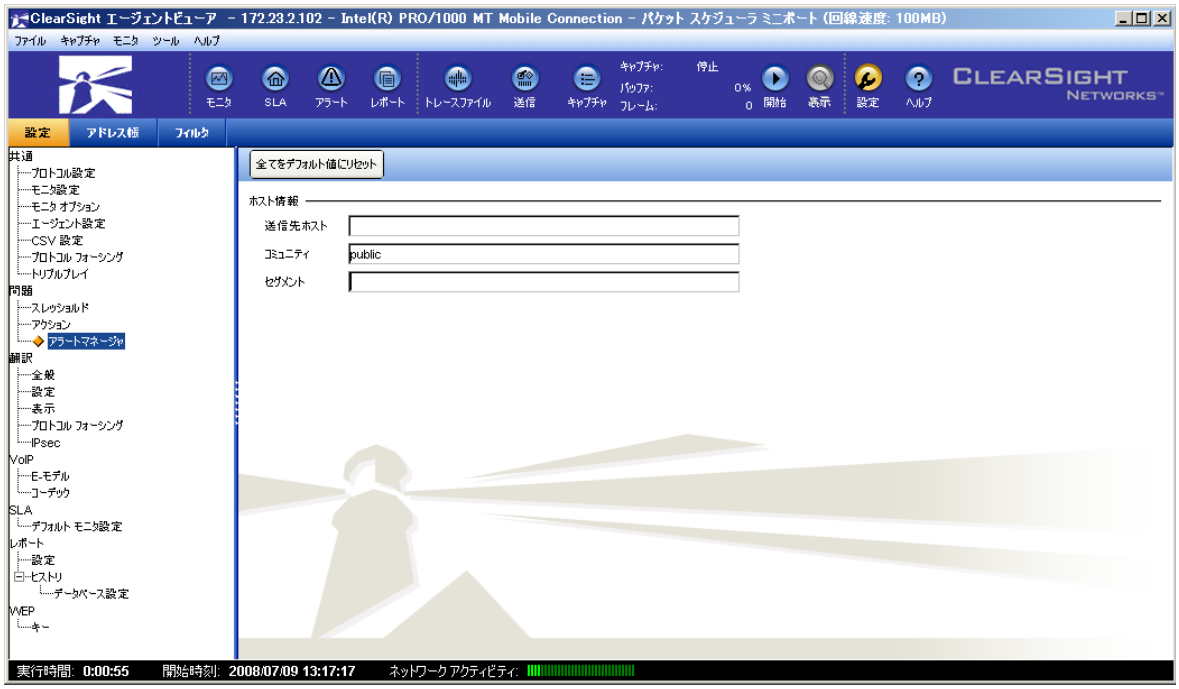


図 4-14: 問題をレポートするためのエージェントの設定

設定データのコピー

あるエージェントの設定データを別のエージェント (複数可) にコピーできます。設定データのコピーは、**[設定]** メニューのオプションを使用して行います (図 4-15)。

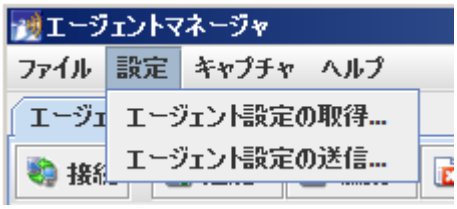


図 4-15: [設定] メニュー

[エージェント設定の取得]

このメニュー項目を使用すると、現在選択しているエージェントの設定をコンソール PC にアップロードできます。**[エージェント設定の取得]** を選択すると、[CFG の取得] ダイアログボックス (図 4-16) が表示されます。**[はい]** をクリックすると、選択したエージェントの設定がアップロードされます。設定のアップロード中に、選択したエージェントの **[ステータス]** 列に、該当するステータス情報が表示されます。



図 4-16: [CFG の取得] ダイアログボックス

[エージェント設定の送信]

このメニュー項目を使用すると、事前にアップロードしたエージェント設定を、1 つまたは複数の対象エージェントにダウンロードできます。このオプションを選択する前に、**[エージェント]** タブで対象エージェントを選択する必要があります。

[エージェント設定の送信] を選択すると、[CFG の送信] ダイアログボックス (図 4-17) が表示されます。**[はい]** をクリックすると、事前にアップロードした設定が、**[エージェント名]** タブで現在選択されているエージェントに送信されます。設定が各エージェントに送信されている間、エージェントの [ステータス] 列が更新され、進捗状況を示します。

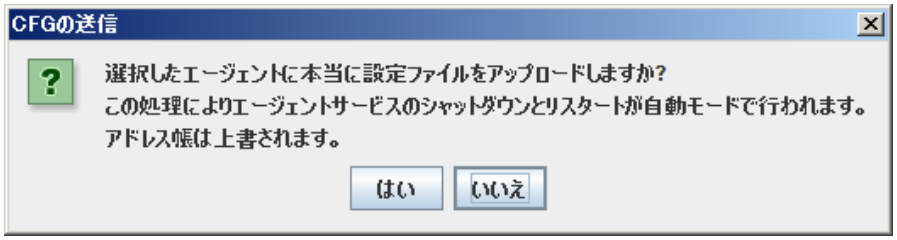


図 4-17: [CFG の送信] ダイアログボックス

設定のマージ

通常、対象エージェントに送信された設定ファイルは「そのまま」対象エージェントにコピーされ、既存の設定に取って代わります。ただし、ネットワークカード関連の特定の設定は、以下で説明する基準に従ってマージされます。

注記 : general.xml または interfaces.xml が存在するかどうかは、エージェントの履歴によって決まります。エージェントがインストール以降ずっと稼動している場合は、これらのファイルが存在します。

Interfaces.xml 内の設定の調整

送信先エージェントに **interfaces.xml** ファイルがない場合、新しい **interfaces.xml** ファイルがそのまま作成されます。送信先エージェントに既存の **interfaces.xml** ファイルがある場合は、マージ処理が実行されます。マージ処理によって、既存の **interfaces.xml** ファイルが変更されます。新しい **interfaces.xml** ファイル内のすべてのインターフェイスが、既存の **interfaces.xml** ファイルと比較してチェックされます。名前が一致する (大文字と小文字の区別なし) インターフェイスは、関連する設定とともに既存の **interfaces.xml** ファイルにコピーされ、そのアダプタの既存の設定に取って代わります。**general.xml** 内の選択したアダプタ設定から新しいインターフェイスがコピーされることはありません。

対象エージェントに **general.xml** がない場合は、選択したアダプタ設定を含め、新しい **general.xml** が「そのまま」対象にコピーされます。**general.xml** がある場合は、指定したアダプタが対象エージェントの **interfaces.xml** に存在する場合にのみ、選択したアダプタ設定がコピーされます。

その他の CSD 固有の機能

ClearSight Distributed (CSD) には、スタンドアロン ClearSight Analyzer (CSA) のすべての機能と、以下の CSD 固有の機能が備えられています。

- 「Secure Socket Layer (SSL) オプション」
- 「Windows セキュリティマネージャオプション」

Secure Socket Layer (SSL) オプション

この機能では、SSL を介した Java RMI を使用できるようになります。この機能を有効にするには、**[設定]** ボタン > **[設定]** タブ > **[共通]** > **[エージェント設定]** > **[コミュニケーション]** にある **[エージェントとビューア間のデータ通信に SSL を使用する]** チェックボックス (図 4-18) をオンにします。



図 4-18: エージェントとビューア間のデータ通信に SSL を使用する設定

Windows セキュリティマネージャオプション

CSD には、ClearSight のユーザセキュリティ実装の代わりに、Microsoft Windows セキュリティサーバを使用するオプションがあります。Windows セキュリティサーバを使用する場合は、以下の仕組みを使用してください。

- すべてのエージェントが同一の Windows ドメイン内に存在するようにします。
- 以下の 3 つのユーザグループを作成します。

  - グループ 1: ClearSightUsersGroup: このグループのユーザは ClearSight にログインできます。

  - グループ 2: ClearSightContentViewGroup: このグループのユーザは、アプリケーションの内容を表示できます。つまり、[ClearSight ユーザ設定] の **[アプリケーションコンテンツ閲覧権限]** と同等です (図 4-6 を参照)。

  - グループ 3: ClearSightCaptureGroup: このグループのユーザは、キャプチャの開始および停止、キャプチャしたトラフィックの表示を実行できます。つまり、**[キャプチャの開始 / 停止 / 表示]** 権限と同等です (図 4-6 を参照)。

  - グループ 4: ClearSightAdminGroup: このグループのユーザは、ソフトウェア更新を実行できます。
- ユーザに ClearSight へのログインを許可する場合は、そのユーザをグループ 1 に割り当てます。また、ユーザに与える許可に応じて、そのユーザを他のグループのいずれかまたは両方に割り当てます。

ClearSight のデフォルトのユーザセキュリティを Windows ユーザセキュリティに切り替える場合は、ClearSight Distributed のインストールディレクトリに移動して、Windows_ActiveUserSecurityManager.txt ファイルの名前を ActiveUserSecurityManager.txt に変更します。

Windows ユーザセキュリティを ClearSight のデフォルトのユーザセキュリティに戻す場合は、ActiveUserSecurityManager.txt の名前を Windows_ActiveUserSecurityManager.txt に戻します。

注記：このファイル名の変更手順は、マネージャの PC とエージェントの PC の両方で行う必要があります。これらのファイル名を変

更する前に必ずマネージャとエージェントの両方が停止していることを確認してください。

第 5 章

ClearSight を使用したネットワークのモニタ

この章では、ClearSight に備わっているリアルタイムネットワークモニタ機能について説明します。この章は、以下の項目で構成されています。

- 「リアルタイムモニタ画面の操作」
- 「アプリケーション層のモニタ」
- 「ネットワーク層のモニタ」
- 「物理層のモニタ」
- 「ClearSight Analyzer の設定」

リアルタイムモニタ画面の操作

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

ClearSight を起動すると、アプリケーションモニタの概要画面が表示され、ClearSight のすべての機能に簡単にアクセスできるようになります (図 5-1)。アプリケーションモニタの概要画面は、ClearSight を使用してネットワーク解析やトラブルシューティングを行う際のベースとなる重要な役割を果たします。ここには、ネットワークで実行されているアプリケーションの状態に関する情報がすぐに表示され、事象や問題が検出された場合はリアルタイムで警告が表示されます。この画面からは、複数の異なるアプリケーションフローに関する ClearSight の詳細表示や、ネットワーク接続とその基盤である物理層の統計にアクセスできます。

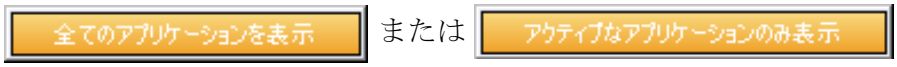


図 5-1: アプリケーションモニタ概要画面

※アプリケーションモニタは、ClearSight Analyzer Light には搭載されていない機能になります。

表示するアプリケーションの選択

[概要] タブに表示するアプリケーションを選択することができます。[概要] タブの任意の場所を右クリックすると、次のいずれかがポップアップボタンとして表示されます。



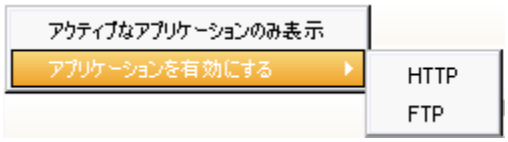
[全てのアプリケーションを表示] をクリックすると、モニタが可能なアプリケーションがすべて表示されます。[アクティブなアプリケーションのみ表示] をクリックすると、現在のセッション中にトラフィックが検出されたアプリケーションのみが表示されます。この 2 つの状態は、交互に切り替えることができます。

さらに、アプリケーションを個別に無効にすることもできます。たとえば、HTTPを停止する をクリックして、HTTP トラフィックのモニタを停止できます。[アクティブなアプリケーションのみ表示] を選択している場合は、単に [概要] タブから HTTP 行が消去されます。[全てのアプリケーションを表示] を選択している場合は、次のように HTTP アイコンが表示されます。



HTTP トラフィックのモニタを再開するには、HTTPを開始する をクリックします。

ただし、[アクティブなアプリケーションのみ表示] を選択している場合は、画面上に HTTP 行は表示されません。その場合は、[概要] タブの任意の場所を右クリックすると、[アプリケーションを有効にする] オプションが含まれたボタンが表示されます。以下はその例です。



[HTTP] をクリックして、HTTP トラフィックのモニタを再開します。

ClearSight ワークスペースの概要とナビゲーション

ClearSight のリアルタイムモニタワークスペースは、柔軟性に富み直感的にわかりやすい複数のペインで構成されています。116 ページの図 5-2 は、ClearSight の画面の例を示したものです。

※アプリケーションモニタは、ClearSight Analyzer Light には搭載されていない機能になります。

ClearSight のワークスペースは、以下のタイプのペインで構成されます。

- **層ペイン**は、画面の左側にあります。層ペインは、**[アプリケーション]**、**[ネットワーク]**、および **[物理層]** という 3 つの個別の層で構成されています。各層には、サーバー、フロー、ホスト、接続、問題、事象の数など、ClearSight が現在測定しているデータを示すカウンタがあります。

  層ペインで数値カウンタをクリックすると、そのカウンタに関する詳細な統計がメインペインに表示されます。

  注記 : ClearSight の 3 つのネットワーク層については、119 ページの「ClearSight のネットワークモデル」でさらに詳しく説明します。

- **メイン**ペインには、層ペインで現在選択されているカウンタに関する詳細情報が表示されます。メインペインで使用できる表示項目は、層ペインで何が選択されているかによって異なります。ただし、これらのペインの一般的な操作方法はどれも同じです。

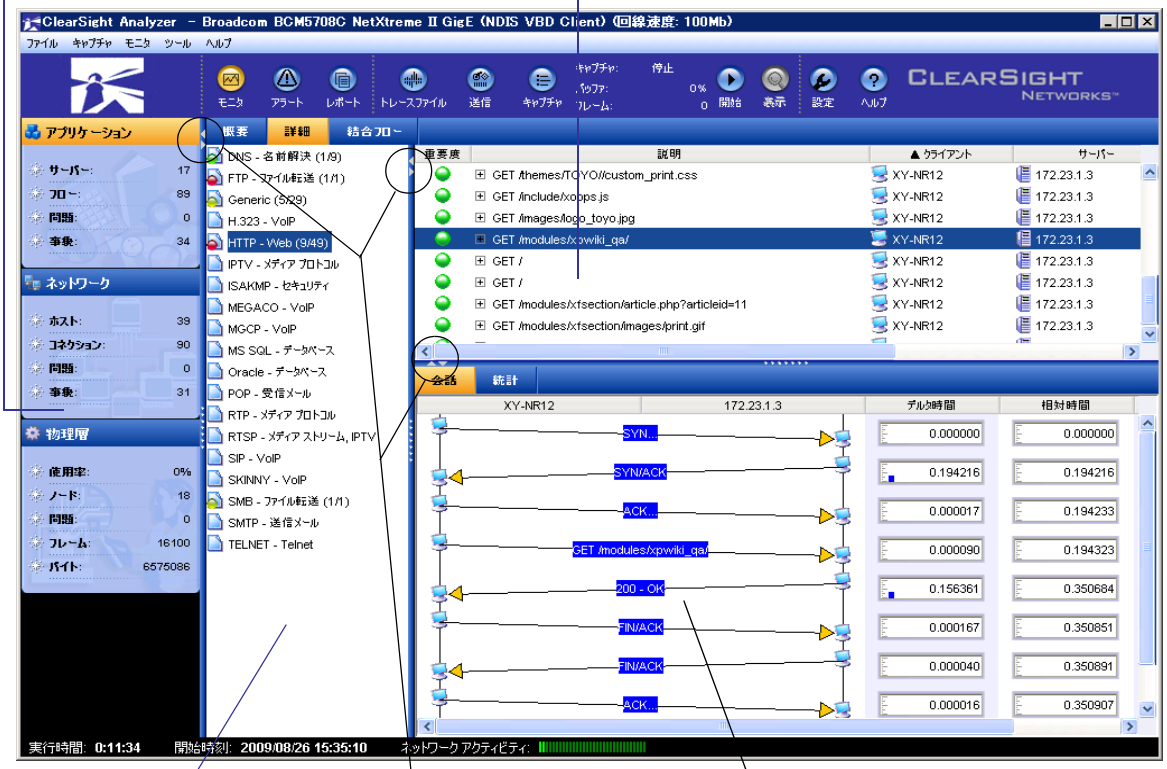
  - 多くの場合、メインペインは複数のサブペインに分割されています。この場合、1 つのペインでカウンタを選択すると、そのカウンタに関する詳細情報が近接した別のペインに表示されます。図 5-2 は、複数のサブペインに分割されたメインペインを示したものです。
  - 多くの場合、メインペインの表示画面にはタブが付いています。つまり、画面の上部にあるタブを使用して、表示するデータを選択することができます。たとえば、図 5-2 の [情報] ペインには、**[会話]** と **[統計]** という 2 つのタブが付いています。

- 通常、ClearSight の画面で、あるカウンタに関する詳細情報は、それをクリックすることにより参照できます。これは「ドリルダウン」と呼ばれます。通常の表示に戻るには、層ペインのカウンタを使用して、概要に戻ります。
- 層ペインで **[問題]** または **[事象]** のカウンタをクリックすると、選択した層に関する ClearSight の **[アラート]** 画面が表示されます。アラートについては、第 10 章「アラートの操作」で詳しく説明します。ツールバーで **[モニタ]** ボタンをクリックすると、モニタ画面に戻ることができます。

ClearSight のユーザインターフェイスを習得する最良の方法は、試してみることです。ClearSight がユーザのネットワークとそのデータについて学習するのと同様に、ユーザインターフェイスの各アイテムをクリックして、どのような統計が表示されるかを調べてください。

層ペインには、**[アプリケーション]**、**[ネットワー ク]**、および **[物理層]** という 3 つのネットワーク層で それぞれ ClearSight が現在測定しているデータが表示されます。層ペインでカウンタをクリックして、メインペインで表示する内容を選択します。

フローペイン。このペインのアイテムを選択すると、**[統計]** ペインがその下に表示され、関連した詳細情報で更新されるようになります。たとえば、問題のあるフローを**フロー**ペインで選択すると、その問題に関するエラーメッセージが **[統計]** ペインに色付けされて表示されます。



メインペインは、層ペインで選択されたカウンタに基づいて更新されます。

メインペインの表示は状況によって大きく異なりますが、通常、選択したエンティティに関するデータを表示するために連動する複数のペインを含みます。この例の**メイン**ペインは、アプリケーション、フロー、統計という 3 つのサブペインで構成されます。

統計ペインには、**フロー**ペインで選択されたカウンタに関する詳細が表示されます。このペインは、タブ付きであり、**[会話]** と **[統計]** の各タブが含まれます。ClearSight の画面の多くはタブ付きであり、選択したサーバー、フロー、接続、ノードなどに関する広範な統計を表示できるようになっています。

これらのトグルを使用して、必要のないペインを非表示にすることができます。

図 5-2: リアルタイムモニタの一般的なペイン

ClearSight 画面における色の使用について

ClearSight の画面では、ClearSight Analyzer によって検出された問題を色を使用してわかりやすく表示します。次のように、それぞれの色が意味する内容は、その色から連想しやすいものに設定されています。

- 赤いボタンは、迅速な処置を必要とする問題を意味します。
- オレンジのボタンは、場合によって注意を喚起する必要がある問題を意味します。
- 黄色のボタンは、軽度なエラーを意味します。
- 緑のボタンは、機能が健全であることを意味します。

  注記：ClearSight に赤いボタンが表示されたら、ボタンをクリックして、問題について調べる必要があります。

アラートレベルの色付け

アラートログでは、色とアラートレベルがそれぞれ次のように対応しています。

- **危険** - 赤
- **注意** - オレンジ
- **やや注意** - オレンジ
- **警告** - 黄
- **情報** - 緑

第 10 章「アラートの操作」では、アラートレベルをアラームに割り当てる方法と、特定のアラートレベルにアクションを関連付ける方法について説明します。

ClearSight の用語

ClearSight Analyzer ソフトウェアを起動すると、ネットワーク上のさまざまなアプリケーション層フローの検出と測定がすぐに開始されます。また、ClearSight では、リアルタイムの解析によって、問題や事象に関するアラートが表示されます。これらの用語は、以下のように定義されます。

- **フロー** - フローは、特定のアプリケーション層の機能を実行するパケットのグループを指します。この機能の例としては、Web サーバーでの **Get** や **Post**、電子メールメッセージの送受信、ドメイン名の解決、電話の発信などがあります。フローは、トランザクションの性質に応じて、わずか 5 のパケットで構成される場合も、200 ものパケットで構成される場合もあります。
- **事象** - 事象は、ネットワークで検出された軽度なエラー状態を指します。事象が一度だけ発生している場合は、必ずしも調査する必要はありません。ただし、繰り返し発生している事象については、詳しく調査する必要があります。また、事象は、同じサーバー、フロー、接続、ノードなどに関して ClearSight によって検出された**問題**をトラブルシューティングする際に役に立つ場合があります。

  事象の典型的な例としては、HTTP クライアントが受け取る「**404 - Not Found**」エラーなどの、単純なものがあります。
- **問題** - 問題は、緊急に調査するに値する深刻なエラーを指します。ネットワークの問題の例としては、IP アドレスが重複している場合など、ネットワークのパフォーマンスを劣化させたり、予測不可能な状態にしたりするものなどがあります。

ClearSight のネットワークモデル

ClearSight のリアルタイムモニタ表示画面では、層ごとのネットワークの動きを測定します。ClearSight では、OSI 7 層モデルを調整したネットワーク 3 層モデルが使用されます。この 3 層とは、アプリケーション層、ネットワーク層、および物理層です。

- **アプリケーション**層では、電子メール、データベース、VoIP、メディア、ファイル転送など、一般的なネットワークアプリケーションのエンドツーエンドのパフォーマンスを測定します。ClearSight は、アプリケーションごとにクライアントとサーバー間の各フローを検出して一覧表示し、アプリケーションのパフォーマンスをモニタして詳細統計を提供します。

  アプリケーション層のモニタについては、121 ページの「アプリケーション層のモニタ」で詳しく説明します。

  ※アプリケーション層は、ClearSight Analyzer Light では表示されません。

- **ネットワーク**層では、アプリケーション層に表示されるアプリケーションフローの基盤となる、OSI の第 3 層と第 4 層のホストとコネクションを測定します。また、TCP/IP 通信の測定も行います。これには UDP、ARP、ICMP などの関連プロトコルなども含まれます。

  ネットワーク層のモニタについては、170 ページの「ネットワーク層のモニタ」で詳しく説明します。

- **物理**層では、フレームタイプやエラータイプ (ブロードキャスト、マルチキャスト、CRC エラーなど) の数など、ネットワークデータの実際の転送状況について説明した統計が表示されます。また、物理層では VLAN の測定も行います。

  物理層のモニタについては、183 ページの「物理層のモニタ」で詳しく説明します。

ClearSight のモデルと OSI モデル

ユーザにとっては、アプリケーションのパフォーマンスやアプリケーションの基盤となるコネクションのパフォーマンスが最も重要な情報であることが多いため、ClearSight の 3 層ネットワークモデルでは、ネットワーク解析が簡略化されています。たとえば、プレゼンテーション層とセッション層のサービスの区別は、実世界のネットワーク解析において必ずしも重要ではありません。表 5-1 は、OSI モデルの 7 層が ClearSight の 3 層にどのように分類されているかを示したものです。

表 5-1: OSI 7 階層の ClearSight 層に対するマッピング

OSI 7 階層	ClearSight 層
アプリケーション	アプリケーション
プレゼンテーション	
セッション	
トランスポート	ネットワーク
ネットワーク	
データリンク	物理層
物理	

アプリケーション層のモニタ

ClearSight Application Flow Analyzer ClearSignt Distributed

この項では、ClearSight のアプリケーションモニタ機能を使用する方法について説明します。以下は、この項の主なトピックです。

- アプリケーションモニタに関する広範な説明 (下記の「アプリケーションモニタについて」)。
- ClearSight のアプリケーションモニタ詳細画面にアクセスする方法 (122 ページの「アプリケーションモニタ詳細画面の表示」)。
- ClearSight のアプリケーションモニタ詳細画面を操作する方法 (122 ページの「アプリケーションモニタ詳細画面の操作」)。
- サポートされる各アプリケーションタイプに関して詳細画面に表示される情報 (133 ページの「アプリケーションモニタ詳細画面」)。

アプリケーションモニタについて

ClearSight では、Oracle や MS SQL などのデータベースアプリケーション、POP や SMTP などの電子メールアプリケーション、H.323 や Skinny などの VoIP アプリケーションなど、多数の重要なネットワークアプリケーションがリアルタイムで詳細に解析されます。サポートされるアプリケーションタイプごとに、サーバーとフローが検出され、ネットワークで問題が発生した場合にトラブルシューティングに利用できるリアルタイム解析と統計が提供されます。情報は、特定のサーバーや特定のフローに関して表示することも、アプリケーションタイプ全体に関して表示することもできます。

ClearSight は、ネットワークラダー表示を使用し、関連したデルタ時間と相対時間を織り込んで、検出したフローごとにクライアントとサーバー間の対話とトランザクションを再構築し、表示します。一部のアプリケーションフロー (HTTP、電子メール、FTP など) では、エンドユーザに対して表示されるコンテンツフローも再構築されます。これにより、アプリケーションへの無許可アクセス、異常なデータパターン、アプリケーションレベルのエラーなどを検出できるようになります。

アプリケーションモニタ詳細画面の表示

ClearSight では、アプリケーションモニタの概要で、サポートされる各アプリケーションタイプの**サーバー**、**フロー**、**問題**、**事象**、および**スループット**を測定します (112 ページの図 5-1)。アプリケーションモニタの概要からは、各アプリケーション、サーバー、およびフローのアプリケーションモニタ詳細画面にアクセスできます。

アプリケーションモニタ詳細画面は、次の方法で表示できます。

- 層ペインの [アプリケーション] 層で **[サーバー]** または **[フロー]** のカウンタをクリックします。
- アプリケーションモニタ概要で **[アプリケーション]**、**[サーバー]**、または **[フロー]** の列をクリックします。

123 ページの図 5-3 は、アプリケーションモニタ詳細画面の例を示したものです。

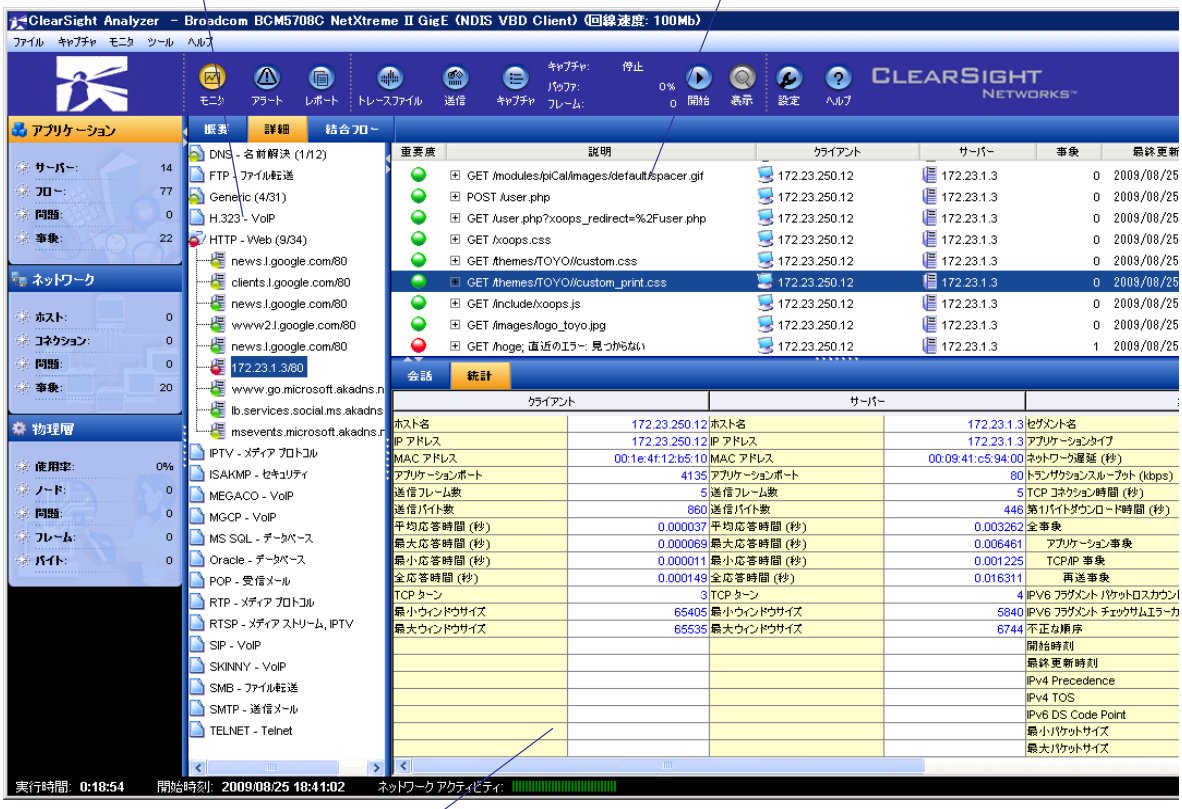
アプリケーションモニタ詳細画面の操作

図 5-3 に示すとおり、アプリケーションモニタ詳細画面は、以下のペインで構成されています。

- **アプリケーション**ペインには、サポートされる各アプリケーションタイプが一覧表示されます。各アプリケーションカウンタを段階的に開くと、対応するアプリケーションタイプに関して ClearSight が検出したサーバーを表示します。個々のサーバーまたはアプリケーションタイプ全体を選択して、対応する統計を**フロー**と**統計**の各ペインで表示することができます。
- **フロー**ペインには、アプリケーションペインで選択したアプリケーションタイプまたはサーバーに関して検出されたフローが表示されます。アプリケーションタイプが選択された場合、フローペインには、そのタイプに関して検出されたすべてのフローが表示されます。同様に、個々のサーバーが選択された場合は、フローペインにはそのサーバーに関するフローだけが表示されます。
- **統計**ペインには、アプリケーションペインまたはフローペインで選択したアプリケーション、サーバー、またはフローに関する詳細情報が表示されます。統計ペインに表示する内容は、ほかの 2 つのペインでどのカウンタを選択するかによって変わります。

アプリケーションペイン
アプリケーションペインには、サポートされる各アプリケーションタイプが一覧表示されます。アイコンにボタンが付いているカウンタは、段階的に開くことにより、検出されたサーバーを表示することができます。括弧内の数値は、検出されたサーバー / フローの数を表します。ボタンの色は、対応するアプリケーションタイプのサーバーで検出されたアラートの最高レベルを示します。

フローペイン
フローペインには、アプリケーションペインで選択したサーバーまたはアプリケーションタイプに関して検出されたフローが表示されます。この場合、アプリケーションペインで FTP の親カウンタが選択されているため、フローペインには検出されたすべての FTP フローが表示されています。



統計ペイン
統計ペインには、アプリケーションペインで選択したアプリケーションタイプまたはサーバー、あるいはフローペインで選択したフローに関する詳細な統計が表示されます。

図 5-3: アプリケーションモニタ詳細画面

アプリケーションペイン

アプリケーションペインには、サポートされる各アプリケーションタイプが一覧表示されます。[詳細] タブでのアプリケーションのカウンタの横には、対応するアプリケーションタイプのサーバーが検出されたことを示す特徴的なボタンが表示されます。カウンタの隣の括弧内の数値は、ClearSight によって検出されたサーバーとフローの数を示します。アイコンの色は、対応するタイプのサーバーで検出されたアラートの最高レベルを示します。

たとえば、

のようなカウンタは、ClearSight によって 3 つの HTTP サーバーと 4 つの HTTP フローが検出され、少なくともサーバーの 1 つが赤レベルのアラートを示していることを意味します。アプリケーションカウンタをダブルクリックして段階的に開くと、検出されたサーバーを表示することができます。

アプリケーションペインでアプリケーションまたはサーバーのカウンタを選択し、フローペインと統計ペインの表示内容を決定します。

- アプリケーション全体のフローと統計を表示するには、アプリケーションカウンタを選択します。たとえば、HTTP を選択すると、ClearSight によって検出されたすべての HTTP フローを表示できます。
- 特定のアプリケーションサーバーのフローと統計を表示するには、サーバーカウンタを選択します。たとえば、HTTP サーバーカウンタを選択すると、そのサーバーの HTTP フローだけを表示できます。

アプリケーションペインの自動キャプチャフィルタ

アプリケーションペインの任意のカウンタを右クリックすると、自動キャプチャフィルタを使用して、選択したアプリケーションタイプまたはサーバーでキャプチャを開始できます。たとえば、**[H.323]** というカウンタを右クリックすると、**[H.323 をキャプチャする]** オプションを含むコンテキストメニューが表示されます。このオプションを選択すると、H.323 以外のすべてのトラフィックを除外するキャプチャが開始されます。同様に、サーバーカウンタを右クリックして、そのサーバーに対してのみキャプチャを開始することもできます。

フローペイン

フローペインには、アプリケーションペインで選択したアプリケーションまたはサーバーに関して、検出されたフローが表示されます。アプリケーションペインでアプリケーションタイプ (FTP など) を選択した場合、フローペインにはそのアプリケーションタイプに関して検出されたすべてのフローが表示されます。同様に、個々のサーバーが選択された場合は、フローペインにはそのサーバーに関するフローだけが表示されます。図 5-4 は、FTP に関するフローペインの例を示したものです。

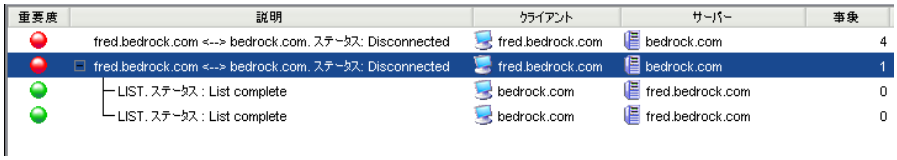


図 5-4: フローペインの例

図 5-4 に示すとおり、フローペインには、検出された各フローが以下の統計とともに表示されます。

[重要度] このフローに関して検出されたアラートの最高レベルを示すアイコン。赤 (最も重大) ～ 緑 (健全) があります。ClearSight における色の使用法について詳しくは、117 ページの「ClearSight 画面における色の使用について」を参照してください。

[説明]	このフローによって実行されるトランザクションのタイプ。たとえば、HTTP サーバーでは **Get**、POP サーバーでは電子メール、VoIP サーバーではコール設定などになります。 一部のトランザクションでは、そのエントリの横にスイッチ型のアイコン ⊞ が表示されます。このアイコンが付いたエントリをクリックし、エントリを段階的に開くと、このフローの一部として含まれる実際のコマンドを表示することができます。たとえば、図 5-4 では、FTP フローが段階的に開かれ、2 つの **LIST** コマンドが表示されています。フローエントリの下のコマンドを選択すると、ClearSight によって実際のコマンドが統計ウィンドウに再構築され、エンドユーザによって実行された電子メール、FTP トランザクション、Telnet セッション、データベース要求、VoIP コールを確認できるようになります。
[クライアント]	このフローのクライアント側のアドレス。
[サーバー]	このフローのサーバー側のアドレス。

注記 : [クライアント] と **[サーバー]** の各フィールドでのアドレス表示方法は、エントリを右クリックすることによりアクセスできるコンテキストメニューを使用して変更できます。これを行う方法については、下記の「フローペインにおけるアドレス表示の切り替え」を参照してください。

[事象]	このフローに関連した事象の数。
[最終更新時間]	ClearSight が前回このフローを新しい統計で更新した時刻。

フローペインの並べ替え

各統計タイプに対応する列見出しをクリックすると、そのタイプを基準にフローペインを並べ替えることができます。もう一度クリックすると、並べ替えの順序を逆にすることができます。統計の列見出しに三角形のアイコンが表示されている場合、ペインが現在その統計を基準にして並べ替えられていることを意味します。

フローペインにおけるアドレス表示の切り替え

[クライアント] と **[サーバー]** の各フィールドでアドレスを表示する方法を変更するには、**[説明]** 列を右クリックします。表示されたコンテキストメニューを使用すると、アドレス表示を IP アドレス、IP ホスト名、または MAC アドレスに変更することができます。

フローペインの自動キャプチャフィルタ

フローペインで任意のカウンタの **[説明]** 列を右クリックすると、自動キャプチャフィルタを使用して、選択したフローの IP アドレスとポート番号に対してキャプチャを開始できます。たとえば、FTP フローを右クリックすると、「**192.168.1.100/3451 <-> 192.168.1.133/21 をキャプチャする**」などのオプションが生成されます。このオプションを選択すると、対応するポートでこれらの 2 つの IP アドレス間のすべてのトラフィックのキャプチャが開始されます。

統計ペイン

表 5-2 で説明するように、**統計**ペインに表示される情報は、アプリケーションペインまたはフローペインで何を選択するかによって決まります。

表 5-2: 統計ペインのタブ

選択する項目	統計ペインに表示される内容
アプリケーションペインの親アプリケーションタイプ	**[概要]**、**[事象]**、**[問題]** の各タブにアプリケーション全体の統計が表示されます。また、一部のアプリケーションでは、アプリケーション特有のタブが含まれる場合があります (たとえば、**[DNS]** を選択すると、**[名前解決]** タブが表示されます)。
アプリケーションペインのサーバー	**[概要]**、**[事象]**、**[問題]** の各タブに選択したサーバーだけに関する統計が表示されます。
フローペインのフロー	**[会話]** と **[統計]** の各タブに選択したフローだけに関する統計が表示されます。

注記 : また、フローペインで ⊞ アイコンをクリックすると、フローの個々のコマンドを表示することができます (HTTP サーバーの **Get** など)。フローペインで個々のコマンドを選択すると、統計ペインにオプションが表示され、トランザクションを再構成できるようになります。これらのタイプの画面は、アプリケーションタイプによって異なります。これについては、後述のアプリケーションごとの項で詳しく説明します。

[概要] タブに関する情報

[概要] タブには、選択したアプリケーションタイプまたはサーバーからのトラフィックに関する統計値や計測値が表形式で表示されます。ClearSight には、トラフィック全体用のカウンタ (フレーム数、バイト数、エラー数など) のほか、特定のアプリケーションに関するフレームタイプカウンタも備わっています。たとえば、HTTP に関する **[概要]** タブには、**[ヒット]**、**[ページ数]**、**[ページが見つからない]** などのエラーのカウンタが含まれます。どのフレームタイ

プカウンタが表示されるかは、選択したアプリケーションタイプによって決まります。

[事象] タブに関する情報

[事象] タブには、選択したアプリケーションまたはサーバーに関して検出された事象が一覧表示されます。事象は、以下の統計とともに表示されます。

[カウント]	グループ化された類似タイプの事象の数
[送信元]	この事象の送信元ステーションの IP アドレス。
[送信先]	この事象の送信先ステーションの IP アドレス。
[説明]	この事象の簡単な説明。
[タイムスタンプ]	事象が検出された時刻。
[重要度]	事象の重要度を示す色付きアイコン。

各統計タイプに対応する列見出しをクリックすると、そのタイプを基準に **[事象]** タブを並べ替えることができます。もう一度クリックすると、並べ替えの順序を逆にすることができます。統計の列見出しに三角形のアイコンが表示されている場合、ペインが現在その統計を基準にして並べ替えられていることを意味します。

[問題] タブに関する情報

[問題] タブには、選択したアプリケーションまたはサーバーに関して検出されたすべての問題が一覧表示されます。問題は、以下の統計とともに表示されます。

[カウント]	グループ化された類似タイプの問題の数
[送信元]	この問題の送信元ステーションの IP アドレス。
[送信先]	この問題の送信先ステーションの IP アドレス。
[説明]	この問題の簡単な説明。
[セグメント]	問題のあるアプリケーションタイプ。
[タイムスタンプ]	問題が検出された時刻。
[重要度]	問題の重要度を示す色付きアイコン。

各統計タイプに対応する列見出しをクリックすると、そのタイプを基準に **[問題]** タブを並べ替えることができます。もう一度クリックすると、並べ替えの順序を逆にすることができます。統計の列見出しに三角形のアイコンが表示されている場合、ペインが現在その統計を基準にして並べ替えられていることを意味します。

[会話] タブに関する情報

[会話] タブには、フローペインで選択されたフローを構成するクライアントとサーバー間におけるデータ交換が表示されます。**[会話]** タブでは、この情報を標準のラダー図で表示されるため、会話を、その発生した順序で測定することが可能です (図 5-5)。クライアントとサーバーはそれぞれラダーの端に表示され、それぞれのアドレスまたはホスト名はペインのタイトルバーに表示されます。矢印は、フローにおけるメッセージの方向を示します。

また、会話のタイミングも次のように表示されます。

[デルタ時間] 表示されているフレームとその前のフレームの間の時間。異常な値は、色付けされた垂直バーでハイライト表示されます。

[相対時間] 表示されているフレームとフローの最初のフレームの間の時間。

[長さ] フレームの長さをバイト単位で表したもの。色付けされた垂直バーが、視覚的にフレームの長さを表示します。

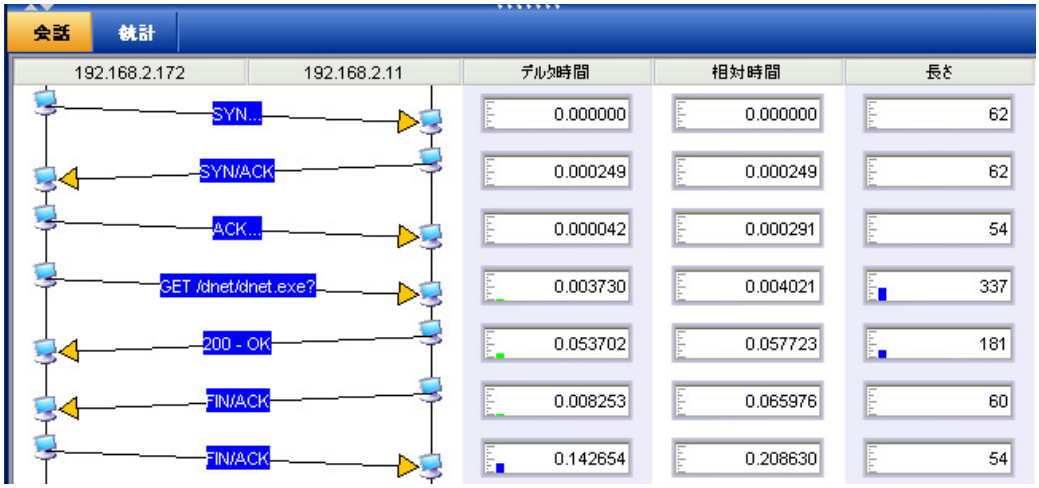


図 5-5: [会話] タブの例 (HTTP フロー)

また、ClearSight では、問題のあるメッセージをすばやく特定できるように、**[会話]** タブのデータ交換が色付けされています。たとえば、図 5-5 では、HTTP フローの **GET 要求**の再送が黄色で表示されています。これより重要度が高いエラー (HTTP フローの「404 - Object not Found」エラーなど) は赤で表示され、エラー以外のメッセージは青で表示されます。

注記 : プルダウンメニューで **[ファイル]** > **[印刷]** と選択して、会話 (ラダー図) を印刷できます。

注記 : 会話は pdf ファイルに保存できます。その場合は、ラダー図上の任意の場所を右クリックします。**[エクスポート]** ボタンが表示されます。**[エクスポート]** ボタンをクリックすると **[エクスポート]** ダイアログボックスが表示されます。このダイアログボックスでファイルの保存先を指定できます。

[統計] タブに関する情報

[統計] タブには、フローペインで選択したフローのトラフィックに関する統計値や計測値が表形式で表示されます。ClearSight には、サーバー側とクライアント側の両方におけるトラフィック全体用のカウンタ (フレーム数、バイト数、エラー数など) のほか、フローの応答時間を測定した統計や特定のアプリケーションに関するフレームタイプカウンタも備わっています。たとえば、FTP に関する **[統計]** タブには、**[ダウンロードファイル数]** と **[直近にダウンロードしたファイル名]** のカウンタが含まれます。どのフレームタイプを使用できるかは、選択したアプリケーションタイプによって決まります。

[レポート] タブに関する情報

[レポート] タブ (VoIP フローのみで使用可能) には、選択したフローの QoS (Quality of Service) レポートが表示されます。詳細については、155 ページの「VoIP QoS レポートの表示」を参照してください。

アプリケーションモニタ詳細画面

この項では、ClearSight がサポートする各アプリケーションタイプの詳細画面について説明します。

- Citrix 詳細画面 (134 ページ)
- DNS 詳細画面 (135 ページ)
- FTP 詳細画面 (136 ページ)
- Telnet 詳細画面 (138 ページ)
- HTTP 詳細画面 (140 ページ)
- POP 詳細画面 (142 ページ)
- SMTP 詳細画面 (144 ページ)
- MS SQL 詳細画面 (146 ページ)
- Oracle 詳細画面 (149 ページ)
- Exchange 詳細画面 (151 ページ)
- MSN 詳細画面 (153 ページ)
- H.323 詳細画面 (154 ページ)
- SIP 詳細画面 (154 ページ)
- Skinny 詳細画面 (154 ページ)
- MGCP 詳細画面 (154 ページ)
- Megaco 詳細画面 (154 ページ)
- RTP 詳細画面 (161 ページ)
- RTSP 詳細画面 (163 ページ)
- IPTV 詳細画面（164 ページ）
- Kerberos 詳細画面 (166 ページ)
- ISAKMP 詳細画面 (167 ページ)
- SMB 詳細画面 (168 ページ)
- Generic 詳細画面 (169 ページ)

Citrix 詳細画面



ClearSight は、ユーザ (Citrix クライアント) と リモートコンピュータ (Citrix サーバー) 間のリモートアクセスセッションのフローを作成して、Citrix のトラフィックをリアルタイムでモニタします。クライアントは、Citrix セッションを使用すると、リモートのマシンが直接接続されているかのように操作することができます。クライアントのコンピュータで入力されたキー操作とマウス操作がリモートマシンに渡され、リモートマシンの画面表示がクライアントの画面にも表示されます。

注記 : Citrix 情報を正しく表示するには、ClearSight 翻訳エンジンを使用する必要があります。ClearSight 翻訳エンジンを選択するには、**[設定]** ボタン > **[設定]** タブ > **[翻訳]** > **[全般]** > **[翻訳エンジン]** 項目に移動し、**[ClearSight]** ラジオボタンを選択します。

ClearSight は、Citrix セッションをラダー表示し、各対話は送信したとおりに表示されます。Citrix セッションをラダー表示するには、フローペインで Citrix フローを選択します。

図 5-6 は、典型的な Citrix 詳細画面を示しています。

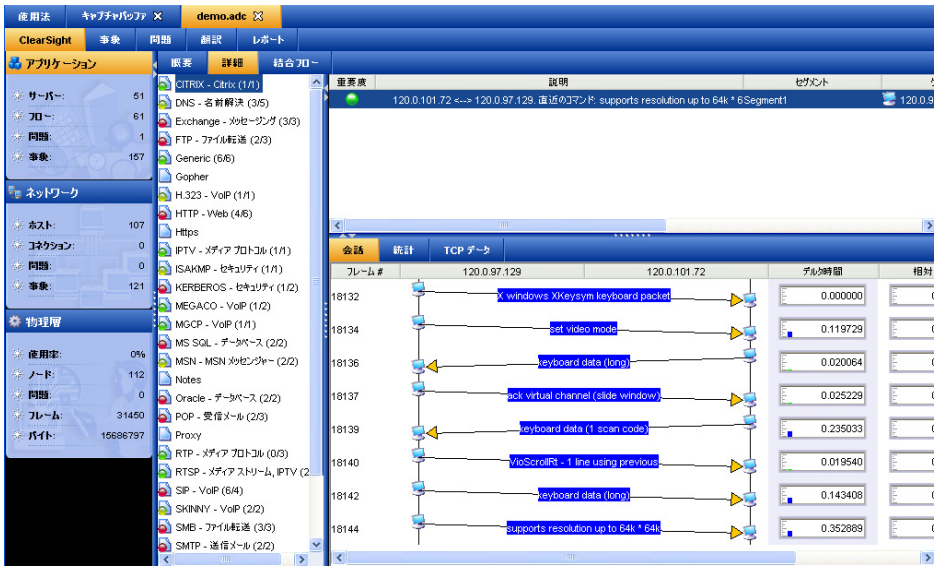


図 5-6: Citrix 詳細画面の例

DNS 詳細画面



ClearSight は、クライアントと DNS サーバー間の名前解決トランザクションのフローを作成して、DNS (Domain Name Service) のトラフィックをリアルタイムでモニタします。ステーションは、DNS を使用して、特定のホスト名と関連付けられた IP アドレスを取得します。これは、「ドメイン名の解決」と呼ばれます。

図 5-7 は、詳細画面における DNS クエリーの典型的なフローを示したものです。

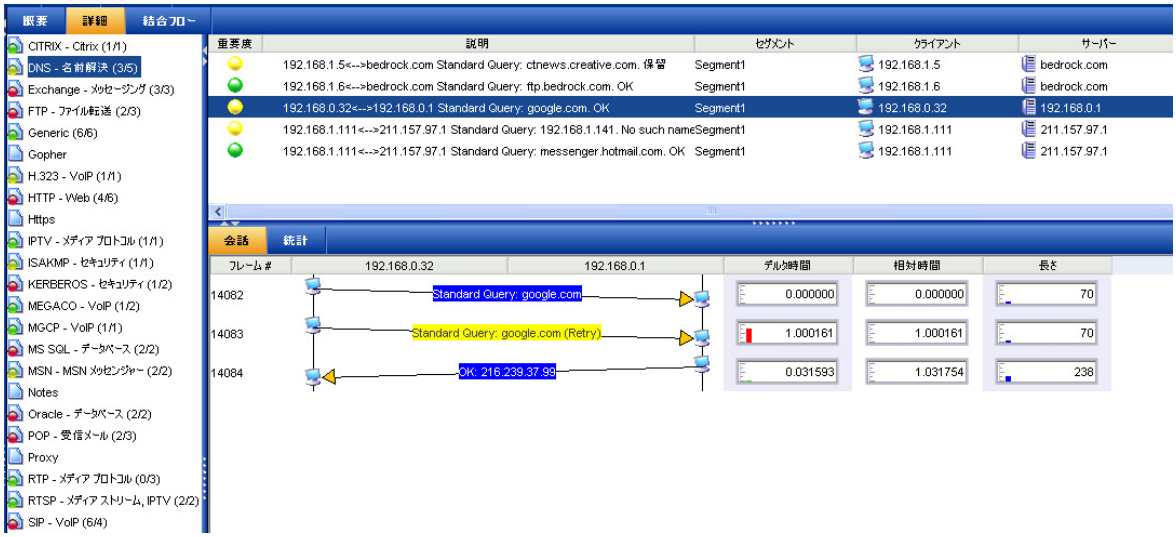


図 5-7: DNS 詳細画面の例

名前解決は、ネットワークトラフィックの非常に高い比率を占める場合があります。そのため、名前要求に対する応答は迅速か、DNS サーバーが遅滞していないかなど、DNS サーバーの応答時間をモニタする必要があります。**[会話]** タブの **[デルタ時間]** フィールドには、DNS サーバーに対して要求を送ってから実際に応答されるまでの遅延をリアルタイムで表示できます。また、**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[スレッショルド]** > **[DNS]** > **[応答時間 (ミリ秒)]** スレッショルドを使用すると、許容可能な最長の応答時間を DNS サーバーに対して指定できます。こうすることにより、指定したスレッショルドよりも遅く応答している DNS サーバーが ClearSight によって検出されると、アラートが生成されるようになります。

DNS 検索されたアドレスのアドレス帳への追加

ClearSight では、リアルタイムモニタの間、DNS で解決された名前と IP アドレスのペアが測定されます。これらのペアは、アドレス帳に追加することが可能です。

DNS 詳細画面からアドレス帳に名前を追加するには、以下を実行します。

1. アプリケーションペインで **DNS - 名前解決**カウンタを選択します。

   新しい **[名前解決]** タブが統計ペインに表示されます。

2. 統計ペインで **[名前解決]** タブをクリックします。

3. **[名前解決]** タブに、現在のモニタセッションで DNS サーバーから解決された名前とアドレスのペアが一覧表示されます。個々の名前とアドレスペアをアドレス帳に追加するには、そのカウンタの横にあるチェックボックスをオンにし、**[追加]** ボタンをクリックします。また、アドレス帳エントリの自動生成機能を有効にすることも可能です。

アドレス帳の操作の詳細については、第 11 章「アドレス帳の使用」を参照してください。

FTP 詳細画面



ClearSight は、クライアントと FTP サーバー間のファイル転送セッションを構成するさまざまなコマンドのフローを作成して、FTP (ファイル転送プロトコル) のトラフィックをリアルタイムでモニタします。また、ClearSight は、FTP トランザクションもリアルタイムで再構成し、転送されているファイル、リストされているディレクトリ (およびリストしているユーザ)、間違ったパスワードなどの情報を図示します。

FTP 詳細画面の情報を使用すると、FTP サーバーの可視性を維持でき、どのファイルが最も頻繁に要求されているか、どの FTP サーバーが過負荷状態になる危険があるか、無許可アクセスが行われていないかどうかなどを簡単に確認できるようになります。

図 5-8 は、ClearSight が FTP トランザクションを統計ペインにどのように再構成するかを示したものです。

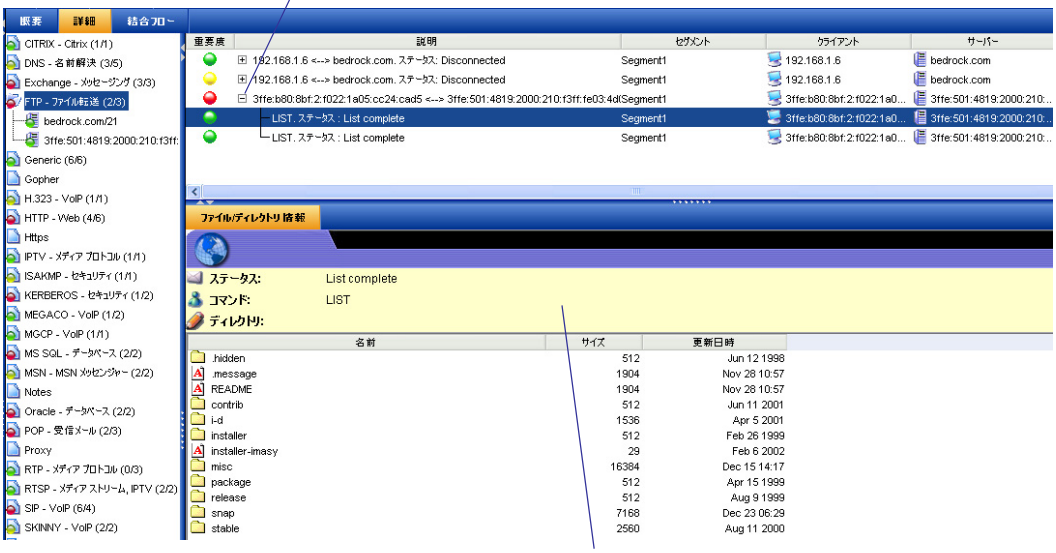


図 5-8: FTP トランザクションの再構成

FTP トランザクションの再構成

図 5-8 に示すとおり、ClearSight は FTP トランザクションをユーザの観点から再構成できます。

FTP トランザクションを再構成するには、以下を実行します。

1. フローペインでエントリの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、フローを構成する個々のコマンドが表示されます。

2. フローからコマンドを選択します。

   統計ペインによって、ユーザの観点からコマンドが自動的に再構成されます。この例では、ClearSight は、FTP トランザクションの現在のステータス、最後のコマンド (**LIST**)、コマンドの結果が表示されています。FTP サーバーからリストされたすべてのファイルが ClearSight で一覧表示されます。

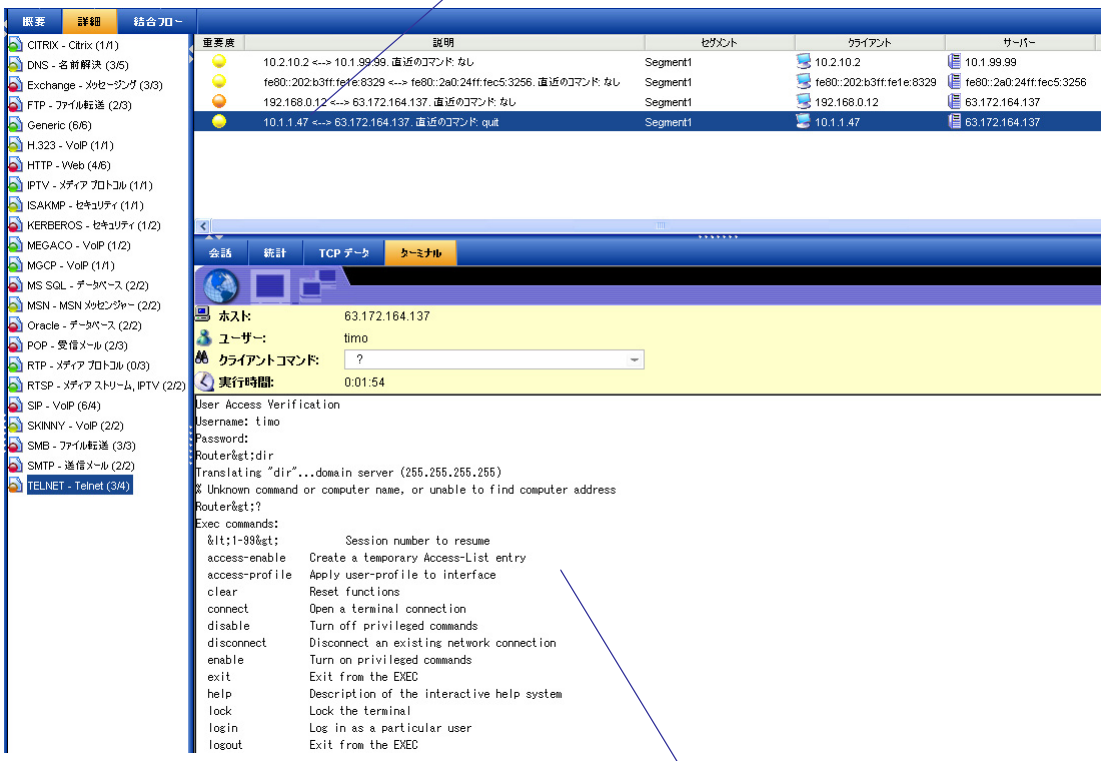
Telnet 詳細画面



ClearSight は、クライアントと Telnet サーバー間のリモートターミナルセッションのフローを作成して、Telnet のトラフィックをリアルタイムでモニタします。クライアントは、Telnet セッションを使用すると、リモートのマシンをそれが直接接続されているかのように操作することができます。クライアントターミナルで入力されたキー操作がリモートマシンに渡される間、リモートマシンの画面がクライアントターミナルに表示されます。

ClearSight は、Telnet セッションをリアルタイムで表示し、サーバーからクライアントに渡される文字指向型のデータをクライアントの観点から表示します。Telnet セッションをクライアントの観点から表示するには、フローペインで Telnet フローを選択します。それにより、統計ペインに [ターミナル] タブが追加され、Terminal セッションがクライアントの観点から表示されるようになります (図 5-9)。

フローペインで Telnet フローを選択します。それにより、**[ターミナル]** タブが統計ペインに表示されるようになります。



[ターミナル] タブには、選択した Telnet セッションがクライアントの観点から表示されます。Telnet セッションの進行に伴って、[ターミナル] タブの情報は、クライアントとサーバー間で渡されるデータによって更新されます。

図 5-9: Telnet セッションの表示

HTTP 詳細画面



ClearSight は、Web サーバーを測定して、Web ページの GET や POST などのフローを作成し、HTTP (HyperText Transfer Protocol) のトラフィックをリアルタイムでモニタします。

HTTP 詳細画面の情報を使用すると、以下を測定できます。

- **Web サーバーのパフォーマンス** : **[会話]** タブの **[デルタ時間]** フィールドでは、HTTP サーバーに対して要求を送ってから実際に応答されるまでの遅延をリアルタイムで表示します。また、**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[スレッショルド]** > **[HTTP]** > **[応答時間 (ミリ秒)]** を設定すると、HTTP サーバーに対して許容可能な最長の応答時間を指定できます。こうすることにより、指定したスレッショルドよりも遅く応答している HTTP サーバーが ClearSight によって検出されると、アラートが生成されるようになります。
- **インターネット攻撃** : DDoS (Distributed Denial of Service) 攻撃は、特定のサーバーまたはファイルに対するアクセスで突然急増する場合があります。
- **不適切なアクセス** : 従業員が社内ネットワーク内から不適切な資料にアクセスしていないかどうかを調べます。

HTTP トランザクションの再構成

ClearSight は、HTTP トランザクションに関するさまざまな統計、アラート、ダイアグラムなどに加え、ClearSight のユーザインターフェイス内で HTTP トランザクションをユーザの観点から再構成することができます。

HTTP トランザクションを再構成するには、以下を実行します。

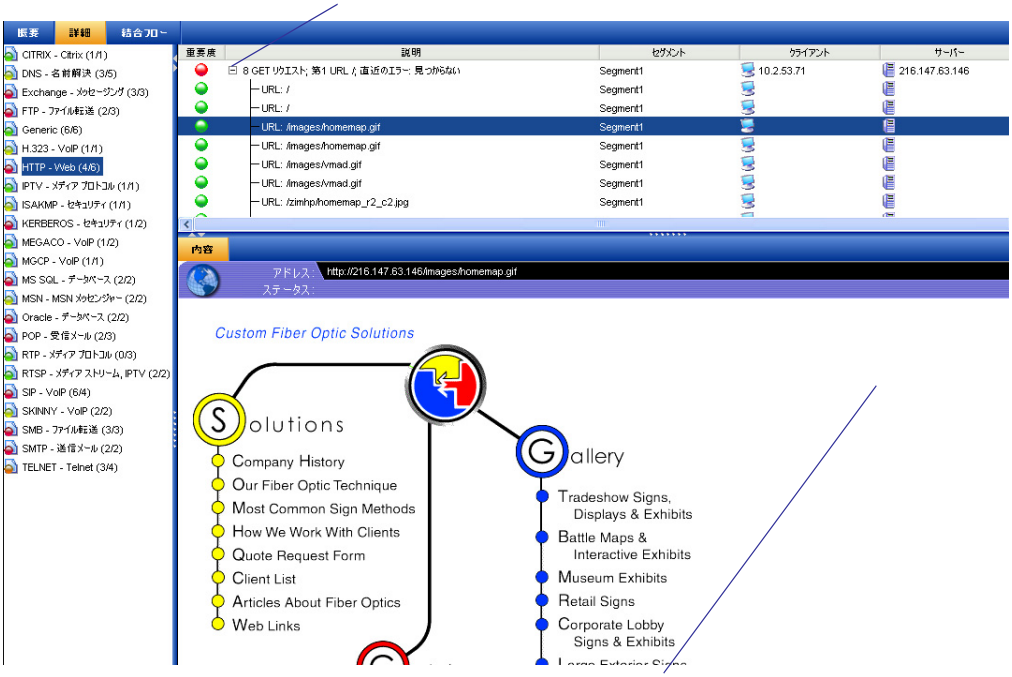
1. フローペインで HTTP カウンタの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、フローを構成する個々の要求が表示されます。

2. フローから HTTP 要求を選択します。

   統計ペインが更新され、**[内容]** タブが表示されます (図 5-10)。**[内容]** タブの右上隅にある **[実行]** ボタンをクリックして、選択した HTTP 要求を発行し、ClearSight ユーザインターフェイス内で結果を表示します。図 5-10 は、HTTP サーバーからの GET 要求例の結果を示したものです。

このアイコンをクリックして、フローを段階的に開きます。次に、フローで個々の要求を選択して、ClearSight によって要求が再構成される様子をユーザの観点から確認してください。このフローには 1 つの GET 要求が含まれています。フローに表示される GET のうち、任意のものを選択して、下の **[内容]** タブでその要求を再構成することができます。



個々の HTTP 要求がフローペインで選択されると、統計ペインに **[内容]** タブが表示され、HTTP コマンドをユーザの観点から再構成できるようになります。関連する Web サイトを表示することもできます。統計ペインの右上隅にある **[GO]** ボタンをクリックするだけで、選択した HTTP コマンドを発行し、結果を表示できます。

図 5-10: HTTP トランザクションの再構成

注記 : この機能を使用するには、**[設定]** ボタン > **[設定]** タブ > **[共通]** > **[モニタオプション]** にある **[HTTP の子フローを表示する]** を有効にする必要があります。195 ページの「モニタオプション」を参照してください。

POP 詳細画面



ClearSight は、クライアントと POP サーバー間の電子メールトランザクションのフローを作成して、POP (Post Office Protocol) のトラフィックをリアルタイムでモニタします。POP は、クライアントがサーバーから電子メールを取得するために一般的に使用する標準のプロトコルです。

その他の詳細画面と同様に、この画面の情報を使用すると、POP サーバーの状態をモニタできます。事前の要請や同意なしに送られてくるスパムメールがサーバーのパフォーマンスにどの程度影響しているかを判定することができます。また、POP サーバーの無許可使用を検出することもできます。

ClearSight によってモニタされるその他のサーバーの場合と同様に、**[会話]** タブのデルタ時間と **[設定]** ボタン > **[設定]** タブ > **[問題]** > **[スレッショルド]** で設定される応答時間アラートは、POP サーバーの応答のパフォーマンスを判定する際に効果的なツールです。

電子メールの表示

ClearSight では、POP サーバーから電子メールを取得するために使用される要求や応答のほか、実際の電子メールメッセージも自然言語で表示されます。電子メールは、エンドユーザによって表示されたのと同様の状態のものを ClearSight のユーザインターフェイス内で表示できます。

重要 : 他人の電子メールを表示することは、プライバシーの侵害とみなされる場合があります。ClearSight を使用して他人の電子メールを表示する前に、それにより派生的に起こる問題を必ず考慮するようにしてください。

電子メールを表示するには、以下を実行します。

1. フローペインで POP エントリの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、そのフローで受信された電子メールが表示されます。

2. 電子メールメッセージをフローから選択します。

   統計ペインが更新され、**[POP 情報]** タブが表示されます (図 5-11)。**[POP 情報]** タブには、電子メールクライアント内でユーザに対して表示される場合と同様に、すべてのフィールドが含まれた状態で電子メールメッセージが表示されます。

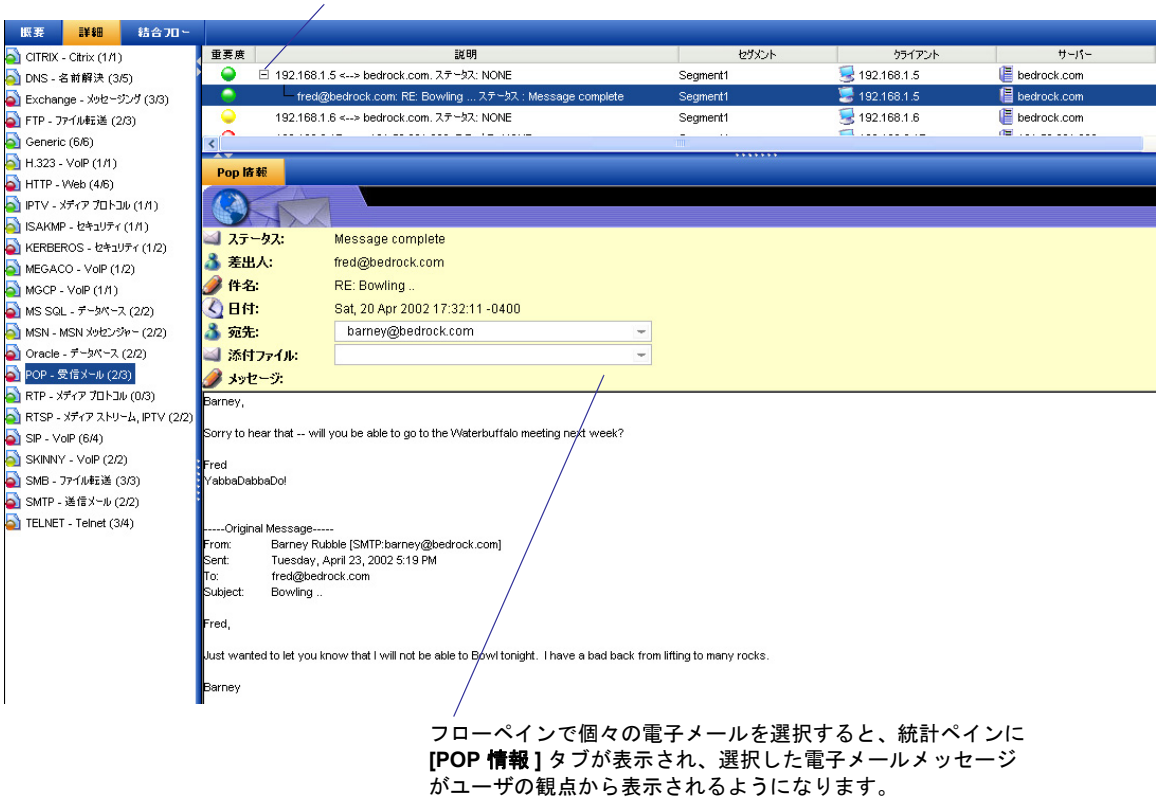


図 5-11: POP フローで取得された電子メールの表示

SMTP 詳細画面



ClearSight は、クライアントと SMTP サーバー間の電子メールトランザクションのフローを作成して、SMTP (Simple Mail Transfer Protocol) のトラフィックをリアルタイムでモニタします。SMTP は、クライアントが電子メールを最終的な送信先に転送する目的でサーバーに送信する際に一般的に使用する、標準のプロトコルです。

その他の詳細画面と同様に、この画面の情報を使用すると、SMTP サーバーの状態をモニタできます。SMTP は、事前の要請や同意なしに電子メールを送る送信者 (“スパム”) の標的になりやすいサーバーです。多くのスパムは、非公開の SMTP サーバーを利用して商業的なスパムメールを“バウンス”させることにより、それらのサーバーを悪用します。これにより、SMTP サーバーのパフォーマンスが劣化する可能性があります。極端な場合、このような不正使用が DoS (サービス拒否) 攻撃に発展することもあります。ClearSight は、SMTP サーバー上を通過する電子メールをモニタすることにより、認証されたメッセージだけが転送されるようにします。

ClearSight によってモニタされるその他のサーバーの場合と同様に、詳細表示の **[会話]** タブにあるデルタ時間と **[設定]** ボタン > **[設定]** タブ > **[問題]** > **[スレッショルド]** ページで設定される応答時間アラートは、SMTP サーバーの応答のパフォーマンスを判定する際に効果的なツールです。

電子メールの表示

ClearSight では、SMTP サーバーに電子メールを送信するために使用される要求や応答のほか、実際の電子メールメッセージも自然言語で表示されます。電子メールは、エンドユーザが送信した状態のものを ClearSight のユーザインターフェイス内で表示できます。

重要 : 他人の電子メールを表示することは、プライバシーの侵害とみなされる場合があります。ClearSight を使用して他人の電子メールを表示する前に、それにより派生的に起こる問題を必ず考慮するようにしてください。

電子メールを表示するには、以下を実行します。

1. フローペインで SMTP エントリの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、そのフローで送信された電子メールが表示されます。

2. 電子メールメッセージをフローから選択します。

   統計ペインが更新され、**[メール情報]** タブが表示されます (図 5-12)。**[メール情報]** タブには、ユーザが送信した状態の電子メールメッセージがすべてのフィールドとともに表示されます。

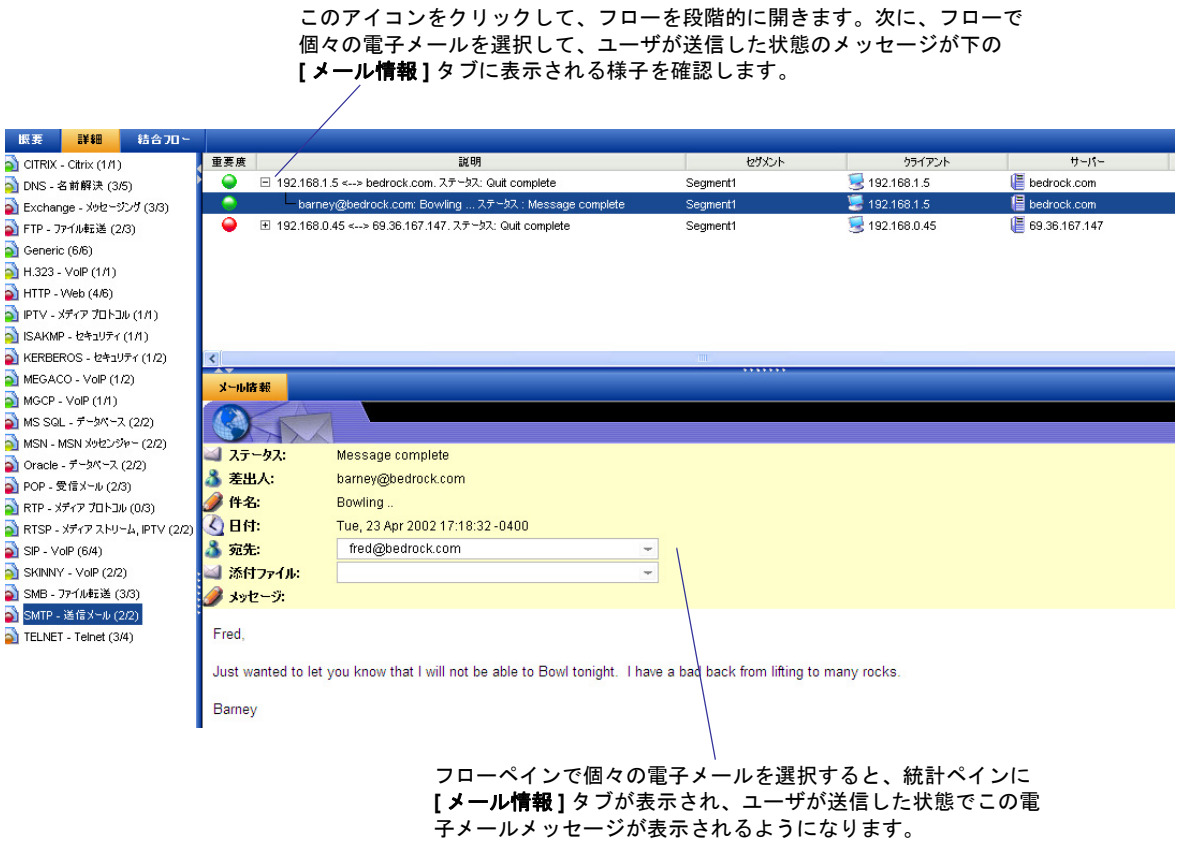


図 5-12: SMTP フローで送信された電子メールの表示

MS SQL 詳細画面



ClearSight は、データベースクライアントと MS SQL サーバー間のトランザクションのフローを作成して、Microsoft SQL Server (MS SQL) のトラフィックをリアルタイムでモニタします。MS SQL は、構造化問合せ言語 (SQL) を使用したエンタープライズデータベースシステム実装で、Microsoft に著作権があります。

その他の詳細画面と同様に、この画面の情報を使用すると、MS SQL サーバーの状態をモニタできます。ClearSight は、**Select**、**Insert**、**Delete** など、さまざまな種類の一般的な SQL コマンドを測定します。

ClearSight によってモニタされるその他のサーバーの場合と同様に、詳細表示の **[会話]** タブにあるデルタ時間は、MS SQL サーバーの応答のパフォーマンスを判定する際に効果的です。また、**[統計]** タブのカウンタには、選択したフローの平均トランザクション時間に関する詳細が表示されます。これらの統計は、現在の MS SQL サーバーがニーズを満たしているかを判定する際に役に立ちます。

MS SQL トランザクションの再構成

ClearSight は、MS SQL トランザクションに関するさまざまな統計、アラート、ダイアグラムなどに加え、ClearSight のユーザインターフェイス内で MS SQL トランザクションをユーザの観点から再構成することができます。

Select 文や **Cursor Open** 文などの結果をデータベースクライアントの観点から表示することができます。ClearSight では、これらの文から返される実際の表形式のデータが表示されるため、データベースに対してどのクエリーが実行されているのかを確認できます。

MS SQL トランザクションを再構成するには、以下を実行します。

1. フローペインで MS SQL エントリの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、フローを構成する個々のクエリーとコマンドが表示されます。

2. フローから MS SQL コマンドを選択します (**Select** や **Cursor Open** など)。

   統計ペインが更新され、**[内容]** タブが表示されます (図 5-13)。**[内容]** タブには、選択したクエリーまたはコマンドから返された実際の表形式データが表示されます。

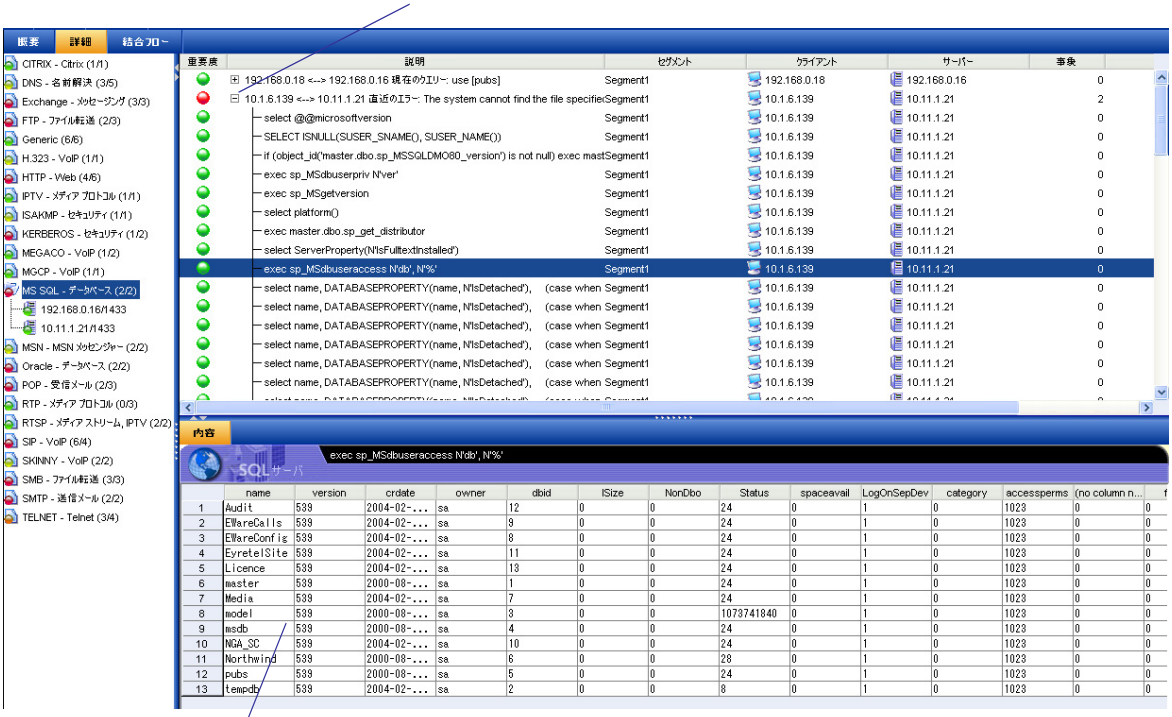


図 5-13: MS SQL トランザクションの再構成

MS SQL フローでのエラーの表示

ClearSight には、MS SQL サーバーに対するクエリーの結果が表示されるだけでなく、MS SQL フローに対して発行されたエラーメッセージを表示するためのタブも備わっています。

MS SQL エラーメッセージを表示するには、以下を実行します。

1. エラーが関連付けられた親フローをフローペインで選択します。通常、エラーのあるフローには、**[重要度]** 列に黄色のアイコンが付いています。

   統計ペインに [エラーログ] タブが生成され、選択したトランザクションに対して生成されたすべての SQL エラーが表示されます。図 5-14 は、MS SQL トランザクションに対して生成された SQL エラーの例を示したものです。

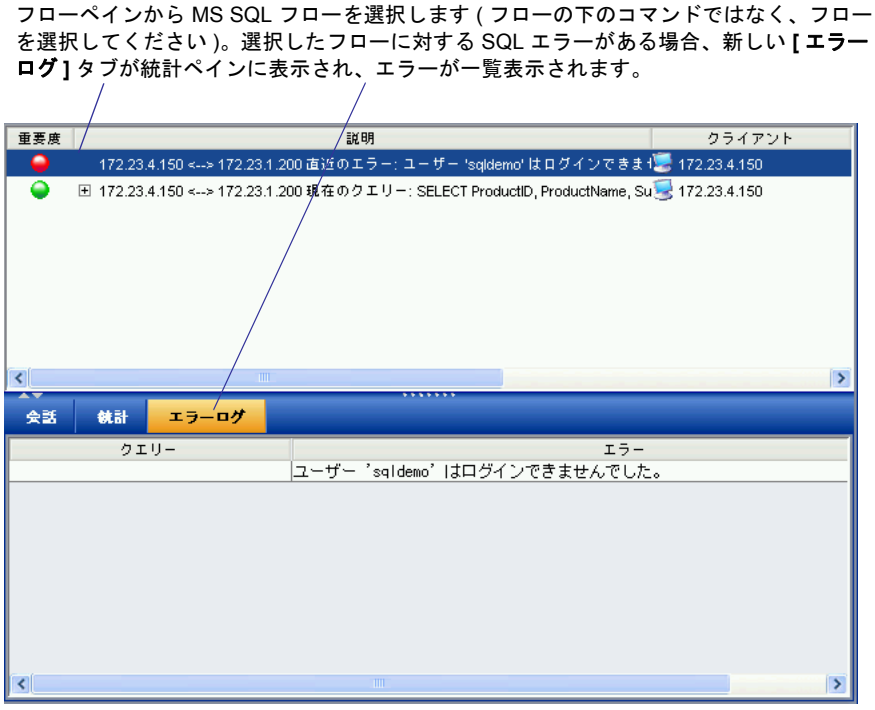


図 5-14: MS SQL フローに対するエラーの表示

Oracle 詳細画面



ClearSight は、データベースクライアントと Oracle サーバー間のトランザクションのフローを作成して、Oracle のトラフィックをリアルタイムでモニタします。構造化問合せ言語 (SQL) の Oracle 実装は、企業内ネットワークで広く使用されています。

その他の詳細画面と同様に、この画面の情報を使用すると、Oracle サーバーの状態をモニタできます。ClearSight は、**Select**、**Insert**、**Delete** など、さまざまな種類の一般的な SQL コマンドを測定します。

ClearSight によってモニタされるその他のサーバーの場合と同様に、詳細表示の **[会話]** タブにあるデルタ時間は、Oracle サーバーの応答のパフォーマンスを判定する際に効果的です。また、**[統計]** タブのカウンタには、選択したフローの平均トランザクション時間に関する詳細が表示されます。これらの統計は、現在の Oracle サーバーがニーズを満たしているかを判定する際に役に立ちます。

Oracle トランザクションの再構成

ClearSight は、Oracle トランザクションに関するさまざまな統計、アラート、ダイアグラムなどに加え、ClearSight のユーザインターフェイス内でトランザクションをユーザの観点から再構成することができます。

Select 文や **Cursor Open** 文などの結果をデータベースクライアントの観点から表示することができます。ClearSight では、これらの文から返される実際の表形式のデータが表示されるため、データベースに対してどのクエリーが実行されているのかを確認できます。

Oracle トランザクションを再構成するには、以下を実行します。

1. フローペインで Oracle エントリの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、フローを構成する個々のクエリーとコマンドが表示されます。

2. フローから Oracle コマンドを選択します (**Select** や **Cursor Open** など)。

   統計ペインが更新され、**[内容]** タブが表示されます (図 5-15)。**[内容]** タブには、選択したクエリーまたはコマンドから返された実際の表形式データが表示されます。

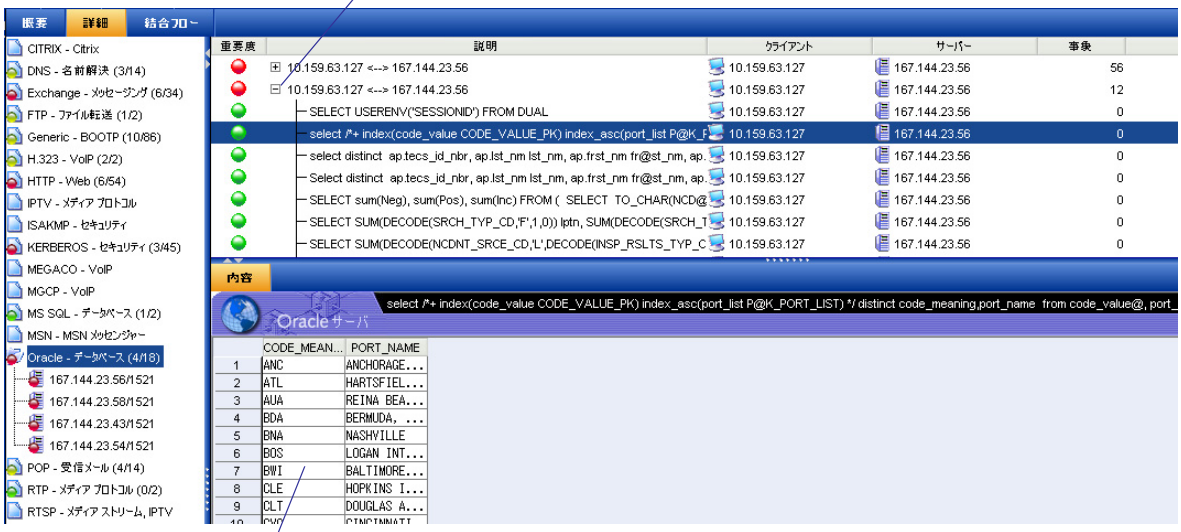


図 5-15: Oracle トランザクションの再構成

Oracle フローに対するエラーの表示

ClearSight には、Oracle サーバーでクエリーなどのトランザクションを実行するために使用される要求と応答が表示されるだけでなく、フローに対して発行されたエラーメッセージを表示するためのタブも備わっています。以下は、Oracle のエラーメッセージを表示する手順を説明したものです。

Oracle のエラーメッセージを表示するには、以下を実行します。

1. エラーが関連付けられたフローをフローペインで選択します。通常、エラーのあるフローには、**[重要度]** 列に黄色のアイコンが付いています。

   注記 : フローカウンタの下にあるコマンドではなく、親フローを選択してください。

   統計ペインに **[エラーログ]** タブが生成され、選択したトランザクションに対して生成されたすべての SQL エラーが表示されます。この画面は、148 ページの図 5-14 に示される MS SQL フロー用の画面とよく似ています。

Exchange 詳細画面



ClearSight は、メッセージングクライアントと Exchange サーバー間のトランザクションのフローを作成して、Microsoft Exchange のトランザクションをリアルタイムでモニタします。Exchange は、電子メール、インスタントメッセージング、スケジューリングなどの目的のために Microsoft によって開発されたサーバーです。

その他の詳細画面と同様に、この画面の情報を使用すると、Exchange サーバーの状態をモニタできます。一般的に、Exchange サーバーでは大量のデータが移動されます。そのため、ネットワークのニーズが高まるにつれ、ハードウェアリソースの負担が過剰になる可能性があります。詳細画面の **[会話]** タブにあるデルタ時間と **[統計]** タブのカウンタを使用すると、お使いの Exchange サーバーの応答パフォーマンスがニーズを満たしているかを判定することができます。

また、ClearSight では、Exchange にインストールされているスパム対策機能が効果的に調整されているかを調べることもできます。ClearSight では Exchange サーバーを通過する電子メールを表示できるため、全体のうちスパムが占める割合や正当なトラフィックが占める割合をすばやく確認できます。これらの知識を利用すると、現在のスパム対策機能の有効性を判定し、必要に応じて是正措置をとることができます。

電子メールの表示

ClearSight では、Exchange クライアントとサーバー間でメッセージを送受信するために使用される要求と応答が表示されるだけでなく、実際の電子メールのメッセージも自然言語で表示できます。電子メールは、エンドユーザによって表示された状態のものを ClearSight のユーザインターフェイス内で表示できます。

重要 : 他人の電子メールを表示することは、プライバシーの侵害とみなされる場合があります。ClearSight を使用して他人の電子メールを表示する前に、それにより派生的に起こる問題を必ず考慮するようにしてください。

電子メールを表示するには、以下を実行します。

1. フローペインで Exchange エントリの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、そのフローで送信された電子メールが表示されます。

2. 電子メールをフローから選択します。

   統計ペインが更新され、ユーザが送信した状態の電子メールがすべてのフィールドとともに表示されます。

MSN 詳細画面



Microsoft Network Messenger (MSN) は、インスタントメッセージングの目的のために Microsoft によって開発されたサーバーです。ClearSight は、メッセージング クライアントと MSN サーバー間のトランザクションのフローを作成して、MSN トランザクションをリアルタイムでモニタします。

MSN アプリケーションを選択すると、ClearSight は、全フレーム数、全バイト数、平均スループット、クライアント / サーバー平均応答時間、ログイン、失敗したログインなど、アプリケーション全体の統計情報を表示します。また、ファイル転送数、音声会話数、映像会話数、IM (インスタントメッセージング) 会話数、およびそれらに対応する転送バイト数も表示します。

サーバーを選択すると、ClearSight は [概要] タブにアプリケーションホスト、サーバー統計、および (そのサーバーの) MSN サーバー統計を表示します。フローを選択すると、ClearSight はそのフローに固有の会話と統計の情報を表示します。

MSN メッセージの表示

MSN クライアントとサーバー間のトラフィックの送受信に使用される要求 / 応答シーケンスの表示に加えて、ClearSight では実際の MSN メッセージを自然言語で表示できます。メッセージはエンドユーザが目にするのと同様のものを ClearSight ユーザ インターフェイス内で表示できます。

重要 : 他人のメッセージを表示することは、プライバシーの侵害と見なされる場合があります。ClearSight を使用して他人のメッセージを表示する前に、それにより派生的に起こる問題を必ず考慮するようにしてください。

MSN メッセージを表示するには、以下を実行します。

1. フローペインで MSN フローをクリックします。
2. フローの中に MSN メッセージがある場合には、その内容が統計ペインの **[MSN メッセージ]** タブに表示されます。

VoIP 詳細画面



ClearSight は、個々のコールのフローを作成し、Voice over IP (VoIP) Gateway、Gatekeeper、Multipoint Control Unit、Client、Call Manager などをモニタして、VoIP をリアルタイムでモニタします。

ClearSight の H.323、SIP、Skinny、MGCP、および Megaco 用の画面は、その内容が類似しています。これらの VoIP アプリケーションはすべて、実際の音声データの転送に RTP を使用します。ClearSight では、RTP と TCP の両方の情報が表示され、RTP ストリームから抽出された音声コンテンツを実際に再現できます (157 ページの「音声の再生」および 159 ページの「ビデオコンテンツの再生」を参照)。

これらの VoIP アプリケーションに固有の特性の一部を以下に示します。

- **H.323** は、リアルタイムの VoIP 機能を提供するプロトコルセットの総称です。T.38 Fax over IP も含まれます。
- **SIP** (Session Initiation Protocol) は、VoIP コールやマルチメディアセッションなどの接続と接続解除に使用されるシグナリングプロトコルです。SIP は、コールの設定、接続、制御などを処理します。
- **Skinny** は、Cisco の Skinny Client Control Protocol (SCCP) を指します。Skinny 環境では、IP テレフォニーデバイスは、最小限の操作を行うために必要な H.323 仕様の一部だけを実装して動作します。それ以外の VoIP サービスに対しては、Call Manager と呼ばれるフル機能の H.323 プロキシが使用されます。
- **MGCP** (Media Gateway Control Protocol) は、H.323 対応のコールエージェントの機能を メディアゲートウェイの機能と調和させます。コールエージェントはシグナリングとコールプロセシングを担当し、メディアゲートウェイはオーディオ信号の変換と電話エンドポイントへの接続を担当します。
- **Megaco** (H.248 とも呼ばれる) は MGCP と似ていますが、ATM などのより広範囲なネットワークをサポートします。さらに、Megaco は、メディアゲートウェイコントローラがメディアゲートウェイの動作をより広範に制御できるようにします。

VoIP QoS レポートの表示

ClearSight では、VoIP コールを説明し定量化する、さまざまな QoS (Quality of Service) 情報が提供されます。これらの情報を使用すると、既存のネットワークが許容レベルの質の VoIP サービスを提供しているかどうかを判定できます。VoIP サービスの質を評価する際は、ジッタを示す統計値に特に注意してください。ジッタのレベルが高いと、VoIP コールが不明瞭になる可能性があります。

VoIP QoS レポートを表示するには、以下の操作を実行します。

1. フローペインの **H.323**、**SIP**、**Skinny**、**MGCP**、または **Megaco** のエントリをクリックします。
2. 2 つのタブ (ほかのペインにも表示される [会話] タブと、VoIP アプリケーションに固有の [レポート] タブ) が統計ペインに表示されます。
3. [レポート] タブをクリックします。図 5-16 のような画面が表示されます。

QoS レポートは、選択したフローに適用され、次の情報を含んでいます。

[概要]	関連する VoIP プロトコルとさまざまなパラメータ (コール間隔、RTP で転送されたフレームの数など) が表示されます。
[VoIP インデックス]	コールの全般的な品質の特性を示す数値インデックス (1 ～ 5 の範囲で表示)。このインデックスは、レポートの右上隅にも星印でその評価が表示されます。
[性能インデックス]	選択したフローで観測された [パケットロス]、[ジッター]、[不正な順序] のパケット、および [遅延] の全体的な数量が要約されます。

レポートの残りの部分には、[性能インデックス] のそれぞれの数量を詳細に示す棒グラフと、各数量の重要度を説明するテキストが表示されます。

- パケットロスレポート

- ジッタ分析
- 不正な順序レポート
- R 値と MOS
- VQFactor （ビデオフローのみ）

[レポート] タブの上部にあるコントロールを使用して、画像のサイズを調整し、見やすくすることができます。複数のページがある場合は、前後に移動できます。また、レポートの保存や印刷も可能です。

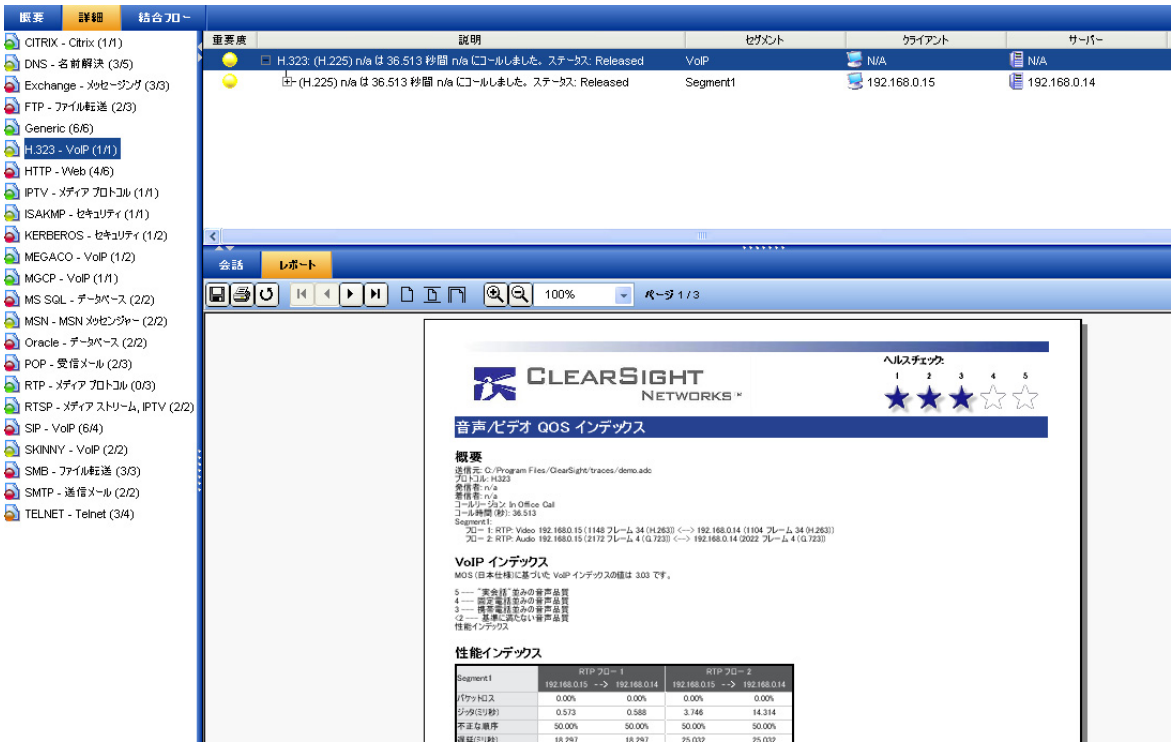


図 5-16: VoIP QoS レポートの表示

音声の再生

ClearSight では、ClearSight のユーザインターフェイス内から PC のスピーカーを使用して音声を再生することもできます。以下はその手順を示したものです。

重要 : 非公開の VoIP 会話を傍受することは、プライバシーの侵害とみなされる場合があります。ClearSight を使用して非公開の VoIP を傍受する前に、それにより派生的に起こる問題を必ず考慮するようにしてください。

VoIP コールを再生するには、以下を実行します。

1. フローペインの **H.323**、**SIP**、**Skinny**、**MGCP**、または **Megaco** のエントリの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、そのフローのさまざまなコマンドやストリームが表示されます。

2. 選択したフローの下にある RTP オーディオストリームのエントリを選択します。

   統計ペインが更新され、ビルトインのメディアプレーヤーを含む **[内容]** タブが表示されます。**[内容]** タブの **[再生]** ボタンをクリックし、選択した RTP オーディオストリームを PC のスピーカーから再生します。

図 5-17 は、VoIP コールの再生準備が整った、**[内容]** タブの例を示したものです (この場合は SIP)。

このアイコンをクリックして、フローを段階的に開きます。次に、個々の RTP オーディオストリームを選択します。下のペインの **[内容]** タブを使用すると、選択したオーディオストリームを PC のスピーカーから再生できます。

選択した RTP オーディオストリームを PC のスピーカーから再生するには、このボタンをクリックします。

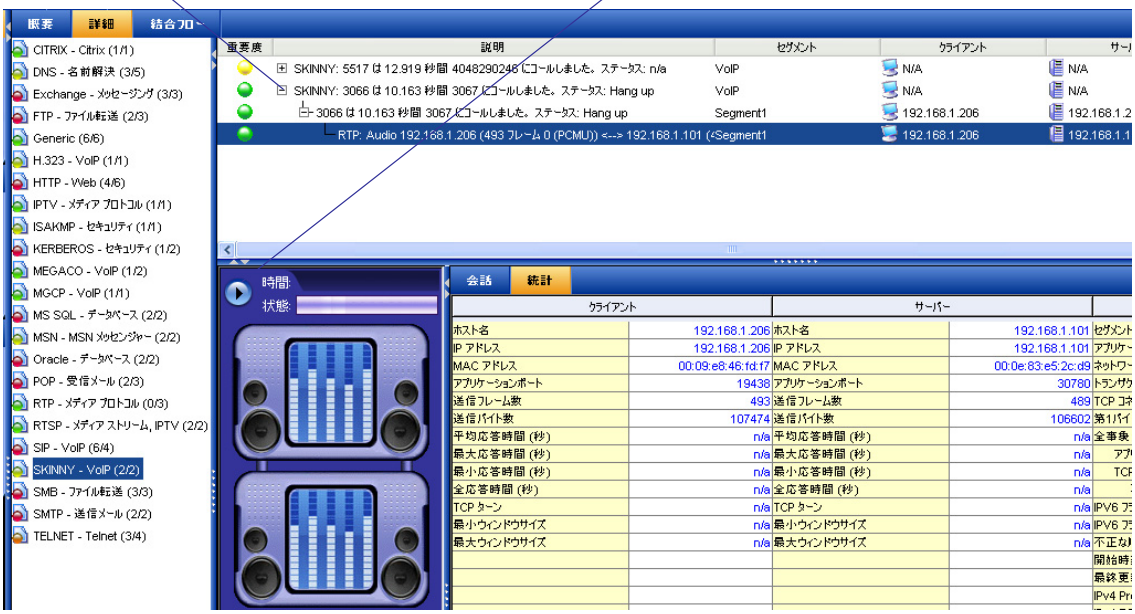


図 5-17: PC のスピーカーを使用した VoIP の再生

注記 : 使用しているコーデックに応じて、オーディオ内容を wav ファイルに保存することができます。162 ページの「wav ファイルへの RTP ストリームの保存」を参照してください。

ビデオコンテンツの再生

ClearSight では、ClearSight のユーザインターフェイス内からビデオコンテンツを再生することもできます。以下はその手順を示したものです。

ビデオコンテンツを再生するには、以下を実行します。

1. フローペインの VoIP フローのエントリの隣にあるスイッチ型のアイコン⊞をクリックします。

   選択したフローが段階的に開き、そのフローのさまざまなコマンドやストリームが表示されます。

2. 選択したフローの下にある RTP ビデオストリームのエントリを選択します。

   統計ペインが更新され、内蔵メディアプレーヤーが表示されます。**[再生]** ボタンをクリックして、選択した RTP ビデオストリームを再生します。

図 5-18 は、再生中の VoIP ビデオストリームが表示されている画面の例です。

フローをクリックして個々の RTP ビデオストリームを選択します。下のペインの左側で、選択したビデオストリームを再生できます。

選択した RTP ビデオストリームを再生するには、このボタンをクリックします。

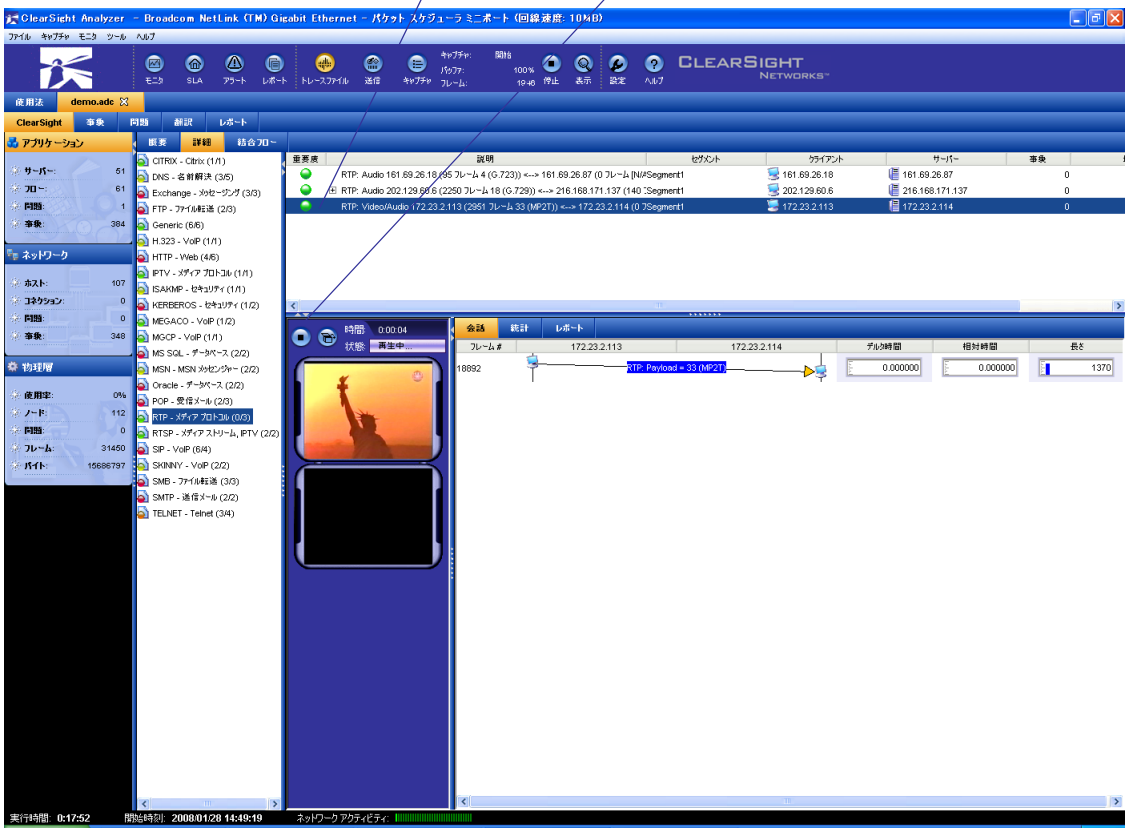


図 5-18: ビデオコンテンツの再生

ビデオ画面のサイズを大きくするには、 ボタンをクリックします。

注記：使用しているコーデックに応じて、ビデオコンテンツを mpg ファイルに保存することができます。165 ページの「MPG ファイルへの RTP ビデオストリームの保存」を参照してください。

RTP 詳細画面



ClearSight は、個々のマルチメディアストリームのフローを作成して、Real-Time Transport Protocol (RTP) トランザクションをモニタします。RTP は、リアルタイムのマルチメディア配布アプリケーションによって広く使用されており、オーディオおよびビデオのリアルタイムな配信が行えます。RTP は、オーディオデータを配布する目的で、H.323、SIP、Skinny、MGCP、Megaco をはじめとした一般的なアプリケーションで使用されています。

ClearSight では、RTP ストリームに関するさまざまな統計値や計測値が提供されます。これらの統計値を使用すると、RTP ストリームをトラブルシューティングして、マルチメディアデータのタイムリーな配布を確実に行うことができます。

RTP ストリームの再生

ClearSight では、ClearSight のユーザインターフェイス内から RTP ストリームを再生することもできます。

RTP ストリームを再生するには、以下を実行します。

1. フローペインで RTP エントリの隣にあるスイッチ型のアイコン ⊞ をクリックします。

   選択したフローが段階的に開き、そのフローのさまざまなコマンドやストリームが表示されます。

2. 選択したフローの下にある RTP ストリームのカウンタを選択します。

   統計ペインが更新され、内蔵メディアプレーヤーを含む **[内容]** タブが表示されます。**[内容]** タブの **[再生]** ボタンをクリックして、選択した RTP ストリームを再生します。

wav ファイルへの RTP ストリームの保存

特定のサポートされているコーデックの場合、RTP ストリームのオーディオ内容を wav ファイルに保存できます。双方向の RTP ストリームの場合、2 つのストリームは別々のチャネルに入れられます。

wav ファイルを作成するには、メディアプレーヤー上の任意の場所を右クリックします。**[エクスポート]** ボタンが表示されます。**[エクスポート]** ボタンをクリックすると **[保存]** ダイアログボックスが表示されます。このダイアログボックスでファイルの保存先を指定できます。

サポートされているコーデックは、G.711 (PCMU)、G.722、G.723、G.726、G.729、AAC (MPEG)、および AMR (3GPP および GSM) です。AMR は、正しいコーデックに設定する必要があります。

RTSP 詳細画面



ClearSight は、Microsoft IPTV を含め、個々のマルチメディアストリームのフローを作成して、Real-Time Streaming Protocol (RTSP) トランザクションをモニタします。RTSP は、オーディオやビデオなどのリアルタイムなマルチメディア配信を調和させるための制御プロトコルです。通常、実際の配信は RTP などの別のプロトコルによって実行されますが、配信の制御は RTSP によって行われます。1 つの RTSP セッションは、複数のマルチメディアサーバーを制御でき、オーディオとそれに対応するビデオストリームの同期などの重要な機能を実行することもできます。RTSP の構成は、意図的に HTTP と類似させているため、Web ブラウザなどの HTTP アプリケーションとの互換性があります。たとえば、Web ページ上のリンクをクリックして RTSP セッションを開始することができます。

図 5-19 は、詳細画面に表示された RTSP ストリームの典型的なフローを示しています。

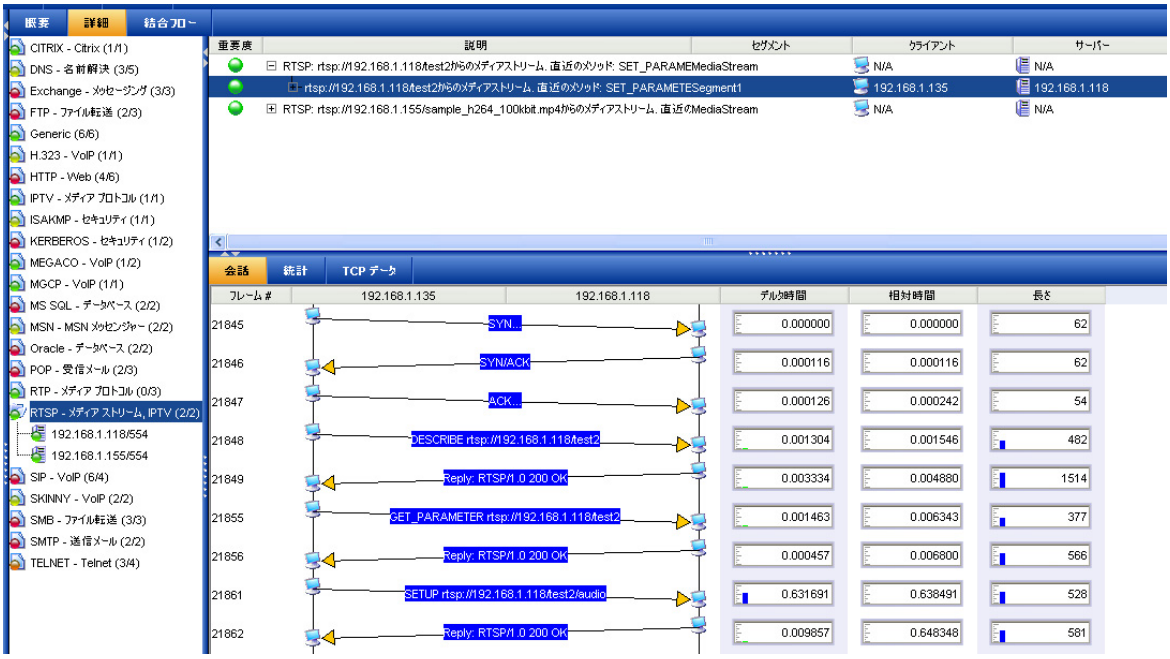


図 5-19: RTSP 詳細画面の例

[会話] タブのラダー表示には、メディアストリームを制御する一連のトランザクションが表示されています。フローペインに展開されたビューには、オーディオおよびビデオコンテンツの実際の配信が RTP プロトコルによってどのように実行されるかが表示されています。

IPTV 詳細画面



ClearSight は、個々のマルチメディアストリームのフローを作成して、IP テレビ（IPTV）トランザクションをモニタします。

図 5-20 は、詳細画面に表示された IPTV ストリームの典型的なフローを示しています。



図 5-20: IPTV 詳細画面の例

[会話] タブのラダー表示には、IPTV の種類が表示されます。

注記 ：MPEG2 over UDP を翻訳するには、ClearSight 翻訳エンジンを使用する必要があります。

IPTV コンテンツの再生

ClearSight では、ClearSight のユーザインターフェイス内から IPTV ストリームを再生することもできます。

IPTV ストリームを再生するには、以下を実行します。

ビデオ画面上部の再生ボタン  をクリックします。

ビデオ画面のサイズを大きくするには、 ボタンをクリックします。

MPG ファイルへの RTP ビデオストリームの保存

IPTV ストリームのビデオコンテンツは、mpg ファイルに保存することができます。

mpg ファイルを作成するには、メディアプレーヤー上の任意の場所を右クリックし、**[エクスポート]** メニューを表示させます。**[エクスポート]** メニューを選択すると、**[保存]** ダイアログボックスが表示されますので、このダイアログボックスでファイルの保存先を指定し、ファイルを作成します。

Kerberos 詳細画面



ClearSight は、クライアントと Kerberos サーバー間のトランザクションのフローを作成して、Kerberos のトランザクションをリアルタイムでモニタします。Kerberos サーバーは、クライアントの ID を検証し、証明書の作成に使用できるチケットを発行するための手段となります。クライアントはこの証明書を使用して、他のサーバーに対して自身を認証することができます。

この画面の情報を使用すると、ネットワーク上のセキュリティ関連のアクティビティを測定できます。たとえば、統計ペインの [概要] タブには、発行されたチケットの数、関連するクライアントの数、およびエラーの数が表示されます。エラーは、サーバーが Kerberos データベースでサーバーが見つからなかった場合や、クライアントの証明書が取り消されているなどの場合に発生します。

ClearSight によってモニタされるその他のサーバーの場合と同様に、詳細画面の **[会話]** タブにあるデルタ時間は、Kerberos サーバーの応答のパフォーマンスを判定する際に効果的です。また、**[統計]** タブのカウンタには、選択したフローの平均トランザクション時間に関する詳細が表示されます。これらの統計は、現在の Kerberos サーバーがニーズを満たしているかどうかを判定する際に役に立ちます。

ISAKMP 詳細画面



ClearSight は、クライアントと ISAKMP サーバー間のトランザクションのフローを作成して、ISAKMP のトランザクションをリアルタイムでモニタします。ISAKMP サーバーは、セキュリティアソシエーションの設定、維持、削除を行います。セキュリティアソシエーションは、会話の当事者が互いを認証し、セキュリティ保護されたトランザクションを実行する際のフレームワークを提供します。

この画面の情報を使用すると、ネットワーク上のセキュリティ関連のアクティビティを測定できます。たとえば、統計ペインの [概要] タブには、セッション数と、フェーズ 1、フェーズ 2、およびクイックモードの成功 / 失敗の数が表示されます。

ClearSight によってモニタされるその他のサーバーの場合と同様に、詳細画面の **[会話]** タブにあるデルタ時間は、ISAKMP サーバーの応答のパフォーマンスを判定する際に効果的です。また、**[統計]** タブのカウンタには、選択したフローの平均トランザクション時間に関する詳細が表示されます。これらの統計は、現在の ISAKMP サーバーがニーズを満たしているかどうかを判定する際に役に立ちます。

SMB 詳細画面



ClearSight は、SMB クライアントと SMB サーバー間のトランザクションのフローを作成して、SMB のトラフィックをリアルタイムでモニタします。SMB (Server Message Block) は、CIFS (Common Internet File System) とも呼ばれています。Microsoft コンピュータのユーザがネットワーク上のファイルやその他のリソース (プリンタなど) にアクセスする際に最もよく使用しているアプリケーションです。

図 5-21 は、詳細画面に表示された SMB クライアントと SMB サーバーの間の一連の要求と応答のやりとりの典型的なフローを示しています。

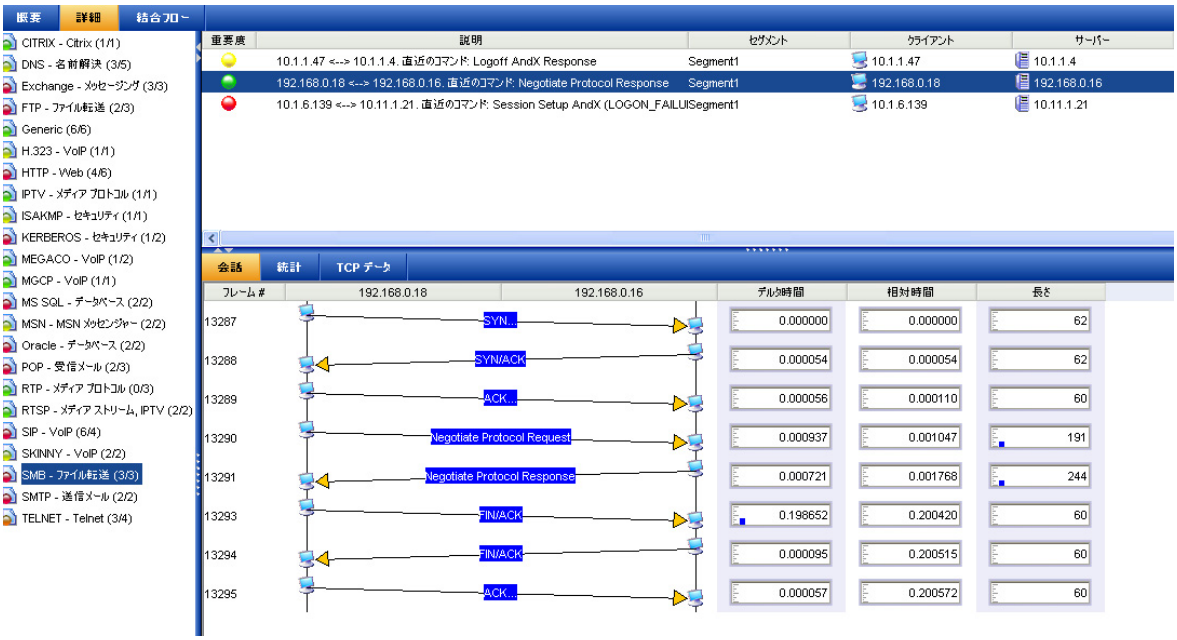


図 5-21: SMB 詳細画面の例

[会話] タブのラダー表示には、クライアントによって送信された一連の要求と、それに続くサーバーからの応答が表示されています。

[統計] タブにある SMB 固有のカウンタには、セッション数、ディレクトリおよびファイルの要求数、各種のエラー数が記録されます。

Generic 詳細画面



ClearSight では、明示的にサポートされているアプリケーションタイプ (**[アプリケーション]** > **[概要]** ページ上に表示されているもの) に当てはまらないか、まだ完全に識別されていないアプリケーション層のトランザクションに対して、「Generic」のフローが作成されます。

ClearSight の統計タブには、Generic のフローに関するトラフィックの統計が表示されます。また、**[会話]** タブには、フローのエンドポイント間の TCP ハンドシェイキングを示す、標準のネットワークラダーダイアグラムが表示されます。

ネットワーク層のモニタ

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

この項では、ネットワーク層における ClearSight のリアルタイムモニタ画面について説明します。ネットワーク層では、アプリケーマルチキャストション層に表示されるアプリケーションフローの基盤となる、第 3 層と第 4 層のホストとコネクションが測定されます。UDP、ARP、ICMP などを含む TCP/IP ファミリーのプロトコルに関しては、カウンタと統計が表示されます。

層ペインの **[ネットワーク]** 層で [ホスト] または [コネクション] のエントリをクリックして、ネットワーク層のリアルタイムモニタ画面を表示します。こうすることにより、メインペインが更新され、ネットワーク層のモニタ画面に以下のタブが表示されます。

[概要] タブ ネットワーク層で観測されたトラフィック全体に関するフレームレベルカウンタを表示します (171 ページ)。

[コネクション] タブ ネットワーク層で検出されたコネクションを、さまざまな統計値とともに一覧表示します (172 ページ)。

[ホスト] タブ ネットワーク層で検出されたノードを、さまざまな統計値とともに一覧表示します (177 ページ)。

[チャート] タブ 観測されたトラフィックのプロトコル構成、は応答時間の分布をグラフ表示します (179 ページ)。

[マルチキャスト] タブ 検出されたマルチキャストグループとサーバーをさまざまな統計値とともに一覧表示します (180 ページ)。

[概要] タブ (ネットワーク層)

[概要] タブには、ネットワーク層で観測されたトラフィック全体に関するさまざまなカウンタや統計値が表示されます。さまざまな TCP/IP トラフィック (IP、TCP、UDP、ARP、ICMP など) に関して、それぞれ別々のフレームカウンタと応答時間カウンタが備わっています。図 5-22 は、**[概要]** タブを示したものです。

層ペインでは現在 [ネットワーク] 層が選択されており、ネットワーク層情報を表示する複数のタブにアクセスできるようになっています。下図では、**[概要]** タブが選択されているため、観測されたネットワーク層トラフィック全体に関するさまざまなカウンタと統計値が表示されています。



説明	IPv4 概要	IPv6 概要	合計
IP マルチキャストフレーム	0	0	0
IP ブロードキャストフレーム	0	N/A	0
IP フレーム	4830	0	4830
IP バイト	1667732	0	1667732
ARP フレーム	44	N/A	44
ARP バイト	2890	N/A	2890
TCP フレーム	4788	0	4788
UDP フレーム	34	0	34
ICMP フレーム	8	0	8
その他のフレーム	0	0	0
事象	16	0	16
フロー	39	0	39
SYN 数	16	0	16
フラグメント数	0	0	0
再送数	15	0	15
タイムアウト数	0	0	0
Ping 数	0	0	0
開始時刻			2009/08/26 15:35:10
最終更新時刻			2009/08/26 15:42:19

図 5-22: ネットワーク層の [概要] タブ

[コネクション] タブ (ネットワーク層)

[コネクション] タブには、ネットワーク層で検出されたクライアントサーバー間の各コネクションに関するカウンタと統計値が表示されます。図 5-23 は、**[コネクション]** タブの例を示したものです。



図 5-23: ネットワーク層の [コネクション] タブ

図 5-23 に示すとおり、**[コネクション]** タブは次のように 2 つのペインに分割されています。

- 上のペインには、検出された各コネクションが以下の統計値とともに一覧表示されます。

[クライアント] コネクションのクライアント側のアドレス。

[サーバー]	コネクションのサーバー側のアドレス。
[プロトコル]	コネクションで使用されている上位層プロトコル。
[IPV6 パケットロス]	このコネクションでの IPV6 フラグメント損失数。 ClearSight は、20 パケットの深さまでのフラグメンテーション解析を保持しています。これは、ClearSight であるパケットの最初のフラグメントを受信したときに、さらに 19 パケットが到着する間は、パケット内の全てのフラグメントの到着を待つことを意味しています。パケット全体が到着しない場合は、ClearSight はパケットのフラグメントの損失を宣言します。 **注記 :** パケットは、先入れ先出しの手法でこのデータ構造から削除されます。
[IPV6 チェックサムエラー]	IPV6 チェックサムエラーを示している、このコネクションでの IPV6 パケットの総数。チェックサムエラーは、RFC 768 の標準のチェックサムアルゴリズムを使用して計算されます。 **注記 :** チェックサムのエラーカウントは、あるパケットのすべてのフラグメントを受信するまで増分されません。パケットの全てのフラグメントを受信していない場合、パケットのカウンタは増分されません。

注記 : [IPV6 パケットロス] と **[IPV6 チェックサムエラー]** の統計は、IPv6 マルチキャスト分析オプションを購入している場合に限って表示されます。

[事象]	コネクションに関連した事象の総数。層ペインの [ネットワーク] 層で **[事象]** カウンタをクリックすると、検出された事象がすべて表示されます。

[最大重要度] このコネクションで検出された最高レベルのアラートを示す色付きアイコン。

[平均応答時間] このコネクションですべてのクライアント要求に対してサーバーが応答するまでにかかった時間の平均。

[全フレーム数] このコネクションで観測されたフレームの総数。

[最終更新時間] ClearSight が前回このコネクションの統計を更新した時刻。

- 下のペインには、標準の **[会話]** タブと **[統計]** タブが含まれ、上のペインで選択したコネクションに関する情報が表示されます。**[会話]** タブと **[統計]** タブには、ネットワーク層特有のデータ以外は、[アプリケーション] 層の場合と同じタイプの情報が表示されます (詳細については 131 ページの「[会話] タブに関する情報」と 132 ページの「[統計] タブに関する情報」を参照)。

  一般的に、以下のことが言えます。

  - **[会話]** タブには、上のペインで選択されたコネクションを構成するクライアントとサーバー間におけるデータ交換が表示されます。**[会話]** タブでは、この情報が標準のネットワークラダーダイアグラムとして表示されるため、会話をその発生した順序で測定することが可能です。クライアントとサーバーはラダーのそれぞれ反対側に表示され、それぞれのアドレスまたはホスト名はペインのタイトルバーに表示されます。矢印は、フローにおけるメッセージの方向を示します。

    注記 : プルダウンメニューで **[ファイル]** > **[印刷]** と選択して、ラダー表示を印刷できます。

    また、会話のタイミングも次のように表示されます。

[デルタ時間] 表示されているメッセージとその前のメッセージの間の時間。

[相対時間] 表示されているメッセージとフローの最初のメッセージの間の時間。

  - **[統計]** タブには、上のペインで選択した接続のトラフィックに関する統計値や計測値が表形式で表示されます。ClearSight には、サーバー側とクライアント側のそれぞれに

おけるトラフィックのほか、コネクション全体のトラフィックについてのカウンタも含まれています (フレーム数、バイト数、エラー数など)。

[コネクション] タブにおけるアドレス表示の切り替え

[コネクション] タブの上部ペインを右クリックすると、**[クライアント]** と **[サーバー]** の各フィールドにおけるアドレスの表示方法を変更することができます。表示されたコンテキストメニューを使用すると、アドレス表示を IP アドレス、IP ホスト名、または MAC アドレスに変更することができます。

[コネクション] タブの自動キャプチャフィルタ

[コネクション] タブには、さまざまな自動キャプチャフィルタが備わっています。自動キャプチャフィルタにアクセスするには、[コネクション] タブの上部ペインでコネクションを右クリックします。これにより、コンテキストメニューが表示され、さまざまな自動キャプチャフィルタの中から選択できるようになります。自動キャプチャフィルタは、選択されたコネクションのアドレスとポートに使用できるほか、これらのアドレスとポートを別の組み合わせで使用してワイルドカード形式のフィルタ処理を行う際にも使用することができます。

[コネクション] タブの IPv6 フラグメンテーション解析

IPv6 マルチキャスト解析オプションが有効な ClearSight ユーザは、検出されたそれぞれの IPv6 マルチキャストフローに対する、フラグメントされたパケットロスと UDP チェックサムエラーについての情報が表示されます。これらの統計は、ネットワーク層のモニタ画面の **[コネクション]** タブに表示されます。

上記のように、**[パケットロス]** と **[チェックサムエラー]** カウンタは、**[コネクション]** タブの上部のペインに表示されます。これらのカウンタに加えて、下部のペインの **[統計]** タブは、**[不正な順序]** カウンタを提供します。このカウンタは、送信先に到着した少なくとも 1 つのフラグメントの順序が正しくなかったパケットの数を示します。ClearSight では、パケットの複数のフラグメントの到着順序が正しくなかった場合でも、パケットの **[不正な順序]** カウンタを 1 つだけ増分します。

正確なフラグメンテーション解析を保証するために、ClearSight では、それぞれのフラグメントの VLAN ID と フラグメント ID をチェックします。このようにすると、フラグメントが誤って別の親パケットに関連付けられることはありません。

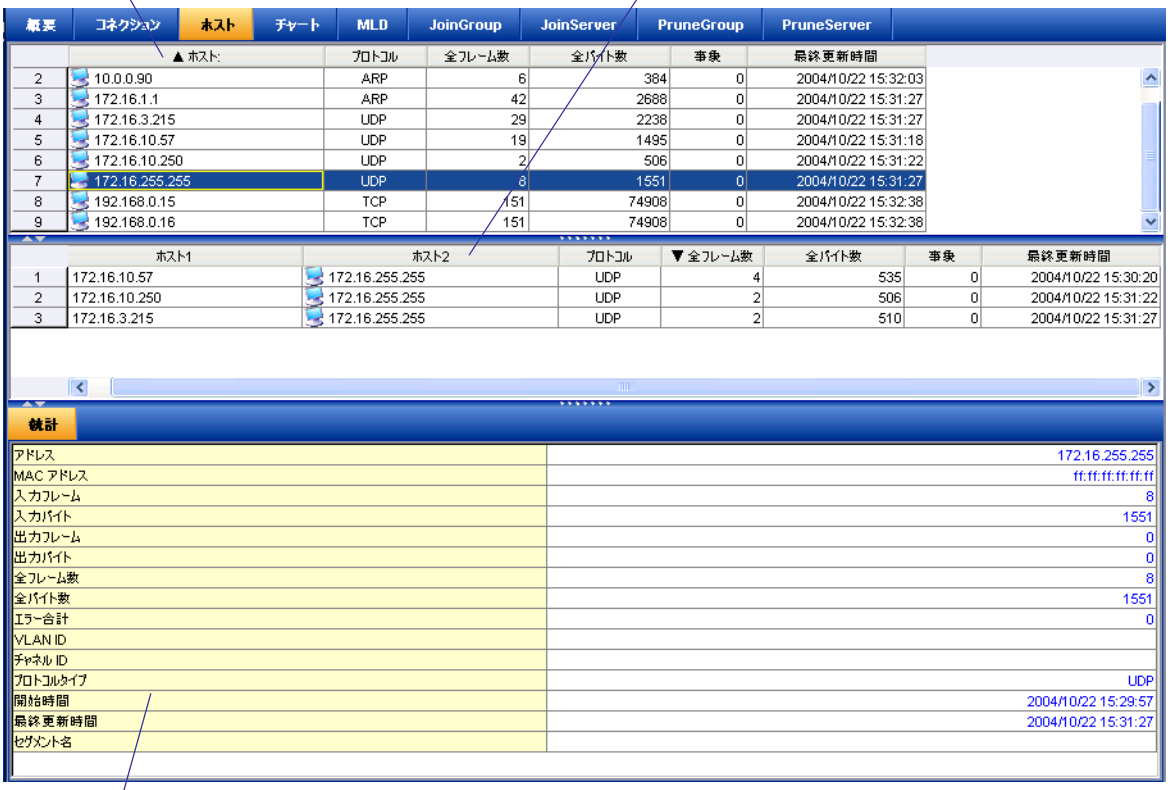
注記 : パケットと**フラグメント**は別のものです。パケットは、1 つまたは複数のフラグメントから構成されます。

[ホスト] タブ (ネットワーク層)

[ホスト] タブには、ネットワーク層で検出された各ホストのトラフィックに関するカウンタと統計値が表示されます。図 5-24 は、[ホスト] タブの例を示したものです。

上のペインには、検出されたホストがさまざまな統計値やカウンタとともに一覧表示されます。

中央のペインには、上のペインで選択したホストが参加したコネクションが一覧表示されます。この例では、上のペインでブロードキャストアドレスが選択されたため、複数のコネクションが一覧表示されています。



下のペインには、上のペインで選択したホストまたは中央のペインで選択したコネクションに関する統計が表示されます。

図 5-24: ネットワーク層の [ホスト] タブ

図 5-24 に示すとおり、**[ホスト]** タブは次のように 3 つのペインに分割されています。

- 上のペインには、検出された各ホストがそれについて観測されたトラフィックの統計値とともに表示されます。
- 中央のペインには、上のペインで選択したホストが参加したコネクションが一覧表示されます。各コネクションは、そのコネクション上のトラフィックに関するさまざまなカウンタが統計値とともに表示されます。
- 下のペインには、上と中央のどちらのペインが選択されているかに応じて、上のペインで選択したホストまたは中央のペインで選択したコネクションに関する統計が表示されます。

[ホスト] タブにおけるアドレス表示の切り替え

ペインを右クリックすると、**[ホスト]** タブでアドレスが表示される方法を変更することができます。表示されたコンテキストメニューを使用すると、アドレス表示を IP アドレス、IP ホスト名、または MAC アドレスに変更することができます。

[ホスト] タブの自動キャプチャフィルタ

[ホスト] タブには、さまざまな自動キャプチャフィルタが備わっています。自動キャプチャフィルタにアクセスするには、**[ホスト]** タブの上部の 2 つのペインでコネクションまたはホストを右クリックします。これにより、コンテキストメニューが表示され、さまざまな自動キャプチャフィルタの中から選択できるようになります。自動キャプチャフィルタは、選択されたホストまたはコネクションのアドレスとポートに使用できるほか、これらのアドレスとポートを別の組み合わせで使用してワイルドカード形式のフィルタ処理を行う際にも使用することができます。

[チャート] タブ (ネットワーク層)

[チャート] タブには、ネットワーク上のプロトコルの分布に関する広範な概要が表示されます。アプリケーション層とネットワーク層の両方のプロトコルに関する棒グラフには、どちらのプロトコルが帯域幅の大半を消費しているかが示されます。また、ネットワークで検出されたすべてのサーバーの応答時間をグラフで表示することもできます。

図 5-25 は、**[チャート]** タブの例を示したものです。

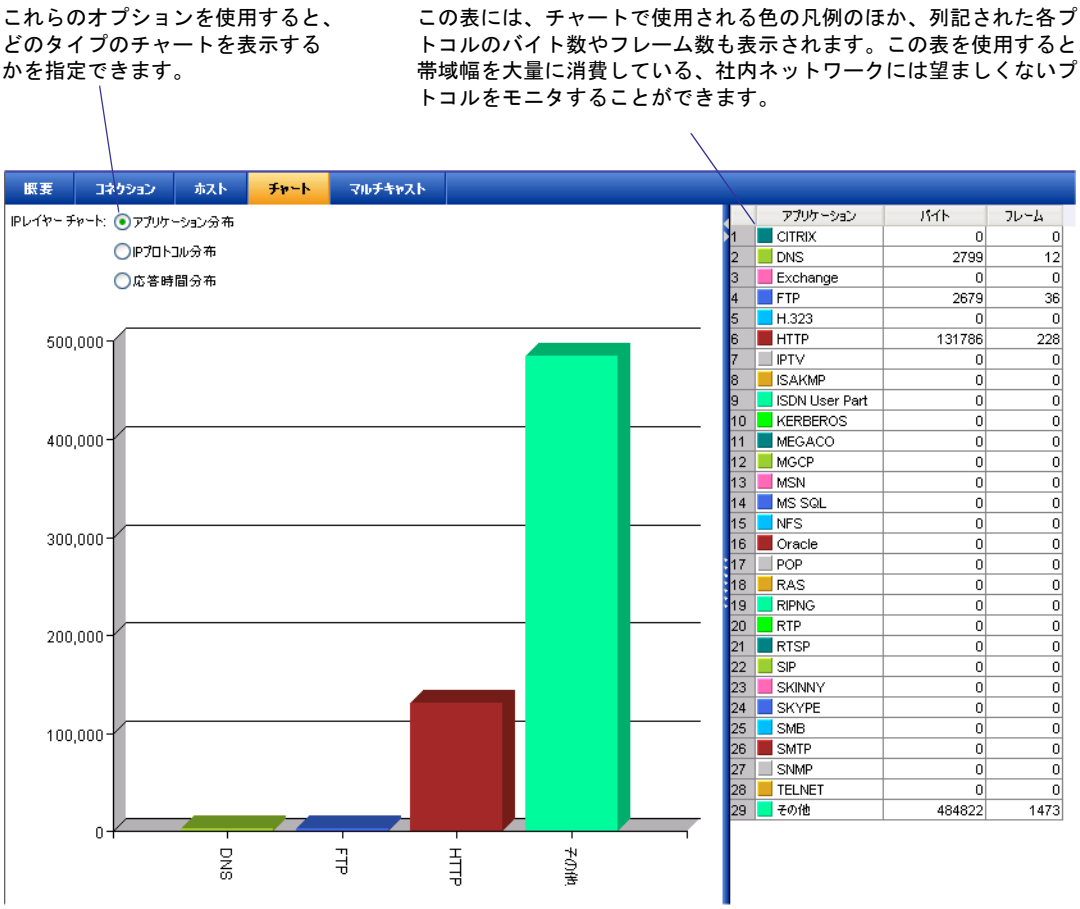


図 5-25: ネットワーク層の [チャート] タブ

[マルチキャスト] タブ (ネットワーク層)

[マルチキャスト] タブには、検出されたそれぞれのマルチキャストアドレスでのトラフィックを表示し定量化するカウンタと統計があります。ClearSight は、ホストが MLD ルータに送信したパケットから、マルチキャストグループアドレス (IPv4 の場合は IGMP、IPv6 の場合は MLD) を抽出します。図 5-26 に、**[マルチキャスト]** タブ内の **[グループ]** タブの例を示します。



図 5-26: ネットワーク層の [マルチキャスト] タブ

図 5-26 に示したように、**[マルチキャスト]** タブ内の **[グループ]** タブには、検出されたそれぞれのマルチキャストアドレスが以下の統計値とともに一覧表示されます。

[VLAN ID]	MLD Report または IGMP メッセージの送信元の VLAN (ある場合) の ID
[マルチキャストアドレス]	MLD または IGMP パケットから抽出されたマルチキャストアドレス
[フレーム]	このマルチキャストアドレスに送信されたフレームの数

[バイト]	このマルチキャストアドレスに送信されたバイト数
[開始時間]	このマルチキャストアドレスの最初の MLD Report または IGMP メッセージが検出された時間
[最終更新時間]	このマルチキャストアドレスの最新の MLD Report または IGMP メッセージが検出された時間
[Join 最大 (us)]	最初の Join パケットが発行された後のフロー開始のマルチキャストトラフィックにかかった最大時間
[Join 平均 (us)]	最初の Join パケットが発行された後のフロー開始のマルチキャストトラフィックにかかった平均時間
[Leave 最大 (us)]	最初の Leave パケットが発行された後のフロー停止のマルチキャストトラフィックにかかった最大時間
[Leave 平均 (us)]	最初 Join 最大 (us) の Leave パケットが発行された後のフロー停止のマルチキャストトラフィックにかかった平均時間

マルチキャストアドレスの代わりにサーバーアドレスが表示されることを除き、**[サーバ]** タブの統計情報は **[グループ]** タブと同じです。

予約済みの IPv6 マルチキャストアドレス

ネットワークでのマルチキャストトラフィックの解析のために ClearSight を使用した場合、特定の予約済み IPv6 アドレスが他のアドレスより頻繁に **[マルチキャスト]** タブに出現する場合があります。表 5-3 に、IPv6 マルチキャストトラフィックのモニタのために ClearSight を使用している場合に出現する、一般的な予約済み IPv6 マルチキャストアドレスの一部を示します。完全なリストについては、RFC 2373 を参照してください。

表 5-3: 一般的な予約済みの IPv6 マルチキャストアドレス

IPv6 マルチキャストアドレス	説明
FF02::1	**全てのノード**。同じリンクの全てのノードに到達するために使用されます。
FF02::2	**全てのルータ**。同じリンクの全てのルータに到達するために使用されます。
FF02::4	**DVMRP ルータ**。同じリンクの全ての DVMRP マルチキャストルータに到達するために使用されます。
FF02::5	**OSPF ルータ**。同じリンクの全ての OSPF ルータに到達するために使用されます。

物理層のモニタ

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

この項では、物理層における ClearSight のリアルタイムモニタ画面について説明します。物理層では、フレームタイプやエラータイプ (ブロードキャスト、マルチキャスト、CRC エラーなど) の数など、ネットワークデータの実際の転送状況について説明した統計が提供されます。カウンタは、グローバルな値に関しても、検出された個々の MAC アドレスに関しても表示されます。また、ClearSight では物理層の VLAN も測定されます。

物理層のリアルタイムモニタ画面を表示するには、層ペインの [物理] 層で任意のカウンタをクリックします。こうすることにより、メインペインが更新され、物理層モニタ画面の以下のタブが表示されます。

[概要] タブ 一般的なフレームタイプとエラータイプのカウンタが表示されます。また、リアルタイムの使用率とエラー数もグラフで表示されます (184 ページ)。

[VLAN] タブ 検出された VLAN がさまざまな統計値とともに一覧表示されます (185 ページ)。

[サブネット] タブ 検出されたサブネットをさまざまな統計値とともに一覧表示します (186 ページ)。

[ノード] タブ 検出された MAC ノードがさまざまな統計値とともに一覧表示されます (187 ページ)。

[チャート] タブ ネットワーク帯域幅の使用率を経過的に示したグラフが表示されます (188 ページ)。

[概要] タブ (物理層)

[概要] タブには、モニタセッション中に観測されたさまざまなタイプのフレームやエラーに関するカウンタが表示されます。また、ネットワーク使用率とエラー頻度の現在の値と履歴がリアルタイムでグラフに表示されます。図 5-27 は、**[概要]** タブの例を示したものです。

層ペインでは現在 [物理] 層が選択されており、**[概要]**、**[VLAN]**、**[サブネット]**、**[ノード]**、**[マトリクス]**、および **[チャート]** の各タブにアクセスできるようになっています。下図では、**[概要]** タブが選択されているため、モニタセッションのフレーム、エラー、使用率を示すカウンタとグラフが表示されています。



図 5-27: 物理層の [概要] タブ

[VLAN] タブ (物理層)

[VLAN] タブには、検出された各 VLAN で観測されたトラフィックに関するカウンタと統計値が表示されます。ClearSight は、802.1Q タグをリアルタイムで解析して、検出された VLAN に関する情報を提供します。

図 5-28 は、**[VLAN]** タブの例を示したものです。

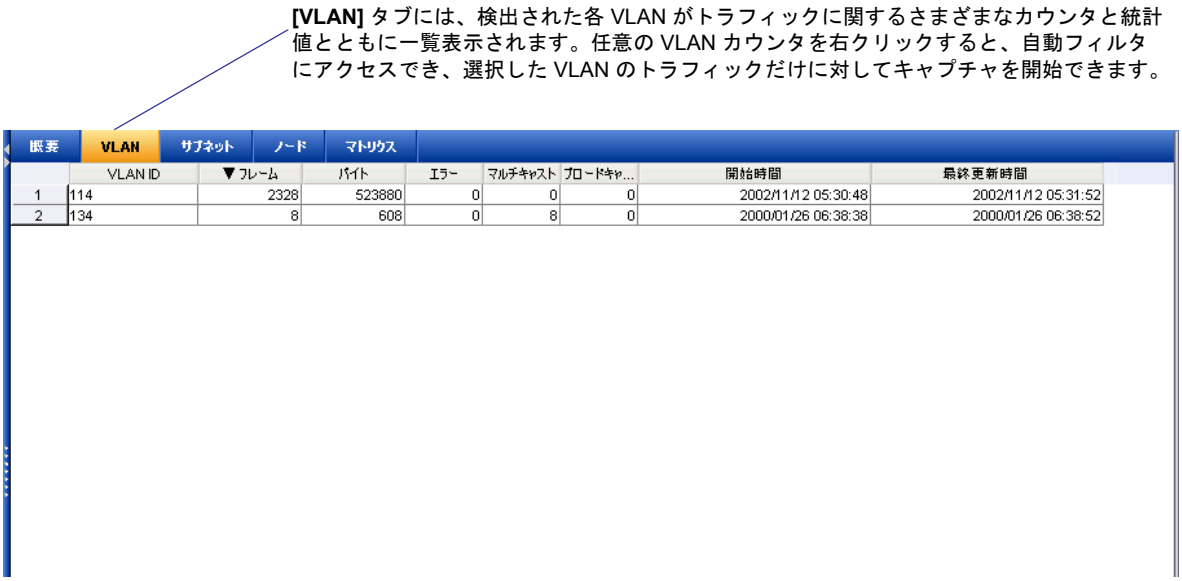


図 5-28: 物理層の [VLAN] タブ

[VLAN] タブの自動キャプチャフィルタ

[VLAN] タブに表示された任意の VLAN カウンタを右クリックし、表示されたコンテキストメニューから **[キャプチャ VLAN xx]** カウンタを選択すると、その VLAN に対してキャプチャを開始できます。

[サブネット] タブ (物理層)

[サブネット] タブには、検出されたそれぞれのサブネット上で見られるトラフィックを表示し定量化するカウンタと統計があります。

図 5-29 に **[サブネット]** タブの例を示します。

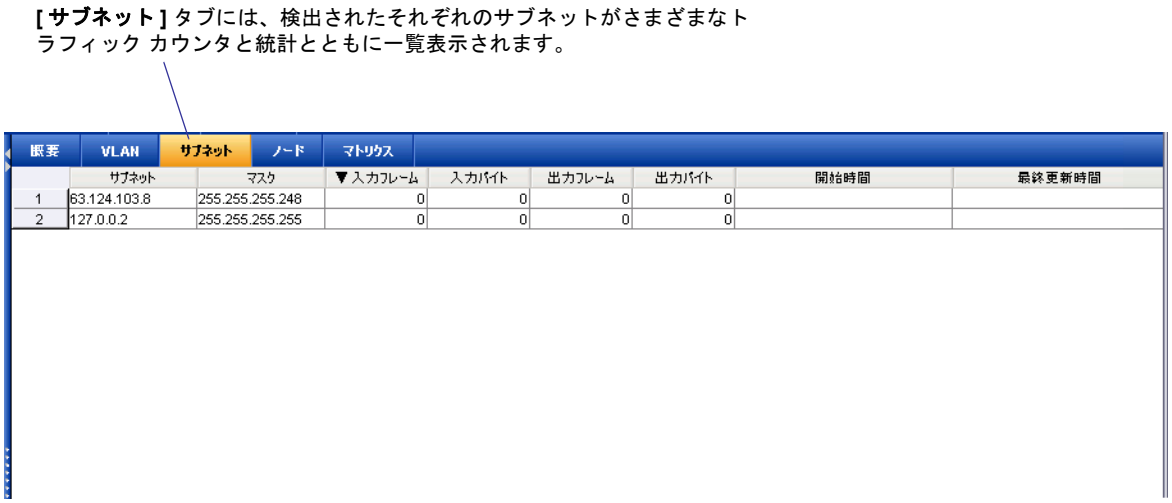


図 5-29: 物理層の [サブネット] タブ

[ノード] タブ (物理層)

[ノード] タブには、ネットワークで検出された各 MAC アドレスのトラフィックに関するカウンタと統計値が表示されます。図 5-30 は、[ノード] タブの例を示したものです。

[ノード] タブには、検出された各 MAC アドレスがノードのトラフィックに関するさまざまな統計値とともに一覧表示されます。大半の ClearSight 画面の場合と同様に、列見出しの統計をクリックすると、その統計を基準にして画面内のデータを並べ替えることができます。

概要 | VLAN | サブネット | ノード | マトリクス | チャート

	アドレス	VLAN ID	チャネル	プロトコル	▼ 入力フレーム数	出力フレーム数	受信バイト数	送信バイト数	エラー	開始時間	最終更新時間
1	Broadcast			IP ARP(2054)	8671	0	1206727	0	0	07/24/2006 15:54:22	07/24/2006 16:50:37
2	Compal:d7:43:1f			IP(2048)	927	1027	664447	87761	0	07/24/2006 15:54:33	07/24/2006 16:50:23
3	00:06:b1:27:1a:6c			IP(2048)	775	4276	61007	903560	0	07/24/2006 15:54:22	07/24/2006 16:50:40
4	01:00:5e:7f:ff:fa			IP(2048)	533	0	176839	0	0	07/24/2006 15:55:11	07/24/2006 16:50:12
5	00:0b:7d:1e:47:3b			IP(2048)	247	0	34413	0	0	07/24/2006 15:55:00	07/24/2006 16:50:10
6	00:13:ce:88:ff:45			IP(2048)	215	7	21738	759	0	07/24/2006 15:54:22	07/24/2006 16:50:40
7	09:00:07:ff:ff:ff			Apple EtherTa...	162	0	10368	0	0	07/24/2006 15:54:28	07/24/2006 16:50:05
8	Askey :a7:16:d7			IP(2048)	85	2	8808	692	0	07/24/2006 15:54:27	07/24/2006 16:48:33
9	01:00:0c:cc:cc:cc			CISCO CDP(8...	56	0	7280	0	0	07/24/2006 15:54:50	07/24/2006 16:49:51
10	Ibase :04:9b:ae			IP ARP(2054)	55	226	3056	16279	0	07/24/2006 15:54:39	07/24/2006 16:50:01
11	Intel :96:39:87			IP ARP(2054)	45	356	4320	43103	0	07/24/2006 15:55:07	07/24/2006 16:50:23
12	03:00:00:00:00:01			Unknown(611...	32	0	5432	0	0	07/24/2006 15:55:34	07/24/2006 16:49:06
13	01:00:5e:00:00:16			IP(2048)	27	0	1844	0	0	07/24/2006 15:55:31	07/24/2006 16:45:50
14	Ibase :05:28:4e			IP ARP(2054)	24	479	1987	36420	0	07/24/2006 15:54:24	07/24/2006 16:50:34
15	00:13:20:52:98:6b			IP(2048)	22	51	2766	8129	0	07/24/2006 15:54:28	07/24/2006 16:45:21
16	00:0f:1f:1d:4c:ac			IP ARP(2054)	21	67	2619	9675	0	07/24/2006 15:55:35	07/24/2006 16:48:30
17	01:00:5e:7f:ff:fd			IP(2048)	16	0	1632	0	0	07/24/2006 16:03:31	07/24/2006 16:48:45
18	33:33:00:00:00:01			IPV6(34525)	11	0	1166	0	0	07/24/2006 15:56:55	07/24/2006 16:46:08
19	00:14:a4:d1:34:98			IP ARP(2054)	10	7	928	793	0	07/24/2006 15:55:09	07/24/2006 16:32:29
20	Xerox :87:07:aa			IP ARP(2054)	9	179	876	23901	0	07/24/2006 15:54:22	07/24/2006 16:50:01
21	01:00:5e:00:01:18			IP(2048)	2	0	130	0	0	07/24/2006 16:01:11	07/24/2006 16:41:12
22	01:00:5e:7f:02:02			IP(2048)	1	0	95	0	0	07/24/2006 16:28:26	07/24/2006 16:28:26
23	00:0b:db:28:43:d4			IP(2048)	0	81	0	9606	0	07/24/2006 15:54:27	07/24/2006 16:50:23
24	00:0b:5d:01:29:a9			IP ARP(2054)	0	38	0	3966	0	07/24/2006 15:54:27	07/24/2006 16:49:17

図 5-30: 物理層の [ノード] タブ

[ノード] タブの自動キャプチャフィルタ

[ノード] タブに表示された任意のノードカウンタを右クリックし、表示されたコンテキストメニューから **[XX (MAC アドレス) をキャプチャする]** カウンタを選択すると、そのノードに対してキャプチャを開始できます。

[チャート] タブ (物理層)

[チャート] タブには、ネットワークの使用率に関する広範な概要が表示されます。ClearSight では、「チェック間隔」と呼ばれる指定期間におけるネットワークの使用率が測定されます。ClearSight は、各チェック間隔のネットワーク使用率を測定し、それを物理層の **[チャート]** タブに記録します。このチャートには、ネットワークの使用率が指定した範囲内にあるチェック間隔の数が示されます。使用率の各範囲におけるチェック間隔の数は、**[チャート]** タブの右側の表の **[発生回数]** 列に表示されます (図 5-31)。

注記 : チェック間隔の値は、**[設定]** ボタン > **[設定]** タブ > **[共通]** > **[モニタ設定]** ページで指定します (詳細については 192 ページの「[共通]>[モニタ設定]」を参照してください)。

図 5-31 は、**[チャート]** タブの例を示したものです。

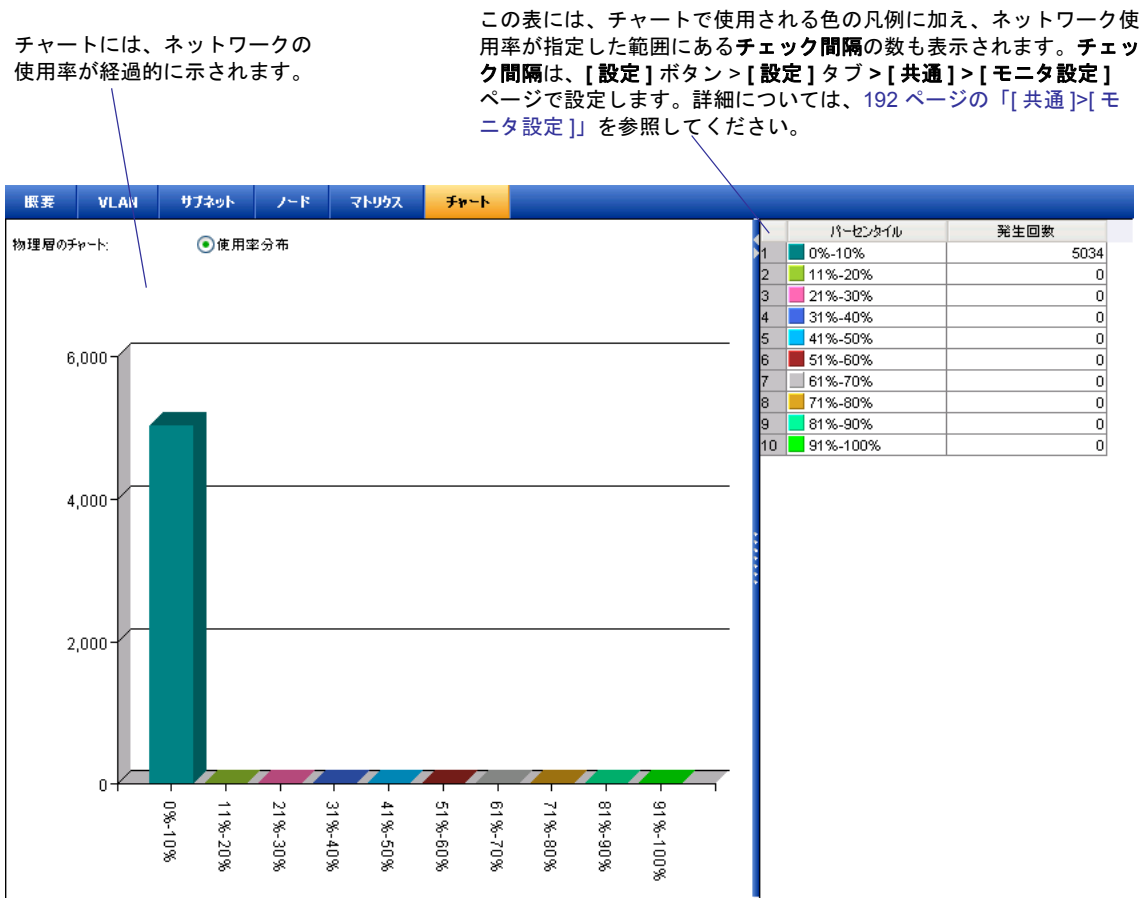


図 5-31: 物理層の [チャート] タブ

ClearSight Analyzer の設定

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSight Distributed

この項では、ClearSight Analyzer の動作に影響を与える設定を行う方法について説明します。設定を行うには、以下を実行します。

ClearSight Analyzer のオプションを設定するには、以下を実行します。

1. ツールバーの **[設定]** ボタンをクリックします。
2. **[設定]** タブをクリックします。
3. 画面左側のメニューで、設定するオプションを選択します (図 5-32)。



図 5-32: 設定

[共通]>[プロトコル設定]

[共通] > [プロトコル設定] オプションを使用すると、以下のことを実行できます (190 ページの図 5-32)。

- ClearSight によってモニタされるプロトコルのリストに、ポートとプロトコルのカスタムの組み合わせを追加できます。
- ClearSight によって標準のプロトコルが観測されることが期待されているポートを編集できます。
- アプリケーション層の [概要] タブに表示するプロトコルを選択できます。

[プロトコル設定] オプションは、非標準のポートで独自のプロトコルや標準のプロトコルを実行しているネットワークの場合に役に立ちます。

[プロトコル設定] を選択すると、ClearSight でモニタするよう現在設定されているプロトコルとポートの組み合わせが一覧表示されます。ClearSight では、一般的なプロトコルに対して既知のポートが使用されます。ただし、この画面のオプションを使用すると、カスタムプロトコルをリストに追加したり、既存のプロトコルとポートの組み合わせを変更したり、プロトコルを完全に削除したりすることができます。

注記 : カンマで区切って複数のポートを指定したり (80,443 など)、ポートの範囲を指定することができます (1720-1729 など)。

目的のアプリケーションの **[概要ページに表示]** チェックボックスをオンまたはオフにして、**アプリケーション**層の **[概要]** タブにプロトコルを表示するかどうかを指定します。ただし、ClearSight で基本とみなされているアプリケーションがあり、この画面でそれらのアプリケーションを無効にすることはできません。これらのアプリケーションに関しては、113 ページの「表示するアプリケーションの選択」に説明されている無効 / 有効の手順に従ってください。

カスタムプロトコルを追加している場合は、**[削除]** 列にゴミ箱型のアイコンが表示されます。このアイコンをクリックすると、行全体が削除されます。

注記 : プロトコルとポートエントリの変更は直ぐに反映されますが、新規に追加したプロトコルが、サマリページ上でアルファベット順に配置されるためには、アプリケーションを再起動する必要があります。

[共通]>[モニタ設定]

※モニタ設定は、ClearSight Analyzer Light には搭載されていない機能になります。

[共通]>[モニタ設定]（194 ページの図 5-33）を使用して、以下のことを実行できます。

- モニタに入ってくるすべてのパケットに適用されるフィルタを選択します。フィルタが現在選択されている場合、**[フィルタ]** 領域にそのフィルタの名前が表示されます。フィルタの選択を解除するには、**[削除]** ボタンをクリックします。フィルタ名が **[なし]** に置き換えられ、フィルタが現在適用されていないことを示します。ボタンの名前は **[設定]** に変わり、新しいフィルタを設定 (選択) できることを示します。

  [設定] ボタンをクリックすると、**[フィルタリスト]** ダイアログボックス (図 9-31) が表示されます。ここで、現在定義されているフィルタのリストから使用したいフィルタを選択できます。

  左下にある **[作成]** ボタンをクリックして、新しいフィルタを作成することができます。新しいフィルタの作成方法や既存のフィルタの編集方法については、第 9 章「フィルタの使用」を参照してください。

- ClearSight がリアルタイムの統計値をモニタし、平均値を算出する間隔を秒単位で指定します。これは、**[間隔] > [チェック]** オプションによって指定できます。デフォルト値は 5 秒です。

  このオプションを使用すると、ClearSight のリアルタイムモニタによって表示する統計値の測定間隔を変更できます。値が大きいほど統計値の偏差が少なくなり、値が小さいほど一時的なバーストによって、統計値が高く表示されてしまう場合があります。一般的に、デフォルト値である 5 秒に近い値を設定すると、最適な結果を得ることができます。

- ClearSight がアプリケーションのスループットをモニタし、その平均値を算出する間隔を、秒単位で指定します。これは、**[間隔] > [スループット]** オプションによって指定できます。デフォルト値は 1 秒です。トラフィックが存在する場合、アプリケーション層の [概要] 画面 (112 ページの図 5-1 を参照) に表示されるスループットは現在値と平均値の間で切り替わります。現在値は、[スループット間隔] で算出された平均値の最新のスループット測定値です。トラフィックが存在しない場合は、そのモニタセッショ

ンの開始以降の平均スループットである平均値だけが表示されます。

このオプションを使用すると、ClearSight のリアルタイムモニタによって表示されるスループット値の測定間隔を変更できます。値が大きいほど統計値の偏差が少なくなり、値が小さいほど一時的なバーストによって、統計値が高く表示されてしまう場合があります。一般的に、デフォルト値である 1 秒に近い値を設定すると、最適な結果を得ることができます。

- 個々の「ラダー表示」できる「段」の最大数を指定します。この数は、アプリケーションやコネクションなどに対して個別に設定することができます。
- ClearSight が測定する「ネットワークコネクション」のフローの最大数を指定します。
- ClearSight で統計を維持するアプリケーションのタイプ別にサーバーとフローの最大数を指定できます。特定のタイプのサーバーまたはフローの上限値に到達すると、ClearSight は新しいサーバーやフローのカウンタをモニタ画面で作成しなくなります。

  ヒント：これらのオプションは、ClearSight のパフォーマンスのためにも、最も重要なサーバーとフローのタイプのために使用してください。ClearSight でモニタするよう指定するサーバーとフローの数が多いほど、消費される ClearSight PC のリソースも多くなります。モニタ用リソースは、最も重要なサーバーとフローに割り当ててください。

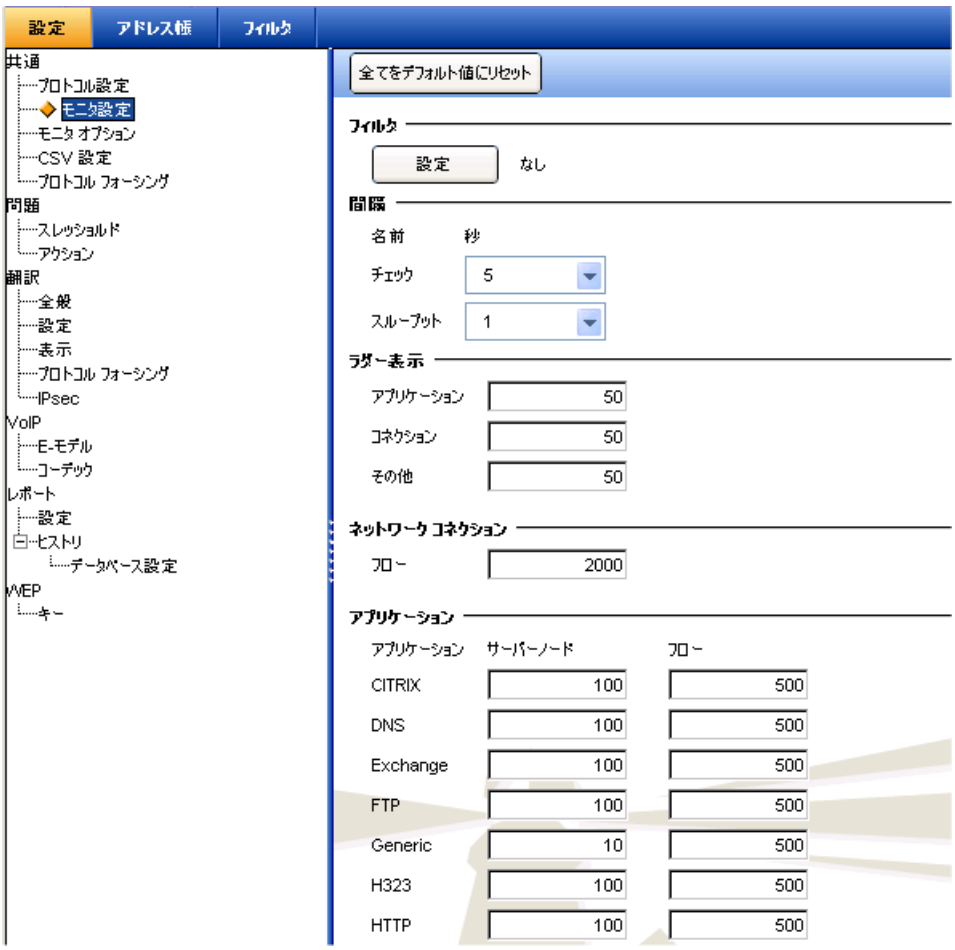


図 5-33: [モニタ設定] 設定画面

モニタオプション

各層 (**アプリケーション**、**ネットワーク**、および**物理層**) でどの統計値を収集するかを指定するには、**[共通] > [モニタ オプション]** (図 5-34) を使用します。収集する統計値のチェックボックスはオンにし、収集しない統計値のチェックボックスはオフにします。



図 5-34: [モニタオプション] 設定画面

アプリケーション層のオプション

※アプリケーション層のオプションは、ClearSight Analyzer Light には搭載されていない機能になります。

[アクティブなアプリケーションのみを表示する (概要)] チェックボックスによって、アプリケーション層の [概要] 画面にアクティブなアプリケーションのみがデフォルトで表示されるように設定することができます。ただし、113 ページの「表示するアプリケーションの選択」に説明されているように、このデフォルト表示は、「アクティブなアプリケーションのみ表示」するか「全てのアプリケーションを表示」するかを切り替えることができます。

[全てのアプリケーションを有効にする] チェックボックスでは、アプリケーション情報の処理および表示をするかどうかを指定することができます。これは、不要なアプリケーション情報がある場合に便利な機能で、必要な統計に対する ClearSight のパフォーマンスを向上させます。このチェック全てのアプリケーションを有効にするボックスをオフにすると、すべてのアプリケーションが無効になります。このチェックボックスをオンにすると、有効になっている全てのアプリケーションが復元されます。

[HTTP の子フローを表示する] チェックボックスでは、HTTP フローの下に子フローを表示するかどうかを制御することができます。このオプションは、モニタ、キャプチャ、および翻訳機能に影響を与えます。

ネットワーク層と物理層のオプション

ネットワーク層または物理層の特定のタイプの統計が不要であることがわかっている場合は、その統計の収集を無効にして、必要な統計に対する ClearSight のパフォーマンスを向上させることができます。ClearSight を再起動すると、選択を解除した統計のタブは表示されますが、「この機能は現在無効になっています」と表示されます。

ジャンボフレームの指定

Ethernet フレームが 1518 バイト (VLAN ID を含む場合は 1522 バイト) よりも大きい場合は、通常そのフレームはオーバーサイズまたはジャバーフレームに分類されます。しかし、**[設定] > [設定] > [共通] > [モニタオプション] > [物理層]** 画面で、**[ジャンボフレーム]**

フィールドに 1518 (または 1522) よりも大きい値を指定することができます。その場合は、1518 (または 1522) バイトよりも大きく、かつユーザが指定した値に等しいまたはそれ以下のフレームは、ジャンボフレームに分類されます。そのようなフレームに CRC エラーがある場合は、CRC カウントに含まれます。

[ジャンボフレーム] ドロップダウンリストから 4 つの値 (2047, 4085, 8191, 9018) の 1 つを選択できます。

チェックサムメッセージ表示の抑制

最近のネットワークカードの中にはパフォーマンス向上のためにチェックサム計算を行わないオプションを持つものがあります。さらにいくつかのカードではこのオプションさえ持たないものもあります。このような場合でも、ドライバは常にチェックサム計算をカードに任せています。これらのネットワークカードを使用すると、ClearSight は多くのパケットにチェックサムエラーを示すフラグを付けてしまいます。

これを改善するためのオプションを新たに導入しました。**[設定] > [設定] > [共通] > [モニタオプション] > [物理層]** 画面で、**[チェックサム計算を有効にする]** のチェックを外すと、チェックサムメッセージ表示を抑制することができます。

短期間ヒストリ

[短期間ヒストリ] を有効にすると、**[物理層]** の **[概要]** タブがトレンドチャートが表示されたヒストリビューに切り替えられます。ドロップダウンリストで、サンプル数とサンプルの時間間隔を選択することができます。

注記 : [短期間ヒストリ] はリアルタイムモニタに適用されます。ポストキャプチャアナリシスには適用されません。

注記 : [モニタオプション] に対して加えた変更は、ClearSight を再起動するまで有効になりません。

CSV 設定

[共通] > **[CSV 設定]** (図 5-35) の **[設定]** 領域を使用して、次の項目を指定します。

- ClearSight の統計が自動的に CSV (comma-separated values) ファイルにエクスポートされる
- チェックされた統計情報がエクスポートされる頻度

チェックボックスにチェックが付けられた統計情報がエクスポートされ、チェックが付けられていない統計情報はエクスポートされません。更新間隔フィールドでエクスポート間隔を指定します。

[保守] 領域では、指定した日数より前の CSV ファイルを自動的に消去するように設定することができます。**[今すぐパージ]** をクリックして、保存されているすべての CSV ファイルを消去することもできます。

※ Pim-Sm 統計は、ClearSight Analyzer Light には搭載されていない機能になります。

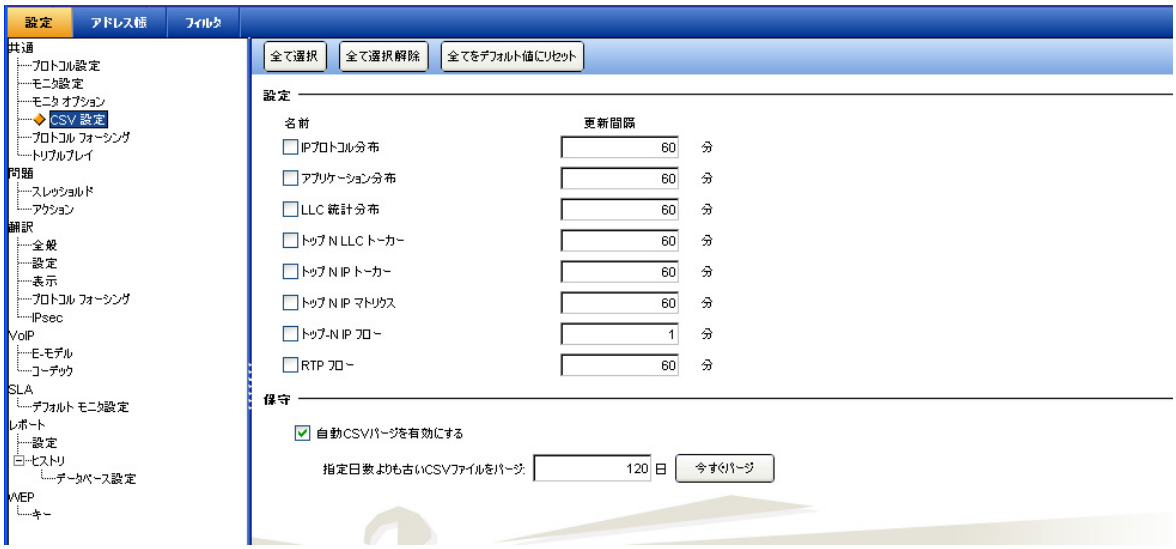


図 5-35: [CSV 設定]

プロトコルフォーシング [共通]>[プロトコルフォーシング] オプション

図 5-36 に **[共通]** > **[プロトコルフォーシング]** 画面を示します。



図 5-36: [共通] > [プロトコルフォーシング] 設定画面

[有効 / 無効]

[有効 / 無効] 領域では、プロトコルフォーシングのオン / オフを切り替えることができます。**[無効]** を選択した場合は、他の領域でさらにオプションを設定できますが、この領域で **[有効]** を選択するまでは設定が有効になりません。

[パターン]

[パターン] 領域では、プロトコルフォーシングのためにマッチさせるパターンを入力することができます。入力するオフセットは、常にフレームの先頭からになります。

パターン入力は 16 進でなければなりません。パターンマッチを有効にするには、**[パターンマッチ]** ボックスをオンにします。

[開始場所] および [スキップオフセット]

[開始場所] 領域では、強制プロトコルの検索を開始する場所を ClearSight に指示することができます。

- **[フレームの開始]** を選択した場合、ClearSight の検索場所はフレームの先頭に **[スキップオフセット]** をプラスしたところになります。
- **[IP の開始]** を選択した場合、ClearSight の検索場所は IP スタックの先頭に **[スキップオフセット]** をプラスしたところになります。

[強制プロトコルタイプ]

[強制プロトコルタイプ] 領域では、ドロップダウンリストから強制プロトコルを選択することができます。リストの内容は、**[開始場所]** 領域で行った選択と相関関係があることに注意してください。

問題のしきい値

[問題] > **[スレッショルド]** を使用して、次の操作を行います。

- ClearSight が平均値を算出する間隔をそれに対応するしきい値と比較する前に、ミリ秒単位で指定します。これは、**[更新間隔]** オプションによって指定できます。デフォルト値は 1 秒です (1000 ミリ秒)。

  このオプションを使用すると、ある状態を問題として特定する際に使用する測定間隔を変更できます。値が大きいほど統計値の偏差が少なくなり、値が小さいほど一時的なバーストによって、統計値が高く表示されてしまう場合があります。一般的に、デフォルト値である 1000 ミリ秒に近い値を設定すると、最適な結果を得ることができます。
- 問題の種類を定義する実際のしきい値を設定する。詳細については、344 ページの「問題レポートスレッショルドの設定」を参照してください。

問題のアクション

[問題] > **[アクション]** を使用して、問題が検出されたときの ClearSight の動作を指定します。詳細については、334 ページの「重要度とアクションの定義」を参照してください。

翻訳

[翻訳] 削除にあるオプションは、ポストアナリシスの **[翻訳]** タブに影響します。詳細については、246 ページの「[翻訳] タブの設定オプション」を参照してください。

VoIP E- モデル

[VoIP] > **[E- モデル]** (図 5-37) を使用して、VoIP フローの R 値の計算で使用するパラメータの値を指定します。

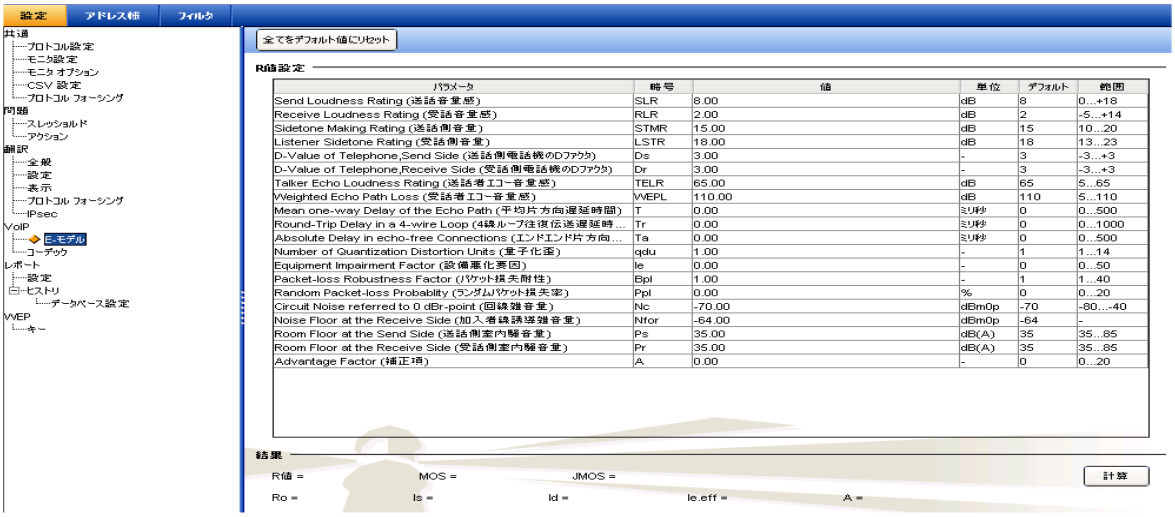


図 5-37: E- モデルの計算

VoIP コーデック

[VoIP] > **[コーデック]** を使用して、**AMR** を **GSM** と **3GPP** のどちらにするかを指定します。

レポートの設定

[レポート] > **[設定]** を使用して、レポートの書式をカスタマイズし、顧客識別情報を追加します。詳細については、381 ページの「レポート形式の制御」を参照してください。

ヒストリレポートのデータベース設定

[レポート] > **[ヒストリ]** > **[データベース設定]** を使用して、ヒストリレポータが累計するデータと、そのデータを保持する期間を指定します。詳細については、381 ページの「レポート形式の制御」を参照してください。

WEP キー

[WEP] > **[キー]** を使用して、無線トラフィック用の WEP 暗号化キーを「128 ビット」、「64 ビット」、または「なし」のいずれにするかを指定します。

[アドレス帳] タブ

[アドレス帳] タブを使用して、アドレス帳を作成します。詳細については、374 ページの「アドレス帳の使用」を参照してください。

[フィルタ] タブ

[フィルタ] タブを使用して、**[ここをクリックして]** ボタンをクリックして **[フィルタリスト]** ダイアログボックスを開きます。このダイアログボックスで **[作成]** ボタンをクリックして、**[新規フィルタ]** ダイアログボックスにアクセスし、新しいフィルタを作成することができます。詳細については、284 ページの「定義済みフィルタの使用」を参照してください。

ウィンドウスタイルの変更

[ツール] メニューから **[ルックアンドフィール]** を選択することにより、ClearSight のウィンドウの外観を変更することができます。図 5-38 に利用可能なウィンドウスタイルを示します。



図 5-38: [ルックアンドフィール] ダイアログボックス

第 6 章

ClearSight を使用したデータのキャプチャ

この章では、ClearSight を使用してデータをキャプチャする方法について説明します。この章は、以下の項目で構成されています。

- 「キャプチャについて」
- 「キャプチャワークスペース」
- 「実行中のキャプチャの観察」

キャプチャについて

ClearSight Application Flow Analyzer ClearSight Analyzer Light ClearSignt Distributed

リアルタイムモニタとは対照的に、ClearSight のキャプチャ機能では、キャプチャフィルタを通過したトラフィックはキャプチャバッファに格納され、ポストキャプチャアナリシスが行われます。データをキャプチャすると、難解なネットワーク問題を解決するために必要な、詳細な情報を取得することが可能です。キャプチャされたデータのバッファまたはトレースファイルを取得したら、ClearSight のポストキャプチャアナリシス機能 (第 7 章「ポストキャプチャアナリシス」を参照) を使用して、ネットワークの状況を把握することができます。

[ファイル] メニューのコマンドを使用して、まだキャプチャバッファに含まれているフレームのトレースファイルを保存し、あとでポストキャプチャアナリシスに使用することもできます。また、キャプチャバッファに新たにキャプチャされたデータに対しても、トレースファイルに対する場合と同様にポストキャプチャアナリシス機能が実行されます。

キャプチャワークスペース

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

ほかの ClearSight 機能と同様に、キャプチャ機能は、ツールバーを使用して使うことができます。ツールバーには、キャプチャの開始と停止のほか、キャプチャの結果をさまざまなポストキャプチャアナリシスページで表示するためのコントロールが備わっています。

キャプチャワークスペースを表示するには、ツールバーの **[キャプチャ]** (図 6-1) ボタンをクリックします (図 6-2)。

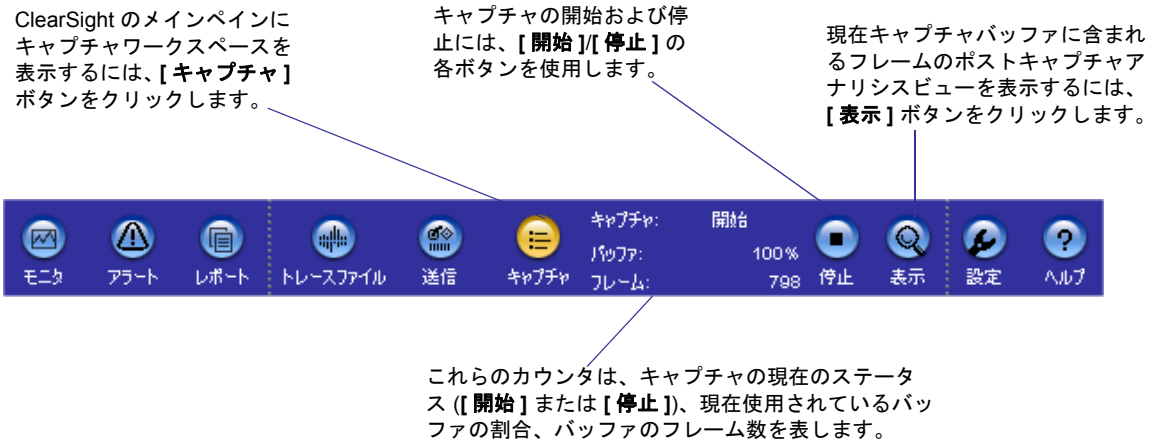


図 6-1: ツールバーのキャプチャコントロール

キャプチャワークスペースには、層ペインの標準のカウンタのほかに追加の **[キャプチャ]** 層も表示されます。**[キャプチャ]** 層の計器からは、バッファのステータスに関する情報を一目で把握することができます。層ペインの **[キャプチャ]** カウンタをクリックすると、キャプチャワークスペースがメインペインに表示されます。

キャプチャワークスペースには複数のタブが含まれ、これらを使用すると、実行中のキャプチャに関する統計値表示、フィルタの作成 / 選択、バッファ設定の調整、層ペイン内のビューのカスタマイズ、トリガの作成 / 選択、事象や問題の表示を行うことができます。

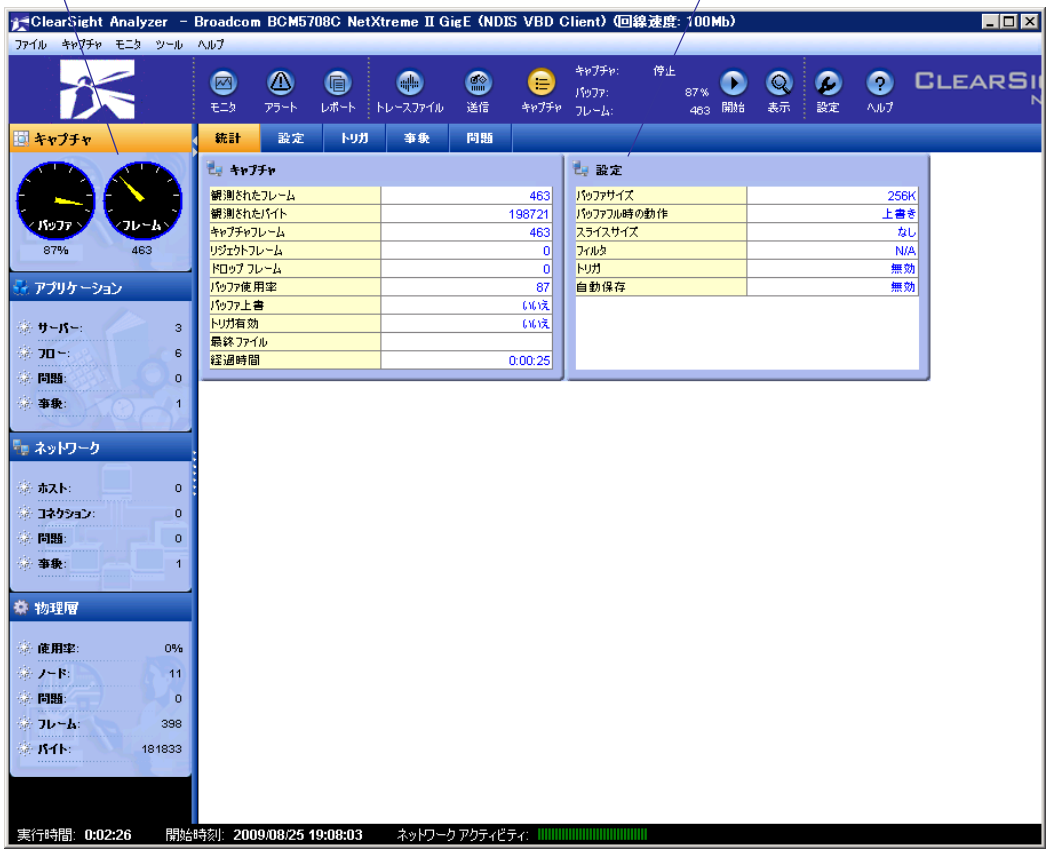


図 6-2: キャプチャワークスペース

キャプチャワークスペース (208 ページの図 6-2) は、以下のタブで構成されています。

[統計] **[統計]** タブには、**[キャプチャ]** ペインと **[設定]** ペインの 2 つのペインがあります。**[キャプチャ]** ペインには、実行中のキャプチャに関する統計、またはキャプチャが停止されている場合は、キャプチャバッファの内容に関する統計が表示されます。**[設定]** ペインには、現在のバッファの設定のサマリが表示されます。これらの設定は、**[設定]** タブのパラメータを調整して変更することができます。詳細については、210 ページの「[統計] タブ」を参照してください。

[設定] キャプチャプロセスに関連するさまざまな設定情報を確認することができます。

- 次回のキャプチャセッションで使用するフィルタを選択できます。また、新しいフィルタを作成することもできます。
- キャプチャのバッファ管理オプションを設定できます。
- 層ペイン内のビューをカスタマイズできます。

詳細については、211 ページの「[設定] タブ」を参照してください。

[トリガ] キャプチャの開始および停止のタイミングを決定する特定の条件を設定することができます。詳細については、219 ページの「[トリガ] タブ」を参照してください。

[事象] 現在のキャプチャセッション中に検出された事象がレポートされます。ただし、現在のキャプチャフィルタを通過したパケットに関する事象のみです。詳細については、129 ページの「[事象] タブに関する情報」を参照してください。

[問題] 現在のキャプチャセッション中に検出された問題がレポートされます。ただし、現在のキャプチャフィルタを通過したパケットに関する問題のみです。詳細については、130 ページの「[問題] タブに関する情報」を参照してください。

[統計] タブ

表 6-1 に、**[統計]** タブの **[キャプチャ]** ペインのカウンタの説明を示します。これらのカウンタには、現在実行中のキャプチャに関する値、またはキャプチャが停止されている場合は、現在キャプチャバッファにあるフレームに関する値が表示されます。

表 6-1: [統計] タブの [キャプチャ] ペインのカウンタ

カウンタ	説明
[観測されたフレーム]	このキャプチャセッション中にネットワーク上で観測されたフレームの数。
[観測されたバイト]	このキャプチャセッション中にネットワーク上で観測されたバイトの数。
[キャプチャフレーム]	このキャプチャセッション中にネットワークからコピーされ、キャプチャバッファに格納されたフレームの数。
[リジェクトフレーム]	観測されたが、キャプチャフィルタが原因でキャプチャされなかったフレームの数。
[ドロップフレーム]	このキャプチャセッション中にドロップされたフレームの数。ギガビット SC1 カードまたはギガビット XD カードでは、フレームの処理中に例外が発生した場合にカウントされます。それ以外のカードでは、これに加え ClearSight 内部のバッファがオーバーランした場合にもカウントされます。
[バッファ使用率]	キャプチャ済みデータによって現在占有されているキャプチャバッファの割合。
[バッファ上書き]	キャプチャバッファがすでに上書きされているかどうか ([はい] または [いいえ])。
[トリガ有効]	トリガによりキャプチャが開始または停止したかどうか ([はい] または [いいえ])。

表 6-1: [統計] タブの [キャプチャ] ペインのカウンタ

カウンタ	説明
[最終ファイル]	最後にバッファが保存された際に使用されたファイル名。
[経過時間]	キャプチャを開始してから経過した時間の長さ。

[設定] タブには、バッファの設定の現在の値が一覧表示されます。これらの値は、**[設定]** タブで選択を行って変更することができます。詳細については、211 ページの「[設定] タブ」を参照してください。

[設定] タブ

キャプチャを開始する前に、**[設定]** タブのオプションを設定して、キャプチャバッファのパフォーマンスを、ネットワーク解析ニーズに合わせて調節します。データのキャプチャが完了したときに、ポストキャプチャアナリシスで使用するフレームがまだバッファに含まれている場合があるため、これらのオプションは慎重に設定する必要があります。

図 6-3 は、**[設定]** タブを示しています。



図 6-3: [設定] タブ

図 6-3 に示すとおり、以下を設定できます。

- [フィルタ] (213 ページ)
- [バッファサイズ] (214 ページ)
- [バッファフル時のアクション] (214 ページ)
- [スライスサイズ] (215 ページ)
- [自動保存] (216 ページ)
- [オプション] (217 ページ)

フィルタの選択

[設定] タブの **[フィルタ]** 項目を使用すると、キャプチャセッションに適用するキャプチャフィルタを選択することができます。キャプチャバッファにどのフレームが格納されるかを制限するキャプチャフィルタは、必要なデータに対してのみキャプチャを集中させることができる手段を提供します。

ClearSight のポストキャプチャアナリシス機能は、キャプチャ機能によって収集されたデータに依存しています。しかし、近頃のネットワークでは帯域幅が大きく速度も速いため、キャプチャバッファは必要のないデータで容易にいっぱいになってしまいます。このような場合にキャプチャフィルタを使用すると、ClearSight の観測の対象を絞り、必要なデータだけを検証して、不要なデータは無視することができます。

フィルタが現在選択されている場合、**[フィルタ]** 項目にそのフィルタの名前が表示されます。フィルタの選択を解除するには、**[削除]** ボタンをクリックします。フィルタ名が **[なし]** に置き換えられ、フィルタが現在適用されていないことを示します。ボタンの名前は **[設定]** に変わり、新しいフィルタを設定 (選択) できることを示します。

[設定] ボタンをクリックすると、**[フィルタリスト]** ダイアログボックス (図 6-4) が表示されます。ここで、現在定義されているフィルタのリストから使用したいフィルタを選択できます。

左下にある **[作成]** ボタンをクリックして、新しいフィルタを作成することができます。新しいフィルタの作成方法や既存のフィルタの編集方法については、第 9 章「フィルタの使用」を参照してください。

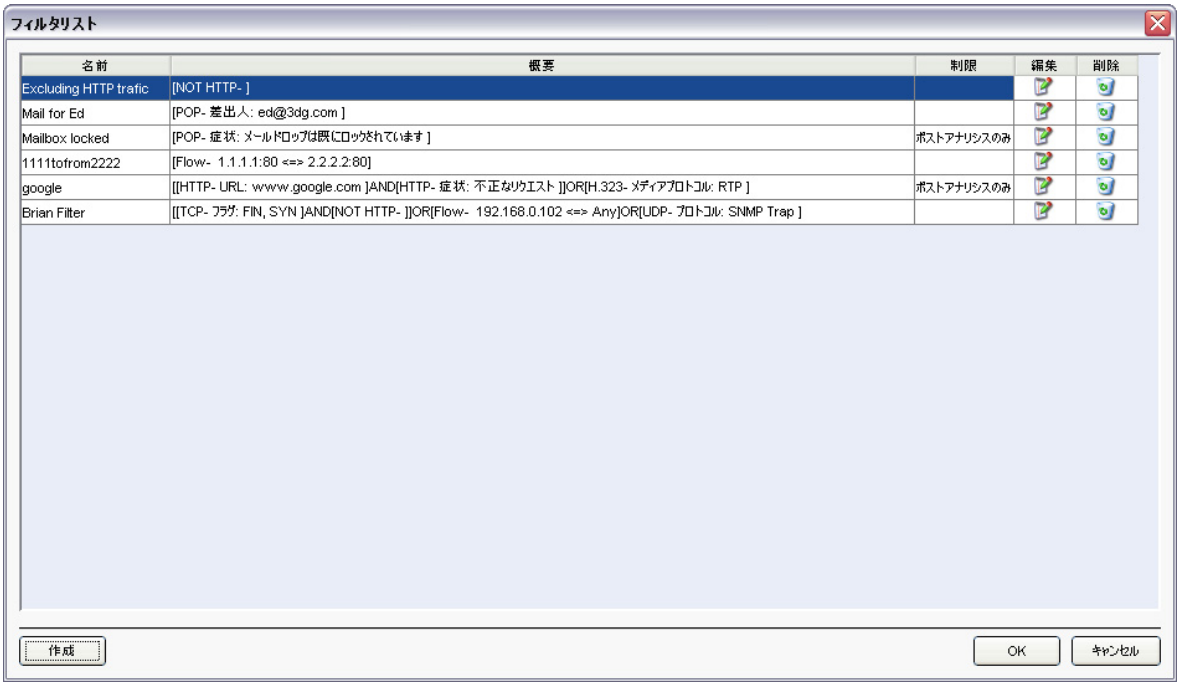


図 6-4: [フィルタリスト] ダイアログボックス

[バッファサイズ] の設定

[バッファ サイズ] オプションは、ClearSight がキャプチャ済みフレームに使用するメモリの量を指定します。ClearSight はインストールした PC が装備している物理メモリの 25% までの大容量のバッファサイズをサポートしています。ただし、キャプチャバッファのサイズが大きいほど、ポストキャプチャアナリシスにかかる時間が長くなります。バッファサイズと処理速度をうまく均衡させるようにしてください。

[バッファフル時のアクション] の指定

[バッファ フル時のアクション] は、キャプチャバッファが観測フレームで一杯になった場合の ClearSight の動作を指定します。ClearSight では、以下のようにキャプチャを**停止**または**上書き**できます。

- **[停止]** オプションを選択した場合、バッファが一杯になるとデータのキャプチャが停止され、それ以上フレームはキャプチャされなくなります。
- **[上書き]** オプションを選択した場合、バッファ内の最も古いフレームが新しく到着したフレームで上書きされます。キャプチャを停止するまで、バッファの上書きが繰り返されます。

[上書き] オプションを有効にし、キャプチャを停止するためのトリガを有効にしていない場合は、ポストキャプチャアナリシスに必要なデータを取得したら、忘れずにキャプチャを手動で停止してください。そうしないと、必要なデータが上書きされることがあります。

[スライスサイズ] の設定

[スライス サイズ] オプションは、下位層フレームごとにキャプチャする量を指定します。各フレームの残りの部分は「スライス」され、キャプチャバッファには格納されません。

フレームスライスを行うと、キャプチャされた各フレームのバッファに格納されるデータの量を削減できます。そのため、スライス機能を有効にすると、使用可能なバッファ領域を長く保つことができます。ただし、**[スライス サイズ]** オプションを使用する際は、ポストキャプチャアナリシスで必要なデータをスライスオフしないよう注意する必要があります。

下位層フレームには、上位層のデータが含まれます。通常、上位層フレームのヘッダは、ポストキャプチャアナリシス用に取っておく必要があります。上位層フレームが単一の下位層フレーム内に完全にカプセル化されると、通常のスライスサイズのほとんどが、カプセル化された上位層フレームのヘッダからなくなります。ただし、複数の上位層プロトコルのフレームが、複数の下位層フレーム全体にわたり、下位層フレームの任意のポイントでヘッダが開始される場合があります。このような場合、ポストキャプチャアナリシスで必要なデータをキャプチャできるよう、**[なし]** を選択する必要が生じることがあります。

[自動保存] パラメータの設定

キャプチャバッファが一杯になった場合は、[自動保存] 機能によって、トレースファイルを自動的に保存できます。以下のオプションがあります。

- デフォルトでは、**自動保存**は **[無効]** です。**自動保存**を有効にする場合は、**[有効]** チェックボックスをクリックしてください。
- **[ファイルプリフィックス]** は、保存するトレースファイルの名前の最初の部分です。デフォルトでは Capture_ です。
- **[ファイルサフィックス]** は、トレースファイルの連続番号に数値を追加します。**[範囲指定 : 1 から]** を選択するか、すでに完了した範囲のファイルの後に数値を追加することができます。たとえば、1 ～ 20 の範囲のファイルまで完了している場合、**[50 までの未使用数]** を選択して、Capture_21 から始まるトレースファイルを続けて保存できます。

  注記 : 各ファイルのサイズは、バッファサイズとほぼ同じです。必要なディスク容量は、**[範囲設定 : 1 から]** オプションで入力した数値によって決定されます。たとえば 10 を入力し、バッファサイズが 128MB の場合、これらの 10 個のファイルは約 1.28GB のハードディスクのドライブ容量を占有します。
- **[ディレクトリ]** ボックスに、ファイルを保存するディレクトリの名前を入力します。デフォルトでは、*traces* です。必要なディレクトリに移動することもできます。

  注記 : バージョン 5.1 以前の ClearSight Distributed では、この参照オプションは許可されていませんでした。ファイルは traces ディレクトリに保存する必要がありました。バージョン 5.1 から、任意のディレクトリにこれらのファイルを保存できるようになりました。残っている制約は、ディレクトリがエージェントの PC 上になければならないということのみです。

キャプチャオプションの設定

[オプション] にある補足設定を使用して、キャプチャ中にパフォーマンスと機能を最適化することができます。

[全て (アプリケーション , ネットワークと物理層)] オプション

[全て (アプリケーション , ネットワークと物理層)] チェックボックスで、ClearSight がフレームをキャプチャバッファにキャプチャしながらネットワークトラフィックを処理するかどうかを指定できます。このボックスをチェックしない場合、ClearSight はフレームを処理しません。これにより、キャプチャ実行中の処理オーバーヘッドが軽減されます。フレームの処理は、ClearSight のツールバーの [表示] ボタンを使用するか、バッファをトレースファイルとして保存しておけば、あとで実行することができます。

図 6-5 は、**[全て (アプリケーション , ネットワークと物理層)]** チェックボックスの状態が、フレームをキャプチャしているときに、キャプチャ画面の層ペインの外観にどのように影響するかを示したものです。

さらに、このチェックボックスをオンにすると、キャプチャワークスペースに **[事象]** タブと **[問題]** タブが表示されます。

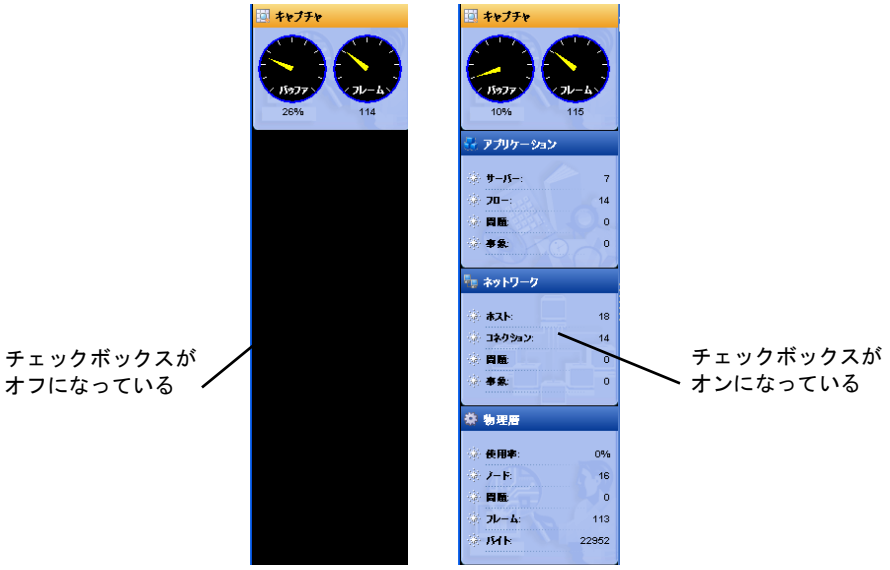


図 6-5: [ClearSight ビュー] の変更

注記：このオプションを変更した場合、その変更は次回 ClearSight を起動したときに有効になります。

キャプチャ中はモニタを無効にするオプション

[キャプチャ中はモニタを無効にする] ボックスをオンにすると、キャプチャが開始されたときにモニタの動作が停止し、キャプチャが停止されたときに再開します。

注記：このオプションを変更した場合、その変更は次回キャプチャを開始したときに有効になります。

キャプチャ中のリアルタイムモニタ

（**[キャプチャ中はモニタを無効にする]** ボックスをオンにしていない場合）第 5 章「ClearSight を使用したネットワークのモニタ」で説明するリアルタイムモニタ画面は、キャプチャ中もすべて使用することができます。キャプチャ中でもリアルタイムモニタ画面の更新は停止されず、進行中のキャプチャに関する詳細情報を含む追加の画面が表示されるようになります。これらの画面の詳細については、223 ページの「実行中のキャプチャの観察」を参照してください。

[トリガ] タブ

[トリガ] タブでは、フレームのキャプチャを開始および停止するタイミングを指定できます。図 6-6 は、**[トリガ]** タブを示しています。

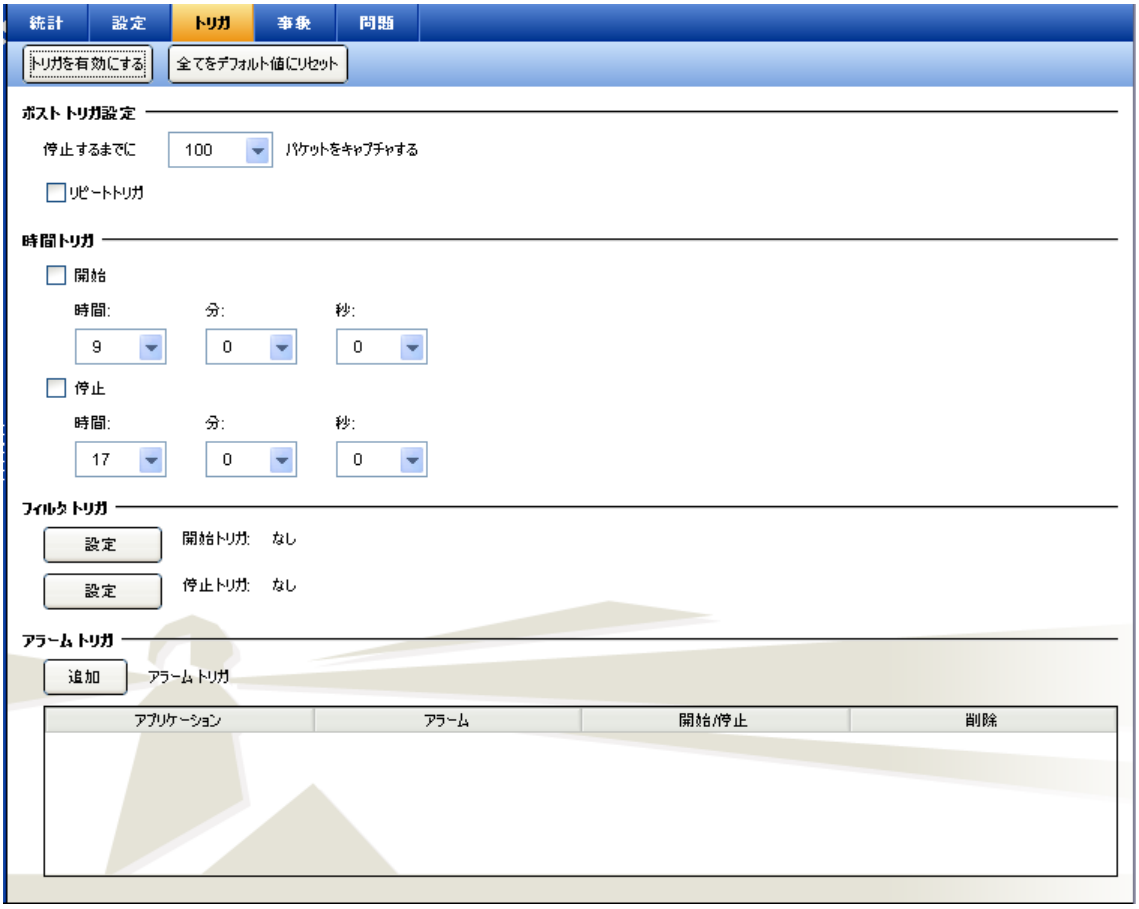


図 6-6: [トリガ] タブ

図 6-6 に示すとおり、以下のトリガオプションを設定できます。

- **[ポストトリガ設定]** (220 ページ)
- **[時間トリガ]** (220 ページ)
- **[フィルタトリガ]** (220 ページ)

- **[アラームトリガ]** (221 ページ)

トリガ設定を実際に使用するには、**[トリガを有効にする]** ボタンをクリックします。トリガ設定の使用を中止するには、**[トリガを無効にする]** ボタンをクリックします。

[ポストトリガ設定] の設定

この項目では、トリガイベントが発生したあとに ClearSight がキャプチャするパケットの数を指定できます。ドロップダウンリストから必要な値を選択します。

[リピートトリガ] チェックボックスをオンにすると、そのトリガイベントが再度発生した場合にキャプチャが再び開始または停止されます。

[時間トリガ] の設定

この項目では、キャプチャの開始 / 停止のための単純な時刻基準を設定できます。**[開始]** チェックボックス / **[停止]** チェックボックスをオンにして、ドロップダウンリストから適切な時刻を選択します。

[フィルタトリガ] の設定

この項目では、フィルタを使用して、指定したトリガを通過したパケットが検出されたときに、キャプチャの開始または停止をトリガすることができます。そのようなトリガがすでに選択されている場合は、そのトリガの名前が表示され、対応するボタンの名前は **[削除]** となっています。トリガが選択されていない場合は、**[なし]** と表示され、対応するボタンの名前は **[設定]** となっています。このボタンをクリックすると、**[フィルタリスト]** ダイアログボックスが表示されます。ここで、定義済みフィルタのリストから必要なフィルタを選択できます。

注記 : フィルタの **[制限]** 列に **[ポストアナリシスのみ]** が表示されている場合、そのフィルタをトリガとして使用することはできません。

[アラームトリガ] の設定

この項目では、キャプチャを開始または停止するためのアラームベースのトリガのリストを作成できます。初期状態では、このリストは空です (図 6-6 を参照)。**[追加]** ボタンをクリックすると、[アラームトリガ] ダイアログボックス (図 6-7) が表示されます。

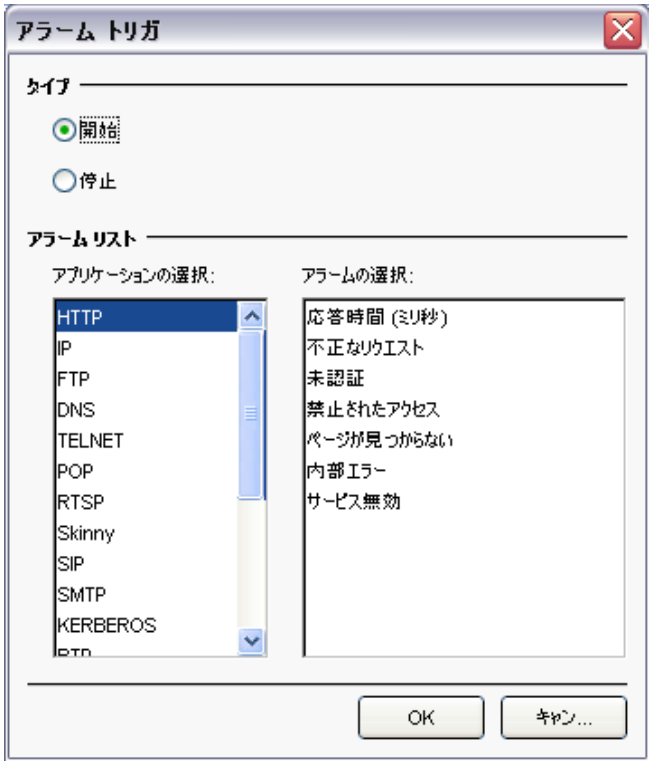


図 6-7: [アラームトリガ] ダイアログボックス

[タイプ] 項目では、トリガによってキャプチャを開始するか停止するかを選択することができます。次に、**[アラームリスト]** 項目でアプリケーションを選択し、**[アラームの選択 :]** ボックスに表示されるそのアプリケーション固有のリストから定義済みのアラームを選択します。アラームを選択したら、**[OK]** をクリックします。そのアラームが **[アラームトリガ]** リストに追加されます。

アラームトリガを実際に使用するには、**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[スレッショルド]** > **[問題]** 項目で対応する問題のしきい値を設定し、**[設定]** ボタン > **[設定]** タブ > **[翻訳]** > **[全般]** > **[問題の生成]** 項目のチェックボックスをオンにして問題生成を有効にします。

実行中のキャプチャの観察

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

目的に合ったキャプチャバッファを設定したら、ツールバーの **[開始]** ボタンをクリックするか、**[キャプチャ]** メニューの **[開始]** オプションを選択して、キャプチャを開始することができます。これにより、ネットワークからのフレームのキャプチャが開始され、キャプチャフィルタを通過したフレームがキャプチャバッファに格納されるようになります。これ以外にも、以下が行われます。

- 層ペインの **[キャプチャ]** 層のメータの値が増加し始め、バッファのフレーム数とフレームに使用できるバッファ領域の割合が表示されます。
- **[全て (アプリケーション , ネットワークと物理層)]** オプションを有効にしている場合には、その他の標準層 (**[アプリケーション]**、**[ネットワーク]**、および **[物理層]**) のキャプチャ中の画面も、現在のキャプチャフィルタを通過したトラフィックの分だけ増加し始めます。ツールバーの **[モニタ]** ボタンをクリックすると、各層のフィルタが適用されていない状態を表示しています。
- **[キャプチャ中はモニタを無効にする]** オプションを無効にしている場合には、リアルタイムモニタ画面は、新しく検出されたフロー、統計、およびカウンタで引き続き更新されます。

  注記 : 上述のとおり、リアルタイムモニタ画面にはフィルタが適用されていません。キャプチャ中の層画面には、現在のキャプチャフィルタを通過したトラフィックのフロー、接続、およびノードしか表示されませんが、リアルタイムモニタ画面には、すべてのトラフィックが表示されます。これらの画面は似ていますが、キャプチャ中の層画面では層ペインの最上部に **[キャプチャ]** 層カウンタが表示される点だけが異なります。このカウンタは、どちらの画面を表示しているかを判断するために使用してください。2 つのワークスペース間を切り替えるには、ツールバーの **[モニタ]** と **[キャプチャ]** のボタンを使用します。
- キャプチャワークスペースの **[統計]** タブのカウンタが増加し始め、キャプチャの進捗状況がリアルタイムで表示されます。**[統計]** タブのカウンタについては、以降に説明します。
- **[全て (アプリケーション , ネットワークと物理層)]** オプションを有効にしている場合には、**[事象]** タブと **[問題]** タブに、現在のキャプチャフィルタを通過したトラフィックに関連する事象と問題が表示され始めます。

第 7 章

ポストキャプチャアナリシス

この章では、ClearSight のポストキャプチャアナリシス機能について説明します。以下は、この章でとり上げるトピックです。

- 「ポストキャプチャアナリシスについて」
- 「ポストキャプチャアナリシス画面の使用」
- 「[翻訳] タブの使用」
- 「[翻訳] タブの設定オプション」
- 「トレースファイルの使用」

ポストキャプチャアナリシスについて

ClearSight では、ポストキャプチャアナリシスが実行されると、豊富なトラブルシューティング機能が 1 つのワークスペースに集められ、キャプチャされたネットワークデータを理解し、解析できるようになります。ポストキャプチャアナリシスは、統合された一連のタブで実行され、各タブからは特定の解析機能にアクセスできます。

ポストキャプチャアナリシスのタブのうち最も重要なのが、ツールバーの **[トレースファイル]** の下の **[ClearSight]** タブです。**[ClearSight]** タブには、リアルタイムモニタ画面に含まれるのと同じ機能がポストキャプチャアナリシス用に備わっており、アプリケーション層のサーバーとフロー、ネットワーク層の接続とホスト、物理層の VLAN とノードが測定されます。

ポストキャプチャアナリシスには、**[ClearSight]** タブに加え、3 ペイン構成の **[翻訳]** 画面が含まれています。ただし、ほとんどの場合、ClearSight のキャプチャ画面の他のタブの使用だけでトラブルシューティングができるため、[翻訳] タブで 16 進数コードを解析する必要が生じることはめったにありません。

[翻訳] タブを実際に使用する必要が生じた場合は、ClearSight のスマートナビゲーション機能と自動フィルタリング機能を使用して、**[ClearSight]** タブと **[翻訳]** タブの間を簡単に移動し、必要なフレームだけを表示できます。

- スマートナビゲーション機能を使用すると、**[ClearSight]** タブの **[会話]** タブでコマンドをクリックし、選択したフレームで親フローがフィルタされた **[翻訳]** タブに直接移動することができます。同様に、**[翻訳]** タブのオプションを使用すると、**[ClearSight]** タブで選択されたフレームの IP またはアプリケーションのフローに直接移動することができます。
- 自動フィルタリング機能を使用すると、**[ClearSight]** タブのカウンタを右クリックして、**[翻訳]** タブに一時的にフィルタをかけ、選択したアプリケーション、フロー、サーバー、ホスト、またはステーションのトラフィックだけを表示することができます。

ポストキャプチャアナリシス画面の使用

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

ClearSight では、現在キャプチャバッファに含まれているフレームまたは保存されたトレースファイルに対して、ポストキャプチャアナリシスを実行できます。

- 現在キャプチャバッファにあるフレームのポストキャプチャアナリシスを実行するには、ツールバーの **[表示]** ボタンをクリックします。
- トレースファイルのポストキャプチャアナリシスを実行するには、**[ファイル] > [開く]** コマンドを使用して、希望のトレースファイルを開きます。

ポストキャプチャアナリシスワークスペースは、バッファとトレースファイルのどちらを解析しているかに関わらず同様に表示されます (図 7-1)。

ツールバーで選択されたアイコンからもわかるとおり、このポストキャプチャアナリシスワークスペースには、現在トレースファイルが表示されています。ワークスペースのタイトルバーには、トレースファイルの名前が表示されます。

ポストキャプチャアナリシスは、統合した複数のタブで実行されます。**[ClearSight]** タブ (図示) からは、リアルタイムモニタ時に使用できるすべての機能にアクセスできます。また、**[翻訳]** タブには、ほかのワークスペースにも含まれる 3 ペイン構成のプロトコル解析が表示されます。スマートナビゲーション機能や自動フィルタリング機能を使用すると、2 つのタブ間を簡単に移動できます。



ポストキャプチャアナリシスワークスペースには、**[ClearSight]** タブと **[翻訳]** タブに加え、アラートタブ (**[事象]** と **[問題]**)、および **[レポート]** タブも含まれます。

図 7-1: ポストキャプチャアナリシスワークスペース

図 7-1 に示すとおり、ポストキャプチャアナリシスワークスペースは複数の統合タブで構成されます。表 7-1 は、ポストキャプチャアナリシスワークスペースで使用できるタブとその説明を列記したものです。

表 7-1: ポストキャプチャアナリシスワークスペースのタブ

タブ	説明
[ClearSight]	**[ClearSight]** タブには、リアルタイムモニタ画面に含まれるのと同じ機能がポストキャプチャアナリシス用に備わっており、アプリケーション層のサーバーとフロー、ネットワーク層の接続とホスト、物理層の VLAN とノードが測定されます。 **[ClearSight]** タブの画面の説明と使用法については、第 5 章「ClearSight を使用したネットワークのモニタ」を参照してください。 **注記 :** ポストキャプチャアナリシスワークスペースの **[詳細]** タブには、TCP プロトコルが含まれている場合は、**[TCP データ]** という追加タブがあります。**[TCP データ]** は、ASCII 文字と 16 進数文字のどちらかで表示することができます。**[TCP データ]** タブからコピーアンドペーストでき、その内容をファイルに保存することもできます。
[事象]	**[事象]** タブには、アラートログの **[事象]** タブのすべての機能がポストキャプチャアナリシス用に備わっており、重要度の低いネットワークエラーが報告されます。 **[事象]** タブの使用法については、第 10 章「アラートの操作」を参照してください。 ポストキャプチャアナリシスでは、**[事象]** タブで追加のドリルダウン機能を使用できます。特定の事象を右クリックすると、アプリケーションフロー、ネットワークコネクション、またはその事象の原因であるその他の項目の詳細情報に移動するためのオプションが表示されます。
[問題]	**[問題]** タブには、アラートログの **[問題]** タブのすべての機能がポストキャプチャアナリシス用に備わっており、現在のバッファまたはトレースファイルで検出されたネットワークエラーが報告されます。 **[問題]** タブの使用法については、第 10 章「アラートの操作」を参照してください。 ポストキャプチャアナリシスでは、**[問題]** タブで追加のドリルダウン機能を使用できます。特定の問題を右クリックすると、アプリケーションフロー、ネットワークコネクション、またはその問題の原因であるその他の項目の詳細情報に移動するためのオプションが表示されます。

表 7-1: ポストキャプチャアナリシスワークスペースのタブ（続き）

タブ	説明
[翻訳]	[翻訳] タブには、ほかのワークスペースにも含まれる 3 ペイン構成のプロトコル翻訳画面が含まれます。ここには、キャプチャされた各フレームの内訳がプロトコル層ごとに表示され、プロトコルが自然言語テキストに翻訳されます。この章では、[翻訳] タブとその使用法について説明するほか、[ClearSight] タブから効率的にアクセスする方法についても説明します。
[レポート]	ClearSight ツールバーの [レポート] ボタンをクリックすると、レポートタブには、リアルタイムモニタ時に使用できるレポートと同じものがポストキャプチャアナリシス用に表示されます。レポートの使用法については、第 12 章「レポートの使用」を参照してください。

[ClearSight] タブと [翻訳] タブの間のスマートナビゲーション

ClearSight Application Flow Analyzer　ClearSight Analyzer Light　ClearSignt Distributed

ポストキャプチャアナリシスでは、[ClearSight] タブと [翻訳] タブが最もよく使用されます。ClearSight には、強力なスマートナビゲーション技術が備わっているため、これらの 2 つのタブ間をすばやく正確に移動して、問題を表示するフレームを見つけることができます。スマートナビゲーションにより、以下を実行できます。

- [ClearSight] タブの [会話] タブでコマンドをクリックし、選択したフレームで親フローがフィルタされた [翻訳] タブに直接移動することができます。

  このテクニックについては、231 ページの「[ClearSight] タブからのスマートナビゲーション」で説明します。

- [翻訳] タブでフレームを選択し、[関連ページに移動] ボタン  をクリックすると、[ClearSight] タブ内のそのフレームの IP またはアプリケーションフローに直接移動できます。

  このテクニックについては、233 ページの「[翻訳] タブからのスマートナビゲーション」で説明します。

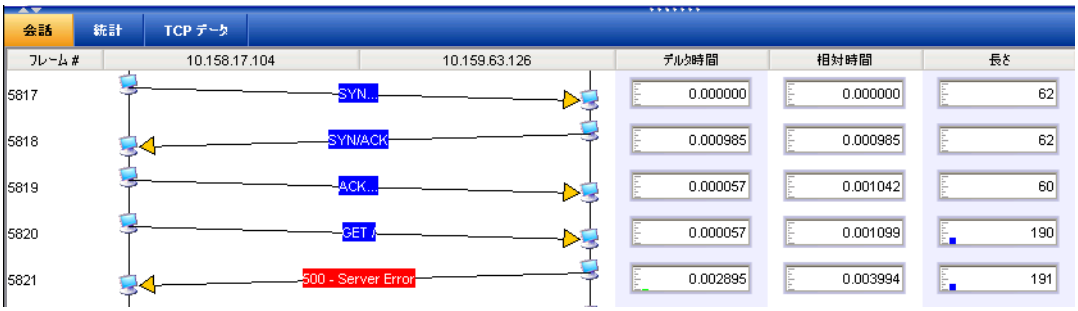
[ClearSight] タブからのスマートナビゲーション

リアルタイムモニタ画面の場合と同様に、**[ClearSight]** タブでポストキャプチャアナリシスを行うと、クライアントとサーバー間の要求と応答の交換が再構築され、選択したフローに関する **[会話]** タブのネットワークラダーに視覚的に表示されます。

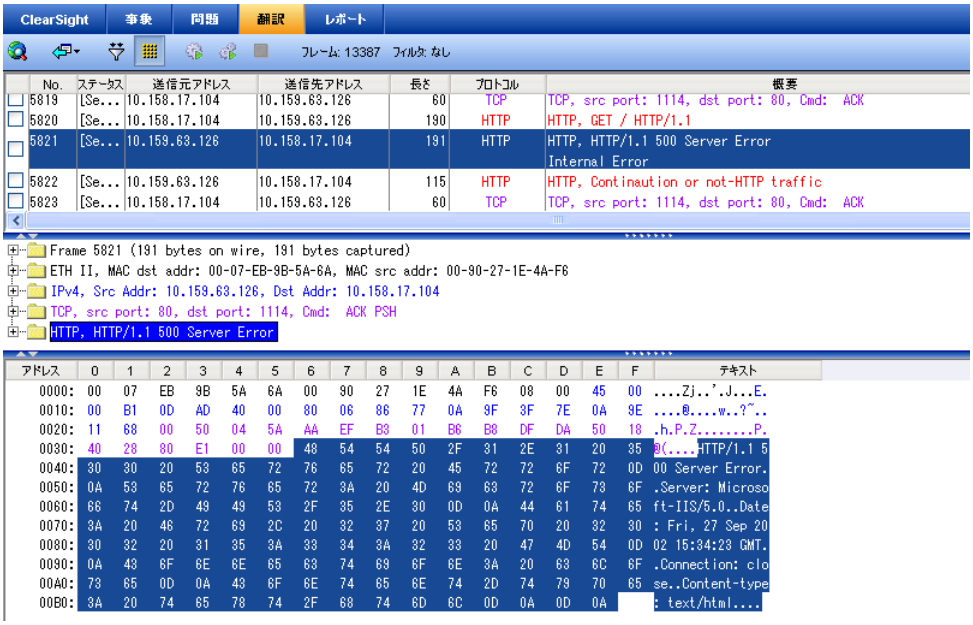
[会話] タブ内のダイアグラムでは、問題を示す要求と応答は、各問題の重要度に基づいて色付けされ、表示されます。問題のある要求や応答を **[会話]** タブのダイアグラムでクリックすると、選択したフロー内の問題のフレームのプロトコル翻訳に直接移動することができます。このように、ClearSight では、問題のあるフレームが表示され、そのフレームを含むフローに関してフィルタされたプロトコル翻訳に直接移動できるため、プロトコル解析の作業が簡略化されています。

たとえば、図 7-2 に示すように、**[会話]** タブのダイアグラムの HTTP サーバーからの「**404 - Not Found**」応答から、問題のあるフレームに関するフィルタが親フローに対して適用された **[翻訳]** タブに直接移動できます。

注記 : [会話] タブでは、問題のないフレームもクリックできます。**[会話]** タブのどのフレームをクリックしても、そのフレームについて親フローがフィルタされた **[翻訳]** タブに移動することができます。



[会話] タブのフレームをクリックして、翻訳を確認します。



[会話] タブの項目をクリックすると、そのフレームに対応する **[翻訳]** タブの項目に直接移動できます。選択されたフレームの番号が両方の画面で同じであることに注意してください (5821)。このスマートナビゲーション技術を使用すると、**[ClearSight]** タブから **[翻訳]** タブに簡単に移動できます。

また、**[翻訳]** タブは自動的にフィルタされるため、選択したフレームを含むフローのフレームだけが表示されます。

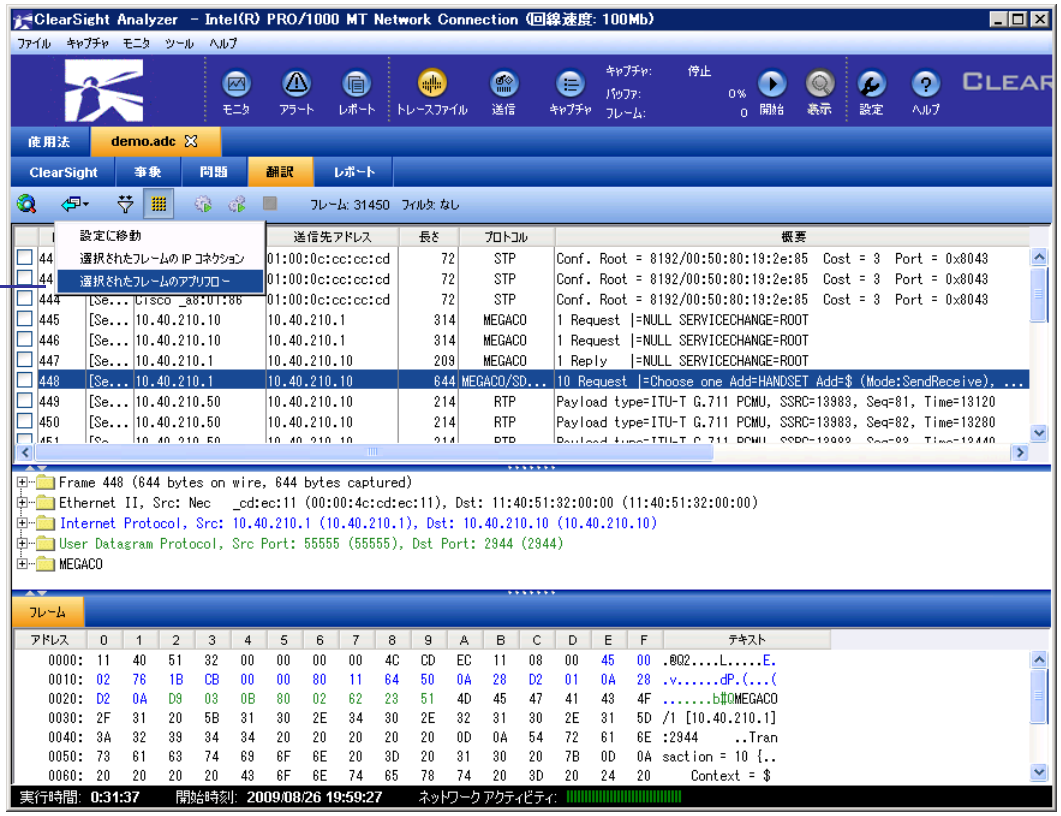
図 7-2: [会話] タブからのスマートナビゲーション

[翻訳] タブからのスマートナビゲーション

ネットワーク問題の根源には、プロトコル翻訳を使用しなければたどり着けない場合があります。ただし、何万ものフレームを含むトレースファイルを取扱う場合、プロトコル翻訳で容易に混乱しかねません。

ClearSight には、コードの処理に煩されずに、ネットワークトラフィック全体の状態を簡単に把握できる方法があります。**[翻訳]** タブを使用する場合、[サマリ] ペインでフレームを選択して、**[関連ページに移動]** ボタン  をクリックすると、**[ClearSight]** タブ内のそのフレームの IP コネクションまたはアプリケーション会話に直接移動できます。このように、視点を変えるだけで、ネットワークの問題が明確になる場合もあります。

図 7-3 は、**[関連ページに移動]** ボタンを使用して、[翻訳] タブから [ClearSight] タブのアプリケーションフローに移動する様子を示したものです。



[関連ページに移動] ボタン を使用すると、**[翻訳]** タブで選択したフレームのカウンタから、**[ClearSight]** タブ内のその親アプリケーションまたは IP フローに移動できます。

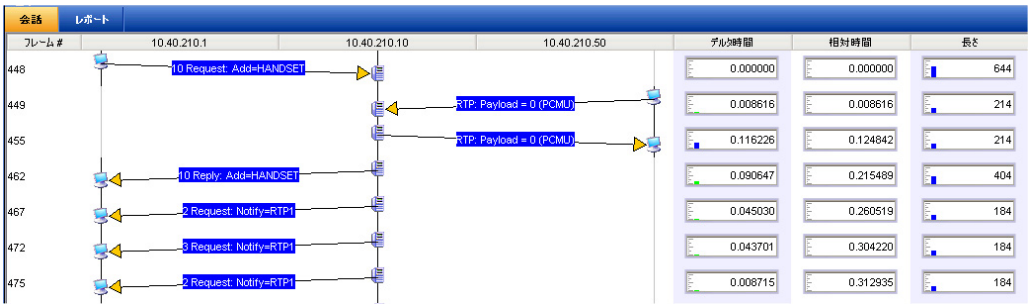


図 7-3: [翻訳] タブからのスマートナビゲーション

ポストキャプチャ画面における自動フィルタの使用

通常、**[ClearSight]** または **[翻訳]** の各タブでカウンタを右クリックすると、自動フィルタを使用できます。これにより、コンテキストメニューが表示され、指定したカウンタに対して使用可能なさまざまな自動フィルタの中から選択できるようになります。どちらのタブを選択するかに応じて、表示フィルタとキャプチャフィルタの両方が一覧表示される場合があります。表示フィルタを選択するには、**[フィルタ xxx]** コマンドを使用します。キャプチャフィルタを選択するには、**[xxx をキャプチャする]** コマンドを使用します。

どのフィルタを使用できるかは、どの層、ペイン、およびカウンタを選択するかによって決まります。通常、自動表示フィルタは、選択されたカウンタのアドレスとポートに使用できるほか、これらのアドレスとポートを別の組み合わせで使用してワイルドカード形式のフィルタ処理を行う際にも使用することができます。

自動表示フィルタを選択すると、そのフィルタが適用された **[翻訳]** タブが自動的に表示されます。フィルタを削除するには、**[ClearSight]** タブの新しい自動フィルタを適用するか、**[翻訳]** タブのステータスバーで **[フィルタのオン / オフ]** ボタン をクリックします。

自動フィルタの使用法の詳細については、282 ページの「自動フィルタの使用」を参照してください。

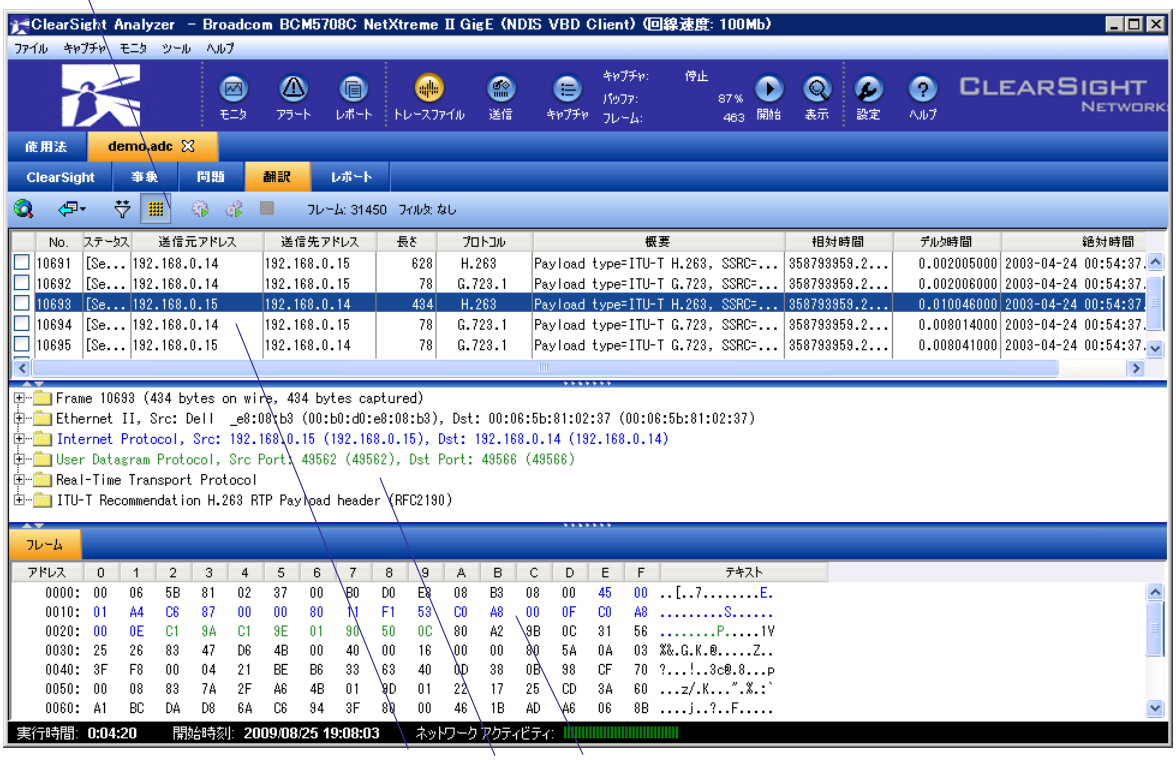
[翻訳] タブの使用

ClearSight Application Flow Analyzer　ClearSight Analyzer Light　ClearSignt Distributed

この項では、ポストキャプチャアナリシスワークスペースの **[翻訳]** タブを使用する方法について説明します。ほとんどの場合、ClearSight のネットワーク解析機能を使用すると、従来からのプロトコル翻訳を確認せずにネットワークをトラブルシューティングできます。ただし、これらのデコードを参照して、各キャプチャフレームに埋め込まれた実際のプロトコル層の明細を確認する必要が生じる場合もあります。ClearSight では、**[翻訳]** タブを使用してこれを行うことができます。

図 7-4 は、**[翻訳]** タブの例を示したものです。

ClearSight の **[翻訳]** タブには、プロトコル翻訳が従来からの 3 ペイン構成で表示されます。タイトルバーには、表示されたトレースファイルの名前が表示されます。**[検索]** ボタンを使用すると、画面で特定のフレームを検索することができます。**[関連ページに移動]** ボタンを使用すると、**[ClearSight]** タブ内の選択したフレームのアプリケーションまたは IP フローに移動できます。**[フィルタの適用]** ボタンを使用すると、フィルタ選択することができます。**[フィルタオン / オフ]** ボタンを使用すると、フィルタのオンとオフを切り替えることができます。



[翻訳] タブの 3 つのペイン (**[サマリ]**、**[詳細]**、および **[Hex]**) は互いに連動し、フレームに埋め込まれたさまざまなプロトコル層を表示します。**[サマリ]** ペインには、キャプチャされたフレームが各行に 1 つずつ列記され、その送信元アドレスと送信先アドレス、フレーム内の最上位層プロトコル、さまざまなタイミング情報などの概要が表示されます。**[詳細]** ペインには、**[サマリ]** ペインで選択したフレームの各層が表示されます。これらの層を段階的に開くと、自然言語に翻訳されたフレーム内のさまざまなフィールドを表示できます。**[Hex]** ペインには、**[サマリ]** ペインで選択したフレームの 16 進数翻訳と ASCII 翻訳の両方が表示されます。**[Hex]** ペインのハイライト表示は、**[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。そのため、どの 16 進数コードがフレーム内の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。

図 7-4: [翻訳] タブ

[翻訳] タブのペイン

図 7-4 に示すとおり、**[翻訳]** タブには、フレームに埋め込まれたさまざまなプロトコル層を表示するために連動する、以下の 3 つのペインがあります。

- **[サマリ]** ペインは **[翻訳]** タブの最上部に表示されます。
- **[詳細]** ペインは **[翻訳]** タブの中央に表示されます。
- **[Hex]** ペインは **[翻訳]** タブの最下部に表示されます。

[サマリ] ペイン

[サマリ] ペインは **[翻訳]** タブの最上部に表示されます。このペインには、キャプチャされたフレームが各行に 1 つずつ表示され、送信元アドレスと送信先アドレス、フレーム内の最上位層プロトコル、さまざまなタイミング情報などの概要が示されます。

[サマリ] ペインをスクロールすると、バッファまたはトレースファイルに含まれる各フレームのカウンタを表示できます。カウンタを選択すると、選択したフレームの翻訳情報で **[詳細]** ペインと **[Hex]** ペインが更新されます。

[翻訳] タブに一覧表示されたアドレスが ClearSight のアドレス帳で検出されると、翻訳画面でアドレスが名前に置換されます。

デフォルトで、**[サマリ]** ペインには、表 7-2 に示すフィールドとともに各フレームが一覧表示されます。**[設定] > [翻訳設定]** タブのオプションを使用すると、これらのフィールドのサブセットを選択することができます。詳細については、246 ページの「[翻訳] タブの設定オプション」を参照してください。

表 7-2: [サマリ] ペインのフィールド

フィールド	説明
[チェックボックス]	複数のフレームを選択するには、この列のチェックボックスを使用します。**[サマリ]** ペインで右クリックしてコンテキストメニューを表示し、使用可能なコマンドの 1 つを選択すると、チェックボックスをオンにしたフレームに対してさまざまなアクションを実行することができます。 使用可能なコマンドについて詳しくは、239 ページの「[サマリ] ペインのコンテキストメニューコマンド」を参照してください。
[No.]	フレームの連続番号が表示されます。
[ステータス]	このフレームに関するステータスフラグ (ある場合)。
[送信元アドレス] **[送信先アドレス]**	このフレームで見つかった送信元アドレスと送信先アドレス。これらのアドレスの名前がアドレス帳で検出されると、画面でその名前が代わりに表示されます。
[長さ]	フレームの長さをバイト単位で表したもの。
[プロトコル]	フレームに出現した最上位層プロトコル。
[概要]	フレームに出現した最上位層の要求、応答、ステータスコードなど、フレームの目的を概観したビュー。**[トランスポート サマリのみ表示]** オプションが有効になっている場合、**[概要]** 列には、送信元ポートや送信先ポートに関する情報など、トランスポート層プロトコルに関する情報 (TCP または UDP) が代わりに表示されるようになります。
[相対時間]	キャプチャの開始とこのフレームの間の間隔、または **[相対時間を元にマーク]** フラグでマークされたフレーム (フラグが有効になっている場合) とこのフレームの間の間隔。 **[相対時間を元にマーク]** フラグの適用方法については、239 ページの「[サマリ] ペインのコンテキストメニューコマンド」を参照してください。
[デルタ時間]	このフレームと前のフレームの間の間隔。
[絶対時間]	このフレームがキャプチャされたときのタイムスタンプ。

[サマリ] ペインのコンテキストメニューコマンド

[サマリ] ペインで任意のカウンタを右クリックすると、**[翻訳]** タブのオプションを含むコンテキストメニューにアクセスできます。表 7-3 は、使用可能なオプションとその説明を列記したものです。

表 7-3: [サマリ] ペインで使用できるコンテキストメニューコマンド

コマンド	説明
[相対時間を元にマーク]	このフレームをマークとして設定し、**[サマリ]** ペインのほかのフレームに関する **[相対時間]** フィールドがここから計算されるようにします。このコマンドを適用すると、**[サマリ]** ペインに表示される **[相対時間]** フィールドは自動的に再計算されます。
[トランスポート サマリのみ表示]	**[概要]** 列に、フレーム内の最上位層プロトコルに関する情報ではなく、トランスポートプロトコル (TCP、UDP など) に関する情報を表示します。
[チェックされたフレームでフィルタ]	**[サマリ]** ペインの一番左の列でチェックボックスがオンになっているものを除き、すべてのフレームを画面から削除します。
[範囲をチェック]	ダイアログボックスを表示し、開始フレームと終了フレームの番号を指定することにより、連続した複数のフレームの範囲をチェックできるようにします。このコマンドを **[チェックされたフレームでフィルタ]** コマンドと併用すると、まとまったフレームをすばやく表示することができます。
[すべてのフレームのチェックをはずす]	チェックボックスがオンになったすべてのフレームの選択を解除します。

[詳細] ペイン

[詳細] ペインは **[翻訳]** タブの中央に表示されます。このペインには、**[サマリ]** ペインで選択したフレームの各層が表示されます。最下位プロトコル層がペインの一番上に表示され、最上位プロトコル層までが順番に並んでその下に表示されます。これらの層を段階的に開くと、自然言語に翻訳されたフレーム内のさまざまなフィールドを表示できます。

注記：[詳細] ペインで各フレームに関して表示される最初の層は、フレーム自体に実際には含まれない層です。この特殊な**フレーム**層には、キャプチャ時刻、フレーム番号、フレーム長など、フレーム全体に関する情報が含まれます。

図 7-5 は、**[詳細]** ペインで IP 層が段階的に開かれ、さまざまなフィールドのデコードを表示した状態の HTTP フレームを示したものです。**[詳細]** ペインの各行を選択すると、それに対応する 16 進数コードと ASCII コードを **[Hex]** ペインでハイライト表示できます。

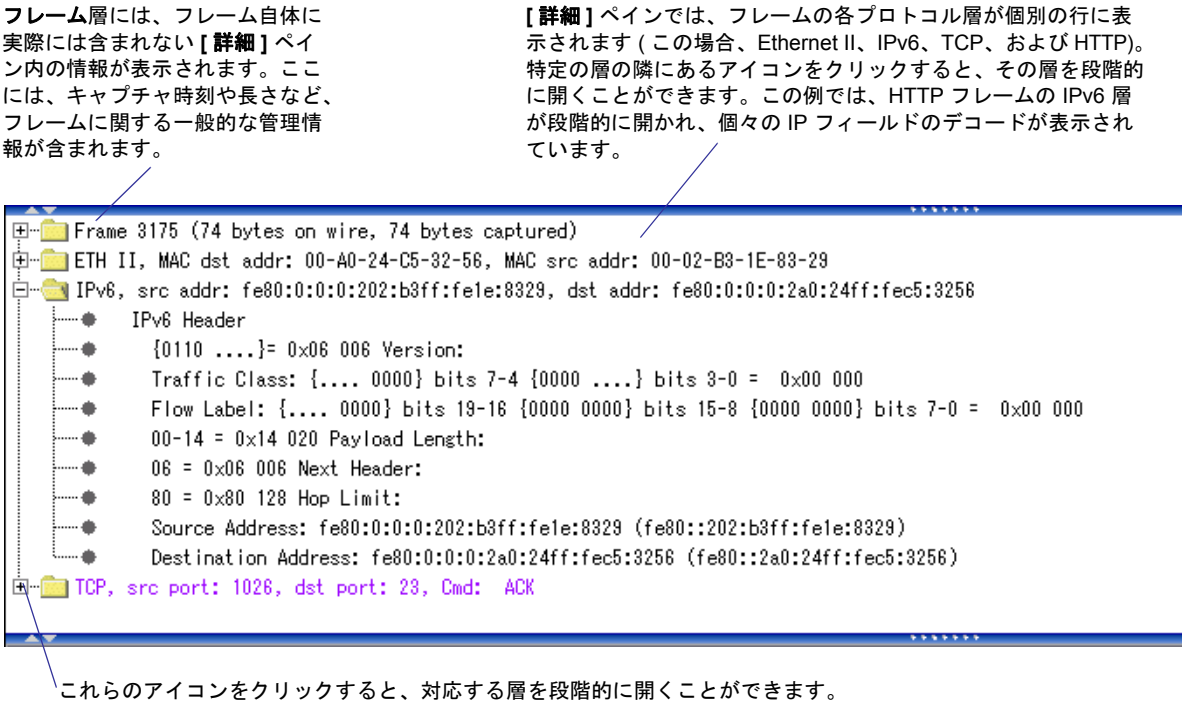


図 7-5: [翻訳] タブの [詳細] ペイン

[Hex] ペイン

[Hex] ペインは **[翻訳]** タブの最下部に表示されます。このペインには、**[サマリ]** ペインで選択したフレームの 16 進数翻訳と ASCII 翻訳の両方が表示されます。**[Hex]** ペインのハイライト表示は、**[詳細]**

ペインでどの行が選択されるかに応じて更新されます。そのため、どの 16 進数コードがフレーム内のどの層またはフィールドに対応しているかを正確に把握することができます。

画面の 16 進数部分には、フレームの各バイトが 2 つの 16 進数文字として表示されます。バイトは、連続した順でテーブルの各行を左から右に向かって並び、その行が終わると次の行に継続していきます。テーブルの左側にある 16 進数コードは、フレームの開始からのオフセットを示します。

画面の ASCII 部分には、**[設定]** ボタン > **[設定]** タブ > **[翻訳]** > **[表示]** > **[オプション]** > **[テキストを EBCDIC で表示]** のオン / オフにより、ASCII または EBCDIC のどちらかの方法を使用した 16 進数コードの翻訳が表示されます。デフォルトは ASCII です。

[翻訳] タブにおけるフレームの検索

[翻訳] タブの **[検索]** ボタン  をクリックすると、**[概要]**、**[詳細]**、または **[Hex]** の各ペインで特定の値を含むフレームを検索できます。これにより、**[翻訳]** タブの左側に一連の検索オプションが表示されます (図 7-6)。検索するテキストを入力し、検索するフィールドを選択して、**[検索]** ボタンをクリックします。または、**[移動する]** オプションを使用して、移動先のフレーム番号を指定することもできます。

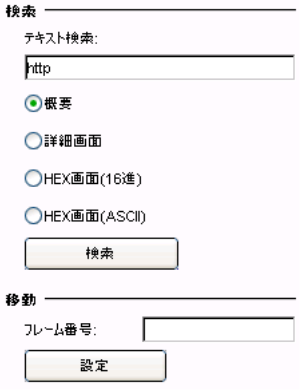


図 7-6: [翻訳] タブの検索オプション

Ethernet OAM フレームの翻訳

Ethernet OAM フレームの翻訳機能はオプションなので、この機能を使用するには特別のライセンスが必要となります。また、ClearSight 翻訳エンジン（**[設定] ボタン >[設定] タブ >[翻訳]>[全般]>[翻訳エンジン]>[ClearSight]**）を選択する必要があります。この 2 つの条件が満たされると、イーサタイプ 0 x 8049 のフレームが Ethernet OAM フレームとして **[翻訳]** タブに表示されます。

ClearSight は、ITU 版および IEEE 版両方の OAM フレームフォーマットの翻訳をサポートしています。IEEE 版フレームフォーマットのサポートによって、翻訳で TLV 情報を認識することができます。

また、異なるイーサタイプの値を持つ Ethernet OAM フレームを翻訳することもできます。ただし、**[設定] ボタン >[設定] タブ >[翻訳] >[プロトコルフォーシング]>[EtherOAM]** の設定画面を使用して異なるイーサタイプの値を設定しておく必要があります。詳細については、256 ページの「[翻訳] > [プロトコルフォーシング] オプション」を参照してください。

現在の ClearSight Analyzer のバージョンでは、以下の Ethernet OAM フレームの翻訳がサポートされています。

Opcode 値	OAM PDU タイプ
0x01	CCM
0x02	LBR
0x03	LBM
0x04	LTR
0x05	LTM

図 7-7 は、**[翻訳]** タブに表示される Ethernet OAM フレーム翻訳の例を示しています。この例では、プロトコルフォーシングを使用して、イーサタイプ 0x8042 が Ethernet OAM フレームとして認識されています。

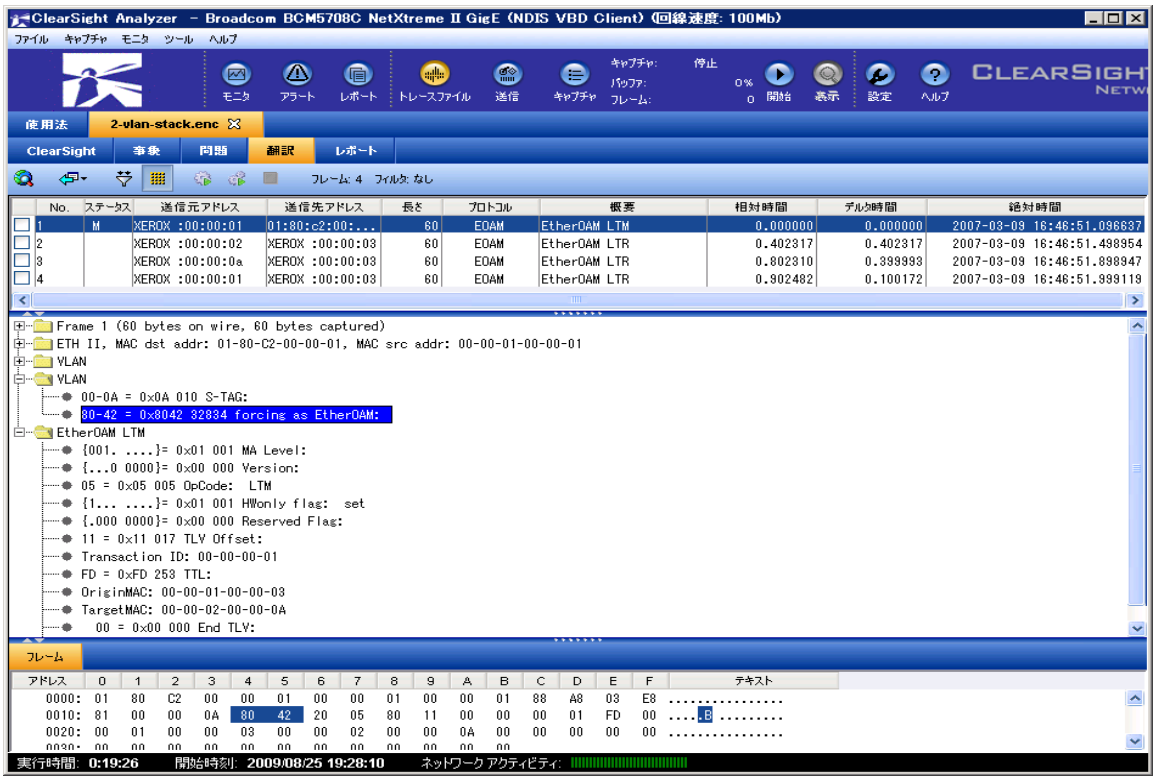


図 7-7: Ethernet OAM フレームの翻訳

3G-324M フレームの翻訳

CSA は 3G-324M フレームを翻訳でき、再構成およびビット反転したフレームを **[Hex]** ペインに表示できます。しかし、3G-324M フレームを正常に翻訳するためには、**[設定]** > **[設定]** > **[共通]** > **[プロトコル設定]** 画面で、**[ポート範囲]** フィールドにポート番号 2000 を指定する必要があります (図 7-8 を参照)。

CSA で 3G-324M にポート番号 2000 を設定するためには、最初に Skinny に 2000 以外のポート番号を一時的に割り当てる必要があります。Skinny に 2000 以外のポート番号が設定されている場合は、CSA は Skinny フレームを正常に翻訳できません。Skinny フレームは TCP フレームと翻訳されます。



図 7-8: 3G-324M プロトコルを翻訳するためのポート番号の設定

3G-324M ビデオコンテンツの再生

ClearSight では、コーデックが AMR または MPEG4 の場合に、ClearSight のユーザインターフェース内から 3G-324M ビデオコンテンツを再生することもできます。

3G-324M ビデオコンテンツを再生するには :

1. [フロー] ペインでの 3G-324M フローをクリックします。
2. [統計] ペインは組み込みメディアプレイヤーの領域を含むように更新します。**[再生]** ボタンをクリックして、3G-324M ビデオストリームを再生します。

図 7-9 は、再生中の 3G-324M ビデオストリームが表示されている画面の例です。

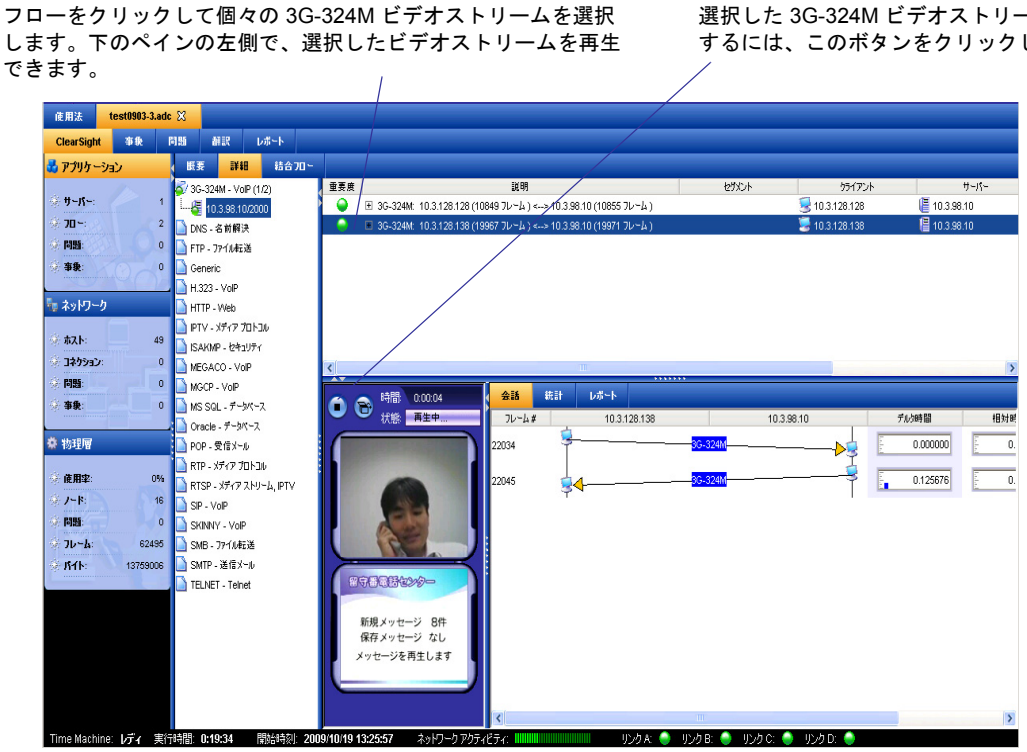


図 7-9: 3G-324M ビデオコンテンツの再生

ビデオ画面のサイズを大きくするには、ボタンをクリックします。

[翻訳] タブの設定オプション

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSight Distributed

[**翻訳**] タブの画面の設定オプションは、**[設定]** ボタン > **[設定]** タブ > **[翻訳]** で設定します。これらの画面における選択は、トレースファイルを開くとき、またはキャプチャバッファを表示するときに表示される情報に影響します。ページの左側のメニューで、対応する項目をクリックしてください。

[翻訳] > [全般] オプション

図 7-10 は、**[翻訳]** > **[全般]** 画面を示しています。

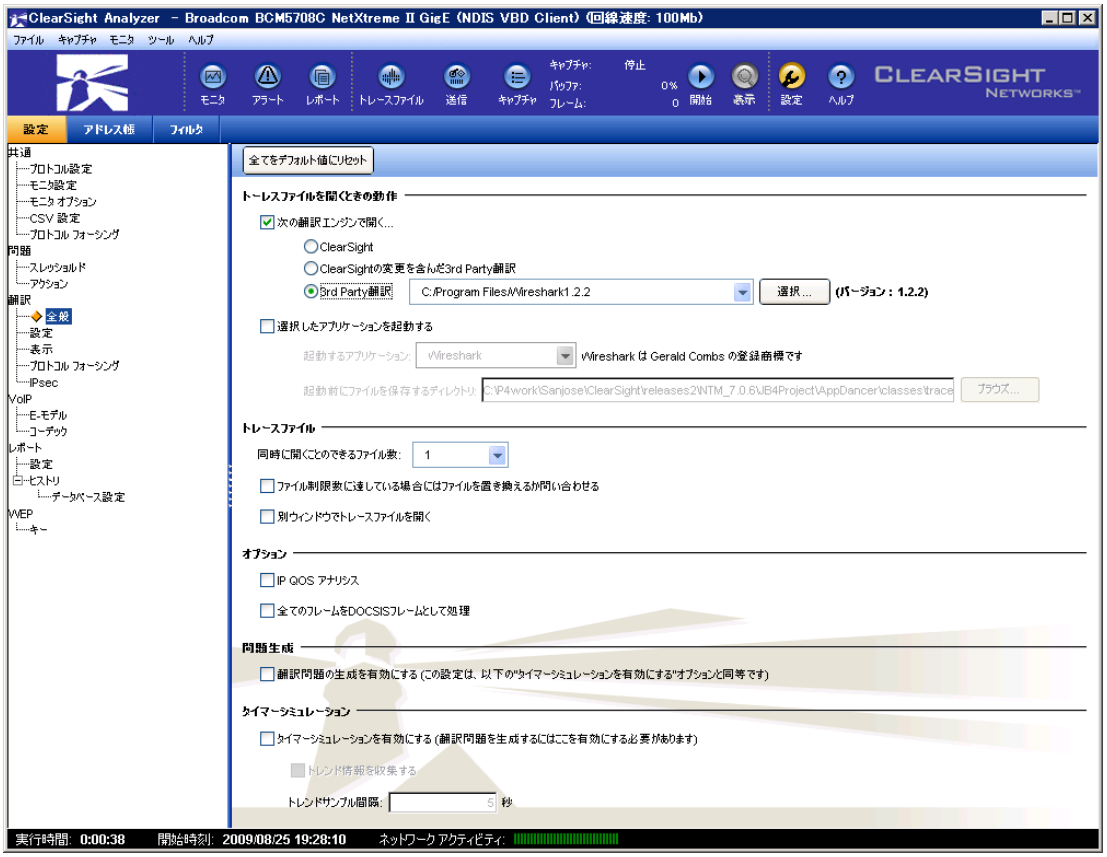


図 7-10: [翻訳] > [全般] 設定画面

[トレースファイルを開くときの動作]

翻訳エンジンを選択し、CSA の [翻訳] タブの表示を構築できます。**[トレースファイルを開くときの動作]** のオプションは、以下の通りです。

[ClearSight]	ClearSight Analyzer で提供されているデフォルトの翻訳エンジン。
[ClearSight の機能を含んだ 3rd Party 翻訳]	ClearSight Analyzer パッケージに含まれる代替翻訳エンジン。
[3rd Party 翻訳]	サードパーティのウェブサイトから取得できる代替翻訳エンジン。

ClearSight Analyzer ソフトウェアを初めてインストールするときに **ClearSight の機能を含んだ 3rd Party 翻訳エンジン**をインストールすると、プログラムによってそれが認識され、自動的に **[ClearSight の機能を含んだ 3rd Party 翻訳]** オプションが選択されます。

3rd Party 翻訳エンジン（現在完全にテストされているものは Wireshark® バージョン 1.2.2 のみになります）をインストールした場合、CSA はプログラム開始時にそれを検出し、ドロップダウンリストにそのインストールフォルダを表示します。3rd Party 翻訳エンジンが一つ以上インストールされている場合には、**[選択 ...]** ボタンをクリックして使用したい翻訳エンジンを選択することができます。1.2.2 以外のバージョンを選択した場合には、そのバージョンの翻訳エンジンは CSA では完全にテストされていませんという警告メッセージが表示されます。また選択したフォルダに 3rd Party 翻訳エンジンが含まれていない場合には、その旨の警告メッセージが表示されます。

外部アプリケーションの起動

[次の翻訳エンジンで開く] 領域で選択した翻訳エンジンに代わりまたは加えて、Wireshark® または Snort® のような外部アプリケーションを起動できます。**[選択したアプリケーションを起動する]** を有効にした場合は、処理されたトレースファイルのデータは、CSA ではなくそのアプリケーション内のウィンドウに表示されます。

ドロップダウンリストに表示され、起動できるようにするために、外部アプリケーションはビューア PC (エージェントマネージャおよび CSA エージェントビューアがインストールされた PC) にインストールされている必要があります。デフォルトでは、Wireshark および Snort は事前設定されており、存在する場合はドロップダウンリストに表示されます。

CSD エージェントにトレースファイルが保存された場合は、アプリケーションを起動する前にビューア PC に転送する必要があります。ローカル (ビューア PC 上) の対象ディレクトリ名を **[起動前にファイルを保存するディレクトリ]** フィールドに指定します。

トレースファイルを開くためには、**[ファイル]** メニューから **[開く]** を選択肢、CSD エージェントのトレースファイルを参照します。ファイルは転送され、.pcap フォーマットでない場合は、.pcap に変換されます。そして、選択されたアプリケーションは自動的に起動します。

開くトレースファイルがビューア PC 上に存在する場合は、**[ファイル]** メニューから **[トレースファイルを開く]** を選択して下さい。トレースファイルが .pcap フォーマットでない場合は、.pcap に変換されます。そして、選択されたアプリケーションは自動的に起動します。

注意 : [次の翻訳エンジンで開く] または **[選択されたアプリケーションを起動する]** のいずれか、または両方を有効にできます。両方を有効にした場合は、**[次の翻訳エンジンで開く]** の選択は、CSA の [翻訳] タブの表示に影響します。**[選択されたアプリケーションを起動する]** の選択は、トレースファイルがそのアプリケーション内のウィンドウに表示される原因になります。

[トレースファイル]

[トレースファイル] のオプションでは、一度に複数のトレースファイルをロードすることができます。**[同時に開くことのできるファイル数]** で、同時に開くことができるトレースファイルの最大数 (1、2、3、4 または 5) を選択できます。

[ファイル制限数に達している場合にはファイルを置き換えるか問い合わせる] をオンにした場合、ClearSight は、開いたトレースファイ

ルのうち最も古いものを置換する前にプロンプトを表示します。たとえば、制限が 3 で、4 番目のトレースファイルを開こうとした場合、最初に開いたものを置換してもよいかどうかが尋ねられます。このボックスをオンにしなかった場合は、4 番目のファイルを開く前に、最初に開いたファイルが自動的に閉じます。

[別ウィンドウでトレースファイルを開く] をオンにした場合、ClearSight は個別のウィンドウに各トレースファイルを開きます。このボックスをオンにしなかった場合は、すべてのトレースファイルが同じウィンドウの中で個別のタブに開きます。

[オプション]

[翻訳] > **[全般]** の **[オプション]** にあるオプション項目とその説明を表 7-4 に示します。

表 7-4: **[翻訳]** > **[全般]** のオプション

翻訳表示設定	説明
[IP QOS アナリシス]	**[詳細]** ペインの [IP] セクションで ToS (Type of Service) 翻訳を DiffServ (Differentiated Services) 翻訳に置き換えるには、このチェックボックスをオンにします。
[全てのフレームを DOCSIS フレームとして処理]	すべてのフレームを、通常の Ethernet フレームではなく DOCSIS フレームとして解釈する場合は、このチェックボックスをオンにします。

[問題生成]

[問題生成] チェックボックスをオンにすると、**[タイマーシミュレーションを有効にする]** チェックボックスをオンにした場合と同じ効果があります。「[タイマーシミュレーション] の設定」を参照してください。

[タイマーシミュレーション] の設定

[タイマーシミュレーション] の下にあるオプション項目とその説明を表 7-5 に示します。

表 7-5: [翻訳] > [全般] オプションの [タイマーシミュレーション] の設定

[タイマーシミュレーション] の設定	説明
[タイマーシミュレーションを有効にする (翻訳問題を生成する必要があります)]	トレースファイルを開くときに、ClearSight の解析機能を使用して問題を報告する必要がある場合は、このオプションを有効にします。 **注記 :** 翻訳問題の生成を行うと、大きなトレースファイルを開く際に時間がかかる場合があります。 このオプションを有効にすると、ポストアナリシスロジックが有効になります。ポストアナリシスロジックは、リアルタイムで生成されたときと同様の方法でポストアナリシスの問題を生成することを主な目的として、トレースファイルの期間の時間経過をシミュレートします。
[トレンド情報を収集する]	トレンド情報を収集する場合は、このオプションを有効にします。この情報は、**[マルチキャスト]** タブの統計ペインにある **[トレンド]** タブ、または VoIP QoS レポートの **[ジッター]** セクションに表示されます。 トレンド情報は、タイマーシミュレーションロジックが実行していないかぎり収集できません。そのため、**[トレンド情報を収集する]** オプションを選択する場合は、**[タイマーシミュレーションを有効にする]** を最初に選択する必要があります。
[トレンドサンプル間隔]	このフィールドで、トレンド情報を収集するためのデータをサンプリングする頻度を秒単位で指定します。

注記 : [翻訳] オプションに対して行った変更は、動的に有効になります。ClearSight を終了して再起動する必要はありません。

現在、**[トレンド情報を収集する]** オプションによって、ポストアナリシスで収集されデータベース内に保存される トレンド情報の収集が制御されています (トレースファイルが長期間である場合は特に、データポイントが無制限に収集される可能性があるため)。トレンド情報は、**[マルチキャスト]** タブの **[トレンド]** タブ (の下部) に表示されます。トレンドフラグがオンになっていてこれらのテーブルにエントリがある場合は、(そのエントリを選択すると) オクテットとフレームが時間の経過とともにどのように到着したかを示すグラフが表示されます。このオプションが有効でない場合は、[トレンド情報を収集する] 設定へのリンクを含むパネルが表示されます。

[翻訳] > [設定] オプション

図 7-11 は、**[翻訳]** > **[設定]** 画面を示しています。



図 7-11: [翻訳] > [設定] 設定画面

[ラダー表示]

[ラダー表示] 項目では、個々のラダー表示ができる「段」の最大数を指定できます。この数は、アプリケーションや接続などに対して個別に設定することができます。

[ネットワークコネクション]

[ネットワークコネクション] 項目では、ClearSight が測定するネットワークコネクションの最大数を指定できます。

[アプリケーション]

[アプリケーション] 項目では、ClearSight で統計を維持するために、サポートされている各アプリケーションタイプのサーバーとフローの最大数を指定できます。特定のタイプのサーバーまたはフローの上限値に到達すると、ClearSight は新しいサーバーやフローのカウンタをモニタ画面で作成しなくなります。

ヒント : これらのオプションは、モニタするうえで最も重要なサーバーとフローのタイプに合わせて ClearSight のパフォーマンスを設定するために使用してください。ClearSight でモニタするよう指定したサーバーとフローの数が多いほど、消費される ClearSight PC のリソースも多くなります。モニタ用リソースは、最も重要なサーバーとフローに割り当ててください。

[翻訳] > [表示] オプション

図 7-12 は、**[翻訳] > [表示]** 画面を示しています。



図 7-12: [翻訳] > [表示] 設定画面

[オプション]

[オプション] 項目の下にあるチェックボックスとその説明を表 7-6 に示します。

表 7-6: [翻訳] > [表示] オプションの [オプション] 設定

翻訳表示設定	説明
[ネットワークアドレスの使用]	[概要] ペインで MAC アドレスではなくネットワークアドレスを使用する場合は、このチェックボックスをオンにします。
[名前の解決]	可能な場合にドメイン名を使用して IP アドレスを表示するには、このチェックボックスをオンにします。
[テキストを EBCDIC で表示]	[Hex] ペインで ASCII ではなく EBCDIC 翻訳を使用する場合は、このチェックボックスをオンにします。
[トランスポート サマリのみ表示]	[概要] 列に、フレーム内の最上位層プロトコルに関する情報ではなく、トランスポートプロトコル (TCP、UDP など) に関する情報を表示するには、このチェックボックスをオンにします。
[詳細画面を展開]	[詳細] ペインのすべての ⊞ スイッチを開くには、このチェックボックスをオンにします。

[サマリオプションフィールド]

[サマリオプションフィールド] 項目の下にある選択肢とその説明を表 7-6 に示します。

表 7-7: [翻訳] > [表示] オプションの [サマリオプションフィールド] 設定

翻訳表示設定	説明
[パケット長]	[サマリ] ペインに含ませるフィールドを選択します。これらの各オプションの説明については、238 ページの表 7-2 を参照してください。
[絶対時間]	
[デルタ時間]	
[相対時間]	
[プロトコル]	

[プロトコルの色]

[翻訳] > **[表示]** の **[プロトコルの色]** のオプションで、**[翻訳]** タブでさまざまなプロトコルに対して使用する色を指定できます。適切な色設定を行うことで、**[翻訳]** タブでの長時間にわたるトラブルシューティングセッションの際に視覚的にわかりやすくすることができます。リストでプロトコルを選択し、使用する色を右側のパレットでクリックします。

[プロトコルのフォント]

[翻訳] > **[表示]** の **[プロトコルのフォント]** のオプションで、**[翻訳]** タブでさまざまなプロトコルに対して使用するフォントを指定できます。フォントを指定するにはドロップダウンリストでフォントを選択します。

[翻訳] > [プロトコルフォーシング] オプション

図 7-13 は、**[翻訳]** > **[プロトコルフォーシング]** 画面を示しています。

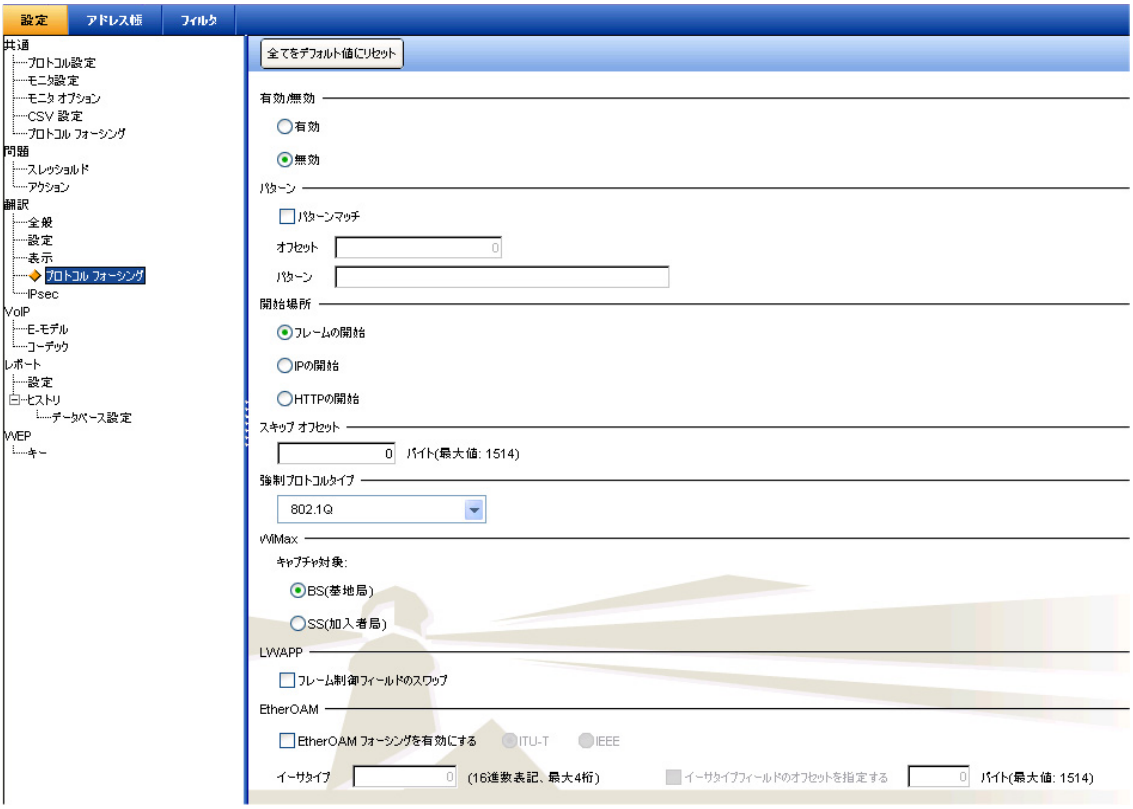


図 7-13: [翻訳] > [プロトコルフォーシング] 設定画面

注記：ClearSight の機能を含んだ 3rd Party 翻訳を選択しない場合は、プロトコルフォーシングをサポートしません。**ClearSight の機能を含んだ 3rd Party 翻訳**以外を選択した場合は、図 7-13 の設定画面が表示される代わりに警告メッセージが表示されます。

[有効 / 無効]

[有効 / 無効] 領域では、プロトコル強制のオン / オフを切り替えることができます。**[無効]** 選択した場合は、他の領域でさらにオプションを設定できますが、この領域で **[有効]** を選択するまでは設定が有効になりません。

[パターン]

[パターン] 領域では、プロトコル強制のためにマッチさせるパターンを入力することができます。入力するオフセットは、常にフレームの先頭からになります。パターン入力は 16 進でなければなりません。パターンマッチを有効にするには、**[パターンマッチ]** ボックスをオンにします。

[開始場所] および [スキップオフセット]

[開始場所] 領域では、強制プロトコルの検索を開始する場所を ClearSight に指示することができます。

- **[フレームの開始]** を選択した場合、ClearSight の検索場所はフレームの先頭に **[スキップオフセット]** をプラスしたところになります。
- **[IP の開始]** を選択した場合、ClearSight の検索場所は IP スタックの先頭に **[スキップオフセット]** をプラスしたところになります。
- **[HTTP の開始]** を選択した場合、ClearSight の検索場所は HTTP スタックの先頭に **[スキップオフセット]** をプラスしたところになります。

[強制プロトコルタイプ]

[強制プロトコルタイプ] 領域では、ドロップダウンリストから強制プロトコルを選択することができます。リストの内容は、**[開始場所]** 領域で行った選択と相関関係があることに注意してください。

[LWAPP]

[LWAPP](Lightweight Access Point Protocol) 領域で **[フレーム制御フィールドのスワップ]** ボックスをオンにすると、フレーム制御レジスタ内のバイトをスワップできます。これらのバイトの位置については、現在 2 つの規定が使用されているため、このボックスをオンにして翻訳する必要があるかどうかはフレームによって異なります。

[EtherOAM]

Ethernet OAM フレームのプロトコルフォーシングを有効にする場合は、**[EtherOAM フォーシングを有効にする]** ボックスをオンにします。Ethernet OAM として翻訳するイーサタイプの値（16 進数）を入力し、[イーサタイプ] フィールドにバイトオフセットをフレームの先頭から入力します。

注記：[EtherOAM] は、Ethernet OAM の特別のライセンスによってこの機能が有効にされている場合にのみ、この画面に表示されます。

WiMax

[強制プロトコルタイプ] から WiMax を選択した場合は、キャプチャを行うのが BS (ベースステーション) なのか SS (加入者ステーション) なのかを指定する必要があります。

注記：[WiMax] は、WiMax の特別のライセンスによってこの機能が有効にされている場合にのみ、この画面に表示されます。

IPsec 翻訳オプション

大半のインターネットセキュリティプロトコルはトランスポート層またはそれ以上の層で動作しますが、IPsec はネットワーク層で動作するため、さまざまな状況で利用することができます。ClearSight は、**[設定] ボタン >[設定] タブ >[翻訳]>[IPsec]** 画面で適切な**暗号ペイロード（ESP：Encapsulation Security Payload）**の選択肢およびパラメータが設定されている場合、IPsec フレームを翻訳することができます。

図 7-14 は、**[翻訳]>[IPsec]** 画面を示しています。この画面では、IP Security（IPsec）の翻訳オプションを設定できます。



図 7-14: IPsec 翻訳構成画面

注記：3rd Party 翻訳は IPsec 翻訳をサポートしません。**3rd Party 翻訳**を選択した場合は、図 7-14 の設定画面に表示される機能は無効になります。IPsec 翻訳を行うには、3rd Party 翻訳ソフトウェア自身の IPsec 翻訳設定を行う必要があります。この場合、設定画面が表示される代わりに警告メッセージが表示されます。

ESP 一般設定

[ESP 一般設定] 領域では、暗号化された ESP フレームを検出して翻訳するかどうか、また、それとは独立して ESP 認証を確認するかどうかを設定できます。認証の使用は強く推奨されているため、実際には認証なしで暗号化を使用することはほとんどありません。

ESP パラメータセット

[ESP パラメータセット] 領域では、翻訳プロセスで使用する ESP パラメータセットを指定することができます。

ESP パラメータセットを追加するには、**[追加]** ボタンをクリックします。パラメータセット領域が表示され、パラメータを入力できます。

ESP パラメータセットを削除するには、削除したいパラメータセットの **[削除]** ボタンをクリックします。

ESP パラメータセットファイルは、標準フォーマットを使用し、通常は .txt ファイルで保存されます。既存の ESP パラメータセットを使用する場合は、**[インポート]** ボタンをクリックします。[開く] ダイアログボックスが表示され、テキストファイルの場所をブラウズできます。

注記：パラメータセットを変更した場合、その変更は次回トレースファイルを開いたときに有効になります。

トレースファイルの使用



ClearSight では、以下を含むさまざまな共通トレースファイル形式を開くことができます。

- ClearSight (*.adc)
- パケットキャプチャ (*.pcap)
- ジェネリックキャプチャファイル (*.cap)

トレースファイルを使用するためのコマンドのほとんどは、**[ファイル]** メニューに含まれます。**[ファイル]** メニューには、ファイルを使用するための以下のコマンドが含まれます。

[開く]	一般的な「開く」ダイアログボックスを表示し、開きたい保存済みトレースファイルに移動できるようにします。
[最近開いたファイル]	最近開いた、または保存したトレースファイルを一覧表示し、よく使用するファイルに簡単にアクセスできるようにします。
[保存]	一般的な「保存」ダイアログボックスを表示し、(現在キャプチャバッファにあるフレームの) 保存するトレースファイルのパスとファイル名を指定できるようにします。 トレースファイルは、ClearSight 形式 (*.adc) または Network General の .enc 形式で保存できます。
[名前をつけて保存]	一般的な「名前をつけて保存」ダイアログボックスを表示し、現在のトレースファイルに別のパスとファイル名を指定して保存できるようにします。
[閉じる]	現在のトレースファイルを閉じます。

[マージ]	最大で 4 つの既存のトレースファイルをマージして、新しいトレースファイルを作成できます。マージできるファイル形式は、.adc、または .pcap です。マージ後に生成されるファイルは、.adc 形式にする必要があります。

第 8 章

複数セグメント解析

この章では、ClearSight の複数 - セグメント解析機能について説明します。この章は、次の項目で構成されています。

- 「複数セグメント解析」
- 「マージしたトレースファイルの作成」
- 「VoIP 結合フローの表示」
- 「その他の結合フローの表示」
- 「自動結合フィルタの使用」
- 「[複数 - ティア] タブの使用」
- 「[NAT] タブの使用」
- 「手動によるフローの結合」
- 「複数セグメントのリアルタイム モニタ」

複数セグメント解析

ClearSight Application Flow Analyzer ClearSignt Distributed

ClearSight には、複数のネットワークセグメントで収集したデータを関連付ける機能があります。最大で 4 つのセグメントを関連付けることができます。複数セグメント解析を使用すると、接続をエンドツーエンドで表示し、2 つ以上のセグメントが関係する場合にトランザクションがどのように伝播するかを確認することができます。これにより、ボトルネックやその他の問題が存在する場所の確認が容易になります。

マージしたトレースファイルの作成

ClearSight Application Flow Analyzer ClearSignt Distributed

一般的に、複数セグメント解析の第一歩は、2 つ以上のネットワークセグメントからデータを収集してそれを個別のトレースファイルに保存することです。次に、それらのトレースファイルをマージする必要があります。ClearSight では、複数のセグメントが関係するトランザクションを表示するときの方法で、トレースファイルのマージを処理することができます。

注記 : また、複数のセグメントからのリアルタイムモニタを実行することもできます (278 ページの「複数セグメントのリアルタイム モニタ」を参照)。ただしこの章では、話が複雑にならないようにトレースファイルのポストキャプチャアナリシスを中心に説明します。

2 つ以上のトレースファイルをマージするには、以下の手順を実行します。

1. **[ファイル]** メニューから **[マージ]** を選択します。**[マージするファイルの選択]** ダイアログボックスが表示されます。
2. マージするファイルがある場所に移動します。目的のファイルをクリック (または Ctrl キーを押しながらクリック) します。図 8-1 のような画面が表示されます。

3. **[開く]** をクリックします。選択したファイルが含まれた状態で、**[ClearSight ファイル マージ]** ダイアログボックスが表示されます。わかりやすいセグメント名を選択できます。ファイルに別のセグメント名を付けるには、そのファイルの **[セグメント]** 列をダブルクリックします。新しい名前を入力するか、ドロップダウンリストから名前を選択します。
4. 最初のパケットのタイムスタンプがすべてのトレースファイル内で同一ではない場合は、**[オフセット時間 (秒)]** 列に任意のファイルの調整係数を入力できます。

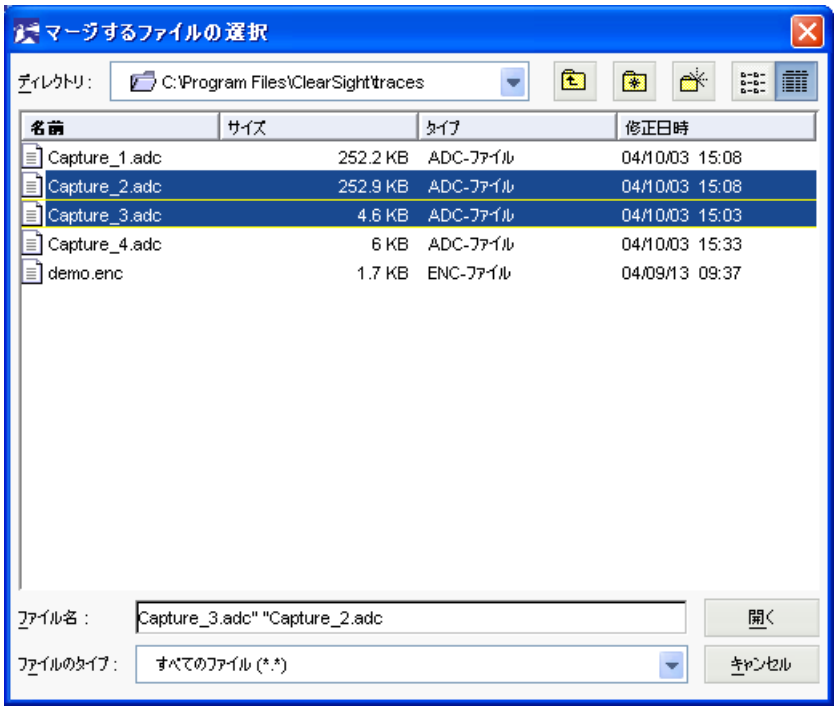


図 8-1: [マージするファイルの選択] ダイアログボックス



図 8-2: [マージするファイル]

5. この処理を続けて、含めるファイルをすべて集めます。次に、**[マージ]** ボタンをクリックします。**[マージ保存先]** ダイアログボックスが表示されます。
6. ファイルを保存する場所に移動し、マージファイルの名前を選択して、**[保存]** をクリックします。これで、新しくマージしたトレースファイルを ClearSight Analyzer で開くことができます。

   注記 : マージできるファイル形式は、.adc、.enc、および .pcap です。マージ後に生成されるファイルは、.adc 形式にする必要があります。

VoIP 結合フローの表示

ClearSight Application Flow Analyzer | ClearSignt Distributed

ClearSight では、VoIP フローはコール ID に基づいて測定されます。特定の VoIP アプリケーションの複数のフローで同じコール ID が出現する場合は、結合フローが作成されます。

VoIP アプリケーションの結合フローを表示するには、以下の操作を実行します。

1. 複数セグメントの VoIP データが含まれたトレースファイルを開きます。
2. **[詳細]** タブの**メイン**ペインで、目的の VoIP アプリケーションを選択します。

3. **フロー**ペインで、フローを段階的に開き、複数のセグメントがリストされているフローを確認します。
4. それらのフローのうちの 1 つを選択して、**統計**ペインの **[会話]** タブで複数セグメントラダー画面を表示します。図 8-3 は、その典型的な例を示したものです。

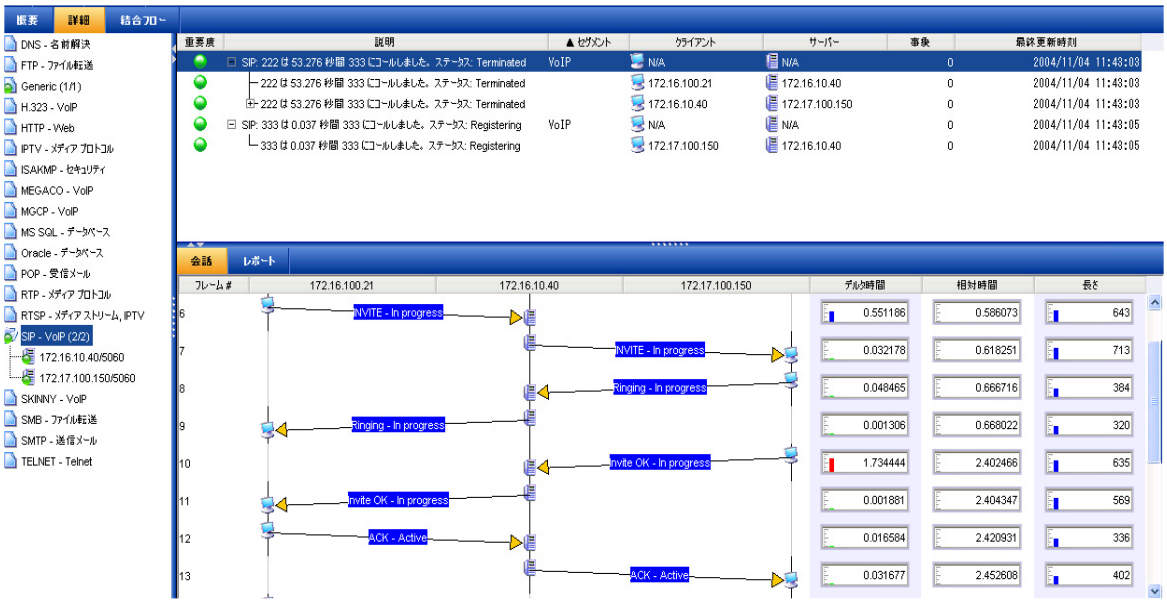


図 8-3: 複数セグメントの VoIP フローの表示

ラダービューの操作

セグメントビュー (図 8-4) と非セグメントビュー (図 8-5) を切り替える必要が生じることがあります。非セグメントビューに切り替えるには、ラダー図上の任意の場所を右クリックして、表示されたメニューで **[セグメント情報を表示しない]** チェックボックスをオンにします。セグメントビューに戻るには、このチェックボックスをオフにします。

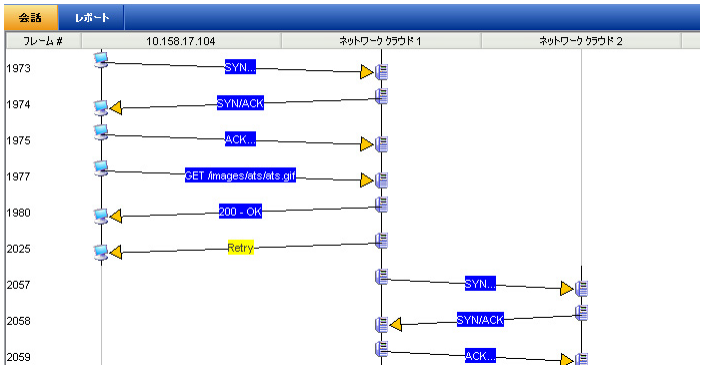


図 8-4: セグメントビュー

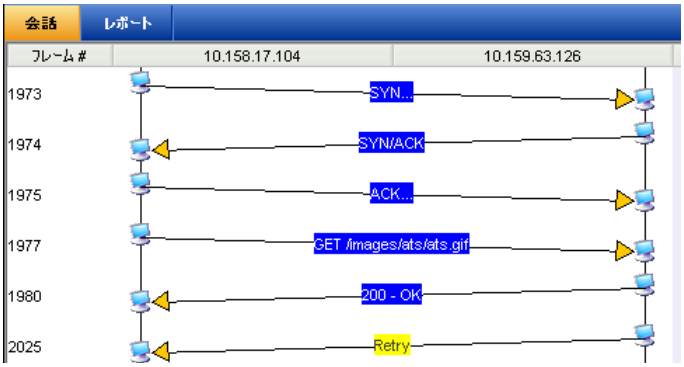


図 8-5: 非セグメントビュー

注記 : プルダウンメニューで **[ファイル]** > **[印刷]** と選択して、ラダー図を印刷できます。また、ラダー図を pdf ファイルに保存することもできます。その場合は、ラダー図上の任意の場所を右クリックします。**[エクスポート]** 項目が含まれたメニューが表示されます。**[エクスポート]** をクリックすると **[エクスポート]** ダイアログボックスが表示されます。このダイアログボックスでファイルの保存先を指定できます。

その他の結合フローの表示

ClearSight Application Flow Analyzer　ClearSignt Distributed

ClearSight では、VoIP 以外のアプリケーションのフローは、送信元 IP アドレスとポート番号に従って測定されます。適度に短い時間間隔で複数のセグメントに同じ IP アドレスとポートのペアが出現する場合に、結合フローが作成されます。

VoIP 以外のアプリケーションの結合フローを表示するには、以下の操作を実行します。

1. 複数セグメントのデータが含まれたトレースファイルを開きます。
2. **アプリケーション**層の **[結合フロー]** タブに移動します。
3. トレースファイル内のすべてのアクティブなアプリケーションについて、結合フローと見なされたフローが、**フロー**ペインにすべて表示されます。個別のフローを選択すると、**統計**ペインの **[会話]** タブに複数セグメントラダービューが表示されます。[レポート] タブにはパフォーマンス関連の統計とアドバイスがいくつか表示されます。

図 8-6 は、DNS が選択されている状態の結合フロー画面を示したものです。

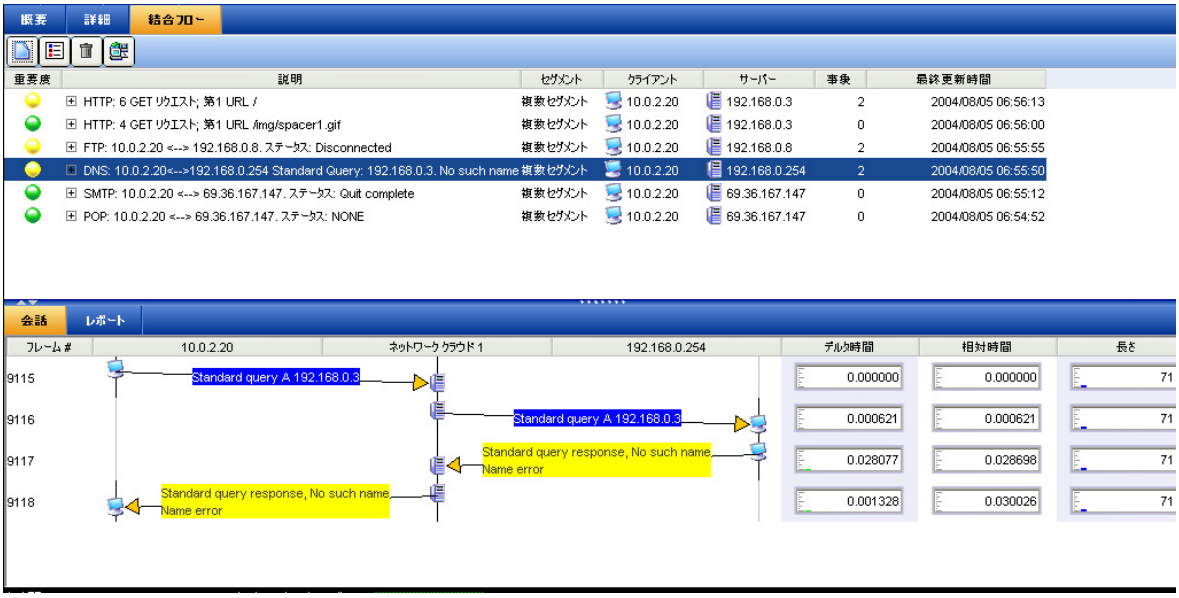


図 8-6: 複数セグメントの DNS フローの表示

ラダービューの操作

セグメントビュー (図 8-7) と非セグメントビュー (図 8-8) を切り替える必要が生じることがあります。非セグメントビューに切り替えるには、ラダー図上の任意の場所を右クリックして、表示されたメニューで **[セグメント情報を表示しない]** チェックボックスをオンにします。セグメントビューに戻るには、このチェックボックスをオフにします。

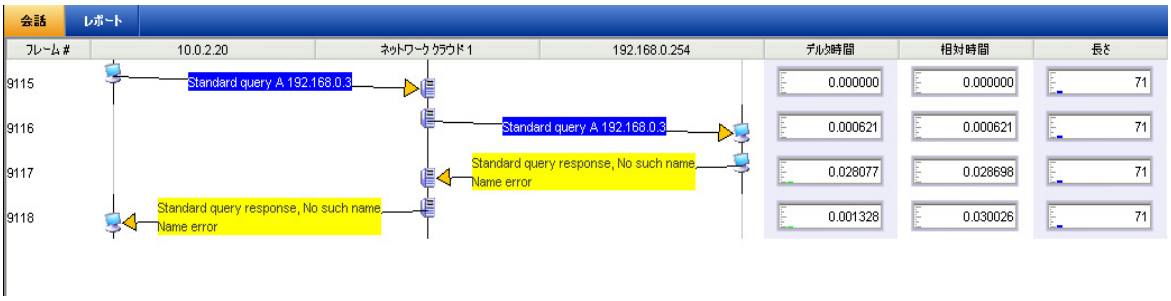


図 8-7: セグメントビュー

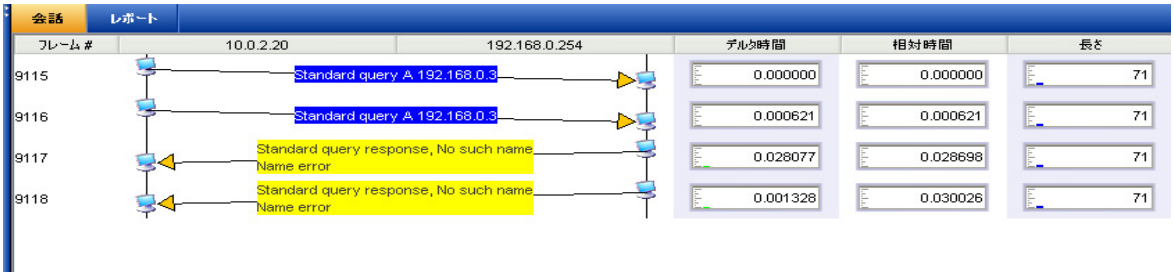


図 8-8: 非セグメントビュー

注記 : プルダウンメニューで **[ファイル]** > **[印刷]** と選択して、ラダー図を印刷できます。また、ラダー図を pdf ファイルに保存することもできます。その場合は、ラダー図上の任意の場所を右クリックします。**[エクスポート]** 項目が含まれたメニューが表示されます。**[エクスポート]** をクリックすると **[エクスポート]** ダイアログボックスが表示されます。このダイアログボックスでファイルの保存先を指定できます。

自動結合フィルタの使用

ClearSight Application Flow Analyzer　ClearSignt Distributed

デフォルトでは、[結合フロー] タブには、トレースファイルにおいて結合フローが認識されたアプリケーションがすべて表示されます。ほとんどの場合、すべてのアプリケーションや送信元 / 送信先アドレスが解析の対象となることはありません。そのため ClearSight では、表示をフィルタして必要な領域に焦点を絞ることができます。

結合フローの表示フィルタを設定するには、以下の操作を実行します。

1. 複数セグメントのデータが含まれたトレースファイルを開きます。
2. **アプリケーション**層の **[結合フロー]** タブに移動します。
3. タブの上部にある **[自動結合フロー]** アイコンをクリックします。図 8-9 に示されるような、複数セグメントフィルタのダイアログボックスが表示されます。

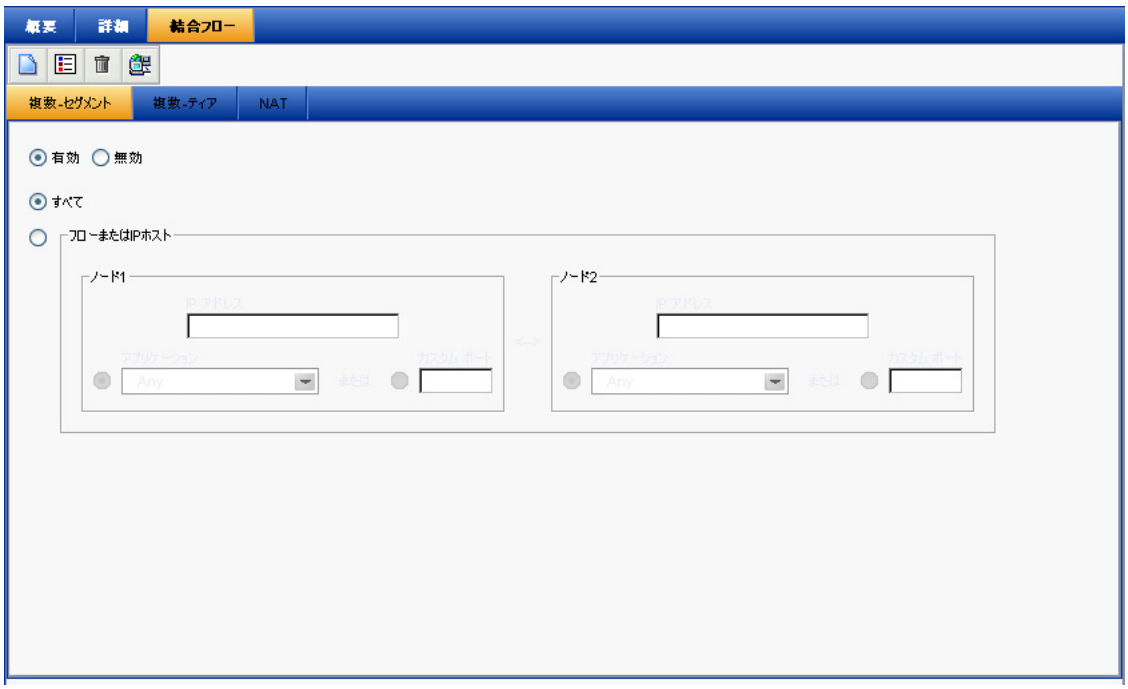


図 8-9: 複数セグメントフィルタのダイアログボックス

[有効] ボタンと **[無効]** ボタンは、複数 - セグメント解析を実行するかどうかを制御するためのトグルボタンです。**[有効]** を選択した場合は、**[すべて]** (すべての複数 - セグメントフローを処理して表示する場合) または **[フローまたは IP ホスト]** (処理および表示の対象を絞り込む場合) を選択できます。

4. **[フローまたは IP ホスト]** を選択します。画面は、図 8-10 のようになります。

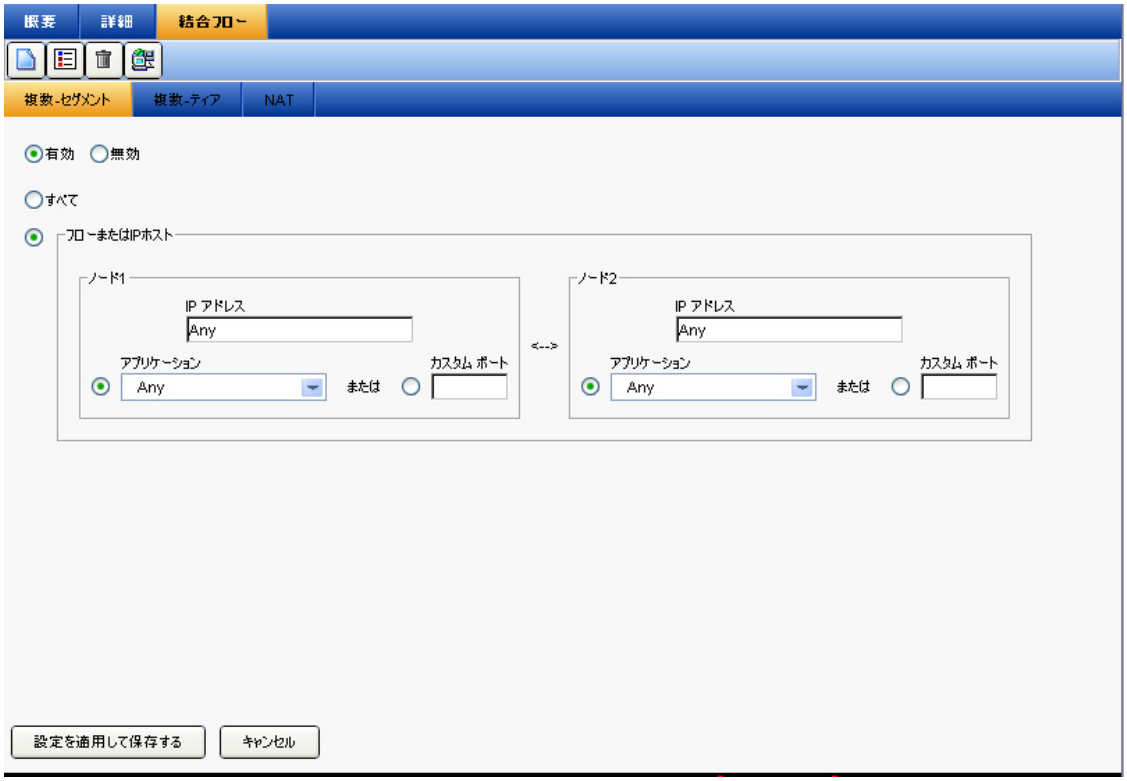


図 8-10: [フローまたは IP ホスト] が選択された画面

5. **[フローまたは IP ホスト]** ボックス内の 2 つの枠は、会話のエンドポイントを示しています。たとえば今、IP アドレス 10.0.2.20 および 69.36.167.147 のホスト間のトランザクションを解析しようとしていると仮定します。その場合、**[IP アドレス 1]** に「10.0.2.20」を、**[IP アドレス 2]** に「69.36.167.147」をそれぞれ入力するだけです。

フィルタを使用して、**[IP アドレス]** ボックスで指定したパーティ間の特定のアプリケーションまたはポート番号に解析対象を絞り込むことができます。その場合は、**[アプリケーション]** のプルダウンリストからアプリケーションを選択するか、**[カスタム ポート]** にポート番号を入力します。**[IP アドレス]** で入力した内容と **[アプリケーション]** または **[カスタム ポート]** で入力した内容は、AND (論理積) の関係にあることに注意してください。

6. アプリケーションに関係なく、IP アドレス 10.0.2.20 および 69.36.167.147 の間のすべての会話が解析対象であると仮定します。その場合、複数 - セグメントフィルタのダイアログボックスは、図 8-11 のようになります。



図 8-11: 2 つの IP ホスト間のトランザクションのフィルタリング

7. **[設定を適用して保存する]** をクリックします。新たにフィルタされた画面が生成され、アプリケーション層の [概要] ペインが表示されます。

8. **[結合フロー]** タブに戻ります。新しい画面には、10.0.2.20 と 69.36.167.147 の間の会話 (この例では SMTP アプリケーションと POP アプリケーション) だけが表示されます。フローを選択すると、複数 - セグメントラダー図が表示されます。図 8-11 で選択されているフローの場合、Isun が自分の電子メールを取得中であることがわかります (図 8-12)。

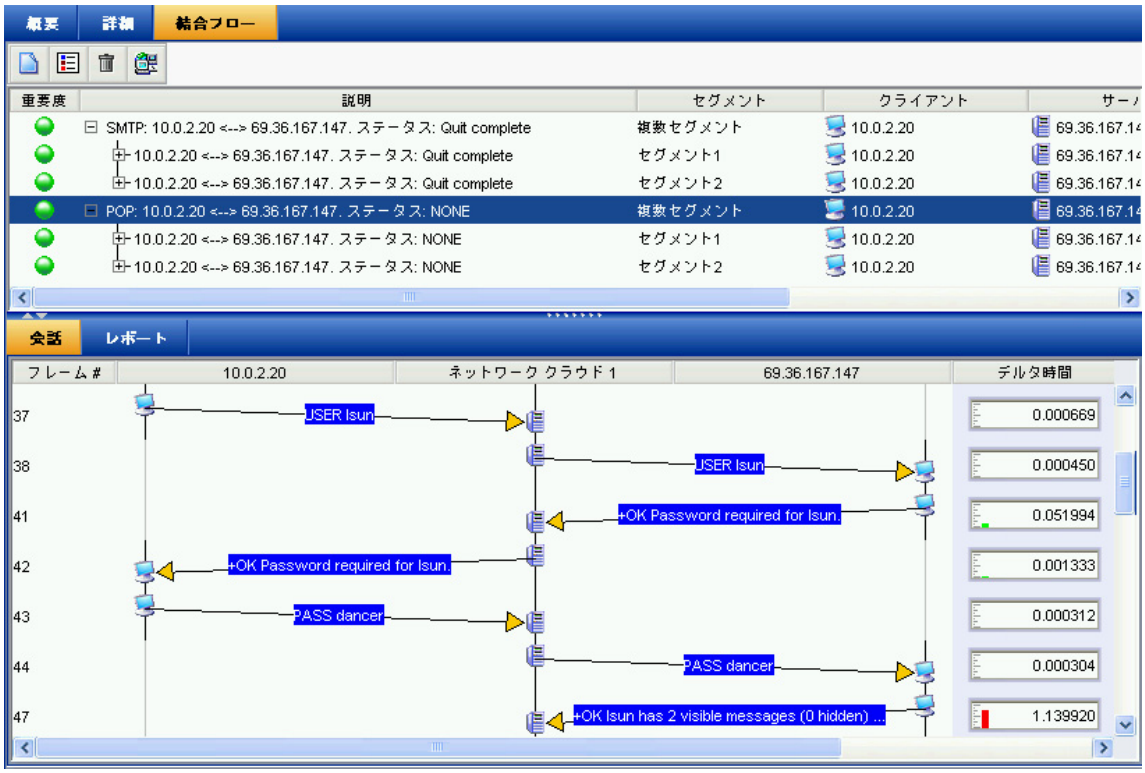


図 8-12: lsun が自分の電子メールを取得する

[複数 - ティア] タブの使用

ClearSight Application Flow Analyzer　ClearSignt Distributed

結合フローをフィルタする方法として、**[自動結合フロー]** 機能の **[複数 - ティア]** タブを使用する方法もあります。[複数 - セグメント] タブのフィルタがすべてのセグメントに適用されるのに対して、**[複数 - ティア]** タブのフィルタは各セグメントに個別に適用できます。ティアは、基本的にはセグメントです。つまり、**[ティア 1]** は [ClearSight ファイル マージ] ダイアログボックスの 1 行目に表示されているセグメントを指し、**[ティア 2]** は 2 行目に表示されているセグメントを指します。以降の番号のティアも同様です。

[有効] ボタンと **[無効]** ボタンは、複数ティア解析を実行するかどうかを制御するためのトグルボタンです。**[有効]** を選択した場合は、2 ティア、3 ティア、または 4 ティアの解析を選択できます。

ティア同士は OR (論理和) の関係にあります。つまり、[ティア 1] で設定した制限と、[ティア 2]、[ティア 3] などで設定した制限が OR で結ばれます。

また、**[複数 - ティア]** タブで定義したフィルタと **[複数 - セグメント]** タブで定義したフィルタも、OR で結ばれます。**[設定を適用して保存する]** をクリックすると、これら両方のタブからの情報によって画面が更新されます。

複数ティアフィルタリングを使用して、実際にはティアが物理的に別個のセグメントになっていない状況を解析することもできます。たとえば、IP アドレスが x.x.x.x のクライアント、IP アドレスが y.y.y.y のサーバー、IP アドレスが z.z.z.z のデータベースがあると仮定します。この場合、[ティア 1] タブには x.x.x.x/y.y.y.y の組み合わせを、[ティア 2] には y.y.y.y/z.z.z.z の組み合わせを、[ティア 3] には x.x.x.x/z.z.z.z の組み合わせをそれぞれ入力できます。こうすることより、これらの 3 つのホストすべてが物理的に同じネットワークセグメントに接続されている場合でも、各ホスト間の対話を 1 つの複数セグメント画面として表示できます。

注記 : 複数ティアフィルタリングは、トレースファイルでのみ使用できます。リアルタイムモニタと併用することはできません。

[NAT] タブの使用

ClearSight Application Flow Analyzer　ClearSignt Distributed

[**NAT**] タブを使用して、ClearSight での結合フローの表示方法に関してさらに微調整を行うことができます。[**NAT**] タブには、[**有効**] ボタンと [**無効**] ボタンというシンプルな対のラジオボタンがあります。

この [**有効**] ボタンと [**無効**] ボタンは、ネットワークアドレス変換 (NAT) の対象になった結合フローを表示するかどうかを制御するためのトグルボタンです。

[**有効**] を選択した場合、ネットワークアドレス変換により IP アドレスが変更になった場合でも、結合フローが表示されます。[**無効**] を選択した場合、そのようなフローは独立したフローとして扱われ、[**結合フロー**] 画面には表示されません。

手動によるフローの結合

ClearSight Application Flow Analyzer　ClearSignt Distributed

複数セグメントフィルタリングと複数ティアフィルタリングで使用される自動結合フロー機能は、トレースファイル全体に対して作用します。フィルタを駆使して、目的の結合フローだけが表示されるように画面をカスタマイズできます。しかし、このフィルタリングの方法では、確認したい状況だけを厳密に抽出することができないことがあります。そのため、ClearSight には、カスタムの結合フローに含めるフローを手動で選択する手段も用意されています。

新しい結合フローを手動で設定するには、以下の操作を実行します。

1. **[結合フロー]** タブの上部にある **[新規結合フロー]** アイコンをクリックします。**[問い合わせ]** ダイアログボックスが表示されます。
2. 新しい結合フローに付ける名前を入力します。図 8-13 にその例を示します。

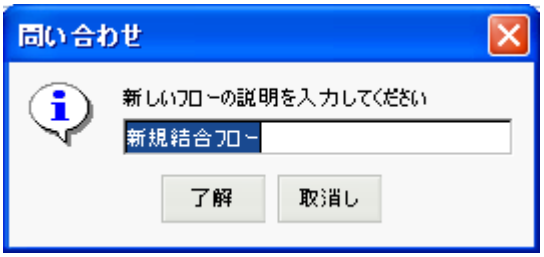


図 8-13: 新規結合フローの名前の入力

3. **[了解]** をクリックします。新しい結合フローの名前が、**[結合フロー]** タブの**フロー**ペインのフローのリストに表示されます。
4. その新しい結合フローを選択します。
5. **[詳細]** タブに移動して、新しい結合フローに含めるフローを右クリックします。
6. ドロップダウンリストから、**[選択している結合フローに追加]** を選択します。選択したフローが、新しい結合フローの一部となります。
7. この処理を続けて、必要なフローをすべて追加します。
8. **[結合フロー]** タブに戻り、この新しい結合フローを選択します。有効なフローの組み合わせを選択すると、該当する複数セグメントラダー画面が統計ペインに表示されます。

手動で構成した結合フローの名前を変更するには、目的のフローを選択して、**[結合フロー]** タブの上部にある **[結合フローの編集]** アイコンをクリックします。**[問い合わせ]** ボックスが再び表示されます。このボックスで名前を変更できます。

手動で構成した結合フローを削除するには、目的のフローを選択して、**[フローの削除]** アイコンをクリックします。

複数セグメントのリアルタイムモニタ

ClearSight Application Flow Analyzer　ClearSignt Distributed

複数のネットワークセグメントを同時にモニタできるアダプタを使用すると、複数セグメント解析をリアルタイムで実行することができます。現在利用できるアダプタは、以下のとおりです。

- 任意の 2 つのイーサネットセグメント上で使用できる 10/100 全二重イーサネットカード。全二重環境に制限する必要はありません。
- 2 つのギガビットイーサネットポートを備えたギガビットイーサネットカード。

複数セグメントモニタでこれらのアダプタのいずれかを使用するには、**[設定]** > **[アダプタ設定]** ページに移動して、**[複数セグメント]** オプションを選択します。次に、**[最初のセグメント名]** ボックスと **[二番目のセグメント名]** ボックスにセグメントの名前を入力します。

注記 : リアルタイムモニタ時に、複数セグメントフィルタや複数ティアフィルタを使用することはできません。

第 9 章

フィルタの使用

この章では、フィルタの操作方法について説明します。この章は次の項目で構成されています。

- 「フィルタについて」
- 「自動フィルタの使用」
- 「定義済みフィルタの使用」

フィルタについて

ClearSight Application Flow Analyzer　ClearSight Analyzer Light　ClearSignt Distributed

フィルタを使用して、極度に大きくなる可能性のあるデータをふるいにかけ、必要なフレームだけを表示できます。ClearSight は、さまざまなアプリケーション、フロータイプ、およびアドレスに対する総合的なフィルタ機能を提供します。

自動フィルタと定義済みフィルタ

ClearSight には、自動フィルタと定義済みフィルタの 2 種類のフィルタがあります。

- 自動フィルタを使用するには、ポストキャプチャアナリシスの間、リアルタイムモニタ表示または **[ClearSight]** タブのいずれか

でカウンタを右クリックします。それに応じて、選択したカウンタで利用可能な自動フィルタを一覧表示するコンテキストメニューが表示されます。

自動フィルタについては、282 ページの「自動フィルタの使用」で説明します。

- 定義済みフィルタを使用するには、**[新規フィルタ]** ダイアログボックスでオプションを設定します。定義済みフィルタは、リストに保存され、必要なときはいつでも再利用できます。

  定義済みフィルタの作成方法の詳細については、284 ページの「定義済みフィルタの使用」を参照してください。

リアルタイムまたはポストアナリシスでのフィルタの使用

自動フィルタを使用して、キャプチャバッファに格納するフレームをフィルタしたり、ポストアナリシス時に **[翻訳]** タブでのフレームの表示をフィルタすることができます。

定義済みフィルタを使用して、モニタに格納するパケットのフィルタ、キャプチャバッファに格納するパケットのフィルタ、ポストアナリシス時に **[翻訳]** タブに表示するパケットのフィルタを行うことができます。

- フィルタをモニタフィルタとして使用すると、モニタに格納されるフレームが決定されます。使用しているフィルタに一致するフレーム以外のフレームをすべて除外できます。これによって、モニタの表示が必要のないデータで一杯になることがなくなります。フィルタが現在モニタに適用されている場合、ウィンドウ下部のステータスバーに **[フィルタオン]** アイコン () が表示されます。
- フィルタをキャプチャフィルタとして使用すると、キャプチャ時にキャプチャバッファに格納されるフレームが決定されます。使用しているフィルタに一致するフレーム以外のフレームをすべて除外します。これによって、キャプチャバッファが必要のないフレームで一杯になることがなくなります。
- フィルタを翻訳表示フィルタとして使用すると、ポストキャプチャアナリシス時に **[翻訳]** タブに表示されるフレームが決定されます。翻訳表示フィルタは、一致するフレームを **[翻訳]** タブから一時的に消すことで、解析の邪魔にならないようにします。表示フィルタは一時的なフィルタです。バッファまたはトレースファイルのすべてのフレームを削除して再表示できます。

ClearSight は、**[新規フィルタ]** ダイアログボックス（図 9-4）のオプションを使って定義したフィルタのリストを管理します。定義済みフィルタはそれぞれに一意の名前を持っていて、使用する必要があるときはいつでもリストから選択できます。定義済みフィルタリスト自体は、フィルタが適用される場所に応じてさまざまな場所から使用することができます。

モニタをフィルタする場合	**[設定]** > **[設定]** > **[共通]** > **[モニタ設定]** の **[設定]** タブの **[フィルタ]** 領域から。
キャプチャをフィルタする場合	キャプチャワークスペースの **[設定]** タブの **[フィルタ]** 領域から。
翻訳表示をフィルタする場合	ポストキャプチャアナリシスワークスペースの **[翻訳]** タブのステータスバーにある **[フィルタの適用]** アイコン から。

注記 : モニタやキャプチャには適用できず、ポストアナリシス時に翻訳表示にのみ適用できるフィルタがあります。これらのフィルタは、[フィルタリスト] の **[制限]** 列に **((ポストアナリシスのみ))** と表示されます。

パケットベースのフィルタとフローベースのフィルタ

ClearSight は、パケットベースのフィルタとフローベースのフィルタを使用します。

- パケットベースのフィルタは、パケット単位で適用されます。ClearSight は、到着するパケットごとに、そのパケットが現在選択されているフィルタの基準を満たすかどうかを確認します。それらの基準に一致したフレームは、モニタまたはキャプチャバッファに渡されるか、翻訳画面に表示されます。
- フローベースのフィルタは、ポストキャプチャアナリシスの際のみに使用され、一般的にさまざまなエラータイプとステータスコードに利用できます。ClearSight が特定のエラータイプまたはステータスフラグを表示するパケットを検出すると、そのフローに属するすべてのパケットの表示にフィルタがかけられます。このようにして、論理的にエラーを追求でき、トラブルシュートが容易になります。

自動フィルタの使用

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

[新規フィルタ] ダイアログボックスで手動で設定したフィルタに加えて、ClearSight では、数多くの自動キャプチャと表示フィルタが提供されます。自動フィルタにより、手動設定の手間を省いて、必要なもののみを表示することが容易になります。

自動キャプチャフィルタ

通常、自動キャプチャフィルタを使用するには、リアルタイムモニタ表示内のカウンタを右クリックします。それに応じて、選択したカウンタで利用可能な、さまざまな自動キャプチャフィルタを表示するコンテキストメニューが表示されます。利用可能なフィルタは、選択するレイヤ、ペイン、およびカウンタによって異なります。通常、自動キャプチャフィルタは、選択したカウンタのアドレスとポートで明示的に使用できるだけでなく、選択したカウンタのアドレスとポートをさまざまに組み合わせて、さまざまな一般的なワイルドカードによるフィルタでも使用できます。図 9-1 は、ネットワーク層の **[コネクション]** タブで使用可能な自動キャプチャフィルタの例を示しています。



図 9-1: 自動キャプチャフィルタ

注記：自動キャプチャフィルタを選択すると、そのフィルタを適用したフレームのキャプチャが直ちに開始されます。

自動表示フィルタ

自動表示フィルタは、自動キャプチャフィルタとほとんど同じように使用できます。ただし、リアルタイムモニタ表示のカウンタを右クリックする代わりに、ポストキャプチャアナリシス表示の **[ClearSight]** タブを右クリックします。それに応じて、選択したカウンタで利用可能な、さまざまな自動フィルタを一覧表示するコンテキストメニューが表示されます。ここには、表示フィルタとキャプチャフィルタの両方が一覧表示されます。**フィルタ xxx** コマンドを使って、表示フィルタを選択し、**xxx をキャプチャする** コマンドを使って、キャプチャフィルタを選択します。**[翻訳]** タブの **[サマリ]** ペインで、必要なフレームのチェックボックスをオンにし、任意のフレームを右クリックし、**[チェックされたフレームでフィルタ]** を選択してそれらのフレームだけを表示することができます。利用可能なフィルタは、選択するレイヤ、ペイン、およびカウンタによって異なります。通常、自動表示フィルタは、選択したカウンタのアドレスとポートで明示的に使用できるだけでなく、選択したカウンタのアドレスとポートをさまざまに組み合わせて、さまざまな一般的なワイルドカードによるフィルタでも使用できます。ただし、カウンタはそれぞれ異なります。例えば、**[ClearSight]** タブの [アプリケーション] ペイン内のアプリケーションカウンタをクリックすると、そのアプリケーションタイプ用の自動表示フィルタにアクセスできます。自動表示フィルタを選択すると、ClearSight は、適用されるフィルタを **[翻訳]** タブに表示します。フィルタを解除するには、**[ClearSight]** タブから新しい自動フィルタを適用するか、**[翻訳]** タブのステータスバーにある **[フィルタのオン / オフ]** ボタン  をクリックします。

図 9-2 は、アプリケーション層のサンプルフローで使用可能な自動表示フィルタの例を示しています。この例では、1 つの親フローの下に子フローがあり、2 種類のフィルタを使用できます。



図 9-2: 自動表示フィルタ

定義済みフィルタの使用

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

[新規フィルタ] ダイアログボックスで定義済みフィルタを設定します。

定義済みフィルタの作成方法

1. **[設定]** > **[フィルタ]** タブで **[ここをクリックして]** ボタンをクリックします。現在のフィルタのリストが格納された **[フィルタリスト]** ダイアログボックスが表示されます。図 9-3 は、**[フィルタリスト]** ダイアログボックスを示しています。

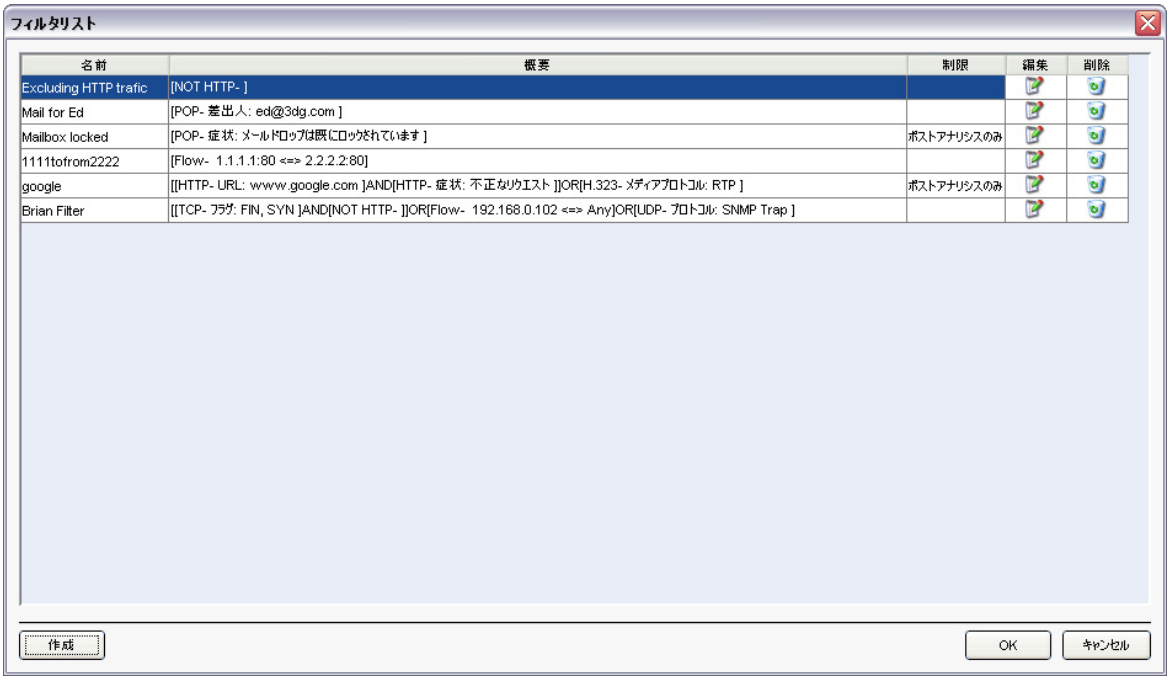


図 9-3: **[フィルタリスト]** ダイアログボックス

2. 新しいフィルタを定義するには、**[作成]** ボタンをクリックします。**[新規フィルタ]** ダイアログボックス (図 9-4) が表示されます。
3. **[フィルタ名]** フィールドにこのフィルタを説明する名前を入力します。

フィルタは、この名前で ClearSight の表示全体で認識されます。ClearSight のさまざまな場所で表示されるフィルタリストからこの名前を選択して、フィルタを利用できます。

- **[設定]** > **[設定]** > **[共通]** > **[モニタ設定]**
- **[キャプチャ]** ボタン > **[設定]** タブ > **[フィルタ]**
- **[キャプチャ]** ボタン > **[トリガ]** タブ > **[フィルタトリガ]**
- **[トレースファイル]** ボタン > **[翻訳]** タブ (ステータスバーの **[フィルタを適用]** アイコンを使用)

注記 : これらの場所から **[作成]** ボタンにアクセスすることもできます。

4. さまざまなフィルタダイアログボックスで、このフィルタのフィルタ基準を設定します。これらのダイアログボックスは、**[新規フィルタ]** ダイアログボックスの左側にある **[新規フィルタ項目]** メニューに一覧表示されています。これらのダイアログボックスにある利用可能なフィルタ基準については、次の各項で詳しく説明します。

   重要 : 特定のフィルタダイアログボックス内で作成された個々のフィルタコンポーネントは、図 9-4 では 1 つの長方形で表されています。名前を付けられたフィルタは、**AND**、**OR**、および **NOT** 論理演算子を使用して、これらの長方形をグループ化して構成されています。**AND** および **OR** の関係は、長方形の相対的位置によって決定されます。**NOT** 演算子は、影響を受ける長方形内の **[NOT]** アイコンをクリックして作成します。詳細については、図 9-4 を参照してください。

   注記 : NOT 演算子を使用すると、指定したフレームが除外されます。

5. **[OK]** をクリックして、フィルタをフィルタリストに保存します。

   フィルタリストが表示され、利用可能なすべてフィルタとその定義の概要が表示されます。

[新規フィルタ項目] リストの選択肢をクリックしてフィルタ設定ダイアログボックスにアクセスすることができます。各フィルタ設定ダイアログボックスで指定したフィルタ条件で定義済みフィルタを作成します。フィルタを作成するときに、フィルタの論理構造がグラフィック表示されます。各ダイアログボックスによって、この画面上の対応する長方形に表示される属性が生成されます。長方形は、AND、OR、および NOT 演算子を使用してグループ化されます。同じ行にある項目は AND で結合されます。各行は OR で結合されます。NOT 演算子を有効にするには、[NOT] ボタンをクリックします。

パケットは、指定した論理的な基準の組合せに一致すると、フィルタを通過し受け入れられます。

[編集] ボタンをクリックすると、元に戻って項目を編集できます。[削除] ボタンをクリックして、項目を完全に削除できます。

ここにフィルタ名を入力します。この名前を使用して、フィルタリストからこのフィルタを選択します。

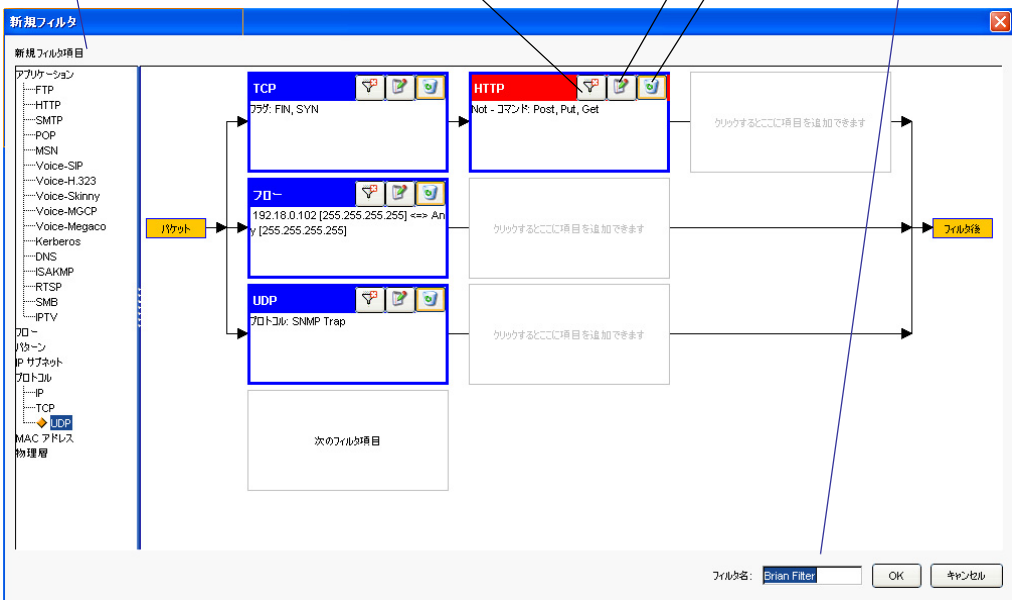


図 9-4: 定義済みフィルタの構成

アプリケーション層フィルタの設定

※アプリケーション層フィルタは、ClearSight Analyzer Light には搭載されていない機能になります。

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[アプリケーション]** エントリをクリックすると、**[アプリケーションフィルタ]** ダイアログボックスが表示されます (図 9-5)。このダイアログボックスで、必要なアプリケーションを選択できます。選択したアプリケーションからのフレームがこのフィルタの一部として組み込まれます。



図 9-5: **[アプリケーションフィルタ] ダイアログボックス**

これらの一般的なアプリケーション層フィルタのほかに、ページの左側にある **[新規フィルタ項目]** メニューのエントリをクリックして、各アプリケーション用の個別のフィルタ条件を選択できます。表示されるダイアログボックスで、フィルタ条件として使用できるさまざまなフレームタイプ、コマンド、ステータスメッセージを選択できます。アプリケーションごとに利用可能なフィルタ条件については、以下の各項で説明します。

DNS フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[DNS]** エントリをクリックすると、**[DNS フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの DNS トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-6 で示すように、DNS トラフィックに対して次の条件でフィルタをかけることができます。

[全般] DNS コマンド内のさまざまなフィールドの値を指定し、このフィルタの一部として組み込みます (**[DNS 名]**、**[クエリー ID]**)。指定されたフィールドの指定された値を含むパケットが、このフィルタの一部として組み込まれます。

[コマンド] さまざまな DNS コマンドタイプを選択し、このフィルタの一部として組み込みます。

[ステータス] さまざまな DNS ステータスフラグを選択し、このフィルタの一部として組み込みます。

[症状] さまざまな DNS エラーメッセージタイプを選択し、このフィルタの一部として組み込みます。

重要 : [ステータス] と **[症状]** のフィルタ条件は、フローベースです。これらは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用されます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。



図 9-6: DNS のフィルタ条件

FTP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[FTP]** エントリをクリックすると、**[FTP フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの FTP トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-7 で示すように、FTP トラフィックに対して次の条件でフィルタをかけることができます。

[全般]	フィルタ条件としてファイル名またはユーザ名を指定します。指定されたファイル名またはユーザ名を含むトラフィックが、このフィルタの一部として組み込まれます。
[タイプ]	このフィルタの一部として FTP の [制御] または [データ] フレームを選択します。
[コマンド]	さまざまな FTP コマンドタイプを選択して、このフィルタの一部として組み込みます。
[症状]	さまざまな FTP エラーメッセージタイプを選択して、このフィルタの一部として組み込みます。

重要 : [症状] のフィルタ条件は、フローベースです。これは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用されます。[症状] 条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

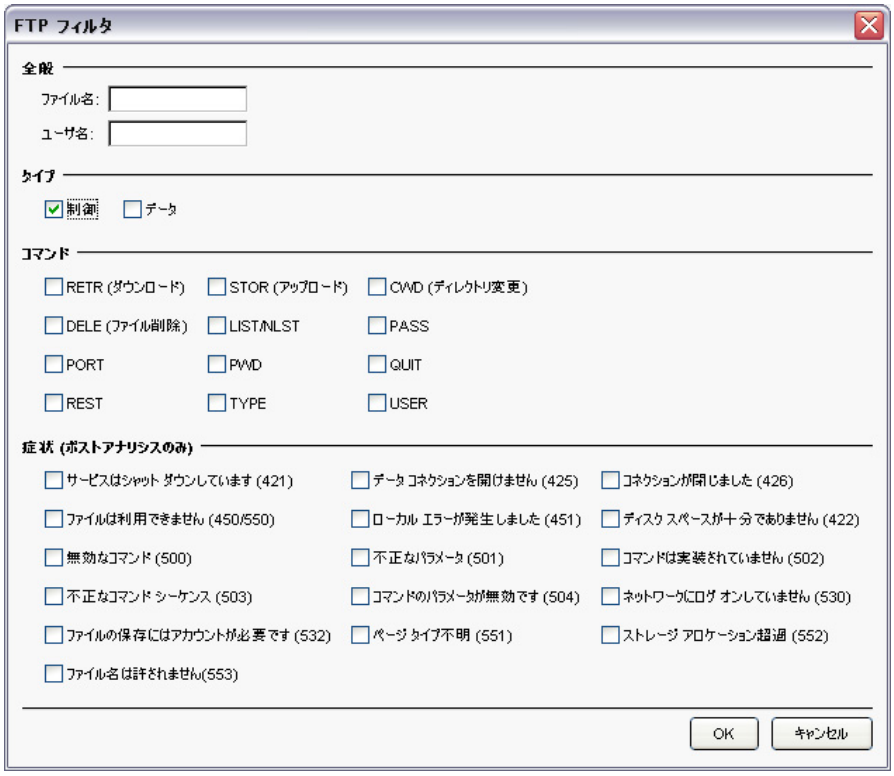


図 9-7: FTP のフィルタ条件

HTTP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[HTTP]** エントリをクリックすると、**[HTTP フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの HTTP トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-8 で示すように、HTTP トラフィックに対して次の条件でフィルタをかけることができます。

[リソース] フィルタ条件として特定の URL を指定します。指定された URL を含むトラフィックが、このフィルタの一部として組み込まれます。最大 5 つの異なる URL を指定できます。

ヒント : このフィルタは、HTTP サーバー上の特定のリソースに関連する問題をトラブルシュートするときに役立ちます。

[コマンド] さまざまな HTTP コマンドタイプを選択して、このフィルタの一部として組み込みます。

[HTTP アプリケーション] ドロップダウンリストを使用してさまざまな HTTP サーバーとブラウザタイプを選択して、このフィルタの一部として組み込みます。指定されたサーバーまたはブラウザタイプを参照する HTTP フィールドを含むフレームが、このフィルタの一部として組み込まれます。

[症状] さまざまな HTTP エラーメッセージタイプを選択して、このフィルタの一部として組み込みます。

重要 : [症状] のフィルタ条件は、フローベースです。これは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用されます。[症状] 条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

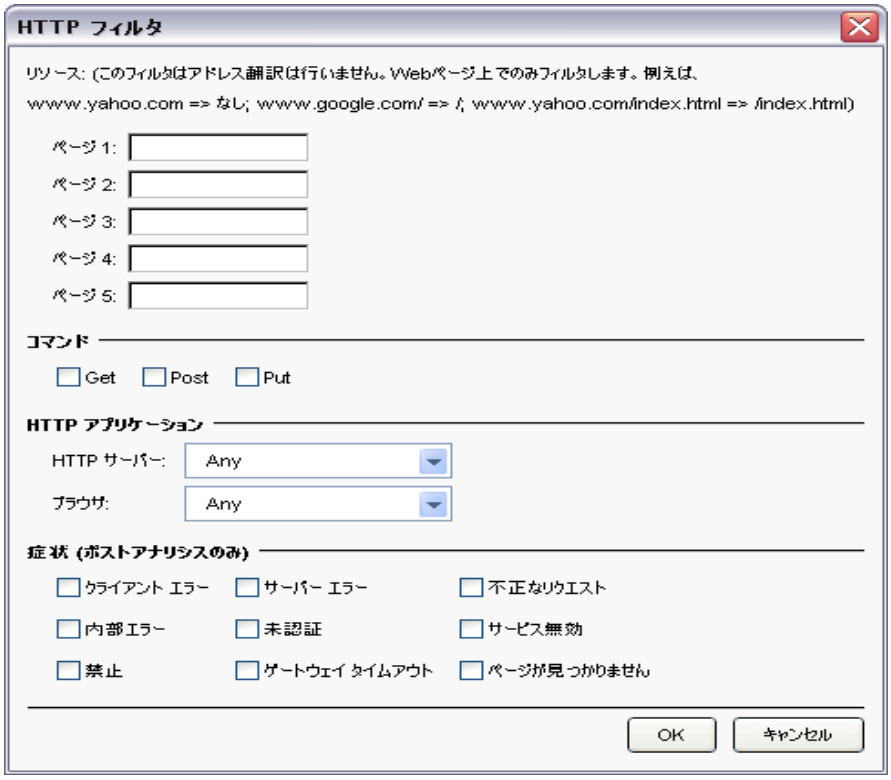


図 9-8: HTTP のフィルタ条件

POP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[POP]** エントリをクリックすると、**[POP フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの POP トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-9 で示すように、POP トラフィックに対して次の条件でフィルタをかけることができます。

[全般] — POP 電子メールメッセージ内のさまざまなフィールドの値を指定して、このフィルタの一部として組み込みます (**[送信元アドレス]**、**[送信先アドレス]**、**[件名]**、および **[メッセージ]**)。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。

[コマンド] — さまざまな POP コマンドタイプを選択して、このフィルタの一部として組み込みます。

[症状] — さまざまな POP エラーメッセージタイプを選択して、このフィルタの一部として組み込みます。

重要 : [症状] のフィルタ条件は、フローベースです。これは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用されます。**[症状]** の条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

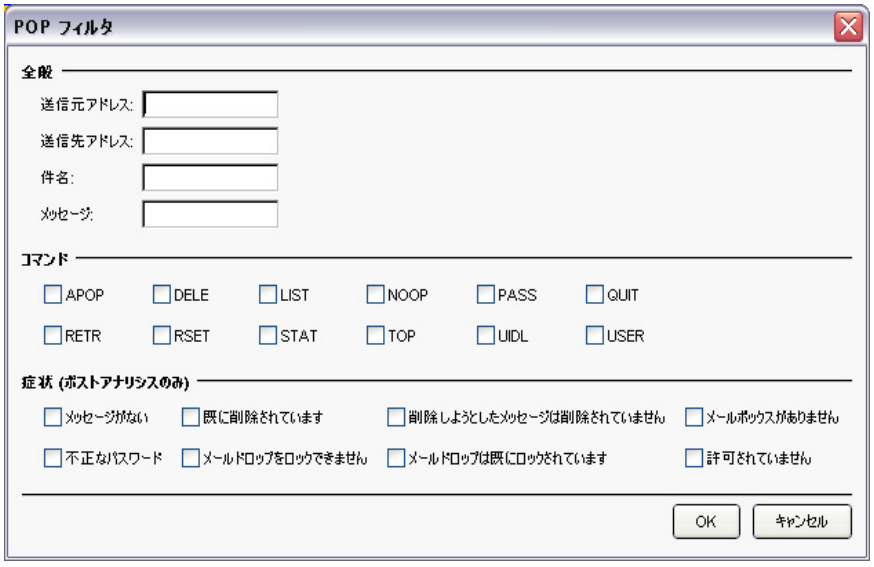


図 9-9: POP のフィルタ条件

SMTP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[SMTP]** エントリをクリックすると、**[SMTP フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの SMTP トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-10 で示すように、SMTP トラフィックに対して次の条件でフィルタをかけることができます。

[全般]	SMTP 電子メールメッセージ内のさまざまなフィールドの値を指定して、このフィルタの一部として組み込みます (**[送信元アドレス]**、**[送信先アドレス]**、**[件名]**、および **[メッセージ]**)。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。
[コマンド]	さまざまな SMTP コマンドタイプを選択して、このフィルタの一部として組み込みます。
[ステータス]	さまざまな SMTP ステータスフラグを選択して、このフィルタの一部として組み込みます。
[症状]	さまざまな SMTP エラーメッセージタイプを選択して、このフィルタの一部として組み込みます。

重要 : [ステータス] と **[症状]** のフィルタ条件は、フローベースです。これらは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用されます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

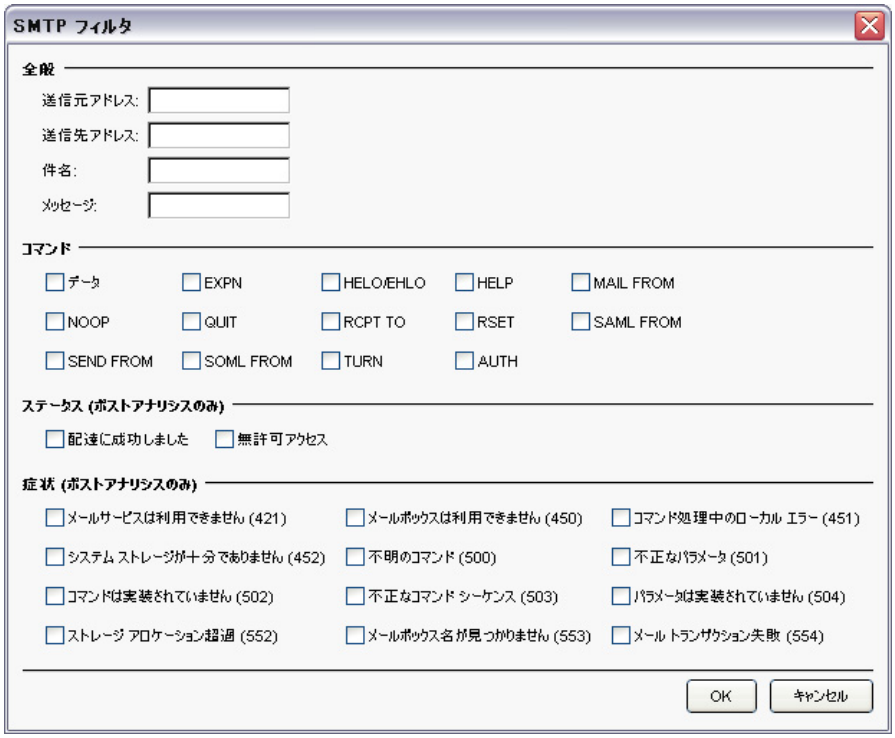


図 9-10: SMTP のフィルタ条件

MSN フィルタの設定

[新規フィルタ] ダイアログボックスの [新規フィルタ項目] メニューで [MSN] エントリをクリックして、[MSN フィルタ] ダイアログボックスを開きます。ここでは、さまざまな種類の MSN トラフィックを対象に指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-11 に示すように、MSN トラフィックに対して次の条件でフィルタをかけることができます。

[全般] 電子メールアドレスまたはスクリーン名の値を指定します。これらのいずれかに一致するトラフィックがこのフィルタの一部として組み込まれます。

[コマンド] どのタイプのサーバーを組み込むかを指定します。オンにしたサーバーで送受信されるトラフィックが組み込まれます。

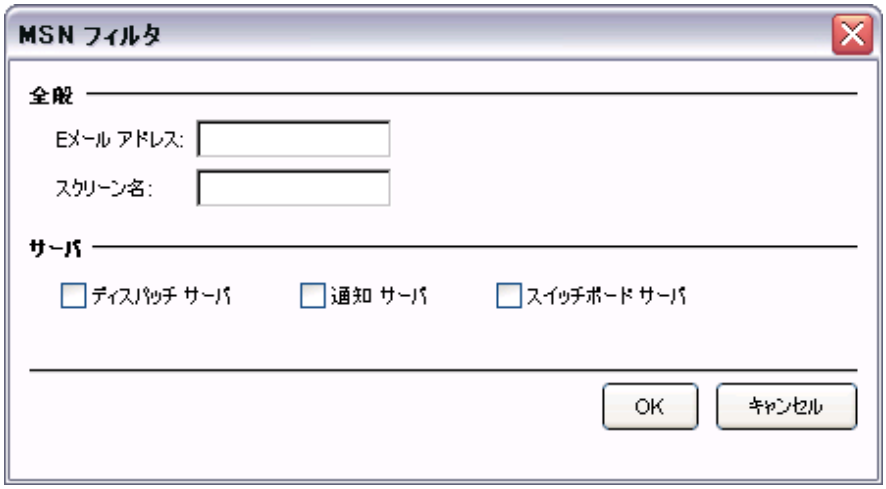


図 9-11: MSN のフィルタ条件

[Voice-H.323] フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[Voice-H.323]** エントリをクリックすると、**[Voice-H.323 フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの H.323 トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-12 で示すように、H.323 トラフィックに対して次の条件でフィルタをかけることができます。

[全般]	[電話番号]、[ユーザ名]、[コール ID] などを含む H.323 コールのさまざまな一般識別子の値を指定します。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。
[メディアプロトコル]	H.323 コール (RTP、RTCP、または両方) でのエンドツーエンドのオーディオ配信に使用するさまざまなセッション層のプロトコルを選択して、このフィルタの一部として組み込みます。RTP の場合は、特定のコーデックを選択することもできます。
[コール制御]	さまざまなコール制御メッセージを選択して、このフィルタの一部として組み込みます。
[コマンド]	さまざまな H.323 コマンドタイプを選択して、このフィルタの一部として組み込みます。
[トラフィック タイプ]	H.323 ファミリー内のさまざまなプロトコルを選択して、このフィルタの一部として組み込みます。
[症状]	さまざまな H.323 エラーメッセージタイプを選択して、このフィルタの一部として組み込みます。

重要：[症状]、[H.245] および **[メディアプロトコル]** フィルタ条件は、フローベースです。これらは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用できます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

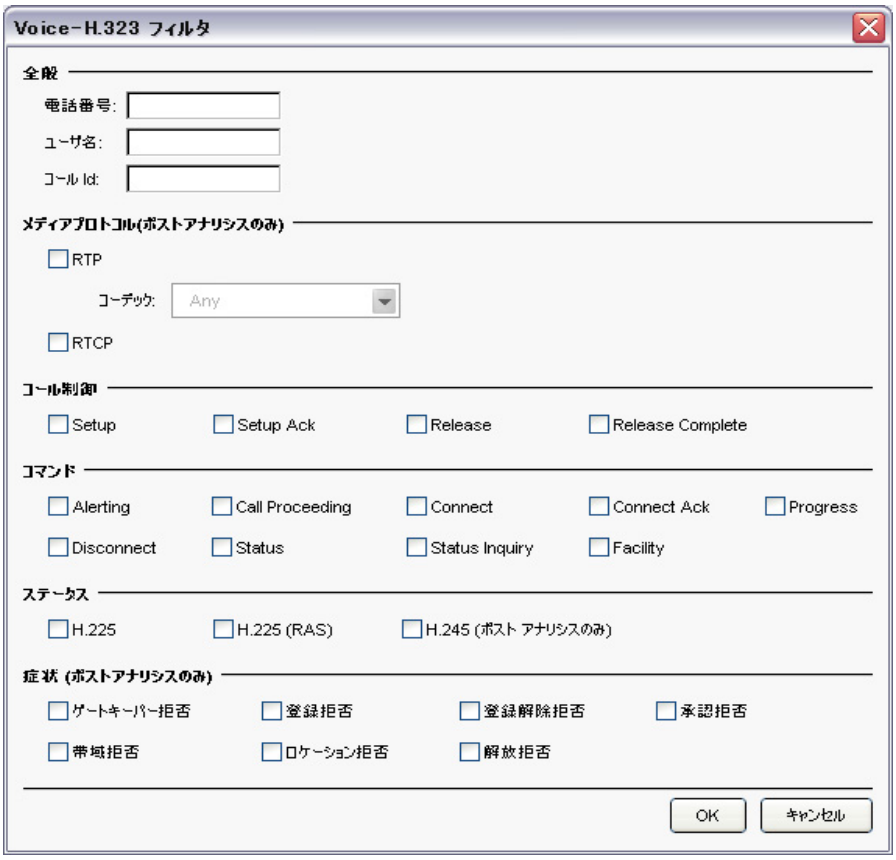


図 9-12: H.323 のフィルタ条件

[Voice-SIP] フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[Voice-SIP]** エントリをクリックすると、**[Voice-SIP フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの SIP トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-13 で示すように、SIP トラフィックに対して次の条件でフィルタをかけることができます。

[全般]	[電話番号]、[ユーザ名]、[コール ID] などを含む SIP コールのさまざまな一般識別子の値を指定します。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。
[メディア プロトコル]	SIP コール (RTP、RTCP、T.38) でのエンドツーエンドのオーディオ配信に使用するさまざまなセッション層のプロトコルを選択して、このフィルタの一部として組み込みます。RTP の場合は、特定のコーデックを選択することもできます。
[電話番号と RTP]	電話番号とそれに関連する RTP フローを選択して、このフィルタの一部として組み込みます。
[コール制御]	さまざまなコール制御メッセージを選択して、このフィルタの一部として組み込みます。
[コマンド]	さまざまな SIP コマンドタイプを選択して、このフィルタの一部として組み込みます。
[ステータス]	さまざまな SIP ステータスフラグを選択して、このフィルタの一部として組み込みます。
[症状]	さまざまな SIP エラーメッセージタイプを選択して、このフィルタの一部として組み込みます。

重要：[ステータス]、[症状] および **[メディアプロトコル]** フィルタ条件は、フローベースです。これらは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用できます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

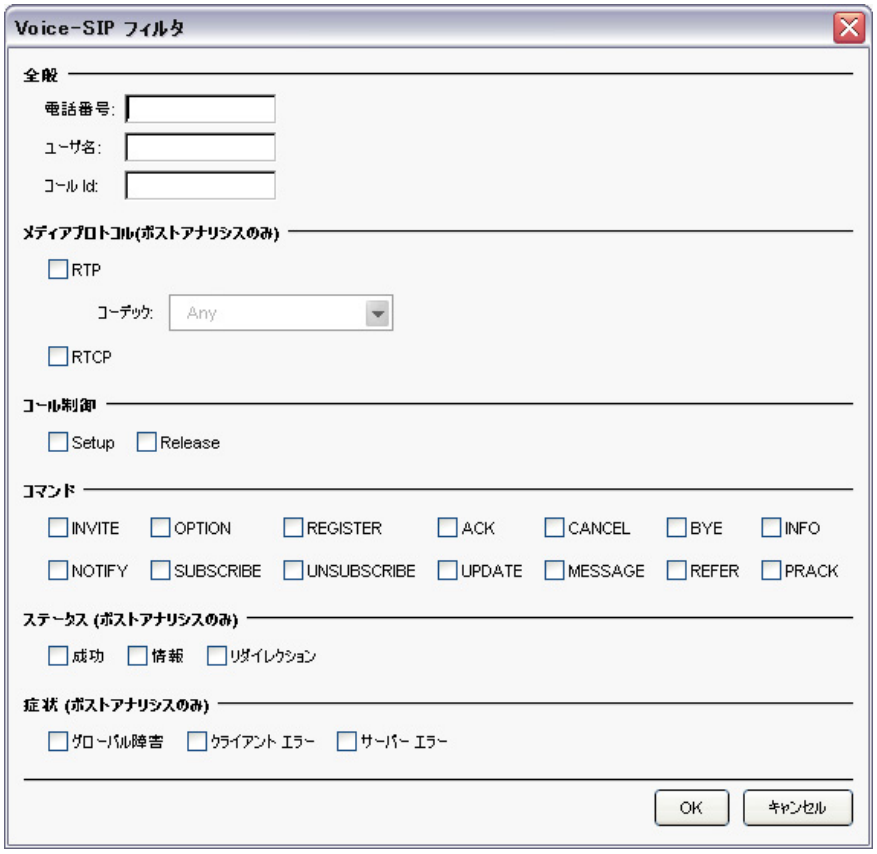


図 9-13: SIP のフィルタ条件

[Voice-Skinny] フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[Voice-Skinny]** エントリをクリックすると、**[Voice-Skinny フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの Skinny トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-14 で示すように、Skinny トラフィックに対して次の条件でフィルタをかけることができます。

[全般] — [電話番号]、[ユーザ名]、[コール ID] などを含む Skinny コールのさまざまな一般識別子の値を指定します。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。

[メディア プロトコル] — Skinny コール (RTP、RTCP、または両方) でのエンドツーエンドのオーディオ配信に使用するさまざまなセッション層のプロトコルを選択して、このフィルタの一部として組み込みます。RTP の場合は、特定のコーデックを選択することもできます。



図 9-14: Skinny のフィルタ条件

重要 : [メディアプロトコル] フィルタ条件は、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用できます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。

[Voice-MGCP] フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[Voice-MGCP]** エントリをクリックすると、**[Voice--MGCP フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの MGCP トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-13 で示すように、MGCP トラフィックに対して次の条件でフィルタをかけることができます。

[全般]	[電話番号]、[コネクション ID] を含め、MGCP コールのさまざまな一般識別子の値を指定します。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。
[メディア プロトコル]	MGCP コール (RTP、RTCP、または両方) でのエンドツーエンドのオーディオ配信に使用するさまざまなセッション層のプロトコルを選択して、このフィルタの一部として組み込みます。RTP の場合は、特定のコーデックを選択することもできます。
[コール制御]	さまざまなコール制御メッセージを選択して、このフィルタの一部として組み込みます。
[症状]	さまざまな MGCP エラーメッセージタイプを選択し、このフィルタの一部として組み込みます。

重要 : [症状] および **[メディアプロトコル]** フィルタ条件は、フローベースです。これらは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用できます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。



図 9-15: MGCP のフィルタ条件

[Voice-Megaco] フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[Voice-Megaco]** エントリをクリックすると、**[Voice-Megaco フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの Megaco トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-13 で示すように、Megaco トラフィックに対して次の条件でフィルタをかけることができます。

[全般]	[メディアゲートウェイ ID]、[終了 ID] を含め、Megaco コールのさまざまな一般識別子の値を指定します。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。
[メディア プロトコル]	Megaco コール (RTP、RTCP、または両方) でのエンドツーエンドのオーディオ配信に使用するさまざまなセッション層のプロトコルを選択して、このフィルタの一部として組み込みます。RTP の場合は、特定のコーデックを選択することもできます。
[コマンド]	さまざまな Megaco コマンドタイプを選択して、このフィルタの一部として組み込みます。

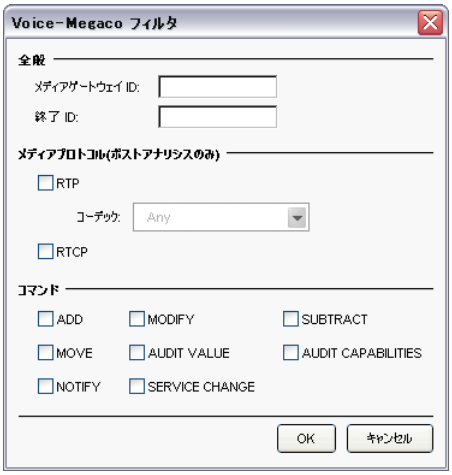


図 9-16: Megaco のフィルタ条件

重要 : [メディアプロトコル] フィルタ条件は、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用できます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。

ISAKMP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[ISAKMP]** エントリをクリックすると、**[ISAKMP フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの ISAKMP トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-13 で示すように、ISAKMP トラフィックに対して次の条件でフィルタをかけることができます。

[交換タイプ] さまざまな ISAKMP 交換タイプを選択して、このフィルタの一部として組み込みます。

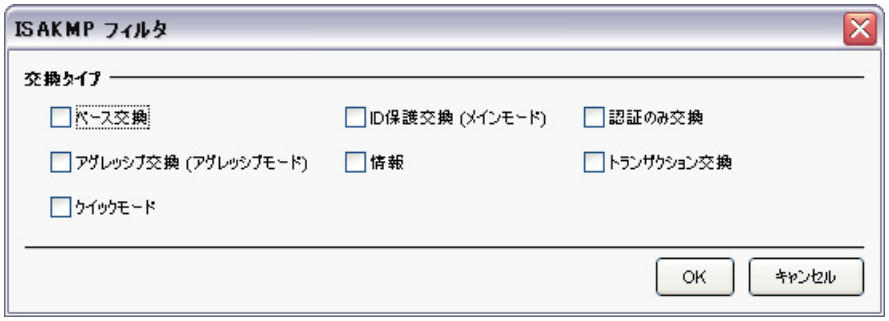


図 9-17: ISAKMP のフィルタ条件

Kerberos フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[Kerberos]** エントリをクリックすると、**[Kerberos フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの Kerberos トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-13 で示すように、Kerberos トラフィックに対して次の条件でフィルタをかけることができます。

[全般]	[プリンシパル名]、[サーバー Realm]、[クライアント Realm] を含め、Kerberos トランザクションのさまざまな一般識別子の値を指定します。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。
[サブプロトコル]	さまざまなサブプロトコルを選択します (AS Exchange、TGS Exchange、および CS Exchange、またはこれらのいずれか)。
[症状]	さまざまな Kerberos エラーメッセージタイプを選択し、このフィルタの一部として組み込みます。

重要 : [症状] のフィルタ条件は、フローベースです。これは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用されます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

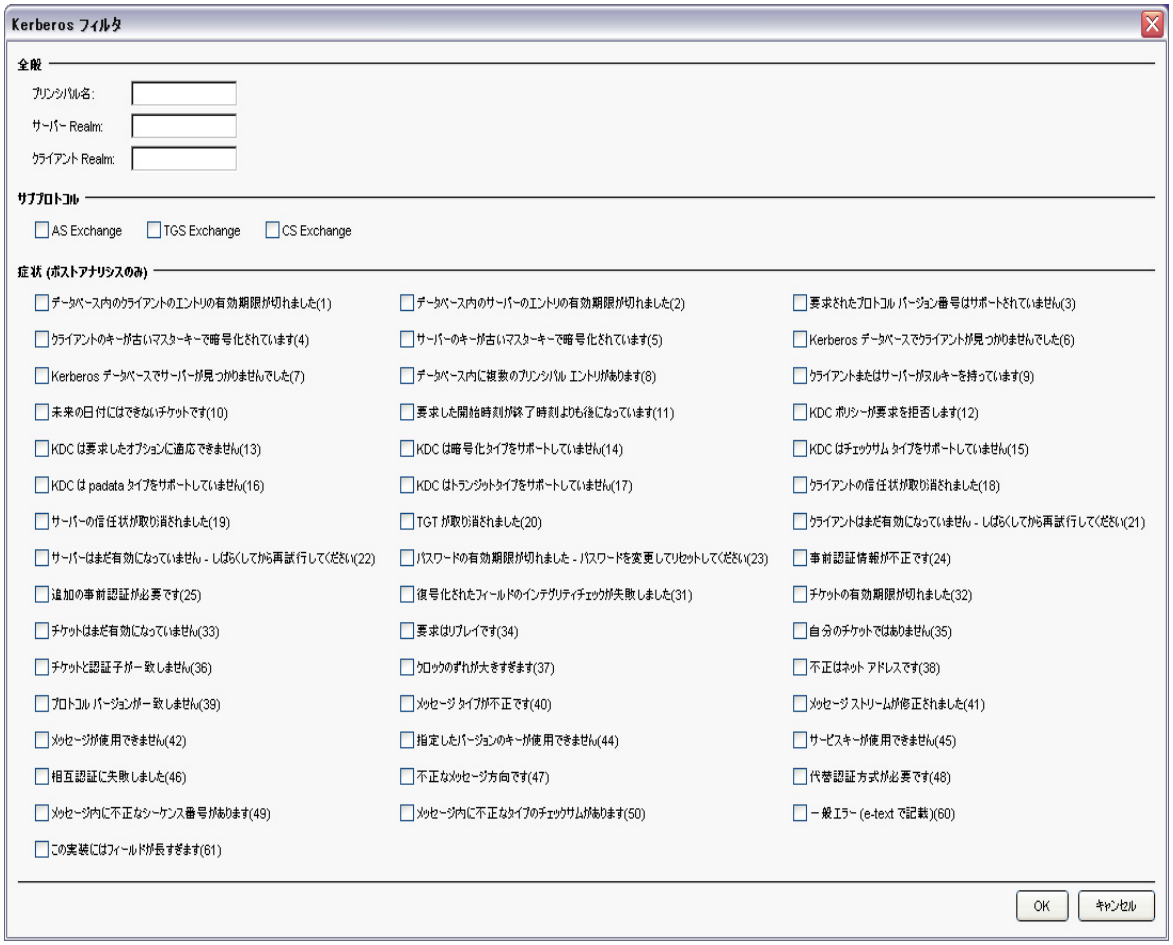


図 9-18: Kerberos のフィルタ条件

RTSP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[RTSP]** エントリをクリックすると、**[RTSP フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの RTSP トラフィックを指定できます。選択した条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-13 で示すように、RTSP トラフィックに対して次の条件でフィルタをかけることができます。

[全般]	[サーバー URL] や [プレゼンテーション] などを含む、RTSP ストリームのさまざまな一般識別子の値を指定します。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。
[メソッド]	必要なメソッドを選択します。指定されたメソッドを含むトラフィックが、このフィルタの一部として組み込まれます。
[症状]	さまざまな RTSP エラーメッセージタイプを選択し、このフィルタの一部として組み込みます。

重要 : [症状] のフィルタ条件は、フローベースです。これは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用できます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

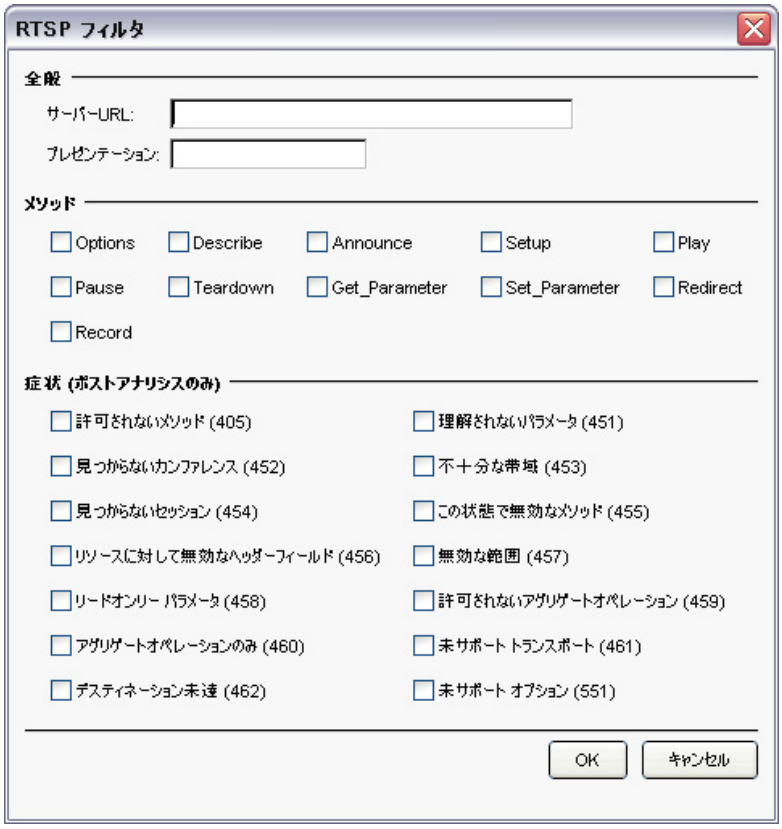


図 9-19: RTSP のフィルタ条件

IPTV フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[IPTV]** エントリをクリックすると、**[IPTV フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要な IPTV トラフィックのさまざまなタイプを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-20 に示すように、IPTV トラフィックに対して次の条件でフィルタをかけることができます。

[全般] — **PID** フレーム、**PAT** フレーム、またはその両方を選択します。**PID** フレームの場合は、範囲を指定できます。指定されたフィールドを含むトラフィックが、このフィルタの一部として組み込まれます。

[症状] — さまざまな IPTV エラーメッセージタイプを選択して、このフィルタの一部として組み込みます。

重要：[全般] および **[症状]** のフィルタ条件は、フローベースです。これは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用できます。これらのグループからの条件を含むどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタ違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

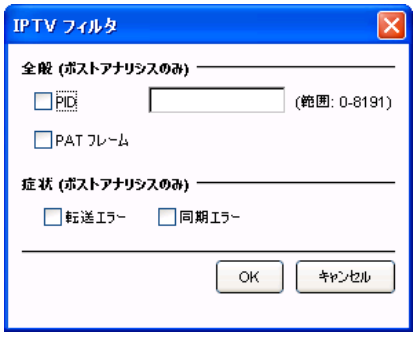


図 9-20: IPTV のフィルタ条件

SMB フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[SMB]** エントリをクリックすると、**[SMB フィルタ]** ダイアログボックスが表示されます。このダイアログボックスで、必要なさまざまなタイプの SMB トラフィックを指定できます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-13 で示すように、SMB トラフィックに対して次の条件でフィルタをかけることができます。

[メッセージタイプ] 必要なメッセージタイプを選択します。指定されたメッセージタイプを含むトラフィックが、このフィルタの一部として組み込まれます。

[エラー] 必要なエラータイプを選択します。指定されたエラータイプを含むトラフィックが、このフィルタの一部として組み込まれます。

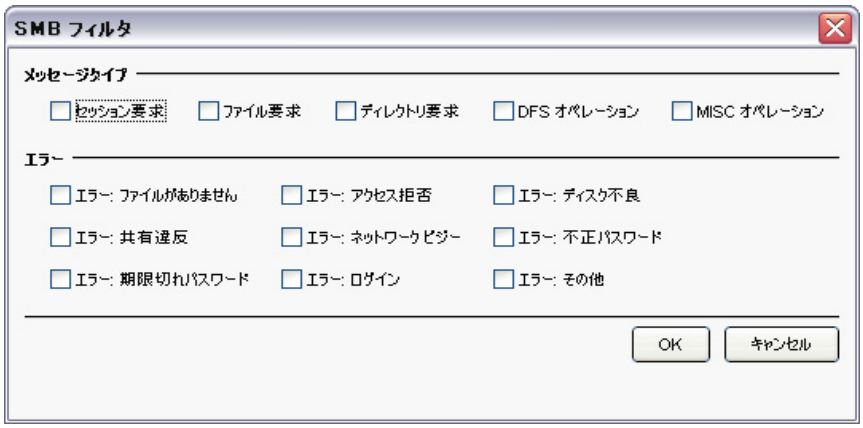


図 9-21: SMB のフィルタ条件

フローフィルタの設定

フローフィルタを使用して、通信するペアの IP ホスト間でのある種のトラフィックを含めます。含めるトラフィックの方向とポート番号を指定できます。

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[フロー]** エントリをクリックして、以下のフローフィルタのオプションを設定します。

[IP アドレス タイプ]	IPv4 アドレスまたは IPv6 アドレスを指定します。
[送信元アドレス]	このホストのペアの最初のアドレス。すべて 0 の値は入力しないでください。
[ポート]	送信元アドレスのトラフィックにフィルタをかけるポート。
[方向]	このステーションのペアで追加されるトラフィックの方向。ドロップダウンリストを使用して、方向を選択します。
[送信先アドレス]	このホストのペアの 2 番目のアドレス。すべて 0 の値は入力しないでください。
[ポート]	送信先アドレスのトラフィックにフィルタをかけるポート。

注記 : ポート番号を空白のままにすると、すべてのポート上のトラフィックが追加されます。アドレスを空白のままにすると、すべてのアドレスのトラフィックが追加されます。



図 9-22: フローフィルタ条件

パターンフィルタの設定

パターンフィルタを使用して、特定のパターンが含まれるフレームを追加します。

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[パターン]** エントリをクリックして、以下のパターンフィルタのオプションを設定します (図 9-23 を参照)。

[パターンマッチ開始場所] ドロップダウンリストを使用して、パターンの検索開始位置を、フレームの開始部分、IP 層の開始部分、またはアプリケーション層の中から選択します。あるいは、ドロップダウンリストで選択した開始ポイントからバイト単位でオフセットしたパターンにマッチさせることもできます。

[オフセット] **[テキスト]** または **[Hex]** を選択して、オフセットの量を入力します。

[パターン] **[テキスト]** または **[Hex]** を選択して、マッチさせるパターンを入力します。

注記 : Hex データは、スペースで区切られた文字のペアとして入力する必要があります (02 AA 03 BC など)。

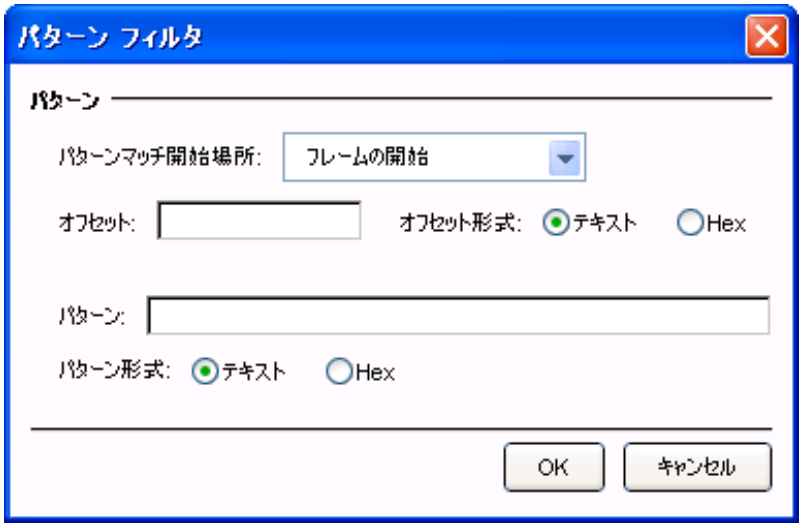


図 9-23: パターンフィルタ条件

IP サブネットフィルタの設定

IP サブネットフィルタリングを使用して、特定の IP サブネットに属するすべてのトラフィックを組み込みます。サブネットのアドレスとマスクを指定して、フィルタの一部として組み込みます (図 9-24 を参照)。ドロップダウンリストを使用して、方向を選択します。

注記 : 両方の IP アドレスに「0.0.0.0」と入力した場合、その入力は無視されます。



図 9-24: IP サブネットフィルタ条件

プロトコルフィルタの設定

プロトコルフィルタを使用して、特定のプロトコルタイプ、プロトコルフラグ、または特質などのパケットを追加します。**[新規フィルタ項目]** メニューにあるメインの **[プロトコル]** カウンタを使用して、**[IP]**、**[ARP]**、および **[IPv6]** に対する一つ上のプロトコルフィルタを設定できます。また、**[IP]**、**[TCP]**、および **[UDP]** のダイアログボックスを使用して、より限定したプロトコルフィルタも設定できます。これらのプロトコルごとのオプションについては、以下に説明します。

親プロトコルフィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[プロトコル]** エントリをクリックすると、**[プロトコルフィルタ]** ダイアログボックスが表示されます (図 9-25)。このダイアログボックスで、必要な親プロトコル **(IP**、**ARP**、**IPv6)** を選択できます。選択したいずれかのプロトコルからのフレームが、このフィルタの一部として組み込まれます。

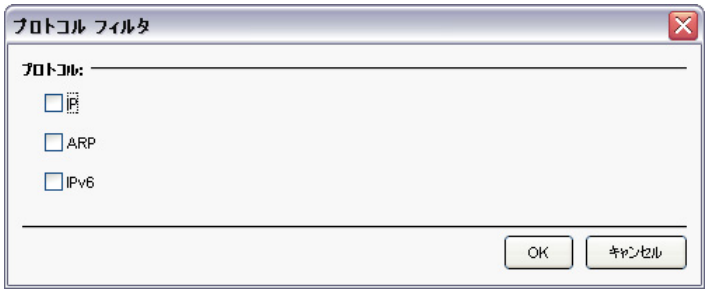


図 9-25: [プロトコル] のフィルタ条件

IP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[IP]** カウンタをクリックして、さまざまな IP トラフィックのタイプを指定し、このフィルタの一部として組み込みます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-26 示すように、IP トラフィックに対して次の条件でフィルタをかけることができます。

[サービス タイプ] IP パケットのヘッダでは、[サービス タイプ] フィールドを使用するさまざまなサービス品質のレベルを示すことができます。[サービスタイプ] フィールドには、[優先度] と [トランスポートタイプ] の項目があります。**[サービス タイプ]** 領域にあるオプションを使って、これらの両フィールドでフィルタをかけられます。指定した QoS 指標を含むパケットは、このフィルタの一部として組み込まれます。

[制御] さまざまな IP 制御フラグを選択して、このフィルタの一部として組み込みます。

[フラグメント] に設定されたフラグメント制御フラグを持つ IP パケットを組み込む場合、**[フラグメント]** ボックスをチェックします。IP ヘッダの [ホップ制限] フィールドの値を持つ IP パケットを組み込む場合、**[ホップ制限]** の値を設定します。

[プロトコル] さまざまな TCP/IP スィートプロトコルを選択して、このフィルタの一部として組み込みます。プロトコルが一覧にない場合、**[他のプロトコル]** フィールドに手動で入力します。ClearSight により、指定されたプロトコルが IP ヘッダのプロトコルフィールドに検出されると、フレームが組み込まれます。

[フレーム] **[ブロードキャスト]** のチェックボックスをオンにして、このフィルタの一部としてブロードキャストフレームを組み込みます。

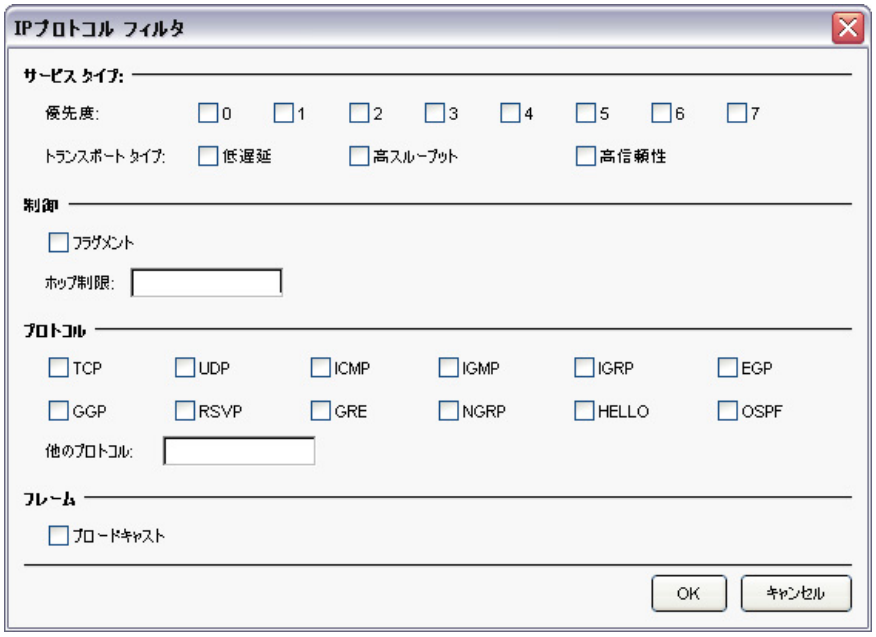


図 9-26: IP のフィルタ条件

TCP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[TCP]** カウンタをクリックして、さまざまな TCP トラフィックのタイプを指定し、このフィルタの一部として含めます。選択された条件のいずれかを含むフレームが、このフィルタの一部として含められます。図 9-27 で示すように、TCP トラフィックに対して次の条件でフィルタをかけることができます。

[TCP フラグ] フィルタを設定して、最大 6 つの制御フラグをそれぞれ TCP ヘッダに組み込むことができます。チェックされたフラグを含むパケットは、このフィルタの一部として組み込まれます。

[ウィンドウ] フィルタを設定して、特定の値を TCP ヘッダのウィンドウ部分に組み込むことができます。**[スライディングウィンドウサイズ :]** フィールドに値を入力します。

[プロトコル] さまざまな上位層のプロトコルを選択して、このフィルタの一部として組み込みます。ClearSight により、指定されたプロトコルに関連付けられたポート番号がパケットの TCP ヘッダに検出されると、パケットが組み込まれます。

特定のプロトコルが一覧にない場合、**[他のプロトコル]** フィールドでポート番号を指定して、それにフィルタをかけることもできます。

[症状] さまざまな TCP の問題タイプを選択して、このフィルタの一部として組み込みます。**[スロー応答]** と **[スロー TCP コネクション]** の問題のスレッショルドを設定できます。これらのスレッショルドについては、368 ページの「IP しきい値の設定」を参照してください。

重要 : [症状] のフィルタ条件は、フローベースです。これは、ポストキャプチャアナリシスの際に表示フィルタとしてのみ使用されま

す。**[症状]** を設定したどのフィルタも、キャプチャ中には使用できません。パケットベースのフィルタとフローベースのフィルタの違いについては、281 ページの「パケットベースのフィルタとフローベースのフィルタ」を参照してください。

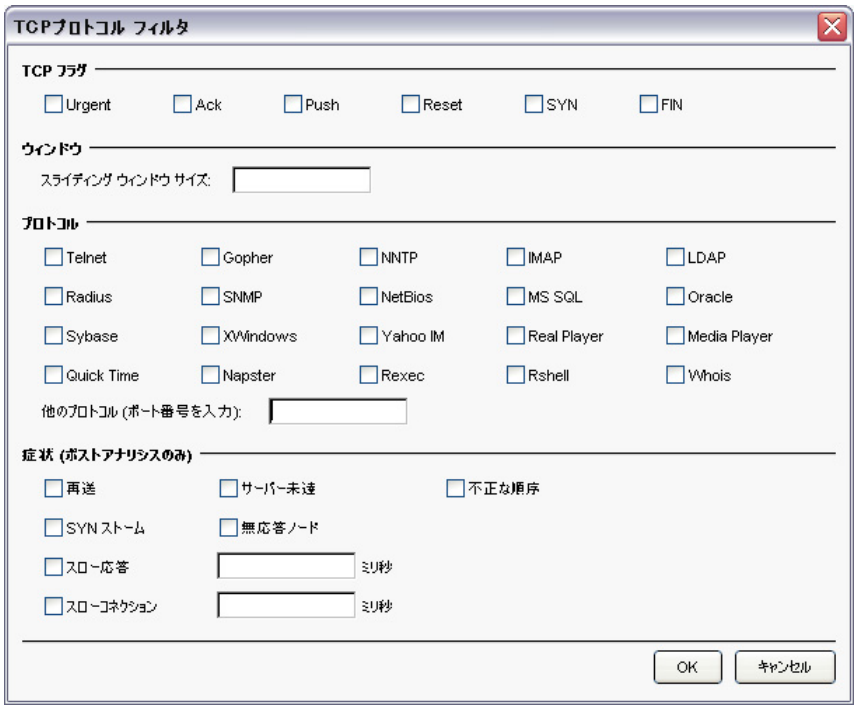


図 9-27: TCP のフィルタ条件

UDP フィルタの設定

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[UDP]** カウンタをクリックして、さまざまな UDP トラフィックのタイプを指定し、このフィルタの一部として含めます。選択された条件のいずれかを含むフレームが、このフィルタの一部として組み込まれます。図 9-28 で示すように、UDP トラフィックに対して次の条件でフィルタをかけることができます。

[プロトコル]

さまざまな上位層のプロトコルを選択して、このフィルタの一部として組み込みます。ClearSight により、指定されたプロトコルに関連付けられたポート番号がパケットの UDP ヘッダに検出されると、パケットが組み込まれます。

特定のプロトコルが一覧にない場合、**[他のプロトコル]** フィールドでポート番号を指定して、それにフィルタをかけることもできます。



図 9-28: UDP のフィルタ条件

MAC アドレスフィルタの設定

MAC アドレス フィルタ (図 9-29) により、通信するペアの MAC アドレス間での特定のタイプのトラフィックを追加できます。必要に応じて、追加するトラフィックの方向を指定できます。**[新規フィルタ]** ダイアログボックスの **[新規フィルタ項目]** メニューにある **[MAC アドレス]** エントリをクリックして、以下の MAC アドレス フィルタのオプションを設定します。

[送信元 MAC] この通信するノードのペアの最初のアドレス。

[方向] このステーションのペアで追加されるトラフィックの方向。ドロップダウンリストを使用して、方向を選択します。

[送信先 MAC] この通信するノードのペアの 2 番目のアドレス。



図 9-29: MAC アドレスフィルタ条件

物理層フィルタの設定

物理層フィルタ (図 9-30) により、特定の VLAN に属するトラフィックを追加できます。全二重イーサネットカードを使用している場合、カードのいずれかのチャネル、または両方のチャネルで検出されたトラフィックを追加することもできます。

[新規フィルタ] ダイアログボックスの **[新規フィルタ項目]** メニューにある **[物理層]** エントリをクリックして、以下の物理層フィルタのオプションを設定します。

[VLAN ID]	トラフィックが追加または除外される VLAN の ID を指定します。
[チャネル]	全二重アダプタのみ。トラフィックが追加または除外されるカード上のチャネルを指定します。
[オートネゴシエーション（ギガビットのみ）]	オートネゴシエーションフレーム、オートネゴシエーション以外のフレーム、またはその両方を、追加するかを指定します。
[フィルタ]	追加するフレームのタイプを指定します。
[サイズ]	ドロップダウンリストから、[>=]（以上）、[==]（等しい）、または [<=]（以下）を選択し、その右側のボックスにバイト数を入力します。これにより、そのバイト数以上、そのバイト数と等しい、またはそのバイト数以下のフレームを含むように設定します。[<=] または [==] を選択した場合、下部のボックスはグレー表示されます。[>=] を選択した場合は、上部のボックスに最小値、下部のボックスに最大値を入力できます。

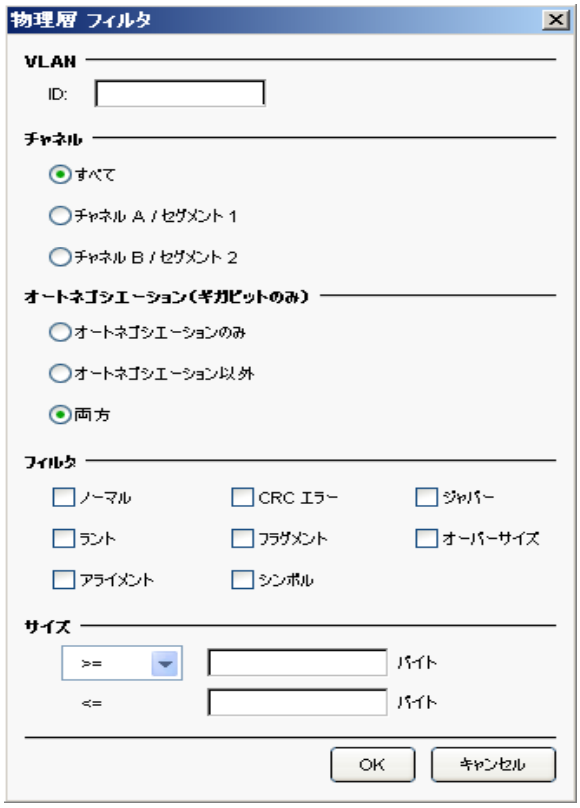


図 9-30: 物理層フィルタ条件

フィルタリスト

フィルタリストは、次のどちらかの方法で表示できます。

- キャプチャワークスペースで、**[設定]** タブの **[フィルタ]** 領域にある **[設定]** ボタンをクリックします (フィルタが有効になっている場合は、最初に **[削除]** ボタンをクリックする必要があります)。
- ポストキャプチャアナリシスワークスペースで、**[翻訳]** タブのステータスバーにある **[フィルタを適用]** アイコン をクリックします。

フィルタリストで、すべての定義したフィルタを管理できます。定義されたフィルタはそれぞれ、その名前、概要の説明、およびフィルタに適用する制限を付けて一覧表示されます。

フィルタリストから、新しいフィルタを作成したり、既存のフィルタの編集や削除ができます。図 9-31 は、フィルタリストを示しています。

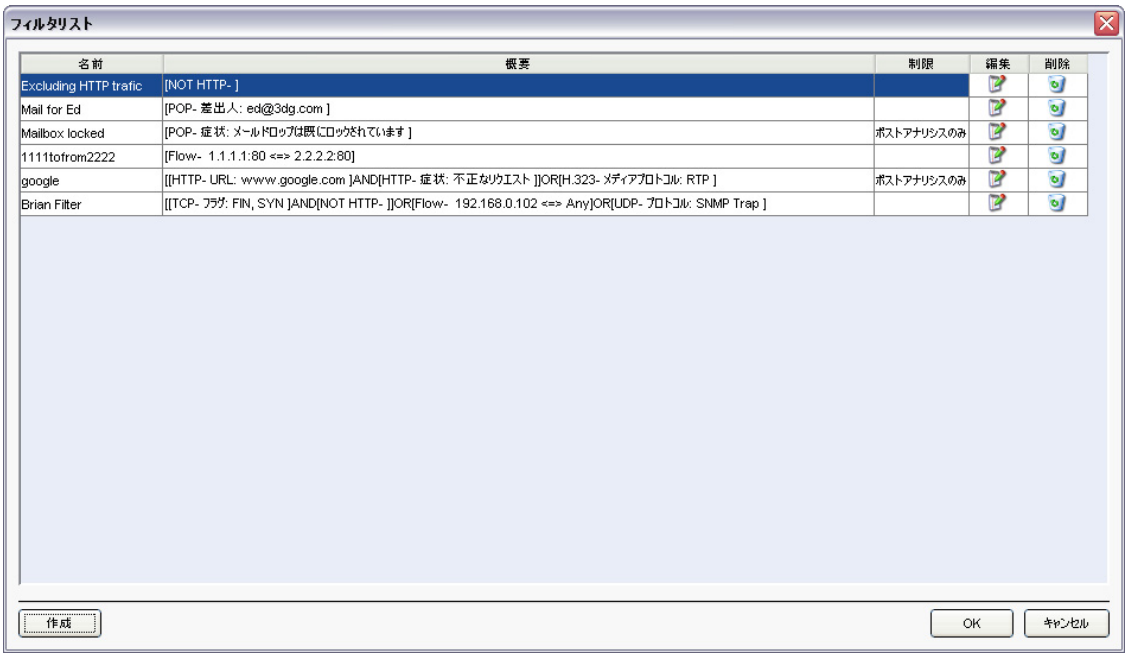


図 9-31: [フィルタリスト] ダイアログボックス

第 10 章

アラートの操作

この章では、ClearSight の**アラート**の操作方法について説明します。ClearSight では、アラート表示での総合的なアラートのレポート機能が提供され、リアルタイムでネットワークの事象と問題を測定できます。さまざまなタイプのアラームにさまざまなアクションを設定できます。アクションには、電子メールの送信、ポケベルの発信、あるいはスクリプトの実行などがあり、特定の重要度のアラームが検出された場合にそれらを実行できます。また、ClearSight がさまざまなタイプのアラートをレポートする方法を指定するスレッショルドも設定できます。

この章は、次の項目で構成されています。

- 「アラートについて」
- 「アラート表示の操作」
- 「重要度とアクションの定義」
- 「問題レポートスレッショルドの設定」

アラートについて

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

ClearSight はアラートをレポートして、ネットワークで検出されたエラー状態への注意を喚起します。ClearSight は、以下のように事象と問題の 2 種類のアラートをレポートします。

- **事象** - 事象は、ネットワーク上で検出された軽度のエラー状態です。単一の事象は詳細に調査する必要はありませんが、事象が何度も繰り返し発生する場合には、よく調べる必要があります。さらに、事象は、同じサーバー、フロー、接続、またはノードに対して、ClearSight が検出した**問題**のトラブルシュートの際に役立ちます。

  代表的な事象としては、HTTP クライアントが受け取る **404 - Not Found** エラーなどの単純なエラーがあります。

- **問題** - 問題は、ただちに調査する必要がある深刻なエラー状態です。ネットワーク上の問題の例として、重複する IP アドレスがあります。この状態は、ネットワークのパフォーマンスを低下させ、予想できない状態を引き起こします。

  ClearSight がレポートするほとんどの問題に対して、スレッショルドを設定できます。この章の 344 ページの「問題レポートスレッショルドの設定」で、スレッショルドの設定方法について説明します。

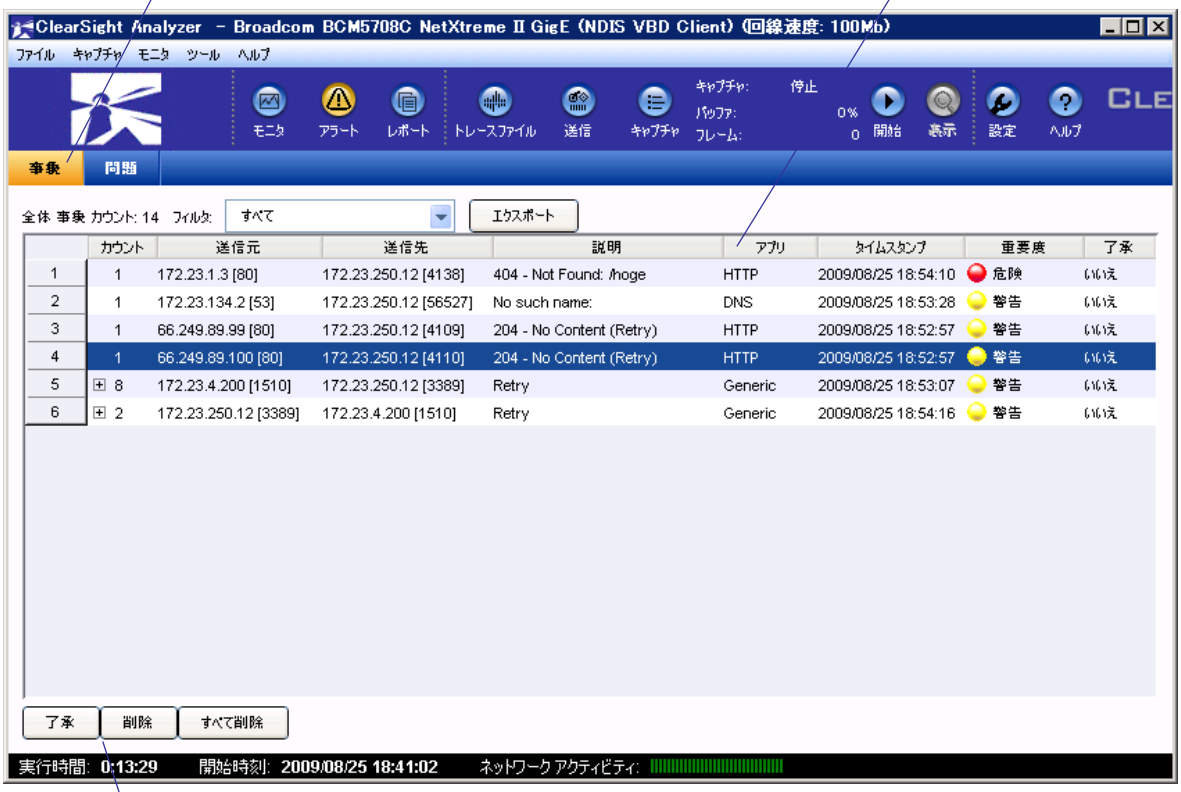
アラート表示の操作

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

ClearSight ツールバーの **[アラート]** ボタンをクリックして、アラートを表示します。アラート表示では、検出した問題と事象を別々のタブに一覧表示します。図 10-1 は、アラート表示の例を示します。

事象と問題は
別々のタブに
表示されます。

列見出しをクリックして、アラート表示を
ソートします。対応する列の三角形は、現
在のソート順を示しています。



これらのボタンを使用して、アラームを
了承および**削除**できます。

図 10-1: アラート表示

アラート表示の [事象] タブの情報

アラート表示の **[事象]** タブに、検出されたすべての事象が一覧表示されます。一覧表示される事象には、以下の統計情報があります。

[カウント]	グループにまとめられた類似タイプの事象の数
[送信元]	この事象の送信元ステーションの IP アドレス。
[送信先]	この事象の送信先ステーションの IP アドレス。
[説明]	事象についての簡単な説明。
[アプリ]	問題のあるアプリケーション。
[タイムスタンプ]	事象が検出された時間。
[重要度]	事象の重要度を示す色分けされたアイコン。
[了承]	この事象が了承されているかどうか。事象を了承するには、そのアラートを選択し **[了承]** ボタンをクリックします。これにより、アラートログをすばやくソートして、了承されていないアラームのみを表示できます。

[事象] タブを統計のタイプごとにソートするには、対応する列見出しをクリックしてから、再度クリックして順番を逆にします。現在ペインをソートしている統計の列見出しに、三角形のアイコンが表示されます。

事象を了承するには **[了承]** ボタンを使用します。事象を削除するには、**[削除]** ボタンを使用します。

アラート表示の [問題] タブの情報

[問題] タブに、検出されたすべての問題が一覧表示されます。一覧表示される問題には、以下の統計情報があります。

[カウント]	グループにまとまられた類似タイプの問題の数
[送信元]	この問題の送信元ステーションの IP アドレス。
[送信先]	この問題の送信先ステーションの IP アドレス。
[説明]	問題についての簡単な説明。
[グループ]	問題のあるアプリケーションタイプ。
[タイムスタンプ]	問題が検出された時間。
[重要度]	問題の重要度を示す色分けされたアイコン。
[了承]	この問題が了承されているかどうか。問題を了承するには、そのアラートを選択し **[了承]** ボタンをクリックします。これにより、アラートログをすばやくソートして、了承されていないアラームのみを表示できます。

[問題] タブを統計のタイプごとにソートするには、対応する列見出しをクリックしてから、再度クリックして順番を逆にします。現在ペインをソートしている統計の列見出しに、三角形のアイコンが表示されます。

問題を了承するには **[了承]** ボタンを使用します。問題を削除するには、**[削除]** ボタンを使用します。

重要度とアクションの定義

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

ClearSight は、特定の重要度のアラートを検出したとき、さまざまなアクションを実行します。**[設定]** ボタン > **[設定]** タブ (344 ページの図 10-7) で重要度とアクションを設定します。

ClearSight Distributed エージェントを操作している場合は、**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[アラートマネージャ]** オプションで、集中的な収集のための問題レポートの送信先とする ClearSight Distributed エージェントマネージャのホスト名または IP アドレスを指定します。詳細については、102 ページの「アラートマネージャの使用」を参照してください。

重要度の定義

ClearSight で発生する問題ごとに、重要度を設定できます。使用可能な重要度は、**[危険]** (高) から、**[注意]**、**[やや注意]**、**[警告]**、**[情報]** (低) まであります。

アラーム重要度の設定方法。

1. ClearSight ツールバーの **[設定]** ボタンをクリックします。
2. **[設定]** タブをクリックします。
3. 左側のリストで **[問題]** > **[スレッショルド]** をクリックします。
4. **[問題]** リスト内のアプリケーション (またはその他の問題グループ) をクリックします。
5. 選択したアプリケーションのアラートがメインペインに一覧表示されます。**[選択]** 列で、アラートのチェックボックスをオンにして選択します。**[しきい値]** 列で、値を編集してしきい値を設定します。ドロップダウンリストを使用して、重要度を設定します。

アクションの定義

[設定] ボタン > **[設定]** タブの左側にある **[問題]** > **[アクション]** オプションを使って、アクションを設定しアラートの重要度に関連付けます。以下のタイプのアクションを設定できます。

- **電子メールアクション** (336 ページ を参照)
- **ポケベルアクション** (338 ページ を参照)
- **スクリプトアクション** (340 ページ を参照)
- **SNMP アクション** (342 ページ を参照)

以下の項では、これらのアクションの設定方法を説明します。アクションの設定を終了したら、**[アクション リスト]** オプションを使用して、アラート重要度に割り当てたアクションの概要を確認できます。[アクション リスト] については、343 ページの「アクション リストの表示」で説明します。

電子メールアクションの設定

電子メールアクションは、特定のアラーム重要度が検出されたときに、1 つ以上のアドレスに電子メールを送信します。**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[アクション]** の **[電子メールアクションの作成]** ボタンをクリックして、電子メールアクションを設定します。次に、図 10-2 に示し、表 10-1 で説明するオプションを設定します。

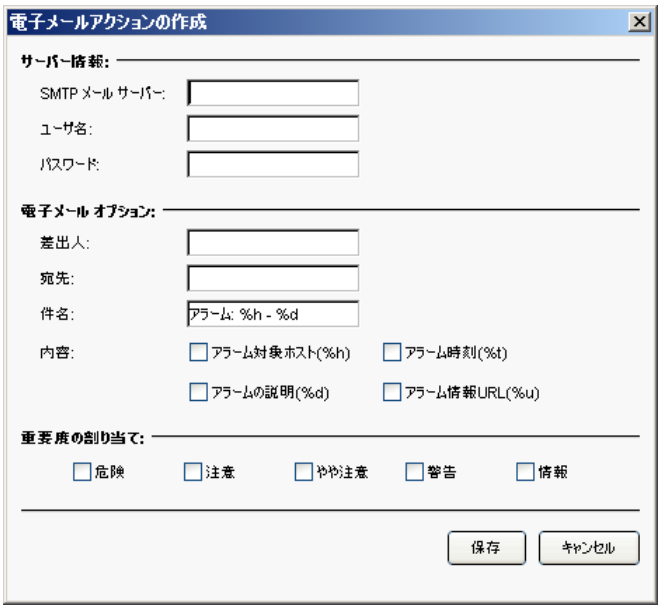


図 10-2: 電子メールアクションの設定

表 10-1: 電子メール アクションのオプション

オプション	説明
[SMTP メールサーバー]	この電子メールの送信に使用する SMTP サーバーのアドレス。
[ユーザ名]	この SMTP サーバー上の送信者のユーザ名。
[パスワード]	この SMTP サーバー上の送信者のパスワード。
[差出人]	この電子メールの **[差出人]** に表示されるアドレス。
[宛先]	この電子メールの宛先のアドレス。

表 10-1: 電子メール アクションのオプション

オプション	説明
[件名]	この電子メールの **[件名]** 行のテキスト。デフォルトで、件名の行には、アラームホストとアラームの説明が含まれます。これを別の値に変更できます。また、以下の [内容] オプションで説明する変数と同じ変数も使用できます。
[内容]	この電子メールの [内容] のテキスト。以下の変数のボックスをチェックして、電子メールの内容を設定します。 • **%h** - この変数により、アラームホストが電子メールの内容に挿入されます。 • **%t** - この変数により、アラームのタイムスタンプホストが電子メールの内容に挿入されます。 • **%d** - この変数により、アラームの説明が電子メールの内容に挿入されます。 • **%u** - この変数により、アラームの詳細情報を提供する URL が電子メールの内容に挿入されます。
[重要度の割り当て]	このアクションに割り当てるアラーム重要度を指定します。このアクションを実行する重要度に対して、各アラーム重要度のボックスをチェックします。ClearSight は、チェックされた重要度のアラームを検出したとき、指定されたアクションを実行します。 例えば、**[危険]** の重要度のみを有効にした場合、ClearSight は [危険] アラートを検出したときに、該当する電子メールのみを送信します。

ヒント : さまざまなアラーム重要度にさまざまな電子メールアクションを設定して、特定の重要度のアラームが検出されたときに適切な対象者に通知できます。例えば、**[やや注意]** アラートを検出したときに、ヘルプデスクに電子メールを送信します。しかし、**[危険]** アラートを検出したときには、ネットワーク管理者に電子メール (ポケベル) で通知するほうが、より適切です。

ポケベルアクションの設定

ポケベルアクション は、特定のアラーム重要度を検出したとき、英数字のページを送信します。**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[アクション]** の **[ポケベル]** ボタンをクリックして、ポケベルアクションを設定します。次に、図 10-3 に示し、表 10-2 で説明するオプションを設定します。

注記：電話をかけて英数字のページを送信するには、ClearSight PC に接続されたモデムが必要です。



図 10-3: ポケベルアクションの設定

表 10-2: ポケベルアクションのオプション

オプション	説明
[モデム番号を選択]	ドロップダウンリストからよく使用するポケベルのアクセス番号 (SkyTel、Airtouch など) を選択するか、または **[入力]** フィールドに番号を入力します。
[PIN 番号]	このポケベルの発信に使用する PIN を入力します。
[メッセージ]	この英数字ページのテキスト。以下の変数を使用してメッセージを設定します。 • **%h** - この変数により、アラームホストがページに挿入されます。 • **%t** - この変数により、アラームのタイムスタンプホストがページに挿入されます。 • **%d** - この変数により、アラームの説明がページに挿入されます。 • **%u** - この変数により、アラームの詳細情報を提供する URL がページに挿入されます。
[モデム設定]	このページで使用する、[ポート]、[パリティ]、[ボーレート] など標準のモデム設定を指定します。
[重要度の割り当て]	このアクションに割り当てるアラーム重要度を指定します。このアクションを実行する重要度に対して、各アラーム重要度のボックスをチェックします。ClearSight は、チェックされた重要度のアラームを検出したとき、指定されたアクションを実行します。 例えば、**[危険]** の重要度のみを有効にした場合、ClearSight は [危険] アラートを検出したときに、該当するページのみを送信します。

スクリプトアクションの設定

スクリプトアクション は、特定のアラーム重要度を検出したとき、JavaScript のカスタムスクリプトを実行します。**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[アクション]** の **[スクリプト]** ボタンをクリックして、スクリプトアクションを設定します。次に、図 10-4 に示し、表 10-3 で説明するオプションを設定します。

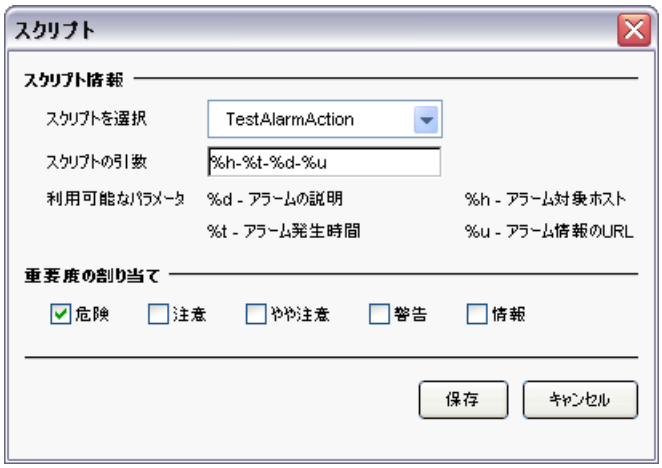


図 10-4: スクリプトアクションの設定

jsfiles¥actions サブディレクトリ内にあるサンプルプログラム **TestAlarmAction.js** をモデルとして使用して、独自のスクリプトを作成できます。

新しい .js ファイルを **jsfiles¥actions** サブディレクトリにコピーすると、**[スクリプトを選択]** ドロップダウンリストにそのファイルが自動的に表示されます。

表 10-3: スクリプトアクションのオプション

オプション	説明
[スクリプトを選択]	ドロップダウンリストからスクリプトを選択します。リストには、**¥Program Files¥ClearSight ¥jsfiles¥actions** に格納されたすべてのスクリプトが含まれます。
[スクリプトの引数]	以下の引数を指定して、選択したスクリプトに渡します。 • **%h** - この変数により、アラームホストがページに挿入されます。 • **%t** - この変数により、アラームのタイムスタンプホストがページに挿入されます。 • **%d** - この変数により、アラームの説明がページに挿入されます。 • **%u** - この変数により、アラームの詳細情報を提供する URL がページに挿入されます。
[重要度の割り当て]	このアクションに割り当てるアラーム重要度を指定します。このアクションを実行する重要度に対して、各アラーム重要度のボックスをチェックします。ClearSight は、チェックされた重要度のアラームを検出したとき、指定されたアクションを実行します。 例えば、**[危険]** の重要度のみを有効にした場合、ClearSight は [危険] アラートを検出したときに、該当するスクリプトのみを実行します。

SNMP アクションの設定

SNMP アクションは、特定のアラーム重要度が検出されたときに、特定のホストに SNMP トラップを送信します。**[設定]** ボタン > **[設定]** タブ > **[問題]** > **[アクション]** の **[SNMP]** ボタンをクリックして、SNMP アクションを設定します。次に、図 10-5 に示し、表 10-4 で説明するオプションを設定します。

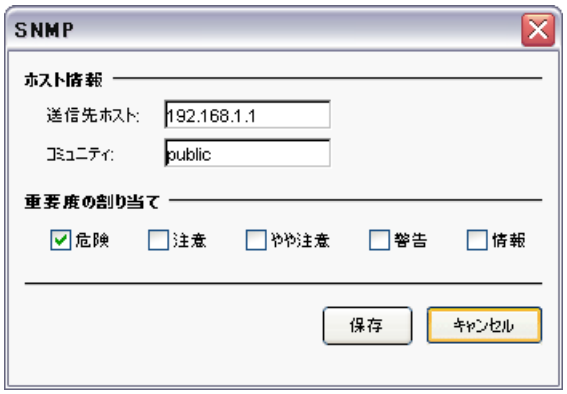


図 10-5: SNMP アクションの設定

表 10-4: SNMP アクションのオプション

オプション	説明
[送信先ホスト]	この SNMP トラップ が送信されるホストの IP アドレス (NMS、あるいは SNMP アクティブモニタ)
[コミュニティ]	コミュニティ名は、トラップとともに含まれます。
[重要度の割り当て]	このアクションに割り当てるアラーム重要度を指定します。このアクションを実行する重要度に対して、各アラーム重要度のボックスをチェックします。ClearSight は、チェックされた重要度のアラームを検出したとき、指定されたアクションを実行します。 例えば、**[危険]** の重要度のみを有効にした場合、ClearSight は [危険] アラートを検出したときに、該当する SNMP トラップのみを送信します。

アクションリストの表示

アクションリストで、現在定義されているアクションを確認できます。**[設定]** ボタン > **[設定]** タブの **[問題]** > **[アクション]** をクリックして、アクションリストを設定します。

アクションリストには、定義されているアクションとそれに割り当てられているアラーム重要度の指標が含まれます。アクションリストから、重要度が割り当てられているアクションを、すばやく確認できます。また、**[編集]** アイコンをクリックしてリスト内のそのアクションを編集したり、**[削除]** アイコンをクリックしてそのアクションを削除できます。テストするアラートの **[テスト]** 列をクリックして、アラートをテストすることもできます。これにより、アラートのシミュレーションが行われ、指定したアクションが実行されます。

図 10-6 は、アクションリストの例を示しています。

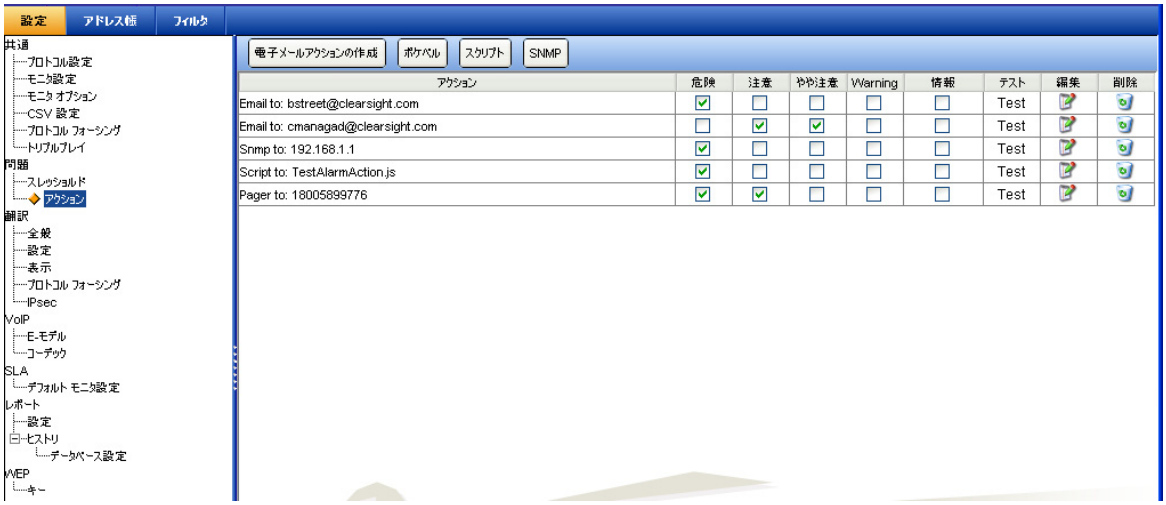


図 10-6: アクションリスト

問題レポートスレッショルドの設定

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

この項では、ClearSight がさまざまなタイプの問題をレポートする方法 (および期間) を制御するスレッショルドの設定方法を説明します。**[設定]** ボタン > **[設定]** タブで問題発生スレッショルドを設定します。このタブ内で、問題のしきい値は、**[問題]** > **[スレッショルド]** セクションにアプリケーション (またはその他の問題グループ) ごとに整理されています。特定の選択肢をクリックして、その選択肢で使用可能な問題のしきい値を設定します。

※この項には、一部 ClearSight Light では実装されていない機能が含まれています。ClearSight Light で、実装されているのは IP 及び DLC の項目のみとなります。

図 10-7 は、HTTP での **[問題]** > **[スレッショルド]** の表示例を示しています。この図のあとに、各プロトコルで使用可能なしきい値の説明を示します。

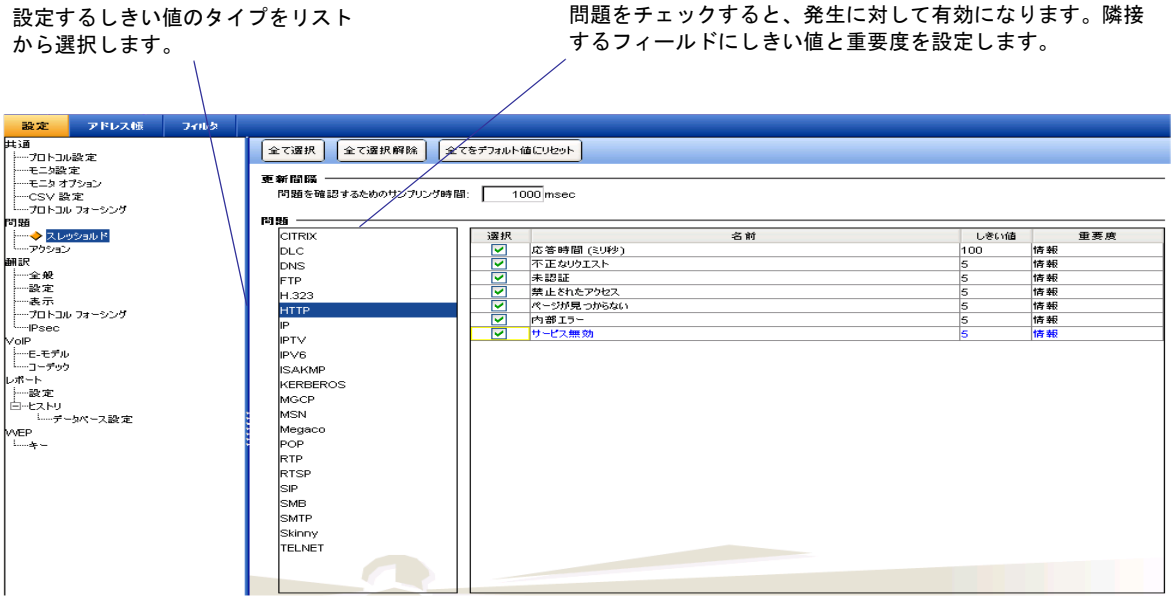


図 10-7: 問題のスレッショルドの設定

DNS しきい値の設定 ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-5 に、DNS で使用可能な問題のしきい値のリストと説明を示します。

表 10-5: DNS の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[アクセス権限なし]	DNS フローで **[アクセス権限なし]** エラー応答コードの数がしきい値を超えたときに、この問題がレポートされます。DNS サーバーでは、認証されていないクライアントがルックアップ要求を送信したときに、このエラーがレポートされます。
[未解決の名前]	DNS フローで **[未解決の名前]** エラー応答コードの数がしきい値を超えたときに、この問題がレポートされます。DNS サーバーでは、ルックアップ要求で送信された名前の IP アドレスを特定できないときに、このエラーがレポートされます。
[クエリー拒否]	DNS フローで **[クエリー拒否]** エラー応答コードの数がしきい値を超えたときに、この問題がレポートされます。DNS サーバーでは、ポリシーに基づいて要求の実行を拒否したときに、このエラーがレポートされます。

FTP しきい値の設定 ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-6 に、FTP で使用可能な問題のしきい値のリストと説明を示します。

表 10-6: FTP の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[最大同時ユーザ]	FTP フローで **[最大同時ユーザ]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、クライアントの同時接続数が最大数になったときに、このエラーがレポートされます。
[アクセス権限なし]	FTP フローで **[アクセス権限なし]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、ユーザ名とパスワードを必要とするファイルをクライアントが要求したときに、このエラーがレポートされます。
[無効なファイル]	FTP フローで **[無効なファイル]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、(取得中などにより) 現在ビジー状態にあるファイルをクライアントが要求したときに、このエラーがレポートされます。
[不正なコマンド]	FTP フローで **[不正なコマンド]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、クライアントのコマンドを認識できないときに、このエラーがレポートされます。
[不正なパラメータ]	FTP フローで **[不正なパラメータ]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、クライアントのコマンドにエラーがあるときに、このエラーがレポートされます。
[未実装のコマンド]	FTP フローで **[未実装のコマンド]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、サーバーが認識するがサポートしないコマンドをクライアントが送信したときに、このエラーがレポートされます。

表 10-6: FTP の問題のしきい値

名前	説明
[不正なコマンド シーケンス]	FTP フローで **[不正なコマンド シーケンス]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、不正なコマンドのシーケンスをクライアントから受信したときに、このエラーがレポートされます。
[コマンドの無効なパラメータ]	FTP フローで **[コマンドの無効なパラメータ]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、不適切なパラメータを含んだクライアントのコマンドを受信したときに、このエラーがレポートされます。
[不明なページタイプ]	FTP フローで **[不明なページタイプ]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、サーバーが理解しないページ要求をクライアントが実行したときに、このエラーがレポートされます。
[許可されないファイル名]	FTP フローで **[許可されないファイル名]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、クライアントが不正なファイル名でファイルを格納しようとしたときに、このエラーがレポートされます。
[ディスク容量が不十分]	FTP フローで **[ディスク容量が不十分]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、クライアントが使用可能なディスク容量より大きいファイルを格納しようとしたときに、このエラーがレポートされます。
[超過したストレージ割り当て]	FTP フローで **[超過したストレージ割り当て]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、クライアントが現在のディレクトリのアロケーションより大きいファイルを格納しようとしたときに、このエラーがレポートされます。
[ローカル エラー発生]	FTP フローで **[ローカル エラー発生]** エラーの数がしきい値を超えたときに、この問題がレポートされます。FTP サーバーでは、クライアントの要求を完了させる妨げとなるローカルエラーに遭遇したときに、このエラーがレポートされます。

Telnet しきい値の設定





表 10-7 に、Telnet で使用可能な問題のしきい値のリストと説明を示します。

表 10-7: Telnet 問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[不正なログイン]	Telnet フローで **[不正なログイン]** エラーの数がしきい値を超えたときに、この問題がレポートされます。Telnet サーバーでは、クライアントが不正なファイル名でファイルを格納しようとしたときに、このエラーがレポートされます。
[最大同時ユーザ]	Telnet フローで **[最大同時ユーザ]** エラーの数がしきい値を超えたときに、この問題がレポートされます。Telnet サーバーでは、クライアントの同時接続数が最大数になったときに接続要求に応じて、このエラーがレポートされます。

Citrix しきい値の設定

表 10-8 に、Citrix で使用可能な問題のしきい値のリストと説明を示します。

表 10-8: Citrix の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。

HTTP しきい値の設定 ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-9 に、HTTP で使用可能な問題のしきい値のリストと説明を示します。

表 10-9: HTTP の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[不正なリクエスト]	HTTP フローで **[不正なリクエスト]** エラー (コード 400) の数がしきい値を超えたときに、この問題がレポートされます。HTTP サーバーでは、クライアントの要求を理解できなかったときに、**[不正なリクエスト]** エラーがレポートされます。
[未認証]	HTTP フローで **[未認証]** エラー (コード 401) の数がしきい値を超えたときに、この問題がレポートされます。HTTP サーバーでは、ユーザ名とパスワードを必要とするページをクライアントが要求したときに、**[未認証]** エラーがレポートされます。
[禁止されたアクセス]	HTTP フローで **[禁止]** エラー (コード 403) の数がしきい値を超えたときに、この問題がレポートされます。HTTP サーバーでは、要求されたページへのアクセスが禁止されているときに、**[禁止]** エラーがレポートされます。
[ページが見つからない]	HTTP フローで **[ページが見つからない]** エラー (コード 404) の数がしきい値を超えたときに、この問題がレポートされます。HTTP サーバーでは、要求されたページが見つからなかったときに、[ページが見つからない] エラーがレポートされます。

表 10-9: HTTP の問題のしきい値

名前	説明
[内部エラー]	HTTP フローで **[内部サーバーエラー]** エラー (コード 500) の数がしきい値を超えたときに、この問題がレポートされます。HTTP サーバーでは、不測のエラー状態に遭遇したときに、このエラーがレポートされます。
[サービス無効]	HTTP フローで **[サービス利用不可]** エラー (コード 503) の数がしきい値を超えたときに、この問題がレポートされます。HTTP サーバーでは、オーバーロードまたは一時的にダウンしているために要求を完了できないときに、このエラーがレポートされます。

POP しきい値の設定 ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-10 に、POP で使用可能な問題のしきい値のリストと説明を示します。

表 10-10: POP の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[メール受信]	POP フローで **[メール受信]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[メッセージがない]	POP フローで **[メッセージがない]** エラーの数がしきい値を超えたときに、この問題がレポートされます。POP サーバーでは、クライアントがサーバーにないメッセージを取り出そうとしたときに、このエラーメッセージが返されます。
[適合するメールボックス無し]	POP フローで **[適合するメールボックス無し]** エラーの数がしきい値を超えたときに、この問題がレポートされます。POP サーバーでは、クライアントがサーバーにないメールボックスにアクセスしようとしたときに、このエラーメッセージが返されます。
[不正なパスワード]	POP フローで **[不正なパスワード]** エラーの数がしきい値を超えたときに、この問題がレポートされます。POP サーバーでは、クライアントが間違ったパスワードを使ってメールボックスにアクセスしようとしたときに、このエラーメッセージが返されます。
[許可がありません]	POP フローで **[許可がありません]** エラーの数がしきい値を超えたときに、この問題がレポートされます。POP サーバーでは、このエラーメッセージを返して、特定の POP 要求を拒否します。

表 10-10: POP の問題のしきい値

名前	説明
[メールドロップがロックされました]	POP フローで **[メールドロップがロックされました]** エラーの数がしきい値を超えたときに、この問題がレポートされます。POP サーバーでは、クライアントが既にロックされたメールボックスにアクセスしようとしたときに、このエラーメッセージが返されます。
[メールボックスをロックできない]	POP フローで **[メールボックスをロックできない]** エラーの数がしきい値を超えたときに、この問題がレポートされます。POP サーバーでは、指定されたメールボックスをロックできないときに、このエラーメッセージが返されます。

SMTP しきい値の設定  

表 10-11 に、SMTP で使用可能な問題のしきい値のリストと説明を示します。

表 10-11: SMTP の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[アクセス権限なし]	フロー上でサーバーがクライアントに返した **[アクセス権限なし]** エラーの数がしきい値を超えたときに、この問題がレポートされます。SMTP サーバーでは、クライアントが許可されていないサービスを要求したときに、[アクセス権限なし] エラーメッセージが送信されます。
[リソースなし]	フロー上でサーバーがクライアントに返した **[リソースなし]** エラーの数がしきい値を超えたときに、この問題がレポートされます。SMTP サーバーでは、クライアントの要求を実行するリソースが不足しているときに、[リソースなし] エラーメッセージが送信されます。

MSN しきい値の設定

ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-12 に、MSN で使用可能な問題のしきい値のリストと説明を示します。

表 10-12: MSN 問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[エラー]	フロー上でサーバーがクライアントに返したエラーの数がしきい値を超えたときに、**[エラー]** 問題がレポートされます。

H.323 しきい値の設定 ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-13 に、H.323 で使用可能な問題のしきい値のリストと説明を示します。

表 10-13: H.323 の問題のしきい値

名前	説明
[コール setup 時間 (マイクロ秒)]	H.323 VoIP コールの確立にかかる時間がしきい値を超えたときに、この問題がレポートされます (マイクロ秒)。コール確立時間は、初期**セットアップ**のメッセージとコールされたパーティからの対応する**アラート**のメッセージとの間の時間として測定されます。
[コール失敗]	特定のフローでのコール失敗の数がしきい値を超えたときに、この問題がレポートされます。[コール失敗] は、H.225 シグナリングメッセージでレポートされます。
[ゲートキーパー拒否]	[ゲートキーパー拒否] メッセージの数がしきい値を超えたときに、この問題がレポートされます。[RAS ゲートキーパー拒否] は、H.225 ターミナルからのゲートキーパー要求が拒否されたことを示します。
[登録拒否]	[登録拒否] メッセージの数がしきい値を超えたときに、この問題がレポートされます。RAS ゲートキーパーは [登録拒否] メッセージを送信して、H.225 ターミナルからの登録要求を拒否します。
[登録解除拒否]	[登録解除拒否] メッセージの数がしきい値を超えたときに、この問題がレポートされます。RAS ゲートキーパーは [登録解除拒否] メッセージを送信して、H.225 ターミナルからの登録解除要求を拒否します。
[アドミッション拒否]	[アドミッション拒否] メッセージの数がしきい値を超えたときに、この問題がレポートされます。RAS ゲートキーパーは [アドミッション拒否] メッセージを送信して、H.225 ターミナルからの承認要求を拒否します。
[帯域拒否]	[帯域拒否] メッセージの数がしきい値を超えたときに、この問題がレポートされます。RAS ゲートキーパーは [帯域拒否] メッセージを送信して、H.225 ターミナルからの帯域要求を拒否します。

表 10-13: H.323 の問題のしきい値

名前	説明
[ロケーション拒否]	[ロケーション拒否] メッセージの数がしきい値を超えたときに、この問題がレポートされます。RAS ゲートキーパーは [ロケーション拒否] メッセージを送信して、H.225 ターミナルからのロケーション要求を拒否します。
[解放拒否]	[解放拒否] メッセージの数がしきい値を超えたときに、この問題がレポートされます。RAS ゲートキーパーは、[解放拒否] メッセージを送信して、H.225 ターミナルからの解放要求を拒否します。

SIP しきい値の設定 ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-14 に、SIP で使用可能な問題のしきい値のリストと説明を示します。

表 10-14: SIP の問題のしきい値

名前	説明
[コール setup 時間 (マイクロ秒)]	SIP VoIP コールの確立にかかる時間がしきい値を超えたときに、この問題がレポートされます (マイクロ秒)。
[コール失敗]	特定のフローでのコール失敗の数がしきい値を超えたときに、この問題がレポートされます。[コール失敗] は、SIP シグナリングメッセージでレポートされます。
[クライアント エラー]	特定のフローでのクライアントエラーの数がしきい値を超えたときに、この問題がレポートされます。
[サーバー エラー]	特定のフローでのサーバーエラーの数がしきい値を超えたときに、この問題がレポートされます。
[グローバル エラー]	特定のフローでのグローバルエラーの数がしきい値を超えたときに、この問題がレポートされます。

Skinny しきい値の設定

ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-15 に、Skinny で使用可能な問題のしきい値のリストと説明を示します。

表 10-15: Skinny の問題のしきい値

名前	説明
[コール setup 時間 (マイクロ秒)]	Skinny VoIP コールの確立にかかる時間がしきい値を超えたときに、この問題がレポートされます (マイクロ秒)。
[コール失敗]	特定のフローでのコール失敗の数がしきい値を超えたときに、この問題がレポートされます。[コール失敗] は、Skinny シグナリングメッセージでレポートされます。
[リリース時間 (ミリ秒)]	サーバーが、しきい値で指定した時間 (ミリ秒) 以内に Skinny VoIP コールをリリースしなかったときに、**[リリース時間]** 問題がレポートされます。

MGCP しきい値の設定





表 10-16 に、MGCP で使用可能な問題のしきい値のリストと説明を示します。

表 10-16: MGCP の問題のしきい値

名前	説明
[コール setup 時間 (マイクロ秒)]	MGCP VoIP コールの確立にかかる時間がしきい値を超えたときに、この問題がレポートされます (マイクロ秒)。
[コール失敗]	特定のフローでのコール失敗の数がしきい値を超えたときに、この問題がレポートされます。[コール失敗] は、MGCP シグナリングメッセージでレポートされます。
[トランシエント エラー]	特定のフローでのトランシエントエラーの数がしきい値を超えたときに、この問題がレポートされます。
[パーマネント エラー]	特定のフローでのパーマネントエラーの数がしきい値を超えたときに、この問題がレポートされます。

Megaco しきい値の設定

ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-17 に、Megaco で使用可能な問題のしきい値のリストと説明を示します。

表 10-17: Megaco の問題のしきい値

名前	説明
[コール setup 時間 (マイクロ秒)]	Megaco VoIP コールの確立にかかる時間がしきい値を超えたときに、この問題がレポートされます (マイクロ秒)。
[コール失敗]	特定のフローでのコール失敗の数がしきい値を超えたときに、この問題がレポートされます。[コール失敗] は、Megaco シグナリングメッセージでレポートされます。
[エラー]	特定のフローでのエラーの数がしきい値を超えたときに、この問題がレポートされます。

RTP しきい値の設定

ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-18 に、RTP で使用可能な問題のしきい値のリストと説明を示します。

表 10-18: RTP の問題のしきい値

名前	説明
[サイレント パケット ギャップ (ミリ秒)]	サイレント パケット ギャップがしきい値を超えたときに、この問題がレポートされます。 サイレント パケット ギャップは、一つの RTP パケットの末尾と次のパケットの先頭との間隔をミリ秒で表したものです。通常の RTP トラフィックでは、この間隔は非常に小さなもので、この問題をレポートするには至りません。しかしながら、RTP エンドポイントの中には、送信すべき音声データがない場合、RTP パケットを送信しないように設定できるものがあります。これは、無音圧縮（Silence Suppression）や発話区間検出（Voice Activity Detection: VAD）などと呼ばれる技術です。受信側では、このサイレント パケット ギャップを RTP のタイムスタンプと RTP パケットの連続性を調べることで評価します。もしパケット間の間隔が小さなものではなく、かつ RTP シーケンス番号が 1 だけ増加している場合、サイレントパケットギャップ問題としてレポートします。
[RTP ジッタ]	特定のフローでの RTP ジッタの値がしきい値を超えたときに、この問題がレポートされます。
[平均遅延時間 (秒)]	特定のフローでのパケットの平均遅延時間がしきい値を超えたときに、この問題がレポートされます。
[ドロップフレーム]	特定のフローでのドロップされたフレームの数がしきい値を超えたときに、この問題がレポートされます。
[不正な順序]	特定のフローでの順序が不正なフレームの数がしきい値を超えたときに、この問題がレポートされます。
[MOS]	特定のフローでのパケットの MOS 値 (平均オピニオン評点) がしきい値を下回るときに、この問題がレポートされます。

表 10-18: RTP の問題のしきい値

名前	説明
[MOS (日本仕様)]	特定のフローでのパケットの MOS (日本仕様) 値 (日本平均オピニオン評点) がしきい値を下回るときに、この問題がレポートされます。
[ドロップフレーム / 全 RTP フレーム (%)]	ドロップされた RTP フレームの割合 (%) がしきい値を超えたときに、この問題がレポートされます。
[IPv6 RTP フラグメントロス / 全 IPv6 RTP フラグメント (%)]	損失した IPV6 RTP フラグメントの割合 (%) がしきい値を超えたときに、この問題がレポートされます。
[IPv6 RTP チェックサムエラー / 全 IPv6 RTP フレーム (%)]	チェックサムエラーのある IPV6 RTP フレームの割合 (%) がしきい値を超えたときに、この問題がレポートされます。
[IPv6 RTP フラグメントパケット (/ サンプル間隔 / フロー)]	損失した IPV6 RTP フラグメントの数 (フロー別のサンプル間隔ごと) がしきい値を超えたときに、この問題がレポートされます。
VQFactor	特定のフローで VQFactor の値がしきい値を下回るときに、この問題がレポートされます。
R 値	特定のフローで R 値がしきい値を下回るときに、この問題がレポートされます。
MDI 平均 DF 値 (ミリ秒)	特定のフローで平均 MDI Delay Factor がしきい値を超えたときに、この問題がレポートされます。
MDI MLR 値	特定のフローで平均 MDI Media Loss Rate がしきい値を超えたときに、この問題がレポートされます。

RTSP しきい値の設定

表 10-19 に、RTSP で使用可能な問題のしきい値のリストと説明を示します。

表 10-19: RTSP の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[許可されないメソッド]	**[許可されないメソッド]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[理解されないパラメータ]	**[理解されないパラメータ]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[見つからないカンファレンス]	**[見つからないカンファレンス]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[不十分な帯域]	**[不十分な帯域]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[見つからないセッション]	**[見つからないセッション]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[この状態で無効なメソッド]	**[この状態で無効なメソッド]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[リソースに対して無効なヘッダフィールド]	**[リソースに対して無効なヘッダフィールド]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[無効な範囲]	**[無効な範囲]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[リードオンリーパラメータ]	**[リードオンリーパラメータ]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[許可されないアグリゲートオペレーション]	**[許可されないアグリゲートオペレーション]** エラーの数がしきい値を超えたときに、この問題がレポートされます。

表 10-19: RTSP の問題のしきい値

名前	説明
[アグリゲートオペレーションのみ]	**[アグリゲートオペレーションのみ]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[未サポートトランスポート]	**[未サポートトランスポート]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[デスティネーション未達]	**[デスティネーション未達]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[未サポートオプション]	**[未サポートオプション]** エラーの数がしきい値を超えたときに、この問題がレポートされます。

IPTV しきい値の設定

表 10-20 に、IPTV で使用可能な問題のしきい値のリストと説明を示します。

表 10-20: IPTV の問題のしきい値

しきい値	説明
[ドロップフレーム]	特定のフローでのドロップされたフレームの数がしきい値を超えたときに、この問題がレポートされます。
[不正な順序]	特定のフローでの順序が不正なフレームの数がしきい値を超えたときに、この問題がレポートされます。
[ドロップフレーム / 全メディアフレーム (%)]	ドロップされたメディアフレームの割合 (%) がしきい値を超えたときに、この問題がレポートされます。
[MDI 平均 DF 値（ミリ秒）]	平均 MDI Delay Factor がしきい値を超えたときに、この問題がレポートされます。
[MDI MLR 値]	平均 MDI Media Loss Rate がしきい値を超えたときに、この問題がレポートされます。
[VQFactor]	特定のフローの Video Quality Factor がしきい値を下回ったときに、この問題がレポートされます。

ISAKMP しきい値の設定

ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-21 に、ISAKMP で使用可能な問題のしきい値のリストと説明を示します。

表 10-21: ISAKMP の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[フェーズ 1 失敗]	特定のフローでのフェーズ 1 失敗の数がしきい値を超えたときに、この問題がレポートされます。

Kerberos しきい値の設定

ClearSight Application Flow Analyzer ClearSignt Distributed

表 10-22 に、Kerberos で使用可能な問題のしきい値のリストと説明を示します。

表 10-22: Kerberos の問題のしきい値

名前	説明
[Kerberos サーバー応答なし]	応答がない Kerberos サーバーに対する連続リトライ回数がこのしきい値を超えた場合に、**Kerberos サーバー応答なし**の問題がレポートされます。
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[エラー]	特定のフローでのエラーの数がしきい値を超えたときに、この問題がレポートされます。

SMB しきい値の設定

表 10-23 に、SMB で使用可能な問題のしきい値のリストと説明を示します。

表 10-23: SMB の問題のしきい値

名前	説明
[応答時間 (ミリ秒)]	サーバーが要求に対してしきい値で指定した時間 (ミリ秒) 以内に応答しなかったときに、**[応答時間]** 問題がレポートされます。
[エラー : ファイルがありません]	**[ファイルがありません]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[エラー : アクセス拒否]	**[アクセス拒否]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[エラー : ディスク不良]	**[ディスク不良]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[エラー : 共有違反]	**[共有違反]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[エラー : ネットワークビジー]	**[ネットワークビジー]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[エラー : 不正パスワード]	**[不正パスワード]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[エラー : 期限切れパスワード]	**[期限切れパスワード]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[エラー : ログイン]	**[ログイン]** エラーの数がしきい値を超えたときに、この問題がレポートされます。
[エラー : その他]	その他のエラーの数がしきい値を超えたときに、この問題がレポートされます。

IP しきい値の設定



表 10-24 に、IP で使用可能な問題のしきい値のリストと説明を示します。

表 10-24: IP の問題のしきい値

名前	説明
[Ping ストーム]	秒当たりに見られる Ping メッセージの数がしきい値を超えたときに、この問題がレポートされます。
[Syn ストーム]	秒当たりに見られる TCP SYN メッセージの数がしきい値を超えたときに、この問題がレポートされます。
[再送]	TCP のシーケンス番号が以前の同じコネクションでの値と同じあるいは小さいフレームを検出したときに、この問題がレポートされます。
[タイムアウト]	コネクションの一方の端が他方の端に対してしきい値で指定した時間制限内に応答しなかったときに、この問題がレポートされます。
[遅い TCP コネクション (ミリ秒)]	平均応答時間がしきい値を超えた TCP コネクションを検出したときに、この問題がレポートされます。
[遅い応答 (ミリ秒)]	TCP コネクションの一方の端から他方の端への応答にかかった時間がしきい値を超えたときに、この問題がレポートされます。
[非常に遅い応答 (ミリ秒)]	TCP コネクションの一方の端から他方の端への応答にかかった時間がしきい値を超えたときに、この問題がレポートされます。 **注記 :** [スロー応答] と [非常に遅い応答] の問題は、あまり問題にならないスロー応答と実際に問題になるスロー応答とを識別できるように、相互に動作します。それに応じて、しきい値を設定する必要があります。
[無応答ホスト (再送)]	何度も再送された同じ要求に対してホストが応答しないことを検出したときに、この問題がレポートされます。

表 10-24: IP の問題のしきい値

名前	説明
[重複した IP アドレス]	重複した IP アドレスをネットワーク上で検出したときに、この問題がレポートされます。
[ポートスキャン (ソケット ポート番号)]	指定したポート番号を使用するパケットを検出したときに、この問題がレポートされます。これに未使用のポート番号を設定できます。指定したポート番号に割り当てられた SYN を検出すると、この問題がレポートされます。未使用のポート番号に割り当てられた SYN の検証はポートスキャンが実行されていることの証拠です。

IPv6 しきい値の設定

表 10-25 に、IPv6 で使用可能な 問題としきい値のリストと説明を示します。

表 10-25: IPv6 の問題のしきい値

名前	説明
[IPv6 フラグメントパケットロス (/ サンプル間隔 / フロー)	損失した IPV6 フラグメントの数 (フロー別のサンプル間隔ごと) がしきい値を超えたときに、この問題がレポートされます。
[IPv6 チェックサムエラー (/ サンプル間隔 / フロー)]	IPV6 チェックサムエラーの数 (フロー別のサンプル間隔ごと) がしきい値を超えたときに、この問題がレポートされます。
[IPv6 フラグメントパケットロス (累積数 / フロー)]	損失した IPV6 フラグメントの数 (フロー別の累計) がしきい値を超えたときに、この問題がレポートされます。
[IPv6 チェックサムエラー (累積数 / フロー)]	IPV6 チェックサムエラーの数 (フロー別の累計) がしきい値を超えたときに、この問題がレポートされます。

DLC しきい値の設定

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

表 10-26 に、DLC 層で使用可能な問題のしきい値のリストと説明を示します。

表 10-26: DLC の問題のしきい値

名前	説明
[使用率 (%)]	ネットワーク使用率が 1 秒間隔でしきい値を超えたときに、この問題がレポートされます。
[ブロードキャスト ストーム]	単一の DLC ステーションからの秒当たりのブロードキャストフレーム数がしきい値を超えたときに、この問題がレポートされます。
[マルチキャスト ストーム]	単一の DLC ステーションからの秒当たりのマルチキャストフレーム数がしきい値を超えたときに、この問題がレポートされます。
[高物理エラーレート]	単一の DLC ステーションからの秒当たりの物理エラー数がしきい値を超えたときに、この問題がレポートされます。物理エラーには、CRC エラー、ラント、フラグメント、オーバーサイズエラー、ジャバー、コリジョン、アライメントなどがあります。
Gigabit Link	ギガビットイーサネットアダプタ使用時にギガビットリンクがダウンしたときに、この問題がレポートされます。

第 11 章

アドレス帳の使用

この章では、ClearSight のアドレス帳を使用する方法について説明します。この章は、次の項目で構成されています。

- 「アドレス帳について」
- 「アドレス帳の使用」

アドレス帳について



ClearSight のアドレス帳を使用すると、ポストキャプチャアナリスワークスペースの **[翻訳]** タブで、IP、IPv6、MAC の各アドレスを簡単に認識できる名前で置き換えることができます。IP アドレスより名前の方が覚えやすい場合がほとんどなので、アドレス帳はネットワークデータをトラブルシューティングする際の貴重なツールとなります。

たとえば、**192.168.1.1** という IP アドレスが社内ネットワークのシアトルのルータのインターフェイスで使用されているということを覚える代わりに、アドレス帳を使用して、このアドレスを単に「**シアトルルータ**」などと呼ぶことができます。アドレス帳のエントリーを慎重に管理すると、ネットワークのトラブルシューティングを直感的にわかりやすく行えるようになります。

アドレス帳の使用

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

アドレス帳を表示するには、ClearSight のツールバーの **[設定]** ボタンをクリックし、**[アドレス帳]** タブをクリックします。図 11-1 は、アドレス帳の図とそのエントリーの追加および削除の方法を示したものです。

注記 : [既存のアドレス帳エントリーを上書きする] オプションをチェックした場合、ClearSight は既にアドレス帳に登録されている IP アドレスや名前を含む DNS パケットを検出すると、自動的にアドレス帳エントリを更新します。

新しいエントリーをアドレス帳に追加するには、**[追加]** ボタンをクリックします。

既存のアドレス帳は、各エントリーの横にある対応するアイコンを使用して **[編集]** および **[削除]** できます。

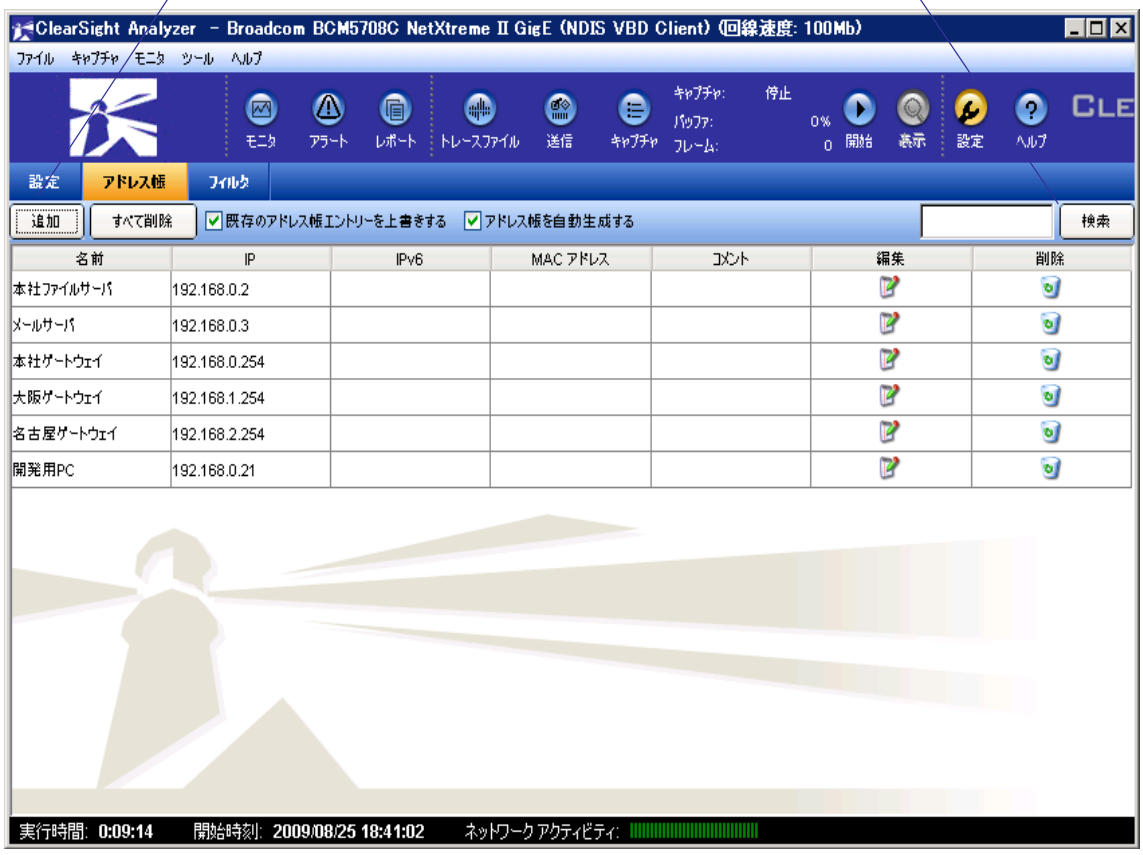


図 11-1: アドレス帳

[追加] ボタンをクリックすると、[ホスト] ダイアログボックスが表示されます (図 11-2)。

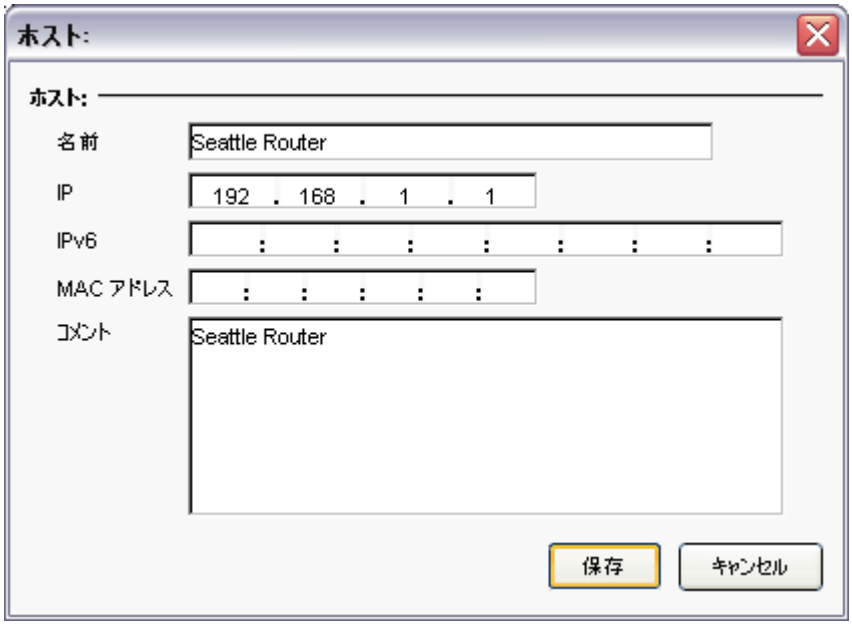


図 11-2: 新しいアドレス帳エントリーの追加

ネットワーク上の IP、IPv6、および MAC の各アドレスのニックネームを追加できます。ここに入力する名前は、ClearSight のポストキャプチャアナリシスで表示される **[翻訳]** タブにある対応するアドレスが置換されます。

アドレス帳の自動生成

ClearSight の検出機能を用いて、アドレス帳のエントリを自動的に生成するようにするには、**[アドレス帳を自動生成する]** チェックボックスにチェックを入れます (374 ページの図 11-1 を参照)。

[既存のアドレス帳エントリーを上書きする] チェックボックスにチェックを入れた場合、既存のアドレス帳エントリーは、新規に検出された名前または IP アドレスで自動的に更新されます。

第 12 章

レポートの使用

この章では、ネットワークデータ用の ClearSight の統合レポートを使用する方法を説明します。この章は次の項目で構成されています。

- 「レポートについて」
- 「アプリケーションレポートの使用」
- 「ネットワークレポートの使用」
- 「DLC レポートの使用」
- 「ユーザ定義レポートの作成」
- 「ヒストリレポーターの使用」

レポートについて

ClearSight Application Flow Analyzer | ClearSight Analyzer Light | ClearSignt Distributed

※アプリケーションレポートは、ClearSight Analyzer Light には搭載されていない機能になります。

ClearSight には、以下のようなさまざまなネットワークの統計情報をチャートにする広範なレポートがあります。

- さまざまなアプリケーションで、最も頻繁にアクセスされるサーバー。
- VoIP アプリケーション のジッター解析とパケットロスの統計情報。
- フレームとバイトごとの、最もアクティブな IP コネクション、会話情報、およびホスト
- フレームとバイトごとの、最もアクティブな DLC ノード
- フレームとバイトごとの、最もアクティブな VLAN
- さまざまな VoIP パフォーマンスレポート
- 以前にモニタしたトラフィックの新しいネットワーク統計を示すヒストリレポート

注記：ヒストリレポートを作成するには、ClearSight Analyzer に **[ヒストリレポーター]** オプションを追加する必要があります。401 ページの「ヒストリレポーターの使用」を参照してください。

ClearSight には、リアルタイムレポートとポストキャプチャレポートがあります。

- リアルタイムレポートは、ClearSight で現在のモニタセッション中に表示されたデータに基づいて作成されます。ClearSight ツールバーの **[レポート]** ボタンをクリックしてから **[リアルタイム]** タブをクリックすると、リアルタイムレポートを表示できます。それに応じて、リアルタイムレポートワークスペースが表示され、さまざまなタイプのリアルタイムレポートにアクセスできます。
- ポストキャプチャレポートは、現在のキャプチャバッファまたはトレースファイル内のデータに基づいて作成されます。ClearSight ツールバーの **[トレースファイル]** ボタンをクリックしてから **[レポート]** タブをクリックすると、ポストキャプチャレポートを表示できます。それに応じて、ポストキャプチャレ

ポートワークスペースが表示され、さまざまなタイプのポストキャプチャレポートにアクセスできます。

注記：リアルタイムモニタ中、ポストキャプチャレポートとリアルタイムレポートは同じように機能します。唯一異なる点は、リアルタイムレポートには使用率分布レポート (399 ページ 参照) が含まれることです。

Windows XP でのレポートの生成

Windows XP で Windows ファイアウォールを無効にしていない場合は、**[レポート]** ボタンをクリックしたときに図 12-1 のダイアログボックスが表示されます。

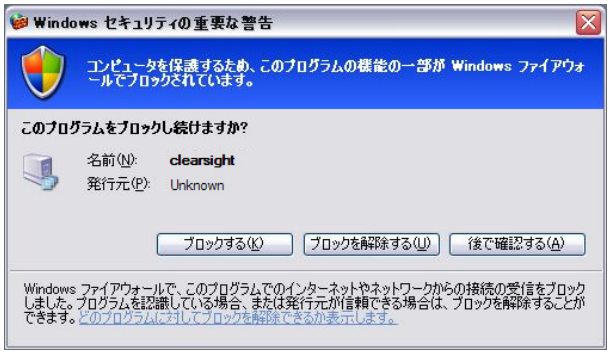


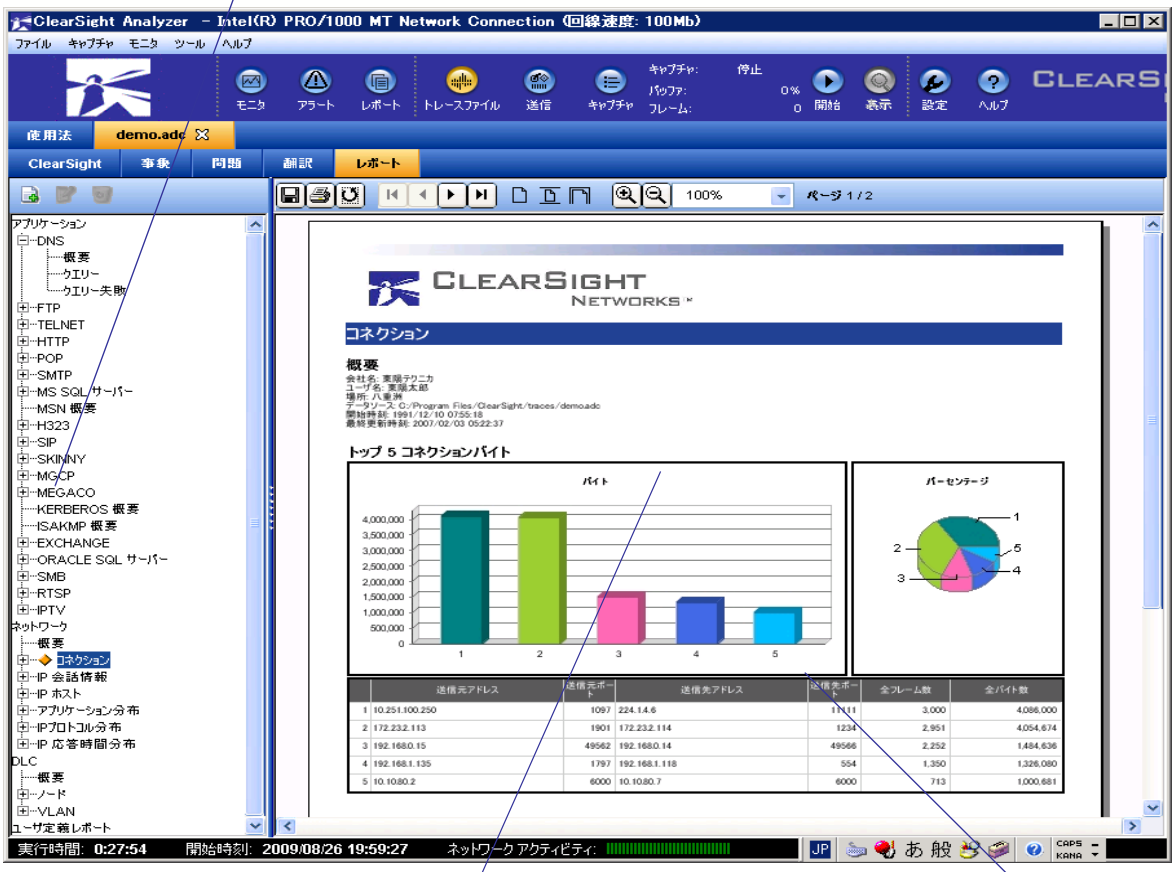
図 12-1: Windows XP での [Windows セキュリティの重要な警告] ダイアログボックス

レポートを有効にするために **[ブロックを解除する]** をクリックしてください。

レポートワークスペース

図 12-2 は標準のレポートワークスペースを示しています。この場合、トレースファイルに基づいたネットワーク接続レポートを示します。

ワークスペースの左側の **[レポート]** メニューを使用して、使用可能な個々のレポートにアクセスできます。項目をクリックすると対応するレポートが表示されます。この例では、ネットワーク接続が選択されています。



ほとんどのレポートには、選択した統計情報を示す単一のチャートとその後に同じ情報を表形式で示すテーブルがあります。

図 12-2: レポートワークスペース

一度レポートをレポートワークスペースに表示すると、レポート上部の右ペインのアイコンを使用して、レポートを表示したり、保存したり、印刷できたりします。html 形式、pdf 形式または rtf 形式でレポートを保存できます。

図 12-6 に示すように、**[設定]** ボタン > **[設定]** タブ > **[レポート]** > **[設定]** 画面では、これらのレポートのいくつかの項目について変更することができます。

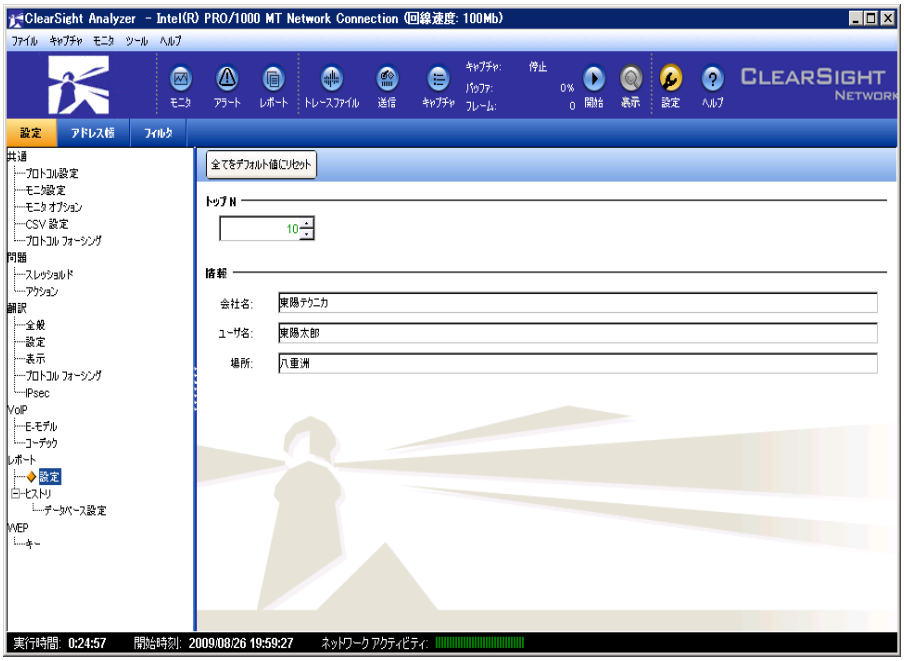


図 12-3: レポート形式の制御

[上位 N] 設定を使用して、レポートの棒グラフに表示されるオブジェクト数を選択できます。たとえば、**[上位 N]** に 10 を選択した場合、HTTP ヒットレポートでは、ヒット数に応じてランク付けされた上位 10 の web サイトの棒グラフが表示されます。5、10、15、または 20 から **[上位 N]** 値を選択できます。

[情報] セクションを使用して、レポートの先頭にある **[サマリ]** セクションに表示する識別情報を入力できます。

アプリケーションレポートの使用

ClearSight Application Flow Analyzer ClearSignt Distributed

ClearSight には、さまざまなアプリケーションのレポートがあります。全てのアプリケーションには、選択したアプリケーションタイプでのトラフィック統計を示す **[概要]** レポートがあります。さらに、いくつかのアプリケーションには、別のレポートもあります。利用可能なレポートについては、アプリケーションごとに以下に説明します。ほとんどのレポートは、380 ページの図 12-2 の例のように構成されています。

- 383 ページの「DNS レポート」
- 384 ページの「FTP レポート」
- 385 ページの「Telnet レポート」
- 386 ページの「HTTP レポート」
- 387 ページの「POP レポート」
- 387 ページの「SMTP レポート」
- 388 ページの「MS SQL サーバーレポート」
- 389 ページの「Oracle SQL サーバーレポート」
- 390 ページの「VoIP レポート」
- 392 ページの「IPTV ビデオ品質レポート」
- 392 ページの「Kerberos レポート」
- 393 ページの「ISAKMP レポート」
- 393 ページの「Exchange レポート」
- 394 ページの「MSN レポート」
- 394 ページの「SMB レポート」
- 395 ページの「RTSP レポート」

DNS レポート

ClearSight には、DNS アプリケーションフロー用の、以下のレポートがあります。

[DNS 概要]

[DNS 概要] レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、クエリー数およびクエリー失敗数を含む、DNS トラフィック統計が表示されます。

[DNS トップ N クエリー]

[DNS トップ N クエリー] レポートには、各上位 N ルックアップの DNS クエリー数を示す棒グラフが表示されます。

さらに、テーブルには各バーの詳細が表示され、要求したホスト名、関連する IP アドレス、ルックアップの実行に使用されたサーバー、クエリーと失敗の数、およびルックアップのタイプが示されます。

[DNS トップ N クエリー失敗]

[DNS トップ N クエリー失敗] レポートには、最も多くクエリーを失敗した上位 N の DNS ルックアップの DNS クエリー失敗数を示す棒グラフが表示されます。

さらに、テーブルには各バーの詳細が表示され、要求したアドレス、失敗したルックアップを報告した DNS サーバー、クエリーと失敗の数、およびルックアップのタイプが示されます。

FTP レポート

ClearSight には、FTP アプリケーションフロー用の、以下のレポートがあります。

[FTP 概要]	**[FTP 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、ダウンロードされたファイル、ダウンロードされたフレーム、ダウンロードされたバイト、アップロードされたファイル、アップロードされたフレーム、アップロードされたバイトを含む、FTP トラフィック統計が表示されます。
[FTP トップ N ダウンロードファイル]	**[FTP トップ N ダウンロードファイル]** レポートには、最も多くファイルをダウンロードされた上位 N の FTP サーバーからダウンロードされたファイル数を示す棒グラフが表示されます。 さらに、テーブルには各バーの詳細が表示されます。
[FTP トップ N アップロードファイル]	**[FTP トップ N アップロードファイル]** レポートには、最も多くファイルをアップロードされた上位 N の FTP サーバーからアップロードされたファイル数を示す棒グラフが表示されます。 さらに、テーブルには各バーの詳細が表示されます。

Telnet レポート

ClearSight には、Telnet アプリケーションフロー用の、以下のレポートがあります。

[TELNET 概要]

[TELNET 概要] レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、現在のセッション数、ログイン数、およびログイン失敗数を含む、Telnet トラフィック統計が表示されます。

[TELNET トップ N ログインセッション]

[TELNET トップ N ログインセッション] レポートには、ログインセッションの最も多かった上位 N の TELNET サーバーのログインセッション数を示す棒グラフが表示されます。

さらに、テーブルには各バーの詳細が表示され、TELNET サーバーアドレス、ログインセッション数、失敗したログイン数、および転送したフレーム数とバイト数が示されます。

[TELNET トップ N ログイン失敗]

[TELNET トップ N ログイン失敗] レポートには、最も多くログインに失敗した上位 N の TELNET サーバーのログインセッション数を示す棒グラフが表示されます。

さらに、テーブルには各バーの詳細が表示され、TELNET サーバーアドレス、ログインセッション数、失敗したログイン数、および転送したフレーム数とバイト数が示されます。

HTTP レポート

ClearSight には、HTTP アプリケーションフロー用の、以下のレポートがあります。

[HTTP 概要]	**[HTTP 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、ヒット数、閲覧ページ数、クライアントエラー、およびサーバーエラーを含む、HTTP トラフィック統計が表示されます。
[HTTP トップ N ヒット]	**[HTTP トップ N ヒット]** レポートには、最もヒットした上位 N の web サーバーを示す棒グラフが表示されます。 さらに、テーブルには各バーの詳細が表示され、HTTP サーバーアドレス、ヒット数、および転送したフレーム数とバイト数が示されます。
[HTTP トップ N トラフィック]	**[HTTP トップ N トラフィック]** レポートには、最も多くトラフィックを転送した上位 N の web サーバーを示す棒グラフが表示されます。 さらに、テーブルには各バーの詳細が表示され、HTTP サーバーアドレス、ヒット数、および転送したフレーム数とバイト数が示されます。

POP レポート

ClearSight には、POP アプリケーションフロー用の、以下のレポートがあります。

[POP 概要]	**[POP 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、受信したメッセージ数、受信したフレーム数、および受信したバイト数を含む、POP トラフィック統計が表示されます。
[POP トップ N メール受信]	**[POP トップ N メール受信]** レポートには、受信したメッセージが最も多い上位 N の POP サーバーを示す棒グラフが表示されます。さらに、テーブルには各バーの詳細が表示され、POP サーバーアドレス、受信したメッセージ数、転送したフレーム数、および転送したバイト数が示されます。

SMTP レポート

ClearSight には、SMTP アプリケーションフロー用の、以下のレポートがあります。

[SMTP 概要]	**[SMTP 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、送信したメッセージ数、送信したフレーム数、および送信したバイト数を含む、SMTP トラフィック統計が表示されます。
[SMTP トップ N メール送信]	**[SMTP トップ N メール送信]** レポートには、送信したメッセージが最も多い上位 N の SMTP サーバーを示す棒グラフが表示されます。さらに、テーブルには各バーの詳細が表示され、SMTP サーバーアドレス、送信したメッセージ数、転送したフレーム数、および転送したバイト数が示されます。

MS SQL サーバーレポート

ClearSight には、MS SQL アプリケーションフロー用の、以下のレポートがあります。

[MSSQL 概要]	**[MSSQL 概要]** レポートには、サーバー数、全フレーム数、全バイト数、および平均スループット、クライアント平均応答時間、サーバー平均応答時間を含む、MS SQL トラフィック統計が表示されます。
[MSSQL SQL コマンド]	**[MSSQL SQL コマンド]** レポートには、10 の SQL コマンド (Commit、Delete、Insert など) ごとの相対頻度を示す棒グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。
[MSSQL トップ N 平均トランザクション時間]	**[MSSQL トップ N 平均トランザクション時間]** には、平均トランザクション時間が最も長い上位 N の MS SQL サーバーを示す棒グラフが表示されます。トランザクション時間は、ClearSight が MS SQL クライアントからの要求を検出した時間とそれに対するサーバーからの応答を検出した時間との間隔で測定されます。 さらに、テーブルには各バーの詳細が表示され、MS SQL サーバーアドレス、平均トランザクション時間、平均 TCP コネクション時間、および平均第 1 バイトダウンロード時間が示されます。

Oracle SQL サーバーレポート

ClearSight には、Oracle SQL アプリケーションフロー用の、以下のレポートがあります。

[ORACLE 概要]

[ORACLE 概要] レポートには、サーバー数、全フレーム数、全バイト数、および平均スループット、クライアント平均応答時間、サーバー平均応答時間を含む、Oracle SQL トラフィック統計が表示されます。

[ORACLE SQL コマンド]

[ORACLE SQL コマンド] レポートには、10 の SQL コマンド (Commit、Delete、Insert など) ごとの相対頻度を示す棒グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。

[ORACLE トップ N 平均トランザクション時間]

[ORACLE トップ N 平均トランザクション時間] レポートには、平均トランザクション時間が最も長い上位 N の ORACLE SQL サーバーを示す棒グラフが表示されます。トランザクション時間は、ClearSight が ORACLE SQL クライアントからの要求を検出した時間とそれに対するサーバーからの応答を検出した時間との間隔で測定されます。

さらに、テーブルには各バーの詳細が表示され、ORACLE SQL サーバーアドレス、平均トランザクション時間、平均 TCP コネクション時間、および平均第 1 バイトダウンロード時間が示されます。

VoIP レポート

ClearSight には、VoIP アプリケーションフロー用の、以下のレポートがあります。

[VoIP 概要]	**[VoIP 概要]** レポートには、サーバー数、全フレーム数、全バイト数、および平均スループット、クライアント平均応答時間、サーバー平均応答時間を含む、VoIP トラフィック統計が表示されます。特定の VoIP プロトコル (H.323、SIP、Skinny、MGCP、および Megaco) の機能と異なるシグナリングおよびエラー統計も表示されます。
[VoIP コールステータス]	**[VoIP コールステータス]** レポートには、各予想コールステータスで観測されるインスタンス数を示す棒グラフおよび円グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。
[VoIP 分布]	**[VoIP 分布]** レポートには、コール数とそれに対する各予想コールタイプで観測される合計通話時間を示す棒グラフおよび円グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。
[**VoIP トップ N 発信者]**	**[VoIP トップ N 発信者]** レポートには、コール数とそれに対する各上位 N 発信者で観測される合計通話時間を示す棒グラフおよび円グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。

[VoIP MOS] レポート

[VoIP MOS] レポートには、以下の内容が表示されます。

0(PCMU) コール品質概要 : コール数、平均オピニオン評点 (MOS)、および全コール品質を示すテーブル。
次のように、品質評価は平均オピニオン評点に関係します。

品質評価	MOS 範囲
1 (良好)	MOS > 4.34
2 (可)	3.60 < MOS ≤ 4.34
3 (不可)	MOS ≤ 3.60

- 0(PCMU) コール品質分布 : 3 つの予想品質値をそれぞれ持つコール数を示す棒グラフおよび円グラフ。同じ情報が、レポートの下部にあるテーブルに示されます。
- 0(PCMU) に基づいたコール品質に影響する要素 : コール品質を低下させる 4 つの要素 (遅延、ジッタ、データ損失およびコーデック) の相対重要度を示す棒グラフおよび円グラフ。同じ情報が、レポートの下部にあるテーブルに示されます。

アプリケーション詳細画面のフローレベルでは、そのほかの VoIP レポートを使用できます。155 ページの「VoIP QoS レポートの表示」を参照してください。

IPTV ビデオ品質レポート

ClearSight には、IPTV アプリケーションフロー用の、以下のレポートがあります。

[ビデオ品質 - 概要] [ビデオ品質 - 概要] レポートには、ビデオストリーム数を含む IPTV トラフィック統計値、MDI DF、MDI MLR、VQFactor、および品質評価の平均値が表示されます。

[ビデオ品質 - 分布] [ビデオ品質 - 分布] レポートには、5 つの品質評価の値それぞれに該当する IPTV ストリームの割合（%）を示す棒グラフおよび円グラフが表示されます。

Kerberos レポート

ClearSight には、Kerberos アプリケーションフロー用の、以下のレポートがあります。

[KERBEROS 概要] **[KERBEROS 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、発行したチケット数、サービスプリンシパル名、AS exchange 数、TGS exchange 数、CS exchange 数およびエラー含む、Kerberos トラフィック統計が表示されます。

ISAKMP レポート

ClearSight には、ISAKMP アプリケーションフロー用の、以下のレポートがあります。

[ISAKMP 概要] **[ISAKMP 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、セッション数、成功数、フェーズ 1 成功数、フェーズ 1 失敗数、フェーズ 2 ネゴシエーション数、クイックモード数、およびクイックモード成功数を含む、ISAKMP トラフィック統計が表示されます。

Exchange レポート

ClearSight には、Exchange アプリケーションフロー用の、以下のレポートがあります。

[Exchange 概要] **[Exchange 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、メッセージ数、メールフレーム数、メールバイト数、失敗数を含む、Exchange トラフィック統計が表示されます。

[Exchange トップ N メール] **[Exchange トップ N メール]** レポートには、最もメッセージを処理した上位 N の Exchange サーバーを示す棒グラフが表示されます。さらに、テーブルには各バーの詳細が表示され、Exchange サーバーアドレス、処理したメッセージ数、転送したフレーム数、転送したバイト数が示されます。

MSN レポート

ClearSight には、MSN アプリケーションフロー用の、以下のレポートがあります。

[MSN 概要] **[MSN 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント / サーバー平均応答時間、ログイン、失敗したログインなど、MSN トラフィックの統計情報が表示されます。また、ファイル転送数、音声会話数、映像会話数、IM (インスタントメッセージング) 会話数、およびそれらに対応する転送バイト数も表示されます。

SMB レポート

ClearSight には、SMB アプリケーションフロー用の、以下のレポートがあります。

[SMB 概要] **[SMB 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、セッション要求数、ファイル要求数、ディレクトリ要求数、DFS 操作数、および MISC 操作数を含む、SMB トラフィック統計が表示されます。

[SMB 要求] **[SMB 要求]** レポートには、5 つの SMB 要求ごとの相対頻度を示す棒グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。

[SMB エラー] **[SMB エラー]** レポートには、9 つの SMB エラーごとの相対頻度を示す棒グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。

RTSP レポート

ClearSight には、RTSP アプリケーションフロー用の、以下のレポートがあります。

[RTSP 概要]	**[RTSP 概要]** レポートには、サーバー数、全フレーム数、全バイト数、平均スループット、クライアント平均応答時間、サーバー平均応答時間、使用した方法の総数、およびクライアントエラーの総数を含む、RTSP トラフィック統計が表示されます。
[RTSP メソッド分布]	**[RTSP メソッド分布]** レポートには、使用した RTSP メソッドごとの相対頻度を示す棒グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。
[RTSP クライアントエラー分布]	**[RTSP クライアントエラー分布]** レポートには、観測された RTSP クライアントエラータイプごとの相対頻度を示す棒グラフが表示されます。同じ情報が、レポートの下部にあるテーブルに示されます。

ネットワークレポートの使用

ClearSight Application Flow Analyzer ClearSignt Distributed

ClearSight には、ネットワーク層のフロー、コネクション、およびホストのレポートがあります。利用可能なレポートについては、以下に説明します。ほとんどのレポートは、380 ページの図 12-2 の例のように構成されています。

- 396 ページの「[ネットワーク概要] レポート」
- 396 ページの「[コネクション] レポート」
- 396 ページの「[IP 会話情報] レポート」
- 397 ページの「[IP ホスト] レポート」
- 397 ページの「[アプリケーション分布] レポート」
- 397 ページの「[IP プロトコル分布] レポート」
- 397 ページの「[IP 応答時間分布] レポート」

[ネットワーク概要] レポート

[ネットワーク概要] レポートには、観測された全 IPv4 トラフィックおよび IPv6 トラフィックの統計が表示されます。さまざまな IP フレームタイプでの数が表示されます。マルチキャストの数、ブロードキャストの数、TCP 数、および UDP 数などの IP プロトコルの構成を一目で見ることができます。

[コネクション] レポート

[コネクション] レポートは、ネットワーク上で最もアクティブな上位 N のコネクションを **[バイト]** と **[フレーム]** で測定します。コネクションは棒グラフ形式と円グラフ形式のほか、テーブルでも表示されます。テーブルには、送信元と送信先の IP アドレスとポート、およびコネクション全体の全フレーム数と全バイト数が一覧表示されます。

[IP 会話情報] レポート

[IP 会話情報] レポートは、ネットワーク上で最もアクティブな上位 N の IP コネクションを **[バイト]** と **[フレーム]** で測定します。コネ

クションは棒グラフ形式と円グラフ形式のほか、テーブルでも表示されます。テーブルには、送信元と送信先の IP アドレスとポート、およびコネクション全体の全フレーム数と全バイト数が一覧表示されます。

注記 : [コネクション] レポートとは異なり、**[IP 会話情報]** レポートは、特定されたペアのポート上のアドレス間の全トラフィックではなく、アドレス間の全トラフィックに関するレポートです。

[IP ホスト] レポート

[IP ホスト] レポートは、ネットワーク上で最もアクティブな上位 N の IP ホストを **[バイト]** と **[フレーム]** で測定します。ホストは棒グラフ形式と円グラフ形式のほか、テーブルでも表示されます。テーブルには、全フレーム数と全バイト数とともに、各ホストが一覧表示されます。

[アプリケーション分布] レポート

[アプリケーション分布] レポートは、トラフィックを **[バイト]** と **[フレーム]** で共通のアプリケーションプロトコルに分類します。アプリケーションプロトコルの構成は棒グラフ形式と円グラフ形式のほか、テーブルでも表示されます。テーブルには、全フレーム数と全バイト数とともに、使用順でプロトコルが一覧表示されます。

[IP プロトコル分布] レポート

[IP プロトコル分布] レポートは、トラフィックを **[バイト]** と **[フレーム]** で共通のトランスポート層プロトコル (UDP、TCP、ICMP など) に分類します。トランスポート層プロトコルの構成は棒グラフ形式と円グラフ形式のほか、テーブルでも表示されます。テーブルには、全フレーム数と全バイト数とともに、使用順でプロトコルが一覧表示されます。

[IP 応答時間分布] レポート

[IP 応答時間分布] レポートは、10 の異なる時間ウインドウに分類された応答数を表示します。応答は、最短時間 (0-25 ms) から最長時間

(2000 ms 以上) で一覧表示されます。レポートの下部にあるテーブルは、各応答時間ウィンドウの正確な発生回数が表示されます。

DLC レポートの使用



ClearSight の **[DLC]** タブには、物理層ノード、VLAN、および一般的な統計情報のレポートがあります。利用可能なレポートについては、以下に説明します。

- 398 ページの「[DLC 概要] レポート」
- 398 ページの「[ノード] レポート」
- 398 ページの「[VLAN] レポート」
- 399 ページの「[使用率分布] レポート」

[DLC 概要] レポート

[DLC 概要] レポートには、観測された全トラフィックの統計が表示されます。使用率、全バイト数、全フレーム数、マルチキャストフレーム数、ブロードキャストフレーム数、およびさまざまなタイプのフレームエラーが表示されます。

[ノード] レポート

[ノード] レポートには、ネットワーク上で最もアクティブな上位 N の DLC レイヤノードが **[バイト]** と **[フレーム]** で表示されます。ノードは棒グラフとテーブルで表示されます。テーブルには、全フレーム数と全バイト数とともに、アドレス順に各ノードが一覧表示されます。

[VLAN] レポート

[VLAN] レポートには、ネットワーク上で最もアクティブな上位 N の VLAN が **[バイト]** と **[フレーム]** で表示されます。VLAN は棒グラフとテーブルで表示されます。テーブルには、全フレーム数と全バイト数とともに、VLAN ID 順に各 VLAN が一覧表示されます。

[使用率分布] レポート

ClearSight では、秒ごとのネットワーク使用率を利用可能なネットワークの帯域の割合で測定します。秒ごとのサンプル値が 10 の使用可能範囲の 1 つに分類されます (20 ～ 30% など)。発生はカウントされ、**[使用率分布]** レポートに棒グラフと円グラフで表示されます。レポートの下部にあるテーブルは、各使用率ウインドウの正確な発生回数が表示されます。

ユーザ定義レポートの作成

レポートワークスペースに一覧表示された定義済みレポートの組み合わせで構成される、複合レポートを作成できます。

ユーザ定義レポートを作成するには、左上の **[新規ユーザ定義レポートの作成]** ボタンをクリックします。[新規ユーザ定義レポートの作成] ダイアログボックス (図 12-4) が表示されます。

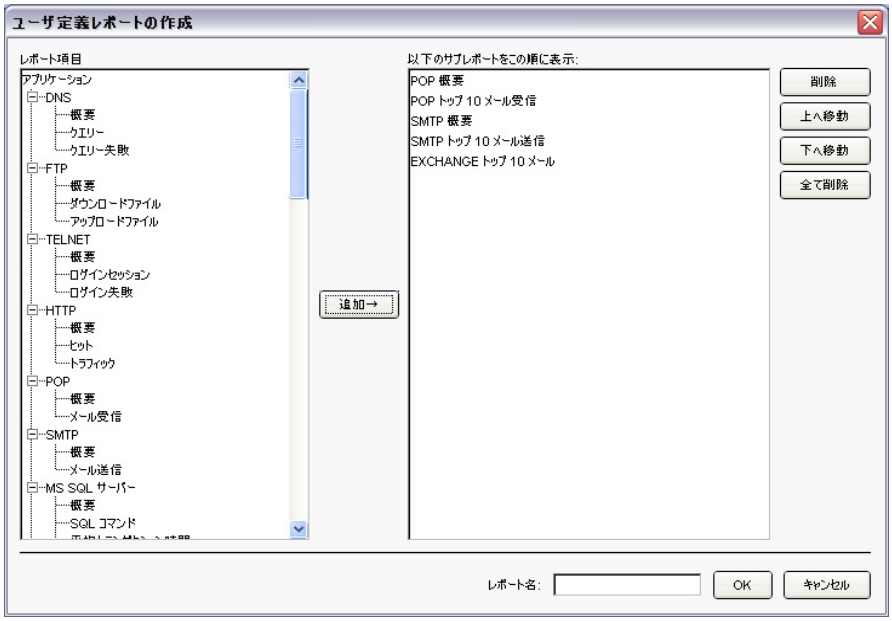


図 12-4: [ユーザ定義レポート] ダイアログボックス

図 12-4 の例では、3 つのメールアプリケーション (POP、SMTP、および Exchange) で利用可能な全レポートを示す複合レポート (AllMailApps) を単一のドキュメントで作成します。

[OK] をクリックすると、図 12-5 に示すように、レポートワークスペースの下部にあるリストに新規ユーザ定義レポートが追加されます。

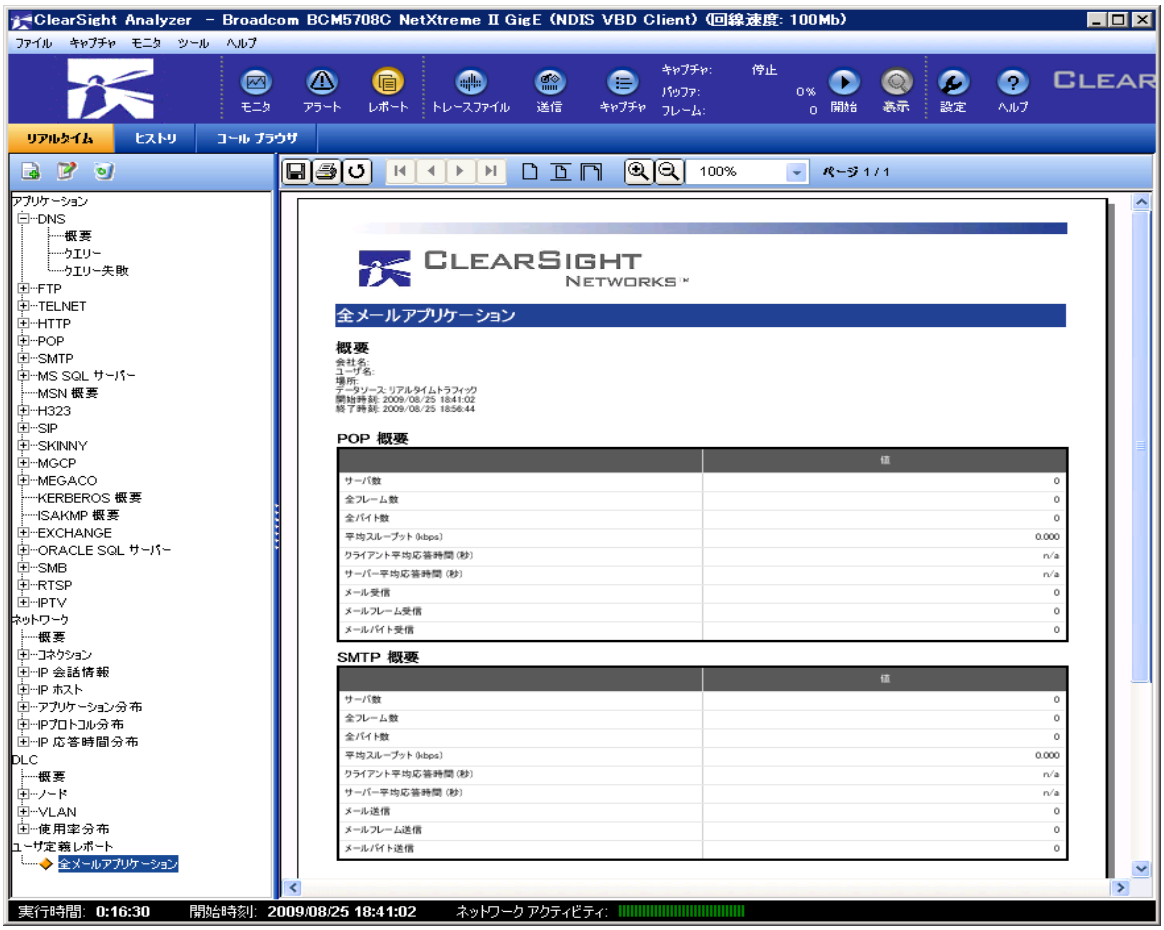


図 12-5: ユーザ定義レポート

レポートワークスペースの既存のユーザ定義レポートを選択してから、**[選択したユーザ定義レポートの編集]** ボタンをクリックすると、既存のユーザ定義レポートの構成を編集できます。

レポートワークスペースの既存のユーザ定義レポートを選択してから、**[選択したユーザ定義レポートの削除]** ボタンをクリックすると、既存のユーザ定義レポートを削除できます。

ヒストリレポーターの使用

[ヒストリレポーター] は、ClearSight Analyzer に追加できるオプションの機能です。この機能があると、ネットワーク上のトラフィックをモニタしながら、アプリケーション、ネットワーク、および DLC レイヤ統計を定期的に保存できます。これらの統計は CSV ファイルに保存され、後でアクセス可能なデータベースに蓄積されます。ネットワークアダプタごとに別個のデータベースがあります。

これらのデータベースの情報に基づいてレポートを作成できます。図 12-6 に示すように、**[設定]** > **[設定]** > **[レポート]** >**[設定]** 画面では、これらのレポートのいくつかの項目について変更することができます。



図 12-6: レポート形式の制御

[上位 N] 設定を使用して、レポートの棒グラフに表示されるオブジェクト数を選択できます。たとえば、**[上位 N]** に 10 を選択した場合、HTTP ヒットレポートでは、ヒット数に応じてランク付けされた上位 10 の web サイトの棒グラフが表示されます。5、10、15、または 20 から **[上位 N]** 値を選択できます。

[情報] セクションを使用して、レポートの先頭にある **[サマリ]** セクションに表示される識別情報を入力できます。

注記 : [レポート] > [設定] 画面は、ヒストリレポートに固有のものではありません。この章で説明している全てのレポートで表示されます。

データ蓄積の制御

[設定] ボタン > **[設定]** タブ > **[レポート]** > **[ヒストリ]** > **[データベース設定]** を選択して、ヒストリレポートに蓄積されるデータを指定できます。これにより、図 12-7 に示すヒストリレポーターのデータベース設定画面が表示されます。

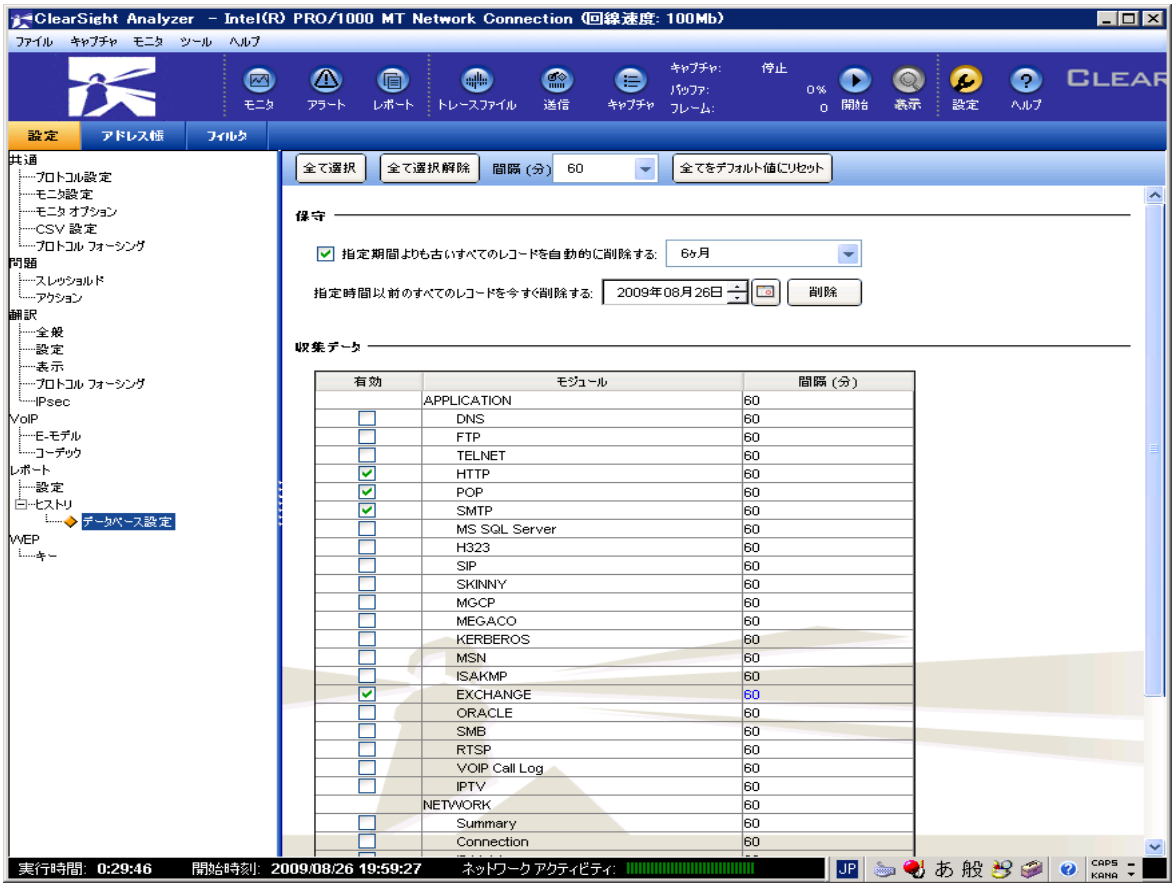


図 12-7: ヒストリレポーターのデータベース設定

画面の上部にある **[メンテナンス]** セクションを使用して、不必要なレコードを削除することにより、データベースのサイズを制御できます。選択した期間 (選択可能な範囲は 1 ヶ月から 2 年) を過ぎたレコードを自動的に削除するように、この制御を設定できます。さ

らに、指定した日付より前に、全てのレコードを即時に削除できます。日付は、提供されるカレンダツールを使用して選択できます。

注記：[即時削除] 機能は、現在のネットワークアダプタのデータベースにのみ影響します。この画面の他の全機能は、全てのネットワークアダプタのデータベースに影響します。

[収集データ] セクションを使用して、データベースに保存する特定のアプリケーション、ネットワーク、および DLC レイヤ統計を選択できます。**[有効]** 列には、これらを選択するためのチェックボックスが表示されます。時間を保存するには、上部にある **[全て選択]**、**[全て選択解除]**、および **[全てをデフォルト値にリセット]** ボタンも使用できます。

選択した統計の各セットについて、それに対応するデータが CSV ファイルに保存されます。その後、**[間隔]** 列を使用して、CSV ファイル内のデータをデータベースに保存する頻度を指定できます。たとえば、**[HTTP]** をチェックして **[間隔]** を 15 分に設定すると、現在 CSV ファイルにある HTTP のデータが 15 ごとにデータベースに保存され、CSV ファイルから削除されます。

ヒストリレポートの作成

データベースの情報に基づいてレポートを作成できます。レポートを作成するには、**[レポート]** > **[ヒストリ]** に進み、作成するレポートを選択します。図 12-9 に示すように、左ペインで選択し、右ペインにレポートが表示されます。

レポートでデータを表示する時間間隔を  ボタンをクリックして選択できます。これによって、図 14-7 に示す、[レポート時刻設定] ダイアログボックスが表示されます。

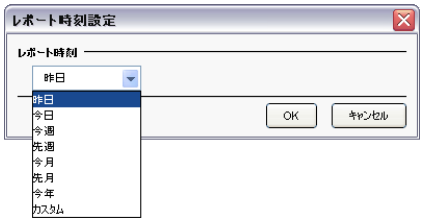


図 12-8: [レポート時刻設定] ダイアログボックス

希望する時間間隔 (または **[カスタム]** 時間間隔) を選択し、**[OK]** をクリックします。その後、図 12-9 に示すようなレポートが表示されます。

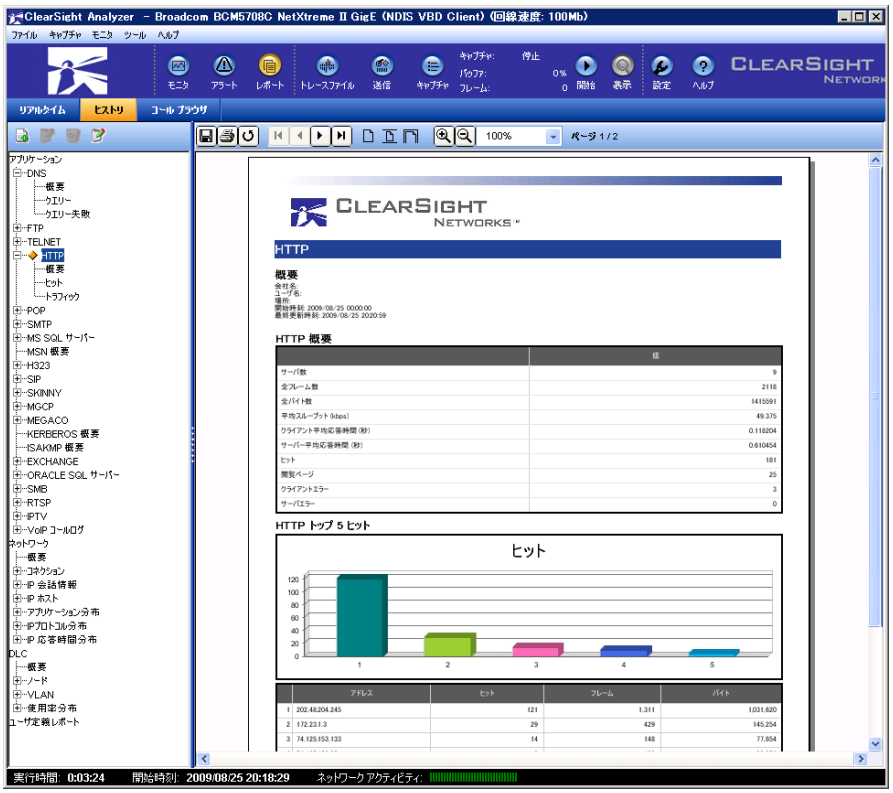


図 12-9: HTTP ヒストリレポートの例

レポート上部の右ペインのアイコンを使用して、レポートを表示したり、保存したり、印刷できたりします。html 形式、pdf 形式または rtf 形式でレポートを保存できます。

トレンドチャート

レポートの任意のテーブル内で、特定の行をクリックして、そのレポートに対して選択したタイムスパンでその統計値がどのように変化するかを示すチャートを生成することができます。

また、特定のテーブルのタイトルをクリックして、複数のトレンドチャートを生成することもできます。その場合、図 12-10 に示したようなダイアログボックスが表示されます。

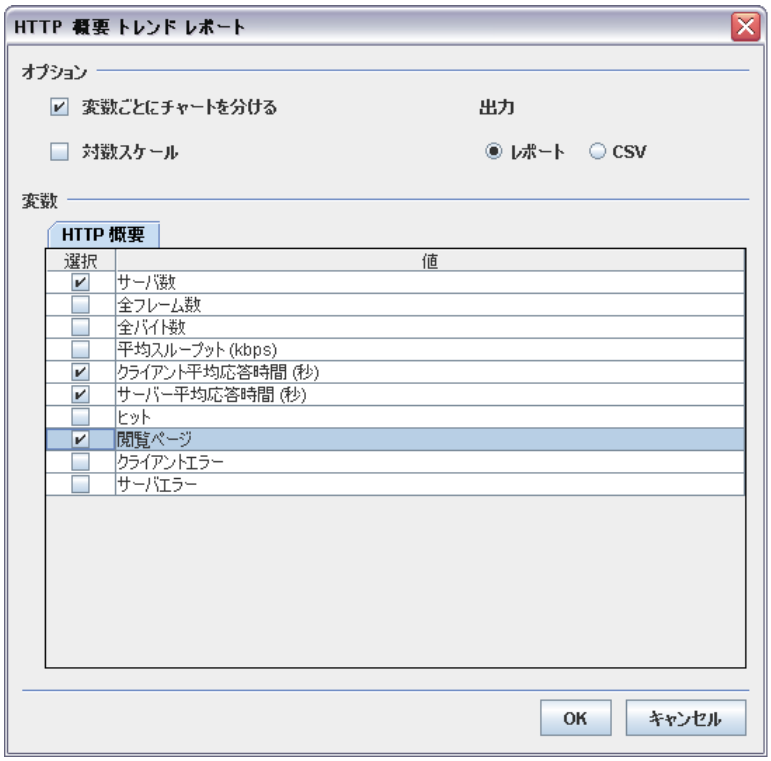


図 12-10: 複数のトレンドチャートの選択

表示する統計値の組み合わせを選択するほかに、それらの統計値を別々のチャートとして表示するか、重ね合わせて表示するかを選択できます。チャートの縦軸の目盛を均等目盛と対数目盛のいずれにするかを選択することもできます。データはレポート形式または CSV データとして出力するよう選択できます。

VoIP コールログの作成

VoIP コールログは、特別な種類のヒストリレポートであり、ネットワーク上の VoIP トラフィックの性能に関するコンパイル情報を見ることができます。図 12-11 に、利用可能な多くの VoIP コールログレポートのうち最初のものを示します。

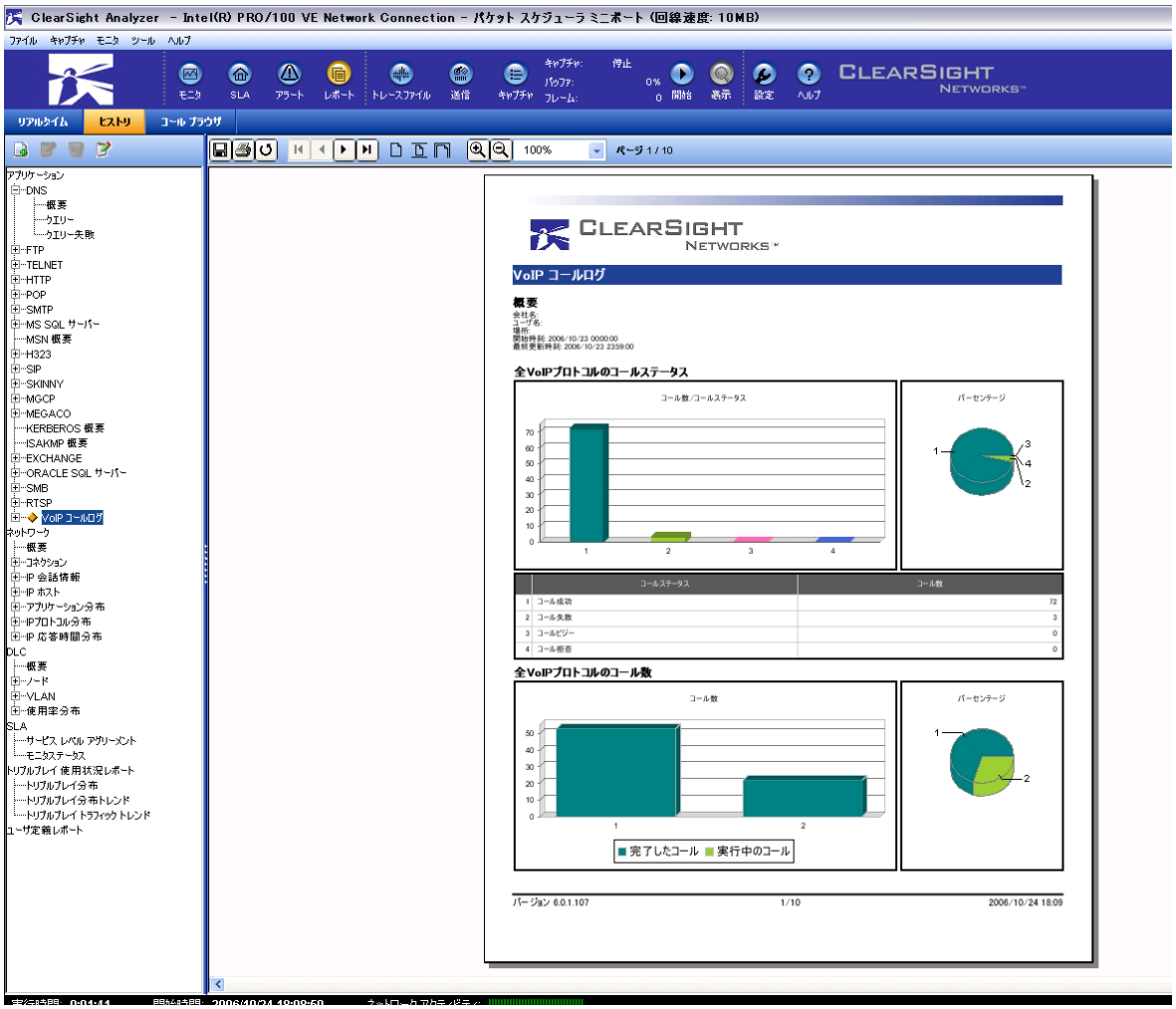


図 12-11: VoIP コールログ

コールブラウザの使用

コールブラウザを使用することにより、ネットワーク上のコールに関する基本情報にアクセスすることができます。図 12-12 にコールブラウザ画面を示します。

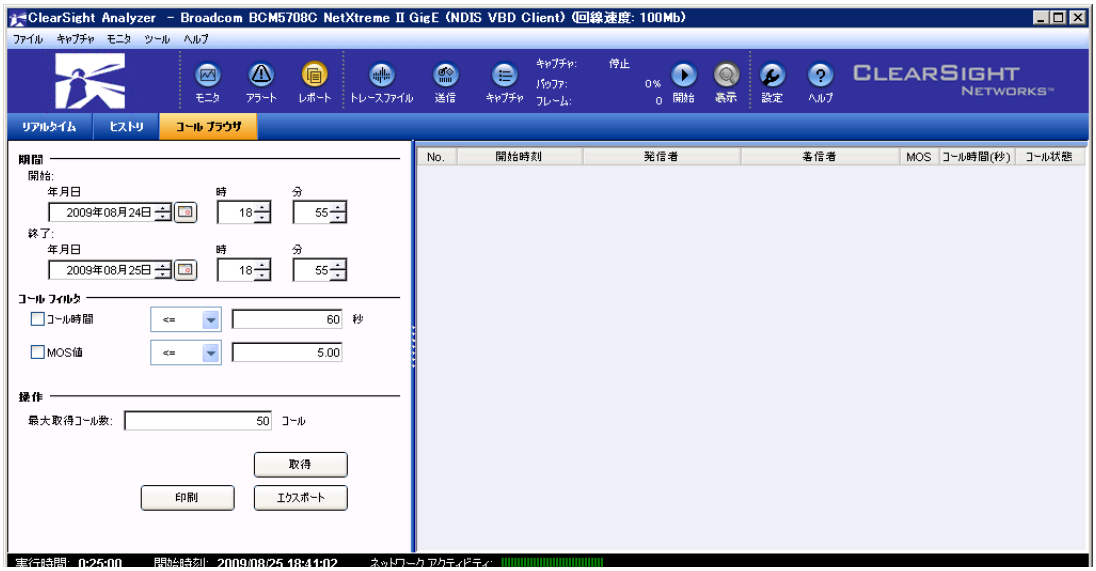


図 12-12: コールブラウザ

図に示したように、特定の時間範囲に調査を制限することができます。**[コールフィルタ]** 領域では、**通話時間**や **MOS 値**の条件を指定できます。また、一覧に載せるコールの最大数を制限することもできます。

条件を満たすコールについて、開始時間、発信者、受信者、**MOS** 採点、および通話時間が一覧に表示され、単に部分的なコールが含まれるかどうかを示します。

第 13 章

パケットジェネレータの使用

この章は、次の項目で構成されています。

- 「パケットジェネレータオプション」
- 「ClearSight パケットジェネレータ機能」
- 「パケットジェネレータの使用」

パケットジェネレータオプション

ClearSight パケットジェネレータが有効になっている場合、ClearSight ツールバーに **[送信]** ボタンが表示されます。**[送信]** ボタンをクリックすると、パケットジェネレータが開始されます。

ClearSight パケットジェネレータ機能

ClearSight パケットジェネレータは、単一のパケットまたはトレースファイルの内容のいずれかに基づいてネットワークトラフィックを生成できます。パケットジェネレータの機能は以下のとおりです。

- ユーザは遅延時間 (パケット間隔) または使用率 (パケットジェネレータトラフィックで使用されるネットワーク帯域幅の割合) のいずれかを設定できます。
- パケットが送信されると、MAC アドレス、IP アドレス、およびアプリケーションポート番号が順次増分されるか、ランダム化されます。
- パケット長をランダム化できます。
- ユーザはパケットの内容を編集できます。
- IPv4 プロトコルおよび IPv6 プロトコルの両方がサポートされます。
- ユーザはパケットジェネレータの設定を保存し再生できます。
- スクリプトを書き、全てのグラフィカルユーザインタフェース機能を実行できます。
- 複数のトレースファイルを開き、遅延オプション、アドレスの変更、およびポート番号の変更を全て制御して、順次再生することができます。

注記 : ClearSight パケットジェネレータは、10/100 全二重イーサネットアダプタまたはギガビットイーサネットアダプタをサポートしません。

パケットジェネレータの使用

ツールバーの [送信] ボタンをクリックし、パケットジェネレータを開始します。

図 13-1 に示すように、パケットジェネレータユーザインタフェースには以下のコンポーネントがあります。

- 「統計テーブル」
- 「トラフィックグラフ」
- 「[トラフィック制御] ボタン」
- 「プロファイルリスト」

それぞれについて、この後で詳しく説明します。

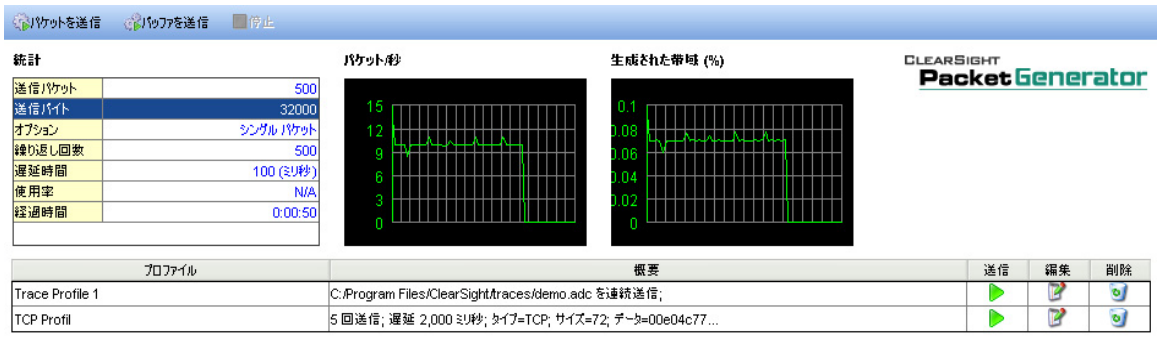


図 13-1: ClearSight パケットジェネレータユーザインタフェース

統計テーブル

統計テーブルは、パケット生成の進捗状況を示し、制御パラメータの一部を一覧表示します。ユーザは、[パケットを送信] ダイアログボックスおよび [バッファを送信] ダイアログボックスでこれらのパラメータを指定します。これらのダイアログボックスについては、この後で説明します。

統計テーブルのフィールドは以下のとおりです。

[送信パケット] このパケット生成セッションを開始してから送信されたパケット数

[送信バイト] このパケット生成セッションを開始してから送信されたバイト数

[オプション] 最初は **[N/A]** が表示されます。**[送信パケット]** オプションを選択した場合は **[シングルパケット]** が表示され、**[送信バイト]** オプションを選択した場合は トレースファイルのフルパスとファイル名が表示されます。

[繰り返し回数] **[送信パケット]** オプションを選択した場合は、このフィールドに送信するパケット数が表示されます。**[送信バイト]** オプションを選択した場合は、このフィールドにトレースファイルを送信する回数が表示されます。継続的なトラフィックの送信を選択した場合は、このフィールドに **[連続]** が表示されます。

[遅延時間] 遅延時間を指定した場合は、各パケットの終了から開始までの間隔 (ミリ秒) が表示されます。指定しない場合は、**[N/A]** が表示されます。

注記 : [遅延時間] と **[使用率]** は、**[送信パケット]** オプションにのみ適用され、どちらかが表示されます。一方には値が表示され、もう一方には **[N/A]** が表示されます。**[送信バイト]** オプションの場合は、両方とも **[N/A]** が表示されます。

[使用率] ネットワーク使用率値を指定した場合は、パケットジェネレータで使用される利用可能なネットワーク帯域幅のパーセントが表示されます。指定しない場合は、**[N/A]** が表示されます。

[経過時間] このパケット生成セッションを開始してからの時間 (時 : 分 : 秒)。

トラフィックグラフ

トラフィックグラフは、パケット生成の進捗状況をリアルタイムで表示します。左の **[パケット / 秒]** グラフは、パケットジェネレータで送信される秒ごとのパケット数を示し、右の **[生成された帯域]** グラフは、パケットジェネレータで使用される帯域幅を所定のネットワーク帯域幅のパーセントで示します。

[トラフィック制御] ボタン

[トラフィック制御] ボタンの機能は以下のとおりです。



[パケットを送信] ダイアログボックスを開きます。



[バッファを送信] ダイアログボックスを開きます。



現在のパケット生成セッションを停止します。

[パケットを送信] ダイアログボックス

[パケットを送信] ダイアログボックス (図 13-2) は、**[シングルパケット]** モードの送信を制御します。これを使用して、送信するパケットのタイプを指定し、さまざまなパラメータを設定して送信を制御できます。

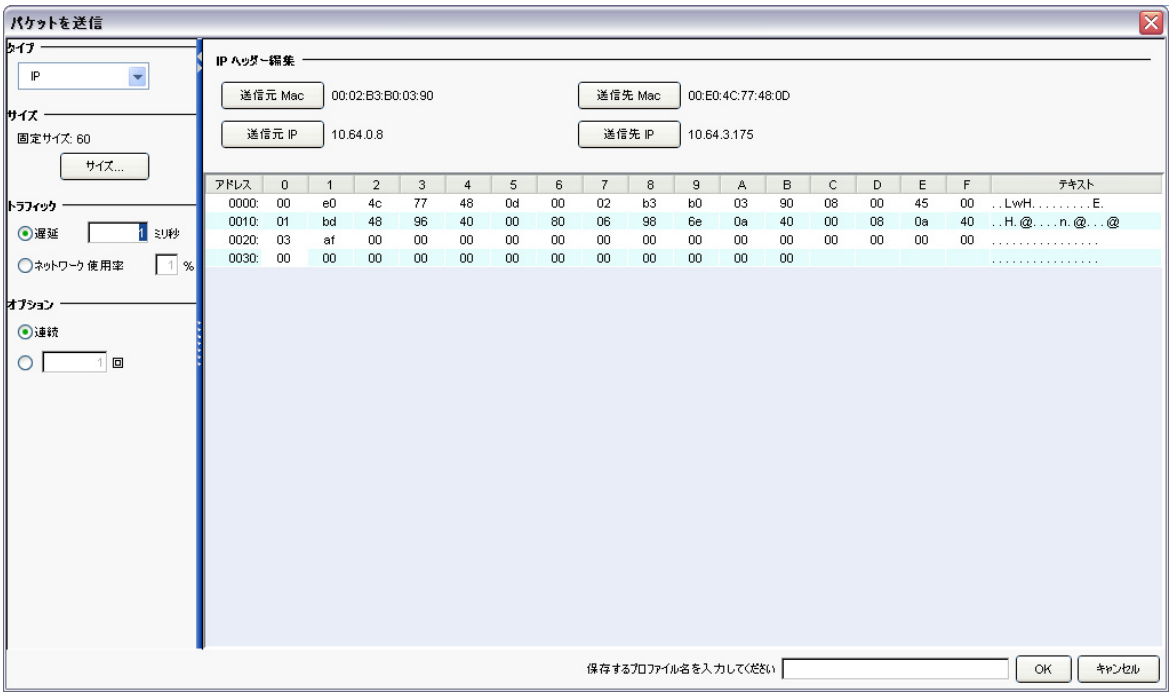


図 13-2: [パケットを送信] ダイアログボックス

以下の段落では、このダイアログボックスの各ペインの項目を設定する方法について説明します。

[タイプ]

[タイプ] ペインを使用して、IP、TCP、UDP、ICMP、IPv6、TCPv6、UDPv6、ICMPv6、またはカスタムからパケットタイプを選択できます。このドロップダウンリストから選択したものは、[サイズ] ペイン、[ヘッダ編集] ペイン、および [Hex] ペインの内容に影響します。

[サイズ]

[サイズ] ペインを使用して、送信するパケットのサイズを指定できます。カスタムタイプを除き、**[固定サイズ]** のデフォルト値は、選択した特定のパケットタイプを送信できる最小のパケットです。たとえば、TCP パケットの場合、デフォルト値のサイズは、CRC を含まない 72 バイトです。カスタムパケットタイプの場合、デフォルト値のサイズは、パケットタイプに関係なく指定した最新の固定サイズになります。

[サイズ] ボタンをクリックすると、[サイズ] ダイアログボックス (図 13-3) が表示されます。



図 13-3: [サイズ] ダイアログボックス

固定サイズパケットを希望する場合は、**[固定]** ラジオボタンをクリックして、CRC を含まないバイト数を入力し、**[OK]** をクリックします。このパケットタイプの最小バイト数よりも小さい値を入力した場合、または 1514 よりも大きい値を入力した場合、エラーメッセージが表示されます。

ランダム長パケットを送信するパケットジェネレータを使用する場合は、**[ランダム]** ラジオボタンをクリックして最小値と最大値を入力し、**[OK]** をクリックします。このパケットタイプの最小バイト数よりも小さい **[最小]** 値を入力した場合、または 1514 よりも大きい **[最大]** 値を入力した場合、エラーメッセージが表示されます。

以下の表に、さまざまなパケットタイプの最小パケットサイズと最大パケットサイズを示します。

パケットタイプ	最小サイズ	最大サイズ
IP, UDP, ICMP	60 バイト	1514 バイト
TCP, IPv6, ICMPv6	72 バイト	1514 バイト
UDPv6	80 バイト	1514 バイト
TCPv6	92 バイト	1514 バイト

[トラフィック]

[トラフィック] ペインを使用して、ネットワークに送信するパケットの頻度を制御できます。制御可能な方法は 2 つあります。

- **[遅延]** ラジオボタンをクリックして、各パケットの終了から次のパケットの開始までに挿入する遅延時間 (ミリ秒) を入力します。許容可能な範囲は、1 ミリ秒 から 1,000,000 ミリ秒 (1000 秒) です。
- **[ネットワーク使用率]** ラジオボタンをクリックして、パケットジェネレータで使用する利用可能なネットワーク帯域幅のパーセントを入力します。許容可能な範囲は、1% から 100% です。

[オプション]

[オプション] ペインを使用して、パケットを送信する回数を制御できます。

- パケットを定義された回数送信するには、**[回数]** ラジオボタンをクリックして、希望する反復回数を入力します。許容可能な範囲は、1 から 1,000,000,000 です。
- **[連続]** ラジオボタンをクリックすると、**[停止]** ボタンをクリックするまで、パケットジェネレータはパケットを継続的に送信します。

[ヘッダ編集]

[ヘッダ編集] ペインを使用すると、送信するパケットの送信元と送信先の MAC アドレスおよび送信元と送信先の IP(または IPv6) アドレスを簡単な方法で編集できます。TCP、UDP、TCPv6、および

UDPv6 パケットの場合、アプリケーションポート番号を簡単な方法で編集できます。

MAC アドレス、IP アドレス、またはポート番号のいずれを編集する場合も、処理は同じです。例のように、TCP パケットの送信元の IP アドレスを編集する場合、**[送信元 IP]** をクリックすると、[IPv4 編集] ダイアログボックス (図 13-4) が表示されます。



図 13-4: [IPv4 編集] ダイアログボックス

全てのパケットに同じアドレスを設定する場合、**[範囲]** ボタンをクリックして、**[開始アドレス]** ボックスにそのアドレスを入力し、**[カウント]** フィールドを **1** に設定します。また、各連続パケットに対してアドレスを 1 増分させることもできます。その場合、**[カウント]** フィールドに使用する連続アドレス数を入力します。たとえば、**[開始アドレス]** が 10.64.0.8 で、**[カウント]** を 8 に設定した場合、アドレスは、値 10.64.0.8、10.64.0.9、...10.64.0.15 のように増分されます。その後、アドレスは 10.64.0.8 に戻り、繰り返されます。最も右の列で 255 を超える値が **[カウント]** に設定された場合、最も右から 2 番目の列が 1 増分されて最も右の列が 0 になり、引き続き最も右の列が 1 増分されていきます。

[カウント] フィールドの許容可能な範囲は、1 から 65536 です。
[開始ポート] フィールドの許容可能な範囲は、0 から 65536 です。

パケットジェネレータでランダム IP アドレスを使用する場合、**[ランダム]** ボタンをクリックします。

[Hex]

[Hex] ペインを使用すると、パケットの実際の内容を手動で編集できます。パケットを編集する 16 進数を単に入力します。カーソルキーを使用して、この 16 進数の配列内にカーソルを移動します。カスタム以外のパケットタイプの場合、CRC が自動的に再計算されます。

注記 : カスタムパケットタイプを選択した場合、これらの 16 進数のいずれも自由に編集できます。他のタイプを選択した場合、実際にそのパケットタイプを定義する全てのフィールドを変更してはなりません。IP タイプでは、たとえば、位置 001D を 08 以外のものに変更すると、IP パケットではなくなります。

プロファイルの保存

全ての編集を行った後、これらの設定を再入力することなく将来使用できるように、プロファイルとして保存できます。設定を保存するには、**[保存するプロファイル名の入力]** ボックスにプロファイル名 (1 ～ 40 文字) を単に入力し、**[OK]** をクリックします。保存したプロファイルの管理の詳細については、423 ページの「プロファイルリスト」を参照してください。

[バッファを送信] ダイアログボックス

[バッファを送信] ダイアログボックス (図 13-6) は、トレースファイルの送信を制御します。これを使用して、送信するトレースファイルを指定し、さまざまなパラメータを設定して送信を制御できます。

[バッファを送信] ダイアログボックスを表示するには、図 13-5 に示すように、[開く] ダイアログボックに使用するトレースファイルを指定する必要があります。

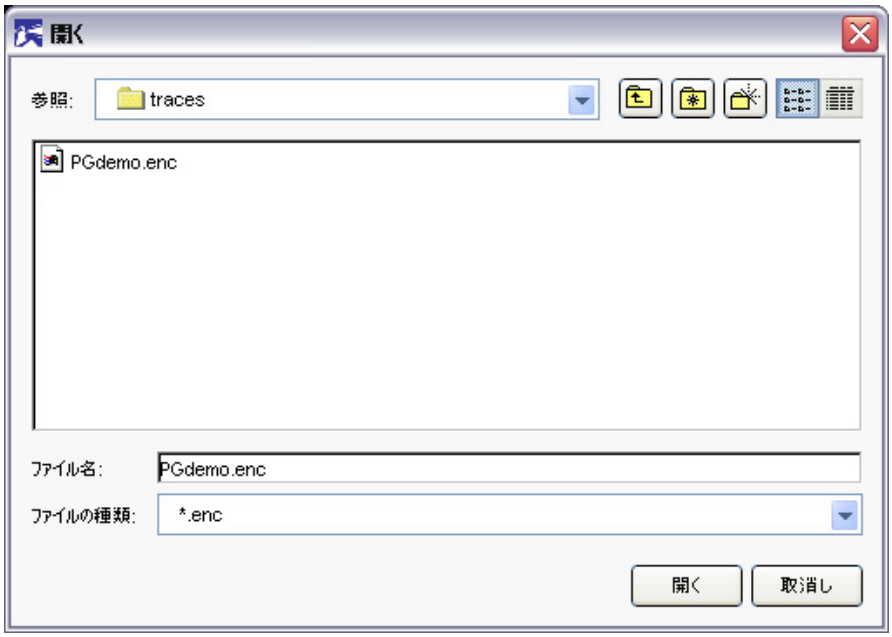


図 13-5: 送信するトレースファイルの指定

[開く] をクリックすると、[バッファを送信] ダイアログボックス (図 13-6) が表示されます。

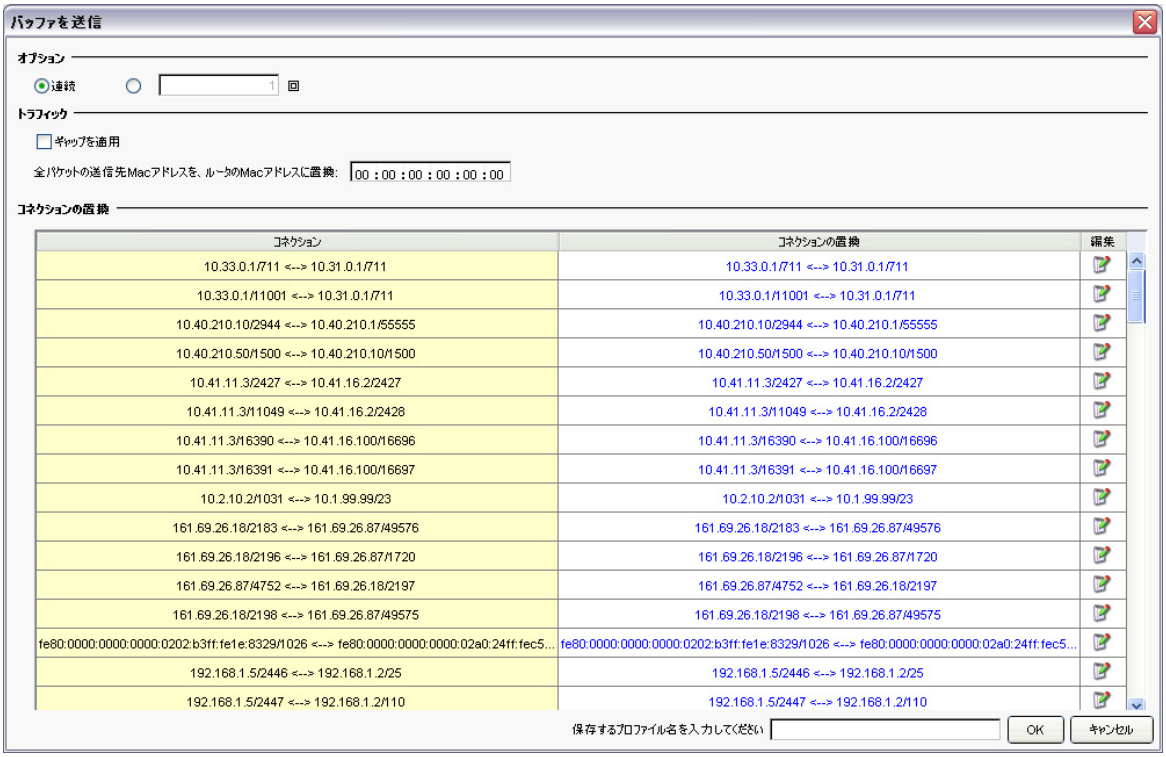


図 13-6: [バッファを送信] ダイアログボックス

以下の段落では、このダイアログボックの各ペインのコントロールを設定する方法について説明します。

[オプション]

[オプション] ペインを使用して、トレースファイルを送信する回数を制御できます。

- トレースファイルを定義された回数送信するには、**[回数]** ラジオボタンをクリックして、希望する反復回数を入力します。許容可能な範囲は、1 から 1,000,000,000 です。
- **[連続]** ラジオボタンをクリックすると、**[停止]** ボタンをクリックするまで、パケットジェネレータはトレースファイルを繰り返し送信します。

[トラフィック]

[トラフィック] ペインは、各パケットの終了から次のパケットの開始までの時間間隔を制御します。

- **[ギャップを適用]** ボックスをチェックすると、パケットジェネレータはトレースファイルに保存された最初の遅延時間を再現しようとします。Microsoft OS タイマの最小精度が 1 ミリ秒であるため、この遅延時間が正確に再現されないことがあります。また、遅延時間は、同時に実行中の他のアプリケーションの影響を受けることもあります。パフォーマンスを最適化するには、アクティブな他の全てのプログラムを閉じます。
- **[ギャップを適用]** ボックスをチェックしないと、パケットジェネレータはパケット間隔を約 1 ミリ秒にします。

また、[トラフィック] ペインを使用して、ローカルネットワークセグメントのルータの MAC アドレスを指定できます。ルータアドレスを指定すると、ローカルネットワークセグメントを超えてパケットを送信できます。

このアドレスを 00:00:00:00:00:00 にすると、送信先 MAC アドレスが変更されません。

[コネクションの置換]

トレースファイルのオープン後、[コネクションの置換] ペインに既知の全ての接続が一覧表示されます。トレースファイル内のパケットをそのまま送信することも、接続アドレスと接続ポートを変更して送信することもできます。これらのパラメータを指定した接続で置換するには、その接続の右側の [編集] 記号をクリックします。これによって、図 13-7 に示す、[コネクションの置換] ダイアログボックスが表示されます。



図 13-7: [コネクションの置換] ダイアログボックス

各アドレス (送信元または送信先) の場合、アドレスを置換しないことも、指定した別のアドレスで置換することも、またパケットジェネレータでランダムアドレスを使用することも選択できます。

同様に、各ポート番号の場合、ポート番号を置換しないことも、指定した別の番号で置換することも、またパケットジェネレータでランダムポート番号を使用することも選択できます。ポート番号を指定する場合、ポート番号 (0 ～ 65536) を入力するか、ドロップダウンリストから既知のアプリケーションポート番号を選択するかいずれかを行います。

プロファイルの保存

全ての編集を行った後、これらの設定を再入力することなく将来使用できるように、プロファイルとして保存できます。設定を保存するには、**[保存するプロファイル名の入力]** ボックスにプロファイル名 (1 ～ 40 文字) を単に入力し、**[OK]** をクリックします。保存したプロファイルの管理の詳細については、423 ページの「プロファイルリスト」を参照してください。

プロファイルリスト

プリファイルリストは、保存されたプロファイルを表示します。プロファイルは、[パケットを送信] ダイアログボックスまたは [バッファを送信] ダイアログボックスで入力された設定の集まりです。「プロファイルリストを表示するパケットジェネレータのメイン画面」では、パケットジェネレータのメイン画面の下部にプロファイルリストが表示されます。

プロファイルリストの各列には以下の項目が表示されます。

[プロファイル] プロファイルに指定した名前

[概要] 設定のショートリスト

[送信] このボックスをクリックすると、このプロファイルに基づいたトラフィックが送信されます。

[編集] このボックスをクリックすると、このプロファイルが編集されます。

[削除] このボックスをクリックすると、プロファイルリストからこのプロファイルが削除されます。

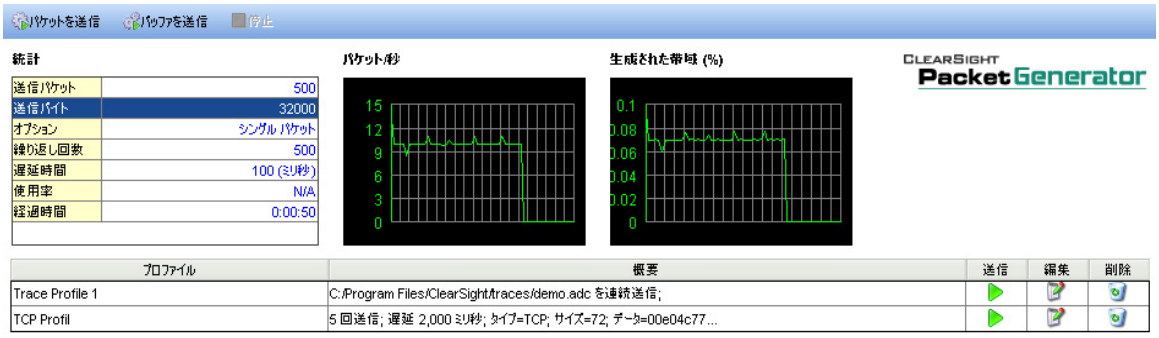


図 13-8: プロファイルリストを表示するパケットジェネレータのメイン画面

第 14 章

ClearSight Apex へのリンク

ClearSight Apex は、バージョン 6.6 から CSA のアドオンとして提供されるライセンスオプションです。

この章では、CSA から ClearSight Apex 製品にリンクする方法について説明します。

ClearSight Apex の詳しい説明については、『ClearSight Apex User Guide』を参照してください。

ClearSight Apex の機能

ClearSight Apex を使用すると、ClearSight のユーザは、ClearSight 製品がモニタしているネットワークで検出可能な問題と事象をさらに詳しく理解することができます。

CSA が問題または事象を検出した場合、Apex オプションを有効にしているユーザは、そのアイテムを右クリックすると、問題や事象の説明、および考えられる原因と推奨するアクションを提供するナレッジベースにアクセスすることができ、状況の改善に役立てることができます。

リンクの場所

CSA 内には、問題および事象のリストが数多く存在します。図 14-1 に示すように、問題のリストで、個々の問題を右クリックできます。**[Apex 解析]** を選択すると、その問題に関するエキスパート情報を提供するナレッジベース項目に即時にジャンプできます。



図 14-1: 問題のリストからのナレッジベースの呼び出し

図 14-2 に示すように、事象のリストでも、個々の事象を右クリックできます。**[Apex 解析]** を選択すると、現在のナレッジベース内でその事象に関連するエキスパート情報が利用可能な場合は、該当するナレッジベース項目に即時にジャンプできます。その事象の情報が利用できない場合は、ナレッジベースのトップレベルにジャンプします。



図 14-2: 事象のリストからのナレッジベースの呼び出し

ラダー図で事象や問題がハイライト表示されたときも、ナレッジベースにジャンプできます。図 14-3 に示すように、ハイライト表示された事象を右クリックし、**[Apex 解析]** を選択します。現在のナレッジベース内でその事象に関連するエキスパート情報が利用可能な場合は、該当するナレッジベース項目に即時にジャンプできます。事象や問題の情報が利用できない場合は、ナレッジベースのトップレベルにジャンプします。



図 14-3: ラダー図からのナレッジベースの呼び出し

第 15 章

ClearSight Networks へのエラーレポートの送信

この章では、ClearSight Analyzer そのものの誤動作時に、ClearSight ネットワーク社へエラーレポートを送信できる機能について説明します。

エラーレポート機能の基本操作

このエラーレポート機能は、ClearSight Analyzer(CSA) が例外を検出したり異常なシャットダウンを行ったりする場合に起動されます。

この機能を使用して、ClearSight ネットワークテクニカルサポートにこのようなエラー状況を報告できます。関連ログファイルとトレースファイルを送信できます。ClearSight ネットワークテクニカルサポートでは、問題を解決するためにこれらを検討した後、ユーザに連絡を取ります。

このタイプのエラーが発生すると、次回 CSA が起動された時に、図 15-1 に示す [エラーレポートオプション] ダイアログボックスが表示されます。



図 15-1: [エラーレポートオプション] ダイアログボックス

CSA でトレースファイル、ログファイルまたは両方を送信する必要があるかどうかを選択できます。ただし、図 15-4 の下の説明のように、最初にデバッグキャプチャを有効にしていない場合、CSA はトレースファイルを送信できません。

ClearSight ネットワークが連絡を取れるように、連絡先情報を必ず入力します。

下部にある 3 つのボタンの 1 つを選択できます。各ボタンの選択結果は以下のとおりです。

- **[無視]** この送信をキャンセルし、設定を保存しません。
- **[送信しない]** 選択項目と連絡先情報は保存しますが、レポートは実際に送信しません。
- **[エラーレポート送信]** 選択項目と連絡先情報を保存し、ClearSight ネットワーク社にレポートを送信します。**[ログファ**

イル送信] をチェックすると、CSA は **C:¥Program Files¥Clearsight¥log** ディレクトリ内のログファイルを全て送信します。**[トレースファイル送信]** をチェックすると、以下の説明のように、デバッグキャプチャが有効になっている場合、CSA は **C:¥Program Files¥Clearsight¥log** ディレクトリ内に保存されているトレースファイルを送信します。

[エラーレポート送信] を選択する場合は、インターネットに接続している必要があります。

[エラーレポート送信] を選択すると、通常、レポート処理が開始され、図 15-2 に示す進捗状況バーが表示されます。



図 15-2: デバッグ情報の進捗状況バー

何らかの理由でレポートを正常に送信できない場合は、図 15-3 に示すエラーメッセージが表示されます。



図 15-3: デバッグ情報のエラーメッセージ

レポートの送信後、または **[送信しない]** を選択した場合、[デバッグキャプチャを有効にする] ダイアログボックス (図 15-4) が表示されます。その後、デバッグキャプチャバッファサイズ (8 MB または 64 MB) を選択できます。**[デバッグキャプチャを有効にする]** ボックスをチェックしている場合、CSA は、クラッシュがまた起こった場合に使用するために最新のモニタ内容を保存します。デバッグ

キャプチャバッファの内容は、**C:¥Program Files¥Clearsight¥log** ディレクトリ内にトレースファイルとして保存されます。

たとえば、8 MB を選択すると、常にキャプチャした最新の 8 MB のパケットがデバッグキャプチャバッファに存在するようになります。例外が発生した場合、デバッグキャプチャは停止され、デバッグキャプチャバッファの内容が Debnnn.adc 形式 (nnn はランダムに割り当てられた番号) の特別なトレースファイルに書き込まれます。このトレースファイルには、例外を起こした可能性のあるパケットを含む、CSA でモニタした最新の 8 MB のトラフィックが含まれます。

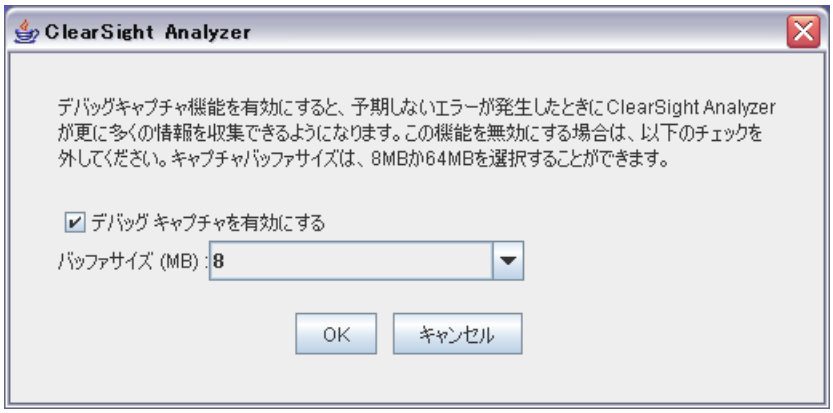


図 15-4: [デバッグキャプチャを有効にする] ダイアログボックス

デバッグキャプチャを有効にした後 CSA を終了すると、デバッグキャプチャが有効になっているが有効にしておくかどうかという、デバッグキャプチャ確認メッセージ (図 15-5) が表示されます。

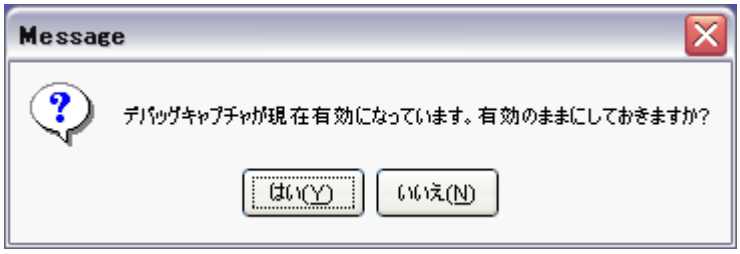


図 15-5: デバッグキャプチャ確認

CSA でデバッグキャプチャ処理を続行し、次回も CSA を起動する場合は **[はい]** をクリックします。起動しない場合は、**[いいえ]** をクリックします。

付録 A

特殊なネットワークカードの設定

この付録では、オプションの ClearSight ネットワークカード用の接続方法を説明します。

- ギガビット XD イーサネットカードの設定
- 10 ギガビットイーサネットカードの設定

また、**[設定]** ボタン > **[設定]** タブ > **[アダプタ設定]** 画面に含まれる、これらのアダプタに関する特殊な設定オプションについても説明します。

注記 : [アダプタ設定] ページは、ClearSight で 10/100 全二重イーサネットカード、またはギガビットイーサネットカードをモニタしている場合にのみ表示されます。

ギガビット XD イーサネットカードの設定

このカードを使用する場合は、**[設定]** ボタン > **[設定]** タブ > **[アダプタ設定]** > **[ギガビット XD]** 画面で、以下のオプションを設定する必要があります。

- **[モード]** オプションで、ギガビット XD イーサネットアダプタカードをネットワークに接続する方法を指定します (435 ページ)。
- **[物理コネクション]** オプションで、使用する特定のタイプのハードウェアポートデバイスを指定します (436 ページ)。

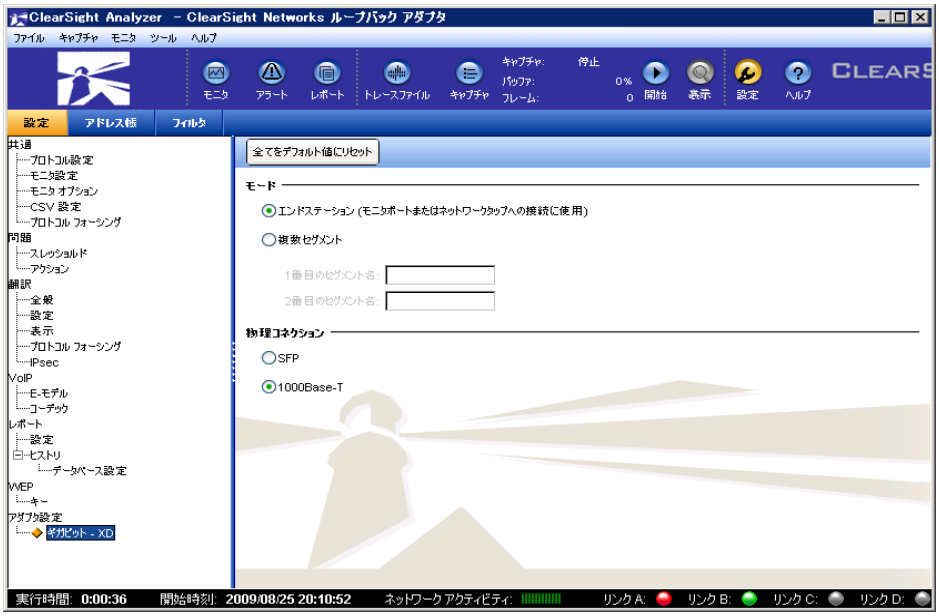


図 A-1: ギガビット XD イーサネットカードのアダプタ設定

[モード] オプション

[モード] オプションで、ギガビット XD イーサネットカードをネットワークに接続する方法を指定します。以下のオプションを選択できます。

エンドステーション

[エンドステーション] オプションを使用します。

- スイッチ上のモニタポートに接続する場合は、ケーブルを 1 本使用します。スイッチにビルドインされた設定ソフトウェアを使用して、ポートミラーリンクを設定し、ギガビット XD イーサネットカードが接続されているポートにトラフィックが送られるようにします。
- ネットワークタップに接続する場合は、ケーブルを 2 本使用します。

[複数セグメント] オプション

複数セグメント解析 (詳細は 263 ページの「複数セグメント解析」を参照) で使用するために、ギガビット XD イーサネットカードの 2 つのポートが 2 つの独立したネットワークセグメントに接続されている場合は、**[複数セグメント]** オプションを使用します。**[最初のセグメント名]** ボックスと **[二番目のセグメント名]** ボックスにセグメントの名前を入力します。

ギガビットイーサネットカードの 2 つのポートを異なった 2 つのスイッチ上の SPAN ポートに接続する場合も、**[複数セグメント]** オプションを使用できます。

スイッチにビルドインされた設定ソフトウェアを使用してポートミラーリングを設定し、ギガビット XD イーサネットカードが接続されているポートにトラフィックが送られるようにします。

[物理コネクション] オプション

[物理コネクション] オプションを使用して、使用する物理ポートデバイスを指定します。

- **SFP** - 次の 2 種類の SFP (Small Form Pluggable) 光ファイバコネクタのいずれか
  - シングルモード光ファイバ
  - マルチモード光ファイバ
- **1000Base-T** - カードに組み込まれているイーサネットポートを使用した、150 オームツイストペア銅線による 10/100/ ギガビットイーサネット接続。

10 ギガビットイーサネットカードの設定

このカードを使用する場合は、**[設定] ボタン > [設定] タブ > [アダプタ設定] > [ギガビット - 10G]** 画面で、以下のオプションを設定する必要があります。

- **[モード]** オプションで、10G NT20X イーサネットアダプタカードをネットワークに接続する方法を指定します (438 ページ)。
- **[キャプチャモード]** オプションで 10G NT20X イーサネットカードが **[ストリーミング]** モードでアナライザのキャプチャバッファ上にキャプチャするか、**[ワイヤスピード]** モードでカードのオンボードバッファ上にキャプチャするかを指定します (439 ページ)。

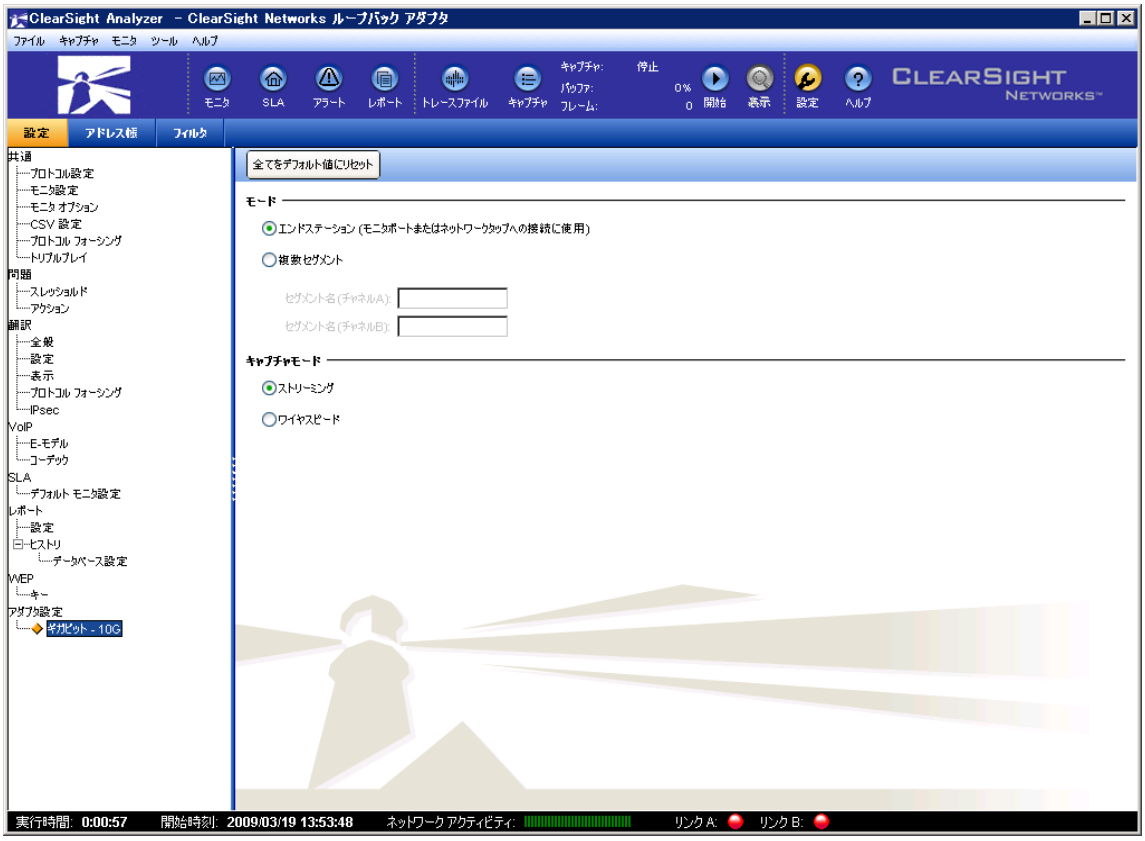


図 A-2: 10 ギガビットイーサネットカードのアダプタ設定

[モード] オプション

[モード] オプションで、10G NT20X イーサネットカードをネットワークに接続する方法を指定します。以下のオプションを選択できます。

エンドステーション

[エンドステーション] オプションは、スイッチのモニタリングポートまたはネットワークタップへ接続するときに使用します。

[複数セグメント] オプション

複数セグメント解析 (詳細は 263 ページの「複数セグメント解析」 を参照) で使用するために、10 ギガビットイーサネットカードの 2 つのポートが 2 つの独立したネットワークセグメントに接続されている場合は、**[複数セグメント]** オプションを使用します。**[最初のセグメント名]** および **[二番目のセグメント名]** ボックスにセグメント名を入力します。

10 ギガビットイーサネットカードの 2 つのポートを異なった 2 つのスイッチ上の SPAN ポートに接続する場合も、**[複数セグメント]** オプションを使用できます。

スイッチにビルドインされた設定ソフトウェアを使用してポートミラーリングを設定し、10 ギガビットイーサネットカードが接続されているポートにトラフィックが送られるようにします。

[キャプチャモード] オプション

10 ギガビットイーサネットカードがネットワークからデータをキャプチャする方法を指定するには、**[キャプチャモード]** オプションを使用します。

- **ストリーミング** — **[ストリーミング]** モードでは、キャプチャの進行に伴い、データはカードからアナライザバッファにリアルタイムで転送されます。
- **ワイヤスピード** — **[ワイヤスピード]** モードでは、キャプチャされたデータは 10 ギガビットイーサネットカードのオンボードバッファに格納されます。キャプチャが停止されると、データはカードのバッファからアナライザのバッファに自動的に転送され、ポストキャプチャアナリシスで使用できるようになります。
- 10 ギガビットイーサネットカードでは、**[ワイヤスピード]** モードにおいてもデータキャプチャ中の使用率データを表示できます。

リアルタイムの統計値を表示するには、**[ストリーミング]** モードを使用します。さまざまな回線速度でバッファフルデータをキャプチャするには、**[ワイヤスピード]** モードを使用します。キャプチャのパフォーマンスは、**[ワイヤスピード]** モードを選択した場合の方が高くなります。

索引

数字

10 ギガビットイーサネットカード
    [コネクションモード] オプション　438
3G-324M
    ビデオの再生　245
3G-324M フレーム
    翻訳　244
[3rd Party] 翻訳エンジンオプション (翻訳設定)　247

A

Apex
    製品　425
    リンク方法　426

C

Citrix しきい値　348
ClearSight
    アプリケーション層のモニタ　121
    アンインストール　42
    お問い合わせ先　20
    機能　60, 410
    システム要件　24
    接続　46
    ネットワーク層のモニタ　170
    ポストキャプチャアナリシス　225
    用語　118
    リアルタイムモニタインターフェイス　112
ClearSight Distributed エージェント　84
    接続　55
    マネージャ　84
ClearSight Distributed システム　84
ClearSight Server サービス　86
ClearSight カーネル　86
[ClearSight] タブ
    ポストキャプチャアナリシス　226
ClearSight のアンインストール　42, 43
[ClearSight ビュー] オプション　217

[ClearSight] 翻訳エンジンオプション (翻訳設定) 247

D

Distributed エージェント
切断 98
DLC
しきい値 371
レポート 398
[DLC 概要]
レポート 398
DNS
しきい値 345
フィルタ 288
レポート 383

E

Ethernet OAM フレーム 242
Exchange
レポート 393

F

FTP
しきい値 346
フィルタ 290
レポート 384

H

H.323
しきい値 355
フィルタ 299
[Hex] ペイン ([翻訳] タブ) 240
HTTP
子フローオプション 196
しきい値 349
フィルタ 292
レポート 386

I

IP
しきい値 368
フィルタ 320
[IP QOS アナリシス] オプション (翻訳設定) 249
IPsec
翻訳 259
IPTV
しきい値 365
フィルター 314
レポート 392
IPv6
しきい値 370
[IP 応答時間分布]
レポート 397
[IP 会話情報]
レポート 396
IP サブネットフィルタ 318
[IP プロトコル分布]
レポート 397
[IP ホスト]
レポート 397
ISAKMP
しきい値 366
フィルタ 309
レポート 393

J

jumbo frames 196

K

Kerberos
しきい値 366

フィルタ　310
レポート　392

L

LAN セグメント 1　56
LAN セグメント 2　56

M

MAC アドレス
フィルタ　325
[MDI DF 値] しきい値
IPTV　365
[MDI MLR] しきい値
IPTV　365
Megaco
しきい値　360
フィルタ　307
MGCP
しきい値　359
フィルタ　305
[MOS] しきい値
RTP　361
[MOS (日本仕様)] しきい値
RTP　362
MS SQL
フローのエラーの表示　148
レポート　388
MSN
MSN メッセージの表示　153
しきい値　354
フィルタ　298
レポート　394

N

[NAT] タブ　276

O

Oracle
トランザクションの再構成　149
フローのエラーの表示　151
Oracle SQL
レポート　389

P

[Ping ストーム] しきい値
IP　368
POP
しきい値　351
電子メールの表示　142
フィルタ　294
レポート　387

R

RAM 要件　29
RTP
しきい値　361
詳細画面　161
ストリームの再生　161
[RTP ジッタ] しきい値
RTP　361
RTSP
しきい値　363
フィルタ　312
レポート　395

S

SIP
しきい値　357
フィルタ　301
Skinny
しきい値　358
フィルタ　303

SMB
しきい値　367
フィルタ　315
レポート　394
SMTP
電子メールの表示　144
フィルタ　296
レポート　387
SNMP アクション　342
[SNMP] オプション　342
SPAN
を使用した ClearSight の接続　52
SSL を介した Java RMI　86
[SYN ストーム] しきい値
IP　368

T

TCP
フィルタ　322
Telnet
レポート　385
Telnet しきい値　348

U

UDP
フィルタ　324

V

[VLAN]
レポート　398
[VLAN] タブ
物理層　185
Voice
フィルタ　301, 303, 305, 307
VoIP
結合フロー　264, 266
コールの再生　157
レポート　390
ビデオの再生　159
[VQFactor] しきい値
IPTV　365

W

Windows セキュリティマネージャ　109

あ

アクション
SNMP　342
アラートの重要度に関連付け　335
スクリプト　340
定義　335
電子メール　336
ポケベル　338
リストの表示　343
[アクセス権限なし] しきい値
DNS　345
FTP　346
SMTP　353
[アダプタを開く] ダイアログボックス　57, 98
[アドミッション拒否] しきい値
H.323　355
アドレス
切り替え　127
アドレス帳
説明　373
の使用　374
アプリケーション層
説明　119
フィルタ　287
モニタ　121
レポート　382
アプリケーションのモニタ
説明　121

[アプリケーション分布]
レポート 397
アプリケーションモニタ
概要画面 112
詳細画面 122, 133
アラート
アクション 335
色付け 117
事象 330
[事象] タブ 332
重要度 334
スレッショルド 344
説明 330
表示の操作 330
問題 330
[問題] タブ 333
アラートマネージャ 84, 86
[アラートマネージャ] タブ 102, 103

い

色
ClearSight 画面 117
とアラートレベル 117
インターフェイスのペイン 114

え

[エージェントの追加] ダイアログボックス 56
エージェントビューアとエージェントの通信 55
エージェントマネージャ 91
エージェントリスト 56
エージェントへの接続 97
[エラー] しきい値
Kerberos 366
MSN 354

お

[応答時間 (ミリ秒)] しきい値
Citrix 348
DNS 345
FTP 346
HTTP 349
ISAKMP 366
Kerberos 366
MSN 354
POP 351
RTSP 363
SMB 367
SMTP 353
Telnet 348
[遅い TCP コネクション (ミリ秒)] しきい値
IP 368
[遅い応答 (ミリ秒)] しきい値
IP 368
お問い合わせ先 20
オペレーティングシステム要件 29
音声
コールの再生 157

か

外部アプリケーションの起動 247
[解放拒否] しきい値
H.323 356
[概要] タブ
ネットワーク層 171
物理層 184
[概要] ペイン ([翻訳] タブ) 237
[会話] タブ 131
カスタマサービス 20
カスタムプロトコル、追加 191
[関連ページに移動] ボタン 233

き

ギガビットイーサネットカード
[モード] オプションの接続　435
規則、表記　19
キャプチャ
観察　223
説明　206
ツールバーのコントロール　207
ワークスペース　207
[統計] タブ　210
キャプチャフレームの表示　225
[許可がありません] しきい値
POP　351
[許可されないファイル名] しきい値
FTP　347
切り替え
アドレス表示　127
[禁止されたアクセス] しきい値
HTTP　349

く

[クエリー拒否] しきい値
DNS　345
[クライアント エラー] しきい値
Megaco　360
SIP　357
[グローバル エラー] しきい値
SIP　357

け

形式
トレースファイル　261
[ゲートキーパー拒否] しきい値
H.323　355
結合フロー
VoIP　264, 266
VoIP 以外　268

こ

[更新間隔] オプション　201
[高物理エラーレート (/ 秒)] しきい値
DLC　371
コール
再生　157
[コール setup 時間 (マイクロ秒)] しきい値
H.323　355
Megaco　360
MGCP　359
SIP　357
Skinny　358
[コール失敗] しきい値
H.323　355
Megaco　360
MGCP　359
SIP　357
Skinny　358
[コネクション]
レポート　396
[コネクション] タブ
ネットワーク層　172
[コネクションモード] オプション
10 ギガビットイーサネットカード　438
このガイドの注意表記　20
このガイドの対象者　16
[コマンドの無効なパラメータ] しきい値
FTP　347

さ

[サーバー エラー] しきい値
SIP　357
[サーバー] しきい値
Kerberos　366
[サービス無効] しきい値

HTTP 350
[再送] しきい値
IP 368
最小システム要件 24
[最大同時ユーザ] しきい値
FTP 346
Telnet 348
[サイレント パケット ギャップ (ミリ秒)] しきい値
RTP 361
サフィックス 216
[サブネット] タブ
物理層 186
サポート 20

し

しきい値
Citrix 348
DLC 371
DNS 345
FTP 346
H.323 355
HTTP 349
IP 368
IPTV 365
IPv6 370
ISAKMP 366
Kerberos 366
Megaco 360
MGCP 359
MSN 354
POP 351
RTP 361
RTSP 363
SIP 357
Skinny 358
SMB 367
SMTP 353
Telnet 348
事象
説明 118
[事象] タブ
アラート 332
[事象] タブ (リアルタイムモニタ 画面) 129
システム要件 24
自動結合フィルタ 271
自動フィルタ 235, 279
キャプチャ 282
スマートナビゲーション 231
表示 283
自動保存 216
重要度
定義 334
[詳細画面を展開] オプション (翻訳設定) 254
[詳細] ペイン ([翻訳] タブ) 239
[使用率 (%)] しきい値
DLC 371
[使用率分布]
レポート 399

す

[スクリプト] オプション 340
ストリーム
再生 161
[全てのフレームを DOCSIS フレームとして処理] オプション (翻訳設定) 249
スマートナビゲーション 230
[翻訳] タブからの 233
スライス (フレームの) 215
[スライスサイズ] オプション 215
[スループット間隔] オプション 192

スレッショルド　344

せ

接続
　概要　46
　タップを使用　49
　とスイッチ　52
　ハブを使用　47
　ポートミラーリングの使用 (SPAN)　52
[接続] ボタン　97
[絶対時間] オプション (翻訳設定)　254
設定
　バッファサイズ　214
　[バッファの設定] タブ　211
　バッファフル時のアクション　214
　フレームスライス　215
　[翻訳設定]　246
[設定] オプション
　[コミュニティ]　104
　[セグメント]　104
　[送信先ホスト]　104

そ

[相対時間] オプション (翻訳設定)　254

た

[帯域拒否] しきい値
　H.323　355
[タイマーシミュレーションを有効にする] オプション (翻訳設定)　250
[タイムアウト] しきい値
　IP　368
タップ
　を使用した ClearSight の接続　49

ち

[チェック間隔] オプション　192
[チャート] タブ
　ネットワーク層　179
　物理層　188
[超過したストレージ割り当て] しきい値
　FTP　347
[重複した IP アドレス] しきい値
　IP　369

つ

通信カード　55
ツールバーのボタン　75

て

定義済みフィルタ　279, 284
[ディスク容量が不十分] しきい値
　FTP　347
[ディレクトリ] ボックス　216
[適合するメールボックス無し] しきい値
　POP　351
[テキストを EBCDIC で表示] オプション (翻訳設定)　254
テクニカルサポート　20
デフォルト
　パスワード　87
　ユーザ名　87
[デルタ時間] オプション (翻訳設定)　254
[電子メール] オプション　336
電話番号　20

と

[統計] タブ (キャプチャ)　210
統計ペイン　128
[登録解除拒否] しきい値

H.323 355
[登録拒否] しきい値
H.323 355
[トランシエント エラー] しきい値
MGCP 359
[トランスポートサマリのみ表示] オプション (翻訳設定) 254
[トリガ] タブによるキャプチャ 219
トレースファイル
形式 261
の使用 261
マージ 264
トレースファイルのマージ 264
[トレンドサンプル間隔] オプション (翻訳設定) 250
[トレンド情報を収集する] オプション (翻訳設定) 250
[ドロップフレーム] しきい値
IPTV 365
RTP 361

な

[内部エラー] しきい値
HTTP 350
ナビゲーション、スマート 230
[名前の解決] オプション (翻訳設定) 254

ね

[ネットワークアドレスの使用] オプション (翻訳設定) 254
[ネットワーク概要]
レポート 396
ネットワーク層
[概要] タブ 171
[コネクション] タブ 172
説明 119
[チャート] タブ 179
[ホスト] タブ 177
[マルチキャスト] タブ 180
モニタ 170
レポート 396

の

[ノード]
レポート 398
[ノード] タブ
物理層 187

は

[パーマネント エラー] しきい値
MGCP 359
[パケット長] オプション (翻訳設定) 254
パケットのキャプチャ
概要 80
パケットベースのフィルタ 281
パスワード
デフォルト 87
パターン
フィルタ 317
[バッファサイズ] オプション 214
[バッファの設定] タブ (設定) 211
[バッファフル時のアクション] オプション 214
ハブ
を使用した ClearSight の接続 47
範囲指定
1 から 216

ひ

[非常に遅い応答 (ミリ秒)] しきい値

IP 368
[ヒストリレポーター] 401
ビデオ
再生 159
表記規則 19

ふ

フィルタ
DNS 288
FTP 290
H.323 299
HTTP 292
IP 320
IP サブネット 318
ISAKMP 309
Kerberos 310
MAC アドレス 325
Megaco 307
MGCP 305
MSN 298
POP 294
RTSP 312
SIP 301
Skinny 303
SMB 315
SMTP 296
TCP 322
UDP 324
Voice 301, 303, 305, 307
アプリケーション層 287
作成 284
自動 235
自動結合 271
自動と定義済み 279
説明 279
パケットベースとフローベース 281
パターン 317
物理層 326
フロー 316
プロトコル 319
リスト 328
フィルター
IPTV 314
[フィルタ] タブ (設定) 284
フィルタリスト 328
[フェーズ 1 失敗] しきい値
ISAKMP 366
[無応答ホスト (再送)] しきい値
IP 368
複数 - セグメント解析 263
複数 - セグメントのモニタ
リアルタイム 278
[複数 - ティア] タブ 275
[不正なコマンド シーケンス] しきい値
FTP 347
[不正なコマンド] しきい値
FTP 346
[不正な順序] しきい値
IPTV 365
RTP 361
[不正なパスワード] しきい値
POP 351
[不正なパラメータ] しきい値
FTP 346
[不正なリクエスト] しきい値
HTTP 349
[不正なログイン] しきい値
Telnet 348
物理層
[VLAN] タブ 185
[概要] タブ 184
説明 119
[チャート] タブ 188
[ノード] タブ 187
フィルタ 326

モニタ　183
[不明なページタイプ] しきい値
FTP　347
プリフィックス　216
フレーム
検索　241
フレームスライス　215
フレームの検索 ([翻訳] タブ)　241
フロー
説明　118
フィルタ　316
[ブロードキャスト ストーム (/ 秒)] しきい値
DLC　371
フローの結合
自動　271
手動　276
フローベースのフィルタ　281
プロセッサ要件　29
プロトコル
フィルタ　319
[プロトコル] オプション (翻訳設定)　254
プロトコル強制
翻訳　199, 256
プロトコルの設定　191
プロトコル翻訳　235

へ

[平均遅延時間 (秒)] しきい値
RTP　361
ペイン
[翻訳] タブの　237
[ページが見つからない] しきい値
HTTP　349

ほ

ポート
追加　191
[ポートスキャン (ソケット ポート番号)] しきい値
IP　369
ポートミラーリング
を使用した ClearSight の接続　52
[ポケベル] オプション　338
ポストキャプチャアナリシス　247, 225
[ClearSight] タブ　226
概要　80
スマートナビゲーション　230
タブ　229
[翻訳] タブ　235
ワークスペース　227
[ホスト] タブ
ネットワーク層　177
[ホスト名] フィールド　56
翻訳
IPsec　259
プロトコル強制　199, 256
[翻訳設定] (設定)　246
[翻訳] タブ
[Hex] ペイン　240
[概要] ペイン　237
からのスマートナビゲーション　233
[詳細] ペイン　239
設定オプション　246
フレームの検索　241
ペイン　237
ポストキャプチャアナリシス　235
[翻訳] タブ
Ethernet OAM フレーム　242

ま

[マルチキャスト ストーム (/ 秒)] しきい値
DLC 371
[マルチキャスト] タブ
ネットワーク層 180

み

[未解決の名前] しきい値
DNS 345
[未実装のコマンド] しきい値
FTP 346
[未認証] しきい値
HTTP 349

む

[無効なファイル] しきい値
FTP 346

め

[メール受信] しきい値
POP 351
[メールドロップがロックされました] しきい値
POP 352
[メールボックスをロックできない] しきい値
POP 352
[メッセージがない] しきい値
POP 351

も

[モード] オプションの接続
ギガビットイーサネットカード 435
モニタ
アプリケーション層 121
ユーザインターフェイス 112
モニタカード 55
問題
スレッショルド 344
説明 118
[問題] タブ
アラート表示 333
リアルタイムモニタ画面 130

ゆ

ユーザインターフェイス
概要 411, 73
ClearSight
ユーザインターフェイスの概要 411
ユーザ設定ユーティリティ 67, 88
ユーザ名
デフォルト 87
ユーザリスト 66, 69, 86, 89

よ

要件
ClearSight Distributed エージェントのみのシステム 30
ClearSight エージェントビューアおよびエージェントのシステム 26
ClearSight エージェントビューアのみのシステム 28
用語
ClearSight 118

り

リアルタイムモニタ
アプリケーション層 121
概要 79
ユーザインターフェイス 112
[リソースなし] しきい値
SMTP 353
リモート

デフォルトのユーザ名とパスワード　87
[リリース時間 (ミリ秒)] しきい値
Skinny　358

れ

レポート
DLC　398
[DLC 概要]　398
DNS　383
Exchange　393
FTP　384
HTTP　386
IPTV　392
[IP 応答時間分布]　397
[IP 会話情報]　396
[IP プロトコル分布]　397
[IP ホスト]　397
ISAKMP　393
Kerberos　392
MS SQL　388
MSN　394
Oracle SQL　389
POP　387
RTSP　395
SMB　394
SMTP　387
Telnet　385
[VLAN]　398
VoIP　390
アプリケーション層　382
[アプリケーション分布]　397
[コネクション]　396
[使用率分布]　399
説明　378
[ネットワーク概要]　396
ネットワーク層　396
[ノード]　398
ヒストリ　401
リアルタイムとポストキャプチャ　378
ワークスペース　379

ろ

[ローカル エラー発生] しきい値
FTP　347
[ロケーション拒否] しきい値
H.323　356