Colasoft®
Maximize Network Value

Capsa

Real-time Portable Network Analyzer

ユーザーガイド

(Enterprise Edition)

お問い合わせ

電話番号

090-7197-9436

Sales

sales.jp@colasoft.com

技術サポート

support.jp@colasoft.com

ウェブサイト

http://www.colasoft.com/jp/

目次

はじめに

ポータブルなネットワークアナライザ Colasoft Capsa を選択していただき、まことにありがとうございます。

企業の管理ソリューションとして、Colasoft Capsa はフォーチュン 500 並びに中小企業に信頼され、簡単かつ強力なネットワーク監視、解析、トラブルシューティングを提供します。よく設計された GUI を介して、鮮やかなグラフ、情報豊富な統計、リアルタイムなアラームを提供している Capsa を利用して、IT 管理者はリアルタイムに有線および無線ネットワーク問題を識別、診断、解決したり、ネットワークにおけるユーザーアクティビティを監視したりすることによって、ネットワーク通信の安全性を確保することができます。

Capsa について

パケットのデコードとネットワーク診断機能を持っている Colasoft Capsa はローカルホストとローカルネットワークで転送されるネットワークトラフィックを監視し、ネットワークトラブルシューティングに役立ちます。リアルタイムなパケットキャプチャーと正確なデータ解析能力を持っている Colasoft Capsa を利用して、迅速にネットワーク問題を特定し、効率的に隠されたセキュリティトラブルを解決することができます。

Colasoft Capsa を利用して、以下のタスクを簡単に実行することができます。

1. ネットワークトラフィック解析
2. ネットワーク通信監視
3. ネットワークトラブルシューティング
4. ネットワークセキュリティ解析
5. ネットワークパフォーマンス検出
6. ネットワークプロトコル解析

Colasoft Capsa は複数アダプタの監視をサポートし、異なるアダプタを介して、ネットワークを通過しているトラフィックを表示することができます。

強力な解析モジュールはネットワークトラフィックの詳細情報を提供し、ここで E メール情報、FTP 転送、HTTP リクエスト、DNS 解析、およびほかのログを確認することができます。

簡易フィルターと上級フィルターを利用して、ターゲットホストの統計量を絞り、迅速に不審なトラフィックに焦点を当て、ネットワークトラブルの問題を特定することができます。

統計やグラフなど様々な方法でネットワーク通信を表示することで、ネットワークに対する全体的且つ視覚的なイメージを与えます。

エキスパート診断はネットワーク診断イベントをリストし、考えられる原因と解決案を提供します。マトリックスではネットワークノード間のネットワークトラフィックが動的に表示されます。レポートでは全体ネットワーク、または特定のグループのリアルタイムな統計レポートが提供されます。

Packet Builder、 Packet Player、MAC Scanner、Ping Tool という四つのビルトインネットワークツールを利用して、監視中にパケットを作成、編集、送信し、パケットファイルをリプレイし、MAC アドレスをスキャンし、IP アドレスとドメインを Ping することができます。さらに外部の Windows アプリケーション、またはツールもカスタマイズされ、Capsa に追加されることができます。

柔軟且つ直感的なインターフェースは Colasoft Capsa の大きな特徴です。したがって、ユーザーは全体的な統計から特定のネットワークノードの詳細情報に簡単に切り替えることができます。新しいユーザーにとっても使い勝手のよい製品です。

Capsa は最低のレベルからアプリケーションレベルまで有線と無線ネットワークを解析することで、ネットワークにおけるすべての問題を見つけ出します。Colasoft Capsa は他のネットワーク管理ツールと協力して、ユーザーのネットワーク価値を最大限にします。

技術サポート

一般的な質問について、 Knowledge Base(英語)をご参照ください。

Capsa を利用しているうちに、このマニュアルや Colasoft ホームページにおける資料を参照しても解決できない問題がある場合、ローカルの代理店にお問い合わせするか、または Colasoft の技術サポートチームに連絡してください。

注意 技術サポートを取得するにはライセンスユーザーが優先されますが、無料ユーザーに対してもサポートを提供します。

1. ウェブサイトサポート

   最新 FAQ や専門用語のほかに、 http://www.colasoft.com/jp/には、Colasoft Capsa のバージョンアップグレード情報と相関する公開リソースがあります。

2. E メールサポート

   技術問題がございましたら、いつでも気軽に support.jp@colasoft.com にお問い合わせください。われわれは可能な限り早く返信します。E メールには製品のシリア

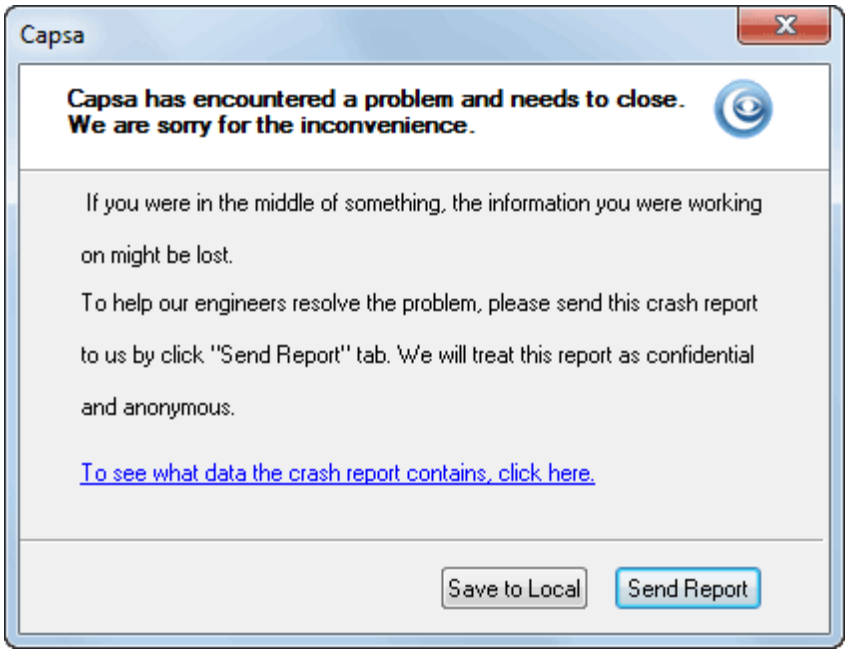
ル番号、製品のバージョンとエディション、オペレーティングシステムのバージョン、トラブルの詳細説明、および他の関連情報を記入する必要があります。

3. フォーラムサポート

   無料版製品を使用している大規模なユーザーを持っている colasoft は、それらのユーザーに対し、E メールを介する直接的なサポートを提供しません。無料版製品を使用している場合、サポートフォーラムで質問を投稿してください。ここで、他の無料版ユーザーから助けや支援をもらうことができます。さらにご提案を提出し、当社の製品について他のユーザーと議論することもできます。ぜひともサポートフォーラムに参加してください。

クラッシュレポート

プログラムがクラッシュする際、Capsa はトラブルの原因など重要な情報を含むダンプファイルを生成します。ダンプファイルを通じて、問題を特定し、製品を向上させることができます。「**クラッシュレポートを送信**」をクリックして、ダンプファイルを弊社に送信してください。インタネットに接続していない場合、**ローカルに保存**をクリックして、E メールを介してダンプファイルを弊社に送信してください。



エラー報告

クラッシュレポートメッセージボックスが表示されない場合、または他の問題を報告したい場合、以下の情報を含めて、E メールしてください。

1. この問題は再現可能ですか。もし可能であれば、どうやって再現しますか。
2. ご利用の Windows バージョン（Windows XP、Windows Vista、 および Windows 7 など）は何ですか。
3. お使いの Capsa のバージョンは何ですか（**製品**メニューにおける **Capsa について**をクリックして、バージョンを確認することができます）。レポートでは「バージョン：」の後につく全ての文字を記入する必要があります。

4. エラーメッセージを含むダイアログボックスが表示された場合、ダイアログボックスの全ての内容とタイトルバーのテキストをレポートに記入する必要があります。

ヒント プログラムを実行しているとき、F1 キーを押して、いつでも関連のヘルプ情報を取得することができます。

表記規則

このドキュメントには三つのタイプの表記規則があります。

アイコン

以下の表はこのドキュメントで使用されているアイコン規則について説明しています。

アイコン	説明
アドバイス	このアイコンはいくつかのアドバイス、提案、および推奨操作を提供します。
注意	このアイコンは注意を払う必要がある事項について、説明しています。
ヒント	このアイコンはより実用的なヒントを提供します。

フォントと符号

以下の表は、このドキュメントで使用されているフォントと符号の規則について説明しています。

アイテム	説明
太字	メニュー、ラベル、コマンド、タブ、およびプログラムインターフェースからのほかの要素
斜体	参照、相互参照、または専門用語集からの用語
>	ステップごとの手順。これらの手順に従って、タスクを完了することができます。

マウス操作

操作	説明
クリック	マウスを移動せずに、マウスの左ボタンを一度押すこと
右クリック	マウスを移動せずに、マウスの右ボタンを一度押すこと
ダブルクリック	マウスを移動せずに、マウスの左ボタンを素早く 2 回クリックすること
ドラッグ	マウスの左ボタンを押したまま、マウスを移動すること

エディション比較

以下の表は Capsa Enterprise と Capsa Professional の主な違いをリストしています。

重要な特徴	Capsa Enterprise	Capsa Professional
WiFi トラフィックをキャプチャー	有り	無し
ローカル IP ノード監視	無制限	無制限
セッションタイムアウト期間	無制限	無制限
最大パケットバッファサイズ	無制限	無制限
カスタムチャート	16	16
カスタムプロトコル	40	40
カスタムアラーム	40	40
複数プロジェクトを同時実行	有り	有り
パケットの自動保存機能	有り	有り
複数トレースファイルをリプレイ	有り	有り
ネットワークタップをサポート	有り	有り
印刷	有り	有り
ログ保存	有り	有り
複数アダプタをサポート	有り	有り
自動スケジューリング	有り	無し
アラームの E メール通知	有り	無し
レポート保存	有り	無し
エキスパート診断	有り	無し
セキュリティ解析プロファイル	有り	無し
レポートをカスタム	有り	無し
ARP 攻撃ビュー	有り	無し
ワームビュー	有り	無し
起こした DoS 攻撃ビュー	有り	無し
受けた DoS 攻撃ビュー	有り	無し
TCP ポートスキャンビュー	有り	無し
不審セッションビュー	有り	無し
VoIP 解析	有り	無し
上級表示フィルター	有り	無し
IMAP4E メールを解析	有り	無し

デプロイメントとインストール

この章では、Capsa を配備、インストール、アンインストール、アクティブ化する方法を紹介し、Capsa のシステム要件について説明しています。

デプロイメント環境

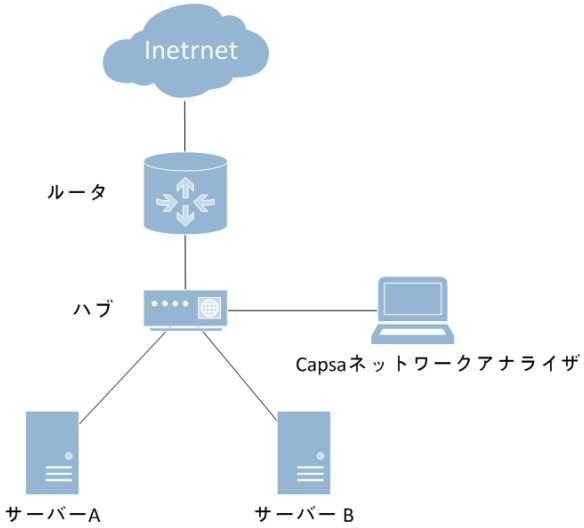
Colasoft Capsa はイントラネットパケット、インタネットからのパケット、さらに VLAN を通過しているパケットを監視し、解析する専門家です。一つの管理マシンにのみインストールされる必要があり、ほかのマシンにインストールされなくてもよいです。インストールするノードによって、キャプチャーされた全体のパケットが違うので、管理者は、需要によって Capsa をどのマシンにインストールかを決める必要があります。したがって、Capsa をセンタースイッチ設備にインストール、または接続するのがお勧めです。そうすると、Capsa はネットワーク全体のパケットをキャプチャーし、包括的な監視と解析を行います。当然、タップを利用して、任意ネットワークセグメントのパケットをキャプチャー、解析することができます。ここで Capsa が十分に監視、解析できるいくつかのデプロイメント環境を紹介します。

共有ネットワーク - ハブ

共有ネットワークは、ハブに接続された、ハブベースのネットワークとしても知られています。

ハブは、一般的に、LAN セグメントに接続するために使用されています。1 つのポートに、パケットが到着すると、そのパケットはその他のポートにコピーされます。すなわちすべての LAN セグメントは、すべてのパケットを見ることができます。パッジブハブは、単なるデータのコンジットとして機能し、データが 1 つのデバイス（またはセグメント）から別のデバイスに移動することを可能にします。いわゆるインテリジェントハブには、管理者がハブを通過するトラフィックをモニターし、ハブの各ポートを設定することができるという追加機能が含まれています。インテリジェントハブは、管理可能なハブとも呼ばれています。3 つ目のハブタイプは、スイッチングハブと呼ばれているもので、各パケットの宛先アドレスを読み取り、パケットを正しいポートに転送します。

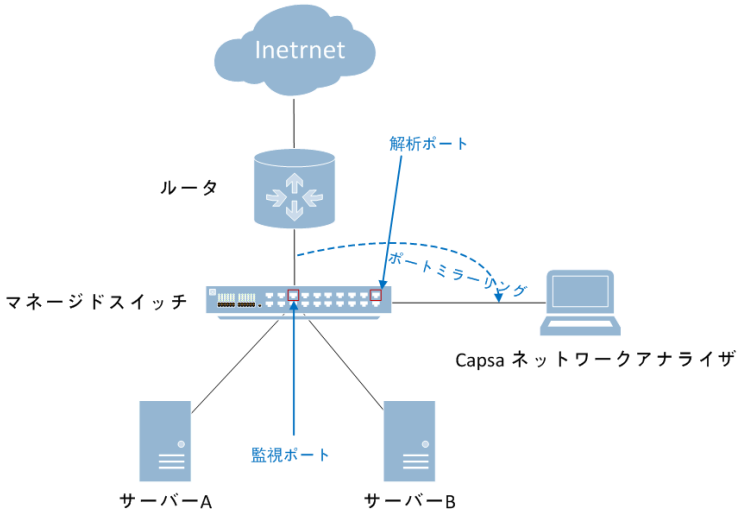
共有環境では、Colasoft Capsa は、LAN 内のホストならどれにでもインストールされることができます。LAN 内の任意の 2 つのホスト間の通信を含む、ハブを経由して伝送された、ネットワークデータ全体がキャプチャーされます。



スイッチドネットワーク - マネージドスイッチ（ポートミラーリング）

スイッチは、OSI のデータリンク層で動作している、ネットワークデバイスです。スイッチは、物理アドレスを習得し、それらのアドレスを自身の ARP テーブルに保存することができます。パケットがスイッチに送信されると、スイッチは、自身の ARP テーブルから、パケットの宛先アドレスを調べて、相当するポートにパケットを送信します。

通常、すべてのレイヤ 3 スイッチと、レイヤ 2 スイッチの一部には、ネットワーク管理能力が備わっています。スイッチのその他のポートを経由するトラフィックを、コアチップ上のデバッグポート（ミラーポート/スパンポート）からキャプチャーすることができます。すべてのポートを経由するトラフィックを 解析するには、Colasoft Capsa をこのデバックポート（ミラーポート/スパンポート）にインストールする必要があります。

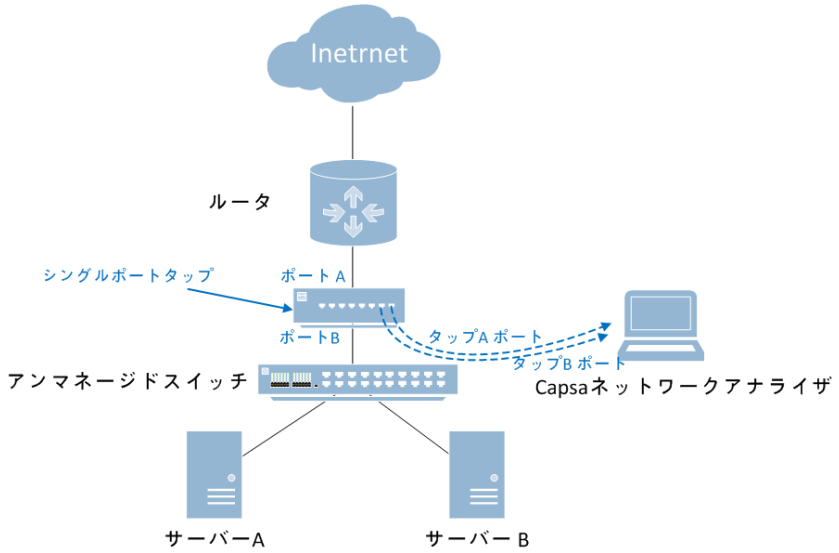


スイッチドネットワーク – アンマネージドスイッチ

ネットワーク管理機能を持っていないスイッチもあります。したがってミラーリングポートもありません。この場合、Colasoft Capsa をインストールし、ハブ、またはタップを利用してネットワークを監視、解析することができます。

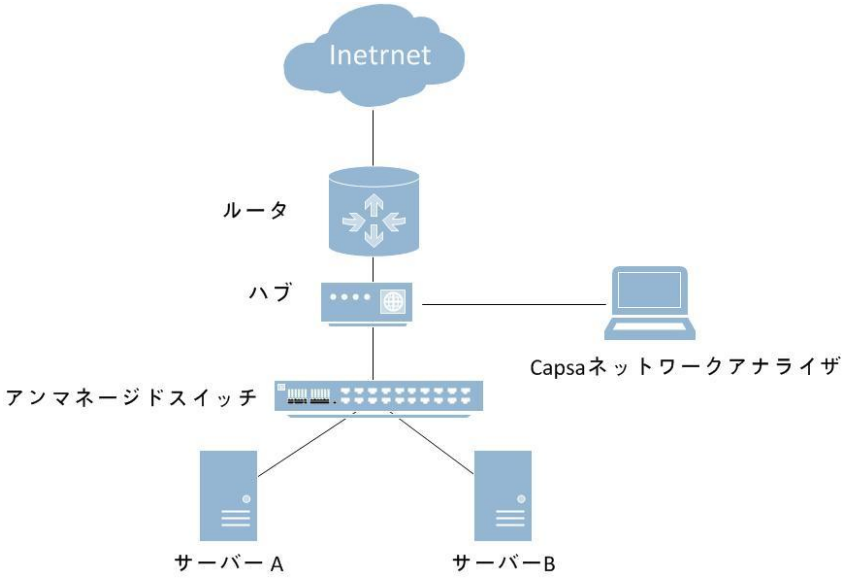
監視対象の回線にタップを接続する

タップは、ネットワーク内の回線ならどれにでも柔軟に設置することが可能です。ネットワークパフォーマンスの要件が非常に高い場合は、ネットワークにタップを追加することができます。



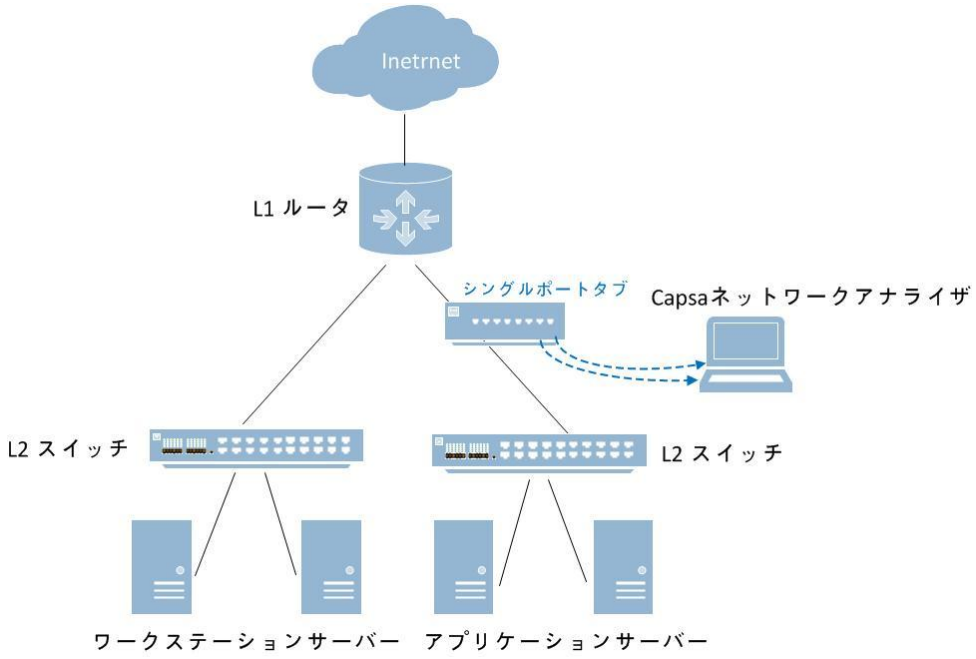
監視対象の回線にハブを接続する

ハブはタップよりコストが低いですが、大規模なトラフィックネットワークでは、タップのほうがよいパフォーマンスを持っています。



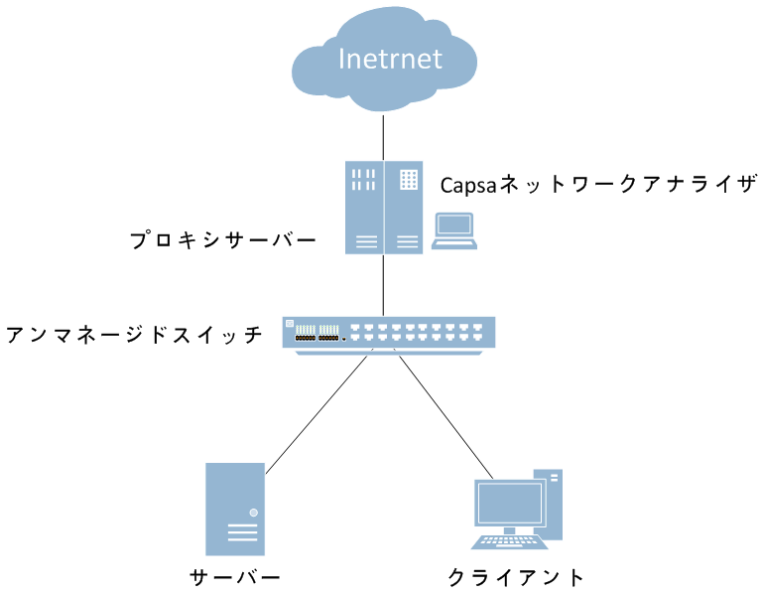
ネットワークセグメントを監視

あるネットワークセグメント（例：財務部、営業部など）内のトラフィックをモニターするだけでよい場合、Colasoft Capsa がインストールされているサーバーを、交換装置を装備した、このネットワークセグメントに接続することができます。交換装置として、ハブ、スイッチ、またはプロキシサーバーが考えられます。



プロキシサーバー

小規模なネットワークでは、プロキシサーバーはネットワークを配備する信頼性の高い選択です。この環境では、Colasoft Capsa をプロキシサーバーに直接にインストールすることができます。



ハブ、タップ 、およびスイッチの区別

	ハブ	スイッチ(ミラーポート)	タップ
利点	• 低コスト • 設定必要なし • 元のネットワークトポロジを変更必要なし	• 他の設備を追加必要なし • 元のネットワークトポロジを変更必要なし	• ネットワーク転送性能に影響なし • データフローと生データに影響なし • IP アドレスを占有しない、ネットワーク攻撃を受けない • 元のネットワークトポロジを変更必要なし
欠点	• 他の設備(ハブ)を追加する必要がある • 膨大なトラフィックの場合、ネットワーク転送性能に影響がある • 大規模なネットワークに適用しない	• スイッチポートを占有 • 膨大なトラフィックの場合、ネットワーク転送性能に影響する可能性がある	• 高コスト • 他の設備(タップ)を追加する必要がある • デュアルアダプタが必要 • インタネットに接続できない
まとめ	ハブは共有ネットワークで動作し、ネットワーク配備の初期に使用されている一般的な設備です。今は簡易スイッチに置き換えられています。ハブは、主に小規模なネットワークで使用されています。	マネージドスイッチは、管理者がネットワークを管理することを可能にするポートミラーリング機能を持っています。ポートミラーリングは 1 対 1、または 1 対すべてのポートという方式でミラーリングすることができ、現在の最も一般的な管理方法となります。	タップは柔軟的にネットワークの任意場所に配置することができます。大きなトラフィックにおいて、高コストが無視される場合、タップは妥当的な選択です。

ヒント スイッチやモデルによって、ポーロミラーリングを設定する方法も違います。よく使用されるスイッチポートミラーリングの設定方法について、スイッチとポートミラーリングをご参照ください。

スイッチとポートミラーリング

スイッチは、OSI 参照モデルのデータリンク層(レイヤ 2)、時にはネットワーク層(レイヤ 3)で動作しているネットワーク交換設備です。ワーキングプロトコルによって分類すると、レイヤ 2 スイッチ、レイヤ 3 スイッチ、レイヤ 4 スイッチ、およびマルチレイヤスイッチがあります。スイッチはマネージドスイッチとアンマネージドスイッチという二つに分けることもできます。一般的には、レイヤ 3 スイッチとレイヤ 3 以上のスイッチは管理機能(マネージドスイッチ)を持っています。

ハブと違い、スイッチはプロミスキャススニッフィングを防ぎます。スイッチドネットワーク環境では、Colasoft Capsa(または他のパケットアナライザ)はマシンが接続しているポー

トからのパケット、ブロードキャストパケット、マルチキャストパケットのキャプチャーに限られいます。

しかし、ほとんどの近代スイッチ(マネージドスイッチ)は、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では、ユーザーはスイッチを設定し、一部、またはすべてのポートで発生したトラフィックを指定されたスイッチの監視ポートにリダイレクトすることができます。この機能のおかげで、ユーザーはスイッチドネットワーク環境で全体の LAN セグメントを監視することができます。この機能と設定手順については、スイッチの使用説明書をご参照ください。

お使いのスイッチがポートミラーリングをサポートしない場合、インタネットゲートウェイとして同じハブに接続されたワークステーション、またはインターネットゲートウェイ(可能な場合)に Colasoft Capsa をインストールすることができます。そうすると、イントラネットとインタネット間のすべてネットワークトラフィックを監視することができます。Colasoft Capsa を配備する方法について、デプロイメント環境 をご参照ください。

一般的に使用されている一部のマネージドスイッチ(ポート監視/スパニングを持つ)のリストは、当社のウェブサイトで利用可能です。詳しいことは Switch Management(スイッチ管理) をご参照ください。

システム要件

Colasoft Capsa は、高性能マシンを必要とせず、64 ビット版の Windows Vista、 Windows 7、Windows 8/8.1、Windows 10 Professional など、様々な Windows オペレーションシステムにインストールすることができます。システムのパフォーマンスと配置は Colasoft Capsa の運行に影響があります。以下の最小要件は Colasoft Capsa を正常にインストールし、実行する最低限の要件です。ビジー状態、または大規模なネットワークの場合、お使いのシステムがよりよいパフォーマンスを持っていたほうがよいのです。

最小要件

- P4 2.8 GHz CPU
- 4 GB RAM
- Internet Explorer 6.0

推奨システム要件

- Intel Dual-Core 3.2 GHz CPU
- 8 GB RAM 以上
- Internet Explorer 8.0 以上

サポートしている Windows オペレーションシステム

- Windows Server 2008 (64-bit)*
- Windows Server 2012 (64-bit)**
- Windows Vista (64-bit)

- Windows 7(64-bit)
- Windows 8/8.1 (64-bit)
- Windows 10 Professional (64-bit)

* はワイヤレス解析モジュールがこのオペレーティングシステムと交換性がないことを示しています。

** は Colasoft Packet Builder がこのオペレーティングシステムと交換性がないことを示しています。

サポートしているワイヤレスネットワークアダプタ

Colasoft Capsa Enterprise は以下のワイヤレスネットワークアダプタをサポートしています。

- Atheros AR7015, AR6004, AR9380, AR9382, AR9390, AR9485, AR9462, AR958x
- Intel 1000, 4965, 5100, 5150, 5300, 5350, 6200, 6250, 6300, 6350, AC 7260, 82579LM
- Realtek RTL8188CU, RTL8192CU, RTL8187
- Broadcom 4313GN 802.11 b/g/n
- TP-Link TL-WDN3200(5.1.7.5014), TL-822N v2
- D-Link DWA-160 B2(5.1.7.5014)

注意 ワイヤレスネットワークアダプタでキャプチャーするのは Capsa Enterprise でのみ利用可能となります。

インストールとアンインストール

インストールする前に、

1. デプロイメント環境 を慎重に読んで、ネットワークトポロジが Colasoft Capsa の動作環境に適合するかどうかを確認してください。
2. システム要件 をよく読んで、お使いのマシンが最小システム要件を満たしていることを確認してください。
3. お使いのマシンで実行中のすべてのアプリケーションを終了してください。
4. Colasoft Capsa の古いバージョン、試用版をアンインストールしてください。

インストール

1. インストールファイルをダブルクリックすることで、**セットアップウィザード**が表示されます。**次へ**をクリックして、インストールを続行します。
2. 使用許諾契約書ページで、使用許諾契約書をよく読んで、Colasoft Capsa の使用に関する条件を確認します。インストールを続行するには、使用許諾契約書に同意する必要があります。
3. **次へ**をクリックすることで、**リリースノート**が書いている Capsa 情報ページが表示されます。製品のアップデートを確認します。
4. **次へ**をクリックすることで、インストール先を指定するページが表示されます。デフォルトでは、インストールディレクトリは C:¥Program Files (x86)¥Colasoft

Capsa9 Enterprise Edition となっています。**参照**をクリックして、他のディレクトリを指定することができます。ダイアログボックスの下の部分にはディスク空き領域の最低要求が表示されます。Capsa をインストールするスペースが十分かどうかを確認してください。

5. **次へ**をクリックすることで、**スタートメニューフォルダを選択する**ポップアップが表示されます。スタートメニューフォルダ名を指定します。**参照**をクリックして、他のスタートメニューフォルダを指定することができます。
6. **次へ**をクリックすることによって、**追加タスクを選択する**ページが表示されます。デフォルトでは**デスクトップアイコンを作成**と**クイックアイコンを作成**にチェックが入っています。アイコンを作成したくない場合、チェックを外せばよいのです。
7. **次へ**をクリックして、**インストール準備完了**ページが表示されます。インストール情報を確認して、すべての情報が正しい場合、**インストール**をクリックして、Colasoft Capsa をインストールします。また**戻る**をクリックして、インストール情報を変更することもできます。
8. インストール後、リードミーファイル情報が書いている**情報**ページが表示されます。リードミー情報を確認し、**次へ**をクリックします。
9. **セットアップ完了**ページがポップアップされます。**完了**をクリックして、インストールを終了します。**プログラムを起動する**にチェックを入れたら、Colasoft Capsa が起動されます。

ヒント デスクトップアイコンとクイックアイコンを作成するチェックボックスのデフォルト設定を変更しない場合、デスクトップと**クイック起動**にはアイコンが表示されます。

アンインストール

以下のいずれを実行して、Colasoft Capsa アンインストールダイアログボックスを開きます。

- Colasoft Capsa をアンインストールするには、**スタート > すべてのプログラム > Colasoft Capsa 9 > Uninstall Colasoft Capsa9** をクリックします。
- **コントロールパネル**を開く > **プログラムと機能**をクリックして、**プログラムのアンインストールまたは変更**ウィンドウが表示される> プログラムリストで Colasoft Capsa 9 を選択し、**アンインストール**をクリックします。

アンインストールダイアログボックスが表示されます。以下のステップに従い、Colasoft Capsa をアンインストールします。

1. Colasoft Capsa 9 とすべての関連コンポーネントを完全に削除したい場合、**はい**をクリックすることで、アンインストールを続行し、または**いいえ**をクリックすることで、アンインストールをキャンセルします。
2. ライセンス情報を削除したい場合、**はい**をクリックして、または**いいえ**をクリックして、ライセンス情報をお使いのマシンに残します。

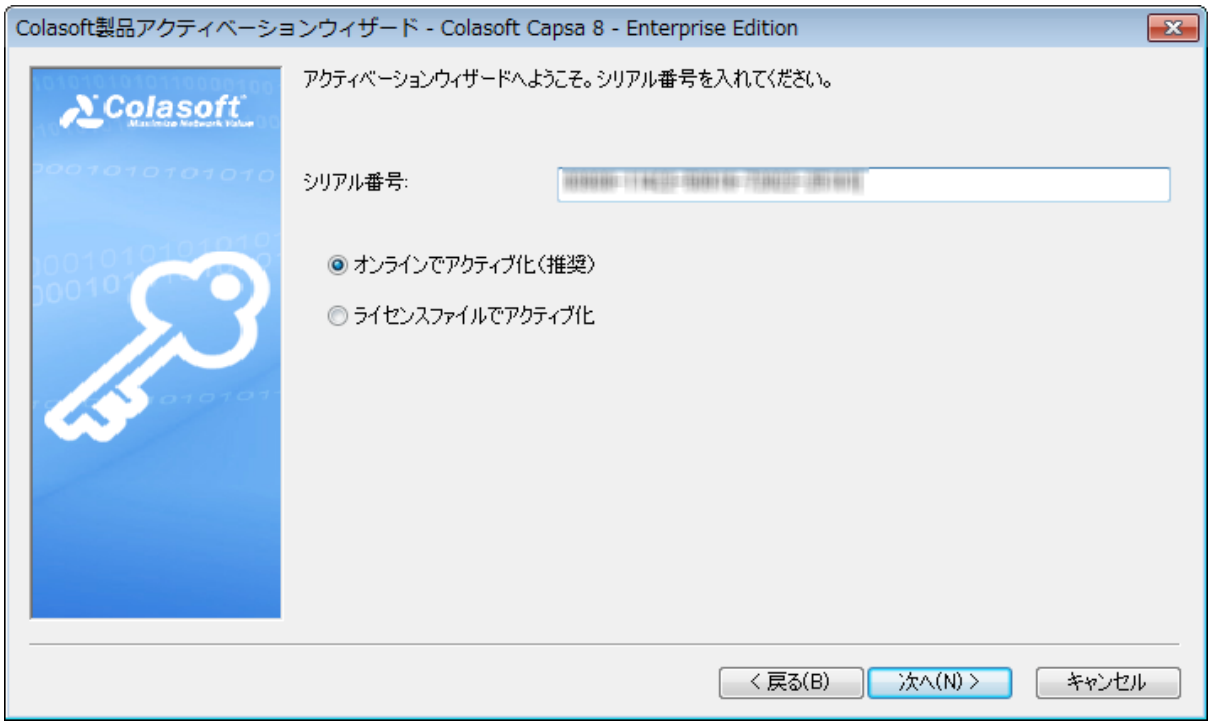
   アドバイス お使いのコンピューターに Colasoft Capsa を再びインストールしたい場合のために、**いいえ**をクリックして、ライセンス情報をお使いのマシンに残すことがお勧めです。

3. アンインストールを完了するために、はいをクリックして、お使いのコンピュータ

ーを再起動します。

製品アクティベーション

インストール後、アクティベーションウィザードが表示され、ステップごとにアクティベーションをガイドします。Colasoft Capsa をアクティブ化するには、**オンラインでアクティブ化**と**ライセンスファイルでアクティブ化**という二つの方法があります。

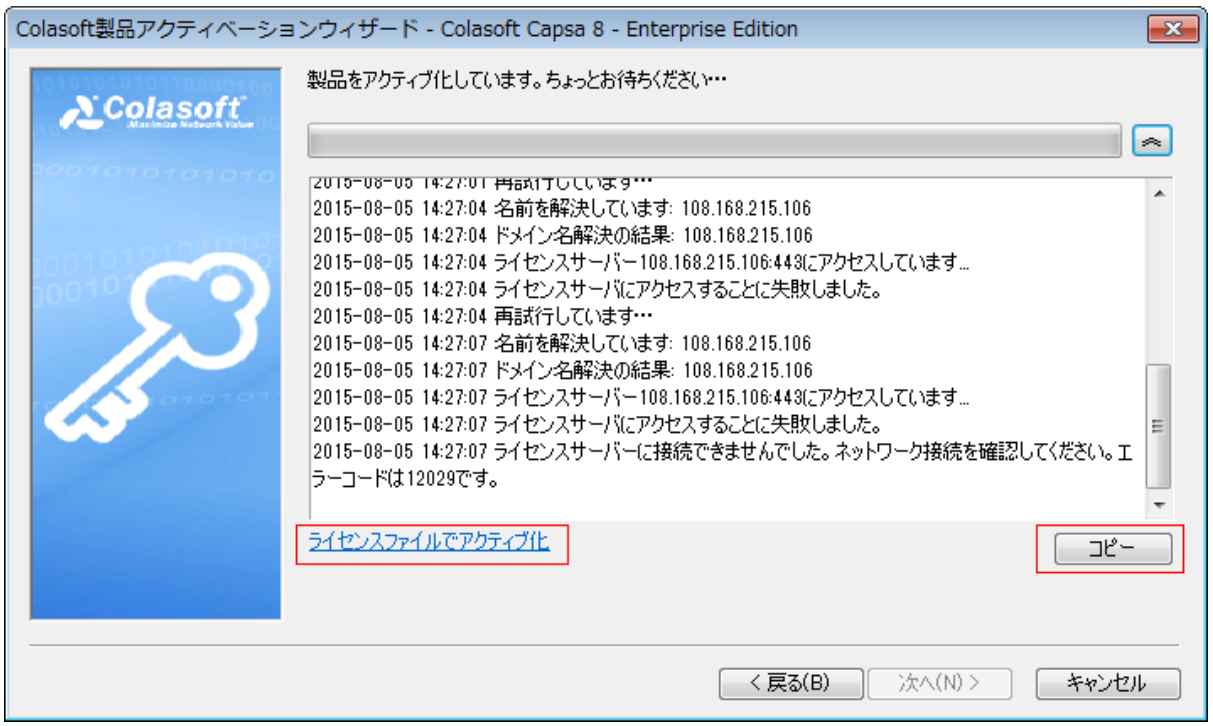


オンラインでアクティブ化

Capsa をオンラインでアクティブ化するには、単にシリアル番号を入力し、「次へ」をクリックして、アクティベーションを完了するだけです。この方法は、迅速かつ簡単で、数秒しかかかりません。

オンラインでアクティブ化に失敗した場合、

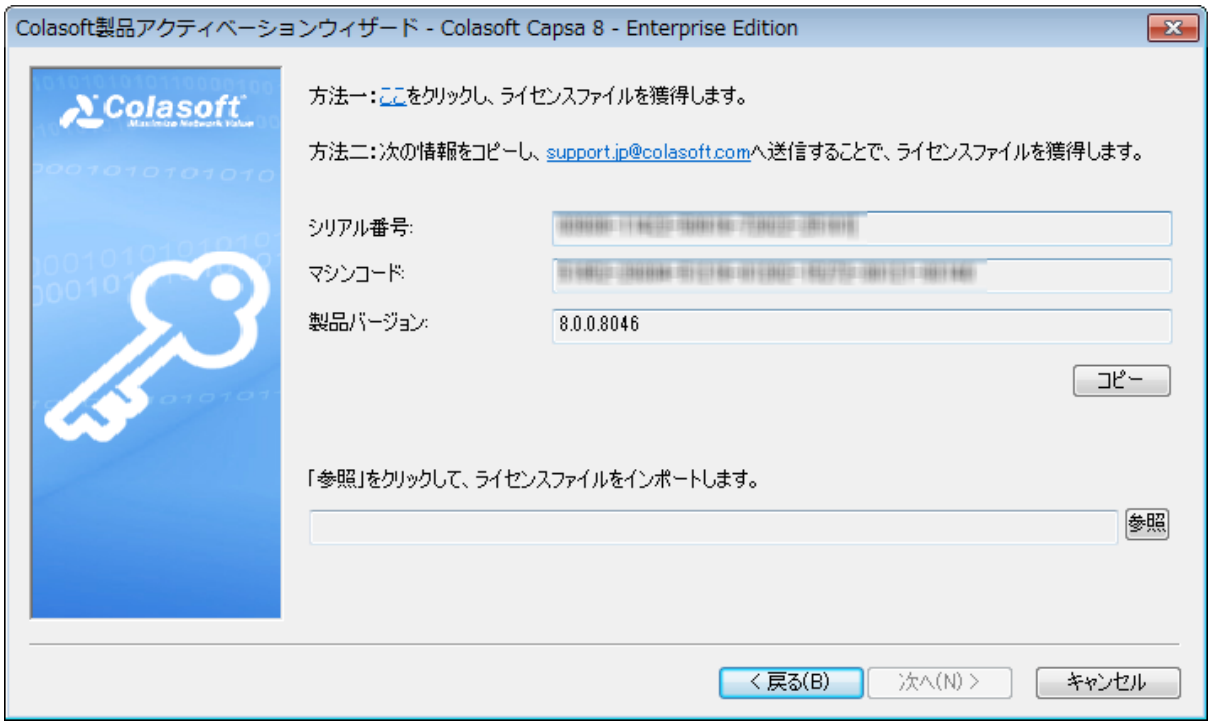
1. アクティベーション詳細を表示する、右側のアクティベーションプログレスバーの横にある二重矢印ボタンをクリックして、**コピー**をクリックします。



2. **ライセンスファイルでアクティブ化**をクリックすることによって、ライセンスファイルでプログラムをアクティブ化します。
3. コピーされた情報を support.jp@colasoft.com に送信します。

ライセンスファイルでアクティブ化

インタネットに接続していない場合、またはオンラインでアクティブ化に失敗した場合、この方法を選択して、Capsa をアクティブ化することができます。この方法を選択すると、下図のようにアクティベーションインターフェースが表示されます。



ライセンスファイルを取得するには、Colasoft ウェブページを介するか、Colasoft Support を介するかという 2 つの方法があります。

Colasoft ウェブページを介する

以下のステップに従い、Colasoft ウェブページを介して、ライセンスファイルを取得します。

1. アクティベーションインターフェースで、方法 1 のリンクをクリックすることによって、Colasoft アクティベーションウェブページがポップアップされます。

2. **Save as Bin** をクリックして、ライセンスファイルを保存します。
3. アクティベーションインターフェースで、ライセンスファイルをインポートして、**次へ**をクリックします。

Colasoft Support を介する

以下のステップに従い、Colasoft Support を介して、ライセンスファイルを取得します。

1. **コピー**ボタンをクリックします。アクティベーションウィザードがシリアル番号、マシンコード、製品バージョンをコピーします。オンラインでアクティブ化を実行した場合、オンラインアクティベーションログも一緒にコピーされます。
2. コピーされた情報を support.jp@colasoft.com に送信します。

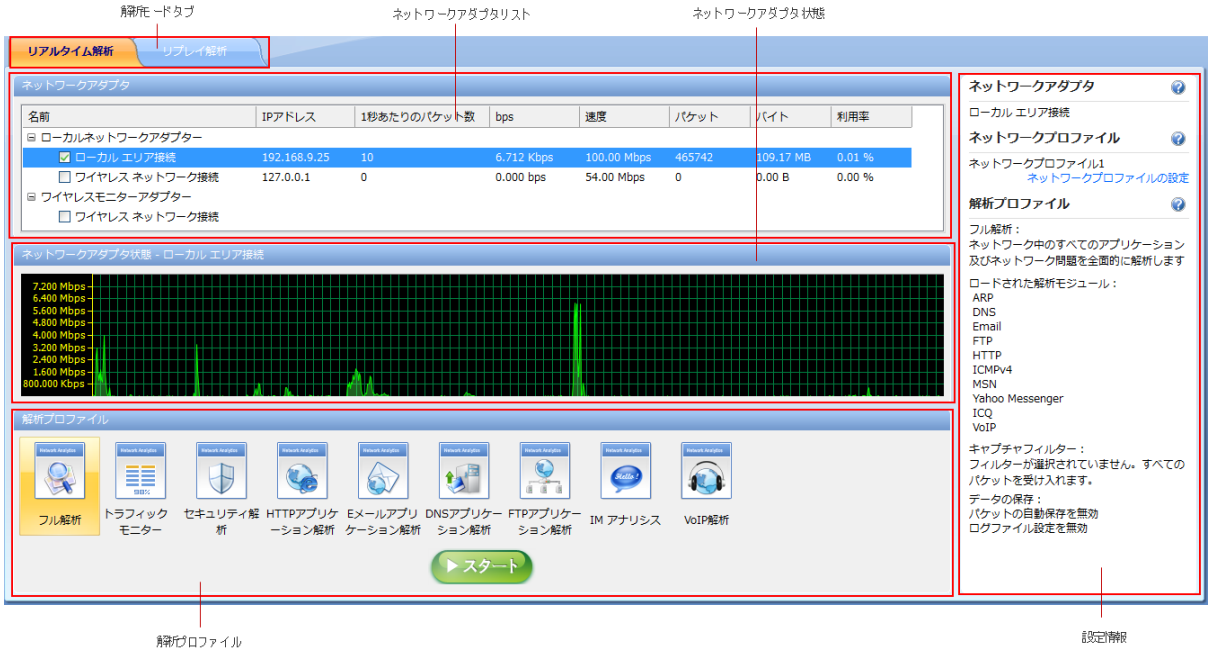
スタートアップ

アクティベーション後、ネットワークトラフィックをキャプチャーすることができます。詳しいことについては、以下のリンクをクリックしてください。

- スタートページ
- キャプチャーを開始
- ワイヤレスネットワークアダプタでキャプチャー
- キャプチャーされたパケットをリプレイ

スタートページ

スタートページは、プログラムを起動する祭に最初に表示される画面で、ステップごとに解析プロジェクトを開始するのをガイドします。



スタートページは以下の五つの部分から構成されています。

1. **解析モードタブ**:**リアルタイム解析タブ**と**リプレイ解析タブ**からなっていて、**リアルタイム解析タブ**はネットワークデータをリアルタイムにキャプチャーし、解析するのに使われています。**リプレイ解析タブ**はキャプチャーされたネットワークデータをリプレイするのに使われています。
2. **ネットワークアダプタリスト**:有線アダプタと無線アダプタを含め、すべての利用可能なネットワークアダプタをリストします。データはネットワークアダプタ（NIC と略して、ネットワークインターフェースカードとも呼ばれる）を介して、ネットワーク経由で転送されています。ネットワークアナライザはネットワークアダプタを介するデータをキャプチャーします。
3. **ネットワークアダプタ状態**:

- **ネットワークアダプタリスト**部分には有線ネットワークアダプタが選択された場合、この部分では、選択されたアダプタのリアルタイムなトラフィック状態を表示します。
- **ネットワークアダプタリスト**部分には無線ネットワークアダプタが選択された場合、これは無線 AP 状態部分となり、すべての利用可能な AP をリストします。

4. **解析プロファイル:**この部分では、すべての利用可能な解析プロファイル(詳しいことについて、解析プロファイルをご参照ください)をリストします。
5. **設定情報**:解析プロジェクトの設定情報を表示し、以下の部分が含まれています。
   - **ネットワークアダプタ**:ネットワーク**アダプタリスト**部分で選択されたアダプタを表示します。
   - **ネットワークプロファイル**:選択されたネットワークプロファイルを表示します。ネットワークプロファイルを編集、変更するには、右側にある**ネットワークプロファイルの設定**をクリックすればよいのです。詳しいことについては、ネットワークプロファイルをご参照ください。
   - **解析プロファイル**:ロードされた解析モジュール、キャプチャーフィルター、データの保存情報を含め、**解析プロファイル**部分で選択された解析プロファイルの詳細情報を表示します。

右側にあるをクリックして、関連するヒントと説明が表示されます。

キャプチャーを開始

この部分は主に有線ネットワークアダプタでキャプチャーを開始するステップについて説明しています。ワイヤレスネットワークアダプタでキャプチャーを開始する詳しい情報については、ワイヤレスネットワークアダプタでキャプチャーをご参照ください。パケットファイルをリプレイする詳しい情報については、キャプチャーされたパケットをリプレイをご参照ください。

迅速にライブネットワークデータキャプチャーを開始するには、ネットワークアダプタを選択し、スタートページにおける**スタート**ボタンをクリックすればよいです。

以下のステップに従い、ユーザー定義の設定でキャプチャーを開始します。

1. 解析モードタブでリアルタイム解析を選択します。
2. アダプタリスト部分でネットワークアダプタを選択します。選択されたアダプタのトラフィック状態がアダプタ状態部分で表示されます。一つ、または同時に複数の有線ネットワークアダプタを選択することができます。
3. 設定情報部分でネットワークプロファイルの設定をクリックして、ネットワークプロファイルを選択します。ネットワークプロファイルには、ノードグループ、ネームテーブル、およびアラームに関する設定が含まれています。
4. 解析プロファイル部分で、適切な解析プロファイルを選択します。解析プロファイ

ルには、解析モジュール、解析オブジェクト、診断、ビュー表示、パケットバッファ、パケットフィルター、パケット保存、及びログに関する設定が含まれています。Capsa はデフォルトでは九つの解析プロファイルを提供します。当然解析プロファイルを新規作成することもできます。

5. スタートページの下にあるスタートボタンをクリックして、解析プロジェクトを開始します。

ワイヤレスネットワークアダプタでキャプチャー

有線ネットワークアダプタでトラフィックデータをキャプチャーするほかに、Capsa はワイヤレスネットワークアダプタでパケットをキャプチャーすることもできます。以下のステップに従い、ワイヤレスネットワークアダプタでキャプチャーを開始します。

1. 解析モードタブでリアルタイム解析を選択します。
2. ネットワークアダプタリスト部分でワイヤレスネットワークアダプタを選択します。そうすると無線 AP 状態が表示され、すべての利用可能な AP がリストされます。
3. AP を選択します。選択された AP が暗号化された場合、キーを入力する必要があります。複数の AP を選択することができますが、これらの AP は同じチャンネルにある必要があります。
4. 設定情報部分でネットワークプロファイルの設定をクリックして、ネットワークプロファイルを選択します。ネットワークプロファイルには、ノードグループ、ネームテーブル、およびアラームに関する設定が含まれています。
5. 解析プロファイル部分で、適切な解析プロファイルを選択します。解析プロファイルには、解析モジュール、解析オブジェクト、診断、ビュー表示、パケットバッファ、パケットフィルター、パケット保存、及びログに関する設定が含まれています。Capsa はデフォルトでは九つの解析プロファイルを提供します。当然解析プロファイルを新規作成することもできます。
6. スタートページの下にあるスタートボタンをクリックして、解析プロジェクトを開始します。

注意

- ワイヤレスネットワークアダプタでキャプチャーするのは Capsa Enterprise の場合にのみ利用可能となります。Capsa Professional はこの機能を持っていません。
- ワイヤレスネットワークアダプタでパケットをキャプチャーするという機能は、Windows Vista 以上のバージョンの場合にのみ、利用可能となります。
- 入力された AP のキーが間違った場合、解析プロジェクトは実行されますが、パケットをデコードしません。
- 一つの解析プロジェクトは、一つのワイヤレスネットワークアダプタからのトラフィックデータだけをキャプチャーします。お使いのマシンに複数のワイヤレスネットワークアダプタがある場合、一つのワイヤレスネットワークアダプタに一つの解析プロジェクトで、複数の解析プロジェクトを作成する必要があります。
- 一つの解析プロジェクトは、複数の AP を同時に監視することができます。

アドバイス WiFi トラフィックをデコード、解析するには、以下のことをお勧めします。

- 監視された AP のパスワードが正しいことを確認してください。
- すべてのパケットをキャプチャーするために、無線ルーター（信号源）に十分近づくことがお勧めです。
- EAPOL ハンドシェイクパケットをキャプチャーするために、他のホストがネットワークにアクセスする前に、AP を監視します。

無線 AP 状態部分

ワイヤレスネットワークアダプタが選択されると、検出されたすべての AP が**無線 AP 状態**部分で AP 名、シグナルの強さ、キーが入力されているかどうか、プロトコルタイプ、AP チャンネル、MAC アドレス、および暗号化タイプによって、表示されます。

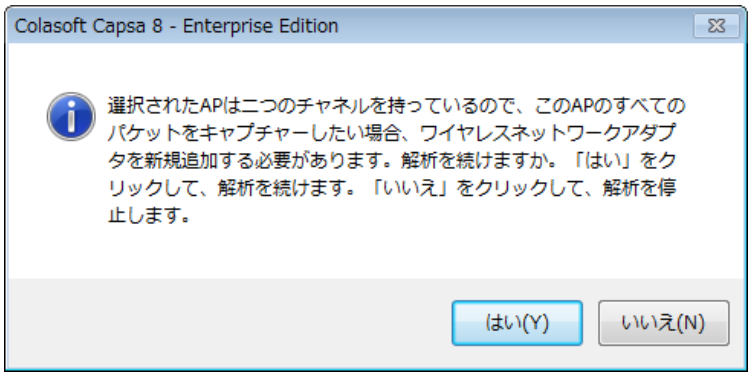
この部分は以下のように表示されます。

AP リストを更新するには、右クリックして、「リフレッシュ」をクリックすればよいのです。

AP のプロパティを修正するには、その AP をダブルクリックすることで、またはその AP を右クリックし、**プロパティ**をクリックすることによって、ワイヤレスネットワークプロパティダイアログボックスが開かれます。ここで別名と暗号化キーを含め、AP を設定することができます。たとえば、AP のために識別しやすい別名を指定することができます。そして、Capsa は暗号化タイプを自動的に識別することができるため、暗号化キーだけを入力すればよいのです。さらにプログラムは AP の設定を記憶することができるため、初めて選択した AP でない場合、キーを入力せずに、ただその AP を選択すればよいのです。

使用されている AP を管理するには、右クリックして、**ワイヤレスネットワーク管理**をクリックすることで、ワイヤレスネットワークの管理ウィンドウが開かれます。ここで、監視されたすべてのワイヤレス AP の履歴リストが表示されます。ここでリストされた AP の設定を変更したり、削除したりすることができます。

Capsa は二つのチャネルを持っているワイヤレス AP のトラフィック解析をサポートしています。お使いのコンピューターにはワイヤレスネットワークアダプタが一つだけある場合、二つのチャネルを持っているワイヤレス AP を選択し、スタートをクリックすると、以下のダイアログボックスがポップアップされます。



キャプチャーされたパケットをリプレイ

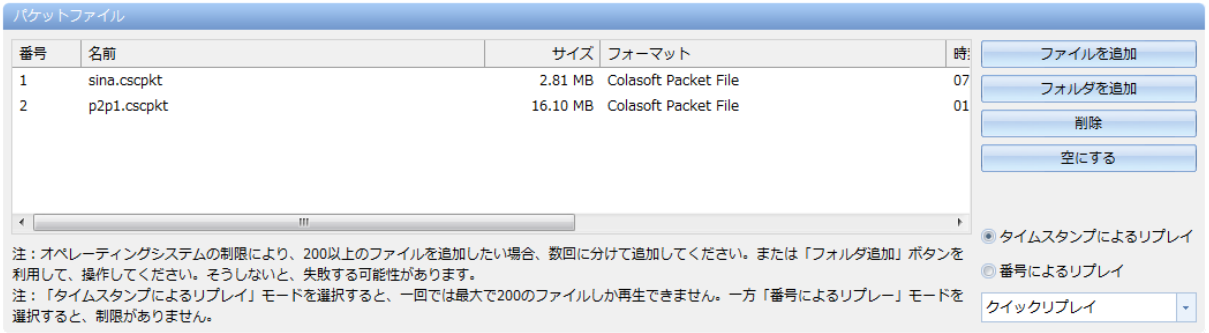
Capsa はライブネットワークデータだけではなく、キャプチャーされたパケットをも解析することができます。Capsa でキャプチャーされたパケット、Wireshark、Omnipeek などのプログラムでキャプチャーされたパケット、および他のパケットが含まれています。

以下のステップに従って、キャプチャーされたパケットをリプレイします。

1. **スタートページ**で**リプレイ解析**を選択します。
2. **パケットファイル**部分における**ファイルを追加**をクリックして、パケットファイルを追加します。
3. **設定情報**部分で**ネットワークプロファイルの設定**をクリックして、ネットワークプロファイルを選択します。ネットワークプロファイルには、ノードグループ、ネームテーブル、およびアラームに関する設定が含まれています。
4. **解析プロファイル**部分で適切な解析プロファイルを選択します。解析プロファイルには、解析モジュール、解析オブジェクト、診断、ビュー表示、パケットバッファ、パケットフィルター、パケット保存、及びログに関する設定が含まれています。Capsa はデフォルトでは九つの解析プロファイルを提供します。当然解析プロファイルを新規作成することもできます。
5. スタートページの下にある**スタート**ボタンをクリックして、解析プロジェクトを開始します。

注意 右側における「前回使ったパケットファイルを使用する」をクリックすることで、前回リプレイされたパケットファイルを直接に追加することができます。

パケットファイル部分は以下のように表示されます。



- **ファイルを追加**: リプレイするファイルを追加します。

- **フォルダを追加**：選択されたファイルフォルダにおけるすべてのパケットファイルを追加します。
- **削除**:パケットファイルリストから選択されたファイルを削除します。
- **空にする**:パケットファイルリストを空にします。
- **リプレイモード**：パケットをリプレイするモードを選択します。
    - **タイムスタンプによるリプレイ**：すべてのパケットは、パケットのタイムスタンプによってリプレイされます。
    - **番号によるリプレイ**：すべてのパケットは、パケットファイルリストにおける順序によってリプレイされます。
- **リプレイスピード**:パケットをリプレイするスピードで、クイックリプレイとノーマルリプレイからなっています。
    - **クイックリプレイ**:キャプチャーされた二つのパケットの間に時間間隔があります。クイックリプレイでは、その時間間隔を無視して、あるパケットがリプレイされた後、すぐ次のパケットをリプレイします。
    - **ノーマルリプレイ**:ノーマルリプレイでは、その時間間隔が終わった後、次のパケットをリプレイします。

Capsa でリプレイできるパケットファイルのフォーマットは以下の通りです。

- Accellent 5Views Packet File (*.5vw)
- Colasoft Packet File (*.cscpkt; *rapkt; *.rawpkt; *.cacproj)
- EtherPeek Packet File (V7/V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO; TRC1)
- Libpcap (Wireshark, Tcpdump, Ethereal, etc.) (*.cap; *pcap)
- Wireshark (Wireshark, etc.) (*.pcapang; *pcapang.gz; *.ntar; *.ntar.gz)
- Microsoft Network Monitor 1.x 2.x (*.cap)
- Novell LANalyer (*.tr1)
- Network Instruments Observer V9.0 (*.bfr)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

そして、キャプチャーされたパケットは以下のフォーマットにエクスポートされることができます。

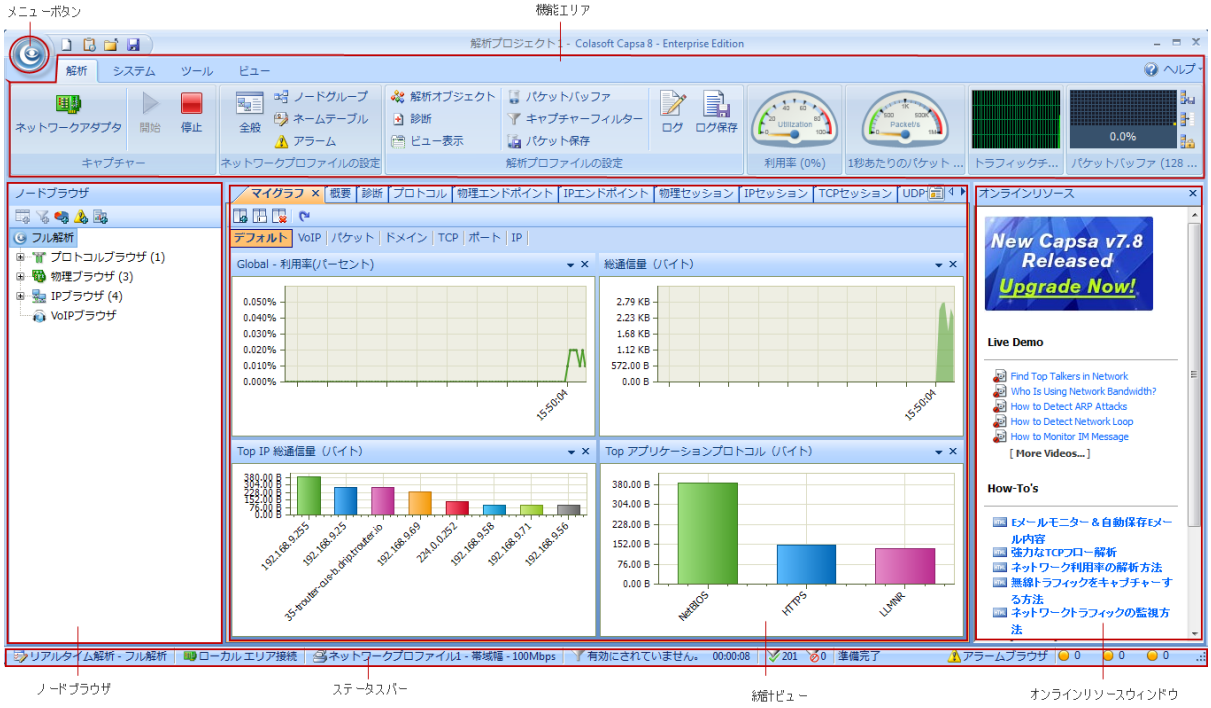
- Accellent 5Views Packet File (*.5vw)
- Colasoft Packet File (V3) (*.rapkt)
- Colasoft Packet File (*.cscpkt)
- Colasoft Raw Packet File (*.rawpkt）
- Colasoft Raw Packet File (V2) (*.rawpkt）
- EtherPeek Packet File (V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO; *.TRC1)
- Libpcap (Wireshark, Tcpdump, Ethereal, etc.) (*.cap; *pcap)
- Wireshark (Wireshark, etc.) (*.pcapang; *pcapang.gz; *.ntar; *.ntar.gz)

- Microsoft Network Monitor 1.x 2.x (*.cap)
- Novell LANalyer (*.tr1)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

メインユーザーインターフェース

リアルタイムキャプチャー、またはパケットのリプレイなどの解析プロジェクトを開始した後、Capsa は様々な統計と解析結果を提供するメインユーザーインターフェースに入ります。メインユーザーインターフェースは六つの部分からなっています。

- メニューボタン
- 機能エリア
- ノードブラウザウィンドウ
- 統計ビュー
- オンラインリソースウィンドウ
- ステータスバー



メニューボタン

メニューボタン  はプロジェクトウィンドウの左上にあります。

メニューボタンにおけるアイテム

以下のリストはメニューボタンにおけるアイテムについて説明しています。

- **新規作成**:新しい解析プロジェクトを作成します。
- **タスクスケジューラ**:システムオプションダイアログボックスにおけるタスクスケジューラタブに移動し、解析タスクをスケジュールします。

- **全体設定のインポートとエクスポート**:全体設定（詳しいことは全体設定のインポートとエクスポートをご参照ください。）をインポート、またはエクスポートします。
- **印刷**:現在開いたページを印刷、または印刷設定をします。
- **ツール**：Ping Tool、 Packet Player、 Packet Builder、MAC Scanner という四つのネットワークツールを提供します。
- **リソース**: Colasoft とネットワーク解析に関するインタネット情報を提供します。
    - Colasoft ホームページ: Colasoft ホームページに移動します。
    - フォーラム:技術フォーラムを開きます。ここで、当社から助けをもらい、ネットワーク解析に関する知識を学ぶことができます。
- **製品**:製品に関する情報を提供します。
    - **製品ライセンス**:ライセンスキーを更新します。
    - **カスタマーポータル**: Colasoft Customer Portal に移動します。
    - **更新**: 新バージョンをチェックします。
    - **Capsa について**:バージョン、著作権、およびライセンス情報などが表示される **Capsa について**ダイアログボックスを開きます。
- **最近開いたパケットファイル**:最近開いたパケットファイルがリストされます。
- **システムオプション**: 解析プロジェクトに関するいくつかの設定をします（詳しいことは、システムオプションをご参照ください）。
- **終了**:プログラムを終了します。

クイックアクセスアイコン

メニューボタンの隣にいくつかのクイックアクセスアイコンがあります。

 :新しい解析プロジェクトを作成します。

 :タスクスケジューラを開き、新しいタスクを追加します（詳しいことはタスクスケジューラをご参照ください）。

 : 現在の解析プロジェクトを閉じて、スタートページに移動します。

 : バッファにおけるパケットをディスクに保存します。パケットを 12 のフォーマットに保存することができます。たとえば、 *Colasoft Packet File (*.cscpkt)*、*Colasoft Raw Packet File (*.rawpkt)*、*Colasoft Raw Packet File (v2) (*.rawpkt)*、*Accellent 5Views Packet File (*.5vw)*、 *EtherPeek Packet File (V9) (*.pkt)*、*HP Unix Nettl Packet File (*.TRC0; TRC1)*、*libpcap (Wireshark*、 *Ethereal*、*Tcpdump など) (*.cap; pcap)*、 *Microsoft Network Monitor 1.x*、*2.x (*.cap)*、*Novell LANalyzer (*.tr1)*、*NetXRay2.0*、*and Windows Sniffer (*.cap)*、 *Sun_Snoop (*.Snoop)*、*Visual Network Traffic Capture (*.cap)*。

機能エリア

機能エリアは以下の四つのタブからなっています。

- 解析:ネットワークプロファイル、解析プロファイルなど設定が含まれています。
- システム:リソース、製品に関する情報を提供します。

- ツール: Colasoft ネットワークツールを提供します。
- ビュー:プログラムの表示に関する設定を提供します。

ヒント マウスポインタが**機能エリア**にある場合、マウスのスクロールホイールを利用して、一つのタブから他のタブに移動することができます。

解析

解析タブは以下のように表示されます。

リプレイ解析モードが選択されると、**キャプチャー**部分は以下のように**リプレイ**部分になります。

解析タブは以下の部分からなっています。

- キャプチャー:
  - ネットワークアダプタ:クリックして、「**ネットワークアダプタを選択**」ダイアログボックスを開くことで、アダプタプロパティを表示したり、アダプタの選択を変更したりします。
  - 開始:パケットのキャプチャーと解析を開始します。
  - 停止:パケットのキャプチャーと解析を停止します。
- リプレイ:
  - パケットファイル:クリックして、スタートページにおける**パケットファイル**部分と同じ**パケットファイルの管理**ダイアログボックスが開かれます。
  - 開始:リプレイを開始します。
  - 一時停止:リプレイを一時停止します。
  - 停止:リプレイを停止します。
- **ネットワークプロファイル**:ネットワークプロファイルのパラメータを設定します（詳しいことは、ネットワークプロファイル をご参照ください）。
- **解析プロファイル**:解析プロファイルのパラメータを設定します（詳しいことは、解析プロファイルをご参照ください）。
- **利用率（%）**:ゲージでネットワーク帯域幅の利用率を表示します。
- **1 秒あたりのパケット**:ゲージでキャプチャーされたパケットの数を表示します。
- **トラフィックチャート（bps）**:選択されたアダプタの毎秒のトラフィックを表示しま

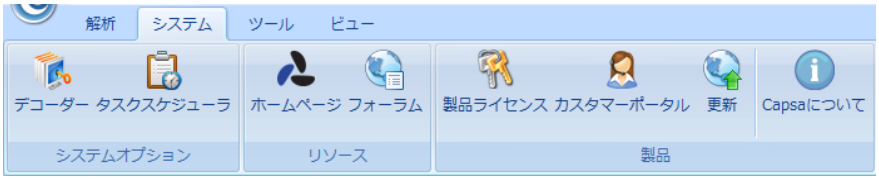
す。マウスをチャートの上に移動して、その時のトラフィック数と時間が表示されます。

- **パケットバッファ**:
  - バッファマップ:解析プロジェクトに使用されたバッファのサイズと総バッファが表示されます。
  - エクスポート:パケットバッファにおけるパケットを選択されたフォーマットに保存します。
  - 空にする:パケットバッファにおけるデータを空にします。
  - ロック:パケットバッファの中のデータをロックします。

注意 パケットバッファをロックしても、プログラムはパケットをキャプチャーします。

システム

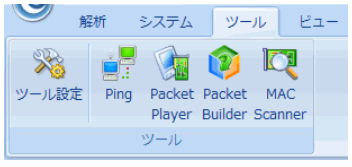
システムタブは以下のように表示されます。



- **デコーダー**:**デコーダーの設定**タブを開き、デコーダーを設定します。
- **タスクスケジューラ**:システムオプションダイアログボックスにおけるタスクスケジューラタブに移動し、解析タスクをスケジュールします。この機能は Capsa *Enterprise* の場合にのみ、利用可能となります。
- **ホームページ**: Colasoft ホームページに移動します。
- **フォーラム**:技術フォーラムを開きます。ここで、当社から助けをもらい、ネットワーク解析に関する知識を学ぶことができます。
- **製品ライセンス**:ライセンスキーを更新します。
- **カスタマーポータル**: Colasoft Customer Portal に移動します。
- **更新**:新バージョンをチェックします。
- **Capsa について**:バージョン、著作権、およびライセンス情報などが表示される **Capsa について**ダイアログボックスを開きます。

ツール

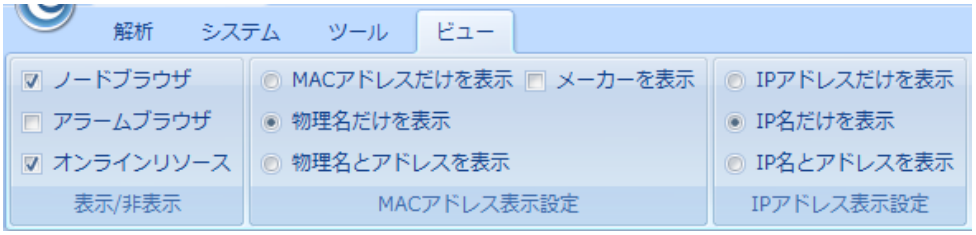
ツールタブは以下のように表示されます。



ツールタブの詳しい情報については、ネットワークツールをご参照ください。

ビュー

ビュータブは以下のように表示されます。



ビュータブは以下の部分から構成されています。

- **表示/非表示**:ノードブラウザ、アラームブラウザ、オンラインリソースを表示、または非表示にします。
- **MAC アドレス表示設定**: MAC アドレスの表示フォーマットを設定します。
    - MAC アドレスだけを表示: 16 進数で MAC アドレスだけを表示します。例えば：*AA:BB:CC:33:44:55*
    - 物理名だけを表示: 別名で MAC アドレスだけを表示します。例えば：*localhost*
    - 物理名とアドレスを表示:16 進数と別名で MAC アドレスを表示します。例えば： *[localhost]-AA:BB:CC:33:44:55*
    - メーカーを表示:アダプタメーカーを表示、非表示にします。
- **IP アドレス表示設定**: IP アドレスの表示フォーマットを設定します。
    - IP アドレスだけを表示: 数字で IP アドレスだけを表示します。例えば：*192.168.1.1*
    - IP 名だけを表示:別名で IP アドレスだけを表示します。例えば： *Localhost*
    - IP 名とアドレスを表示: 数字と別名で IP アドレスを表示します。例えば：*[Localhost]-192.168.1.1*

ノードブラウザウィンドウ

ノードブラウザウィンドウは、機能的には、表示フィルターです。ここで、ノード別に様々なセッションデータを迅速且つ正確に確認することができます。**ノードブラウザ**ウィンドウで選択したノードのタイプによって、統計ビューで提供しているビューも違い、各ビューにおける統計も異なります。

ボタン

ノードブラウザウィンドウには以下アイコンが含まれています。

 :選択したノードをネームテーブルに追加します。

 :選択したノードに基づいて、フィルターを作成します。

 :選択したノードに基づいて、チャートを作成します。

 :選択したノードに基づいて、アラームを作成します。

 :選択したノードに基づいて、レポートを作成します。

キーボードを利用して、ノードブラウザを操作することができます。例えば、キーボードにおける**上向き矢印**を押すことで上のノードを、**下向き矢印**を押すことで下のノードを選択することができます。**左向き矢印**を押すことでノードを折りたたみ、**右向き矢印**を押すことでノードを展開します。

ノードブラウザウィンドウでは、単一ノードでもノードグループでもノートと呼ばれることができます。

ノードブラウザの詳しい情報については、ノードブラウザをご参照ください。

統計ビュー

統計ビューは、膨大な解析統計（詳しいことは、統計をご参照ください）、チャート、レポート、ログ、および他の情報を提供します。

デフォルトの統計ビューの状態は、選択された解析プロファイルによって違います。

統計ビューを表示、非表示、または配列することができます。

- 統計ビューを表示するには、**機能エリア**における**解析**タブの**ビュー表示**アイコンをクリックして、表示したいビューを選択すればよいのです。
- 統計ビューを配列するには、**機能エリア**における**解析**タブの**ビュー表示**アイコンをクリックし、**上に移動**、または**下に移動**をクリックすればよいのです。

ノードブラウザウィンドウで選択したノードのタイプによって、統計ビューで提供しているビューも違います。

セキュリティ解析と VoIP 解析は Capsa Enterprise の場合にのみ、利用可能となります。

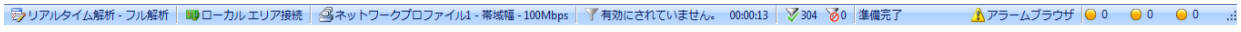
オンラインリソースウィンドウ

オンラインリソースウィンドウはライブデモ、How tos、および技術フォーラムを含むオンラインリソースを提供します。

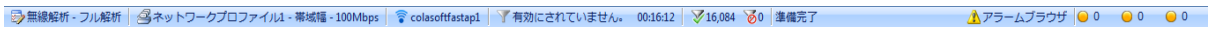
オンラインリソースウィンドウは、デフォルトでメインユーザーインターフェースの右の部分に表示されます。右上にある閉じるボタンをクリックして、オンラインリソースウィンドウを閉じることができます。解析プロジェクトを起動するとき、それを表示したくない場合、**メニュー**ボタンをクリックし、**システムオプション**をクリックして、**全般**タブで、「起動する際、オンラインリソースウィンドウを表示します。」にチェックを外せばよいのです。

ステータスバー

ステータスバーは、解析プロジェクトの一番下にあり、現在プロジェクトの一般的な情報を提示します。ステータスバーは下図のように表示されます。



ワイヤレスネットワークを監視している場合、ステータスバーは以下のように表示されます。



ステータスバーは、左から右まで以下七つの部分からなっています。

解析モード - 解析プロファイル

この部分では選択された解析モードと解析プロファイルを表示します。ここをクリックして、**解析プロファイルの設定**ダイアログボックスを開き、解析プロファイルを設定できます。

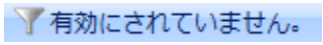
アダプタ

リアルタイム解析モードで、この部分では、選択されたワイヤレス AP、または有線ネットワークアダプタの名前、あるいは数を表示します。ここをクリックして、詳細情報を確認することができます。

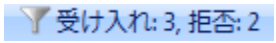
リプレイ解析モードで、この部分では、リプレイされたファイルの数とリプレイ状態を表示します。ここをクリックして、詳細情報を確認することができます。

フィルター

この部分は、フィルター情報を表示します。有効にされるフィルターがない場合、



のように表示されます。一方、有効にされるフィルターがある場合、



のように、**受け入れ**と**拒否**それぞれのフィルター数が表示されます。

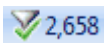
ここをクリックして、**キャプターフィルター**ダイアログボックスを開き、フィルターを設定することができます。

運行時間

リアル解析モードで、この部分は、現在の解析プロジェクトの運行時間を表示します。

リプレイ解析モードで、この部分は、パケットファイルをリプレイして、かかった時間を表示します。

キャプチャーしたパケット数とフィルターアウトしたパケット数

この部分は、 

のように、プログラムによってキャプチャーされたパケットの数と

のように、フィルターによってフィルターアウトされたパケットの数を表示します。

ボタンとメニューヒント

マウスが**メニュー**におけるアイテム、または**機能エリア**におけるボタンに移動する時、この部分は、そのアイテム、あるいはそのボタンのヒントを表示します。デフォルトでは、*準備完了*と表示されます。

アラーム通知エリア

この部分は、**アラームブラウザ**アイコンと三つのトリガーされたアラームのカウンタからなっています。

ネットワークプロファイル

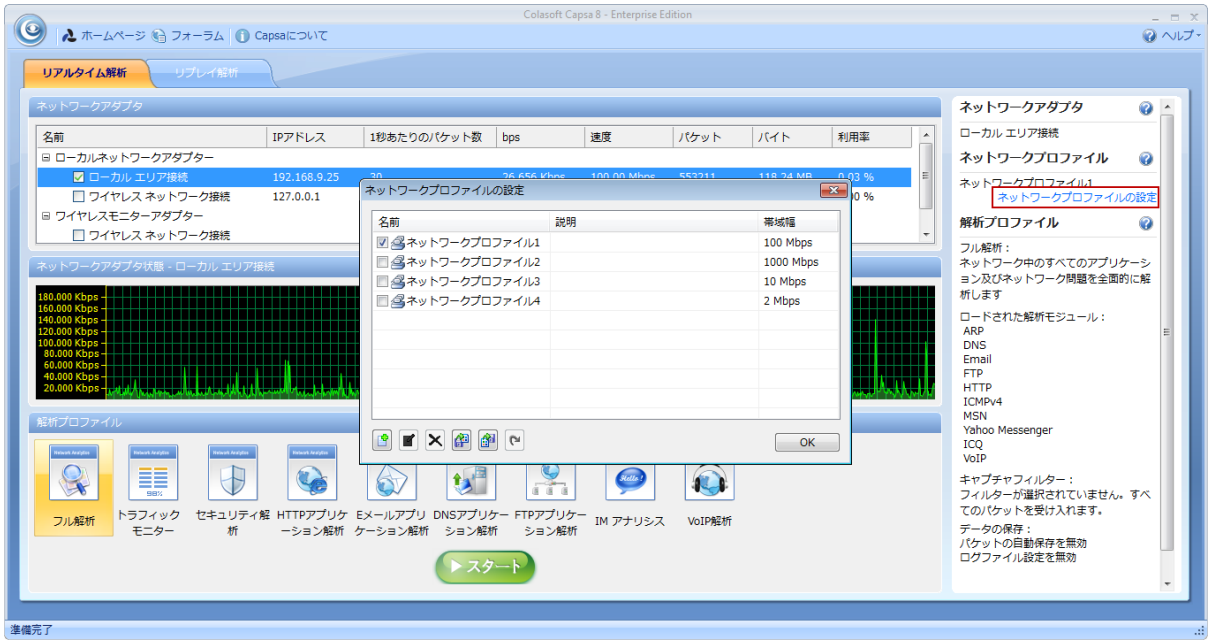
ネットワークプロファイルについて

ネットワークプロファイルは、異なるネットワークの一般的なプロパティを保存するために設計されたものです。ネットワークセグメントによって、持っている環境も違います。Colasoft Capsa を利用して、帯域幅、ネットワーク構造、ネームテーブル、およびアラームを含め、最も一般的に使用されているプロパティを保存することができます。デフォルトでは、ネットワークプロファイルが適用されていません。ネットワークグループ、ネームテーブル、またはアラームを変更する場合、まずネットワークプロファイルを作成する必要があります。

ラップトップに Capsa をインストールし、ネットワーク間で Capsa を利用する必要がある場合、各ネットワークのために専用のネットワークプロファイルを作成し、そのネットワークならではのプロパティを保存したほうがいいです。そうすると、再びそのネットワークに接続する時、対応のネットワークプロファイルを選択すればよいのです。

新しいネットワークプロファイルを作成するには、

1. スタートページで、**ネットワークプロファイルの設定**をクリックして、ネットワークプロファイルの設定ダイアログボックスを開きます。



2. ネットワークプロファイルの設定ダイアログボックスで、  ボタンをクリックして、ネットワークプロファイルを定義します。

既存のネットワークプロファイルを修正することもできます。ネットワークプロファイルを修正するには、修正したいネットワークプロファイルをダブルクリックし、ポップアップされたボックスで設定を修正すればよいのです。

全般

全般の設定タブは下図のように表示されます。

全般の設定タブには、以下のオプションが含まれています。

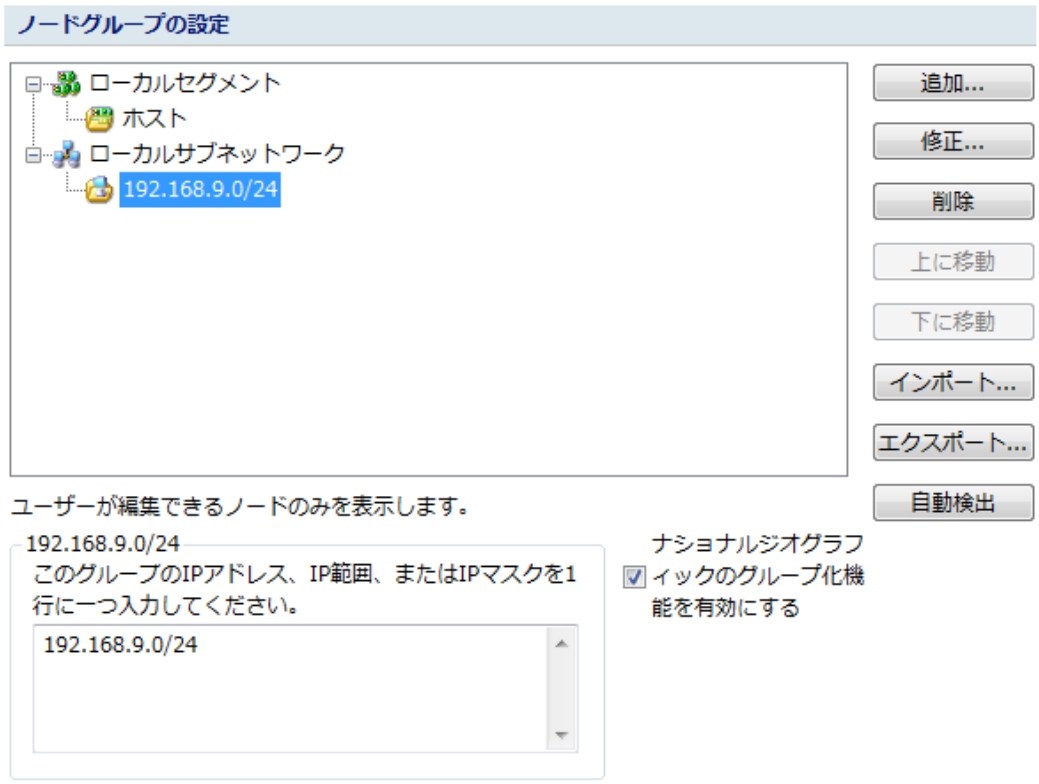
- **名前**:ネットワークプロファイルの名前を入力します。
- **説明**:ネットワークプロファイルについての説明を入力します。
- **帯域幅**:現在ネットワークの実際の帯域幅を入力します。
- **自動的にホスト名を積極解決する**:自動的且つ積極的にアドレスをホスト名とドメイン名に解決します。
- **自動的にホスト名を受動解決する**:自動的に且つ受動的にアドレスをホスト名とドメイン名に解決します。デフォルトでは有効になっています。
- **自動的に解決されたホスト名を保存**:自動的に解決されたホスト名を保存します。デフォルトでは、有効になっています。
- **未使用の名前の保存日数**:未使用の名前を保存する日数を指定します。デフォルトでは、二日となっています。

注意 帯域幅はネットワーク利用率を計算するベンチマークで、非常に重要なパラメータです。デフォルトで、帯域幅は、アダプタのプロパティから計算されています。

ノードグループ

Capsa では、ネットワークにおけるすべての IP アドレスノードと MAC アドレスノードは、異なるノードグループに分けることができます。そのため、ローカルトラフィックとインタネットトラフィックを、ブロードキャストトラフィックとマルチキャストトラフィックを区別するのは簡単です。

MAC アドレスの場合、ローカルセグメント、ブロードキャストアドレス、およびマルチキャストアドレスという三つのノードグループがあります。IP アドレスの場合、ローカルサブネットワーク、プライベート用ネットワーク、マルチキャストアドレス、ブロードキャストアドレス、インタネットアドレス、およびリンクローカルアドレスという六つのノードグループがあります。利用可能な場合、これらすべてのノードグループは**ノードブラウザ**ウィンドウに表示されます。



ノードグループタブは、ネットワークにおけるローカル MAC アドレスと IP アドレスを管理するために設計されたもので、ノードグループリストと呼ばれる上のパネル、ノードリストと呼ばれる下のパネル、および複数のボタンからなっています。上のパネルでは、すべてのノードグループをリストし、下のパネルでは、ノードグループリストで選択されたノードグループのすべてのノードをリストします。ボタンについては、以下のように説明しています。

- **追加**: ノードグループリストで選択されたノードグループに属する新しいノードグループを追加します。

- **修正**:ノードグループリストで選択されたノードグループの名前を修正します。
- **削除**:ノードグループリストから選択されたノードグループを削除します。
- **上に移動**:選択されたノードグループを上に移動します。
- **下に移動**: 選択されたノードグループを下に移動します。
- **インポート**:保存された.cscng ファイルのノードグループリストをインポートします。
- **エクスポート**:現在のノードグループリストを.cscng ファイルにエクスポートします。
- **自動検出**:現在ネットワークにおけるローカル MAC アドレスと IP アドレスを検出し、グループ分けします。
- **ナショナルジオグラフィックのグループ化機能を有効にする**:**インタネットアドレス**というノードグループを国や地域によって、グループ分けします。

ノードグループリストでは、**ローカルセグメント**はローカル MAC アドレスのノードグループを管理し、**ローカルサブネットワーク**は、ローカル IP アドレスのノードグループを管理します。デフォルトでは、ネットワークアダプタを介して検出されたノードグループが自動的に生成されます。**自動検出**をクリックして、同じ結果を得ることができます。

- MAC アドレスのノードグループを追加するには、ノードグループリストで**ローカルセグメント**を選択し、**追加**ボタンをクリックし、新しいノードグループの名前を入力して、OK をクリックします。そして、ノードリストで新しいノードグループの MAC アドレスを一行に一つ入力します。
- IP アドレスのノードグループを追加するには、ノードグループリストで**ローカルサブネットワーク**を選択し、**追加**ボタンをクリックし、新しいノードグループの名前を入力して、OK をクリックします。そして、ノードリストで新しいノードグループの IP アドレス、IP アドレス範囲、IP アドレスマスクを一行に一つ入力します。

注意 新しいノードグループは選択されたノードグループのサブノードグループとなります。

ネームテーブル

ネームテーブルタブで、すべての MAC アドレスと IP アドレスの別名を管理します。「**ネームテーブルタイプを選択**」を利用して、MAC ネームテーブル、または IP ネームテーブルを選択することができます。ネームテーブルリストにアイテムがたくさんある場合、**検索**テキストボックスにキーワードを入力することで、興味を持っているアイテムを見つけることができます。

このタブにおけるボタンについて、以下のように説明しています。

- **追加**:アドレスの別名を追加します(詳しいことは、ネームテーブルに追加 をご参照ください)。
- **修正**:選択されたアイテムを修正します。
- **削除**:選択されたアイテムを削除します。
- **インポート**:.cscont ファイル、または.cscntab ファイルからネームテーブルをインポートします。
- **エクスポート**:現在のネールテーブルを.cscont ファイルにエクスポートし、保存します。

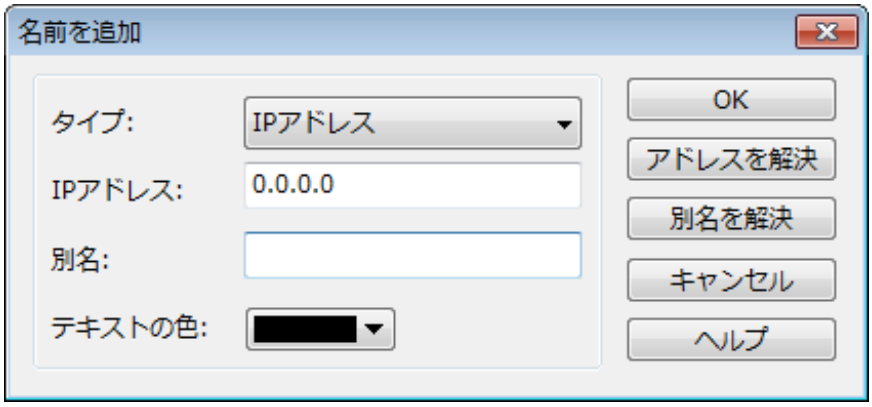
ホストは IP アドレスではなく、解決された別名で表示されます。

注意 自動解決機能は、ネットワークプロファイルが適用されている場合にのみ、利用可能となります。

ネームテーブルに追加

以下のステップに従い、アドレスの別名を追加します。

1. **解析**タブの**機能エリア**における**ネームテーブル**ボタンをクリックして、ネームテーブルタイプを一つ選択し、**追加**ボタンをクリックすることで、下図のような**名前を追加**ダイアログボックスを開きます。



2. アドレスとアドレスの別名を入力します。
3. このダイアログボックスにおける OK をクリックして、**ネームテーブル**タブにおける OK をクリックします。

アドレスの別名が分からない場合、「**アドレスを解決**」ボタンを利用して、自動的にアドレスを解決することができます。または、ある別名のアドレスが分からない場合、**別名を解決**ボタンを利用して、自動的に別名を解決することができます。

以下のステップに従い、指定されたアドレスの別名を追加します。

1. アドレスノードを一つ選択して、**ノードブラウザ**ウィンドウのツールバー、または統計ビューのツールバーにおける  をクリックすることで、**名前を追加**するダイアログボックスが開きます。

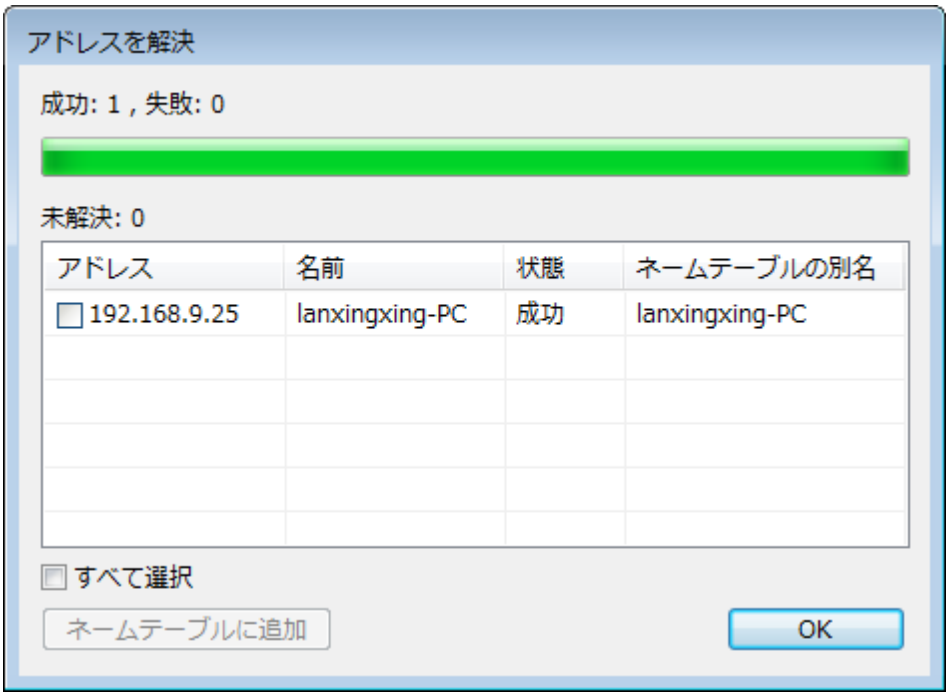
   ヒント 選択されたアドレスノードを右クリックし、**ネームテーブルに追加**をクリックすることで、**名前を追加**するダイアログボックスが開きます。

2. アドレスの別名を入力して、OK をクリックします。

自動解決されたアドレスに対しても、それを右クリックして、**ネームテーブルに追加**をクリックすることで、**ネームテーブル**に追加することができます。

アドレスを解決

別名をネームテーブルに追加するだけでなく、**アドレスを解決**するダイアログボックスを利用して、アドレスと別名を自動的に解決することができます。アドレスを解決ダイアログボックスは以下のように表示されます。



アドレスを解決ダイアログボックスには、以下のカラムが含まれています。

- アドレス：解決するアドレスを表示します。
- 名前：解決されたアドレスの名前を表示します。
- 状態：解決の状態を表示します。
- ネームテーブルの別名：ネームテーブルにおけるアドレスの別名を表示します。

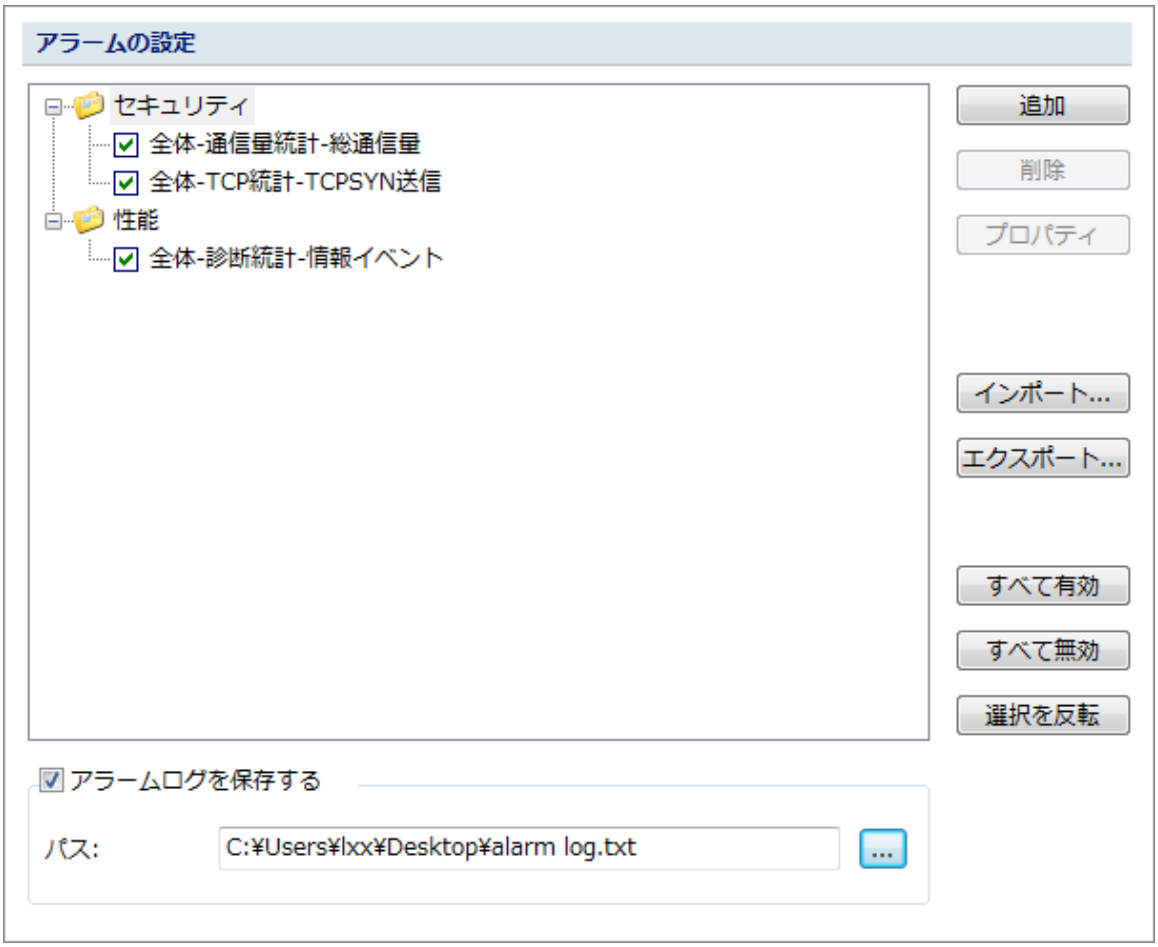
ネームテーブルに追加:選択されたアイテムをネームテーブルに追加し、*アドレスを解決*ダイアログボックスから削除します。

IP アドレスノードを右クリックして、**アドレスを解決する**をクリックすることで、アドレスを解決するダイアログボックスを開くことができます。

注意 IP アドレスだけが*アドレスを解決*ダイアログボックスで解決されることができます。

アラーム

アラームタブはネットワークプロファイルにおけるすべてのアラームを管理し、アラームタイプに応じて階層的にすべてのアラームをリストします。



アラームタブにおける各ボタンについては、以下のように説明しています。

- **追加**:新しいアラームを作成します(詳しいことは、アラームを作成をご参照ください)。
- **削除**:選択されたアラームを削除します。
- **プロパティ**:選択されたアラームのプロパティを確認したり、修正したりします。
- **インポート**:.csalarm ファイルからアラーム設定をインポートします。
- **エクスポート**:.csalarm ファイルにアラーム設定をエクスポートします。
- **すべて有効**:リストにおけるすべてのアラームを有効にします。
- **すべて無効**:リストにおけるすべてのアラームを無効にします。
- **選択を反転**:リストにおけるアラームの選択を反転します。

アラームログを保存する:トリガーされたアラーム記録を.txt ファイルに保存します。このオプションにチェックを入れ、[...]をクリックして保存するパスを指定して、アラームログファイルの名前を入力します。

アラームを作成

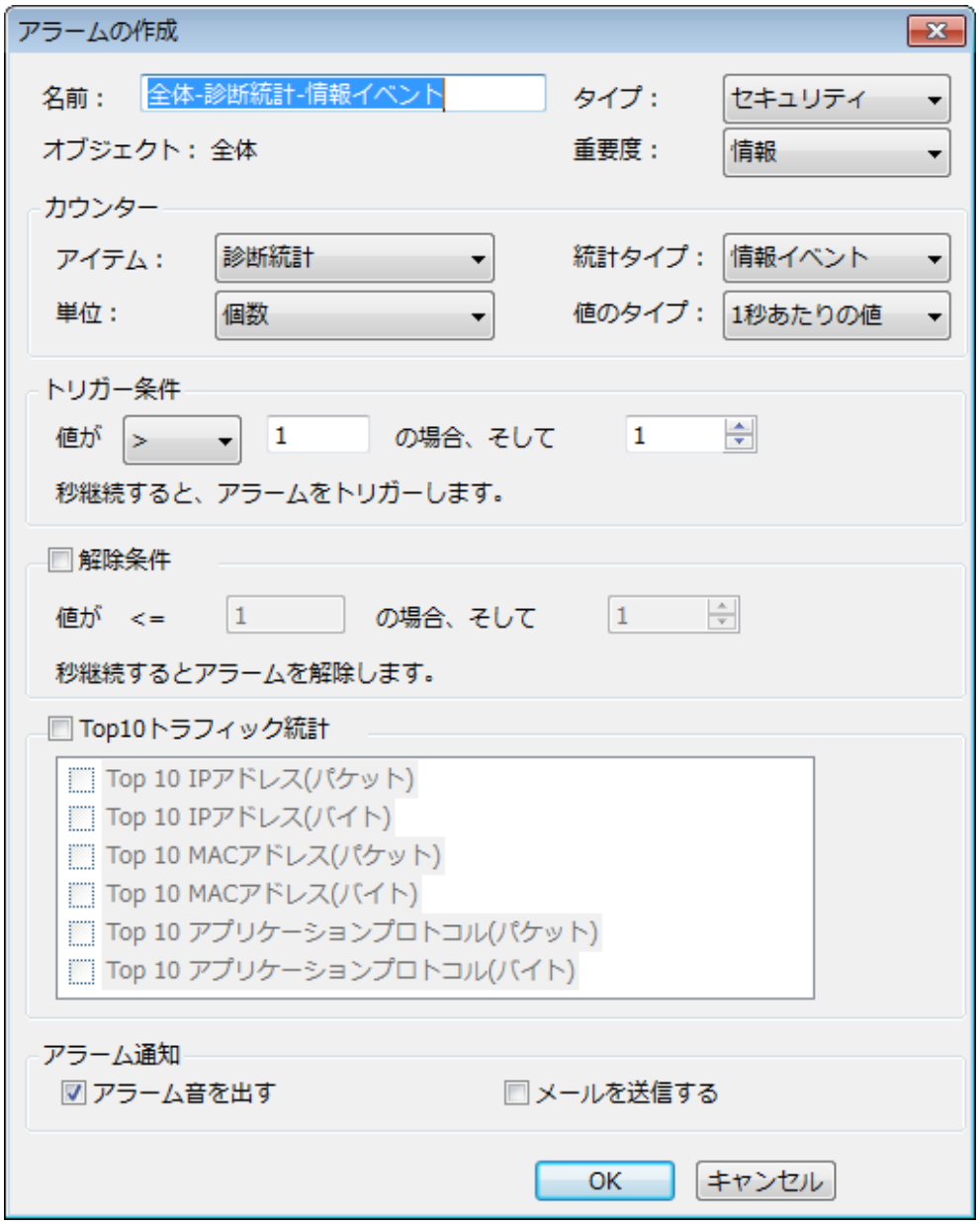
アラームを作成するには、以下のいずれに従い、**アラームの作成**ダイアログボックスを開き、開かれたダイアログボックスの設定を完了します。

- **アラームブラウザ**ウィンドウで**アラームを追加**ボタンをクリックします。
- **ネットワークプロファイル設定**ダイアログボックスを開き、**アラーム**タブを選択し、**追加**ボタンをクリックします。
- **ノードブラウザ**ウィンドウで  アイコンをクリックします。
- **ノードブラウザ**ウィンドウと統計ビューのポップアップメニューで**アラームを作成**を選択します。

ヒント

1. 前の二つの方法で作成されたアラームは、解析プロジェクトでキャプチャーされたすべてのパケットの統計によって、トリガー、または解除されます。
2. 最後の二つの方法で作成されたアラームは、**ノードブラウザ**や統計ビューで右クリック、または選択したノードの統計によって、トリガー、または解除されます。

アラームの作成ダイアログボックスは以下のように表示されます。



アラームの作成ダイアログボックスは以下の部分から構成されています。

- **一般情報**
  アラーム名、アラームタイプ、オブジェクト、およびアラーム重要度を含むアラームの一般情報を設定します。オブジェクトオプションは、プログラムによって自動的に設定されます。
- **カウンター**
  アラームの統計アイテムを設定します。アラーム統計アイテムは、オブジェクトによって、違います。
- **トリガー条件**
  アラームのトリガー条件を設定します。
- **解除条件**
  アラームの解除条件を設定します。

- **Top 10 トラフィック統計**
  このオプションにチェックを入れると、アラームがトリガーされた時、top 10 トラフィック統計はアラームログに記録されます。
- **アラーム通知**
  この機能は、Capsa Enterprise の場合にのみ、利用可能となります。アラームがトリガーされる際、アラームメッセージを通知する方法を設定することができます。音で通知するには、**アラーム音を出す**にチェックを入れます。E メールで通知するには、**メールを送信する**にチェックを入れます。

アラームを修正

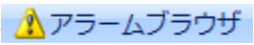
任意アラームをダブルクリックすることで、**アラームを修正**ダイアログボックスを開き、アラームを修正することができます。**アラームを修正**ダイアログボックスは、**アラームの作成**ダイアログボックスとまったく同じです。

アラームを修正ダイアログボックスでは、アラームの**名前**と**タイプ**、カウンターにおける**値のタイプ**、**トリガー条件**、及び**解除条件**しか修正できません。他のオプションを修正したい場合、まずそのアラームを削除し、新しいアラームを作成する必要があります。

アラームブラウザウィンドウ

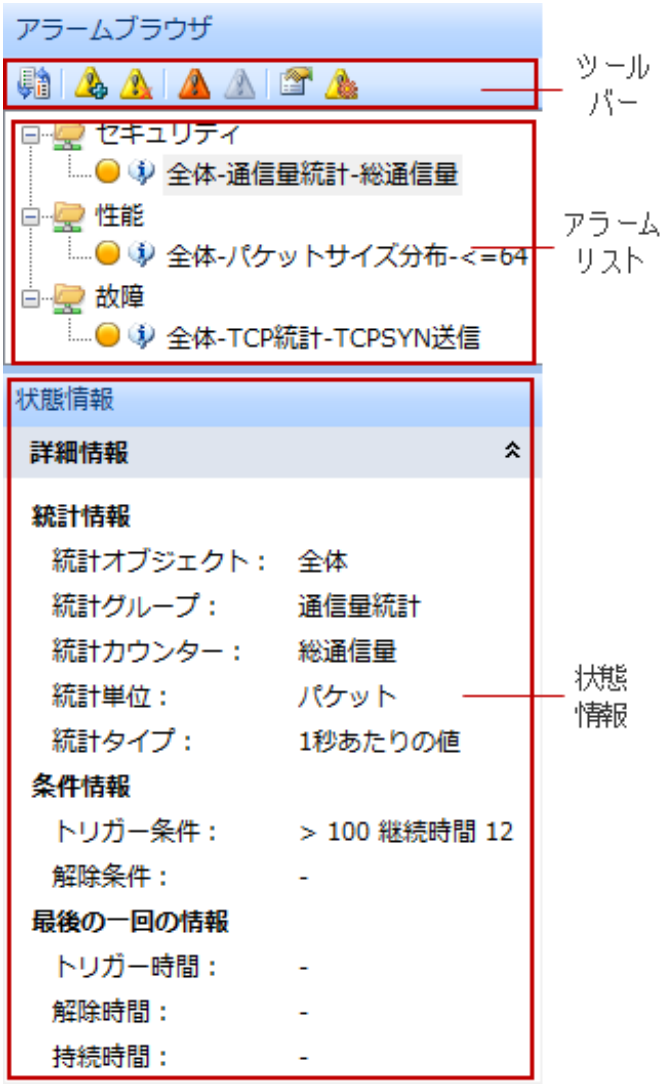
ネットワークの統計を確認する時、特定のネットワーク統計、またはトラフィック状態を警告するツールが必要とする場合もあります。Capsa アラーム機能を利用して、作成されたアラームルールに違反する場合、アラーム音を出したり、E メールを送信したりして、警告を出します。

Capsa はアラームを管理する**アラームブラウザ**ウィンドウを提供します。**アラームブラウザ**ウィンドウで、アラームを作成、修正、および表示することができます。ステータスバーの右におけるアラーム通知エリアでトリガーされたアラーム情報を取得することもできます。アラームを作成、修正する方法については、アラームを作成をご覧ください。

アラームブラウザウィンドウを開くには、ステータスバーの右におけるアラーム通知エリアで  をクリックすればよいのです。

解析プロジェクトを起動する時に**アラームブラウザ**ウィンドウを表示したい場合、**機能エリア**における**ビュー**タブをクリックして、**アラームブラウザ**にチェックを入れればよいのです。

アラームブラウザウィンドウは以下のように表示されます。



ツールバー

ツールバーは以下のアイコンから構成されています。

:アラームリストを階層化に表示するかどうかを切り換えます。

:**アラームの作成**ダイアログボックスを開き、新しいアラームを作成します。

:選択されたアラームを削除します。

:トリガーされたアラームだけを表示します。

:トリガーされたアラームを解除します。

:アラームのプロパティを表示したり、アラームを修正したりします。

:ネットワークプロファイル設定ダイアログボックスの**アラーム**タブを開きます。

アラームリスト

作成されたすべてのアラームは階層的に**セキュリティ**、**性能**、**故障**という 3 種類に分けています。アラームアイテムをダブルクリックして、**アラームを修正**ダイアログボックスを開き、そのアラームを修正することができます。

あるアラームアイテムをクリックすると、**状態情報**パネルはそのアラームの詳細情報を表示します。

状態情報

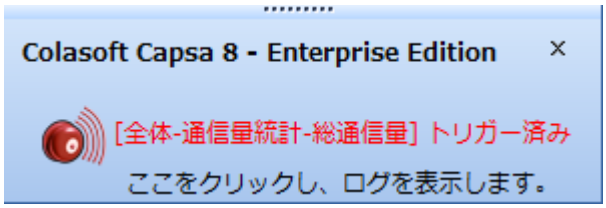
状態情報パネルは選択されたアラームのプロパティを詳細的に表示します。

ヒント をクリックして、アラームの詳細情報を折りたたむことができます。

アラームがトリガーされた場合、知らせのボックスがポップアップされます。

アラーム通知

あるアラームがトリガーまたは解除された際、プログラムウィンドウがアクティブでない場合でも、アラーム情報を通知するポップアップがアラームブラウザウィンドウの下から出てきます。



「**ここをクリックし、ログを表示します。**」をクリックして、アラームログを確認することができます。

ヒント あるアラームがトリガーされると、ステータスバーの右にあるアラームバブルは点滅します。

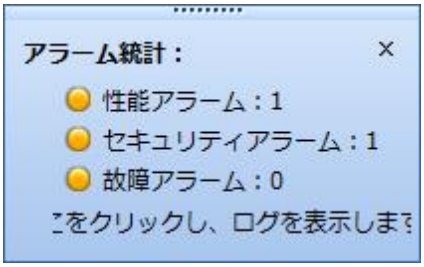
注意

1. ポップアップは 1 秒間だけ表示し、その後はフェードアウトします。
2. **ネットワークプロファイルの設定**ダイアログボックスにおける**アラーム**タブの**アラームログを保存する**にチェックが入っていない場合、「**ここをクリックし、ログを表示します。**」が「**ここをクリックし、アラームログを保存します。**」になっています。

アラームブラウザウィンドウの下に三つのバブルがあり、それぞれセキュリティ、性能、故障という三つのアラームタイプを表します。

バブルの後の番号はトリガーされた各アラームタイプのアラームの数を表します。

バブルをクリックして、タイプごとに統計するアラーム統計ポップアップが表示されます。

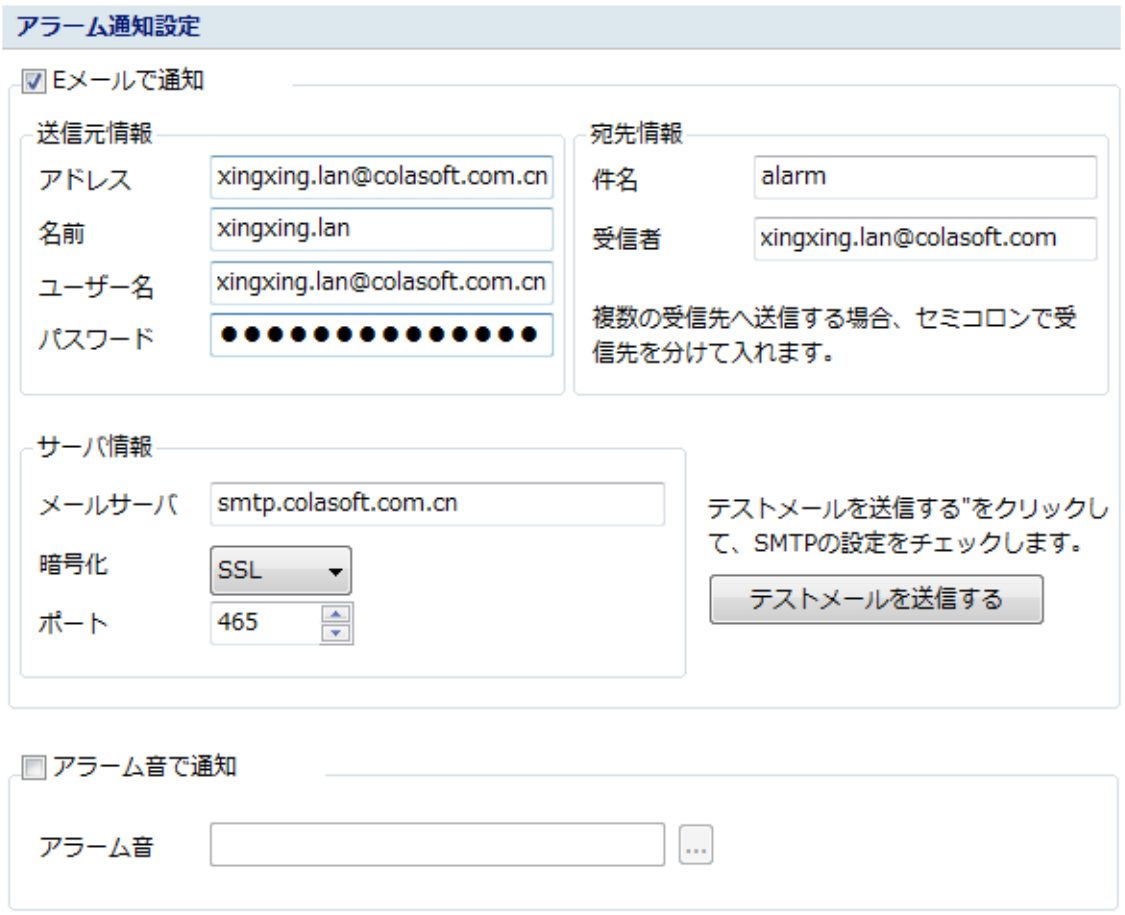


さらに、アラームを作成する際、「アラーム音を出す」と「メールを送信する」にチェックを入れれば、アラームがトリガーされると、アラーム音が聞こえ、E メールを受信します。

アラーム通知設定

このタブはアラーム通知を設定するために設けたものです。アラームがトリガーされると、アラームメッセージは E メールまたはアラーム音で通知されます。

注意 アラーム通知機能は Capsa Enterprise の場合にのみ利用可能となります。Capsa Professional はこの機能をサポートしません。



E メールで通知

以下のステップに従い、E メールでアラームを通知します。

1. アラーム通知タブにおける **E メールで通知**にチェックを入れます。
2. **送信元情報**で、送信者情報を入力します。
   - **アドレス**:送信者の E メールアドレスを入力します。
   - **名前**:送信者の名前を入力します。
   - **ユーザー名**:送信者が E メールサーバーにログインするときのユーザー名を入力します。
   - **パスワード**:送信者が E メールサーバーにログインするときのパスワードを入力します。
3. **宛先情報**で、受信者情報を入力します。
   - **件名**:アラーム通知 E メールの件名を入力します。
   - **受信者**:アラーム通知 E メールの受信者アドレスを入力します。セミコロンで複数の受信者アドレスを入力することができます。
4. **サーバー情報**で、E メールサーバー情報を入力します。
   - **メールサーバー**: E メールサーバーのアドレスを入力します。
   - **暗号化**: E メールサーバーの暗号化タイプを選択します。
   - **ポート**:E メールサーバーに接続するポート番号を入力します。
5. **テストメールを送信する**をクリックして、設定をチェックします。設定が正しい場合、テストメールが受信トレイに届きます。
6. **OK** をクリックして、設定を保存します。

注意 今のところ、Capsa は AUTH LOGIN、 AUTH PLAIN、 AUTH NTLM、 ANONYMOUS という四つの認証タイプだけをサポートします。

アラーム音で通知

以下のステップに従い、アラーム音でアラームを通知します。

1. アラーム通知タブにおける**アラーム音で通知**にチェックを入れます。
2. ... をクリックして、音声ファイルを選択します。

解析プロファイル

セキュリティ解析に関する設定について、セキュリティ解析をご参照ください。

解析プロファイルについて

解析プロファイルは、解析プロジェクトの設定に利用され、柔軟且つ効率的な解析パフォーマンスを提供します。解析プロファイルにあるすべての設定は、プログラムさらにオペレーティングシステムがシャットダウンされても、プログラムに記憶され、他の解析プログラムに適用することもできます。

スタートページにおける**解析プロファイル**部分では、いくつかのビルトイン解析プロファイルがあります。

解析プロファイル	説明
フル解析	すべてのアプリケーションとネットワーク問題に対する包括的な解析を提供します。
トラフィックモニター	トラフィック統計と、MAC アドレス、IP アドレスおよびプロトコルを含むメインオブジェクトの効率的な解析を提供します。
セキュリティ解析	潜在的なネットワークセキュリティリスクの専用的な解析を提供します。
HTTP アプリケーション解析	Web アプリケーション(HTTP に基づく)を解析し、クライアントの web アクティビティと web 通信ログを記録します。
E メールアプリケーション解析	E メールアプリケーション(POP3 と SMTP に基づく)を解析し、E メール内容と添付ファイルをモニターし、E メールトランザクションを記録します。
DNS アプリケーシ	DNS アプリケーションを解析し、DNS アプリケーションエラーを診断し、

ョン解析	DNS アプリケーションログを記録します。
FTP アプリケーション解析	FTP アプリケーション(TCP ポート 21 と 20 に基づく)と FTP トランザクションログを解析します。
IM アナリシス	インスタントメッセンジャ解析を提供します。
VoIP 解析	VoIP コールに対する解析とトラブルシューティングを提供します。
プロセス解析	すべてのローカルプロセスに基づき、ネットワークトラフィック解析と統計を提供します。

特定のネットワークトラフィックを解析するには、特定の解析プロファイルが必要としています。解析プロファイルによって、ロードされている解析モジュールとキャプチャーフィルターも違っています。任意解析プロファイルを右クリックして、その解析プロファイルを編集、コピー、削除したり、新しい解析プロファイルを作成したりすることができます。

- 編集:**解析プロファイルの設定**ダイアログボックスを開き、選択された解析プロファイルを編集します。
- 新規作成:**解析プロファイルの設定**ダイアログボックスを開き、新しい解析プロファイルを作成します。
- コピー:選択された解析プロファイルをコピーして、変更を行います。
- 削除:選択された解析プロファイルを削除します。
- リセット:**解析プロファイル**をリセットします。

解析プロファイルの設定

このタブは、以下のように表示されます。

このタブは以下のアイテムから構成されています。

- **名前**:解析プロファイルの名前を入力します。
- **説明**:解析プロファイルに関する説明を入力します。
- **プロファイルアイコン**:**変更**ボタンをクリックして、解析プロファイルのイメージを選択します。
- **解析モジュール**:ネットワーク上のトラフィックを解析するための解析モジュールを有効にします。

解析オブジェクト

解析オブジェクトの設定は、プロトコル、アドレス、セッション、および最大オブジェクト数などをカスタマイズすることに利用されます。

このタブには三つのカラムがあります。

- **解析オブジェクト**:ネットワークプロトコル、物理アドレス、ローカル IP アドレス、リモート IP アドレス、物理アドレスグループ、IP アドレスグループ、物理セッション、IP セッション、TCP セッション、UDP セッション、VoIP コール、およびポートが含まれています。デフォルトでは、すべての解析オブジェクトにチェックが入っています。チェックが入っていないと、プログラムはその解析オブジェクトを解析しません。
  例えば、**ローカル IP アドレス**にチェックが入っていないと、**IP ブラウザ**におけるローカル IP アドレスと統計ビューにあるローカル IP アドレスに関するすべての統計を含め、ローカル IP アドレスに基づくすべての統計情報は、利用できなくなります。
- **解析プロトコルの詳細**:**プロトコル**ビューで詳細なトラフィック情報を表示するかどうかを設定します。以下の表は、このカラムが有効になっている時の機能をリストしています。

解析オブジェクト	機能
物理アドレス	**物理ブラウザ**である MAC アドレスが選択された時、**プロトコル**ビューは詳細なプロトコル統計情報を表示します。そして**プロトコル**ビューにおける**物理エンドポイント** z

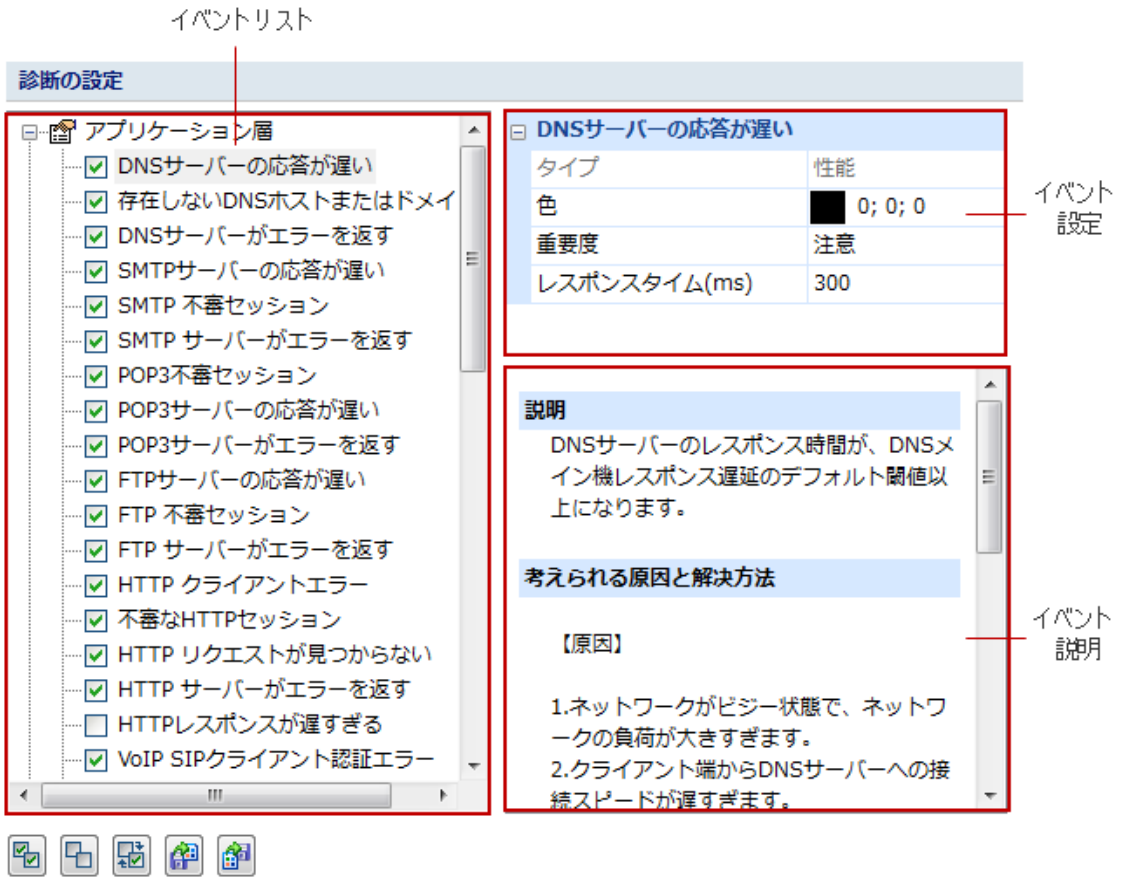
ローカル IP アドレス	カラム**解析プロトコルの詳細**が選択され、さらに **IP ブラウザ**であるローカル IP アドレスが選択された場合、**プロトコル**ビューは詳細なプロトコル統計情報を表示します。そして**プロトコル**ビューにおける **IP エンドポイント**タブは単一ローカル IP アドレスの詳細なトラフィック情報を表示します。
リモート IP アドレス	**IP ブラウザ**であるリモート IP アドレスが選択された時、**プロトコル**ビューは詳細なプロトコル統計情報を表示します。そして**プロトコル**ビューにおける **IP エンドポイント**タブは単一リモート IP アドレスの詳細なトラフィック情報を表示します。
物理アドレスグループ	**物理ブラウザ**である MAC アドレスグループが選択された時、**プロトコル**ビューは詳細なプロトコル統計情報を表示します。そして**プロトコル**ビューにおける**物理エンドポイント**タブは MAC アドレスグループの詳細なトラフィック情報を表示します。
IP アドレスグループ	**IP ブラウザ**である IP アドレスグループが選択された時、**プロトコル**ビューは詳細なプロトコル統計情報を表示します。そして**プロトコル**ビューにおける **IP エンドポイント**タブは IP アドレスグループの詳細なトラフィック情報を表示します。
物理セッション	**物理ブラウザ**で IP アドレスノードを除く任意ノードが選択された時、**プロトコル**ビューにおける**物理セッション**タブは MAC アドレスセッションの詳細なトラフィック情報を表示します。
IP セッション	**IP ブラウザ**での任意ノードまたは、**物理ブラウザ**における IP アドレスノードが選択された時、**プロトコル**ビューにおける **IP セッション**タブは IP アドレスセッションの詳細なトラフィック情報を表示します。

- **最大オブジェクト数**: 各解析オブジェクトの最大オブジェクト数で、デフォルトでは 10,000 となります。その数字をクリックして、設定することができます。設定可能な範囲は 1 から 100,000 までです。

リセット:このタブにおける設定をリセットします。

診断

このタブは現在の解析プロジェクトでロードされる解析モジュールのすべての利用可能な診断イベントをリストします。すべての診断イベントはプロトコル層によって分けているので、ネットワーク問題がどのプロトコル層に属しているかを簡単にわかることができます。**診断**タブは以下のように表示されています。



このタブは三つの部分から構成されています。

- **イベントリスト**:現在解析プロファイルのすべての利用可能な診断イベントをリストします。発生したイベントは、イベントリスト部分で有効にされた場合にのみ、**診断**ビューに表示されます。
- **イベント設定**:色、重要度および他のパラメータオプションをクリックすることで、イベントリストで選択されたイベントの設定を修正することができます。イベントによって、修正できるパラメータオプションが違います。
- **イベント説明**:.イベント説明、考えられる原因と解決方法を提供することで、ネットワーク問題が発生すると、迅速にネットワーク問題をトラブルシューティングすることができます。

以下のリストはこのタブにおけるボタンについて説明しています。

 :リストにおけるすべての診断イベントを有効にします。

 :リストにおけるすべての診断イベントを無効にします。

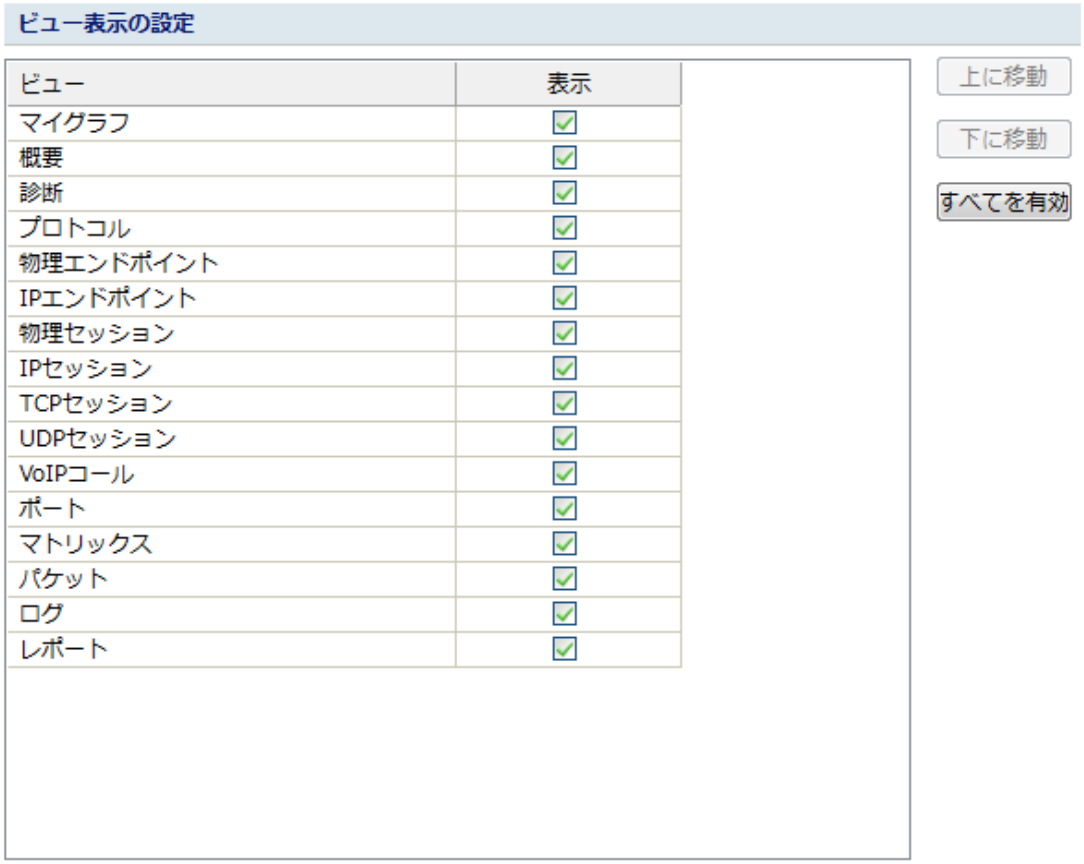
 :リストにおける診断イベントの選択を反転します。

 :.cscdiag ファイルから診断イベントの設定をインポートします。

 :現在の診断イベントの設定を.cscdiag ファイルにエクスポートします。

ビュー表示

このタブは、表示または非表示する統計ビューを指定したり、統計ビューの表示順序を設定したりするために設けられたものです。



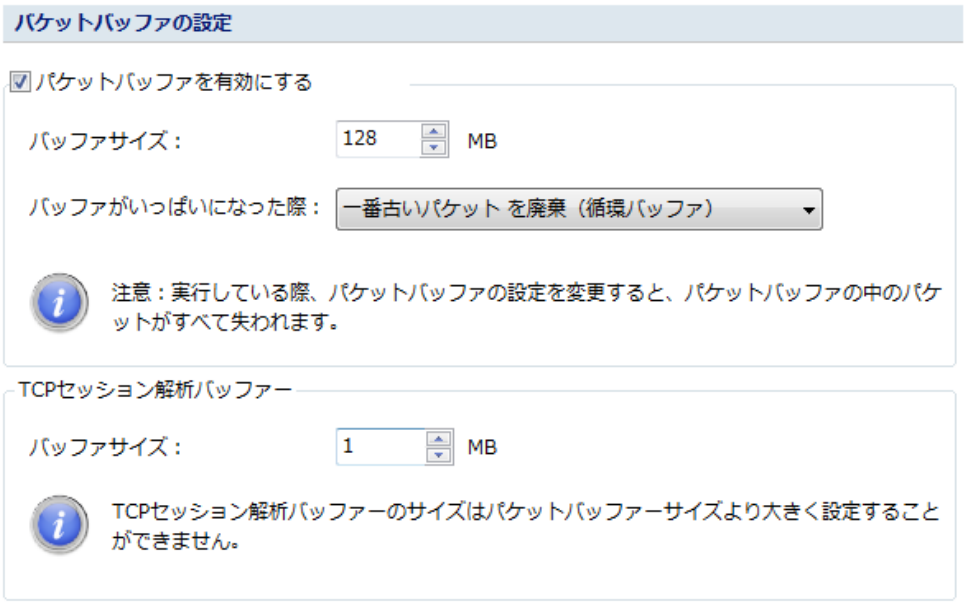
フル解析では、デフォルトですべての解析ビューが表示されることになります。

ある統計ビューを非表示するには、**表示**カラムにあるチェックを外せばよいのです。

上に移動、または**下に移動**をクリックして、統計ビューの表示順序を変更することができます。

パケットバッファ

パケットビューに表示されるすべてのパケットは**パケットバッファ**に保存されています。従って**パケット**ビューに表示されるパケット数は、バッファサイズによって決められています。



パケットバッファを有効にする

パケットバッファはパケットを保存するために、有効されています。この機能が無効にされると、**パケット**ビューにおける詳細なパケットデコード情報、**TCP セッション**ビューにおける**パケット**タブ、**データフロー**タブ、**シーケンスチャート**タブの統計、**パケット**ウィンドウと **TCP フロー解析**ウィンドウの統計を含む、パケットに基づくすべての統計情報は利用できません。

バッファサイズ

バッファサイズを変更することができますが、システムメモリを考慮に入れる必要があります。

ヒント パケットバッファサイズをオペレーティングシステムの使用可能な物理メモリの半分以下に設定することをお勧めします。

バッファがいっぱいになった際

パケットバッファがキャプチャーされたパケットでいっぱいになった際、次の操作を選択することができます。

- **一番旧いパケットを廃棄(循環バッファ)**
  最新のパケットを保存するために一番古いパケットを廃棄することをお勧めします。
- **新しくキャプチャーしたパケットを廃棄**
  すべての新しくキャプチャーされたパケットは解析された後、パケットバッファに保存されなく、廃棄されます。
- **すべての旧いパケットを廃棄**
  プログラムはパケットバッファを空にして、新しいパケットをバッファに保存します。
- **キャプチャー、あるいはリプレイを停止**
  現在実行しているキャプチャー、またはリプレイを停止します。

注意 キャプチャーするときに、すべてのパケットを見逃したくない場合、パケット保存をご参照ください。そこですべてのパケットを保存する方法を学ぶことができます。

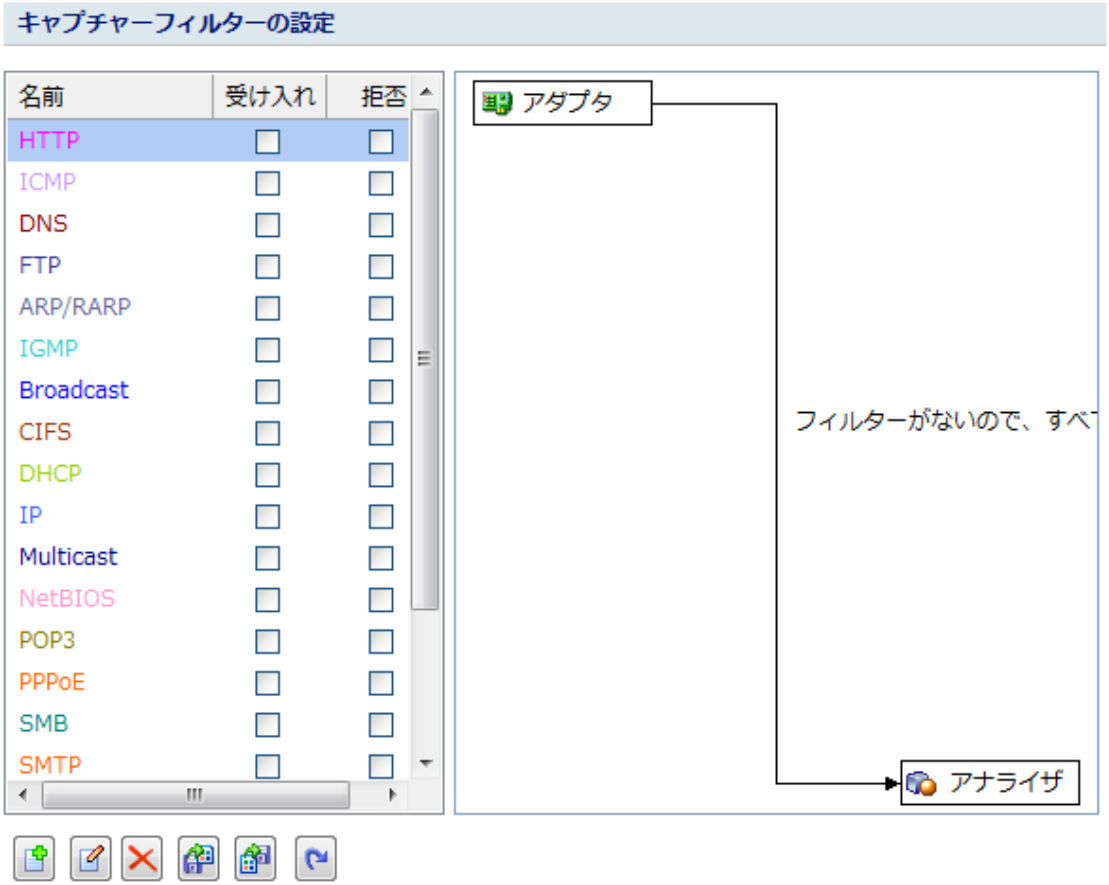
TCP セッション解析バッファ

TCP セッション解析バッファは、TCP フローのパケットをバッファリングするためのものです。TCP セッションビューにおける TCP セッション記録をダブルクリックすることで、TCP フロー解析ウィンドウが開かれます。TCP フロー解析ウィンドウが開かれると、TCP セッション解析バッファが使用されます。

キャプチャーフィルター

このタブはキャプチャーフィルターを設定したり、適用したりするためのものです。キャプチャーフィルターは特定のパケットを分離することに利用されています。有効にされているフィルターがない場合、Capsa はアダプタを介して転送されたすべてのパケットをキャプチャーし、解析します。フィルターが作成された後、任意の解析プロジェクトに適用することができます。

このタブには、左側のパネルと右側のパネルが含まれています。



左側パネルは、ビルトインフィルターとユーザー定義のフィルターを含め、すべての利用可能なフィルターをリストします。各フィルターは、**受け入れ**と**拒否**という二つのオプションがあります。**受け入れ**は、フィルターに一致しているパケットだけが Capsa にキャプチャーされるということを意味します。**拒否**は、フィルターに一致していないパケットだけが Capsa にキャプチャーされるということを意味します。有効にされているすべてのフィルターは OR 関係で結ばれています。

右側のパネルは、**受け入れ**フィルターと**拒否**フィルターを含む、フィルターリストで選択されたすべてのフィルターアイテムを表示するフィルターフローチャートです。フィルターに変更が行われると、この部分が更新されます。フローチャートにおけるフィルターをダブルクリックすることで、フィルターを修正することができます。

ボタン

ここには、キャプチャーフィルターを設定するボタンが六つあります。

 :新しいフィルターを作成します。

 :選択されたフィルターを修正します。

 :選択されたフィルターを削除します。

 :保存されたフィルターファイルを現在のフィルターリストにインポートします。フィルターファイルがインポートされると、現在のリストにおける全てのフィルターは削除されます。

 :現在のフィルターリストにおける全てのフィルター設定をディスクにエクスポート、保存します。

 : フィルターをデフォルトにリセットします。

キャプチャーフィルターを作成するには、

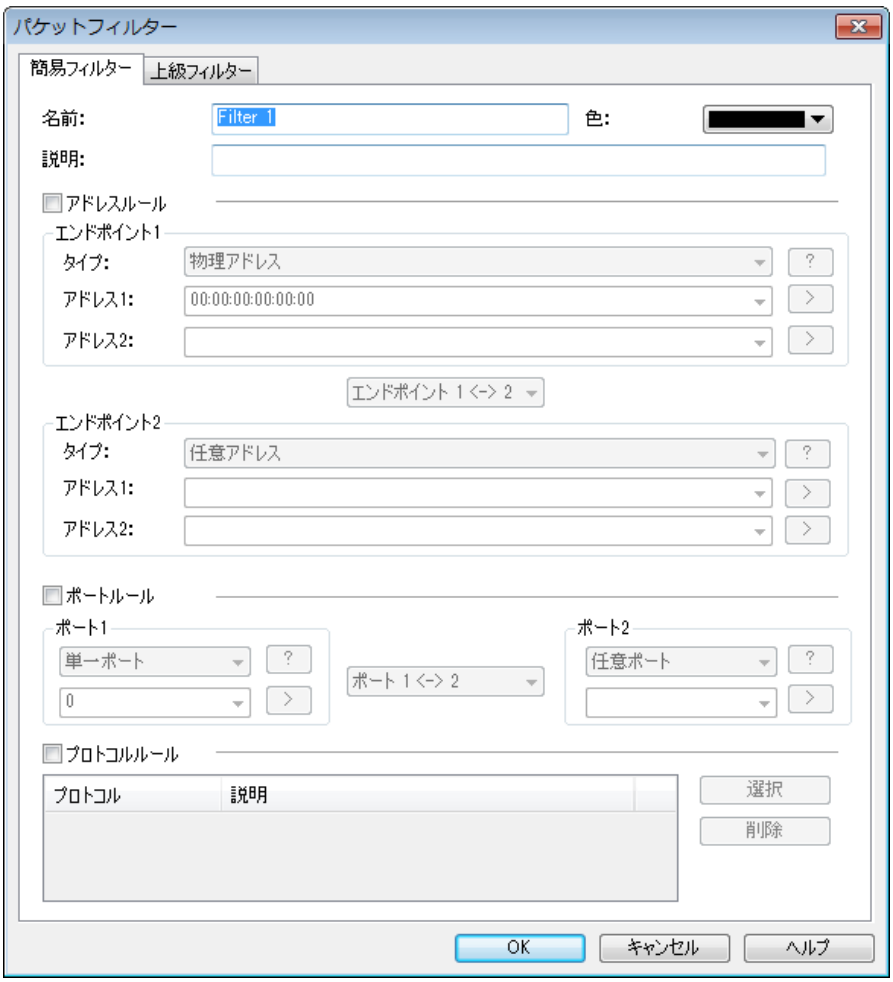
1. **解析プロファイルの設定**ダイアログボックスにおけるキャプチャーフィルタータブで  をクリックして、**パケットフィルター**ダイアログボックスを開きます。
2. 簡易フィルター、または上級フィルターを選択して、フィルター名、フィルター説明、およびフィルタールールを含め、フィルターを設定します(詳しいことは簡易フィルターを作成と上級フィルターを作成をご参照ください)。
3. **パケットフィルター**ダイアログボックスにおける OK をクリックして、**解析プロファイルの設定**ダイアログボックスにおける OK をクリックします。

注意 フィルターを作成した後、**受け入れ**、または**拒否**にチェックを入れ、フィルターを適用する必要があります。

キャプチャー中、選択されたオブジェクトに基づいて、キャプチャーフィルターを作成することができます。

簡易フィルターを作成

フィルターを作成するとき、簡易フィルターを作成するか、上級フィルターを作成するかを選択することができます。簡易フィルタータブは以下のように表示されます。



簡易フィルタータブでは、アドレス、ポート、およびプロトコルによる簡易なフィルターを作成することができます。二つ、または三つのルールが設定されると、これらのルールは「And」関係で結ばれます。すなわち、フィルターに一致するには、パケットは全ての条件に一致する必要があります。

区別や読みやすさを考えて、ここで名前、色、および説明を指定することができます。

正確にパケットをキャプチャーするために、IP アドレスルール、MAC アドレスルール、およびポートルールにおいて、パケットの転送方向（エンドポイント 1 -> エンドポイント 2、エンドポイント 2 -> エンドポイント 1、およびエンドポイント 1 <-> エンドポイント 2）を指定することができます。簡易フィルターでは、アドレス、ポート、およびプロトコルルールの条件を組み合わせて、フィルターをカスタマイズすることができます。

ヒント さらに上級フィルタータブで簡易フィルターを定義することもできます。

アドレスルールを定義する

以下のステップに従い、アドレスルールを定義します。

1. **アドレスルール**にチェックを入れます。
2. **エンドポイント 1** において、アドレスタイプを選択します。MAC アドレス、IP アドレス、IP 範囲、IP サブネットから選択することができます。
3. **アドレス 1** と**アドレス 2** にアドレスを入力します。アドレスタイプに IP 範囲が選択された場合にのみ、アドレス 2 が利用可能となります。
4. 方向ドロップダウンリストボックスをクリックし、パケット転送方向を選択します。
5. **エンドポイント 2** において、アドレスタイプを選択し、アドレスを入力します。
6. **パケットフィルター**ダイアログボックスにおける **OK** をクリックします。

ヒント アドレス形式に詳しくない場合、アイコンをクリックして、アドレス形式ダイアログボックスがポップアップされます。そして、 アイコンをクリックすると、入力された全ての項目が削除されます。

ポートルールを定義する

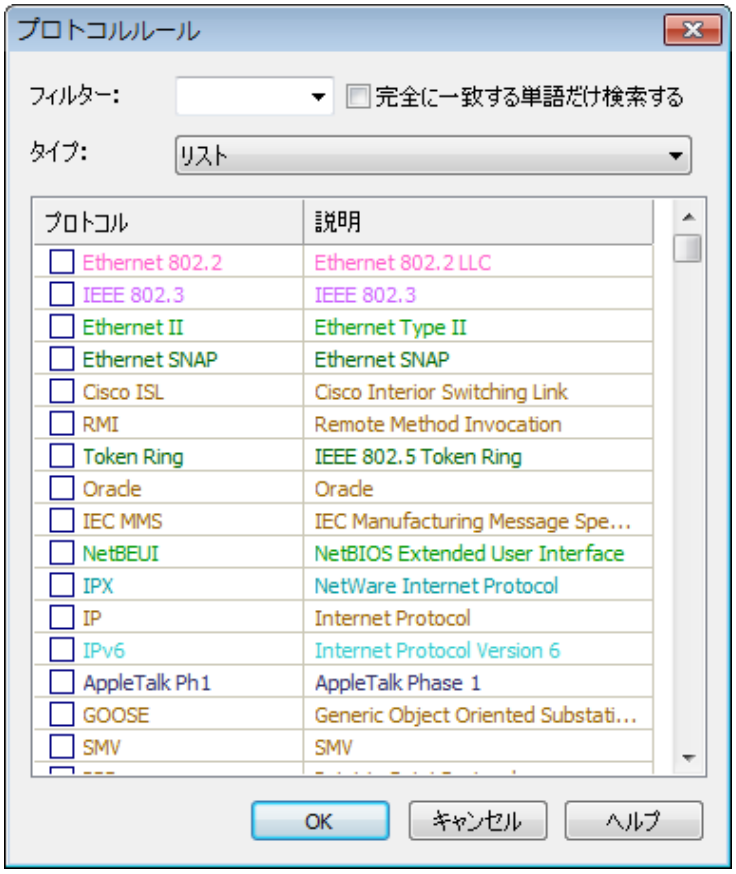
以下のステップに従い、ポートルールを定義します。

1. **ポートルール**にチェックを入れます。
2. **ポート 1** において、ポートタイプを選択します。単一ポート、ポート範囲、および複数ポートから選択することができます。
3. ポートタイプの下にあるテキストボックスにポート番号を入力します。
4. 方向ドロップダウンリストボックスをクリックし、ポート間のパケット転送方向を選択します。
5. **ポート 2** において、ポートタイプを選択し、その下にあるテキストボックスにポート番号を入力します。
6. パケットフィルターダイアログボックスにおける OK をクリックします。

プロトコルルールを定義する

以下のステップに従い、プロトコルルールを定義します。

1. **プロトコルルール**にチェックを入れます。
2. **選択**をクリックすることで、下図のようにプロトコルルールダイアログボックスが表示されます。

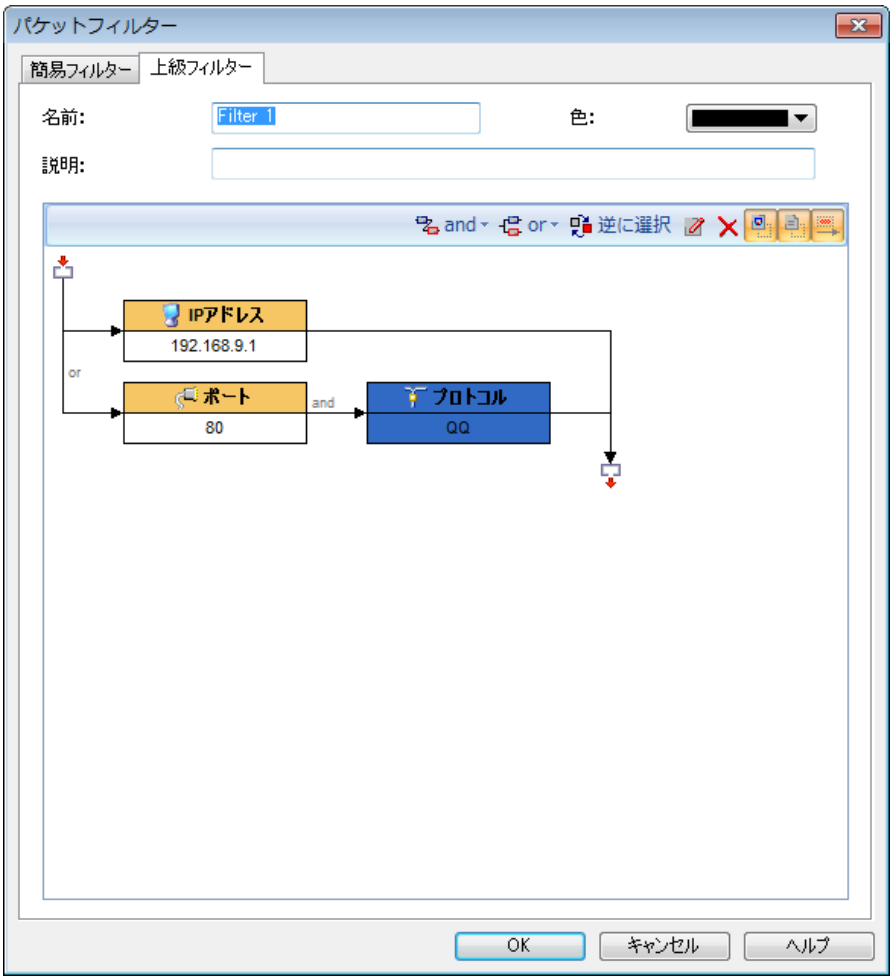


3. 適切なプロトコルを選択し、**OK** をクリックします。
4. パケットフィルターダイアログボックスにおける OK をクリックします。

選択されたプロトコルは、**プロトコルルール**部分にリストされます。**削除**ボタンを使用して、リストからプロトコル項目を削除することができます。

上級フィルターを作成

上級フィルターは以下のように表示されます。



フィルタールールはフィルター関係マップによって表示されます。関係マップはアダプタから解析プロジェクトまでルール間の論理的関係を示しています。ルールをダブルクリックして、修正することができます。

ツールバー

ツールバーには、以下のアイテムが含まれています。

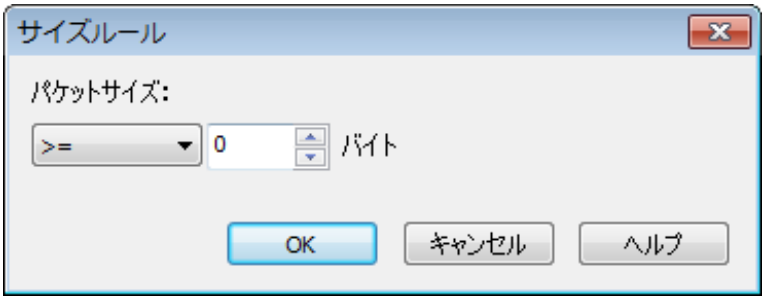
- And: この部分で入力されたルールは「ANd」関係で結びます。
- Or: この部分で入力されたルールは「Or」関係で結びます。
- 逆に選択:条件に一致していないパケットだけがキャプチャーされます。「逆に選択」関係ルールは赤でマークされます。
- :選択されたルールを修正します。
- :選択されたルールを削除します。
- :各ルールのアイコンを表示します。
- :各ルールの詳細を表示します。
- : ルール間の論理的関係を表示します。

上級フィルターにはアドレス、ポート、プロトコル、サイズ、値、パターンという六種類のルールがあります。アドレス、ポートとプロトコルのルールは簡易フィルターと同じです（詳しいことについては、簡易フィルターを作成をご参照ください）。

パケットサイズルールを定義する

パケットサイズルールはパケットのサイズに関するルールを定義するものです。ルールを満たす大きさのパケットだけがキャプチャーされます。

パケットサイズルールを定義するには、ツールバーにおける And、または Or をクリックし、**サイズ**を選択することで、下図のように**サイズルール**ダイアログボックスが表示されます。

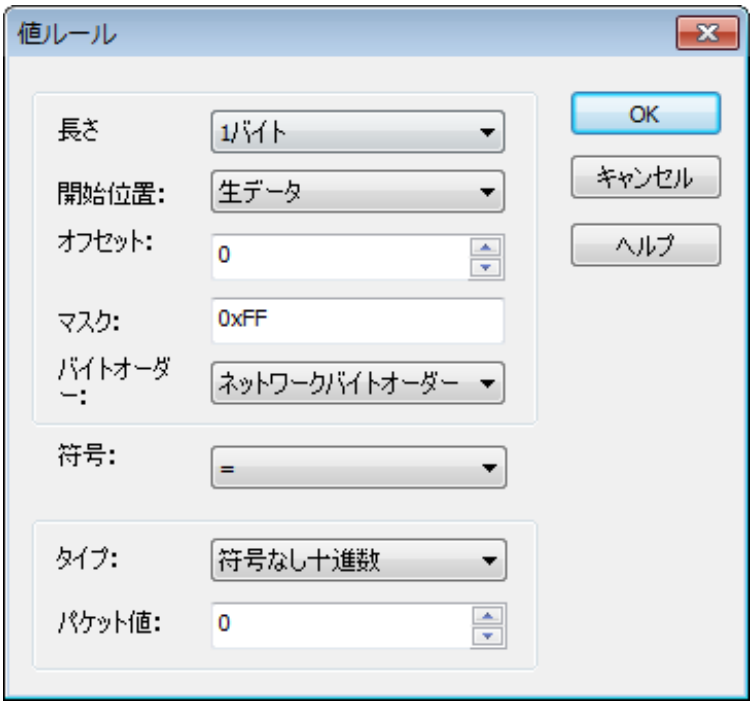


<（より小さい）、>（より大きい）、<=（小なりイコール）、>=（大なりイコール）、=（イコール）、!=（等しくない）、範囲（パケットサイズ範囲）を選択して、パケットサイズルールを定義することができます。

値ルールを定義する

値ルールは、パケットにおけるデコードされたフィールド値のルールを定義するものです。

値ルールを定義するには、ツールバーにおける And、または Or をクリックし、**値**を選択することで、**値ルール**ダイアログボックスが表示されます。



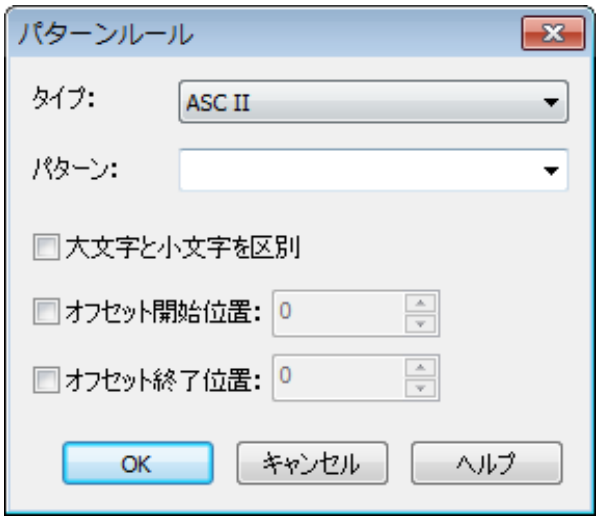
- 長さ:マスクの長さを指定します。1 バイト、2 バイト、と 4 バイトから選択することができます。
- 開始位置:パケットにおけるオフセットの開始位置を指定します。生データ、IP ヘッダー、ARP ヘッダー、TCP ヘッダー、および UDP ヘッダーから選択することができます。
- オフセット: オフセットされたバイトを指定します。
- マスク: パケット値の 16 進数マスクを入力します。
- バイトオーダー: バイトのオーダーで、ネットワークバイトオーダーとホストバイトオーダーから選択することができます。
- 符号: <（より小さい）、>（より大きい）、<=（小なりイコール）、>=（大なりイコール）、=（イコール）、!=（等しくない）から選択することができます。
- タイプ: パケット値のタイプで、2 進数、8 進数、符号なし 10 進数、16 進数から選択することができます。
- パケット値: このルールのパケット値を入力します。

値ルールが有効になっている場合、パケットにおける指定されたバイト数とマスクの間で And 演算を行い、そして演算結果をそのルールのパケットと比較します。比較した結果が一致した場合、そのパケットがキャプチャーされ、そうでなければ、パケットは除外されます。

パターンルールを定義する

パターンルールはパケットのコンテンツに関するルールを定義するものです。

パターンルールを定義するには、ツールバーにおける **And**、または **Or** をクリックし、**パターン**を選択することによって、下図のように**パターンルール**ダイアログボックスが表示されます。そして、パターンのタイプを選択し、パターンを入力し、オフセットオプションを設定して、**OK** をクリックします。

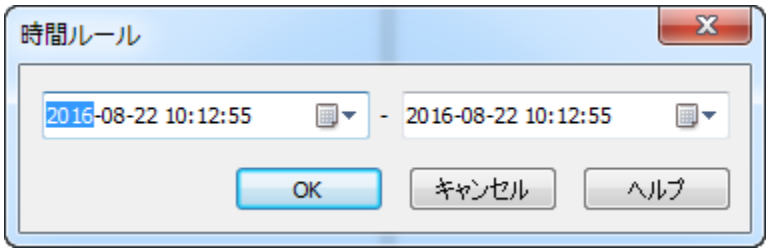


オフセットの単位はバイトです。

時間ルールを定義する

時間ルールはパケットの時間に関するルールを定義するものです。つまり時間ルールを設定することで、設定された時間に基づきパケットをフィルターすることができます。

時間ルールを定義するには、ツールバーにおける And 、または Or をクリックし、 時間を選択することによって、下図のように時間ルールダイアログボックスが表示されます。時間範囲を設定して、OK をクリックします。



注意 上級フィルターは簡易フィルターに変換することもできますが、上級フィルターは簡易フィルターより多くのフィルター条件を持っているので、変換されると、いくつかのフィルタールールが失われます。

パケット保存

パケットビューにおけるすべてのパケットを自動的に保存したい場合、**パケット保存**を有効にすることができます。

パケットをディスクに保存する

この機能は、パケットを自動的に.rawpkt ファイルに保存するために設けられています。

- **パケットサイズ制限**:各パケットのサイズを制限します。この機能を有効にすると、**パケット**ビューは指定されたサイズのパケットだけをデコードします。パケットの詳細なデコード情報を表示したい場合、この機能を無効にすることをお勧めします。
- **単一ファイル**:すべてのパケットを一つのファイルに保存します。
- **分割ファイル**:すべてのパケットは時間やサイズによって分割され、複数ファイルとして保存します。合計サイズを減らすには、最近のファイルを保存することを選択することができます。
- **フォルダに保存**:分割されたパケットファイルを保存するパスを指定します。
- **ベースファイル名**:ファイル名のプレフィックスで、  をクリックして、例を表示することができます。
- **ファイルタイプ**：パケットファイルを保存するファイルタイプを指定します。
- **ファイル分割間隔**:ファイルサイズが大きすぎる場合、パケットファイルを分割する間隔を指定することができます。時間やサイズによって、ファイルを分割することができます。
- **すべてのファイルを保存する**:すべての分割ファイルを保存します。
- **最近の＊＊個ファイルを保存する**:保存する最近の分割ファイルを指定します。

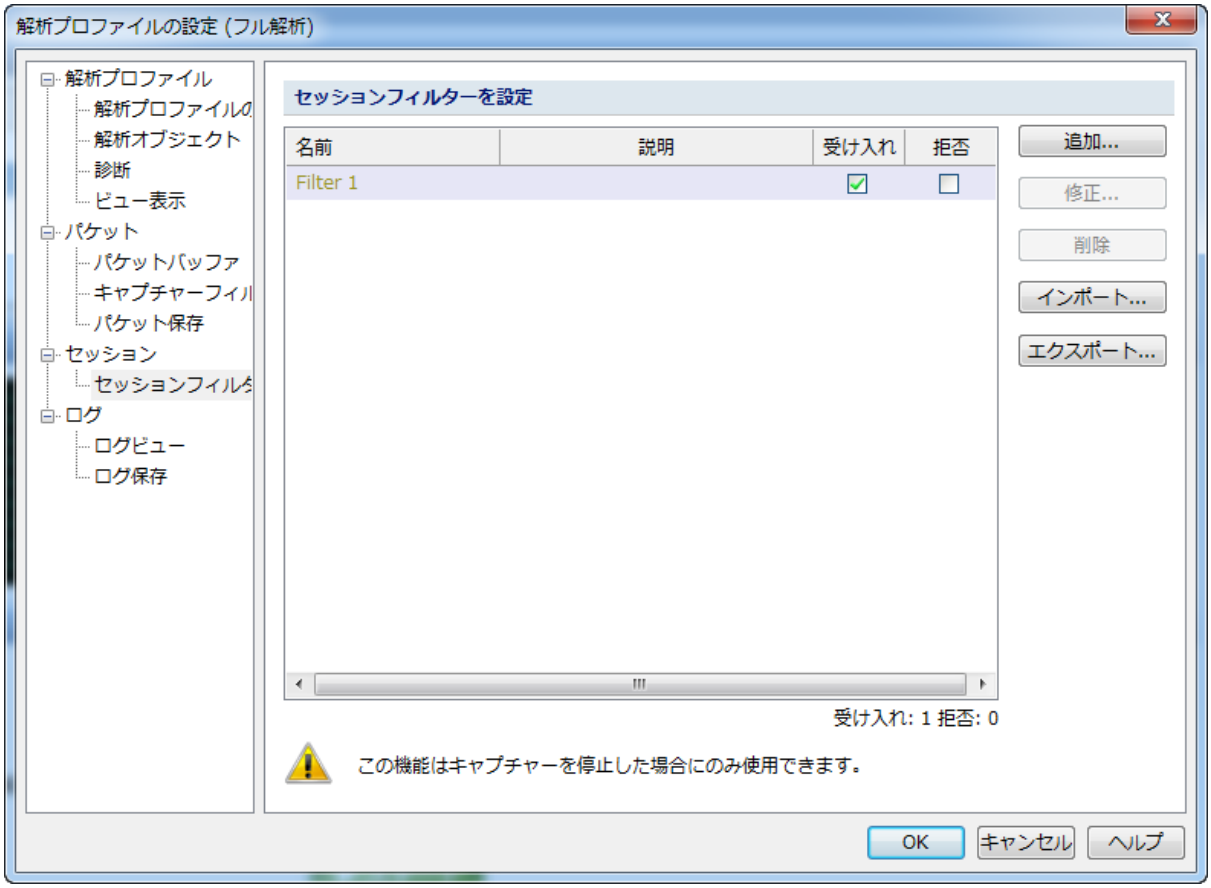
パケットバッファとパケット保存の区別

パケットバッファはパケットビューにおけるパケットをバッファリングするためのものです。例えば、30M のトラフィックをキャプチャーした場合、パケットバッファサイズを 16MB に設定すると、パケットビューは 16MB のパケットだけを表示します。残りの 14MB のパケットは、バッファサイズが不十分なため廃棄されます。30MB のパケットが全部 Capsa によって解析されたが、パケットビューに表示できるのは、16MB のパケットだけです。すなわちパケットバッファサイズはパケットビューに表示できるパケット数だけに影響します。

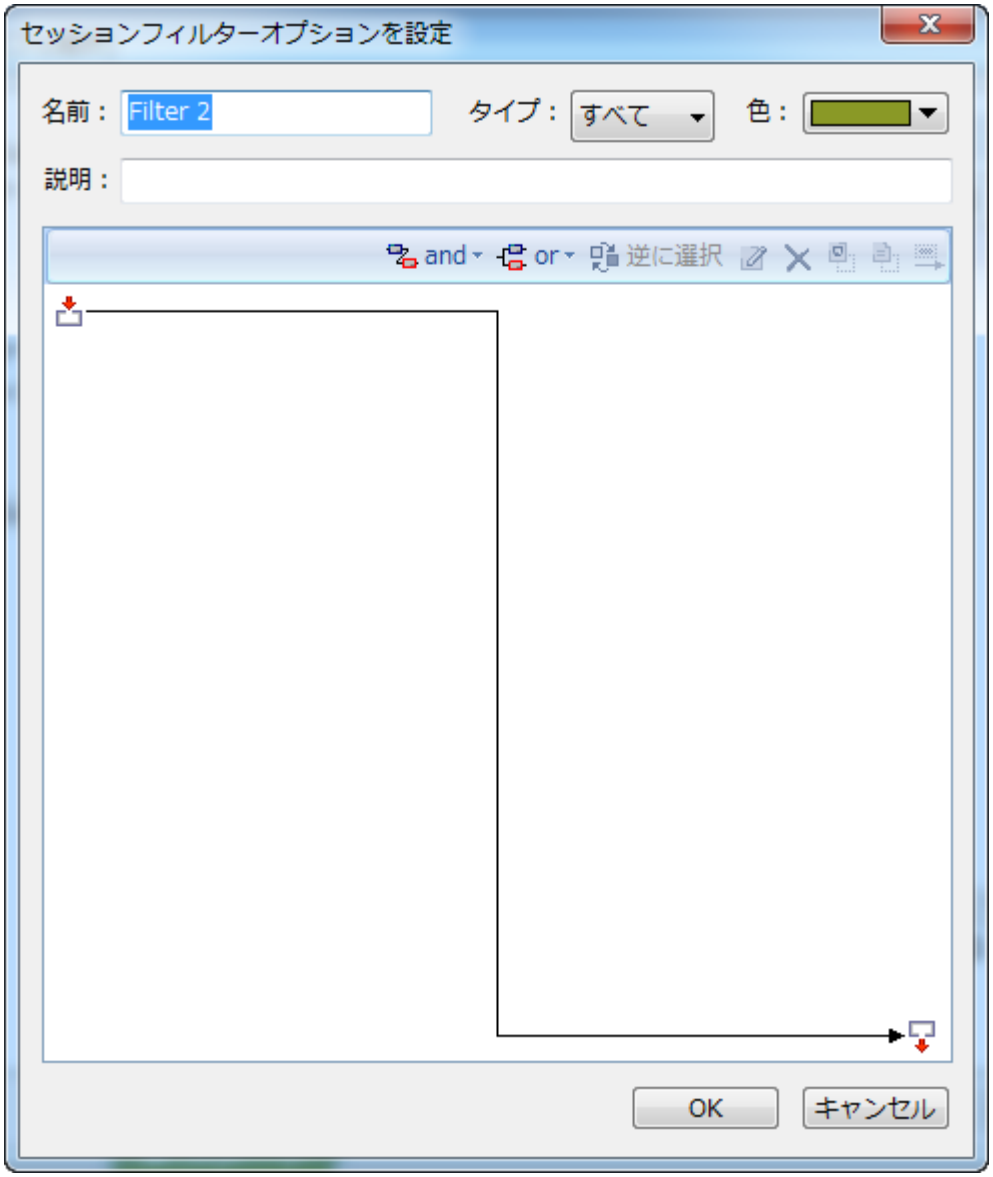
パケット保存は、キャプチャーの開始から終了までのすべてのパケットを自動的に保存するためのものです。パケットバッファとは関係がありません。パケットバッファサイズと関係なく、パケット保存機能を有効にすると、Capsa はすべてのパケットを保存します。

セッションフィルター

プロジェクトを開始する前に、下図のようにセッションフィルターを設定することで、特定のセッションパケットをキャプチャーすることができます。



追加ボタンをクリックして、セッションフィルターを追加することができます。

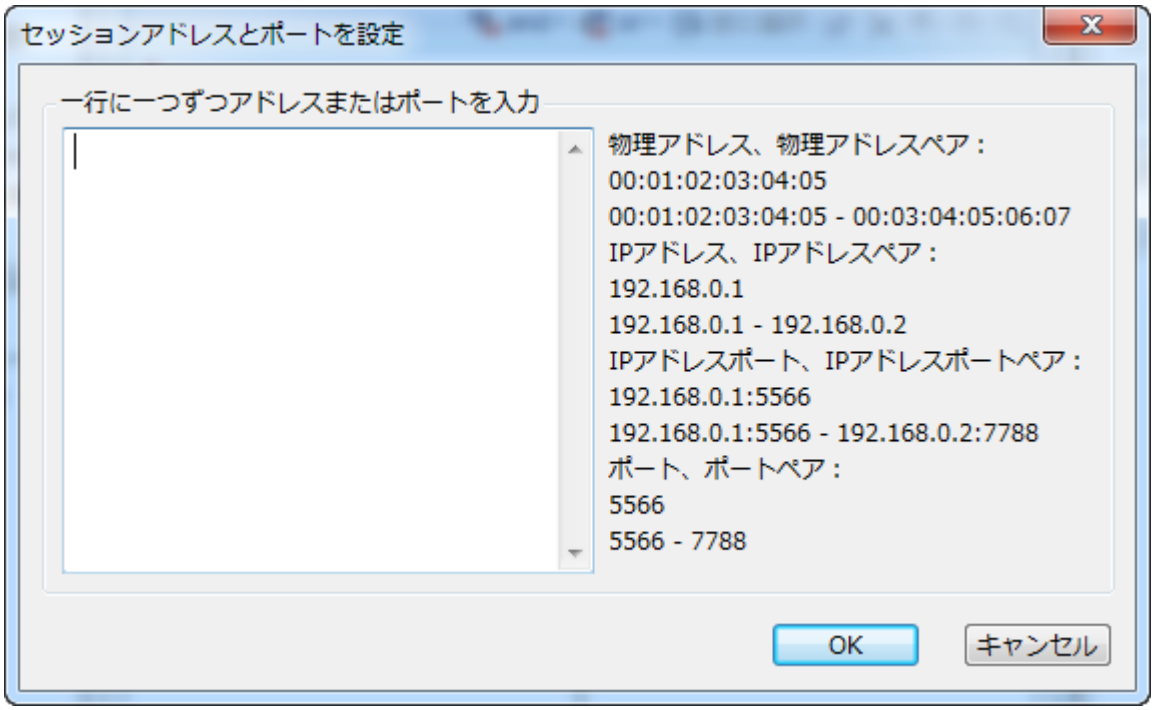


セッションフィルターで以下のアイテムを設定することができます。

アイテム	説明
名前	フィルターの名前を設定します。
タイプ	MAC セッション、IP セッション、TCP セッション、及び UDP セッションという四つのセッションフィルターを提供します。ドロップダウンボックスから一つ、または全てを選択することができます。
色	色を選択し、フィルターの名前を色づけることができます。
説明	フィルターについて簡単な説明を入力します。
ルール	1. アドレスとポート、ロケーション、セッションプロトコル、セッションパケット、セッションコンテンツ、及びセッションオプションという六つのルールを提供します。 2. 複数ルールを設定することができます。更に複数ルールの間では、and 関係または or 関係で結ばれることができます。

アドレスとポートルール

アドレスまたはポートを入力し、入力されたアドレスまたはポートに基づきセッションをフィルターします。

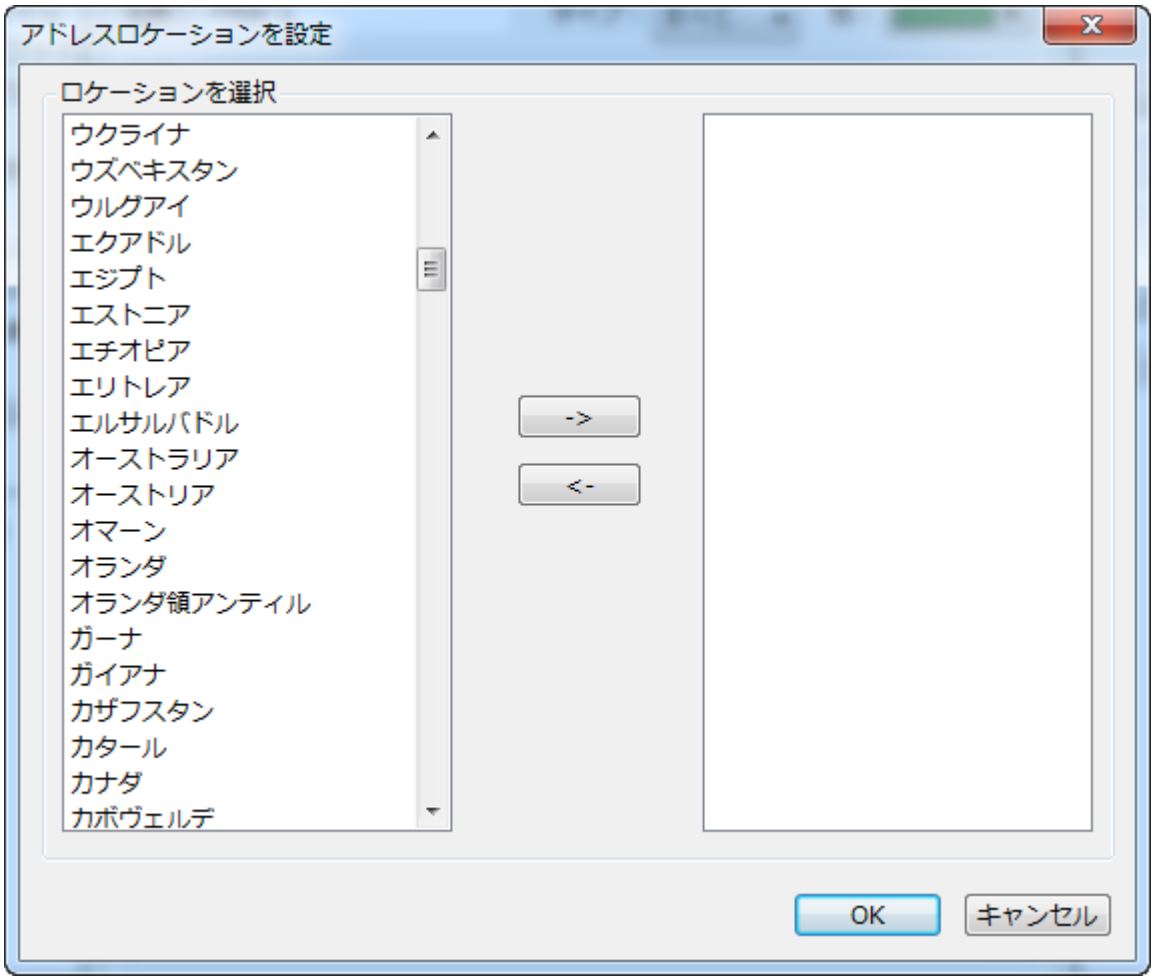


下図で表示されるようにアドレスとポートルールには、以下の四つのタイプがあります。タイプにより、フィルターされたセッションは違います。

- 物理アドレス、物理アドレスペア: MAC アドレスに基づき、セッションをフィルターします。
- IP アドレス、IP アドレスペア: このタイプのルールは IP セッション、TCP セッション、及び UDP セッションに対してのみ有効です。
- IP アドレスポート、IP アドレスポートペア: TCP セッションと UDP セッションに対して、Capsa は IP アドレスポート/IP アドレスポートペアに基づきセッションをフィルターします。IP セッションに対して、Capsa は設定された IP アドレス/IP アドレスペアのみに基づきセッションをフィルターします。
- ポート、ポートペア: TCP セッションと UDP セッションに対してのみ有効です。

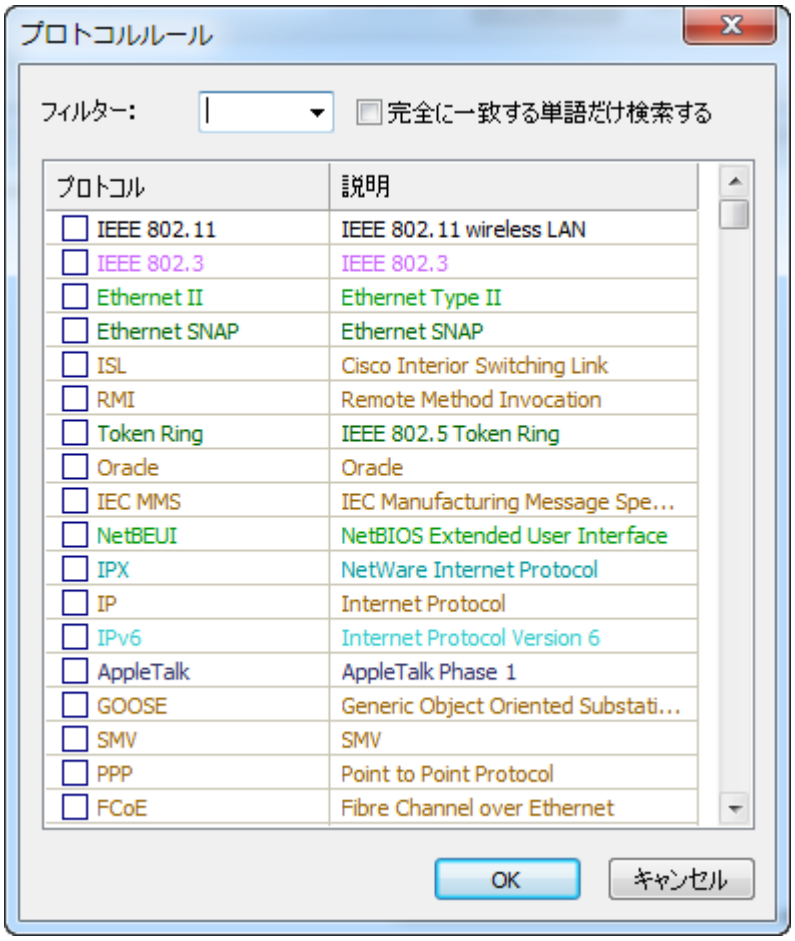
ロケーションルール

Capsa では、セッション IP アドレスのロケーションに基づき、セッションをフィルターすることができます。物理セッションにおいて、ロケーションに基づき、セッションをフィルターすることはサポートしません。



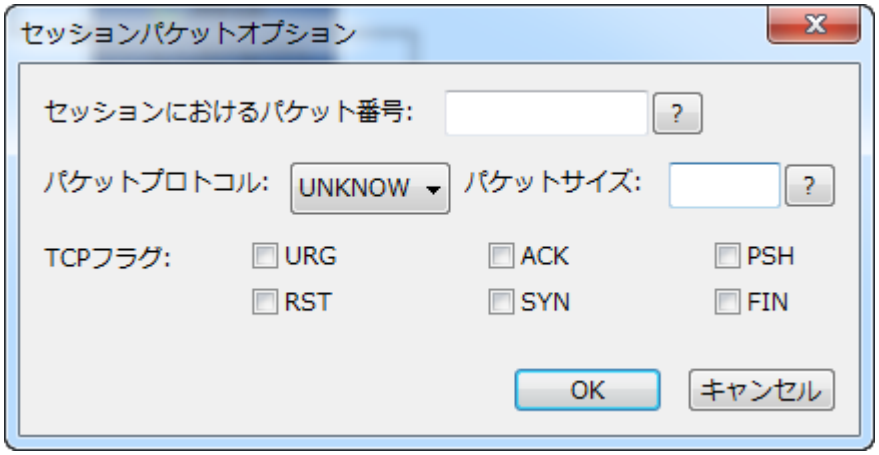
セッションプロトコルルール

一つまたは複数のプロトコルを選択します。Capsa は選択されたプロトコルに基づきセッションをフィルターします。



セッションパケットルール

セッションパケットについて設定することで、設定されたセッションパケットをフィルターします。



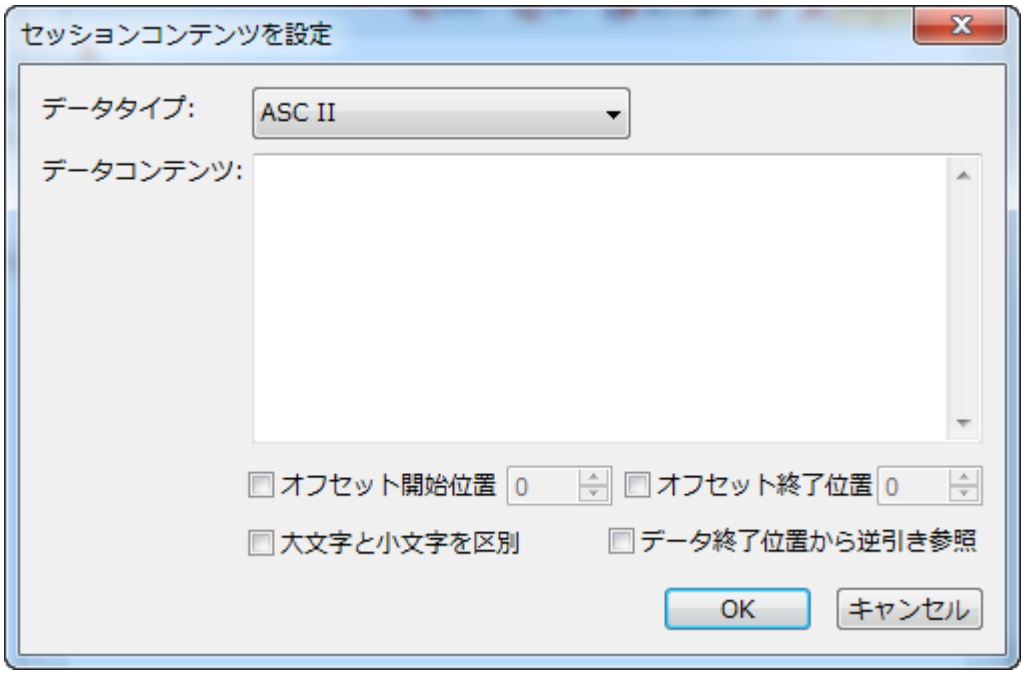
- セッションにおけるパケット番号：セッションにおけるパケットの番号を設定します。
- パケットプロトコル：パケットのプロトコルタイプを選択します。

- パケットサイズ：この番号のパケットのサイズを設定します。
- TCP フラグ：この番号のパケットのフラグにチェックを入れます。これは TCP セッションに対してのみ有効です。

注意 「セッションにおけるパケット番号」は必需設定アイテムです。パケットサイズと TCP フラグはその中の一つを設定する必要があります。両方とも設定することもできます。

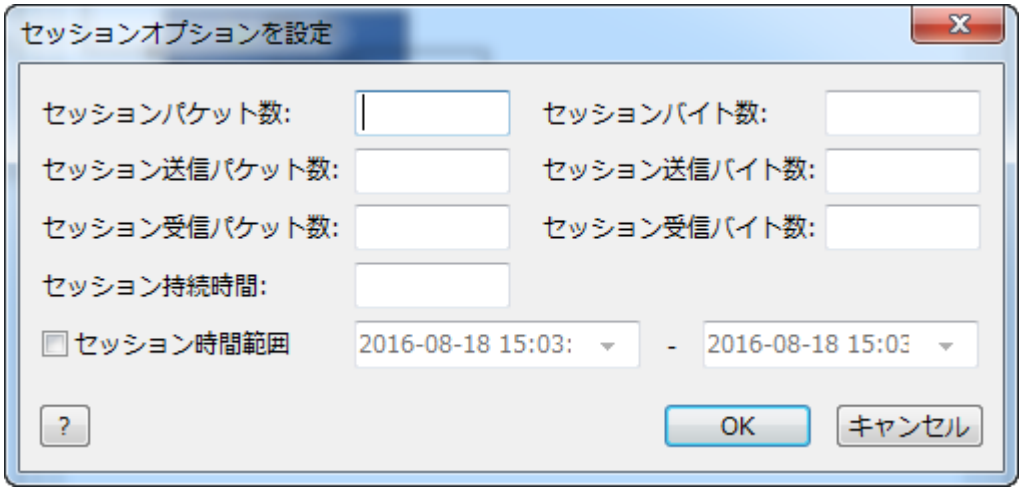
セッションコンテンツ

Capsa ではセッションコンテンツに基づきセッションをフィルターすることができます。セッションコンテンツを設定するとき、コンテンツのデータタイプ（例えば、ASCII、HEX、UTF-8、UTF-16）を選択することができます。同時に、セッションコンテンツのオフセット位置などを設定することができます。



セッションオプション

Capsa では、セッションオプションに基づきセッションをフィルターすることができます。セッションオプションを設定するダイアログボックスは下図のように表示されます。



- セッションパケット数：セッションに含まれるパケット数です。
- セッションバイト数:セッションの総通信バイト数です。
- セッション送信パケット数：セッションが送信したパケット数です。
- セッション送信バイト数:セッションが送信したバイト数です。
- セッション受信パケット数：セッションが受信したパケット数です。
- セッション受信バイト数:セッションが受信したバイト数です。
- セッション持続時間:セッションの持続時間です。
- セッション時間範囲:特定時間範囲内のセッションをフィルターします。

フィルターの設定が完了したら、設定されたフィルターを受け入れまたは拒否することができます。

- 受け入れ：セッション統計では、このフィルターのルールと一致したセッションを表示します。
- 拒否：セッション統計では、このフィルターのルールと一致しないセッションを表示します。

「エクスポート」ボタンをクリックすることで、作成されたフィルターを.csconvflt ファイルにエクスポートすることができます。同時に、「インポート」ボタンをクリックすることで、ローカルの.csconvflt ファイルを Capsa にインポートすることができます。

ログビュー

Capsa は DNS、HTTP、 E メール、FTP トラフィックなど、アプリケーション層のトラフィックを解析し、記録することができます。そして、MSN と Yahoo メッセンジャーのチャットメッセージを監視します。このタブではログビューで表示するログのタイプとバッファサイズを指定することができます。

このタブは二つのカラムから構成されています。

- **ログタイプ**:**ログ**ビューで表示するログタイプを指定します。
  ヒント **診断ログ**が選択されると、**診断**ビューにおける**診断イベント**パネルでイベントの詳細な情報を表示します。そうしないと、**診断イベント**パネルでは、表示するアイテムがありません。
- **ログバッファサイズ**:各ログタイプの表示バッファを設定します。番号をクリックして、サイズを変更することができます。各ログバッファの最大値は 16MB です。

注意 ログバッファサイズを小さくした場合、一番旧いログデータは廃棄される可能性があります。

ログ保存

ログビューにおけるログ記録を自動的に保存したい場合、**ログ保存**を有効にすることができます。

以下のリストはこのタブにおけるオプションについて説明しています。

- **ファイルパス**:ログファイルを保存するフォルダを指定します。
- **フォーマット**:保存するログファイルフォーマットを選択します。
- **ファイル分割間隔**:ログファイルが大きすぎる場合、ファイルを分割する間隔を指定することができます。時間やサイズによって、ログファイルを分割することができます。
- **すべてのファイルを保存する**:すべてのログファイルを保存します。
- **最近の＊＊個ファイルを保存する**:保存する最近のログファイル数を指定します。
- **保存するログタイプを選択する**:保存したログタイプを指定します。

注意 **Eメールコピー**にチェックを入れると、ネットワークで監視されたEメールのコピーが保存されます。Eメールコピーを保存したくない場合、このアイテムにチェックを外せばよいのです。

ログ保存機能を有効にした場合、保存するログのタイプを指定します。カラム**フォルダ**は各タイプのログを保存するフォルダの名前を表示します。カラム**ファイルのプレフィックス**はログファイル名のプレフィックスを表示します。

ノードブラウザ

Colasoft Capsa は、表示フィルターのように機能している革新的なノードブラウザを提供します。ノードはプロトコル、MAC アドレス、および IP アドレスのいずれである可能性があります。ノードブラウザであるノードが選択されると、解析ビューはこのノードに関するデータだけを表示します。

- プロトコルブラウザ
- 物理ブラウザ
- IP ブラウザ
- プロセスブラウザ
- ノードブラウザでトラブルシューティング

VoIP ブラウザの詳しいことについて、VoIP ブラウザをご参照ください。

プロトコルブラウザ

プロトコルブラウザはプロトコル層によって、プロトコルノードをグループ分けします。キャプチャーされたすべてのプロトコルは**プロトコルブラウザ**に表示されます。上位プロトコルまたはサブプロトコルを右クリックして、そのプロトコルに基づいて、フィルター、チャート、アラーム、およびレポートを作成することができます。

ノードブラウザであるプロトコルノードが選択されると、解析ビューは選択されたプロトコルに関する解析結果を表示します。選択されたプロトコルによって、解析ビューも違います。例えば、プロトコルノード「TCP」が選択されると、TCP セッションビューは利用可能となりますが、UDP セッションビューは利用できません。プロトコルノード「UDP」が選択されると、UDP セッションビューは利用可能となりますが、TCP セッションビューは利用できません。

ヒント Capsa によって識別できないプロトコルは、*Other* として表示されます。

キーボードを利用して、ノードを操作することができます。例えば、キーボードにおける**上向き矢印**を押すことで上のノードを、**下向き矢印**を押すことで下のノードを選択することができます。**左向き矢印**を押すことでノードを折りたたみ、**右向き矢印**を押すことでノードを展開します。

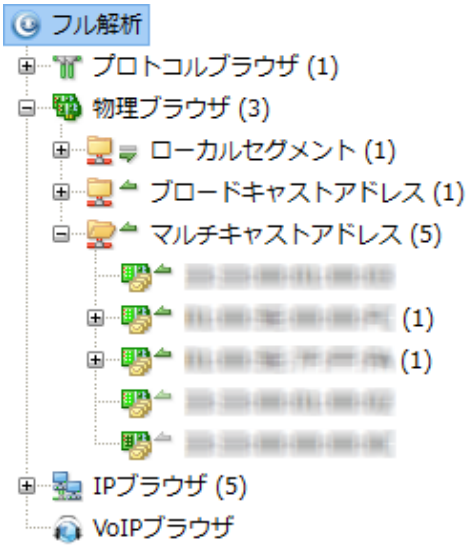
各プロトコルノードの前に三つのタイプのアイコンがあります。赤いアイコンは 5 秒以内でデータ転送があること、緑のアイコンは 30 秒以内でデータ転送があること、グレーのアイコンは 30 以内でデータ転送がないことを意味します。

物理ブラウザ

物理ブラウザはすべての MAC アドレスをグループ分けします。キャプチャーされたすべての MAC アドレスは物理ブラウザに表示されます。ある MAC ノードを右クリックして、その MAC アドレスに基づいて、フィルター、チャート、アラーム、およびレポートを作成したり、その MAC アドレスをネームテーブルに追加したりすることができます。

ノードブラウザである MAC ノードが選択されると、解析ビューは選択された MAC アドレスに関する解析結果だけを表示します。

物理ブラウザは以下のように表示されます。



物理ブラウザにはローカルセグメント、ブロードキャストアドレス、およびマルチキャストアドレスという三つのタイプのノードがあります。

- ノード「ローカルセグメント」にはローカル MAC アドレスが含まれています。サブノード「ホスト」には、ノードグループ（詳しいことはノードグループをご参照ください）で定義されている MAC アドレスが含まれています。
- ノード「マルチキャストアドレス」には、マルチキャスト MAC アドレスが含まれています。
- ノード「ブロードキャストアドレス」には、ブロードキャスト MAC アドレスが含まれています。

各 MAC アドレスの後の番号は、対応する IP アドレスの数を表します。

キーボードを利用して、ノードを操作することができます。例えば、キーボードにおける**上向き矢印**を押すことで上のノードを、**下向き矢印**を押すことで下のノードを選択することができます。**左向き矢印**を押すことでノードを折りたたみ、**右向き矢印**を押すことでノードを展開します。

ノードブラウザにおける上向き矢印はノードに転送されたパケットを、真ん中のライン
は、ノード内の転送を、下向き矢印はノードから転送されたパケットを表します。緑は転送中、グレーンは転送完了を表します。

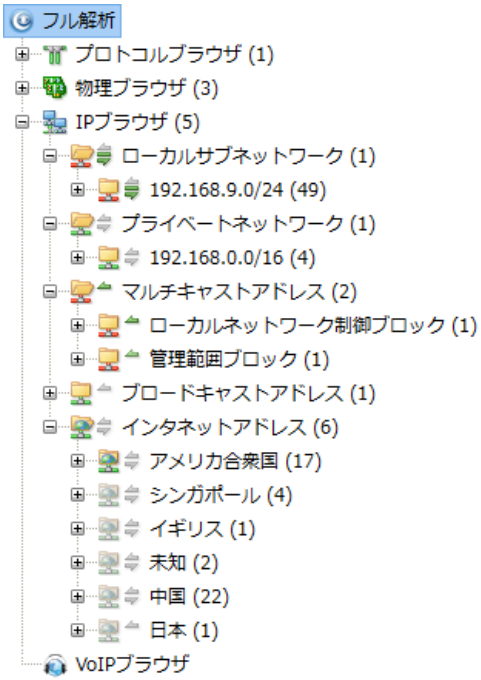
矢印アイコンの前にノードのアドレスタイプを表すアイコンがあります。はブロードキャスト IP アドレスを、はマルチキャスト IP アドレスを表します。

IP ブラウザ

IP ブラウザはすべての IP アドレスをグループ分けします。キャプチャーされたすべての IP アドレスは IP ブラウザに表示されます。ある IP ノードを右クリックして、その IP に基づいて、フィルター、チャート、アラーム、およびレポートを作成したり、その IP を解決し、ネームテーブルに追加したりすることができます。

ノードブラウザである IP が選択されると、解析ビューは選択された IP に関する解析結果だけを表示します。

IP ブラウザは以下のように表示されます。



一般的には、IP ブラウザにはローカルサブネットワーク、プライベートネットワーク、マルチキャストアドレス、ブロードキャストアドレス、およびインタネットアドレスという五つのタイプのノードがあります。

- ノード「ローカルサブネットワーク」にはノードグループルール（詳しいことは[ノードグループ]をご参照ください）によって定義された IP アドレスが含まれています。

- ノード「プライベートネットワーク」には、事前定義されたノードグループに属していないプライベート用の IP アドレスが含まれています。
- ノート「マルチキャストアドレス」には、マルチキャスト IP アドレスが含まれています。
- ノード「ブロードキャストアドレス」には、ブロードキャスト IP アドレスが含まれています。
- 「ナショナルジオグラフィックのグループ化機能を有効にする」にチェックを入れる場合、ノード「インタネットアドレス」には、国によってグループ分けされたインタネット IP アドレスが含まれます。

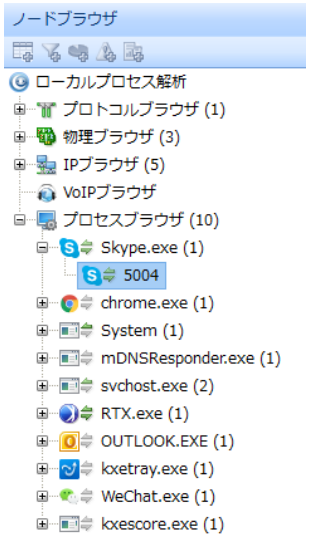
キーボードを利用して、ノードを操作することができます。例えば、キーボードにおける**上向き矢印**を押すことで上のノードを、**下向き矢印**を押すことで下のノードを選択することができます。**左向き矢印**を押すことでノードを折りたたみ、**右向き矢印**を押すことでノードを展開します。

ノードブラウザにおける上向き矢印 はノードに転送されたパケットを、真ん中のライン は、ノード内の転送を、下向き矢印 はノードから転送されたパケットを表します。そして緑は転送中、グレーンは転送完了を表します。

矢印アイコンの前にノードのアドレスタイプを表すアイコンがあります。 はブロードキャスト IP アドレスを、 はマルチキャスト IP アドレスを、 はインタネットアドレスを表します。

プロセスブラウザ

プロセスブラウザはプロセス名、プロセス ID を階層構造でリストすることで、すべてのプロセスをグループ分けします。



プロセス名またはプロセス ID など特定のノードを選択することで右側の統計ビューは選択されたノードに関するデータだけを表示します。

プロセス名またはプロセス ID を右クリックすることで、プロセスファイルの含むフォルダを開くことができます。

ノードブラウザでトラブルシューティング

ノードブラウザは表示フィルターとして機能しているので、それをネットワークトラブルシューティングに利用するのが非常に便利です。

ここでノードブラウザを利用する例を挙げます。

マイグラフには Top IP 総通信量(バイト)と Top アプリケーションプロトコル(バイト)という二つのグラフがあります。

Top IP 総通信量(バイト)グラフで統計値が一番大きいアイテムをダブルクリックして、その IP をノードブラウザにロケートすることができます。この方法で解析ビューはその IP に関する解析結果だけを表示します。そして、プロトコルビューに移動して、その IP のトッププロトコルを確認することができます。

同様に Top アプリケーションプロトコル(バイト)グラフで統計値が一番大きいアイテムをダブルクリックして、そのプロトコルをノードブラウザにロケートすることができます。この方法で、解析ビューはそのプロトコルに関する解析結果だけを表示します。そして IP エンドポイントビューに移動して、そのプロトコルのトップ IP を確認することができます。

他の機能に加えて、Capsa を利用して、便利にネットワークトラブルシューティングすることができます。

統計

Capsa は統計ビューで様々な統計を提供します。詳しいことについては、以下のリンクをご覧ください。

ツールバーとポップアップメニュー

統計データを便利に表示、解析するために統計ビューは、ツールバーとポップアップメニューを提供します。統計ビューによって、ツールバーとポップアップメニューにおけるアイテムも違います。しかしツールバーとポップアップメニューにおけるアイコン/コマンドが同じであれば、その機能も同じになります。

ツールバー

以下のリストは、統計ビューにおけるツールバーアイテムについて説明しています。

:マイグラフビューで新たしいパネルを作成し、またはレポートビューで**新規レポート**ダイアログボックスを開きます。

:マイグラフビューで選択されたパネルの名前を変更して、またはレポートビューで選択されたレポートを修正します。

:選択されたアイテムを削除します。

:デフォルト設定にリセットします。

:表示を更新して、または小さな三角形をクリックすることで表示の更新間隔を設定します。**手動で更新**に設定すると、**更新**ボタンがクリックされた場合にのみ、表示が最新情報に更新されます。

:選択された診断イベントの設定を表示します。イベントをダブルクリックして、そのイベントの設定を表示することもできます。

:現在の統計結果をエクスポートし、保存します。

:診断ビューの**診断アドレス**パネルを表示、非表示します。

:　診断ビューの**診断イベント**パネルを表示、非表示します。

 : 選択されたアイテムに基づいて、パケットフィルターを作成します。

 :選択されたアドレスのために別名を**ネームテーブル**に追加します。

 :選択されたアイテムを**ノードブラウザ**にロケートします。

 :下位パネルを表示、非表示します。

 :階層的に表示するかどうかを選択します。

 :マトリックスグラフにおけるノードのフォントサイズを設定します。

 :データフローの方向を選択します。**双方向**は全体データフローを表示することを、**ノード 1 からノード 2 まで**はノード 1 からノード 2 までデータを表示することを、**ノード 2 からノード 1 まで**は、ノード 2 からノード 1 までのデータを表示することを表します。

 :**データフロー**タブで表示するセッションのパケット数を制限します。

 :マトリックス表示の設定を行い、またはシステムオプションにおけるレポートを設定します。

 : **シーケンス番号の絶対値を表示**:パケットにおける実際のシーケンス番号を表示します。**シーケンス番号の相対値を表示**:セッションにおける最初のパケットの番号が 0 である、相対的なシーケンス番号を表示します。

 :データフローを .txt ファイルに保存します。

 :**マトリックスを追加**ダイアログボックスを開き、新しいマトリックスを作成します。

 :**選択したマトリックスを編集**ダイアログボックスを開き、マトリックスを修正します。

 :選択されたマトリックスを削除します。

 :マトリックスビューをデフォルトの設定にリセットします。

 :選択されたパケットを保存し、またはパケットリストにおけるすべてのパケットをエクスポートします。*ファイルの種類*ドロップダウンリストからフォーマットを選択し、パケットを保存することができます。

 :リストにおける前のパケットを選択します。

 :リストにおける次のパケットを選択します。

 :**パケットリスト**パネルを表示します。

 :**フィールドデコード**を表示します。

 :**Hex デコード**を表示します。

 :**パケットリスト**パネル、**フィールドデコード**パネル、および **Hex デコード**パネル

のためにレイアウトスタイルを選択します。

 :自動的に最新のデータを表示するようにスクロールします。

 :指定したフィルタールールでアイテムを表示します。

各統計ビューの右上に現在ビューの統計結果を表示する統計ボックスがあります。**ノードブラウザ**での選択によって、統計ボックスの名前も変わります。

ポップアップメニュー

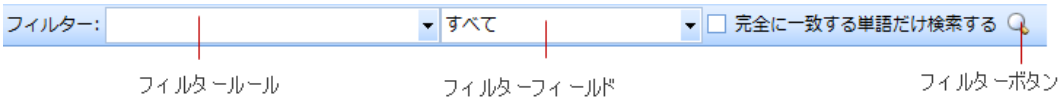
統計ビューで右クリックして、ポップアップメニューが出てきます。統計ビューによって、ポップアップメニューに含まれるコマンドアイテムも違います。以下のリストはポップアップメニューにおけるすべてのコマンドアイテムについて説明しています。

- **コピー**:つい最近選択された行、あるいは現在選択された行とヘッダー行をクリップボードにコピーします。
- **カラムをコピー**:選択されたカラムをクリップボードにコピーします。
- **カラムを表示する**: 統計ビューで表示するカラムを選択します。デフォルトをクリックすると、デフォルトカラムしか表示されません。ヘッダーカラムを右クリックすることで、表示したいカラムを選択することもできます。
- **統計を保存**:現在統計ビューにおける統計結果を.csv ファイルに保存します。
- **検索**:検索ダイアログボックスを開きます。
- **ログをエクスポート**: 現在のアドリストリストを.csv ファイルにエクスポートし、保存します。
- **アドレスを解決**: IP アドレスの場合にのみ、利用可能となります。選択された IP アドレスを解決します。
- **フィルターを作成**:選択されたアイテムに基づいて、パケットフィルターを作成します。
- **ネームテーブルに追加**:選択されたアドレスのために、別名を**ネームテーブル**に追加します。
- **チャートを作成**:選択されたアイテムに基づいて、**マイグラフ**ビューでチャートを作成します。
- **アラームを作成**:選択されたアイテムに基づいて、アラームを作成します。
- **ノードブラウザにロケートする**:選択されたアイテムを**ノードブラウザ**にロケートします。
- **すべてを選択**:このビューにおけるすべてのアイテムを選択します。
- **更新**:現在統計ビューを更新します。
- **新しいウィンドウでパケットを表示する**:**パケット**ビューと同じような**パケット**ウィンドウで選択されたアイテムのパケットのデコード情報を表示します。
- **Ping**:ビルトイン **Ping Tool** を呼び出して、選択されたノードを ping します。

表示フィルター

フィルターは特定のパケットを分離するために利用されています。キャプチャーフィルターを利用して、特定のパケットだけをキャプチャーすることができます。一方、表示フィルターは統計ビューで表示する特定のアイテムを分離する場合にのみ、利用されています。簡単に言えば、表示フィルターにおけるキーワードと一致したアイテムだけが統計ビューで表示されます。一致しないアイテムは、キーワードが削除されるまでずっと非表示となります。

表示フィルターは以下のように表示され、多くのビューで利用可能です。



- **フィルタールール**テキストボックスにフィルタールールを入力します。
- 現在統計ビュー、または現在タブのカラムを表示する**フィルターフィールド**ドロップリストから、カラムを一つ選択します。統計ビュー、またはタブによって、ドロップリストにおけるカラムが違います。
- **完全に一致する単語だけ検索する**にチェックを入れるとキーワードと完全に一致する単語のみ検索します。

表示フィルターを適用するには、フィルタールールを入力し、フィルターフィールドを選択して、表示フィルターボタンをクリックする必要があります。

例えば、TCP セッションビューで**フィルタールール**に「HTTP」を入力し、**フィルターフィールド**で「プロトコル」を選択して、**フィルター**ボタンをクリックすると、TCP セッションビューでは、「プロトコル」カラムに「HTTP」があるアイテムだけが表示されます。

キャプチャーフィルターの詳しいことについて、キャプチャーフィルター をご参照ください。

概要統計

概要ビューは、現在キャプチャーまたはリプレイの概要統計を提供します。**更新**ボタンをクリックして、現在の統計結果を更新することができます。

ノードブラウザでの選択によって、概要ビューでの統計アイテムが違います。統計ビューは、ノードブラウザで選択されたノードに関する統計結果だけを表示します。

- ルートノードが選択された場合、概要ビューは、選択した解析プロファイルに基づいて、すべての利用可能な統計アイテムを提供します。
- あるプロトコルノードが選択された場合、概要ビューは、そのノードに関する総通信量とパケットサイズ分布統計を提供します。
- ある MAC アドレスノードが選択されると、概要ビューはそのノード通信量統計、データストリーム統計および TCP 統計を提供します。解析プロファイルがセキュリテ

ィ解析の場合、ARP 攻撃アドレスの統計も提供します。

- ある IP アドレスノードが選択された場合、概要ビューが提供する統計は、解析プロファイルによって違います。

ワイヤレスネットワークを監視している場合、ワイヤレス解析の統計アイテムが提供されます。

さらに解析プロファイルによって、提供される統計アイテムが違います。以下のリストはすべての統計アイテムについて説明しています。

- 診断統計
  情報イベント、注意イベント、警告イベント、エラーイベントというタイプごとにトリガーされたイベント数を統計します。

- ワイヤレス解析
  ワイヤレス解析通信量:ノイズ通信量、コントロールフレーム通信量、管理フレーム通信量、暗号化解除済みのデータフレーム通信量、未暗号化のデータフレーム通信量、暗号化未解除のデータフレーム通信量
  ノイズ通信量は、同じチャンネルを利用している他の AP からの通信量を表します。
  暗号化解除済みのデータフレーム通信量は、Capsa によって復号化されたデータフレーム通信量を表します。
  未暗号化のデータフレーム通信量は、通信中において暗号化されていないデータフレーム通信量を表します。
  暗号化未解除のデータフレーム通信量は、Capsa によって復号化されていないデータフレーム通信量を表します。
  監視された AP の総通信量=コントロールフレーム通信量+管理フレーム通信量+データフレーム通信量

- 通信量統計
  総通信量、ブロードキャスト通信量、マルチキャスト通信量、および平均パケット長さというタイプごとに、それぞれのバイト数、パケット数、利用率、毎秒ビット数、毎秒パケット数をリストします。
  総通信量の利用率が 50%を超えると、ネットワークはオーバーロードされた可能性があります。
  ブロードキャスト、またはマルチキャスト通信量の利用率が 20%を超えると、ブロードキャスト/マルチキャストストームと ARP 攻撃が発生した可能性があります。

- パケットサイズ分布
  <=64、65-127、 128-255、 256-511、 512-1023、1024-1517、 >=1518 というサイズ範囲ごとに、それぞれのバイト数、パケット数、利用率、毎秒ビット数、毎秒パケット数をリストします。
  パケットサイズが<=64、または>=1518 のトラフィックが大きい場合、フラグメント攻撃またはフラッディング攻撃が発生した可能性があります。

- アドレス統計

物理アドレス、IP アドレス、ローカル IP アドレス、リモート IP アドレスのそれぞれの数をリストします。
アドレス数が以上に多い場合、MAC フラッディング攻撃、TCP フラッディング攻撃などが発生した可能性があります。

- プロトコル統計
  総プロトコル数と、データリンク層、ネットワーク層、トランスポート層、セッション層、プレゼンテーション層、アプリケーション層のそれぞれのプロトコル数をリストします。
- データストリーム統計
  物理セッション、IP セッション、TCP セッション、UDP セッションという四つのセッションの数をリストします。
- TCP 統計
  TCP SYN 送信、TCP SYNACK 送信、TCP FIN 送信、TCP RST 送信という TCP 接続パケットの数をリストします。ノードブラウザで IP アドレスが選択された場合、 TCP SYN 受信、 TCP SYNACK 受信、 TCP FIN 受信、 TCP RST 受信という TCP 接続パケットの数をもリストします。
  TCP SYN パケットが TCP SYNACK パケットより遥かに多い場合、ポートスキャン（TCP SYN フラッディング攻撃）が発生した可能性があります。
- アラーム統計
  セキュリティアラーム、性能アラーム、故障アラームのそれぞれのトリガー回数をリストします。
- DNS 解析
  DNS クエリとレスポンスの数をリストします。
- Email 解析
  SMTP 、POP3 、IMAP4 接続の数をリストします。
- FTP 解析
  FTP アップロードとダウンロードアクティブティの数をリストします。
- HTTP 解析
  送信された HTTP リクエスト、受信した HTTP リクエスト、および HTTP 接続の数をリストします。
- セキュリティ解析統計
  ワームに感染したアドレス、起こした DoS 攻撃のアドレス、DoS 攻撃を受けたアドレス、不審セッションアドレス、TCP ポートスキャンアドレス、ARP 攻撃アドレスのそれぞれの数をリストします。

注意 ワイヤレス解析と診断解析は Capsa Enterprise の場合のみ、利用可能となります。

Capsa Professional はこの機能を持っていません。

プロトコル統計

プロトコルビューは、プロトコルに基づいて、ネットワークトラフィックの統計を提供します。各プロトコルは独自の色を持っているので、色によって簡単に目標プロトコルを見つけることができます。

デフォルトでは、プロトコルは展開された構造で表示されます。プロトコル前の折りたたむ/展開アイコンをクリックすることで、それを折りたたむ/展開します。

カラムヘッダーにおける統計フィールドをクリックすることで、関心のあるフィールドによってリストを並べ替えることができます。カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。プロトコルビューにおける統計フィールドの詳しいことについて、プロトコルビューにおけるカラムについてをご参照ください。

ノードブラウザウィンドウでの選択によって、プロトコルリストに表示されるアイテムが違います。ルートノード、**プロトコルブラウザ**ノード、**物理ブラウザ**ノード、または **IP ブラウザ**ノードを選択した場合、**プロトコル**ビューはネットワークにおけるすべてのプロトコルとその統計情報を表示します。**ノードブラウザ**ウィンドウで特定のノードを選択した場合、**プロトコル**ビューはそのノードに関するプロトコルと統計情報だけを表示します。

プロトコルリストで特定のアイテムを選択した場合、下位パネルタブはこのアイテムに関する詳細情報を提供します。詳しいことはプロトコルビュー下位パネルをご参照ください。下位パネルが見えない場合、  をクリックして、それを表示することができます。

プロトコルリストで、あるプロトコルをダブルクリックして、**パケット**ウィンドウで詳細なパケット情報が表示されます。**パケット**ウィンドウは**パケット**ビューと同じように表示されています。

プロトコルビュー下位パネル

プロトコルビュー下位パネルタブには、**プロトコル**ビューで選択されたプロトコルの詳細情報が表示されます。デフォルトでプロトコル下位パネルは表示されますが、**プロトコル**ビューにおける  ボタンをクリックして、それを隠すことができます。プロトコル下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

ノードブラウザウィンドウでの選択によって、プロトコル下位パネルで表示するタブが違います。

- ルートノート、または**プロトコルブラウザ**で任意ノードを選択した場合、下位パネルは**物理エンドポイント**タブと **IP エンドポイント**タブからなっています。
- **物理ブラウザ**で任意グループノードを選択した場合、下位パネルは**物理エンドポイント**タブと**物理セッション**タブからなっています。
- **物理ブラウザ**で MAC アドレスノードを選択した場合、下位パネルは**物理セッション**タブと **IP セッション**タブからなっています。
- **IP ブラウザ**で IP アドレスノードを除いて、他の任意ノードを選択した場合、下位パネルは **IP エンドポイント**タブと **IP セッション**タブからなっています。
- **物理ブラウザ**、または **IP ブラウザ**で IP アドレスノードを選択した場合、下位パネルは **IP セッション**タブ、**TCP セッション**タブ、および **UDP セッション**タブからなっています。

下位パネルタブで任意アイテムをダブルクリックして、**パケット**ビューと同じように表示される**パケット**ウィンドウで詳細なパケット情報を確認することができます。

以下のリストは下位パネルにおけるタブについて説明しています。

- **物理エンドポイント**タブは**プロトコル**ビューで選択されたプロトコルを利用しているすべての MAC アドレスノートとそのトラフィック情報をリストします。このタブにおけるツールバーとカラムは**物理エンドポイント**ビューとまったく同じです。
- **IP エンドポイント**タブは**プロトコル**ビューで選択されたプロトコルに関するすべての IP アドレスノードとそのトラフィック情報をリストします。このタブにおけるツールバーとカラムは **IP エンドポイント**ビューとまったく同じです。
- **物理セッション**タブは**プロトコル**ビューで選択されたプロトコルに関するすべての

MAC アドレスセッションをリストします。このタブにおけるツールバーとカラムは**物理セッション**ビューとまったく同じです。

- **IP セッション**タブは**プロトコル**ビューで選択されたプロトコルを利用しているすべての IP アドレスセッションをリストします。このタブにおけるツールバーとカラムは **IP セッション**ビューとまったく同じです。
- **TCP セッション**タブは TCP プロトコルを利用しているセッションをリストします。このタブにおけるツールバーとカラムは **TCP セッション**ビューとまったく同じです。
- **UDP セッション**タブは UDP プロトコルを利用しているセッションをリストします。このタブにおけるツールバーとカラムは **UDP セッション**ビューとまったく同じです。

ノードブラウザと組み合わせて、便利に関心の統計を表示することができます。

プロトコルビューにおけるカラムについて

以下の表は、プロトコルビューにおけるカラムについて説明しています。

カラム	説明
名前	プロトコルの名前です。
バイト	このプロトコルを利用しているパケットの合計バイト数です。
パケット	このプロトコルを利用しているパケット数です。
毎秒バイト	1 秒当たりのバイト数です。
毎秒ビット	1 秒当たりのビット数です。
毎秒パケット	1 秒当たりのパケット数です。
バイト%	このプロトコルタイプの合計バイト数の割合です。
パケット%	このプロトコルタイプのパケット数の割合です。
毎秒バイト%	1 秒当たりのバイト数の割合です。
毎秒パケ	1 秒当たりのパケット数の割合です。

ット%

ポート統計

Capsa は TCP/UDP プロトコルに基づくポート統計を表示する**ポート**ビューを提供します。

ポートビューはポート番号のリストを表示する上側パネルと、上側パネルで選択されたアイテムのセッション情報を表示する下側パネルから構成されています。

カラム**ポート**をクリックして、ポート番号によって、統計データを並べ替えることができます。カラムヘッダーにおける他のカラムをクリックすることで、関心の統計フィールドによって、リストを並べ替えることができます。各カラムの詳しいことについて、[ポートビューにおけるカラムについて]をご参照ください。

ポートビューであるアイテムが選択された場合、下位パネルはこのアイテムに関する詳細な情報を提供します。下位パネルは TCP セッションと UDP セッションという二つのタブからなっています。

ポートの IP プロトコルが TCP である場合、このポートに関する詳細な情報は下位パネルにおける TCP セッションタブに表示されます。このタブである TCP セッションをダブルクリックして、TCP フロー解析ウィンドウが表示されます。一方ポートの IP プロトコルが UDP である場合、このポートに関する詳細な情報は下位パネルにおける UDP セッションタブに表示されます。ポートが TCP と UDP の両方のプロトコルを採用している場合、ポートビューには、二つのレコードが存在します。

ポートビューのほかに、Capsa はマイグラフビューで Top ポート総通信量、Top TCP ポート総通信量、Top UDP 総通信量という三つの top ポート統計チャートを提供します。統計単位はパケット、またはバイトです。

Top ポートチャートでは、top 5、top 10 、および top 20 から Top ポートの数量を選択することができます。

ポートビューにおけるカラムについて

以下の表はポートビューにおけるカラムについて説明しています。

カラム	説明
ポート	通信に利用されるポート番号です。
IP プロトコル	通信ポートが採用しているプロトコルです。UDP、または TCP である可能性があります。
パケット	そのポートのパケット数です。
バイト	そのポートのトラフィックです。
平均パケット長さ	そのポートにおけるパケットの平均長さです。
一般的なサービス	通信ポートを利用している一般的なアプリケーションです。一般的なアプリケーションでない場合、「不明」と表示されます。

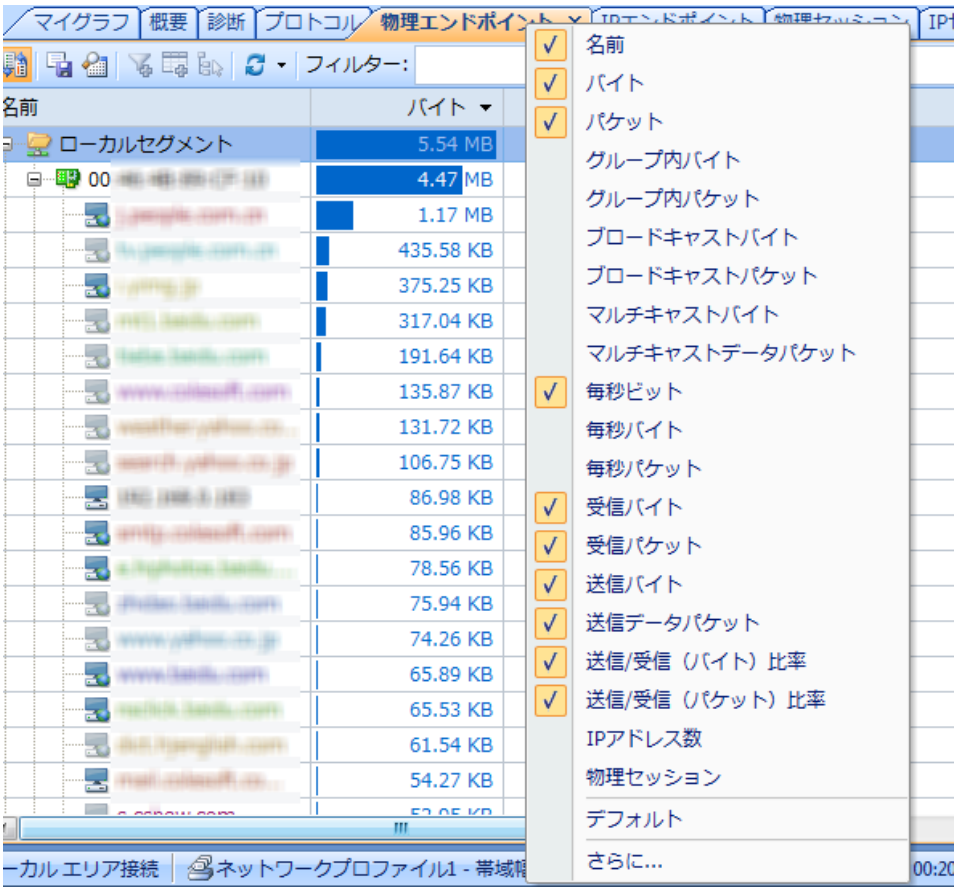
アドレス統計

Capsa は**物理エンドポイント**ビューと **IP エンドポイント**ビューで、それぞれ MAC アドレス統計と IP アドレス統計を提供します。

注意 **物理ブラウザ**で IP アドレスノード、または **IP ブラウザ**で任意ノードを選択した場合、**物理エンドポイント**ビューは利用できません。一方**物理ブラウザ**でノードグループ、または MAC アドレスノードを選択した場合、**IP エンドポイント**ビューは利用できません。

デフォルトでは、アドレスは階層構造で展開表示されています。  ボタンをクリックすると、アドレスは、階層構造で表示されません。

カラムヘッダーにおける統計フィールドをクリックすることで、関心のあるフィールドによってリストを並べ替えることができます。カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。エンドポイントビューにおける統計フィールドの詳しいことについて、エンドポイントビューにおけるカラムについてをご参照ください。



エンドポイントビューであるアイテムを選択した場合、下位パネルタブはこのアイテムに関する詳細な情報を提供します。詳しいことについては、物理エンドぽインドビュー下位パネルと IP エンドポイントビュー下位パネル をご参照ください。下位パネルが目に見えない場合、  をクリックして、それを表示することができます。

エンドポイントビューであるアイテムをダブルクリックして、パケットビューと同じように表示されるパケットウィンドウでそのアイテムの詳細なパケット情報を確認することができます。

物理エンドポイントビュー下位パネル

物理エンドポイントビュー下位パネルは、**物理エンドポイント**ビューで選択されたノードの詳細な情報を表示します。デフォルトでは、下位パネルは表示されますが、**物理エンドポイント**ビューにおける  ボタンをクリックして、それを隠すことができます。下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

下位パネルには、**物理エンドポイント**ビューで選択されたノードのすべての MAC アドレスセッションをリストする**物理セッション**タブが表示されます。このタブにおけるツールバーとカラムは**物理セッション**ビューのとまったく同じです。

下位パネルタブで任意アイテムをダブルクリックして、**パケット**ビューと同じように表示される**パケット**ウィンドウで詳細なパケット情報を確認することができます。

IP エンドポイントビュー下位パネル

IP エンドポイントビュー下位パネルタブは **IP エンドポイント**ビューで選択されたノードの詳細情報を表示します。デフォルトで下位パネルは表示されますが、**IP エンドポイント**ビューにおける  ボタンをクリックして、それを隠すことができます。下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

IP エンドポイントビュー下位パネルは **IP セッション**タブ、**TCP セッション**タブ、および **UDP セッション**タブを提供します。

- **IP セッション**タブは **IP エンドポイント**ビューで選択されたノードのすべての IP アドレスセッションをリストします。このタブにおけるツールバーとカラムは **IP セッション**ビューとまったく同じです。
- **TCP セッション**タブは **IP エンドポイント**ビューで選択されたノードの中で TCP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーと

カラムは**TCP セッション**ビューとまったく同じです。

- UDP セッションタブは**IP エンドポイント**ビューで選択されたノードの中で UDP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは**UDP セッション**ビューとまったく同じです。

下位パネルタブで任意アイテムをダブルクリックして、**パケット**ビューと同じように表示される**パケット**ウィンドウで詳細なパケット情報を確認することができます。

エンドポイントビューにおけるカラムについて

以下の表は、**物理エンドポイント**ビュー、**IP エンドポイント**ビュー、**ARP 攻撃**ビュー、**ワーム**ビュー、**起こした DoS 攻撃**ビュー、**受けた DoS 攻撃**ビュー、**TCP ポートスキャン**ビューにおけるカラムについて説明しています。

カラム	説明
名前	ノードの名前です。MAC アドレス、IP アドレス、ノードグループ、または解決された別名である可能性があります。
バイト	そのノードの送受信した合計バイト数です。
パケット	そのノードの送受信した合計パケット数です。
グループ内バイト	ノードグループアイテムの場合にのみ、利用可能となります。ノートグループ内(詳しいことノードグループをご参照ください)で転送された合計バイト数です。
グループ内パケット	ノードグループアイテムの場合にのみ、利用可能となります。ノートグループ内で転送された合計パケット数です。
ブロードキャストバイト	そのノードの送受信した合計ブロードキャストバイト数です。
ブロードキャストパケット	そのノードの送受信した合計ブロードキャストパケット数です。
マルチキャストバイト	そのノードの送受信した合計マルチキャストバイト数です。
マルチキャストパケット	そのノードの送受信した合計マルチキャストパケット数です。
毎秒ビット	1 秒当たりのビット数です。
毎秒バイト	1 秒当たりのバイト数です。

カラム	説明
毎秒パケット	1 秒当たりのパケット数です。
受信バイト	受信したバイト数です。
受信パケット	受信したパケット数です。
送信バイト	送信したバイト数です。
送信パケット	送信したパケット数です。
送信/受信(バイト)比率	送信バイト数対受信バイト数の比率です。
送信/受信(パケット)比率	送信パケット数対受信ぱっと数の比率です。
IP ドレス数	P アドレスの数です。リストにおけるノードグループアイテムと MAC アドレスアイテムの場合のみ、利用可能となります。
物理セッション	物理セッションの数です。
IP セッション	IP セッションの数です。
TCP セッション	TCP セッションの数です。
UDP セッション	UDP セッションの数です。
TCP SYN 送信	SYN フラグが 1 に設定された送信パケット数です。
TCP SYN 受信	SYN フラグが 1 に設定された受信パケット数です。
TCP SYNACK 送信	ACK と SYN フラグの両方が 1 に設定された送信パケット数です。正常の TCP 接続確立に対して、このアイテム値は **TCP SYN 受信**の値に等しい必要があります。
TCP SYNACK 受信	ACK と SYN フラグの両方が 1 に設定された受信パケット数です。正常の TCP 接続確立に対して、このアイテム値は **TCP SYN 送信**の値に等しい必要があります。
ジオロケーシ	そのノードが属している国、または地域です。

カラム	説明
ョン	
TCP FIN 送信	FIN フラグが 1 に設定された送信パケット数です。
TCP FIN 受信	FIN フラグが 1 に設定された受信パケット数です。正常の TCP 接続終了に対して、このアイテム値は **TCP FIN 送信**の値に等しい必要があります。
TCP RST 送信	RST フラグが 1 に設定された送信パケット数です。
TCP RST 受信	RST フラグが 1 に設定された受信パケット数です。
バイト%	そのノードの送受信したバイト数の割合です。
パケット%	そのノードの送受信したパケット数の割合です。
グループ内バイト%	ノードグループ内で送受信したバイト数の割合です。
グループ内パケット%	ノードグループ内で送受信したパケット数の割合です。
ブロードキャストバイト%	ブロードキャストバイト数の割合です。
ブロードキャストパケット%	ブロードキャストパケット数の割合です。
マルチキャストバイト%	マルチキャストバイト数の割合です。
マルチキャストパケット%	マルチキャストパケット数の割合です。
受信バイト%	受信したバイト数の割合です。
受信パケット%	受信したパケット数の割合です。
送信バイト%	送信したバイト数の割合です。
送信パケット%	送信したパケット数の割合です。

カラム	説明
毎秒ビット%	1 秒当たりにおけるビット数の割合です。
毎秒バイト%	1 秒当たりにおけるバイト数の割合です。
毎秒パケット%	1 秒当たりにおけるパケット数の割合です。
毎秒ブロードキャストパケットピーク値	1 秒当たりにおけるブロードキャストパケットのピーク値です。
毎秒マルチキャストパケットピーク値	1 秒当たりにおけるマルチキャストパケットのピーク値です。
毎秒受信バイトピーク値	1 秒当たりにおける受信バイト数のピーク値です。
毎秒受信パケットピーク値	1 秒当たりにおける受信パケット数のピーク値です。
毎秒送信バイトピーク値	1 秒当たりにおける送信バイト数のピーク値です。
毎秒送信パケットピーク値	1 秒当たりにおける送信パケット数のピーク値です。
TCP SYN 毎秒送信パケットピーク値	SYN フラグが 1 に設定された 1 秒当たりにおける送信パケット数のピーク値です。
TCP SYN 毎秒受信パケットピーク値	SYN フラグが 1 に設定された 1 秒当たりにおける受信パケット数のピーク値です。

セッション統計

Capsa は物理セッションビュー、IP セッションビュー、TCP セッションビュー、および UDP セッションビューを提供し、各ビューでそれぞれ物理セッション統計、IP セッション統計、TCP セッション統計、および UDP セッション統計が表示されます。

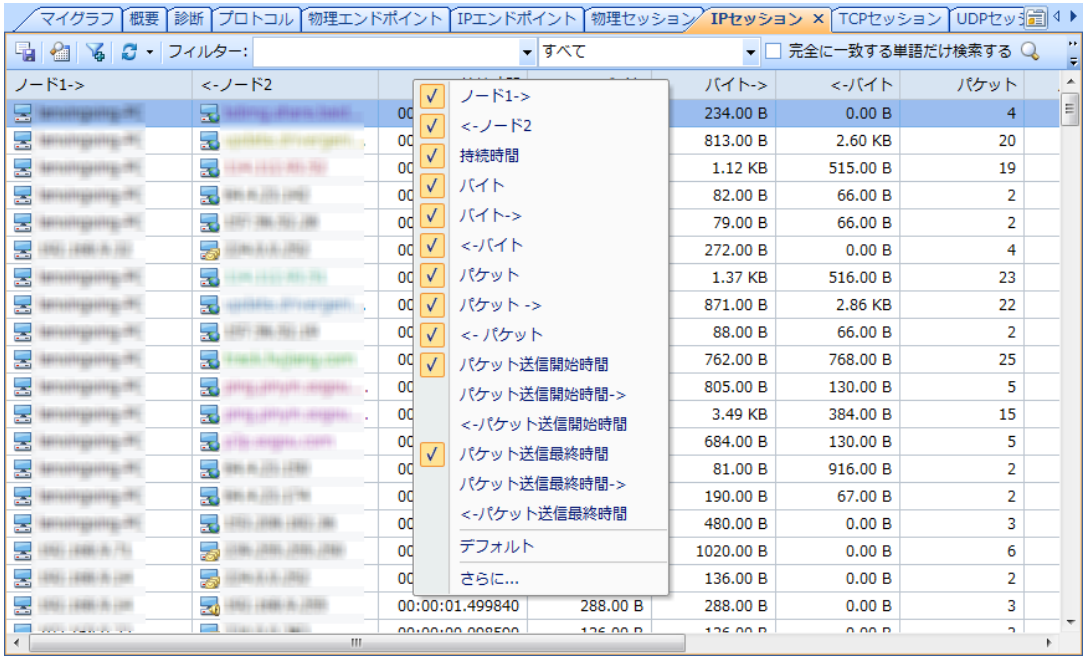
物理セッションビューは二つの MAC アドレス間のネットワーク通信の統計を提供します。

IP セッションビューは二つの IP アドレス間のネットワーク通信の統計を提供します。

TCP セッションビューは TCP プロトコルに基づくネットワーク通信の統計を提供します。

UDP セッションビューは UDP プロトコルに基づくネットワーク通信の統計を提供します。

カラムヘッダーにおける統計フィールドをクリックすることで、関心のあるフィールドによってリストを並べ替えることができます。カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。セッションビューにおける統計フィールドの詳しいことについて、セッションビューにおけるカラムについてをご参照ください。



物理セッションビュー、IP セッションビュー、および UDP セッションビューで統計情報を確認するとき、あるセッションをダブルクリックすることで、そのセッションの詳細なパケット情報が表示されます。

TCP セッションビューで統計情報を確認するとき、あるセッションをダブルクリックすることで、更なる解析を行うことができます。詳しいことについては、TCP フロー解析ウィンドウ をご参照ください。

IP セッションビューであるアイテムを選択すると、下位パネルは選択されたアイテムの詳細な情報を表示します。詳しいことは IP セッションビュー下位パネル をご参照ください。

下位パネルが隠されている場合、  をクリックすることで、それを表示することができます。

TCP セッションビューであるアイテムを選択すると、下位パネルは三つのタブで選択された TCP フローの詳細情報を表示します。詳しいことは、TCP フロー解析をご参照ください。

UDP セッションビューであるアイテムを選択すると、下位パネルは選択されたアイテムの詳細情報を表示します。詳しいことは、UDP セッションビュー下位パネルをご参照ください。

IP セッションビュー下位パネル

IP セッションビュー下位パネルは **IP セッションビュー**で選択されたセッションの詳細情報を表示します。デフォルトで下位パネルは表示されますが、**IP セッション**ビューにおける  ボタンをクリックして、それを隠すことができます。下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

IP セッション下位パネルは TCP セッションタブと UDP セッションタブから構成されています。

- **TCP セッションタブ**は **IP セッションビュー**で選択されたセッションの中で TCP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは **TCP セッション**ビューとまったく同じです。
- **UDP セッションタブ**は **IP セッションビュー**で選択されたセッションの中で UDP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは **UDP セッションビュー**とまったく同じです。

下位パネルタブで任意アイテムをダブルクリックして、**パケット**ビューと同じように表示される**パケット**ウィンドウで詳細なパケット情報を確認することができます。

UDP セッションビュー下位パネル

UDP セッションビューにおけるセッションリストであるアイテムを選択すると、下位パネルは選択されたアイテムの詳細な情報を表示します。デフォルトで下位パネルは表示されますが、**UDP セッション**ビューにおける  ボタンをクリックして、それを隠すことができます。下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

UDP セッションビュー下位パネルは**パケット**タブと**データフロータブ**から構成されています。

- **パケットタブ**は **UDP セッションビュー**で選択されたセッションのすべてのパケット

をリストします。このタブにおけるツールバーとカラムは**パケットビュー**とまったく同じです。このタブで任意アイテムをダブルクリックして、詳細なパケット情報を表示することができます。

- **データフロータブ**は**UDP セッションビュー**で選択されたセッションの生データを表示します。
- **シーケンスチャートタブ**は DNS プロトコルを利用して通信している UDP セッションのタイムシーケンスチャートを表示します。このタブは DNS プロトコルを利用して通信している UDP セッションのみ利用可能となります。

デフォルトで**データフロータブ**は二つのノード間のすべてのデータを表示します。色によって、異なるノードのデータを区別することができます。青はノード 1 からノード 2 までのデータを表し、緑はノード 2 からノード 1 までのデータを表します。

 ボタンをクリックすることで、ノード 1 からノード 2 までのデータ或いはノード 2 からノード 1 までのデータだけを表示することもできます。

選択された UDP セッションのパケットがたくさんある場合、  をクリックして、上位 50 個、或いは上位 100 個のパケットを表示することができます。

データフローに興味を持っている場合、  をクリックすることでデータを保存することができます。

他のフォーマットでデータフローを表示したい場合、右クリックして、**コード**を選択し、関心のあるフォーマットをクリックします。

セッションビューにおけるカラムについて

以下の表は**物理セッションビュー**、**IP セッションビュー**、**TCP セッションビュー**、**UDP セッションビュー**および**不審セッションビュー**を含むセッションビューにおけるカラムについて説明しています。

カラム	説明
ノード 1 ->	セッションにおける最初パケットの送信元アドレスです。
<- ノード 2	セッションにおける最初パケットの宛先アドレスです。
持続時間	セッションの持続時間で、セッションにおける最初パケットのタイムスタンプから最終パケットのタイムスタンプまでの時間です。

バイト	このセッションで送受信した合計バイト数です。
バイト –>	ノード 1 からノード 2 に送信したバイト数です。
<– バイト	ノード 2 からノード 1 に送信したバイト数です。
パケット	このセッションで送受信した合計パケット数です。
パケット–>	ノード 1 からノード 2 に送信したパケット数です。
<– パケット	ノード 2 からノード 1 に送信したパケット数です。
パケット送信開始時間	セッションにおける最初パケットのタイムスタンプです。
パケット送信開始時間 –>	ノード 1 からノード 2 に送信した最初パケットのタイムスタンプです。
<– パケット送信開始時間	ノード 2 からノード 1 に送信した最初パケットのタイムスタンプです。
パケット送信終了時間	セッションにおける最終パケットのタイムスタンプです。
パケット送信終了時間 –>	ノード 1 からノード 2 に送信した最終パケットのタイムスタンプです。
<– パケット送信終了時間	ノード 2 からノード 1 に送信した最終パケットのタイムスタンプです。
プロトコル	セッションのプロトコルです。
プロセス	セッションの属しているプロセスを表示します。TCP セッションビューと UDP セッションビューだけはこのカラムを持っています。

プロセス統計

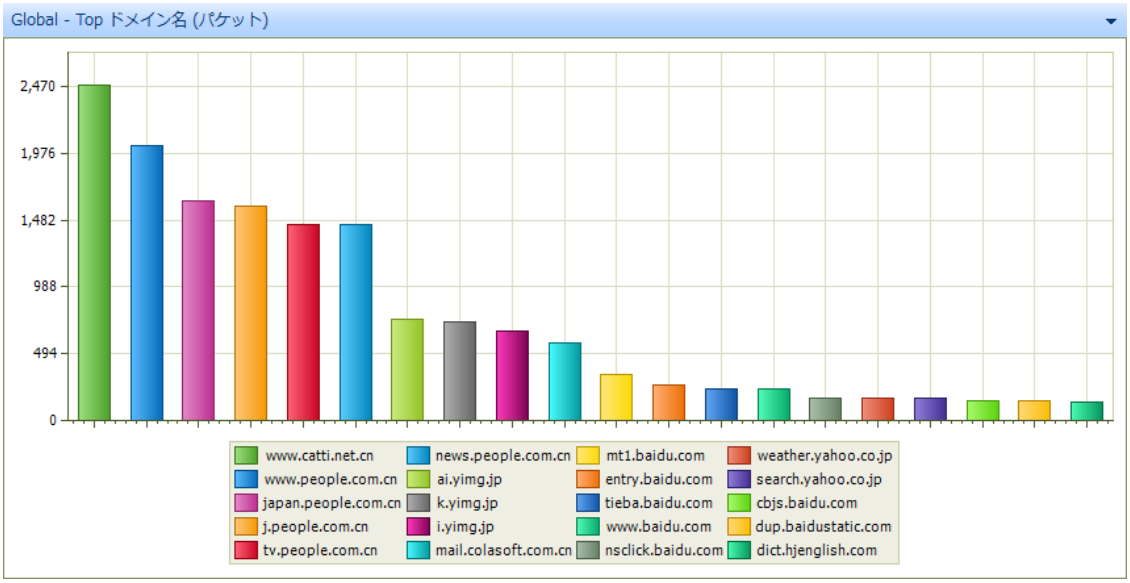
プロセスビューは下図のようにバイト、パケット、毎秒ビット、毎秒バイト、毎秒パケット、パスなどに基づき、ローカルプロセスのトラフィック統計を提供します。

あるプロセスをダブルクリックすることでそのプロセスに関するすべてのパケット情報が表示されます。

プロセスビューの上側であるアイテムを選択した場合、下側のタブではそのアイテムに関連しているプロトコルまたはセッション情報が表示されます。さらに TCP セッションビューと UDP セッションビューでは「プロセス」カラムが提供されているので、各 TCP/UDP セッションの属するプロセスを確認することができます。これはユーザーの迅速なトラブルシューティングに役立ちます。マイグラフビューにおけるプロセスタブでネットワークトラフィックに基づく Top プロセスを確認することもできます。

トップドメイン統計

Capsa は Top ドメイン名チャートを通じて、トップドメイン統計を提供します。Top ドメイン名チャートは一番多く訪問されたドメイン名をリストします。右クリックして、Top 数量を選択し、リストしたい Top 数を選択することができます。



Top ドメイン名チャートが表示されない場合、或いは他のマイグラフパネルでそれを表示したい場合、手動的にそれを追加することができます。適切なマイグラフパネル（新しいパネルを追加したり、既存のパネルを選択したりすることができます）を選択して、選択されたパネルでドメインチャート(チャートを作成する方法について、チャートを作成をご参照ください)を追加することができます。

統計情報の表示と保存

統計情報を表示するには、いくつかのヒントがあります。

- カラムヘッダーで関心のある統計フィールドをクリックすることで、そのフィールドによって統計結果を並べ替えることができます。
- カラムヘッダーを右クリックして、表示または非表示したい統計フィールドを選択することができます。
- あるアイテムをダブルクリックして、そのアイテムに関するパケット詳細情報を表示するパケットビューが表示されます。
- あるアイテムを右クリックして、そのアイテムに基づいて、チャート、アラーム、およびフィルターを作成したり、ノードブラウザにそのアイテムをロケートしたりすることができます。

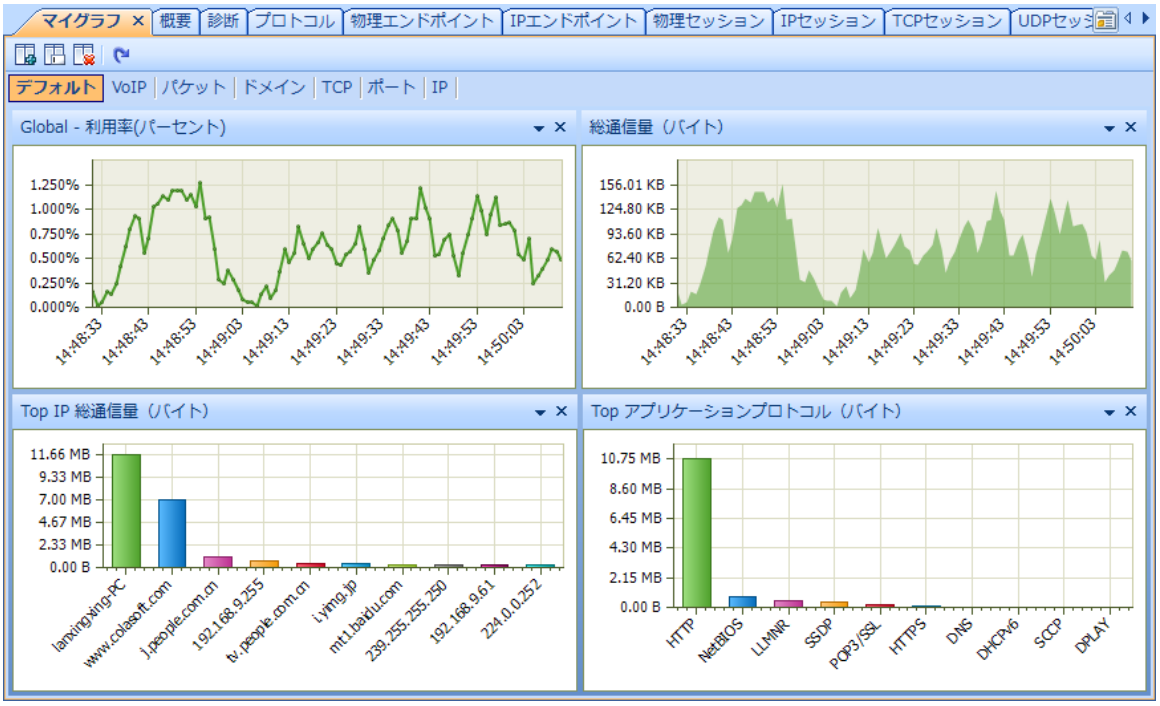
統計情報を保存するには、保存ボタン  をクリックすればよいのです。概要ビューを除いて、他のすべての統計ビューは保存ボタンを提供します。保存ボタンをクリックすることで、現在表示されている統計を保存することができます。

グラフ

マイグラフビュー

マイグラフビューは様々なチャートで統計を動的に表示します。

デフォルトでマイグラフビューは下図のように八つのマイグラフパネルを提供します。



マイグラフパネル「無線」が表示されない場合、をクリックすることで表示されることができます。

マイグラフパネル「無線」は WIFI ネットワークを監視している場合にのみ、利用可能となります。「VoIP」パネルは VoIP 解析モジュールが有効にされている場合にのみ、利用可能となります。

マイグラフパネル名をクリックして、他のパネルにおけるチャートを表示することができます。

デフォルトのマイグラフパネルのほかに、をクリックして、新しいパネルを追加することができます。各パネルには一から四までのチャートが含まれています。もちろん各パネル

で新しいチャート(チャートを作成する方法について、チャートを作成をご参照ください)を追加することもできます。

ノードブラウザでルートノードが選択された場合にのみ、マイグラフビューは表示されます。それでも表示されない場合、機能エリアにおける**解析**タブで**ビュー表示**アイコンをクリックして、**マイグラフ**にチェックを入れます(詳しいことはビュー表示をご参照ください)。

マイグラフビューにおけるチャートは、サンプリング時間、または更新間隔によって、更新されます。Capsa にはサンプルチャートとチャートという二つのタイプのチャートがあります。サンプルチャートはサンプリング時間によって自動的に更新します。一方、Top チャートは更新間隔によって、自動的に更新します。その間隔はユーザーによって定義されることができます。チャートを右クリックして、サンプリング時間または更新間隔を選択し、適切な間隔をクリックすればよいのです。

サンプルチャートを右クリックして、以下のアイテムを含むポップアップメニューが表示されます。

- **更新を一時停止**:チャートの更新を一時停止します。
- **凡例**:凡例ボックスを表示、または非表示したり、表示する位置を指定したりします。
- **折れ線グラフ**:折れ線グラフでチャートを表示します。
- **面グラフ**:面グラフでチャートを表示します。
- **タイトル**:チャート、X 軸、および Y 軸のタイトルを表示、または非表示します。
- **指示線**:マウスポインタをチャート上に移動すると、水平線とそのときの Y 軸の値を表示します。
- **サンプリング時間**:チャートのサンプリング時間を選択します。
- **チャートを保存**:選択されたチャートをディスクに保存します。.png、 .emf、 および .bmp フォーマットでチャートを保存することができます。

Top チャートを右クリックして、以下のアイテムを含むポップアップメニューが表示されます。

- **更新を一時停止**:チャートの更新を一時停止します。
- **凡例**:凡例ボックスを表示、または非表示したり、表示する位置を指定したりします。
- **棒グラフ**:棒グラフでチャートを表示します。
- **円グラフ**:円グラフでチャートを表示します。
- **タイトル**:チャート、X 軸、および Y 軸のタイトルを表示、または非表示します。
- **Top 数量**:チャートにおける統計アイテムの Top 数を選択します。Top5、 Top 10、および Top 20 から選択することができます。
- **サンプリング値**:統計値のタイプを選択します。**累積値**はチャートアイテムの統計がキャプチャーの開始から計算することを表します。**最後の 1 秒の値**は、最後の 1 秒の値だけを計算することを表します。
- **更新間隔**:チャートの更新間隔を選択します。
- **チャートを保存**:選択されたチャートをディスクに保存します。.png、 .emf、 および .bmp フォーマットでチャートを保存することができます。

チャートの位置は変更可能です。チャートのタイトルバーをクリックし、ドラッグすることで、チャートの位置を変更できます。

注意 チャートの右上にある閉じるアイコンは、閉じるではなくて、パネルからそのチャートを削除することを表します。

チャートを作成

チャートを作成する前に、チャートを作成するマイグラフパネルを指定する必要があります。

新しいマイグラフパネルを追加するには、  をクリックします。

全体ネットワークから指定されたノードまで幅広い範囲に基づいて、統計チャートを作成することができます。例えば、MAC アドレス、IP アドレス、およびプロトコルに基づいて、チャートを作成することができます。

以下のいずれに従い、**チャートを作成**ダイアログボックスを開き、チャートを作成します。

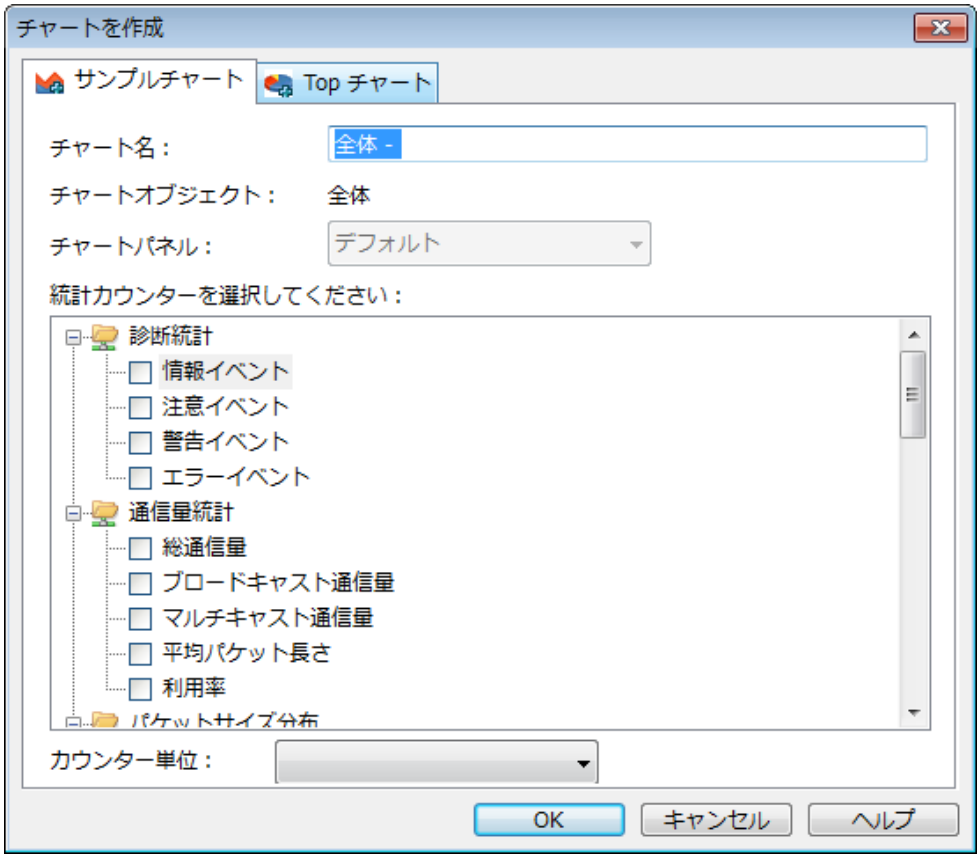
- マイグラフパネルにおけるチャートの右上にある  をクリックします。
- マイグラフパネルにおける「ここをクリックし、チャートを追加します。」をクリックします。
- **ノードブラウザ**ウィンドウにおける  をクリックします。
- **ノードブラウザウィンドウ**と、**マイグラフビュー**、**概要ビュー**、**マトリックスビュー**、および**レポートビュー**を除くすべての統計ビューで利用可能となる**ポップアップメニュー**で**チャートを作成**をクリックします。

ヒント

1. 前の二つの方法で作成されたチャートは、解析プロジェクトによってキャプチャーされたすべてのパケットの統計を表示します。
2. 最後の二つの方法で作成されたチャートは、右クリックされたノード、または**ノードブラウザ**ウィンドウで選択されたノードに関するパケットの統計を表示します。

例えば、特定のネットワークセグメントのトラフィック状態をチャートで表示したい場合、**ノードブラウザ**ウィンドウにそのセグメントをロケートして、そのセグメントを右クリックし、**チャートを作成**を選択することで、**チャートを作成**するダイアログボックスが開かれます。このダイアログボックスにおける**サンプルチャート**で、**通信量統計**における**総通信量**にチェックを入れます。

チャートを作成するダイアログボックスは以下のように表示されます。



チャートを作成するダイアログボックスは、**サンプルチャート**と **Top チャート**という二つのタブからなっています。各タブはそれぞれ以下のアイテムが含まれています。

- **チャート名**:チャートの名前で、自動的に生成されたり、ユーザーに定義されたりすることができます。
- **チャートオブジェクト**:チャートの統計オブジェクトを表示します。プログラムによって定義されます。
- **チャートパネル**:作成されるチャートが属しているパネルを指定します。
- **統計カウンター**:すべての利用可能な統計アイテムを表示します。このオプションはチャートオブジェクトによって、変わります。
- **カウンター単位**:統計カウンターの単位を指定します。

チャートタイプ

Capsa では以下の二つのチャートタイプを提供し、多くの統計アイテムに対するチャートを作成することができます。

- サンプルチャート
- Top チャート

サンプルチャート

サンプルチャートには、以下の統計アイテムが含まれています。

- **診断統計**:情報イベント、注意イベント、警告イベント、およびエラーイベントからなっています。
- **無線解析**:ノイズ通信量、コントロールフレーム通信量、管理フレーム通信量、暗号化解除済みのデータフレーム通信量、未暗号化のデータフレーム通信量、および暗号化未解除のデータフレーム通信量からなっています。
- **通信量統計**:総通信量、ブロードキャスト通信量、マルチキャスト通信量、平均パケット長さ、および利用率からなっています。
- **パケットサイズ分布**:パケットサイズは <=64、65-127、128-255, 256-511、512-1023、1024-1517 、および >=1518 からなっています。
- **TCP 統計**:TCP SYN 送信、TCP SYNACK 送信、TCP FIN 送信、および TCP RST 送信からなっています。
- **アラーム統計**:セキュリティアラーム、性能アラーム、および故障アラームからなっています。
- **DNS 解析**: DNS クエリと DNS レスポンスからなっています。
- **Email 解析**: SMTP 接続、POP3 接続、および IMAP4 接続からなっています。
- **FTP 解析**: FTP アップロードと FTP ダウンロードからなっています。
- **HTTP 解析**: 送信された HTTP リクエスト、受信した HTTP リクエスト、および HTTP 接続からなっています。

Top チャート

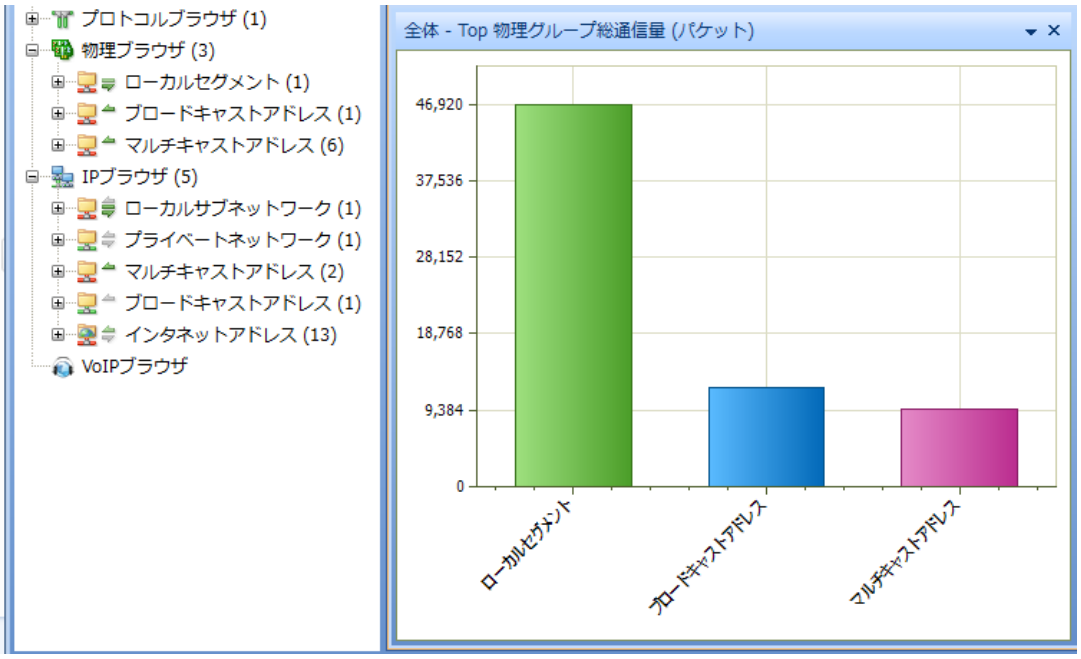
Top チャートには、以下の統計アイテムが含まれています。

- Top 物理グループ総通信量
- Top 物理グループ受信通信量
- Top 物理グループ送信通信量
- Top IP グループ総通信量
- Top IP グループ受信通信量
- Top IP グループ送信通信量
- Top 物理ホスト総通信量
- Top 物理ホスト受信通信量
- Top 物理ホスト送信通信量
- Top IP ホスト総通信量
- Top ローカル IP ホスト総通信量
- Top リモート IP ホスト総通信量
- Top IP ホスト受信通信量
- Top IP ホスト送信通信量
- Top ローカル IP ホスト受信通信量
- Top ローカル IP ホスト送信通信量
- Top リモート IP ホスト受信通信量
- Top リモート IP ホスト送信通信量
- Top アプリケーション層プロトコル

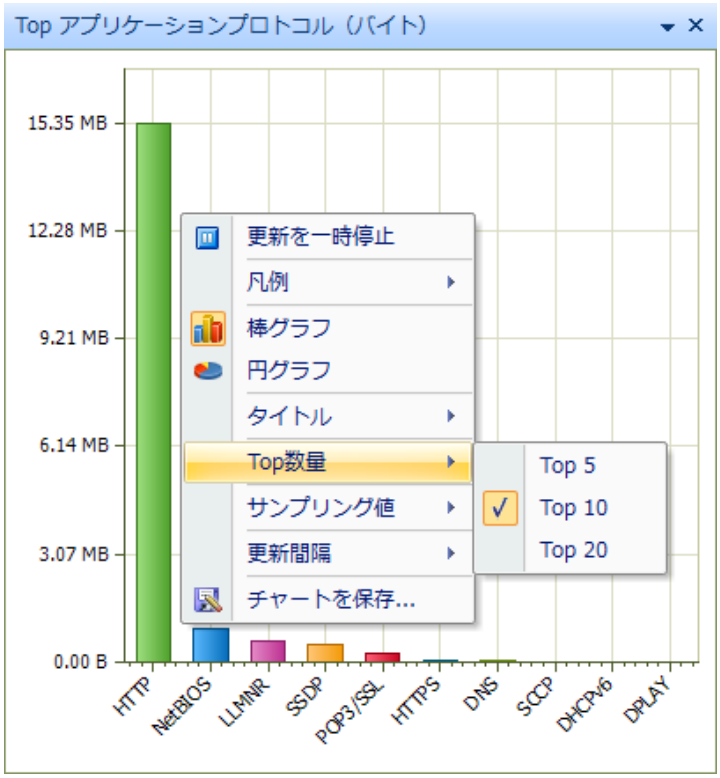
- パケットサイズ分布
- VoIP コールステータス分布
- VoIP コール MOS 分布
- Top IP コール頻度
- Top IP コール持続時間
- Top IP コール通信量
- Top ポート通信量
- Top TCP ポート通信量
- Top UDP ポート通信量
- Top プロセス総通信量
- Top プロセス TCP セッション数
- Top プロセス UDP セッション数
- Top ドメイン名
- エラーパケット比による Top コール

ヒント

1. 物理グループ/IP グループは、ノードブラウザウィンドウにおける物理ブラウザ/IP ブラウザのノードグループを表します。
2. Top アイテムによって、Top 数も変わります。例えば、物理ブラウザが三つのグループだけを持っているので、Top 物理グループ総通信量というチャートは、Top 3 の統計だけを表示します。



3. チャートで右クリックして、ポップアップメニューで **Top 数量**を選択することで、表示したい Top 数を変更することができます。
4. チャートで右クリックして、ポップアップメニューで**サンプリング値**を選択することで、サンプリング値を変更することができます。



エキスパート診断

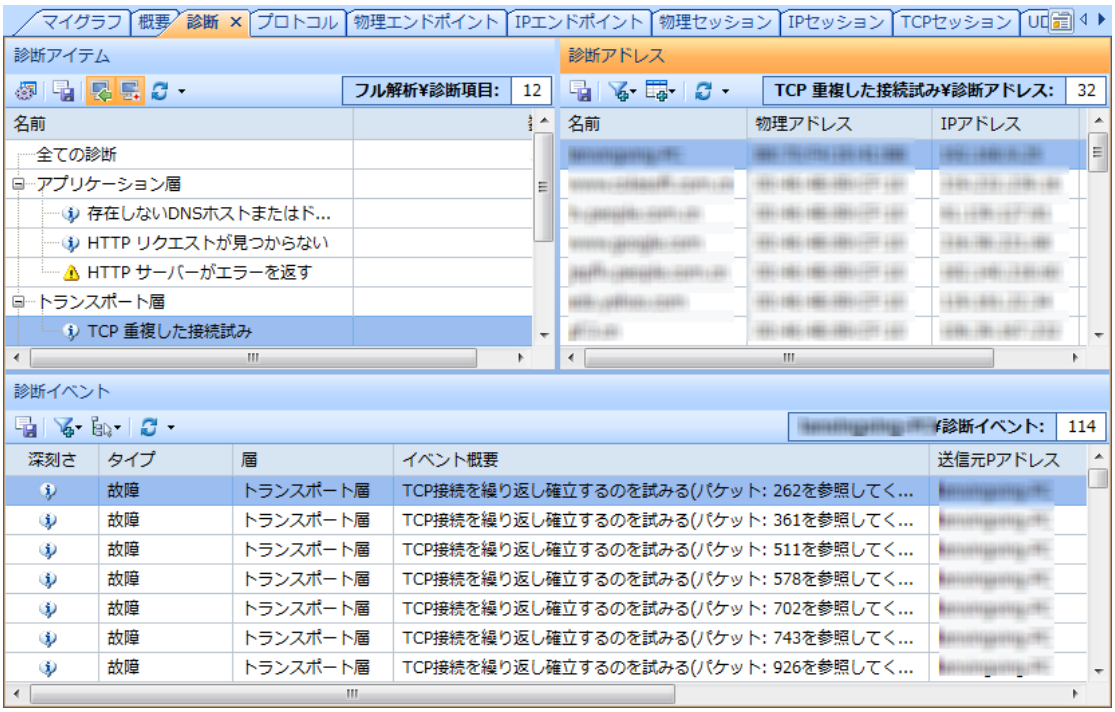
Capsa は数多くの診断イベントから構成されたエキスパート診断機能を持っています。診断イベントがトリガーされると、トリガーされたイベントの詳細情報が診断ビューに表示されます。

- 診断ビュー
- 診断イベントを解析

注意 エキスパート診断機能は Capsa Enterprise の場合にのみ、利用可能となります。

診断ビュー

診断ビューは、キャプチャーされたパケットの解析を通じて、全体ネットワークから特定のノードまでのネットワークイベントをリアルタイムに表示します。ネットワークイベントは、大量のネットワークデータに基づいて、Capsa によって定義されています。ユーザーによって、診断の設定を定義することもできます。



診断ビューは三つのパネルから構成されています。

- 診断アイテム
- 診断アドレス
- 診断イベント

マウスポインタをパネル間の境界線に移動し、ポインタが二重矢印になったとき、ポインタをドラッグすることで、パネルの幅を変更することができます。

診断アイテム

このパネルは、イベントが属している層によって、すべての診断イベントの名前と数量をリストします。すべてのイベントは以下のように重要度によって四つのタイプに分類されています。

重要度	アイコン	説明
情報		一般のメッセージで、ネットワーク問題がないことを表します。
注意		正常ではあるが、注意を払う必要がある重要な条件を表します。
アラーム		注意を払い、解決する必要があることを表します。
エラー		深刻なネットワーク問題を防ぐために、すぐに管理者による介入が必要とすることを表します。

診断イベントをダブルクリックして、そのイベントの定義とトリガー設定を確認することができます。

ノードブラウザウィンドウで特定のノードを選択された場合、このパネルは選択されたノードに関するイベントだけを表示します。

ヒント 名前と数量をクリックして、すべてのアイテムを名前、または数量によって並べ替えることができます。上位ノードと上位ノードの数量だけ並べ替えることができることに注意してください。つまり、**アプリケーション層**、**トランスポート層**、**ネットワーク層**、および**データリンク層**だけが並べ替えることができます。

右上の数は、診断イベントの数ではなくて、現在リストにおける行の数を表します。このオプションの名前は**ノードブラウザ**ウィンドウにおける選択によって、違います。

プラス/マイナスの記号をクリックすることで、イベントリストを展開したり、折りたたんだりすることができます。

ヒント すべてのイベントを.csv フォーマットで保存したい場合、すべてを展開し、**エクスポート**ボタンをクリックする必要があります。そうしないと、折りたたんだイベントは保存されません。

診断アドレス

このパネルは診断アイテムパネルで選択されたイベントのアドレスを表示します。

データリンク層におけるイベントに対して、カラム **IP アドレス**は利用できません。

カラムヘッダーをクリックして、すべてのアイテムを並べ替えることができます。

ヒント **診断アイテム**パネルで「すべての診断」を選択し、**診断アドレス**パネルでカラム**数量**をクリックすると、すべてのアドレスはイベント数によって、並べ替えます。

診断アドレスログを保存するには、エクスポートボタンをクリックします。

あるアイテムを右クリックして、そのアドレスを解決し、ネームテーブルに追加したり、そのアイテムをノードブラウザにロケートしたり、チャート、アラーム、フィルターを作成したりすることができます。

診断イベント

このパネルは診断イベントの詳細情報をリストします。このパネルのリストは**診断アイテム**パネルと**診断アドレス**パネルにおける選択によって、変わります。**診断アドレス**パネルで特定のアイテムが選択されると、**診断イベント**パネルは詳細的に選択されたアドレスのイベントだけを表示します。

カラム

カラムヘッダーを右クリックして、このリストで表示、または非表示することカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。

以下の表は、このパネルにおけるカラムについて説明しています。

カラム	説明
時間	イベントが発生した日付と時刻です。
深刻さ	イベントの深刻さで、  、  、  、  という四つのタイプがあります。
タイプ	イベントのタイプで、性能、セキュリティ、および故障という三つの種類があります。
層	イベントが属しているネットワーク層です。
イベント概要	イベントの説明で、イベントの原因とパケット番号などが含まれています。
送信元 IP アドレス	パケットの送信元 IP アドレスです。

送信元 MAC アドレス	パケットの送信元 MAC アドレスです。
宛先 IP アドレス	パケットの宛先 IP アドレスです。
宛先 MAC アドレス	パケットの宛先 MAC アドレスです。
送信元ポート	パケットの送信元ポートです。
宛先ポート	パケットの宛先ポートです。

ヒント あるアイテムをダブルクリックして、**パケット**ウィンドウで詳細なパケット情報を表示することができます（あるアイテムを右クリックして、**新しいウィンドウでパケットを表示する**を選択することもできます）。**パケット**ウィンドウは**パケット**ビューと同じように表示されます。

診断イベントを解析

トリガーされた診断イベントがあるとき、何が発生したかを知りたい場合もあります。ここではそのヒントをいくつか紹介します。

トリガーされたイベントが表示される場合、診断アイテムパネルでそのイベントを選択して、診断アドレスパネルはそのイベントのアドレスをリストします。診断アドレスパネルで関心のアドレスをクリックすると、診断イベントパネルは、そのアドレスの詳細情報を表示します。診断イベントパネルにおけるイベント概要はそのイベントの概要情報を提供します。それをダブルクリックして、パケットのデコード情報が表示されます。

イベントアドレスの他のトラフィックデータを表示したい場合、そのアドレスを右クリックし、ノードブラウザにロケートすることで、統計ビューではそのアドレスに関するデータだけが表示されます。たとえばプロトコルビューで top アプリケーションを、ログビューでそのアドレスのアクティビティログを、マトリックスビューでそのアドレスの通信状態を確認することができます。

イベントが発生した原因と解決する方法を知りたい場合、診断アイテムパネルでそのイベントをダブルクリックして、**診断の設定**ダイアログボックスが開かれます。ここでそのネットワークイベントの考えられる原因と解決方法がリストされています。

以下のリストはすべての診断イベントの考えられる原因と解決方法について説明しています。

- アプリケーション層診断イベント
- トランスポート層診断イベント
- ネットワーク層診断イベント
- データリンク層診断イベント

アプリケーション層診断イベント

以下の表はアプリケーション層における診断イベントについて説明しています。

イベント	説明	タイプ	考えられる原因	解決方法

イベント	説明	タイプ	考えられる原因	解決方法
DNS サーバーの応答が遅い	DNS サーバーのレスポンス時間がレスポンス遅延閾値以上になります。	性能	ネットワークがビジー状態で、ネットワークの負荷が大きすぎます。 クライアント側から DNS サーバーへの接続スピードが遅すぎます。 DNS サーバーの性能が悪いです。 DNS サーバーが過負荷です。	ネットワーク上で実行されるアプリケーションサービスをチェックしてください。 他の DNS サーバーアドレスを使用します。 DNS サーバーのセキュリティと動作状態をチェックしてください。 DNS サーバーをアップグレードします。
存在しない DNS ホストまたはドメイン名	リクエストされたホスト、またはドメイン名が存在しません。	故障	IP アドレスまたはドメイン名は無効です。 DNS サーバーの DNS 一覧表が不完全です。 DNS の逆引きが無効になっています。	IP アドレスまたはドメイン名が正しいことを確認してください。 DNS サーバーアドレスを変更します。
DNS サーバーがエラーを返す	DNS サーバーは無効な名前以外のエラーを返します。すなわちリクエストされたホスト、またはドメイン名が返されません。	故障	クエリフォーマットエラーです。 クエリに失敗しました。 DNS サーバーは未実現、拒否、または保留を返します。	DNS クエリが正しいことを確認してください。 DNS サーバーアドレスを変更します。
SMTP サーバーの応答が遅い	SMTP サーバーのレスポンス時間がレスポンス遅延閾値以上になります。	性能	ネットワークがビジー状態で、ネットワークの負荷が大きすぎます。 クライアント側から SMTP サーバーへの接続スピードが遅すぎます。 SMTP サーバーの性能が悪いです。 SMTP サーバーが過負荷です。	ネットワーク上で実行されるアプリケーションサービスをチェックしてください。 ルーターの設定を更新します。 SMTP サーバーのセキュリティと動作状態をチェックしてください。 SMTP サーバーをアップグレードします。
SMTP 不審セッション	TCP ポート 25 を利用して、非 SMTP データを転送します。	セキュリティ	TCP ポート 25 で動作するアプリケーションは、非 SMTP トラフィックを生成しています。	ポート 25 を利用しているアプリケーションをチェックしてください。 送信元ポートと宛先ポートのトラフィック内容をチェックしてください。
SMTP サーバ	TCP 接続が確	故障	クライアントプログラ	クライアントが正しいコ

イベント	説明	タイプ	考えられる原因	解決方法
ーがエラーを返す	立された後、SMTP 接続又はリクエストは、SMTP サーバーに拒否されます。		ムが無効なコマンドを実行しています。 クライアントアプリケーションが設定されたユーザー名とパスワードが間違っています。 SMTP サーバーが過負荷です。 SMTP サーバー側のソフトウェア設定が不正確です。	マンドを実行しているのを確認してください。 クライアントアプリケーションにおけるユーザー名とパスワードをチェックしてください。 SMTP サーバーが攻撃されていないかを調べます。 SMTP サーバーのソフトウェア設定が正しいことを確認してください。
POP3 サーバーの応答が遅い	POP3 サーバーのレスポンス時間がレスポンス遅延閾値以上になります。	性能	ネットワークがビジー状態で、ネットワークの負荷が大きすぎます。 クライアント側から POP3 サーバーへの接続スピードが遅すぎます。 POP3 サーバーの性能が悪いです。 POP3 サーバーが過負荷です。	ネットワーク上で実行されるアプリケーションサービスをチェックしてください。 ルーターの設定を更新します。 POP3 サーバーのセキュリティと動作状態をチェックしてください。 POP3 サーバーをアップグレードします。
POP3 不審セッション	TCP ポート 110 を利用して、非 POP3 データを転送します。	セキュリティ	TCP ポート 110 で動作するアプリケーションは、非 POP3 トラフィックを生成しています。	ポート 110 を利用しているアプリケーションをチェックしてください。 送信元ポートと宛先ポートのトラフィック内容をチェックしてください。
POP3 サーバーがエラーを返す	TCP 接続が確立された後、POP3 接続又はリクエストは、POP3 サーバーに拒否されます。	故障	クライアントプログラムが無効なコマンドを実行しています。 クライアントアプリケーションが設定されたユーザー名とパスワードが間違っています。 POP3 サーバーが過負荷です。 POP3 サーバー側のソフトウェア設定が不正確です。	クライアントが正しいコマンドを実行しているのを確認してください。 クライアントアプリケーションにおけるユーザー名とパスワードをチェックしてください。 POP3 サーバーが攻撃されていないかを調べます。 POP3 サーバーのソフトウェア設定が正しいことを確認してください。
FTP サーバーの応答が遅い	FTP サーバーのレスポンス時間がレスポンス遅延閾値以上になります。	性能	ネットワークがビジー状態で、ネットワークの負荷が大きすぎます。 クライアント側から FTP サーバーへの接続	ネットワーク上で実行されるアプリケーションサービスをチェックしてください。 ルーターの設定を更新します。

イベント	説明	タイプ	考えられる原因	解決方法
			スピードが遅すぎます。 FTP サーバーの性能が悪いです。 FTP サーバーが過負荷です。	FTP サーバーのセキュリティと動作状態をチェックしてください。 FTP サーバーをアップグレードします。
FTP 不審セッション	TCP ポート 21 を利用して、非 FTP データを転送します。	セキュリティ	TCP ポート 21 で動作するアプリケーションは、非 FTP トラフィックを生成しています。	ポート 21 を利用しているアプリケーションをチェックしてください。 送信元ポートと宛先ポートのトラフィック内容をチェックしてください。
FTP サーバーがエラーを返す	TCP 接続が確立された後、FTP 接続又はリクエストは、FTP サーバーに拒否されます。	故障	クライアントプログラムが無効なコマンドを実行しています。 クライアントアプリケーションが設定されたユーザー名とパスワードが間違っています。 FTP サーバーが過負荷です。 クライアントの動作モードはサーバーと一致しません。 FTP サーバー側のソフトウェア設定が不正確です。	クライアントが正しいコマンドを実行しているのを確認してください。 クライアントアプリケーションにおけるユーザー名とパスワードをチェックしてください。 FTP サーバーが攻撃されていないかを調べます。 サーバーがクライアントの動作モードをサポートしているのを確認してください。 FTP サーバーのソフトウェア設定が正しいことを確認してください。
HTTP クライアントエラー	HTTP サーバーは 404 以外の 4xx コードを返して、クライアントエラーを示します。クライアント側がリクエストしたページが見つからないことを表します。	故障	リクエストが不完全です。 無許可リクエストです。 アクセスが禁止されています。 リクエスト方法が許可されません。 リクエストがタイムアウトになります。 リクエストした URL が長すぎます。 サポートされていないメディアタイプです。	リクエスト内容をチェックしてください。 リクエストを変更します。 リクエストを変更したり、許可されているアカウントを使用します。 リクエスト方法を変更します。 クライアントからリクエストを再送信します。 リクエストした URL を変更します。 メディアタイプを変更します。
不審な HTTP セッション	TCP ポート 80 を利用して、非 HTTP データを転送しま	セキュリティ	TCP ポート 80 で動作するアプリケーションは、非 HTTP トラフィックを生成していま	ポート 80 を利用しているアプリケーションをチェックしてください。 送信元ポートと宛先ポー

イベント	説明	タイプ	考えられる原因	解決方法
	す。		す。	トのトラフィック内容をチェックしてください。
HTTP リクエストが見つからない	リクエストした URL が見つからない場合、HTTP サーバーがこのエラーを返します。	故障	無効な URL です。 DNS サーバーのデータシートには、入力されたドメイン名と対応の IP のマップ関係が含まれていません。	URL の有効性を確認してください。 DNS サーバーアドレスを変更します。
HTTP サーバーがエラーを返す	HTTP サーバーは 5xx エラーコードを返して、サーバーエラーを示します。通常、クライアントのリクエストが有効です。	故障	サーバー内部エラーです。 その HTTP のバージョンがサポートされていません。 サーバー未完了です。 サーバーがタイムアウトになります。 サーバーの利用できないサービスです。	HTTP サーバーの設定を変更します。 バージョンタイプをサポートするために HTTP サーバーをアップグレードします。
HTTP レスポンスが遅すぎる	HTTP サーバーのレスポンス時間がレスポンス遅延閾値以上になります。	性能	ネットワークがビジー状態で、ネットワークの負荷が大きすぎます。 クライアント側から HTTP サーバーへの接続スピードが遅すぎます。 HTTP サーバーの性能が悪いです。 HTTP サーバーが過負荷です。	ネットワーク上で実行されるアプリケーションサービスをチェックしてください。 ルーターの設定を更新します。 HTTP サーバーのセキュリティと動作状態をチェックしてください。 HTTP サーバーをアップグレードします。
VoIP SIP クライアント認証エラー	クライアント側のリクエストは、「407 プロキシ認証」というサーバーからのレスポンスを引き起こしました。	故障	クライアントは、認証を要求するリクエストを送信する前に、クライアント自身が認証されません。	クライアントは正しい認証情報を送信します。
VoIP RTP パケット順番誤り	RTP パケットは送信順番によって到着しません。後に送信されたパケットは、前に送信された	性能	送信側と受信側の転送距離が長すぎるか、又は転送スピードが遅すぎます。	ルーターの設定を変更したり、ネットワーク環境を最適化します。

イベント	説明	タイプ	考えられる原因	解決方法
	パケットより早く到着しました。			
VoIP RTP パケットロス	RTP パケットが不完全なシーケンス番号を持つ場合、RTP パケットロスが発生します。	性能	ネットワークがビジー状態で、或いはネットワークがオーバーロードしました。 送信側と受信側の転送距離が長すぎるか、又は転送スピードが遅すぎます。 受信側のバッファがオーバーフローしました。	ネットワーク上で実行されるアプリケーションサービスをチェックします; ソフトウェアとハードウェアの配置をチェックしたり、アップグレードしたりします。 ルーターの設定を変更したり、ネットワーク環境を最適化します。 受信側のホストの動作状態をチェックします。
SDP 情報欠損またはフォーマットエラー	SIP パケットでは、SDP データが欠損しているか、あるいは SDP 情報のフォーマットが正しくありません。	性能	パケットが MTU の制限を超えました。 伝送中、パケットにエラーが発生しました。 パケットが改ざんされました。	ネットワークデバイス上で MTU の設定をチェックします。 ネットワーク上でソフトウェアとハードウェアの配置をチェックしたり、アップグレードしたりします。 ネットワークセキュリティを向上させます。

トランスポート層診断イベント

以下の表はトランスポート層における診断イベントについて説明しています。

イベント	説明	タイプ	考えられる原因	解決方法
TCP 接続が拒否された	クライアントは TCP 接続の初期化を試みるが、ホストに拒否されます。	故障	クライアントは、サーバーの提供していないサービスをリクエストしています。 サーバーのバッファメモリが不足し、そのリクエストを処理する十分なリソースがありません。	ホストでサービスの可用性を確認してください。 ホストが処理できる接続の最大数をチェックします。
TCP 重複した接続試み	クライアントは TCP 接続確立を複数回試みます。	故障	サーバーが存在しないか、あるいは起動されていません。 クライアントは、サーバーの提供していないサービスをリク	サーバーが確かに存在し、起動していることを確認します。 そのサービスに対応するサーバーのポートを開きます。

イベント	説明	タイプ	考えられる原因	解決方法
			エストしています。 クライアントからのSYN パケット、またはサーバーからのACK パケットは、紛失または破損しています。 クライアントからのSYN パケット、またはサーバーからのACK パケットは、ファイアウォールに阻止されます。	SYN パケットがサーバーに到着することを確認します。そしてサーバーが ACK している場合、ACK パケットがクライアントに到着することを確認します。 ファイアウォールのアクセス制御ポリシーを開きます。
TCP 再送信パケット	送信側は受信側のあるパケットに対する ACK 応答を受信しない場合、このパケットを再送信します。	性能	ネットワークがビジー状態で、ネットワークの負荷が大きすぎます。 スイッチ、またはルーターの過負荷により、クライアントからのパケット、またはサーバーからのACK パケットが紛失しています。 送信側と受信側の転送距離が長すぎるか、又は転送スピードが遅すぎます。 受信側のバッファがオーバーフローしました。 転送中、TCP パケットは紛失または破損しています。 分割された TCP パケットのあるセグメントは紛失または破損しています。	ネットワーク上で実行されるアプリケーションサービスをチェックしてください。 スイッチとルーターの動作状態をチェックします。 ルーターの設定を更新します。 受信側のホストの動作状態をチェックします。
TCP 不正チェックサム	送信側はパケットの送信前にチェックサムを計算し、その値をパケットに書き込みます。受信側はパ	故障	このパケットは転送中に破損しています。 すべてのパケットのTCP チェックサムが間違った場合、TCP チェックサムの計算が有効にされていない可能性がありま	

イベント	説明	タイプ	考えられる原因	解決方法
	ケットの受信後にそのチェックサムを再度計算します。その二つの値が一致しません。		す。 Windows の TCP/IP プロトコルスタックは TCP チェックサムを計算しません。	
TCP 応答が遅い	ACK パケットのレスポンス時間はレスポンス遅延閾値以上になります。	性能	ネットワークがビジー状態で、ネットワークの負荷が大きすぎます。 送信側と受信側の転送距離が長すぎます。 ACK パケットは転送中に紛失、または破損しています。 送信側と受信側のルーターはオーバーロードしています。	ネットワーク上で実行されるアプリケーションサービスをチェックしてください。 ルーターの設定を更新します。 ACK パケットが紛失または破損していないかをチェックします。 ルーターをアップグレードします。
TCP 繰り返し確認	同じ ACK 番号と SEQ 番号を持っているパケットは少なくとも三つ存在します。	性能	ネットワークビジーにより、TCP セグメントは失われています。 他のネットワーク問題により、パケットロスが発生しています。 TCP 接続の反対側はレスポンスしません。	ネットワークがビジーになっていないかを調べます。 他のネットワーク問題によりパケットロスが発生していないかを調べます。 TCP 接続の両側のホストは正常に動作しているかをチェックします。
TCY SYN ストーム	大量の TCP SYN パケットは閾値を上回るスピードで送信されます。	セキュリティ	DoS または DDoS 攻撃が発生しています。	DoS または DDoS 攻撃が発生していないかを調べます。
TCP ヘッダーオフセットエラー	5 以下の TCP ヘッダーオフセット値が現れます。	セキュリティ	送信元ホストは間違った TCP パケットを送信しています。	送信元ホストが攻撃を行っていないかを調べます。 関連のプロセスが正常かどうかを調べます。
TCP ポートスキャン	ローカルまたはリモートホストに	セキュリティ	ワームウィルスに感染しているローカルホストは自動的に	ホストがワームウィルスに感染していないかを調べます。

イベント	説明	タイプ	考えられる原因	解決方法
	よってスキャンされた TCP ポートの数は閾値以上になります。		TCP ポートをスキャンしています。スキャンソフトウェアは TCP ポートをスキャンしています。	送信元ホストで手動スキャンがあるかどうかをチェックします。

ネットワーク層診断イベント

以下の表はネットワーク層における診断イベントについて説明しています。

イベント	説明	タイプ	考えられる原因	解決方法
IP 不正なチェックサム	送信側はパケットの送信前に IP チェックサムを計算し、その値をパケットに書き込みます。受信側はパケットの受信後にそのチェックサムを再度計算します。その二つの値が一致しません。	故障	このパケットは転送中に破損しています。すべてのパケットの IP チェックサムが間違った場合、IP チェックサムの計算が有効にされていない可能性があります。Windows の TCP/IP プロトコルスタックは IP チェックサムを計算しません。	伝送回路の電磁干渉をチェックしたり、転送設備に故障がないかを調べたりします。
IP TTL サイズが小さすぎる	IP パケットの TTL 値が 0 又は 1 になると、そのパケットはまもなく期限切れになり廃棄されることを示します。	故障	ネットワークループが発生しています。発信元 IP ホストは低 TTL 値でパケットを送信しています。	ルーターのルーティングテーブル情報を調べます。送信元ホストが故障している可能性があります。
IP アドレス競合	ホストは、他のデバイスが自分の IP アドレスを使用しようとしていることを検出し、ARP 情報でそのデバイスに通知します。	セキュリティ	あるデバイスはすでに使用されている IP アドレスを使用しようとしています。	
ICMP 宛先到	ルーターは、	故障	送信元ホストが利用し	送信元ホストのトランス

イベント	説明	タイプ	考えられる原因	解決方法
達不可能	ネットワーク到達不可能、ホスト到達不可能、ポート到達不可能以外の宛先到達不可能情報を送信元ホストに報告しています。		ているトランスポートプロトコルは宛先ホストまたはルーターで利用できません。 ルーターでセグメント化することができません。 ルーティングは失敗しました。 ルーターは特定の ToS のパケットを転送できません。 ルーターの通信監理ルールによって制限されています。	ポートプロトコルを変更したり、あるいはルーターと宛先ホストがサポートしているトランスポートプロトコルを追加したりします。 ルーターの設定をチェック、更新します。
ICMP ネットワーク到達不可能	ルーターは、ネットワークが利用できない、または目的ネットワークへのパスが利用できないことを送信元ホストに報告しています。	故障	ルーターにデフォルトルートが設定されていません。 目的ネットワークが存在しません。 ルーターは目的ネットワークへのパスを見つけることができません。 目的ネットワークまでの距離は、ルーターのルーティングプロトコルに指定された最大距離を超えています。	ルーターにデフォルトルートを追加します。 ルーターにそのネットワークのルート又はデフォルトルートを追加します。 ルーターにデフォルトルートを追加します。 ルーターでルーティングプロトコルを変更します。
ICMP ホスト到達不可能	ルーターは、宛先ホストが見つからないことを送信元ホストに報告しています。	故障	宛先ホストが存在しません。 宛先ホストが起動していません。	宛先ホストが存在するかどうかをチェックします。 宛先ホストが起動しているかどうかをチェックします。
ICMP ポート到達不可能	宛先ホストまたはルーターは、リクエストされたポートが非アクティブであることを送信元ホストに報告しています。	故障	リクエストされたポートのサービスは有効になっていません。 リクエストされたポートのサービスは故障状態にあります。 そのポートへのアクセスはファイアウォールまたはルーターに阻止されています。	リクエストされたポートのサービスを有効にします。 そのサービスの設定をチェックします。 ファイアウォールまたはルーターでそのポートのアクセス制御ポリシーを有効にします。
ICMP ホスト	ルーターは、	性能	ポートマッピングを設	内部 IP アドレスを利用

イベント	説明	タイプ	考えられる原因	解決方法
リダイレクト	宛先ホストのための他のルートを使用する必要があることを送信元ホストに報告しています。		定した後、LAN 内のホストは外部ドメインを利用して、内部サーバーにサクセスしています。 ICMP 攻撃が発生しています。	して、サーバーにアクセスします。 パケットに基づいて、攻撃の源を調べます。
ICMP ネットワークリダイレクト	ルーターは、目的ネットワークのための他のルートを使用する必要があることを送信元ホストに報告しています。	性能	ポートマッピングを設定した後、LAN 内のホストは外部ドメインを利用して、内部サーバーにサクセスしています。 ICMP 攻撃が発生しています。	内部 IP アドレスを利用して、サーバーにアクセスします。 パケットに基づいて、攻撃の源を調べます。
ICMP 送信元抑制	ルーターまたは宛先ホストは、ICMP 送信元抑制パケットを送信元ホストに送信しています。	故障	ネットワークがビジー状態で、ネットワークの負荷が大きすぎます。 宛先ホストのメモリが不足しているか、あるいはサービスが利用できません。 ルーターのキャッシュスペースが不足しています。 DoS または DDoS 攻撃が発生しています。	ネットワーク上で実行されるアプリケーションサービスをチェックしてください。 宛先ホストをチェックし、不必要なサービスを終了します。 ルーターのキャッシュスペースを拡大します。 送信元ホストから悪意攻撃がないかを調べます。
ルーティングループ	ルーティングプロトコルを不適切に有効にしているため、冗長リンクがなくても、ルーティングループになる可能性があります。	故障	スタティックルーティング設定が不合理です。 ダイナミックルーティング設定が正しくありません。定期的なブロードキャストがこの問題を引き起こしました。	スタティックルーティングの設定が正しいことを確認してください。 ルーターの設定が正しいことを確認してください。

データリンク層診断イベント

以下の表はデータリンク層における診断イベントについて説明しています。

イベント	説明	タイプ	考えられる原因	解決方法
ARP フォーマットエラー	イーサネットで正しく実行	セキュリティ	ARP ヘッダーにおけるアドレス情報は、攻撃	ARP 攻撃が発生していないかを調べます。

イベント	説明	タイプ	考えられる原因	解決方法
	できない、RFC の定義に違反しているフレームフォーマットです。例えば、MAC アドレスがマルチキャストアドレスであること、あるいは ARP ヘッダーにおけるアドレス情報が MAC ヘッダーにおける情報と一致しないこと。		のために改ざん、偽造されています。	
ARP リクエストストーム	事前定義のサンプリング期間において、毎秒の ARP リクエストパケット数は閾値以上になります。	セキュリティ	送信元ホストが ARP リクエストを大量に送信していないかを調べます。 ホストは自動的に ARP スキャンを実行するウィルスに感染しています。 スキャンアプリケーションは ARP スキャンを実行しています。 トラフィックをキャプチャーするポートがミラーリングされていないか、あるいはプログラムがインストールされているマシンがミラーポートに接続されていません。	ウィルス対策ソフトウェアを利用して、ARP リクエストを大量に送信するホストをスキャンします。 ARP スキャンを実行しているアプリケーションを終了します。 トラフィックをキャプチャーするポートをミラーリングし、ミラーポートに接続しているマシンにプログラムをインストールします。
ARP スキャン	事前定義のサンプリング期間において、未応答の ARP リクエストパケットの割合は閾値以上になります。	セキュリティ	ARP パケットを送信する送信元ホストはスキャンを実行するプログラムを持っています。 ネットワークにはモニターアプリケーションがあります。 ホストは自動的に ARP スキャンを実行するウィルスに感染しています。	送信元ホストは、スキャンを実行しているプログラムを持っていないかをチェックします。 モニタープロセスを終了します。 ウィルス対策ソフトウェアを利用して、ARP スキャンを実行するホストをスキャンします。 スキャンアプリケーショ

イベント	説明	タイプ	考えられる原因	解決方法
			スキャンアプリケーションは ARP スキャンを実行しています。	ンを終了します。
ARP 応答が多すぎる	事前定義のサンプリング期間において、リクエストしていないホストの ARP レスポンスパケット数は閾値以上になります。	セキュリティ	ネットワークに ARP スプーフィングがあります。 プログラムはコアスイッチデバイスにインストールされ、ARP リクエストパケットは隔離されています。	ARP レスポンスパケットを大量に送信しているホストにおいて ARP スプーフィングがあるかどうかを調べます。
物理ループ	設定または接続が誤って、冗長リンクが発生したので、物理ループを引き起こしました。	故障	異なるスイッチ間の相互接続によって、物理ループを引き起こしました。 ネットワークケーブルを制作する際にライン 1、2 とライン 3、6 がショットして、物理ループを引き起こしました。 ロードバランスをとる際、一端のスイッチは設定されましたが、他端のスイッチまたはサーバーは設定されていないので、物理ループを引き起こしました。 同じスイッチにおいて、直接ネットワークケーブルを同じ VLAN の二つのポートに接続したので、物理ループを引き起こしました。	すべての設備が 802.1d をサポートすれば、spanning tree プロトコルを有効にして、物理ループを避けます。 EIA/TIA 568A、EIA/TIA 568B 標準によって、ネットワークケーブルを制作します。同時にネットワークケーブルテスターでケーブルをテストし、品質を確保します。 ロードバランスをとる際、接続されたすべての設備の設定が正しいことを確認してください。 ネットワークケーブルにおける二つの RJ45 ヘッダーを同じスイッチに挿入しないでください。BAS の MAC アドレスとアップリンクポートをバインドすることで、ある VLAN で物理ループが発生した後、MAC アドレスの学習混乱がほかの VLAN に影響を与えることを避けます。

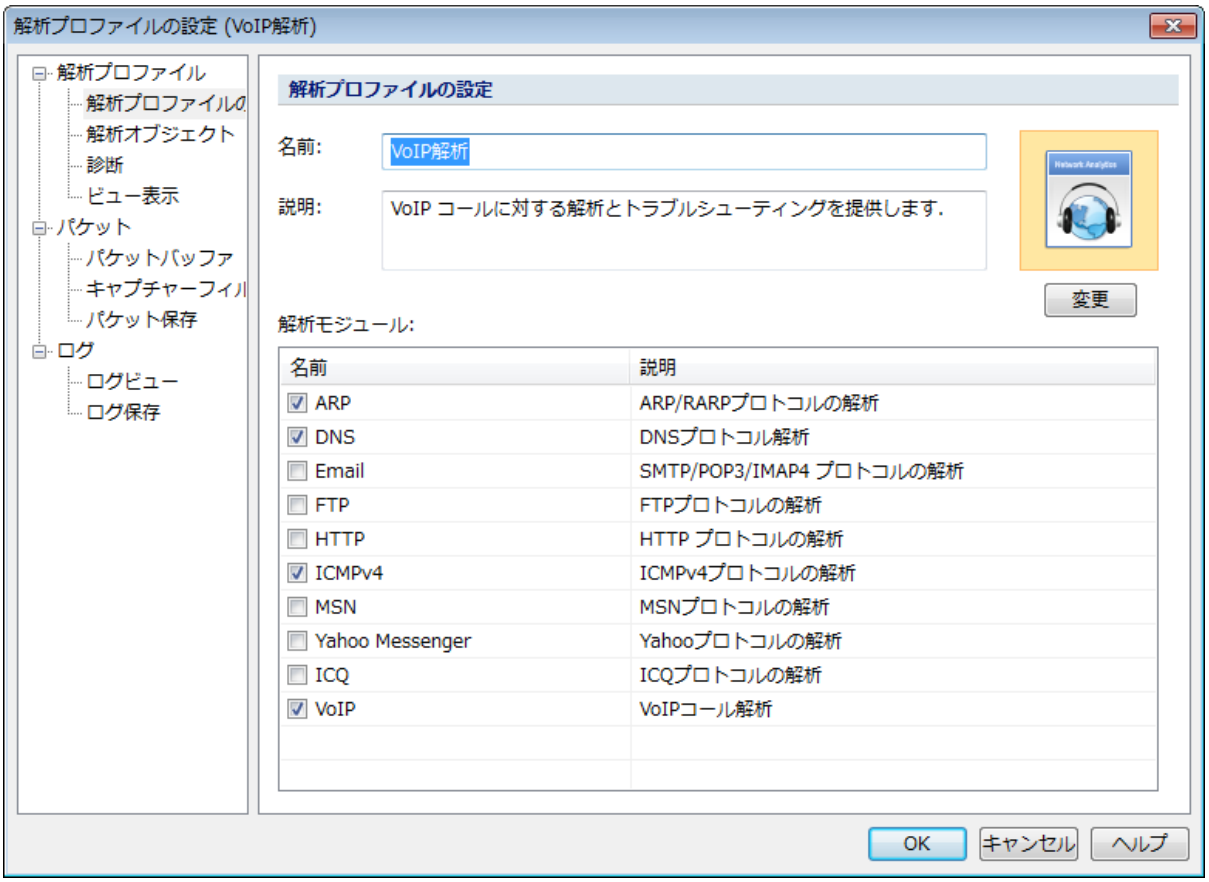
VoIP 解析

VoIP 解析はフル解析と VoIP 解析という二つの解析プロファイルの場合にのみ、利用可能となります。

VoIP 解析プロファイル

他の解析プロファイルと同じように VoIP 解析プロファイル設定を変更するには、スタートページにおける VoIP 解析プロファイルアイコンをダブルクリックして、設定ボックスが開かれます。

設定ボックスは以下のように表示されます。



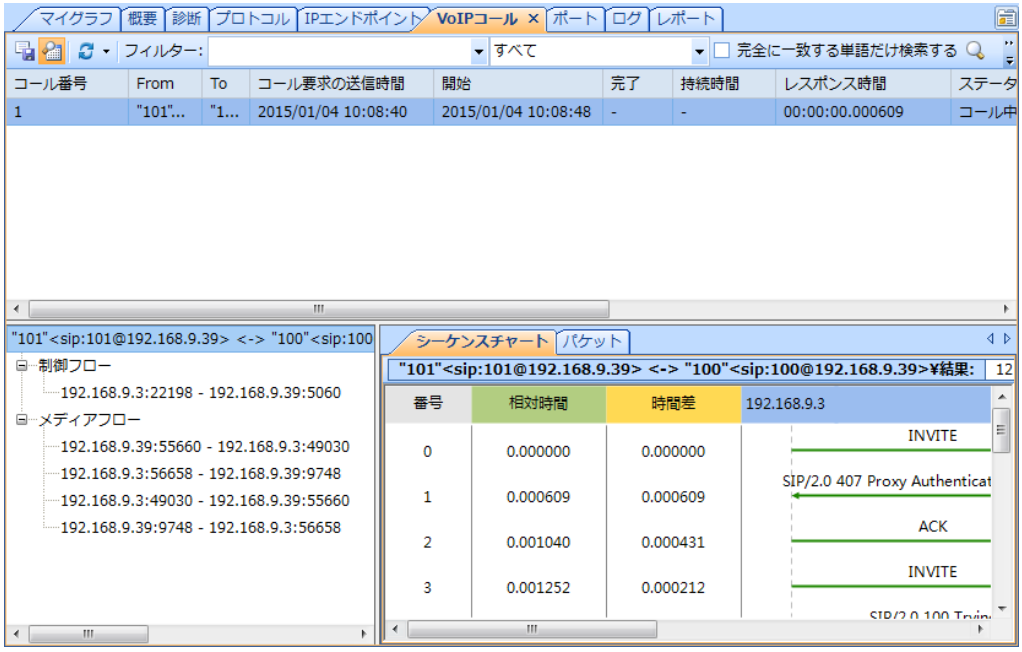
VoIP コールを解析するには、VoIP 解析モジュールを有効にする必要があります。

解析モジュール設定の他に、VoIP 解析プロファイルには解析オブジェクト、診断、ビュー表示、キャプチャーフィルター、パケット保存、ログビュー、およびログ保存の設定も含まれています。これらの設定の詳しいことについては、解析プロファイルをご参照ください。

VoIP 解析のために、Capsa は VoIP SIP クライアント認証エラー、VoIP RTP パケットロス、VoIP RTP パケット順番誤りという三つの診断イベントと、VoIP シグナリングログ、VoIP コールログという二つのログタイプを提供します。

VoIP コールビュー

VoIP コール上側パネルと下側の下位パネルから構成されています。  をクリックして、下側パネルを表示、非表示することができます。



上側パネルはすべての VoIP コール記録をリストします。ツールバーとポップアップメニューにおけるボタンは他の統計ビューとまったく同じです（詳しいことは[ツールバーとポップアップメニュー]をご参照ください）。

デフォルトでは、VoIP コールビューは、VoIP コール番号に基づいて VoIP コールを表示します。カラムヘッダーにおける他の統計フィールドをクリックして、そのフィールドに基づいて VoIP コールを並べ替えることもできます。例えば、カラムヘッダーにおける「持続時間」をクリックして、コール持続時間に基づいて、VoIP コールを並べ替えることができます。VoIP カラムの詳しいことについて、[VoIP コールビューにおけるカラムについて]をご参照ください。

下位パネルは上側パネルで選択された VoIP コールの情報を表示します。下位パネルの詳しいことについて、[VoIP ビュー下位パネル] をご参照ください。

注意 このバージョンでは、SIP プロトコルに基づくコールしか解析されることができません。

VoIP コールビュー下位パネル

VoIP コールビュー下位パネルは左側の部分と右側の部分から構成されています。

左側の部分は、上側パネルで選択されたコールの制御フローとメディアフロー情報を含め、階層的に VoIP コールを表示します。右側の部分は、左側の部分で選択されたフローをメディア情報タブ、シーケンスチャートタブ、パケットタブで詳細的に表示します。

あるメディアフローを選択して、コーデック、ジッタ、MOS などを含むそのフローの関連情報がメディア情報タブで表示されます。

- **送信元 IP**:選択されたメディアフローの送信元 IP ドレスです。
- **送信元ポート**:選択されたメディアフローの送信元ポートです。
- **宛先 IP**:選択されたメディアフローの宛先 IP ドレスです。
- **宛先ポート**: 選択されたメディアフローの宛先ポートです。
- **SSRC 識別子**:選択されたメディアフローの同期ソース識別子です。
- **開始**:選択されたメディアフローの開始時間です。
- **完了**:選択されたメディアフローの完了時間です。
- **持続時間**:選択されたメディアフローの持続時間です。
- **ジッタ**:選択されたメディアフローのジッタ値です。ジッタ値が小さいほど、メディア信号がよくなります。
- **MOS**:選択されたメディアフローの MOS 値です。
- **パケットロス**:選択されたメディアフローのパケットロスの割合です。
- **メディアタイプ**: 選択されたメディアフローのメディアタイプです。オーディオまたはビデオである可能性があります。
- **コーデック**:選択されたメディアフローのエンコードタイプです。スタティックタイプの場合、実際のタイプで表示され、ダイナミックタイプの場合、不明と表示されます。

シーケンスチャートタブは、選択されたコールまたはフローのタイムシーケンスを表示します。

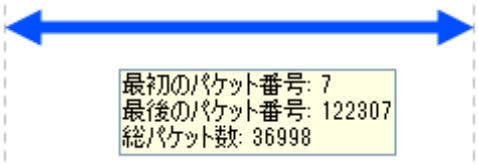
以下のリストは、シーケンスチャートタブにおけるカラムについて説明しています。

- **番号**:パケット、または VoIP コールのメディアフローの番号です。0 から始めます。
- **相対時間**:選択されたパケットからフローにおける最初のパケットまでのタイムスタンプの時間です。
- **時間差**:選択されたパケットとその前のパケットの時間差です。
- **呼び出し IP**:呼び出しの IP アドレスです。
- **呼び出し先 IP**:呼び出し先の IP アドレスです。

シーケンスチャートタブは矢印付きのラインでパケットの方向を表します。左向きの矢印は呼び出し先 IP から呼び出し IP までのパケットを、右向きの矢印は呼び出し IP から呼び出し先 IP までのパケットを、双方向の矢印は呼び出し IP と呼び出し先 IP の間のパケットを表します。

制御フローとメディアフローはラインの色で区別します。緑のラインは制御フローのパケットを表し、青のラインはメディアフローのパケットを表します。

マウスをシーケンスチャートタブにおけるラインに移動すると、そのラインは厚く表示されます。さらにそのフローのヒントも表示されます。制御フローの場合、制御フローパケットのカレントパケットナンバーが表示されます。メディアフローの場合、下図のように最初のパケット番号、最後のパケット番号、および総パケット数が表示されます。



- 最初のパケット番号:メディアフローにおける最初のパケット番号です。
- 最後のパケット番号:メディアフローにおける最後のパケット番号です。
- 総パケット数:メディアフローの総パケット数です。

VoIP コールビューにおけるカラムについて

以下の表は VoIP ビューにおけるカラムについて説明しています。

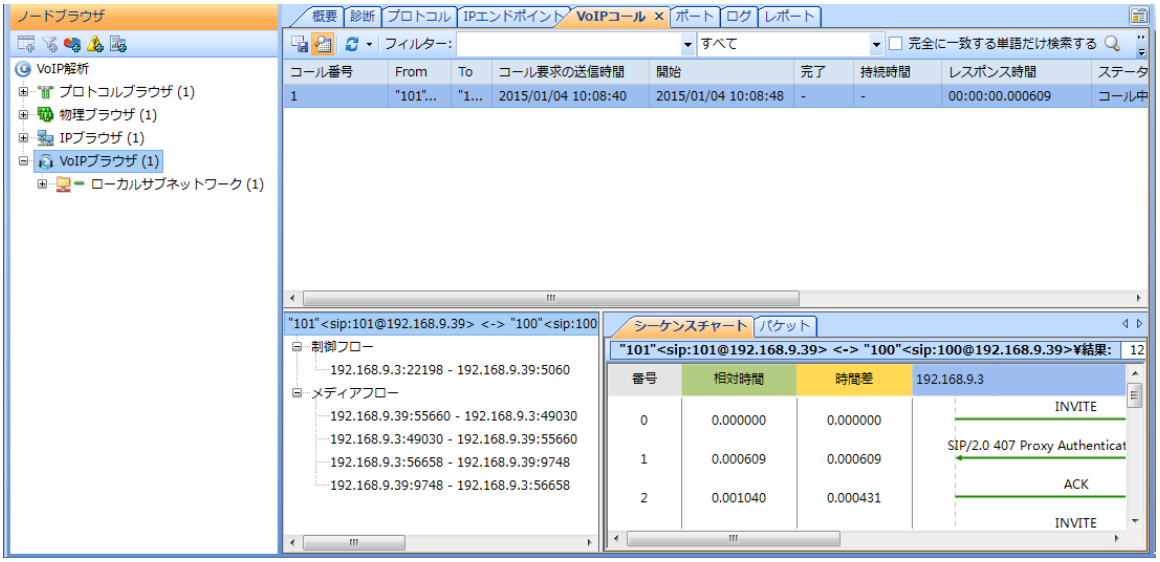
カラム	説明
コール番号	コールの番号で、1 から始めます。
開始	コールの開始時間で、コールまたはメディアフローにおける最初のパケットのタイムスタンプです。ミリ秒の精度で表示されます。
完了	コールの完了時間で、コールまたはメディアフローにおける最後のパケットのタイムスタンプです。ミリ秒の精度で表示されます。
持続時間	コールの持続時間で、開始時間から完了時間を引いたものです。
レスポンス時間	サーバーがコールリクエストにレスポンスする時間です。コール要求の送信時間（Invite）から 100 Trying までの持続時間はミリ秒の精度で表示されます。
From	コールを開始する ID です。
To	コールを引き受ける ID です。
コール ID	プロトコルが H.248 の場合、コール ID がないので、「N/A」と表示されます。 プロトコルが SIP の場合、実際のコール ID で表示されます。
ステータス	各コールは以下の四つのステータスがあります。 ダイヤル中:コールが開始されているが、メディアフォローを受信していません。 コール中:メディアフォローの受信から開始し、コールが切れたら、終了します。 失敗:シグナリングは正常であるが、何のメディアフォローもありませ

カラム	説明
	ん。 終了:コールが終了しました。
MOS-V	MOS スコアはコールのビデオストリームに対して、計算します。
MOS-A	MOS スコアはコールのオーディオストリームに対して、計算します。
シグナリング	VoIP コールのシグナリングです。
パケット数	メディアフローと制御フローを含むコールのパケット数です。
バイト数	ペイロード長さではなくて、あるコールのすべてのパケットのバイト数です。
エラーパケット数	エラーパケットの数です。エラーパケットは SDP データが欠損して、または SDP 情報のフォーマットが正しくない SDP パケットを表します。

VoIP ブラウザ

VoIP 解析のために、Capsa は VoIP ブラウザを提供します。VoIP ブラウザはフル解析と VoIP 解析プロファイルの場合にのみ、利用可能となります。

IP ブラウザのように機能している VoIP ブラウザには VoIP コールに関連している IP アドレスが含まれています。それらの IP アドレスは IP ブラウザのルールに従い並べ替えます。



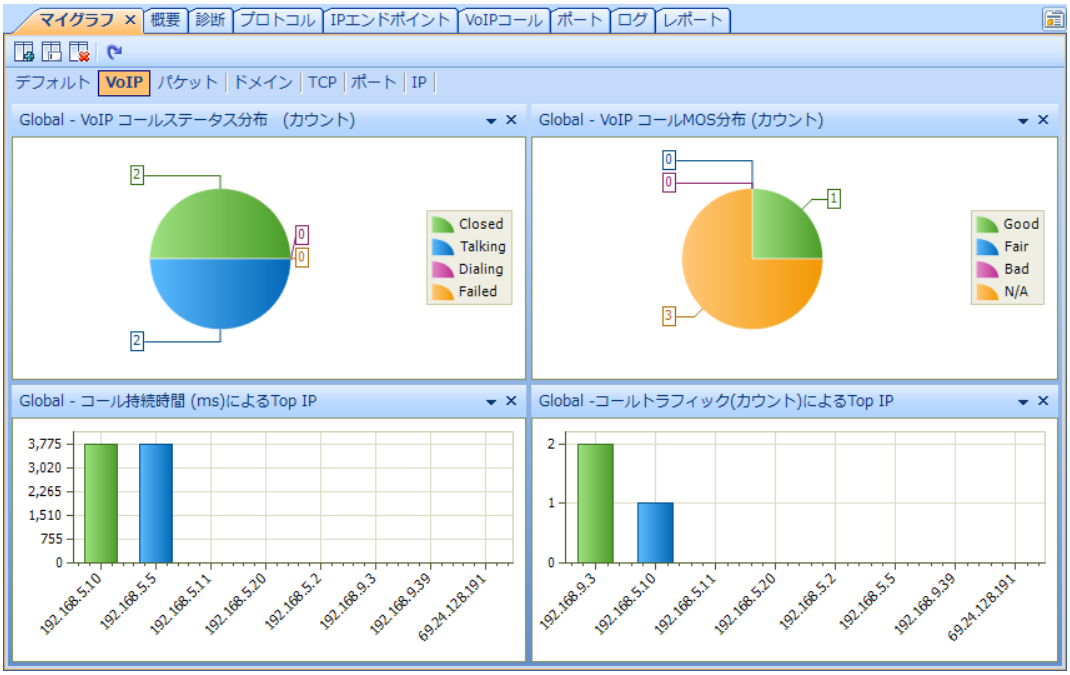
VoIP ブラウザで特定のノードが選択されると、右側のパネルにはそのノードに関する統計ビューだけが表示されます。詳しい情報について、IP ブラウザをご参照ください。

VoIP チャート

Capsa は VoIP コールステータス分布、VoIP コール MOS 分布、コール持続時間による Top IP、およびコール頻度による Top IP を含む、VoIP 解析にために四つのチャートを提供します。

マイグラフビューにおいて、VoIP チャートが表示される VoIP パネルがあります。

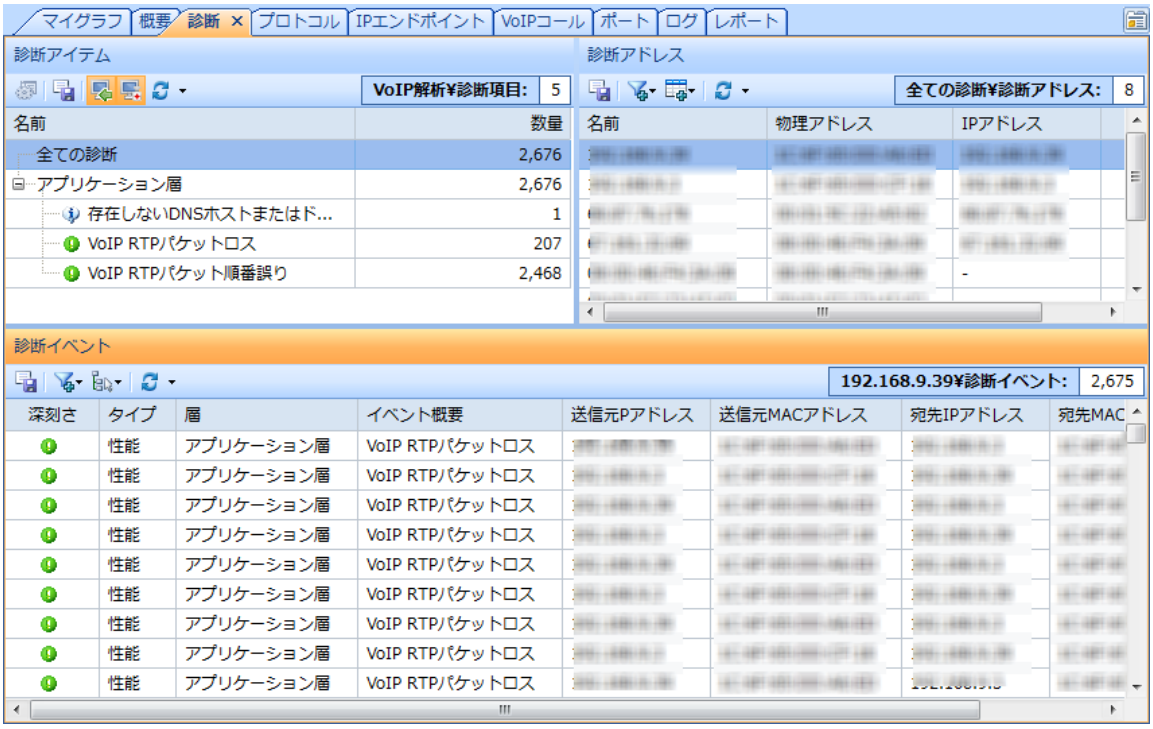
下図のようにデフォルトで VoIP パネルには四つチャートが表示されます。



手動的に他の VoIP チャートを VoIP パネルに追加することもできます。チャートを追加する方法について、チャートを作成をご参照ください。

VoIP 診断

全体ネットワークの診断イベントの他に、Capsa は VoIP 解析のために、VoIP SIP クライアント認証エラー、VoIP RTP パケットロス、VoIP RTP パケット順番誤り、および SDP 情報ケソンまたはフォーマットエラーという四つの診断イベントを提供します。



これらの診断イベントがトリガーされると、診断ビューに表示されます。診断ビューからは、送信元アドレス、宛先アドレス、概要情報、ポート番号を含むイベントの関連情報を取得することができます。詳しいことは診断ビューをご参照ください。

VoIP ログ

ログビューにおいて、VoIP コールログと VoIP シグナリングログという二つの VoIP ログがあります。

VoIP シグナリングログはタイムスタンプ、送信元と宛先アドレス、コール ID、概要情報などを含むすべてのコールとその詳細情報を表示します。詳しいことは VoIP シグナリングログをご参照ください。

VoIP コールログはすべての VoIP コールを表示します。一つの VoIP コールは一つの VoIP コールログとして記録されます。詳しいことは VoIP コールログをご参照ください。

VoIP レポート

VoIP 解析統計を報告するために、レポートビューは VoIP レポートを提供します。

VoIP レポートには VoIP 診断統計、VoIP コールステータス統計、VoIP MOS 分布、および Top アドレスとホストが含まれています。

VoIP レポートの他に、VoIP 統計が含まれる新しいレポートを作成することができます。レポートの作成方法について、レポートを作成をご参照ください。

TCP フロー解析

Capsa を利用して、TCP セッションフローのために単独に転送されたパケットを再構築し、オリジナルセッションコンテンツを表示することができます。一目で確認することで、パケットロス、再送信、またはネットワークにおいて順番誤りがあるかどうかが分かります。Capsa は TCP セッションビューと TCP フロー解析ウィンドウを提供することで、解析結果を表示し、さらなる解析のために役立ちます。

TCP セッションビュー

TCP セッションビューは TCP プロトコルに基づくネットワーク通信トラフィックの統計を表示します。TCP セッションは、1 に設定された TCP SYN フラグ、または 0 以上のロード長さによって識別されます。

注意 **物理ブラウザ**でノードグループまたは MAC アドレス、あるいは**プロトコルブラウザ**で TCP プロトコルに属していないプロトコルノードを選択している場合、**TCP セッション**ビューは利用できません。

カラムヘッダーにおける統計フィールドをクリックして、そのフィールドに基づいて統計情報を並べ替えることもできます。例えば、カラムヘッダーにおける「持続時間」をクリックして、通信持続時間に基づいて、Top 通信を確認することができます。カラムヘッダーにおける「バイト」をクリックして、転送されたトラフィックに基づいて、Top 通信を確認することができます。

TCP セッションの詳細情報を確認したい場合、そのセッションをダブルクリックして、TCP フロー解析ウィンドウを開くことで、TCP トランザクションプロセスと時間が表示されます。詳しいことは、TCP フロー解析ウィンドウをご参照ください。TCP セッションビュー下位パネルを通じてトランザクションプロセスを確認することもできます。

TCP セッションビュー下位パネルはパケット、データフロー、シーケンスチャートという三つのタブから構成されています。

- パケットタブは選択された TCP セッションに関係するパケットだけをリストします。そのタブにおける**デコードビューを表示**ボタンをクリックして、パケットのデコード情報を表示、または非表示することができます。詳しいことはパケットをデコードをご参照ください。
- データフロータブは TCP セッションのオリジナルフロー情報を表示します。詳しいことはデータフロータブをご参照ください。

- シーケンスチャートタブはセッションプロセスを図表で表示します。詳しいことは、シーケンスチャートタブをご参照ください。

下位パネルが隠されている場合、  をクリックして、それを表示することができます。

データフロータブ

このタブには、TCP セッションビューで選択されたセッションのオリジナル情報が表示されます。ネットワークで実現された TCP セッションは、複数のパケットに切られ、切られたパケットは順番誤りでネットワークで転送されています。Capsa は正しい順番でこれらのパケットを整理し、TCP フローに再構築します。ウェブ（HTTP）、E メール（SMTP/POP3）、FTP および MSN などを含む TCP プロトコルを利用しているセッションは再構築されることができます。**データフロー**タブは以下のように表示されます。

注意 転送中暗号化されているデータがあるので、文字化けが表示されることもあります。

デフォルトでは、**データフロー**タブは二つのノード間のすべてのデータフローを表示します。色によって、異なるノードのデータを区別することができます。青はノード 1 からノード 2 までのデータを、緑はノード 2 からノード 1 までのデータを表します。

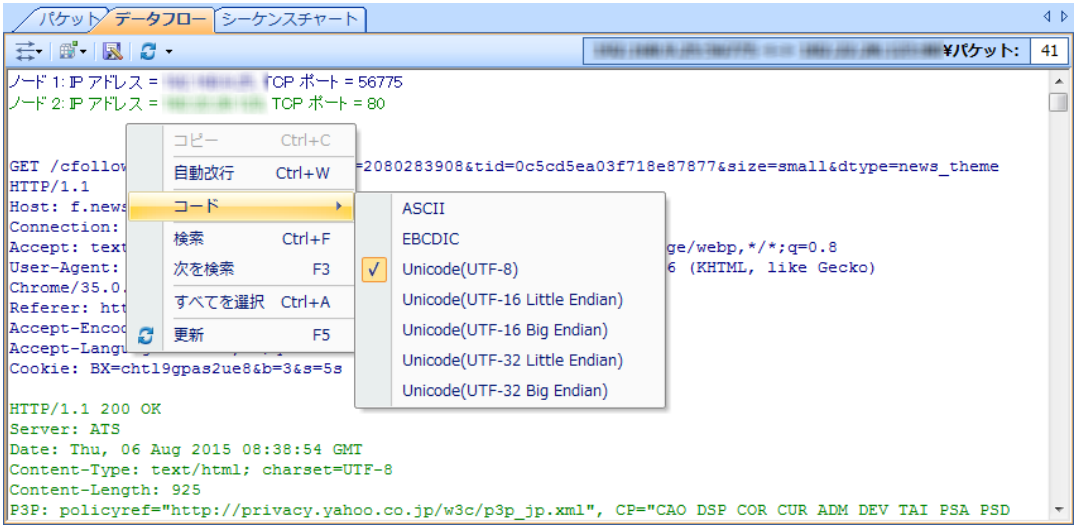
 をクリックすることで、ノード 1 からノード 2 までのデータ、またはノード 2 からノード 1 までのデータだけを表示することができます。

TCP セッションにはパケットがたくさんある場合、  をクリックして、前の 50、または 100 個パケットのデータだけを表示することができます。

 をクリックして、16 進数でデータを表示することができます。

データフローに興味を持っている場合、  をクリックして、選択されたセッションのデータフローを保存することができます。

他のフォーマットでデータフローを表示したい場合、データフロータブで右クリックして、**コード**にマウスを移動し、表示したいフォーマットを選択すればよいのです。



シーケンスチャートタブ

シーケンスチャートタブは TCP セッションビューで選択されたセッションのためにタイムシーケンスチャートを提供します。そのチャートを確認することで、TCP セッションにおけるパケットの転送メカリズムを把握することができます。グレーはノード 1 からノード 2 までのパケットを、黄色はノード 2 からノード 1 までのパケットを表します。

 をクリックして、TCP セッションにおけるシーケンス番号の絶対値、または相対値を表示することができます。

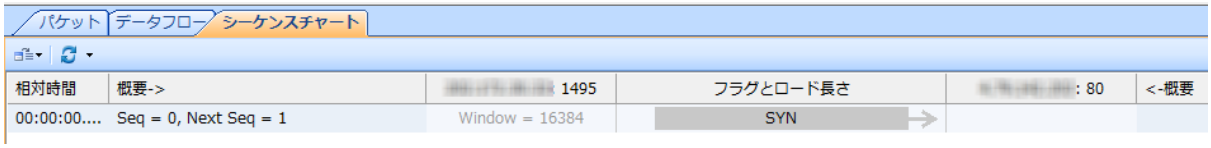
タイムシーケンスチャートは以下で説明されている六つのカラムから構成されています。

- **相対時間**:選択されたパケットからセッションにおける最初のパケットまでのタイムスタンプの時間です。すなわちセッションにおける最初のパケットを参照オブジェクトとしています。
- **概要->**:ノード 1 に送信されたパケットのシーケンス番号、ACK 番号、次のシーケンス番号に関する情報を表示します。

- **ノード 1->**: ノード 1 のウィンドウサイズ情報を表示します。ウィンドウサイズが 0 の場合、ノード 2 が送信を停止する必要があることを示しています。
- **フラグとロード長さ**: フラグは TCP セグメントヘッダーにおける制御フラグで、ロード長さは TCP セグメントのデータ部分のサイズです。
- **<- ノード 2**: ノード 2 のウィンドウサイズ情報を表示します。ウィンドウサイズが 0 の場合、ノード 1 が送信を停止する必要があることを示しています。
- **<-概要**: ノード 2 に送信されたパケットのシーケンス番号、ACK 番号、次のシーケンス番号に関する情報を表示します。

タイムシーケンスチャートは全体の TCP フロープロセスを理解するのに非常に有用であり、ネットワーク問題の特定にも役立ちます。例えば、以下は TCP セッションビューのスクリーンショットです。

一目だけで、何か異常なことが起きているのが分かります。正常のネットワークはこのようなトラフィックを持つ可能性がありません。したがって、  をクリックして、下位パネルを表示し、シーケンスチャートタブに移動します。

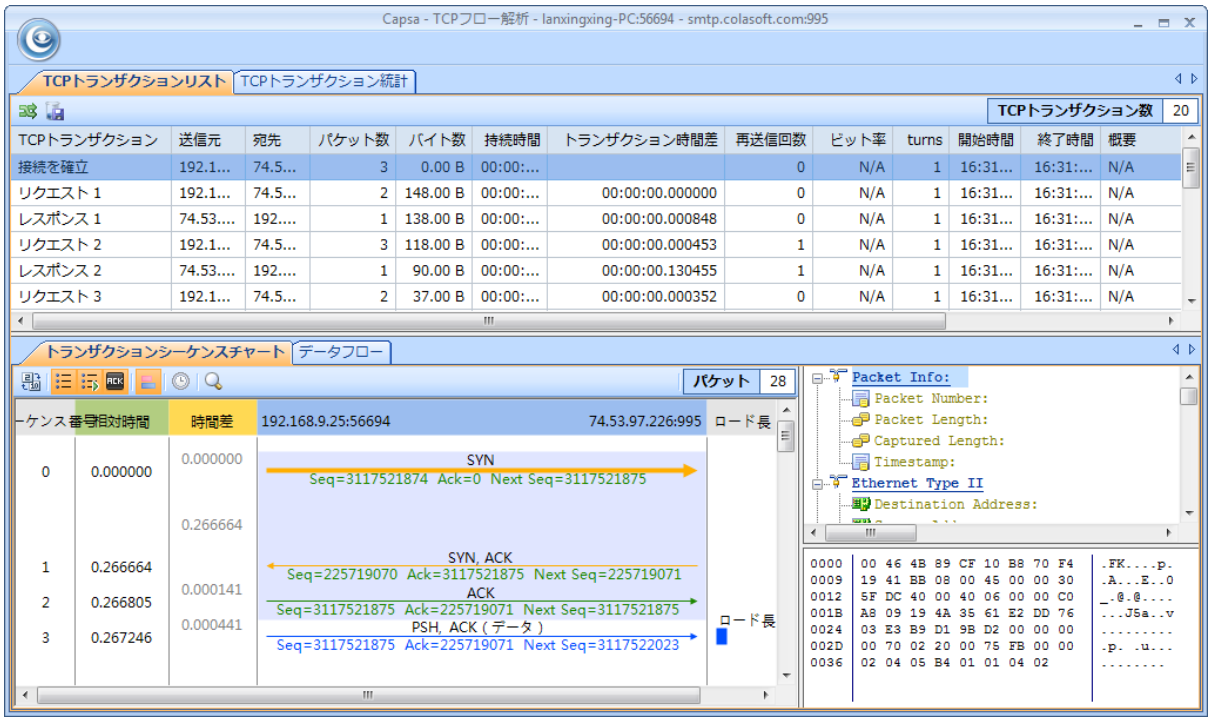


各 TCP セッションのシーケンスチャートタブを確認した後、すべて同じであることが分かりました。他の証拠に加え、最後にネットワークで DoS 攻撃が発生していることが分かりました。

TCP フロー解析ウィンドウ

TCP フロー解析ウィンドウを開くには、**TCP セッション**ビューにおけるセッションリストで任意アイテムをダブルクリックしたり、または任意アイテムを右クリックしたりして、**新しいウィンドウでパケット/TCP フロー情報を表示する**を選択たりします。

TCP フロー解析ウィンドウは以下のように表示されます。



TCP フロー解析ウィンドウは以下の二つのビューから構成され、**TCP セッション**ビューで選択されたセッションの詳細なトランザクション情報、パケット情報、およびデータフロー情報を提供します。

- TCP トランザクションリストビュー
- TCP トランザクション統計ビュー
- パケットビュー
- データフロービュー

TCP トランザクションリストビュー

TCP トランザクションリストビューは、解析された TCP セッションのトランザクションリスト情報を提供する上側パネルと、**トランザクションシーケンスチャート**タブと**データフロー**タブから構成されている下側パネルからなっています。

トランザクションリスト

以下は上側パネルのツールバーにおけるアイテムについて説明しています。

 : トランザクションのリクエストレスポンスを反転します。

 : トランザクションリストで選択されたトランザクションのパケットを保存します。ファイルの種類におけるドロップダウンリストから保存したいフォーマットを選択し、パケットを保存することができます。

トランザクションリストにおけるカラムヘッダーを右クリックして、表示、または非表示するカラムを指定することができます。以下はトランザクションリストにおける各カラムについて説明しています。

- **TCP トランザクション**:**接続を確立**、**リクエスト**数、**レスポンス**数、および**接続を閉じる**、を含むトランザクションの名前をリストします。
- **送信元**: IP アドレスとポート番号を含むトランザクションの送信元情報です。
- **宛先**: IP アドレスとポート番号を含むトランザクションの宛先情報です。
- **パケット数**:トランザクションのパケット数です。
- **バイト数**:ロード長さの合計バイト数で、TCP セグメントのデータ部分のサイズです。
- **持続時間**:トランザクションの持続時間です。
- **トランザクション時間差**:隣接する二つのトランザクションの時間差です。
- **再送信数**:トランザクションの再送信回数です。
- **ビット率**:トランザクションのビット率です。パケット数が 10 以上の場合にのみ利用可能となります。
- **Turns**: TCP turn の数です。TCP turn は対になっている ACK パケットとデータ部分があるパケットの数を表します。トランザクションの終わりにデータ部分のパケットがある場合、1 を足す必要があります。対になって隣接する ACK パケットが一ペアだけある場合、TCP turn は 1 になります。一つのトランザクションには、少なくとも一つの TCP turn があります。
- **開始時間**:トランザクションの開始時間です。
- **終了時間**:トランザクションの終了時間です。
- **概要**:トランザクションの概要情報です。

特定のトランザクションが選択された場合、**トランザクションシーケンスチャート**タブは自動的にシーケンスチャートでそのトランザクションの情報を表示します。

トランザクションシーケンスチャート

トランザクションリストであるトランザクションが選択された場合、トランザクションシーケンスチャートは灰色の背景色でそのトランザクションのパケット情報を表示します。

シーケンスチャートでは矢印付きのラインでパケットの方向を表します。緑のラインは接続を確立するパケットを、青のラインはアプリケーションデータのパケットを、黄色のラインは ACK パケットを、赤のラインは再送信、ACK を重複するなど異常が発生しているパケットを表します。

矢印付きのラインをクリックして、そのラインは厚い黄色のラインになります。同時に右側ではそのパケットのデコード情報が表示されます。

以下のリストは、このタブのツールバーにおけるボタンについて説明しています。

 : 0 からパケットの相対的な番号、またはプロジェクトバッファにおける実際のパケット番号を表示します。

 :パケットのシーケンス番号を表示します。

:パケットの次のシーケンス番号を表示します。

:パケットの ACK 番号を表示します。

:パケットのロード長さ情報を表示します。

:パケットの相対時間を設定します。

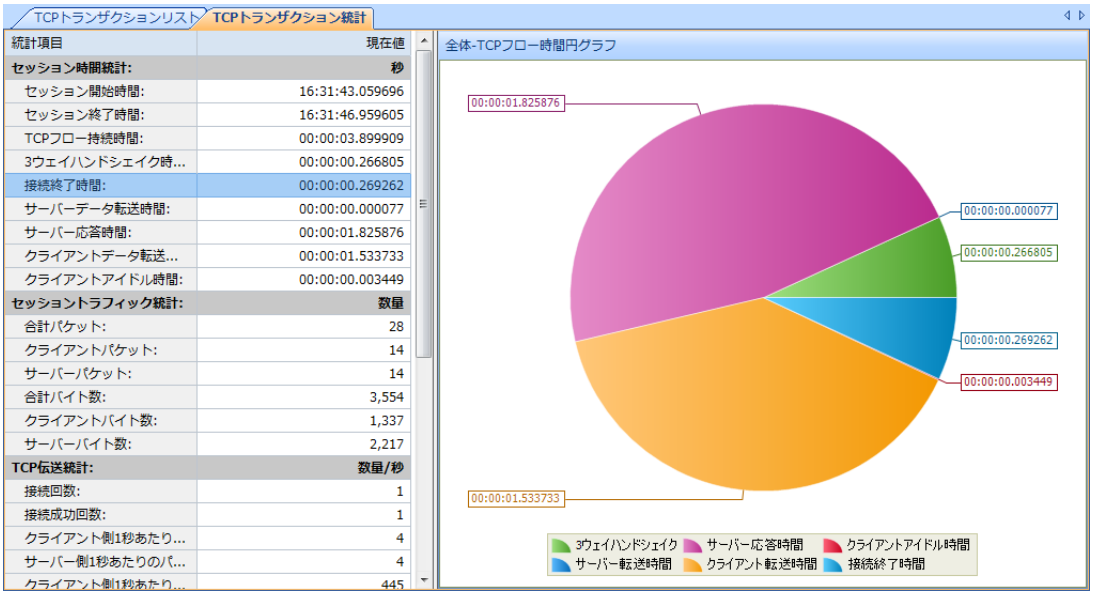
:**パケット内で検索**ダイアログボックスを開き、右側におけるパケットデコード部分で検索します。一致するものが見つかったら、パケットの矢印付きラインはハイライト表示されます。

データフロータブ

このタブは、トランザクションリストで選択されたトランザクションのオリジナル情報を表示します。詳しいことは[データフロータブ]をご参照ください。

TCP トランザクション統計ビュー

TCP トランザクション統計ビューは左側パネルで TCP トランザクションの統計と、右側パネルで円グラフで TCP フローの時間情報を表示します。TCP トランザクション統計ビューは以下のように表示されます。



左パネルで提供している統計アイテムは以下の通りです。

- セッション時間統計: セッション開始時間、セッション終了時間、TCP フロー持続時間、3 ウェイハンドシェイク時間、接続終了時間、サーバーデータ転送時間、サーバー応答時間、クライアントデータ転送時間、クライアントアイドル時間からなっています。
- セッショントラフィック統計:合計パケット、クライアントパケット、サーバーパケット、合計バイト数、クライアントバイト数、サーバーバイト数からなっています。
- TCP 転送統計:接続回数、接続成功回数、クライアント側 1 秒当たりのパケット数、サーバー側 1 秒当たりのパケット数、クライアント側 1 秒当たりのバイト数、サー

バー側 1 秒当たりのバイト数、クライアント側再送信回数、サーバー側再送信回数、クライアントロスセグメント回数、サーバーロスセグメント回数、最大 Ack 時間、最小 Ack 時間、クライアント平均 Ack 時間、サーバー平均 Ack 時間からなっています。

- セッショントランザクション統計:トランザクション総回数、トランザクション処理時間、平均トランザクション処理時間、最大トランザクション処理時間からなっています。

右側パネルは 3 ウェイハンドシェイク、サーバー応答時間、クライアントアイドル時間、サーバー転送時間、クライアント転送時間、および接続終了時間という六つのアイテムが含まれる全体 TCP フロー統計の円グラフを提供し、TCP セッションビューで選択されたセッションの TCP フロー時間情報を表示します。

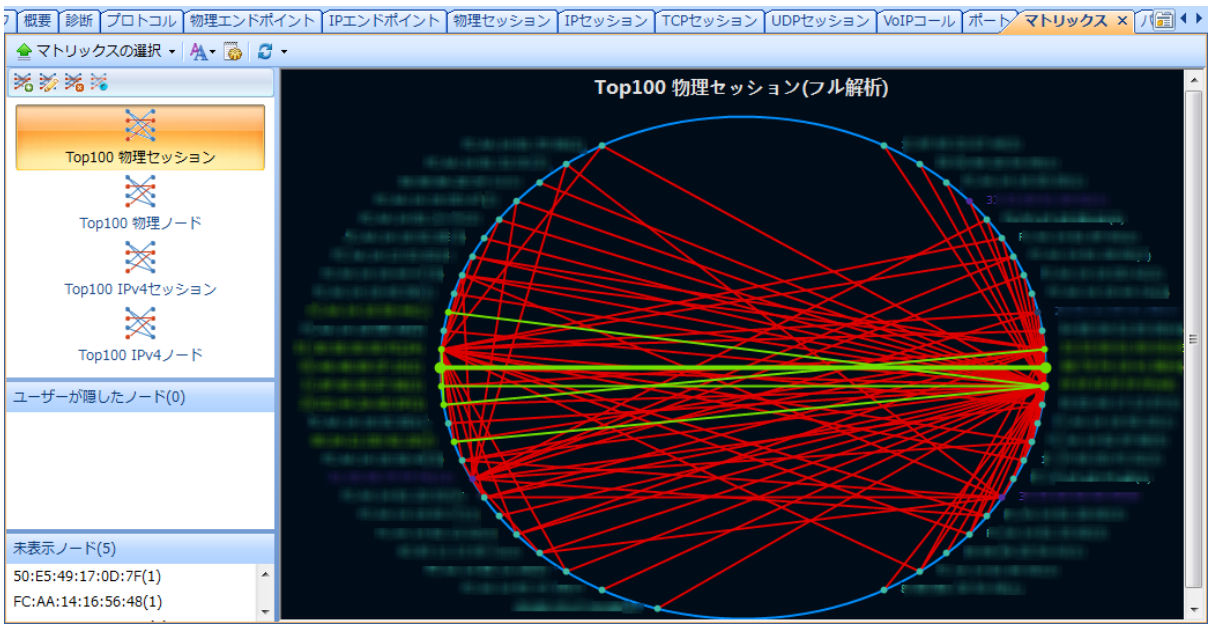
マトリックス

マトリックスは**マトリックス**ビューによって提供され、ピアノードとピアノードを結ぶラインでネットワークトラフィックを表示します。ノードはネットアークノードを、ラインはノード間のネットワーク通信を表します。

- マトリックスビュー
- マトリックスを作成
- マトリックスをカスタマイズ

マトリックスビュー

マトリックスビューは左側パネルとピアノードとピアノードを結ぶライでなっている楕円のマトリックスから構成されています。ノードは MAC/IP アドレスで、ラインはアドレス間の通信を表します。ノードの後ろの番号はピアホストの数です。



マトリックスビューの右上にある**マトリックスの選択**をクリックして、左側パネルを表示、または非表示することができます。後の小さな三角形をクリックすることで、このビューで表示するマトリックスのタイプを選択することができます。

更新ボタン  をクリックして、マトリックスビューを更新したり、更新間隔を設定したりすることができます。

左側パネルの一番上に四つのデフォルトマトリックスタイプをリストしています。この四つのマトリックスタイプに対して変更を行ったり、新しいマトリックスを追加したりすることができます。詳しいことは、マトリックスを作成をご参照ください。

マトリックスにおける色とフォントサイズはユーザーによって定義されることができます。詳しいことは、マトリックスをカスタマイズをご参照ください。

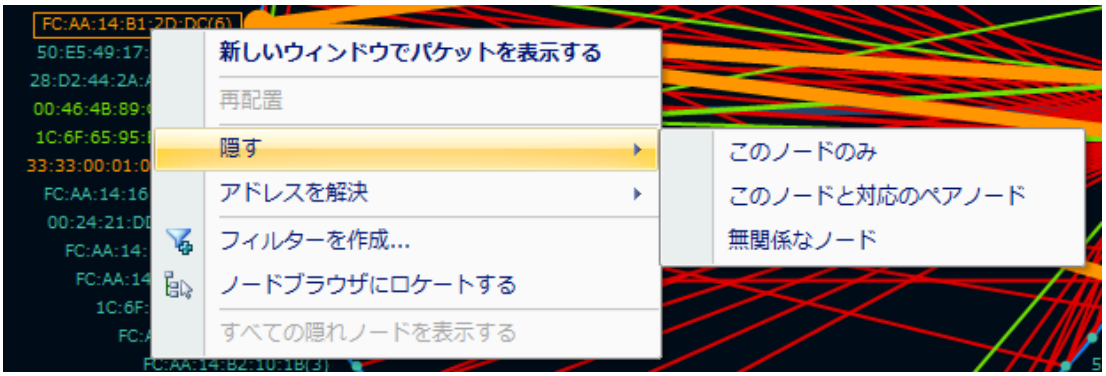
マウスをノードに移動すると、そのノードに接続しているノードとラインは黄色になりハイライト表示されます。そのノートに関するトラフィック統計情報も表示されます。マウスをラインに移動すると、ラインとそのラインに接続された二つのノードは黄色になりハイライト表示されます。そのペアノード間の通信トラフィック統計情報も表示されます。

マトリックスを確認している時、ノードまたはラインをダブルクリックして、パケットウィンドウが表示されます。パケットウィンドウで、そのノードまたはラインに接続されたノードに関するパケットをリスト、デコードします。

ユーザーが隠したノード

マトリックスにはノードがたくさんある場合、トラフィックの状況をはっきり表示するために、ノードを他の位置にドラッグしたり、不必要なノードを隠したりすることができます。

ノードを隠すには、下図のように、ノードを右クリックして、隠したいノードを選択すればよいのです。



- **このノードのみ**:選択されたノードだけを隠します。
- **このノードと対応のペアノード**:選択されたノードとその対応のペアノードだけを隠します。
- **未関係なノード**:選択されたノードとその対応のペアノードだけを表示します。

ノードが隠されると、**ユーザーが隠したノード**という部分に表示されます。**ユーザーが隠したノード**の後のつく括弧にある数字は隠されたノードの数を表します。

ユーザーが隠したノードを表示するには、この部分を右クリックして、選択したノードを表示したり、すべてのノードを表示したりすることができます。またはマトリックスで右クリックして、**すべての隠れノードを表示する**を選択することで、ユーザーが隠したすべてのノードを表示することができます。

未表示ノード

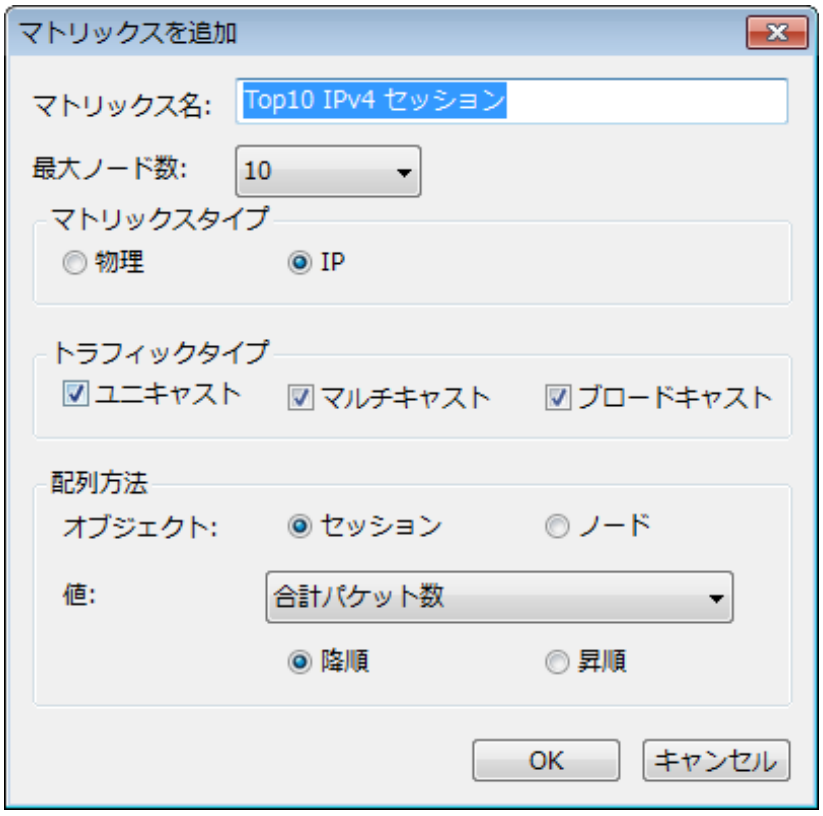
この部分は、マトリックスの設定に一致しないため、マトリックスで一時的に隠されているノードをリストします。**未表示ノード**の後につく括弧の中の数字は未表示ノードの数を表します。

例えば、マトリックスタイプが Top100 IP ノードの場合、マトリックスは Top100IP アドレスだけを表示します。マトリックスタイプが Top 100IP セッションの場合、マトリックスは Top 100IP セッションだけを表示します。残りのノードは全部**未表示ノード**にリストします。

マトリックスを作成

デフォルトでは、Capsa は Top 100 物理セッション、Top 100 物理ノード、Top 100 IPv4 セッション、および Top 100 IPv4 ノードという四つのマトリックスを提供します。

新しいマトリックスを追加するには、  をクリックして、**マトリックスを追加**ダイアログボックスが開かれます。そのダイアログボックスを完了します。



マトリックスを追加するダイアログボックスにおける各アイテムは以下のように説明しています。

- マトリックス名:マトリックスの名前です。
- 最大ノード数:ノードの最大数を選択します。
- マトリックスタイプ:**物理**は MAC アドレスに基づく統計を表し、**IP** は IP アドレスに基づく統計を表します。

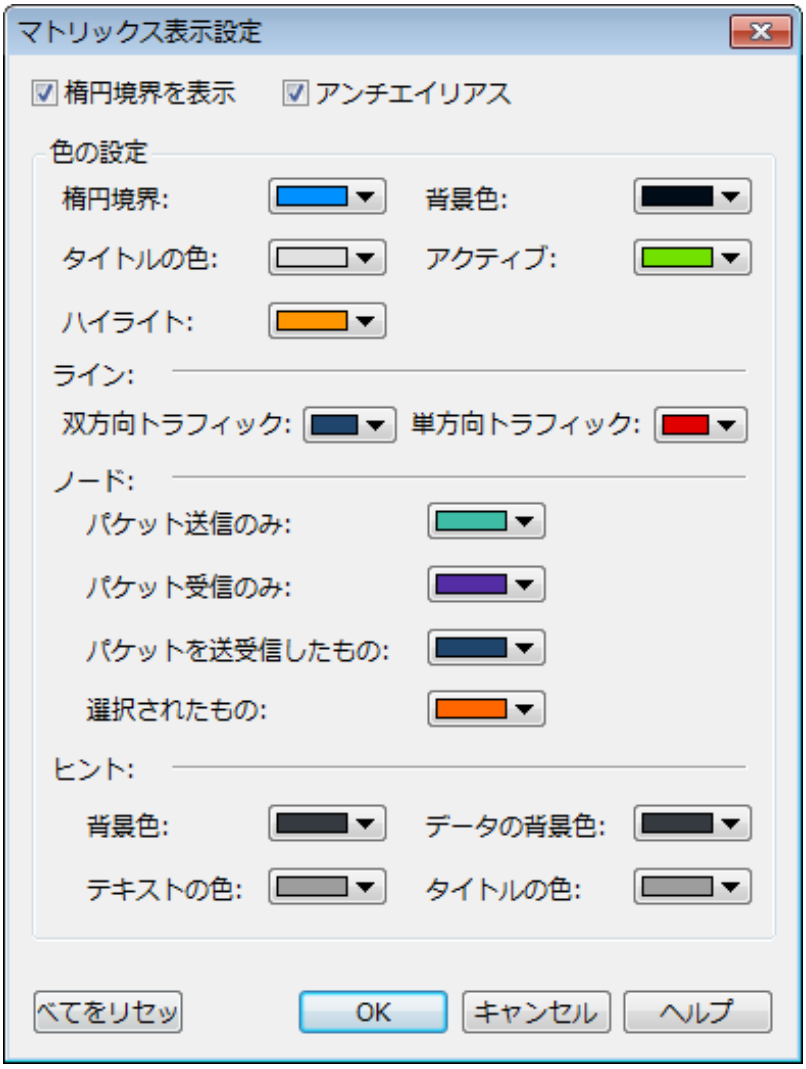
- トラフィックタイプ:統計のトラフィックタイプを選択します。
- オブジェクト:マトリックスの統計オブジェクトを指定します。
- 値:統計オブジェクトの値のタイプを選択します。
- 降順:マトリックスは一番大きいものから統計を表示します。
- 昇順:マトリックスは一番小さいものから統計を表示します。

既存のマトリックスに対して、  をクリックして、変更を行うことができます。

マトリックスをカスタマイズ

デフォルトでは、カラースキームのセットを提供します。ユーザーは自分で新しいカラースキームを定義することもできます。

カラースキームを変更するには、  をクリックして、**マトリックス表示設定**ダイアログボックスが表示されます。



- **楕円境界を表示**:楕円の境界線を表示します。
- **アンチエイリアス**:楕円、ライン、およびノードを滑らかにします。

- **色の設定**:楕円境界線、背景、マトリックスタイトル、アクティブなノードとライン、およびハイライトされたノードとラインの色を指定します。
- **ライン**:双方向トラフィックと単方向トラフィックを表示する色を指定します。
- **ノード**:パケット送信のみのノード、パケット受信のみのノード、パケットを送受信したノード、選択されたノードを表示する色を指定します。
- **ヒント**:ノードまたはラインがハイライトされた場合、ヘントを表示する色を指定します。

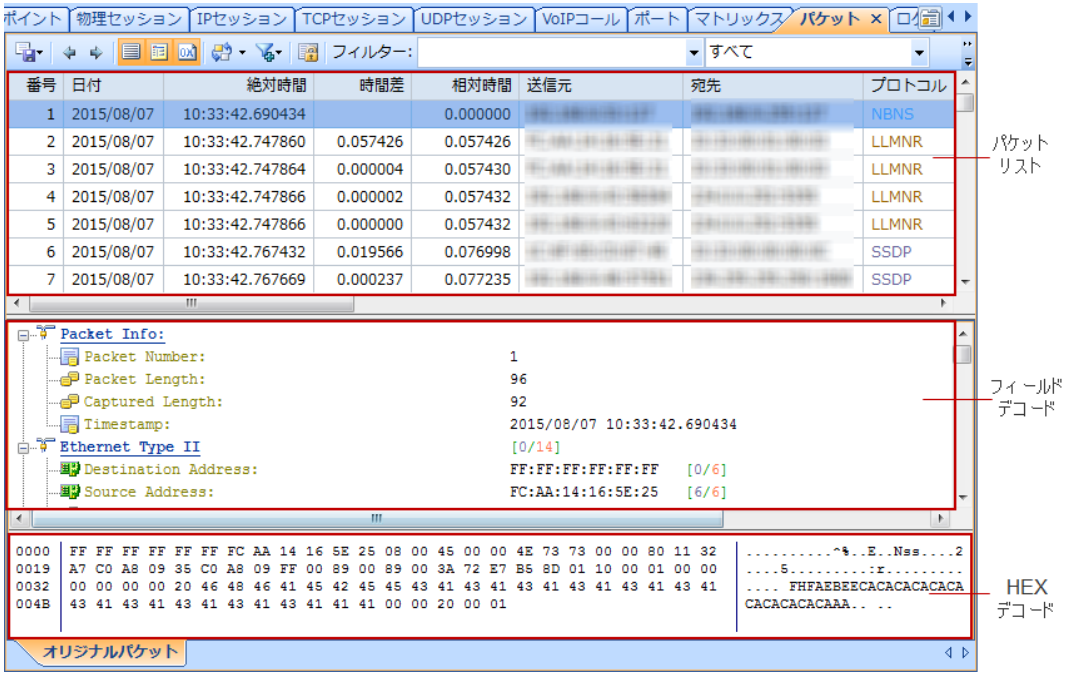
マトリックスビューにおけるフォントサイズを変更することもできます。  をクリックして、適切なものを選択すればよいのです。

パケットを表示

Colasoft Capsa はキャプチャーされたパケットを一つ一つデコードすることができます。すべてのパケットは**パケット**ビューに表示されます。

パケットビュー

パケットビューはキャプチャーされたすべてのパケットをリストし、パケットのデコード情報も提供します。このビューは、上から下まで三つのパネルから構成されています。



- パケットリストパネル:キャプチャーされたパケットをリストします。リストにおけるすべてのパケットは一時的にパケットバッファに保存されます。パケットバッファはキャプチャーされたすべてのパケットを保存する十分なスペースを持っていない場合、一部のパケットのパケットバッファの設定によって廃棄されます。
- フィールドデコードパネル:パケット転送のプロトコルに基づいて、デコード情報を表示します。
- HEX デコードパネル:パケットリストパネルで選択されたパケットの 16 進数デコード情報を表示します。

をクリックして、パケットリストパネルを表示、または非表示することができます。

をクリックしてフィールドデコードパネルを、をクリックして HEX デコードパネルを表示、または非表示することができます。

 をクリックして、パケットビューのレイアウトを変更することができます。

パケットビューにおけるカラムヘッダーを右クリックして、リストで表示、または非表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。各カラムの詳しいことはパケットビューにおけるカラムについてをご参照ください。

パケットビューにおける表示フィルターについては、上級な表示フィルターをご参照ください。

パケットデコードの詳しいことはパケットをデコードをご参照ください。

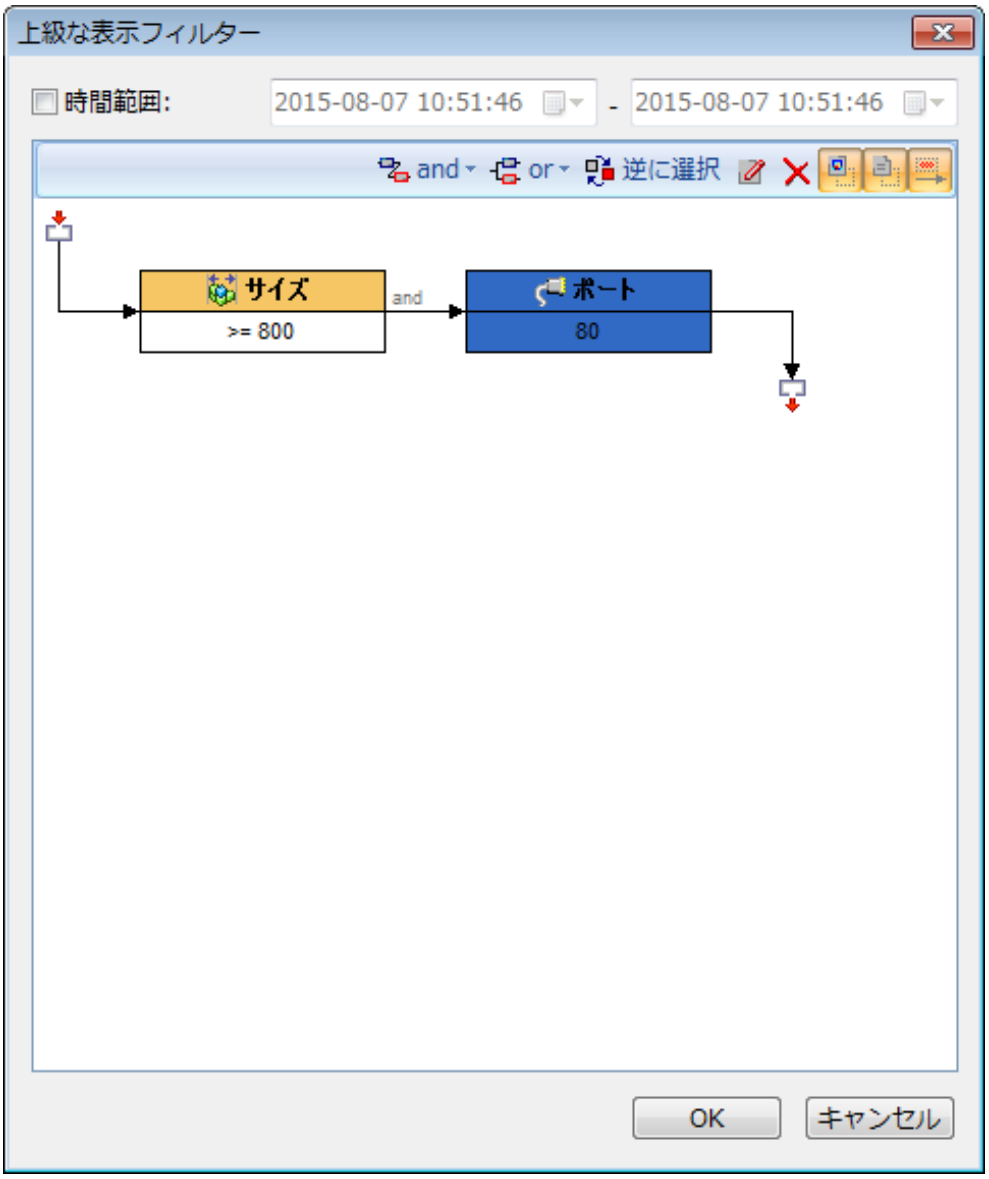
上級な表示フィルター

Capsa は上級な表示フィルターを提供し、パケットビューで表示するパケットをフィルタリングすることができます。上級な表示フィルターは、パケットビューのツールバーにおける一般的な表示フィルターの横にあります。

一般的な表示フィルターは、統計ビューにおけるカラムのフィールドに基づいて、レコードを表示フィルタリングするためのもので、リストにおけるレコードを表示キーワードと一致させます。複数のビューに提供されています。詳しいことは、表示フィルターをご参照ください。

上級な表示フィルターは、パケットを表示フィルタリングするためのもので、フィルタールールをパケットコンテンツと一致させます。パケットビューでのみ、利用可能となります。

上級な表示フィルターを適用するには、上級な表示フィルターアイコンをクリックして、上級な表示フィルターダイアログボックスを開きます。



時間範囲にフィルタールールと一致させるパケットの時間範囲を指定します。

ルールを追加するには、**and** または **or** をクリックして、ルールを定義すればよいのです。

ルール部分は上級キャプチャーフィルターとまったく同じです（詳しいことは、上級フィルターを作成をご参照ください。）

上級な表示フィルターを削除するには、上級な表示フィルターアイコンの後にある削除ボタンをクリックします。

パケットビューにおけるカラムについて

以下の表は**パケット**ビューにおけるカラムについて説明しています。

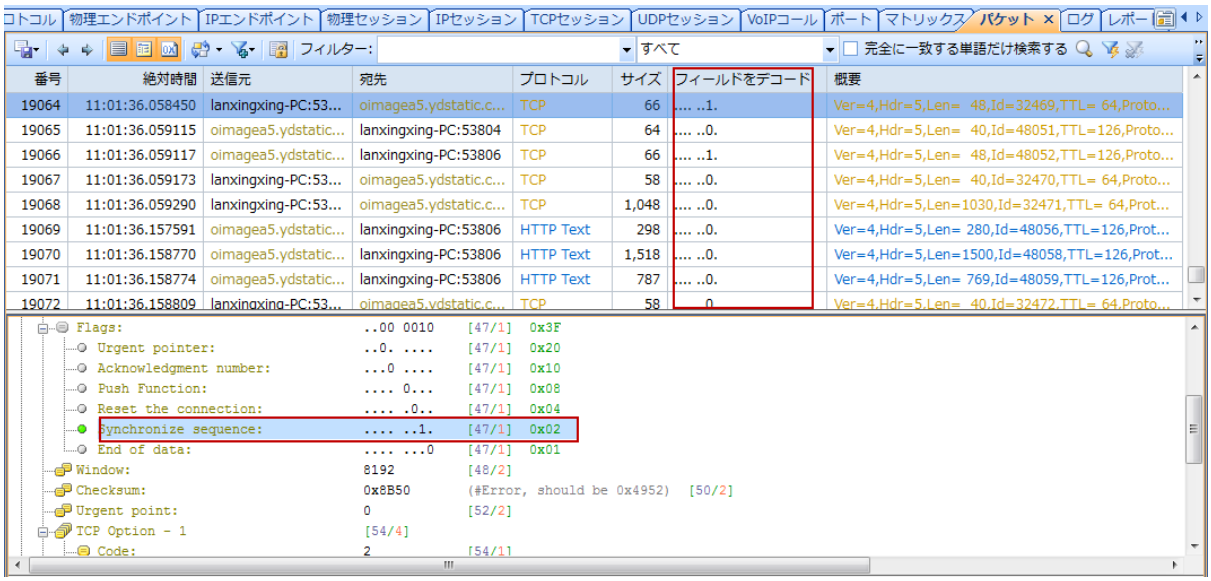
カラム	説明
番号	パケットの番号です。
日付	パケットがキャプチャーされたとき、オペレーティングシステムの日付です。
絶対時間	パケットがキャプチャーされたとき、オペレーティングシステムの時間です。
時間差	選択されたパケットと前のパケットの時間差です。
相対時間	パケットがキャプチャーされたときの相対時間です。相対時間を設定するには、パケットリストであるアイテムを右クリックして、**相対時間の設定**をクリックすることで、選択されたアイテムの時間を基準時点にして、相対時間を計算します。
備考	選択されたパケットに関する備考です。パケットの備考を作成するには、パケットリストにおけるあるアイテムを右クリックして、**備考->備考を編集**を選択します。
送信元	パケットの送信元情報です。
宛先	パケットの宛先情報です。
プロトコル	パケットの最上位層プロトコルの名前です。
サイズ	パケットのサイズです。
送信元 MAC アドレス	パケットの送信元 MAC アドレスです。
宛先 MAC アドレス	パケットの宛先 MAC アドレスです。
送信元 IP	パケットの送信元 IP アドレスです。
宛先 IP	パケットの宛先 IP アドレスです。
送信元ポート	パケットの送信元ポート番号です。
宛先ポート	パケットの宛先ポート番号です。
フィールドをデコード	フィールドデコードパネルで選択されたフィールドのデコード情報です。
概要	パケットの概要情報です。
プロセス	パケットの属しているプロセスを表示します。

パケットをデコード

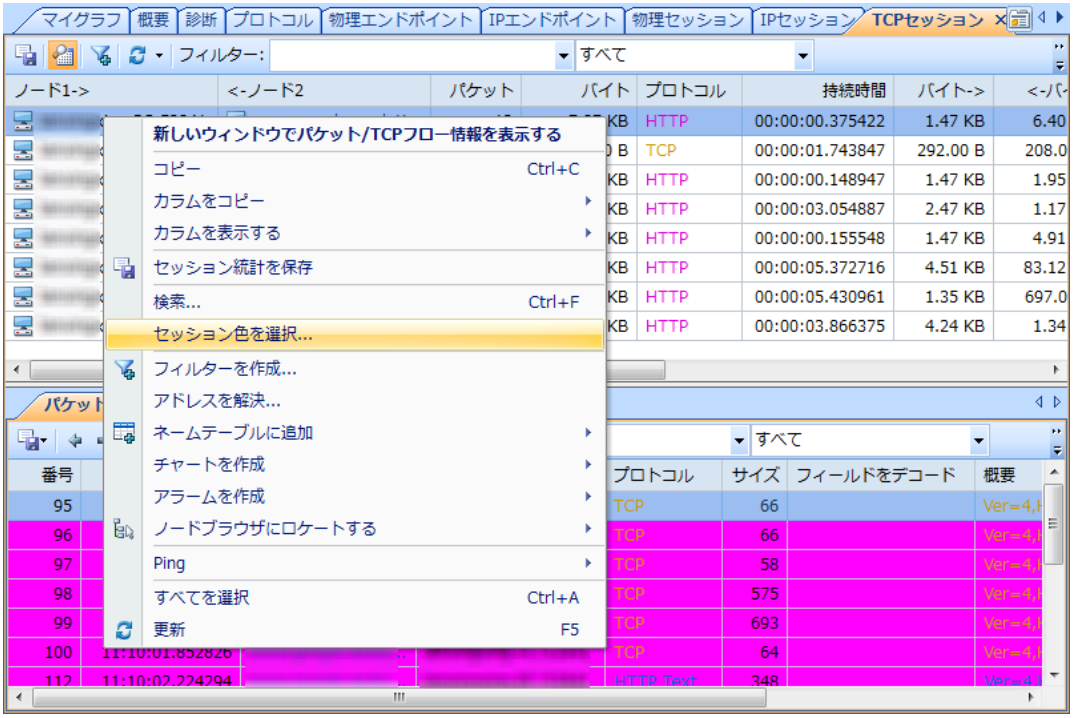
パケットビューを利用して、デコード情報を確認するのは簡単かつ便利です。パケットリストパネルでパケットを選択して、フィールドデコードパネルは、プロトコル層に基づいて、パケットのデコード情報を表示します。

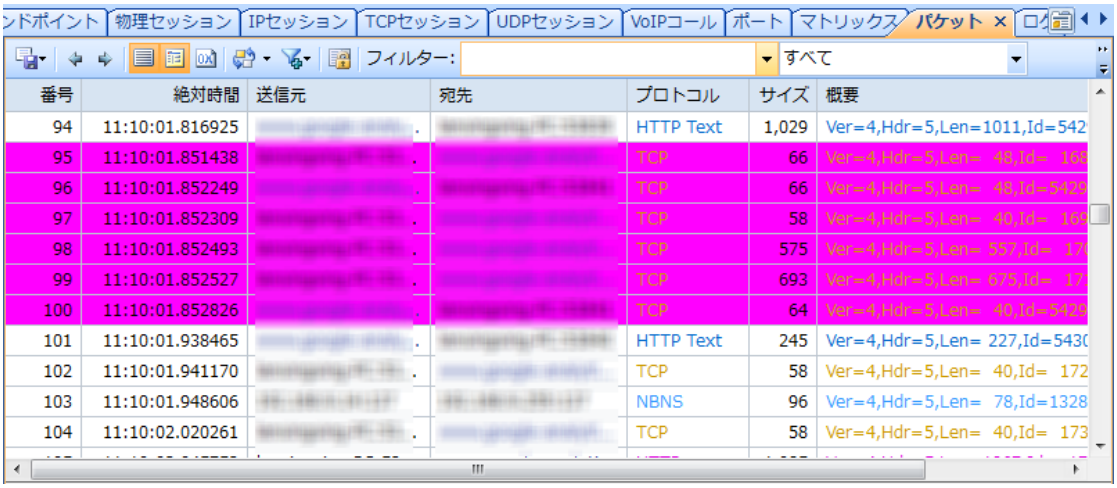
フィールドデコードパネルであるフィールドを選択すると、HEX デコードパネルは、選択されたフィールドの対応 16 進数データを表示します。パケットリストパネルにおけるカラム**フィールドをデコード**もすべてのパケットに対して、そのフィールドのデコード内容を表

示します。例えば、あるパケットの TCP プロトコルの SYN フラッグを選択した場合、カラム**フィールドをデコード**は、すべてのパケットの SYN フラッグをリストします。



TCP セッションビューはセッションの色付け機能を提供します。TCP セッションビューであるセッションを選択し、右クリックして、ポップアップメニューで**セッション色を選択**をクリックすることで、**色を選択**ダイアログボックスが開かれます。このダイアログボックスでセッションの色を設定することができます。セッション色が設定されると、このセッションに関するパケットもこの色で表示されます。





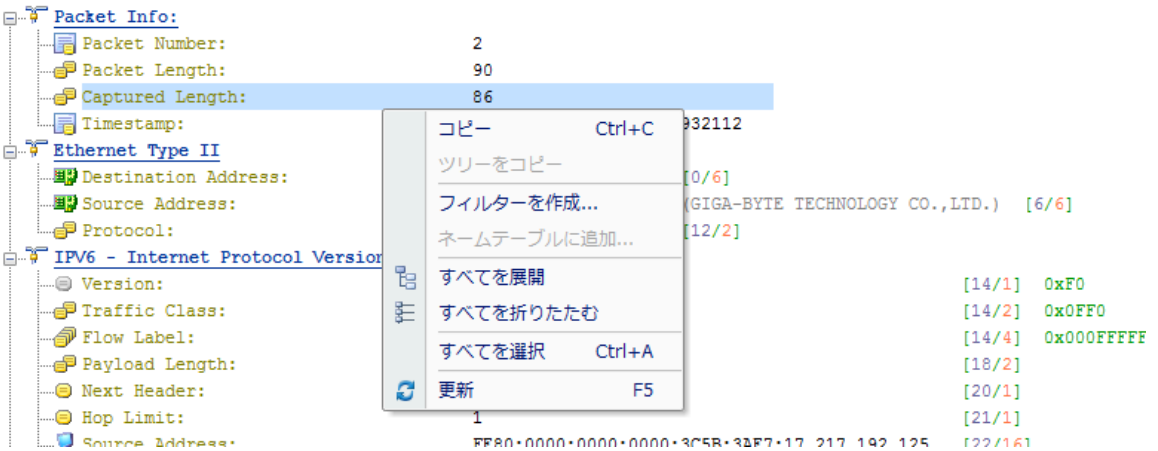
セッションのパケットの色を設定するほかに、あるパケットに興味を持っている場合、そのパケットをハイライト表示することもできます。パケットをハイライト表示するには、パケットリストパネルで、あるパケットを右クリックして、**ハイライト**をクリックすればよいのです。

以下のリストは、ポップアップメニューにおける各アイテムについて説明しています。

- **新しいウィンドウでパケットをデコード**:新しいウィンドウを開き、パケットのデコード情報を表示します。同時に、パケットをダブルクリックすることもできます。
- **コピー**:オリジナルの形式で選択されたものをクリップボードにコピーします。
- **カラムをコピー**:オリジナルのケー式で選択されたカラムをクリップボードにコピーします。
- **カラムを表示する**:カラムを表示、非表示したり、カラムの表示順序を変更したりします。
- **パケット概要**:パケット概要を表示します。
  - **自動**:最上位プロトコル概要を表示します。
  - **IP 概要**: IP プロトコルのパケット概要を表示します。IP プロトコルがない場合、最上位プロトコル概要を表示します。
  - **TCP/UDP 概要**: TCP/UDP プロトコルのパケット概要を表示します。TCP/UDP プロトコルがない場合、最上位プロトコル概要を表示します。
- **パケットをエクスポート**:選択したパケット、またはパケットリストンにおけるすべてのパケットをエクスポートします。**ファイルの種類**ドロップダウンリストにおける任意フォーマットでパケットを保存することができます。
- **検索**:リストでアイテムを検索します。
- **相対時間の設定**:選択されたアイテムの時間を基準時点として、相対時間を計算します。
- **フィルターを作成**:選択されたアイテムに基づいて、フィルターを作成します。

- **アドレスを解決**:選択されたアイテムのホスト名を解決します。解決された名前で、簡単にネットワークにおけるマシンを特定することができます。
- **ネームテーブルに追加**:選択されたノード別名をネームテーブルに追加します。
- **チャートを作成**:選択されたアイテムに基づいて、マイグラフビューでチャートを作成します。
- **アラームを作成**:選択されたアイテムに基づいて、アラームブラウザウィンドウでアラームを作成し、ネットワークの異常を警告します。
- **ノードブラウザにロケートする**:選択されたノードをノードブラウザウィンドウにロケートします。
- **セッションビューにロケートする**:選択されたノードをセッションビューにロケートします。
- **Ping**:ビルトイン Ping Tool を呼び出して、選択したエンドポイントを Ping します。
- **Packet Builder にパケットを送信**:選択したパケットをビルトインツール Packet Builder に送信します。
- **関連パケットを選択する**:送信元、宛先、送信元と宛先、セッション、またはプロトコルに基づいて、関連パケットを選択します。
- **選択したパケットを隠す**:選択したパケットを隠します。
- **未選択のパケットを隠す**:選択したパケットを除き、リストにおけるすべてのパケットを隠します。
- **隠されたすべてのパケットを表示する**:隠されたすべてのパケットをリストに表示します。
- **すべてを選択**:リストにおけるすべてのアイテムを選択します。
- **備考**:選択されたパケットのために、備考を作成します。
- **ハイライト**:選択されたパケットをハイライト表示します。
- **デコード**:選択されたパケットを強制的にデコードします。「デコード」をクリックし、表示されたダイアログボックスでデコード条件を設定し、デコードプロトコルを選択することで、デコード条件と一致するパケットは全部選択されたデコードプロトコルに基づき強制的にデコードされます。

デコード情報を確認するとき、各階層における-マイナスまたは+プラス記号をクリックして、その階層を展開したら、折りたたんだりすることができます。フィールドデコードパネルで右クリックして、すべてを展開したり、折りたたんだりすることができます。



以下のリストはフィールドデコードパネルにおけるポップアップメニューの各アイテムについて説明しています。

- **コピー**:選択したアイテムをクリップボードにコピーします。
- **ツリーをコピー**:選択したパケットデコードツリーをクリップボードにコピーして、上位ノードが選択された場合にのみ、利用可能となります。
- **フィルターを作成**:選択したアイテムに基づいて、フィルターを作成します。
- **ネームテーブルに追加**:選択したノードの別名をネームテーブルに追加します。
- **すべてを展開**:すべてのアイテムを展開します。
- **すべてを折りたたむ**:すべてのアイテムを折りたたみます。
- **すべてを選択**:フィールドデコードパネルにおけるすべてのアイテムを選択します。
- **更新**:現在のパネルを更新します。

HEX デコードパネスの右側で、ASCII コードまたは EBCDIC コードでデータを表示することができます。右クリックして、興味を持っているコードを選択すればよいのです。

以下のリストは、HEX デコードパネルにおけるポップアップメニューの各アイテムについて説明しています。

- **コピー**:データをクリップボードにコピーします。
- **HEX をコピー**: HEX 数字をクリップボードにコピーします。
- **テキストをコピー**: ASCII/EBCDIC デコードエリアで選択したテキストをコピーします。
- **ASCII コードで表示**: ASCII でデコード情報を表示します。
- **EBCDIC コードで表示**: EBCDIC でデコード情報を表示します。
- **すべてを選択**:すべての HEX 数字を選択します。
- **更新**:現在パネルを更新します。

セキュリティ解析

セキュリティ解析は、ワームアクティビティ、TCP ポートスキャン、ARP 攻撃、DoS 攻撃、および不審セッションを検出するために、設計されたものです。セキュリティ解析を実行するには、セキュリティ解析プロファイルを使用する必要があります。

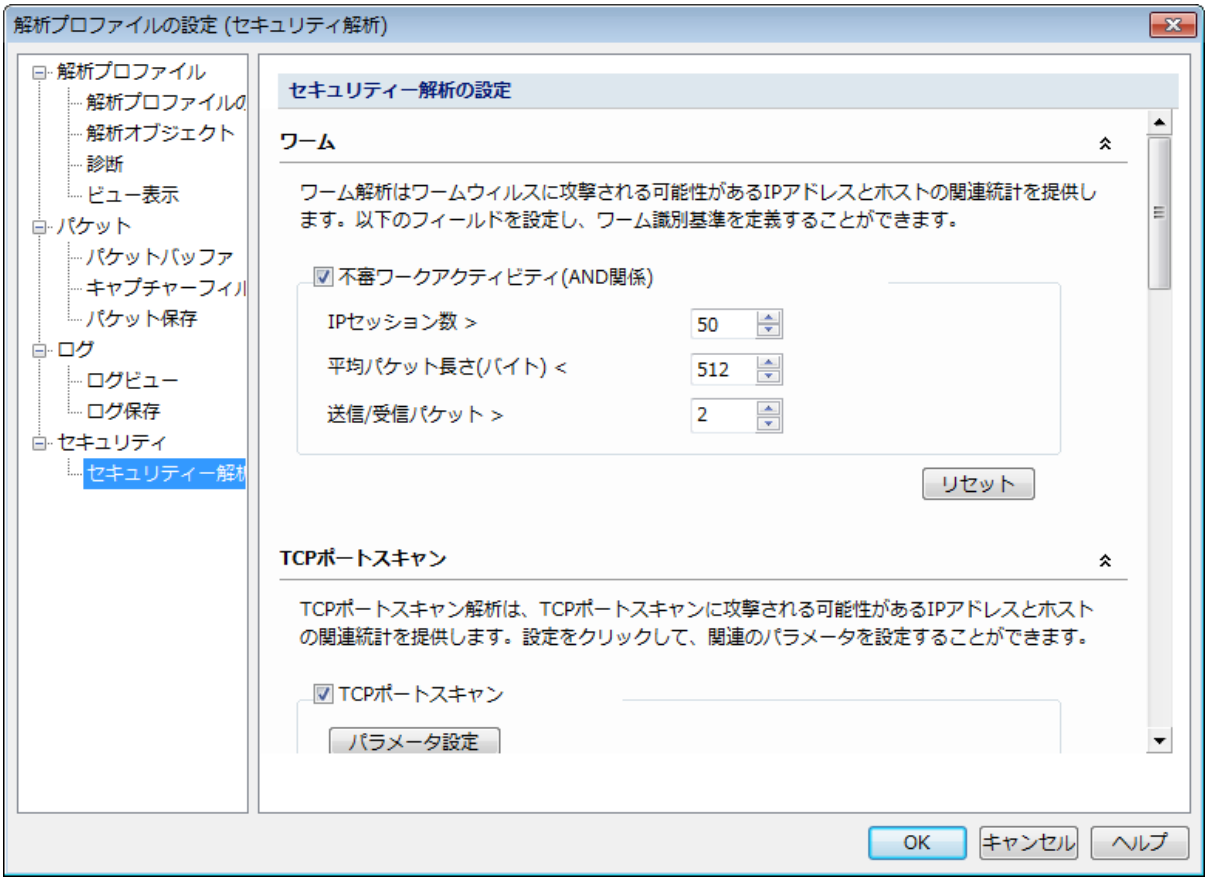
- セキュリティ解析プロファイル
- セキュリティ解析ビュー

注意 セキュリティ解析は、Capsa Enterprise の場合にのみ、利用可能となります。

セキュリティ解析プロファイル

セキュリティ解析プロファイルを適用するには、スタートページで、それを選択すればよいのです。

セキュリティ解析プロファイルをダブルクリックして、セキュリティ解析の設定を確認、変更することができます。



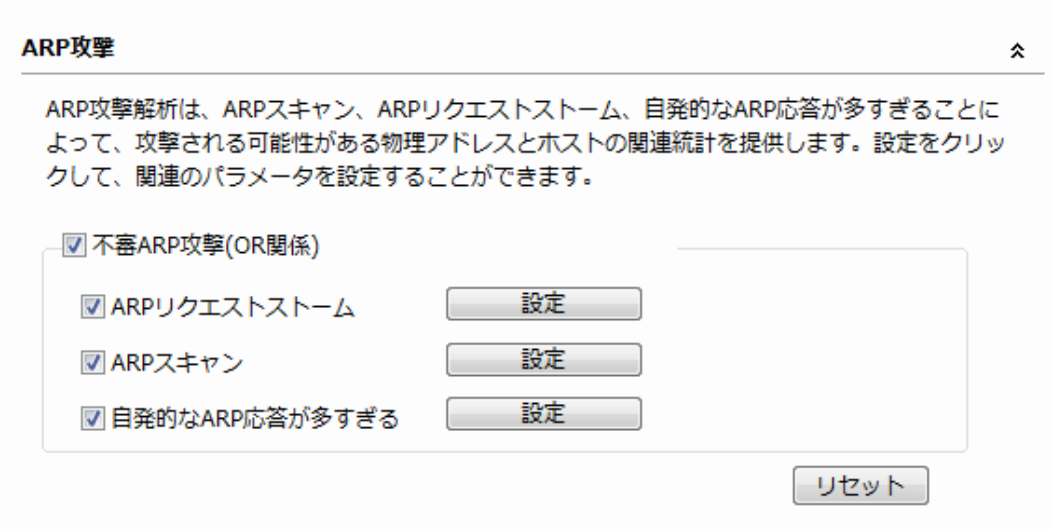
セキュリティ解析タブを除き、セキュリティ解析プロファイルにある他のすべての設定タブは、フル解析プロファイルとまったく同じです。それらの設定タブを変更するには、解析プロファイルをご参照ください。

セキュリティ解析タブには、以下の設定が含まれています。

- ARP 攻撃設定
- ワーム設定
- 起こした DoS 攻撃設定
- 受けた DoS 攻撃設定
- TCP ポートスキャン設定
- 不審セッション設定

ARP 攻撃設定

ARP 攻撃解析は、ARP 攻撃アクティビティを検出します。ARP 攻撃設定部分は以下のように表示されます。



不審 ARP 攻撃: ARP 攻撃解析を有効にします。そうしないと、**ARP 攻撃**ビューには、何も表示されません。**OR 関係**は、以下の三つの条件のいずれを満たしている場合、ARP 攻撃が発生していると思われることを表します。

- **ARP リクエストストーム**: ARP リクエストストーム解析を有効にします。**設定**をクリックして、**診断**タブにおける **ARP リクエストストーム**診断イベントにロケートします。このイベントには主に二つのパラメータがあります。
- **サンプリング時間**:サンプリング時間で、秒を単位としています。1 から 3,600 までの整数を設定することができます。デフォルトでは、20 となります。
- **リクエスト回数**: ARP リクエストの回数です。ARP リクエスト回数が設定された値を上回ると、ネットワークにおいて ARP リクエストストームが発生していると考えられます。1 から 10,000 までの整数を設定することができます。デフォルトでは、10 となります。
- **ARP スキャン**: ARP スキャン解析を有効にします。**設定**をクリックして、**診断**タブにおける **ARP スキャン**診断イベントにロケートします。このイベントには主に二つのパラメータがあります。
- **サンプリングタイムのスキャン**:サンプリング時間で、秒を単位としています。15 から 180 までの整数を設定することができます。デフォルトでは、60 となります。
- **無応答のパケットパーセンテージ(%)**:無応答のパケットパーセンテージの割合です。その割合が設定された値を上回ると、ネットワークにおいて ARP スキャン攻撃が発生していると考えられます。1 から 100 までの整数を設定することができます。デフォルトでは、20 となります。
- **自発的な ARP 応答が多すぎる**:自発的な ARP 応答が多すぎることに対する解析を有効にします。**設定**をクリックして、**診断**タブにおける **ARP 応答が多すぎる**という診断

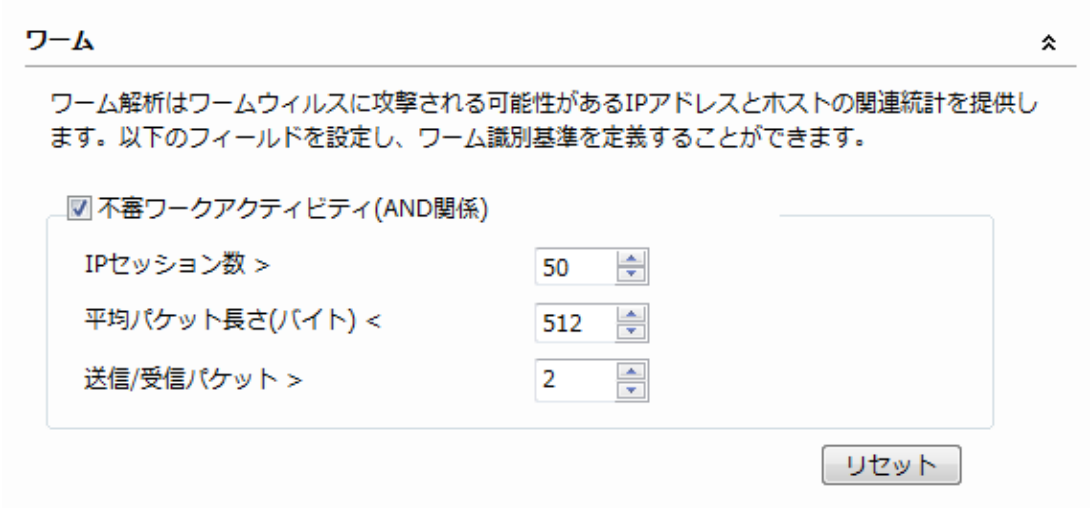
イベントにロケートします。このイベントには主に二つのパラメータがあります。

- **時間単位**:サンプリング時間で、秒を単位としています。30 から 3,600 までの整数を設定することができます。デフォルトでは、60 となります。
- **送信応答数**:送信応答の回数です。送信応答数が設定された値を上回ると、ネットワークにおいて自発的な ARP 応答が多すぎるというイベントが発生していると考えられます。30 から 20,000 までの整数を設定することができます。デフォルトでは、300 となります。

リセット:このタイプのセキュリティ解析の設定をデフォルトにリセットします。

ワーム設定

ワーム解析は不審なワームアクティビティを検出します。ワーム設定部分は以下のように表示されます。



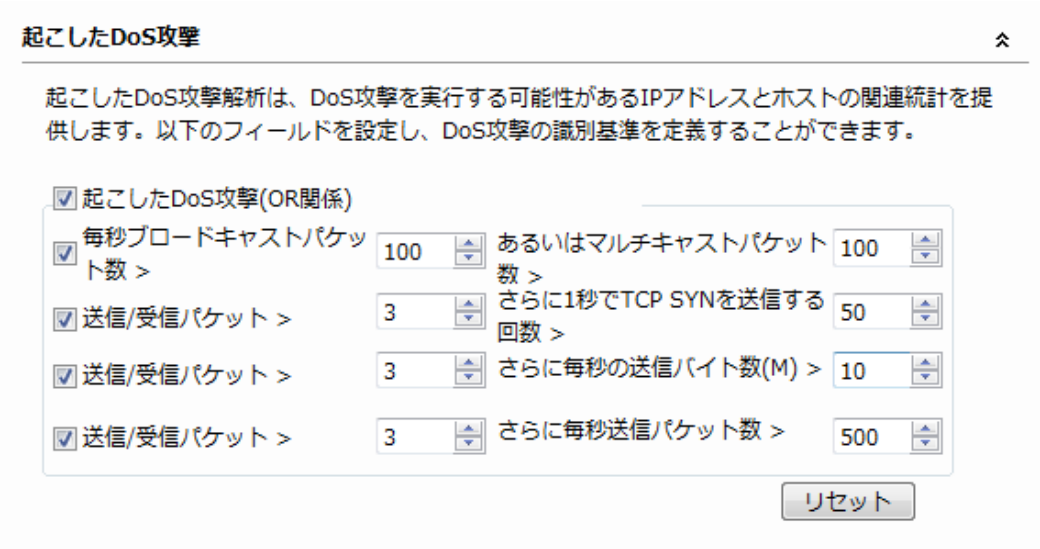
不審ワームアクティビティ:ワーム解析を有効にします。そうしないと、**ワーム**ビューには何も表示されません。**AND 関係**は、以下の三つの条件をすべて満たしている場合にのみ、ワーク攻撃が発生していると思われることを表します。

- **IP セッション数**:ホストの IP セッション数を設定します。IP セッション数が設定された値を上回ると、ホストがワームウィルスに感染していると考えられます。1 から 1,000 までの整数を設定することができます。デフォルトでは、50 となります。
- **平均パケット長さ**:バイトを単位としています。ホストの平均パケット長さが設定された値を下回ると、ホストがワームウィルスに感染していると考えられます。64 から 1,514 までの整数を設定することができます。デフォルトでは、512 となります。
- **送信/受信パケット**:送信パケット対受信パケットの比率です。その比率が設定された値を上回ると、ホストがワームウィルスに感染していると考えられます。1 から 100 までの整数を設定することができます。デフォルトでは、2 となります。

リセット:このタイプのセキュリティ解析の設定をデフォルトにリセットします。

起こした DoS 攻撃設定

起こした DoS 攻撃解析は、DoS 攻撃を実行しているホストを検出します。起こした DoS 攻撃設定部分は以下のように表示されます。



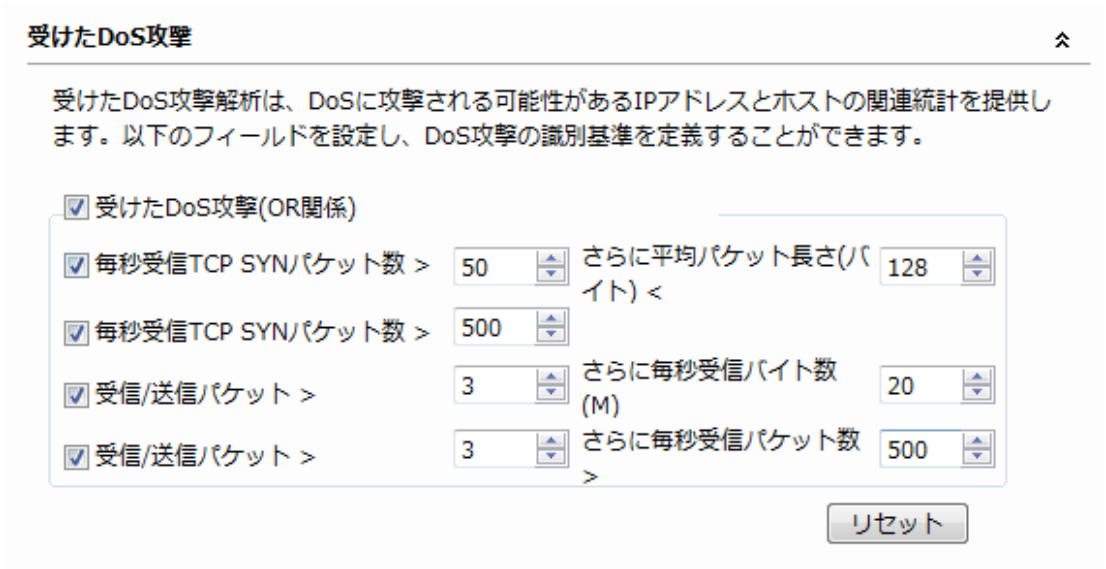
起こした DoS 攻撃:起こした DoS 攻撃解析を有効にします。そうしないと、**起こした DoS 攻撃**ビューには、何も表示されません。**OR 関係**は、以下の四つの条件のいずれを満たしている場合、起こした DoS 攻撃が発生していると思われることを表します。

- 毎秒ブロードキャストパケット数、あるいは毎秒マルチキャストパケット数が設定された値を上回ると、起こした DoS 攻撃が発生していると考えられます。両方とも 10 から 500 までの整数を設定することができます。デフォルトでは、100 となります。
- 送信パケット対受信パケットの比率が設定された値を上回り、さらに 1 秒で TCP SYN パケットを送信する回数が設定された値を上回る場合、起こした DoS 攻撃が発生していると考えられます。前者は 1 から 5 までの整数を設定することができ、デフォルトでは 3 となります。後者は 3 から 200 までの整数を設定することができ、デフォルトでは 50 となります。
- 送信パケット対受信パケットの比率が設定された値を上回り、さらに毎秒の送信バイト数が設定された値を上回る場合、起こした DoS 攻撃が発生していると考えられます。前者は 1 から 5 までの整数を設定することができ、デフォルトでは 3 となります。後者は 1 から 100 までの整数を設定することができ、デフォルトでは 10 となります。
- 送信パケット対受信パケットの比率が設定された値を上回り、さらに毎秒送信パケット数が設定された値を上回る場合、起こした DoS 攻撃が発生していると考えられます。前者は 1 から 5 までの整数を設定することができ、デフォルトでは 3 となります。後者は 100 から 1,000 までの整数を設定することができ、デフォルトでは 500 となります。

リセット:このタイプのセキュリティ解析の設定をデフォルトにリセットします。

受けた DoS 攻撃設定

受けた DoS 攻撃解析は、DoS 攻撃を受けたホストを検出します。受けた DoS 攻撃設定部分は以下のように表示されます。



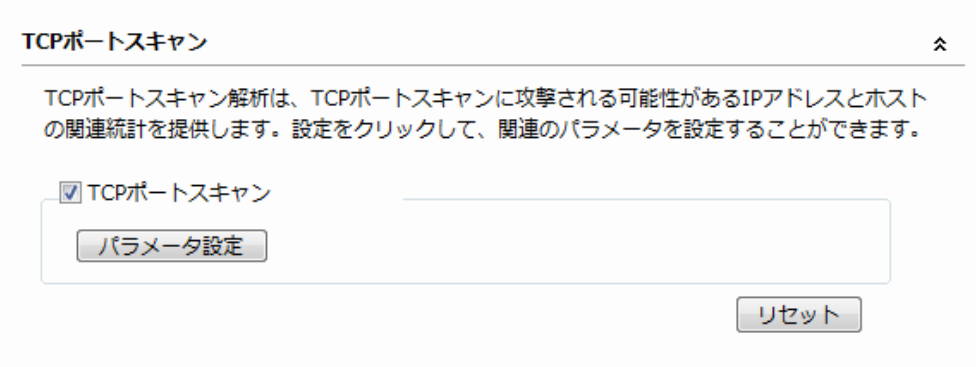
受けた DoS 攻撃:受けた DoS 攻撃解析を有効にします。そうしないと、受けた DoS 攻撃ビューには何も表示されません。**OR 関係**は、以下の四つの条件のいずれを満たしている場合、受けた DoS 攻撃が発生していると思われることを表します。

- 毎秒受信 TCP SYN パケット数が設定された値を上回り、さらに平均パケット長さが設定された値を下回る場合、受けた DoS 攻撃が発生していると考えられます。前者は 5 から 500 までの整数を設定することができ、デフォルトでは 50 となります。後者は 64 から 1,518 までの整数を設定することができ、デフォルトでは 128 となります。
- 毎秒受信 TCP SYN パケット数が設定された値を上回る場合、受けた DoS 攻撃が発生していると考えられます。5 から 1,000 までの整数を設定することができます。デフォルトでは、500 となります。
- 送信パケット対受信パケットの比率が設定された値を上回り、さらに毎秒の受信バイト数が設定された値を上回る場合、受けた DoS 攻撃が発生していると考えられます。前者は 1 から 5 までの整数を設定することができ、デフォルトでは 3 となります。後者は 1 から 100 までの整数を設定することができ、デフォルトでは 20 となります。
- 送信パケット対受信パケットの比率が設定された値を上回り、さらに毎秒受信パケット数が設定された値を上回る場合、受けた DoS 攻撃が発生していると考えられます。前者は 1 から 5 までの整数を設定することができ、デフォルトでは 3 となります。後者は 50 から 1,000 までの整数を設定することができ、デフォルトでは 500 となります。

リセット:このタイプのセキュリティ解析の設定をデフォルトにリセットします。

TCP ポートスキャン設定

TCP ポートスキャン解析は、TCP ポートスキャンアクティビティを検出します。TCP ポートスキャン設定部分は以下のように表示されます。



TCP ポートスキャン: TCP ポートスキャンを有効にします。そうしないと、**TCP ポートスキャン**ビューには何も表示されません。

パラメータ設定:**診断**タブにおける **TCP ポートスキャン**診断イベントにロケートします。イベント設定パネルにおけるパラメータ**宛先ポート数**はローカルまたはリモートホストに接続された TCP ポートの数を表します。宛先ポート数が設定された値を上回る場合、そのホストが TCP ポートスキャンを実行していると考えられます。5 から 50 までの整数を設定することができます。デフォルトでは 6 となります。

リセット:このタイプのセキュリティ解析の設定をデフォルトにリセットします。

不審セッション設定

不審セッション解析は、不審な HTTP、FTP、SMTP および POP3 セッションを検出します。不審セッション設定部分は以下のように表示されます。

不審セッション:不審セッション解析を有効にします。そうしないと、**不審セッション**ビューには何も表示しません。**OR 関係**は、以下の四つの条件のいずれを満たしている場合、不審セッションが発生していると思われることを表します。

- **不審な HTTP セッション**:不審な HTTP セッション解析を有効にします。**診断**タブで設定されています。ポート 80 を利用して、非 HTTP データを転送する場合、ネットワークにおいて不審な HTTP セッションが発生していると考えられます。
- **不審な POP3 セッション**:不審な POP3 セッション解析を有効にします。**診断**タブで設定されています。ポート 110 を利用して、非 POP3 データを転送する場合、ネットワークにおいて不審な POP3 セッションが発生していると考えられます。
- **不審な FTP セッション**:不審な FTP セッション解析を有効にします。**診断**タブで設定されています。ポート 21 を利用して、非 FTP データを転送する場合、ネットワークにおいて不審な FTP セッションが発生していると考えられます。
- **不審な SMTP セッション**:不審な SMTP セッション解析を有効にします。**診断**タブで設定されています。ポート 25 を利用して、非 SMTP データを転送する場合、不審な SMTP セッションが発生していると考えられます。

リセット:このタイプのセキュリティ解析の設定をデフォルトにリセットします。

セキュリティ解析ビュー

セキュリティ解析は、ワームアクティビティ、TCP ポートスキャン、ARP 攻撃、DoS 攻撃、および不審セッションを検出するために、設計されたものです。ネットワークにこれらの攻撃が発生したら、攻撃情報は対応のセキュリティ解析ビューに表示されます。

- ARP 攻撃ビュー
- ワームビュー
- 起こした DoS 攻撃ビュー
- 受けた DoS 攻撃ビュー
- TCP ポートスキャンビュー
- 不審セッションビュー

注意 セキュリティセッションビューは Capsa Enterprise の場合にのみ、利用可能となります。

ARP 攻撃ビュー

ARP 攻撃ビューは、**セキュリティ解析プロファイル**を利用している場合にのみ、利用可能となります。

ARP 攻撃解析は、ARP スキャン、ARP スプーフィング、ARP リクエストストームを検出することができます。これらの ARP 問題は、デフォルトの設定値に基づいて識別されます。これらの問題をより正確に検出するために、自分で設定値を定義することもできます。

注意 **プロトコルブラウザ**と IP **ブラウザ**で任意ノードを選択した場合、あるいは**物理ブラウザ**で IP アドレスノードを選択した場合、**ARP 攻撃**ビューは利用できません。

このビューは、ARP 攻撃を受けた可能性があるホストの MAC アドレスとトラフィック情報をリストします。リストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

ARP 攻撃ビューにおけるカラムについて

カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。カラムの詳しいことは、エンドポイントビューにおけるカラムについてをご参照ください。

ARP 攻撃ビュー下位パネル

ARP 攻撃ビューにおけるノードリストであるアイテムを選択した場合、下位パネルは、このアイテムの詳細情報を表示します。デフォルトで下位パネルは表示されますが、**ARP 攻撃**ビューにおける  ボタンをクリックして、それを隠すことができます。ARP 攻撃ビュー下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

下位パネルは、**ARP 攻撃**ビューで選択されたノードのすべての MAC アドレスセッションをリストする**物理セッション**タブを提供します。**物理セッション**タブにおけるツールバーとカラムは**物理セッション**ビューとまったく同じです。

セッションリストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

ワームビュー

ワームビューは、**セキュリティ解析プロファイル**を利用している場合にのみ、利用可能となります。

コンピュータワームは、自身を複製するマルウェアコンピュータプログラムです。ユーザー操作なしで自発的にネットワークを利用して自身のコピーを他のノードに送信します。自分自身を拡散するには、直接他のコンピューターに感染したり、電子メールで送信したりして、

いつもネットワークを必要としています。ワーム攻撃は、デフォルトの設定値に基づいて識別されます。攻撃をより正確に検出するために、自分で設定値を定義することもできます。

注意 **プロトコルブラウザ**で任意ノードを選択した場合、あるいは**物理ブラウザ**で IP アドレスノードを除く他のノードを選択した場合、**ワーム**ビューは利用できません。

このビューは、ワームに感染した可能性があるホストの IP アドレスとトラフィック情報をリストします。リストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

ワームビューにおけるカラムについて

カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。カラムの詳しいことは、エンドポイントビューにおけるカラムについてをご参照ください。

ワームビュー下位パネル

ワームビューにおけるノードリストであるアイテムを選択した場合、下位パネルは、このアイテムの詳細情報を表示します。デフォルトで下位パネルは表示されますが、**ワーム**ビューにおける  ボタンをクリックして、それを隠すことができます。ワームビュー下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

ワームビュー下位パネルは、**IP セッション**タブ、**TCP セッション**タブ、および**UDP セッション**タブを提供します。

- **IP セッション**タブは、**ワーム**ビューで選択されたノードのすべての IP アドレスセッションをリストします。このタブにおけるツールバーとカラムは、**IP セッション**ビューとまったく同じです。
- **TCP セッション**タブは、**ワーム**ビューで選択されたノードの中で TCP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは**TCP セッション**ビューとまったく同じです。
- **UDP セッション**タブは、**ワーム**ビューで選択されたノードの中で UDP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは**UDP セッション**ビューとまったく同じです。

セッションリストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

起こした DoS 攻撃ビュー

起こした DoS 攻撃ビューは、**セキュリティ解析プロファイル**を利用している場合にのみ、利用可能となります。

このビューで表示されるアイテムがある場合、それはリストされたコンピューターがリモートまたはローカルサイトの攻撃に参加させられることを表します。このように攻撃に参加させられるマシンは、ボットネットと呼ばれています。ボットネットは、かなり多くの帯域幅を消費します。起こした DoS 攻撃は、デフォルトの設定値に基づいて識別されます。根本的な問題をより正確に検出するために、自分で設定値を定義することもできます。

注意 **プロトコルブラウザ**で任意ノードを選択した場合、あるいは**物理ブラウザ**で IP アドレスノードを除く他のノードを選択した場合、**起こした DoS 攻撃**ビューは利用できません。

このビューは、起こした DoS 攻撃を実行している可能性があるホストの IP アドレスとトラフィック情報をリストします。リストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

起こした DoS 攻撃ビューにおけるカラムについて

カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。カラムの詳しいことは、エンドポイントビューにおけるカラムについてをご参照ください。

起こした DoS 攻撃ビュー下位パネル

起こした DoS 攻撃ビューにおけるノードリストであるアイテムを選択した場合、下位パネルは、このアイテムの詳細情報を表示します。デフォルトで下位パネルは表示されますが、

起こした DoS 攻撃ビューにおける  ボタンをクリックして、それを隠すことができます。

起こした DoS 攻撃ビュー下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

起こした DoS 攻撃ビュー下位パネルは、**IP セッション**タブ、**TCP セッション**タブ、および**UDP セッション**タブを提供します。

- **IP セッション**タブは、**起こした DoS 攻撃**ビューで選択されたノードのすべての IP アドレスセッションをリストします。このタブにおけるツールバーとカラムは、**IP セッション**ビューとまったく同じです。
- **TCP セッション**タブは、**起こした DoS 攻撃**ビューで選択されたノードの中で TCP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは**TCP セッション**ビューとまったく同じです。
- **UDP セッション**タブは、**起こした DoS 攻撃**ビューで選択されたノードの中で UDP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは**UDP セッション**ビューとまったく同じです。

セッションリストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

受けた DoS 攻撃ビュー

受けた DoS 攻撃ビューは、**セキュリティ解析プロファイル**を利用している場合にのみ、利用可能となります。

受けた DoS 攻撃は、お使いのネットワークにおけるホストが DoS または DDoS 攻撃を受けていることを表します。DoS 攻撃（ denial-of-service attack）または DDoS 攻撃（分散 DoS 攻撃、distributed denial-of-service attack）は、コンピューターに負荷をかけることによって、コンピューター資源を提供できなくする攻撃です。攻撃の一般的な方法として、大量の外部通信リクエストで目標マシン（被害者）を高負荷状態にさせることによって、目標マシンが正当なトラフィックにレスポンスできなくなったり、あるいはレスポンスが遅くなったりすることがあります。一般的に DoS 攻撃は目標コンピューターを強制的にリセットさせたり、あるいはコンピューター資源を消費したりすることで、サービスを提供できないようにします。または目標マシンと他のユーザーの間の通信媒体を妨害することで、目標マシンがほかのユーザーと通信できないようにします。

受けた DoS 攻撃は、デフォルトの設定値に基づいて識別されます。根本的な問題をより正確に検出するために、自分で設定値を定義することもできます。

注意 **プロトコルブラウザ**で任意ノードを選択した場合、あるいは**物理ブラウザ**で IP アドレスノードを除く他のノードを選択した場合、**受けた DoS 攻撃**ビューは利用できません。

このビューは、DoS または DDoS 攻撃を受けた可能性があるホストの IP アドレスとトラフィック情報をリストします。リストにおける任意アイテムをダブルクリックして、開かれた**パ**

ケットウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

受けた DoS 攻撃ビューにおけるカラムについて

カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。カラムの詳しいことは、エンドポイントビューにおけるカラムについてをご参照ください。

受けた DoS 攻撃ビュー下位パネル

受けた DoS 攻撃ビューにおけるノードリストであるアイテムを選択した場合、下位パネルは、このアイテムの詳細情報を表示します。デフォルトで下位パネルは表示されますが、**受けた DoS 攻撃**ビューにおける  ボタンをクリックして、それを隠すことができます。受けた DoS 攻撃ビュー下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

受けた DoS 攻撃ビュー下位パネルは 、**IP セッション**タブ、**TCP セッション**タブ、および**UDP セッション**タブを提供します。

- **IP セッション**タブは、**受けた DoS 攻撃**ビューで選択されたノードのすべての IP アドレスセッションをリストします。このタブにおけるツールバーとカラムは、**IP セッション**ビューとまったく同じです。
- **TCP セッション**タブは、**受けた DoS 攻撃**ビューで選択されたノードの中で TCP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは **TCP セッション**ビューとまったく同じです。
- **UDP セッション**タブは、**受けた DoS 攻撃**ビューで選択されたノードの中で UDP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは **UDP セッション**ビューとまったく同じです。

セッションリストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

TCP ポートスキャンビュー

TCP ポートスキャンビューは、**セキュリティ解析プロファイル**を利用している場合にのみ、利用可能となります。

スキャンは、マルウェアがほかのホストに感染したり、あるいはハッカーがシステムに侵入したりする最初のステップです。ネットワーク管理者は、ポートスキャンに注意を払う必要があります。ホストは短時間で大量の TCP SYN パケットを連続でターゲットホストに送信する場合、それは TCP ポートスキャンだと思われます。TCP ポートスキャン攻撃は、デフォルトの設定値に基づいて識別されます。根本的な問題をより正確に検出するために、自分で設定値を定義することもできます。

注意 **プロトコルブラウザ**で任意ノードを選択した場合、あるいは**物理ブラウザ**で IP アドレスノードを除く他のノードを選択した場合、**TCP ポートスキャン**ビューは利用できません。

このビューは、TCP ポートスキャンを受けた可能性があるホストの IP アドレスとトラフィック情報をリストします。リストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

TCP ポートスキャンビューにおけるカラムについて

カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。カラムの詳しいことは、エンドポイントビューにおけるカラムについてをご参照ください。

TCP ポートスキャンビュー下位パネル

TCP ポートスキャンビューにおけるノードリストであるアイテムを選択した場合、下位パネルは、このアイテムの詳細情報を表示します。デフォルトで下位パネルは表示されますが、**TCP ポートスキャン**ビューにおける  ボタンをクリックして、それを隠すことができます。

TCP ポートスキャンビュー下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

TCP ポートスキャンビュー下位パネルは、**IP セッション**タブ、**TCP セッション**タブ、および**UDP セッション**タブを提供します。

- **IP セッション**タブは、**TCP ポートスキャン**ビューで選択されたノードのすべての IP アドレスセッションをリストします。このタブにおけるツールバーとカラムは、**IP セッション**ビューとまったく同じです。
- **TCP セッション**タブは、**TCP ポートスキャン**ビューで選択されたノードの中で TCP プロトコルを使用しているセッションをリストします。このタブにおけるツールバー

とカラムは**TCP セッション**ビューとまったく同じです。

- **UDP セッション**タブは、**TCP ポートスキャン**ビューで選択されたノードの中で UDP プロトコルを使用しているセッションをリストします。このタブにおけるツールバーとカラムは**UDP セッション**ビューとまったく同じです。

セッションリストにおける任意アイテムをダブルクリックして、開かれた**パケット**ウィンドウで詳細なパケット情報を確認することができます。**パケット**ウィンドウは**パケット**ビューとまったく同じです。

不審セッションビュー

不審セッションビューは、**セキュリティ解析プロファイル**を利用している場合にのみ、利用可能となります。

TCP ポートを利用して、対応のトラフィックデータを転送しないセッションは不審セッションだと思われます。Capsa は不審 HTTP セッション、不審 POP3 セッション、不審 SMTP セッション、および不審 FTP セッションを識別することができます。不審セッションはデフォルトの設定値に基づいて識別されます。不審セッションを検出しないように設定することができます。

注意 **プロトコルブラウザ**で任意ノードを選択した場合、あるいは**物理ブラウザ**で IP アドレスノードを除く他のノードを選択した場合、**不審セッション**ビューは利用できません。

このビューは、不審セッションのトラフィック統計情報をリストします。リストにおける任意アイテムをダブルクリックして、開かれた **TCP フロー解析**ウィンドウで詳細なセッション情報を確認することができます。

不審セッションビューにおけるカラムについて

カラムヘッダーを右クリックして、リストで表示したいカラムを指定することができます。**デフォルト**をクリックして、デフォルトカラムだけが表示されます。**さらに**をクリックして、**カラムを表示する**ダイアログボックスが表示されます。ここで表示したいカラムを設定したり、カラムの表示順序や配置方法、カラムの幅などを設定したりすることができます。カラムの詳しいことは、セッションビューにおけるカラムについてをご参照ください。

不審セッションビュー下位パネル

不審セッションビューにおけるセッションリストであるアイテムを選択した場合、下位パネルは、このアイテムの詳細情報を表示します。デフォルトで下位パネルは表示されますが、

不審セッションビューにおける  ボタンをクリックして、それを隠すことができます。不

審セッションビュー下位パネルが隠されている場合、  ボタンをクリックすると、それがまた表示されます。

不審セッションビュー下位パネルはパケット、データフロー、シーケンスチャートという三つのタブから構成されています。

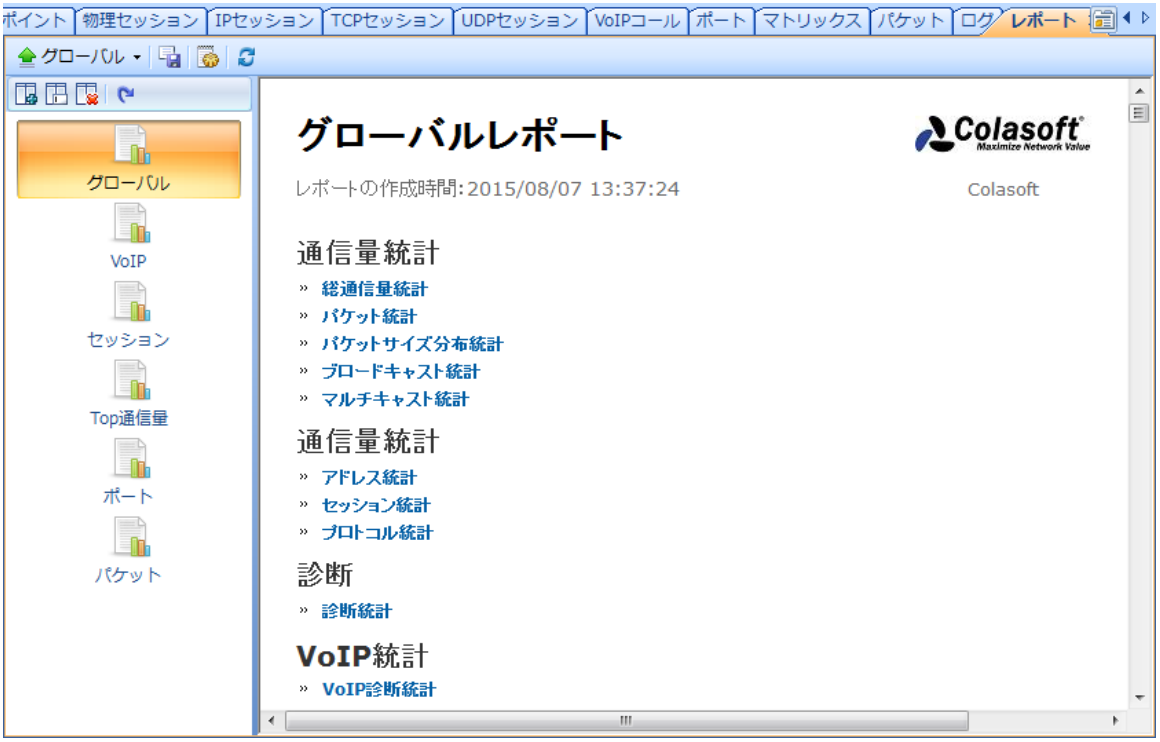
- **パケット**タブは、**不審セッション**ビューで選択されたセッションのすべてのパケットをリストします。このタブにおけるツールバーとカラムは**パケット**ビューとまったく同じです。
- **データフロー**タブは**不審セッション**ビューで選択された TCP セッションに対する再構築データフローを提供します。詳しいことはデータフロータブをご参照ください。
- **シーケンスチャート**タブは TCP セッションを時間順で表示します。詳しいことは、シーケンスチャートタブをご参照ください。

レポート

レポートビュー

レポートビューは左側パネルと右側パネルから構成され、全体ネットワークのリアルタイム通信量統計を提供します。左側パネルはすべてのレポートが含まれていて、右側パネルは左側パネルで選択されたレポートを表示します。

デフォルトでは、左側パネルは下図のように七つのレポートが含まれています。



グローバルレポートには解析プロジェクトのすべてのレポートアイテムが含まれています。VoIP レポートは VoIP 解析の統計を記録します。レポート名をクリックして、各レポートを確認することができます。

「無線」レポートは WiFi ネットワークを監視している場合にのみ、利用可能となり、「VoIP」レポートは、VoIP 解析モジュールが有効にされている場合にのみ、利用可能となることに注意してください。

デフォルトのレポートの他に、新しいレポートを作成することもできます（詳しいことは、レポートを作成をご参照ください）。

すべてのレポートはレポートヘッダー、レポート本文、およびレポートフッターという三つの部分から構成されています。

- レポートヘッダー部分はレポート名、レポート作成時間、会社ロゴ、および会社名を表示します。
- レポート本文部分は、レポートの主要部分です。複数の表、統計、および棒グラフから構成されています。棒グラフを利用して、ユーザーは容易にネットワーク状況を把握することができます。
- レポートフッター部分はレポートの作成者を表示します。

デフォルトでは、レポート作成時間、会社ロゴ、会社名、およびレポート作成者は未表示にされています。これらの情報を表示するには、  をクリックして、設定を変更する必要があります（詳しいことはレポート をご参照ください）。

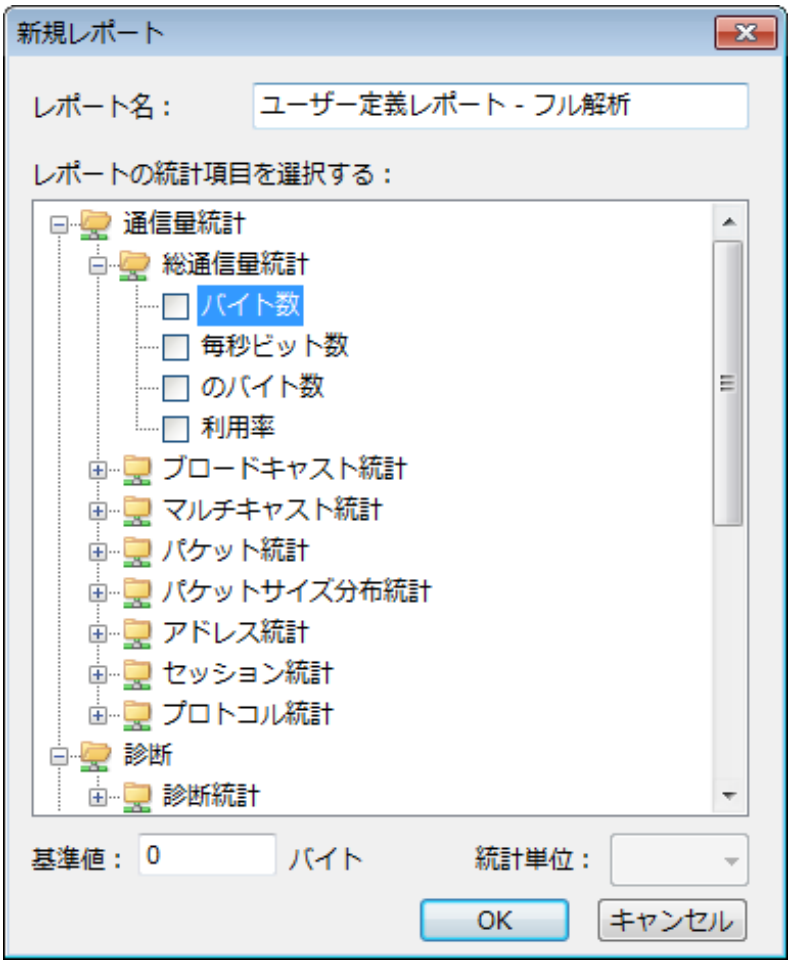
レポートを保存するには、  をクリックして、保存することができます。レポートを.pdf および.html フォーマットで保存することができます。

レポートを作成

Capsa では、ユーザーは必要に応じて全体ネットワークまたは特定のノードに基づいてレポートを作成することができます。

以下のステップに従い、全体ネットワークに基づいて、レポートを作成します。

1. レポートビューで、  をクリックして、下図のように**新規レポート**ダイアログボックスが開かれます。



2. レポートの名前を入力します。
3. レポートの統計項目を選択し、基準値を入力して、各統計項目の統計単位を指定します（レポート項目 をご参照ください）。
4. OK をクリックします。

以下のステップに従い、特定のノードに基づいてレポートを作成します。

1. **ノードブラウザ**でレポートを作成したいノードを選択し、ツールバーにおける  をクリックすることで、**新規レポート**ダイアログボックスが開かれます。
2. レポートの名前を入力します。
3. レポートの統計項目を選択し、基準値を入力して、各統計項目の統計単位を指定します。
4. OK をクリックします。

ヒント

1. **診断統計**と **Top 統計**という二つの統計項目は基準値を持っていません。
2. **Top 統計**という項目だけは統計単位を持っています。

レポートを作成した後、**レポート**ビューのツールバーにおける  をクリックして、会社名、レポート名のプレフィックス、作成者、会社ロゴ、作成時間を表示するかどうかを設定することができます（詳しいことはレポート をご参照ください）。

レポート項目

以下はすべての利用可能なレポート項目をリストします。

通信量統計

- 総通信量統計:バイト数、毎秒ビット数、毎秒バイト数、利用率
- パケット統計:総パケット数、毎秒パケット数、平均パケット長さ
- パケットサイズ分布統計: <=64、65-127、 128-255、256-511、512-1023、1024-1517、 >=1518
- ブロードキャスト統計:ブロードキャストバイト数、ブロードキャストパケット数、毎秒ブロードキャストバイト数、毎秒ブロードキャストパケット数
- マルチキャストパケット:マルチキャストバイト数、マルチキャストパケット数、毎秒マルチキャストバイト数、毎秒マルチキャストパケット数
- アドレス統計: MAC アドレス数、IP アドレス数、ローカル IP アドレス数、リモート IP アドレス数
- セッション統計:物理セッション数、IP セッション数、TCP セッション数、UDP セッション数
- プロトコル統計:総プロトコル数、データリンク層プロトコル数、ネットワーク層プロトコル数、トランスポート層プロトコル数、セッション層プロトコル数、プレゼンテーション層プロトコル数、アプリケーション層プロトコル数

診断統計

情報イベント、注意イベント、警告イベント、エラーイベント

Top 統計

- Top アドレス、ホストとドメイン: Top MAC ホスト総通信量、Top MAC ホスト受信通信量、Top MAC ホスト送信通信量、Top IP ホスト総通信量、Top IP ホスト受信通信量、Top IP ホスト送信通信量、Top IP ホスト接続数、Top ローカル IP ホスト総通信量、Top ローカル IP ホスト受信通信量、Top ローカル IP ホスト送信通信量、Top ローカル IP ホスト接続数、Top リモート IP ホスト総通信量、Top リモート IP ホスト受信通信量、Top リモート IP ホスト送信通信量、Top ドメイン名
- Top セッション:物理セッション、Top IP セッション、Top TCP セッション、Top UDP セッション
- Top アプリケーション: Top アプリケーションプロトコル
- Top ポート : Top グローバルポート通信量、Top TCP ポート通信量、Top UDP ポート通信量

VoIP 統計

- VoIP 診断統計: VoIP SIP クライアント認証エラー、VoIP RTP パケットロス 、VoIP RTP パケット順番誤り、SDP 情報け損またはフォーマットエラー
- VoIP コールステータス統計:ダイヤル中のコール数、通話中のコール数、コール終了数、失敗コール数、総コール数
- VoIP MOS 分布:良い、普通、良くない、N/A

Top VoIP 統計

Top VoIP アドレスとホスト: Top IP コール頻度、 Top IP コール持続時間、Top IP コール通信量、Top コールエラーパケット比

ユーザーアクティビティログ

ユーザーアクティビティログはユーザーのネットワークアクティビティを記録します。
Capsa は以下のログタイプを提供します。

- ログビュー
- 全体ログ
- DNS ログ
- Email 情報
- FTP 転送
- HTTP リクエストログ
- ICQ ログ
- MSN ログ
- YAHOO ログ
- VoIP シグナリングログ
- VoIP コールログ

すべての解析プロジェクトには、すべてのログタイプが表示されるわけではありません。解析プロジェクトに表示されるログタイプは、選択された解析モジュールによって決まります。解析プロファイルによって、表示されるログタイプも異なります。

ログビュー

ログビューはキャプチャーされたパケットを解析することで、詳細的にユーザーのアクティビティをタイプごとに記録します。プログラムは自動的にキャプチャーされたパケット内のコマンドを解析し、アプリケーションタイプを識別します。アプリケーションのログ機能が有効になっている場合、コマンドとアクションは対応のログに記録されます。

ログビューは左側パネルと右側パネルから構成されています。左側パネルは現在解析プロファイルのすべてのログタイプをリストします。右側パネルは左側パネルで選択されたログタイプのログをリストします。ログビューでは、統計フィールドによってログを並べ替えることができます。

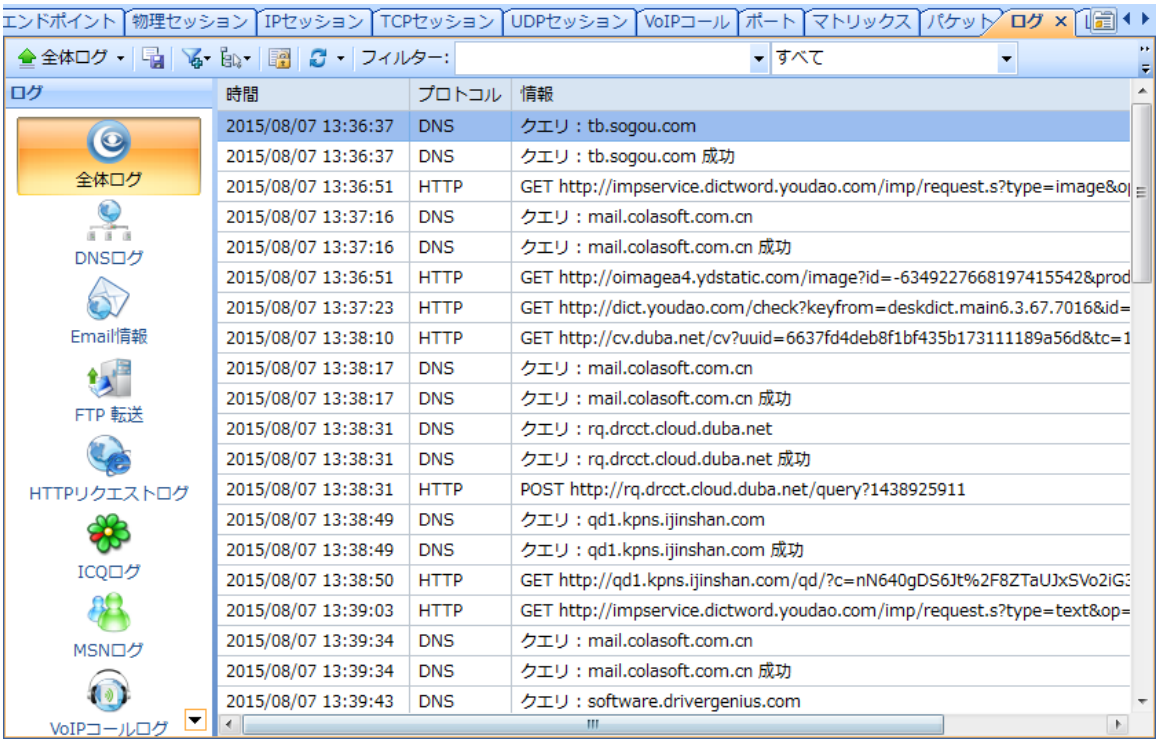
ツールバーにおける  をクリックして、選択されたログタイプのログリストを保存することができます。さらにログはキャプチャーを開始してから自動的に保存することができます。詳しいことはログ保存 をご参照ください。

注意 ログタイプが有効にされている場合にのみ、このタイプのログは表示されます。

詳しいことはログビューをご参照ください。

全体ログ

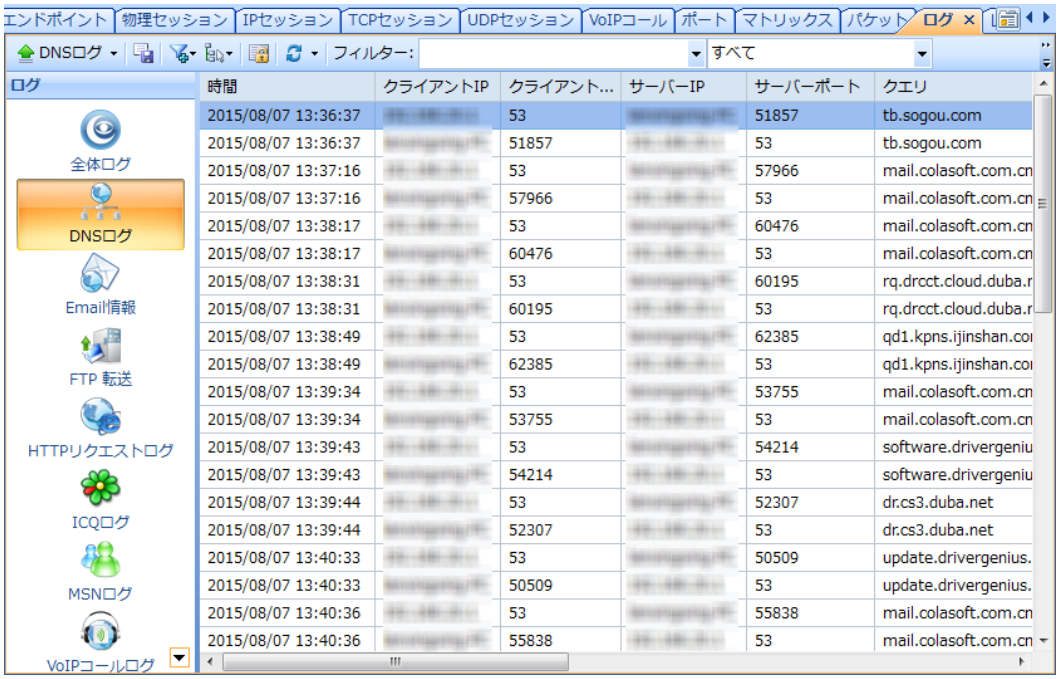
全体ログは下図のように他の九つのログタイプのログを収集し、時間に基づいてログ情報を表示します。



全体ログには、**時間**、**送信元 MAC アドレス**、**送信元 IP アドレス**、**宛先 MAC アドレス**、**宛先 IP アドレス**、**プロトコル**、および**情報**などのカラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。

DNS ログ

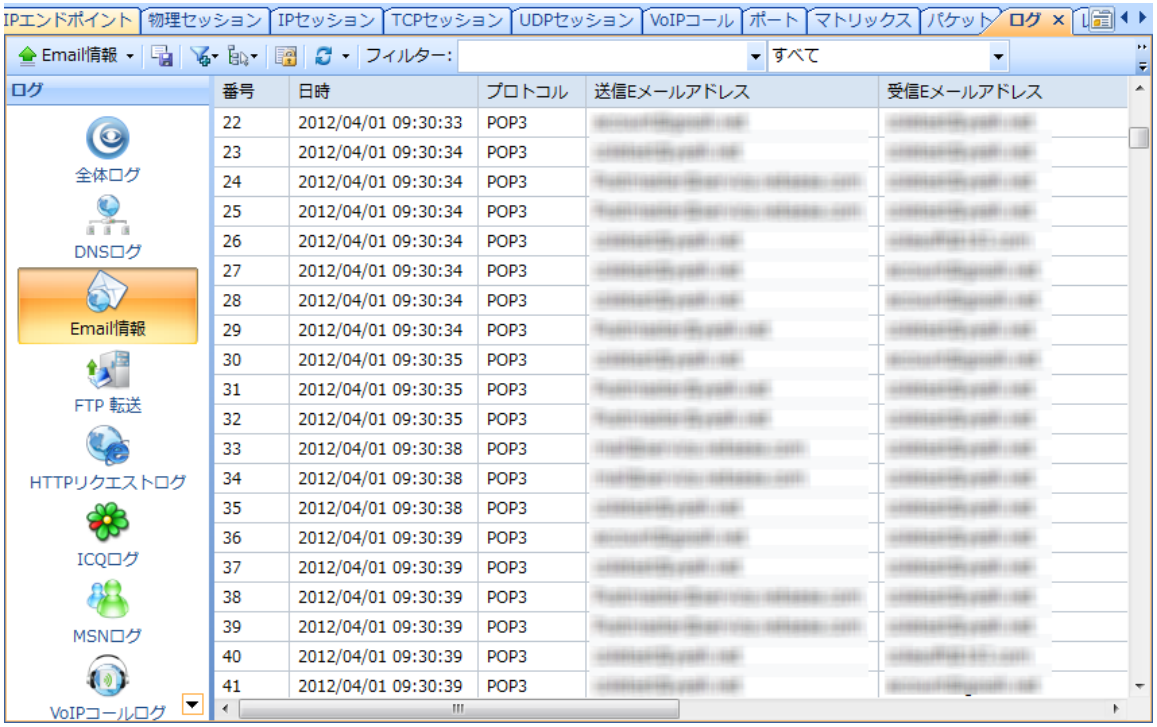
DNS ログは DNS クリエアプリケーションを記録し、下図のように表示されます。



DNS ログには、**時間**、**クライアント MAC アドレス**、**クライアント IP**、**クライアントポート**、**サーバーMAC アドレス**、**サーバーIP**、**サーバーポート**、**クエリ**、**ステータス**、および**結果**などのクラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。

Email 情報

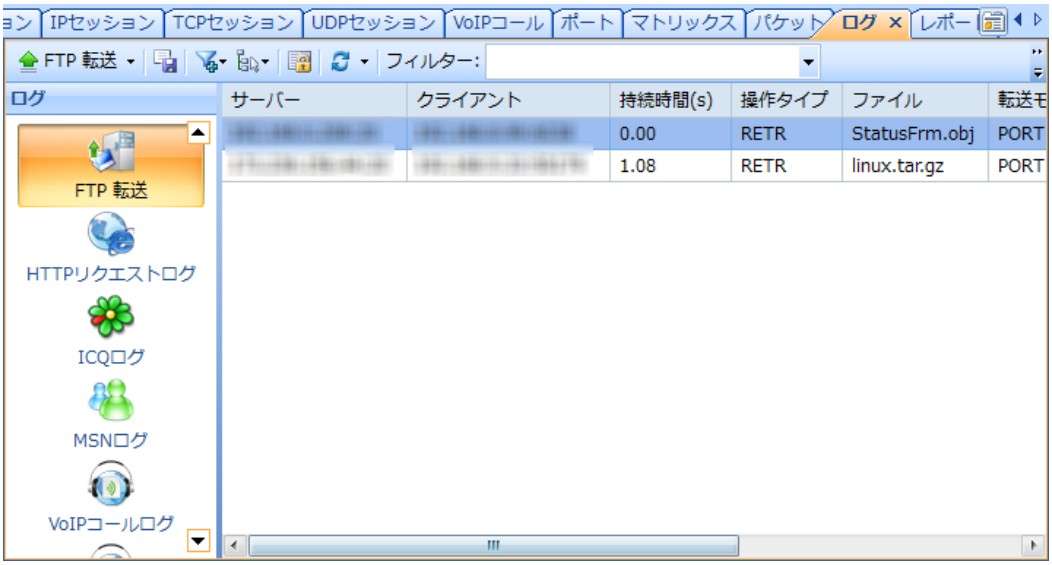
Email 情報は下図のように SMTP と POP3 プロトコルを利用して送受信したメールに関する情報を記録します。E メールログリストで任意アイテムをダブルクリックして、その E メールが開かれます。



E メール情報には**番号、日時、クライアント MAC アドレス、クライアント IP アドレス、クライアントポート、サーバーMAC アドレス、サーバーIP アドレス、サーバーポート、サーバー、クライアント、送信者、送信 E メールアドレス、受信者、受信 E メールアドレス、CC、タイトル、送信時間、E メールクライアント、アカウント、添付ファイル、ファイルサイズ（バイト）、持続時間（s）、平均スピード（B/S）**などのカラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。

FTP 転送

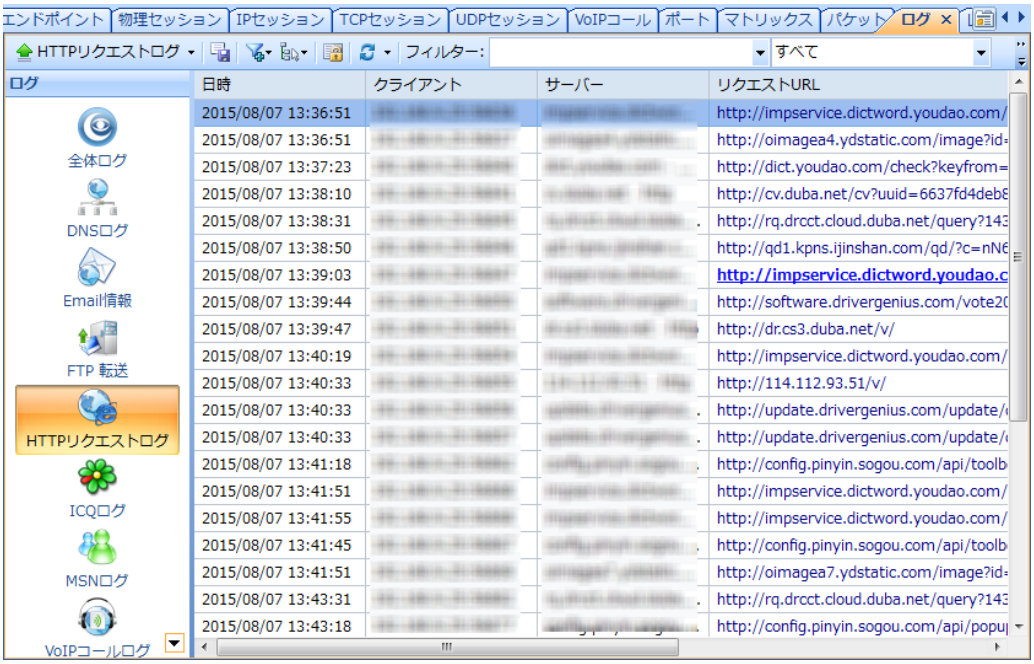
FTP 転送は FTP サーバーからのアップロードとダウンロードを記録します。



FTP 転送には、**日時、クライアント MAC アドレス、クライアント IP、クライアントポート、サーバーMAC アドレス、サーバーIP、サーバーポート、クライアント、転送開始時間、転送終了時間、持続時間（s）、アカウント、操作タイプ、ファイル、転送モード、合計バイト数、サーバーバイト数、クライアントバイト数、合計パケット数、サーバーパケット数、クライアントパケット数（B/S）、平均スピード（B/S）**などのカラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。

HTTP リクエストログ

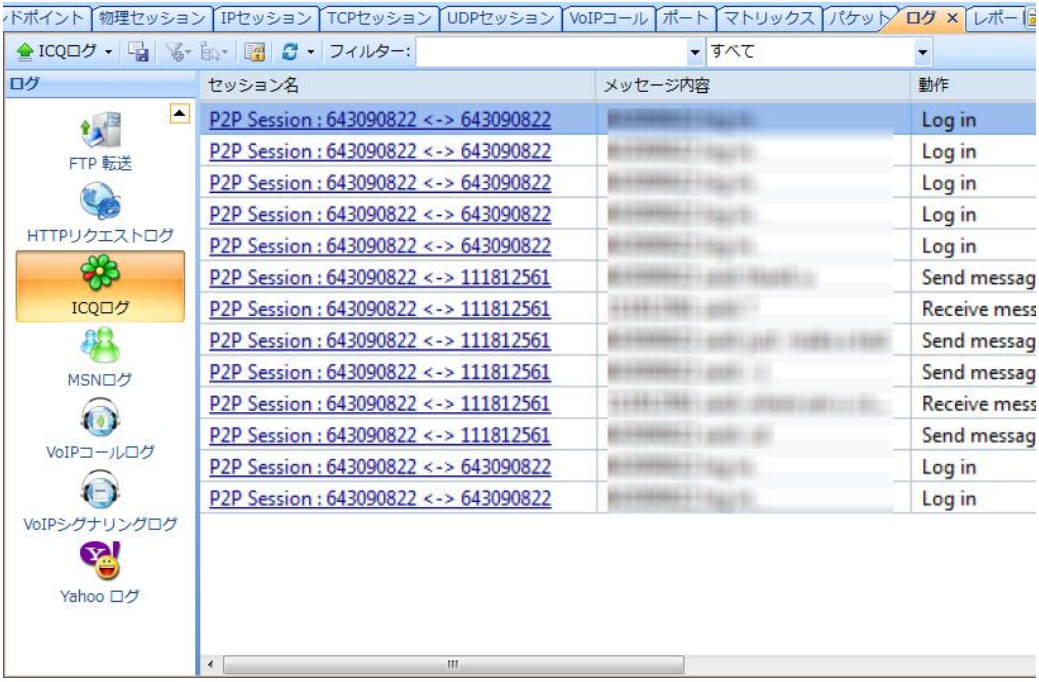
HTTP リクエストログは、すべてのウェブアクティビティを記録し、時間、クライアントとサーバーアドレス、リクエスト URL、コンテンツ長さ、コンテンツタイプを含むログ情報を提供します。



HTTP リクエストログには、**日時、クライアント MAC アドレス、クライアント IP アドレス、クライアントポート、サーバーMAC アドレス、サーバーIP アドレス、サーバーポート、クライアント、サーバー、リクエスト URL、方法、ユーザーエージェント、引用、コンテンツ長さ、コンテンツタイプ、アクセス認証、クライアント HTTP バージョン、持続時間、平均スピード（B/S）、ステータスコード、サーバー応答**などのクラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。

ICQ ログ

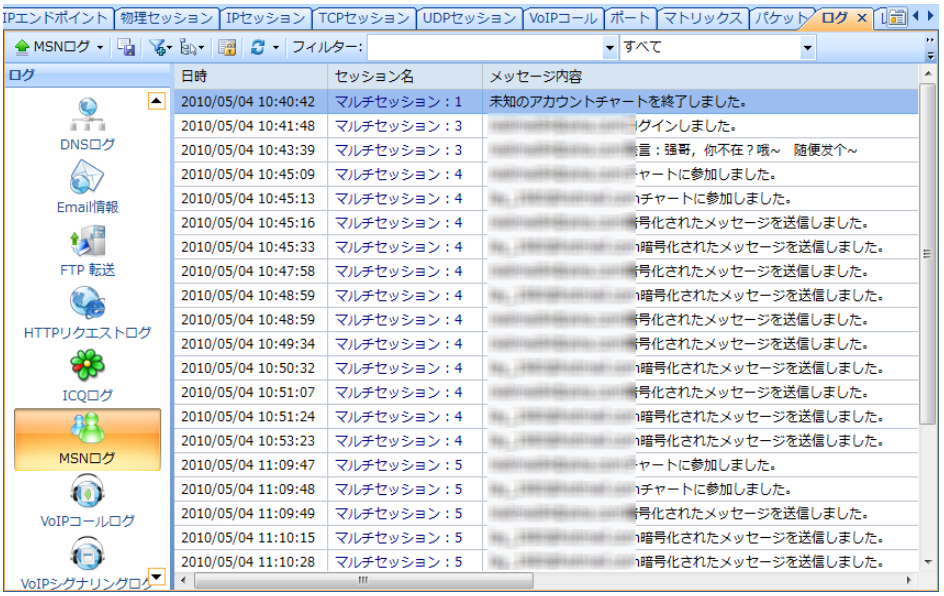
ICQ ログは自動的かつリアルタイムに ICQ セッションを記録します。後の処理及び解析のために、すべてのインターセプトされたメッセージをエクスポートすることができます。



ICQ ログには、**日時、クライアント MAC アドレス、クライアント IP アドレス、クライアントポート、サーバーMAC アドレス、サーバーIP アドレス、サーバーポート、セッション名、メッセージ内容、動作、送信アカウント、受信アカウント、IM タイプ**などのカラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。

MSN ログ

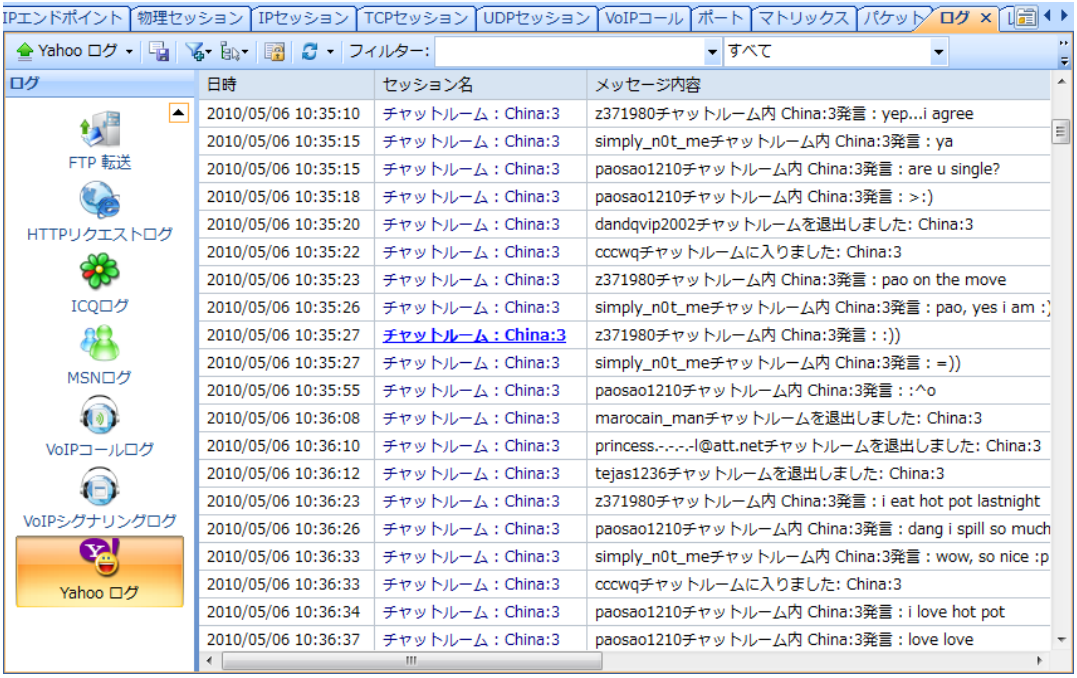
MSN ログは、通信日時、セッション名、メッセージ内容、動作、通信アカウントなどを含むネットワークにおける MSN 通信を記録します。プレーンテキストでメッセージを確認し、ステータスレコードをログイン、とログアウトすることができます。



MSN ログには、**日時、クライアント MAC アドレス、クライアント IP アドレス、クライアントポート、サーバーMAC アドレス、サーバーIP アドレス、サーバーポート、セッション名、メッセージ内容、動作、送信アカウント、受信アカウント、IM タイプ**などのカラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。

YAHOO ログ

YAHOO ログは、下図のように通信日時、セッション名、メッセージ内容、動作、通信アカウントなどを含むネットワークにおける YAHOO 通信を記録します。

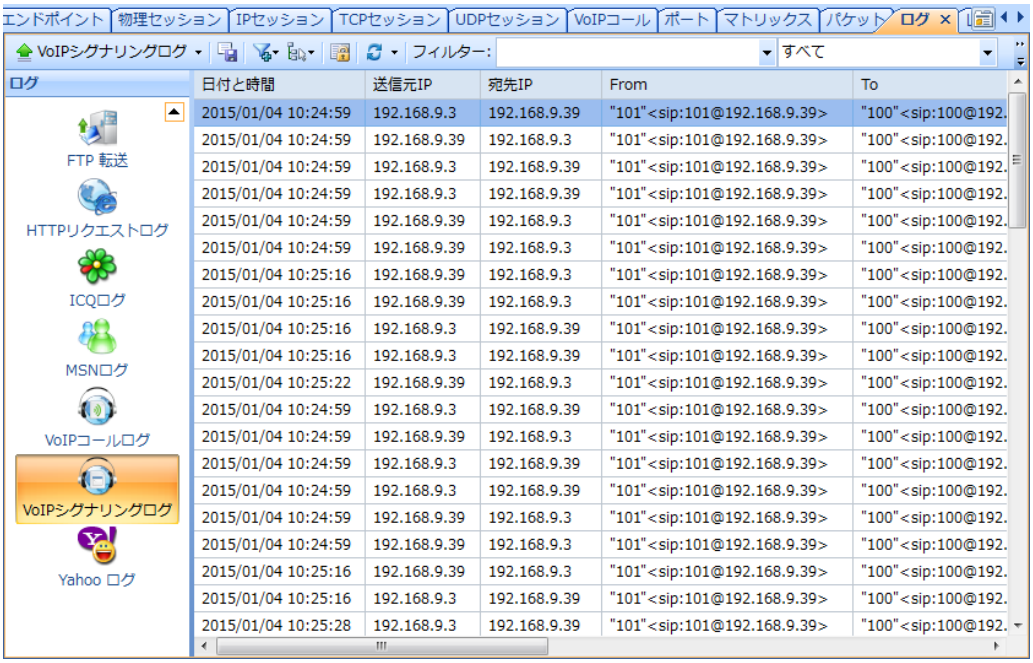


セッション名をクリックしたり、そのアイテムをダブルクリックしたりすることで、メモ帳でそのセッション名に関する詳細な通信を確認することができます。YAHOO ログには、**日時、クライアント MAC アドレス、クライアント IP アドレス、クライアントポート、サーバー MAC アドレス、サーバーIP アドレス、サーバーポート、セッション名、メッセージ内容、動作、送信アカウント、受信アカウント、IM タイプ**などのカラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。

VoIP シグナリングログ

VoIP シグナリングログは、VoIP コールの詳細情報を記録します。

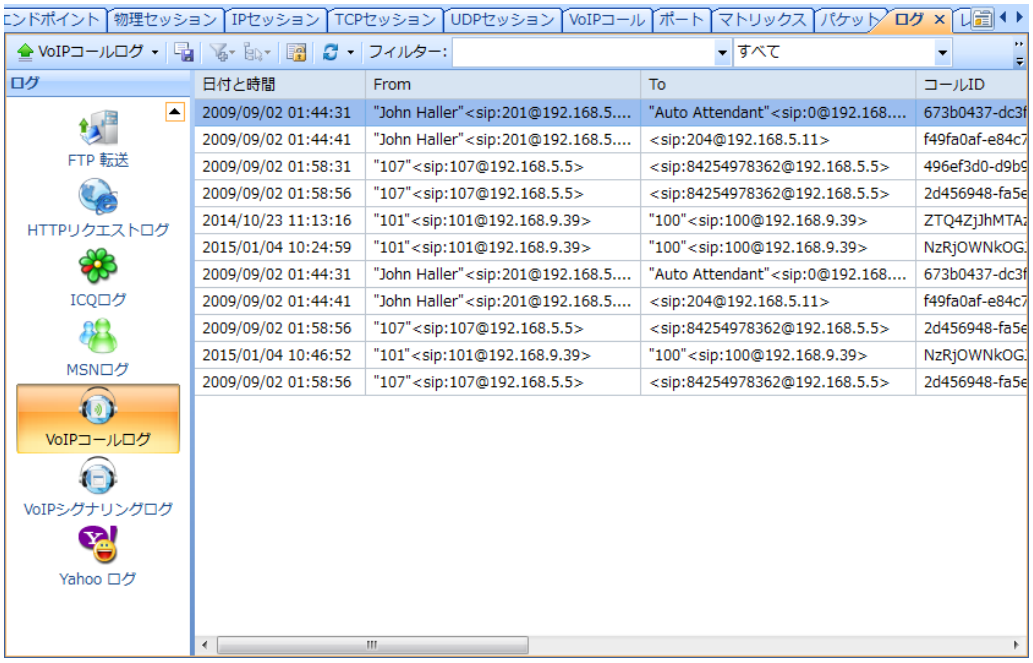
VoIP シグナリングログには、**日付と時間、送信元 IP、宛先 IP、From、 To、コール ID、概要、番号**などのカラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。



VoIP コールログ

VoIP コールログは VoIP コールを記録します。一つの VoIP コールは、一つの VoIP コールログとして記録されています。

VoIP コールログには、**日付と時間、From、 To、コール ID、シグナリング、MOS-A、MOS-V、サーバーレスポンス時間、コール時間、ステータス**などのカラムが含まれています。あるカラムを表示するには、カラムヘッダーを右クリックして、表示したいカラムを選択すればよいのです。



Capsa の設定について

全体設定

全体設定は、解析プロジェクトの設定を表し、以下の設定が含まれています。

- ネットワークプロファイル設定：デフォルトのネットワークプロファイル、ユーザー定義のネットワークプロファイル、ネットワークプロファイルにおける選択、全般設定、ノードグループ、ネームテーブル、およびアラーム設定が含まれています。
- 解析プロファイル設定：デフォルトの解析プロファイル、ユーザー定義の解析プロファイル、解析プロファイルの基本設定、解析オブジェクト、診断設定、ビュー表示、パケットバッファ、キャプチャーフィルター、パケット保存、ログビュー設定、ログ保存が含まれています。
- マイグラフ：デフォルトのマイグラフパネル、ユーザー定義のマイグラフパネル、およびパネルにおけるチャートが含まれています。
- マトリックス：デフォルトのマトリックスとユーザー定義のマトリックスが含まれています。
- レポート：デフォルトのレポートとユーザー定義のレポートが含まれています。

Capsa を利用してネットワークトラフィックをキャプチャーする前に、システムオプション、ネットワークプロファイル、解析プロファイルの設定などプログラムを設定することができます。解析プロジェクトを開始した後、アドレス表示設定、統計ビューにおけるカラムの設定、チャートとレポートにおける操作、および他の設定などを行うことができます。

上に触れたすべての設定は、Capsa に記憶されることができるので、プログラムを起動するとき、毎回設定を行う必要がありません。例えば、解析プロジェクトのために、**IP エンドポイント**ビューにおけるカラムの表示順序とカラムの幅を指定することができます。次回プログラムを起動するとき、**IP エンドポイント**ビューは、指定された表示順序と幅でカラムを表示します。

Capsa によって記憶され、毎回行う必要がない設定は以下の通りです。

- ネットワークアダプタにおける選択、ネットワークプロファイルにおける選択、及び解析プロファイルにおける選択
- 無線 AP のキー
- ネットワークプロファイルのすべての設定
- 解析プロファイルのすべての設定
- すべての統計ビューにおけるカラムの表示状態と幅
- すべてのマイグラフパネルとパネルにおけるすべてのチャート
- すべてのマトリックスとすべてのマトリックスの設定
- すべてのレポートとすべてのレポートの設定

- システムオプションのすべての設定
- アドレス表示の設定
- すべての統計ビューにおけるツールバーとポップアップメニューからの設定

注意 ネットワークアダプタにおける選択、ネットワークプロファイルにおける選択、及び解析プロファイルにおける選択は、解析プロジェクトに適用された場合にのみ、Capsa によって記憶されます。

全体設定のインポートとエクスポート

異なるマシンに同じ設定で Capsa を利用したい場合、またはオペレーティングシステムを再インストールした後、Capsa を設定する場合、この機能は非常に便利です。簡単にいくつかのクリックをして、以上の目的を達成することができます。

- **メニュー**ボタン  をクリックして、**全体設定のインポートとエクスポート**にマウスを移動し、**エクスポート**をクリックすることで、全体設定をローカルファイルにエクスポートすることができます。
- **メニュー**ボタン  をクリックして、**全体設定のインポートとエクスポート**にマウスを移動し、**インポート**をクリックすることで、バックアップされた全体設定をインポートすることができます。

バックアップされた設定がインポートされると、設定を有効にするために Capsa は自動的に再起動します。

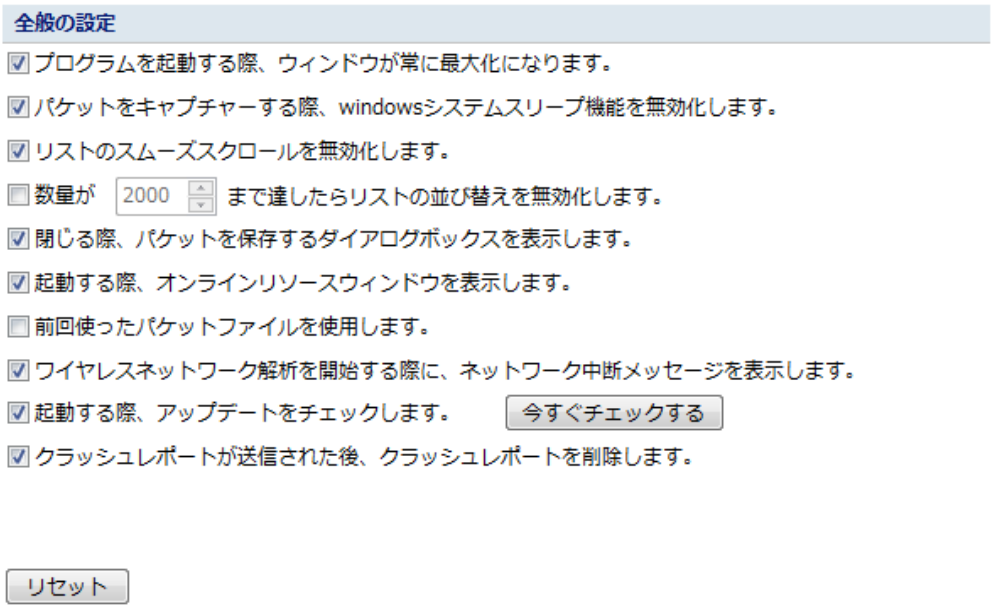
システムオプション

メニューボタン  をクリックして、メニューの右下で**システムオプション**をクリックすることで、**システムオプション**ダイアログボックスが開かれます。

システムオプションダイアログボックスには以下の六つのタブが含まれています。

- 全般
- デコーダー
- プロトコル
- タスクスケジューラ
- レポート
- フォーマット

全般



このタブには、九つのオプションが含まれています。

- **プログラムを起動する際、ウィンドウが常に最大化になります**:プログラムを起動する際、いつもプログラムウィンドウを最大化にします。
- **パケットをキャプチャーする際、windows システムスリープ昨日を無効かします**:お使いのシステムにおけるコントロールパネルの電源オプションスキーマが無視されます。Capsa のキャプチャーを停止していない場合、システムをスリープまたは休止状態にすることができません。
- **リストのスムーズスクロールを無効化します**:このオプションにチェックを入れると、インスタントスクロールが有効になります。
- **数量が＊＊まで達したらリストの並び替えを無効かします**:リストのアイテム数が制

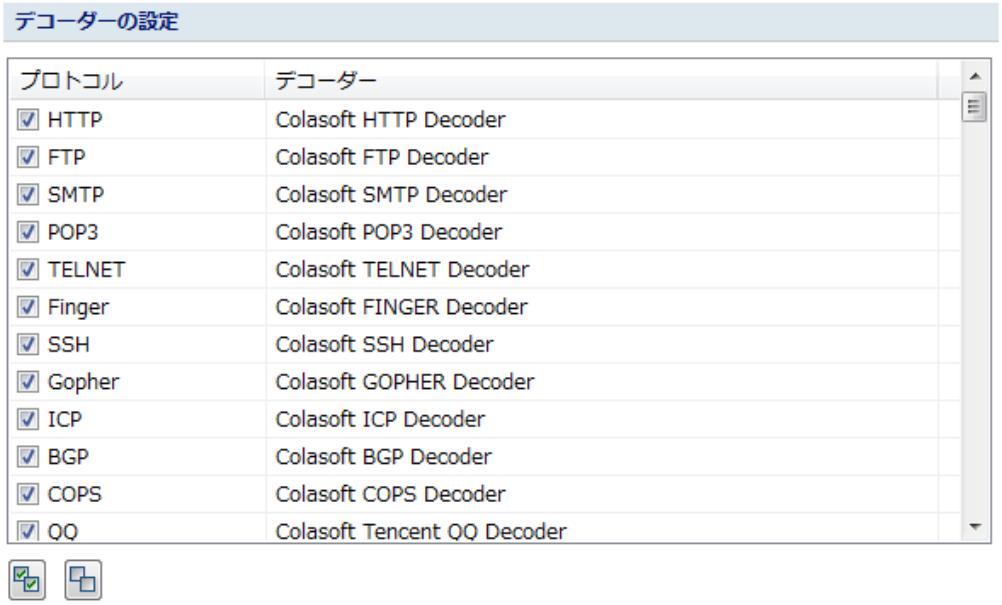
限に達したら、統計ビューにおけるカラムは、カラムヘッダーをクリックすることで自動的に並べ替えることができません。

- **閉じる際、パケットを保存するダイアログボックスを表示します**:プログラムを閉じる際、バッファにおけるパケットを保存するかどうかを確認するダイアログボックスがポップアップされます。
- **起動する際、オンラインリソースウィンドウを表示します**:プログラムを起動する際、**オンライリソース**ウィンドウはプログラムの右側に表示されます。
- **前回使ったパケットファイルを使用します**：リプレイ解析する際、前回リプレイされたパケットファイルを自動的にリプレイリストに追加するかどうかを選択します。
- **ワイヤレスネットワーク解析を開始する際に、ネットワーク中断メッセージを表示します**:ワイヤレスネットワークアダプタを使用してワイヤレス解析を開始している際、ワイヤレスネットワーク中断メッセージを表示します。このオプションは、Capsa Enterprise の場合にのみ、利用可能となります。
- **起動する際、アップデートをチェックします**: Capsa を起動する際、自動的に製品のアップデートをチェックします。**今すぐチェックする**をクリックして、すぐアップデートをチェックすることができます。
- **クラッシュレポートが送信された後、クラッシュレポートを削除します**:このオプションにチェックを入れると、クラッシュレポートが送信された後、クラッシュレポートファイルが削除されます。デフォルトでは、このオプションは有効にされています。

リセット:クリックして、このタブにおけるすべての設定をリセットします。

デコーダー

このタブは Capsa のすべてのデコーダーモジュールをリストします。すべてのデコーダーはチェックボックスによって有効または無効にすることができます。デフォルトでは、すべてのデコーダーは有効にされています。



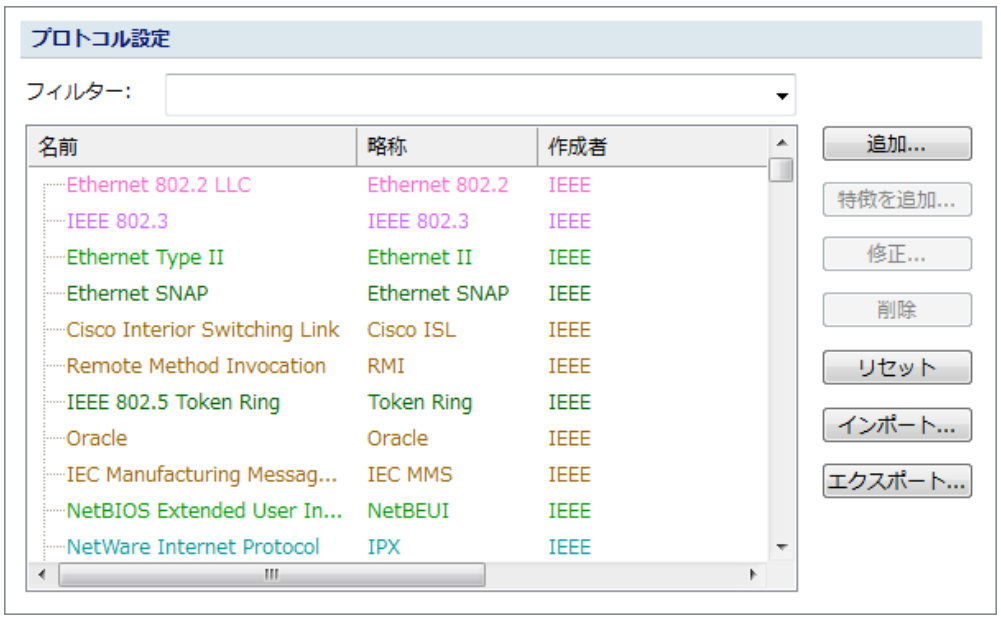
このタブには二つのボタンがあります。

 :すべてのデコーダーを有効にします。

 : すべてのデコーダーを無効にします。

プロトコル

このタブは、デフォルトプロトコルとユーザー定義のプロトコルを管理するために設けられたものです。



実行しているキャプチャーがある場合、プロトコルを変更したり、または新しいプロトコルを作成したりすることができません（すべてのキャプチャーを停止し、スタートページに移

動する必要があります）。キャプチャーを実行している場合、既存のプロトコルだけを確認することができます。

プロトコルリスト

プロトコルリストにおける任意アイテムをダブルクリックして、そのプロトコルを修正することができます。

表示フィルター

フィルターを利用して、関心のあるプロトコルを表示することができます。フィルターテキストボックスに適切なキーワードを入力することで、キーワードが含まれているプロトコルのみがリストに表示されます。

ボタン

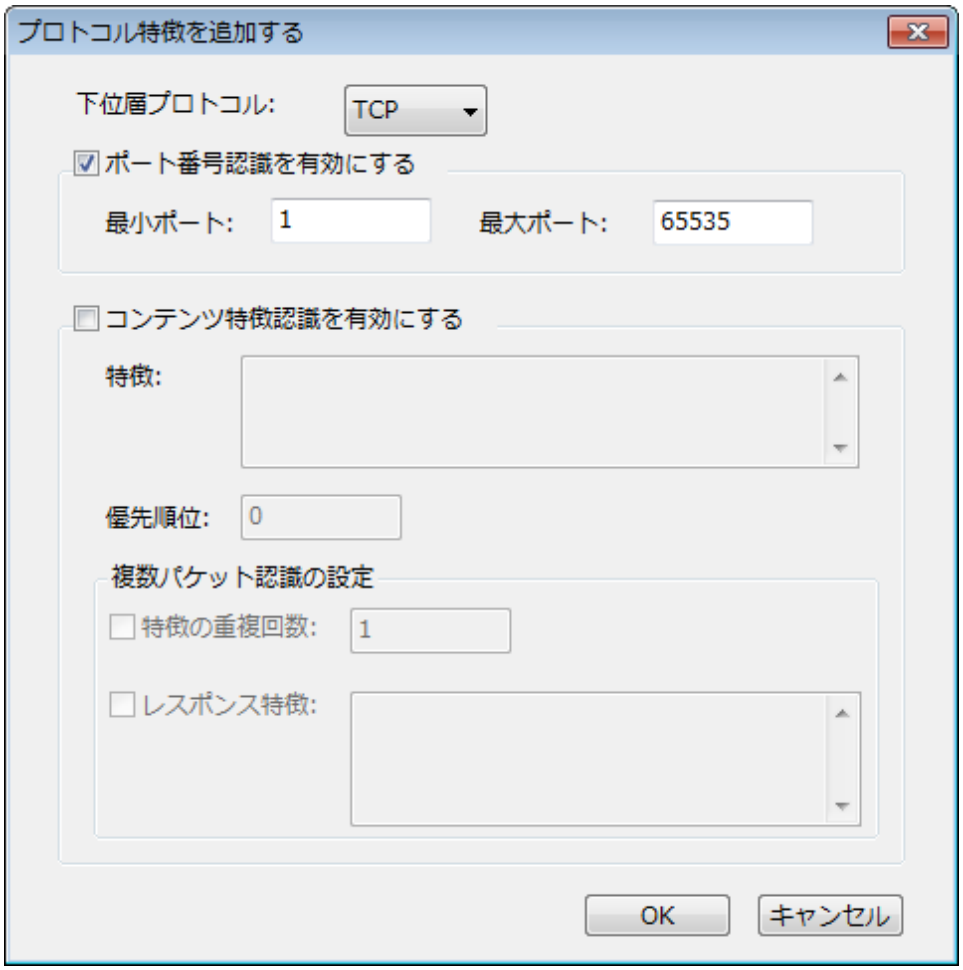
- **追加**:新しいプロトコルを作成します。
- **特徴を追加**:プロトコルを識別するために、ルールを作成します。
- **修正**:選択されたプロトコルを修正します。
- **削除**:選択されたプロトコルを削除します。
- **リセット**:すべてのビルトインプロトコルをリセットします。ユーザー定義のプロトコルは削除されます。
- **インポート**:保存された*.cscpro*ファイルからプロトコルをプロトコルリストにインポートします。
- **エクスポート**:プロトコルリストにおけるすべてのプロトコルを *.cscpro* ファイルにエクスポートします。

プロトコルを追加

プロトコルを追加するには、**追加**をクリックして、**プロトコルを追加**ダイアログボックスが開かれます。ここでプロトコル名、略称、作成者、説明、プロトコル番号、およびプロトコルの色を指定することができます。**プロトコル番号**は、システムによって自動的に生成されます。ユーザーはそれを修正することができます。

プロトコルを追加ダイアログボックスは以下のように表示されます。

プロトコルリストにおける新しく追加されたプロトコルを選択して、**特徴を追加**をクリックすることで、下図のように**プロトコル特徴を追加する**ダイアログボックスが表示されます。



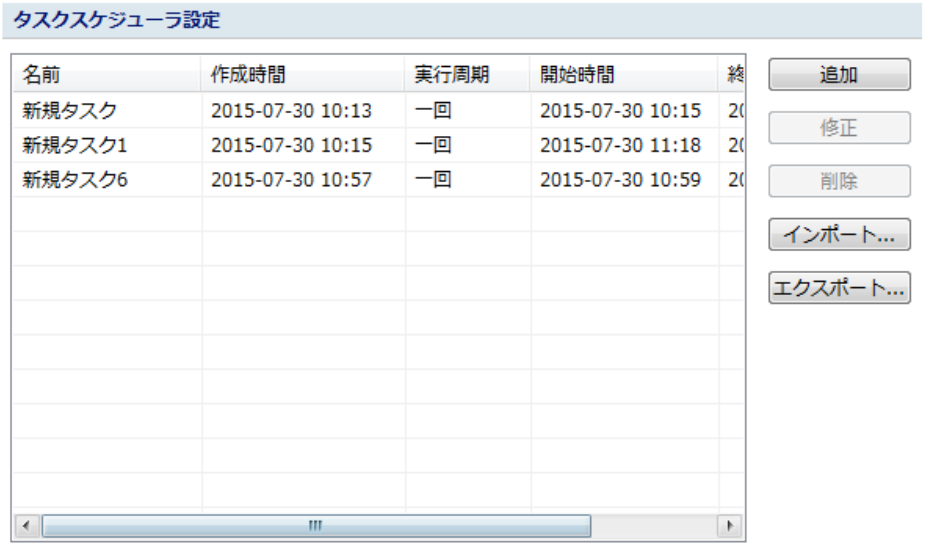
ダイアログボックスで詳細な特徴を設定します。プロトコル特徴には、ポート番号とコンテンツ特徴が含まれています。システムは、設定されたポート番号、あるいはコンテンツ特徴に基づいて、プロトコルを識別します。

タスクスケジューラ

特定の時間帯でネットワークパケットをキャプチャーしたい場合、解析プロジェクトをスケジュールする機能を利用することができます。プロジェクトのスケジュール機能を利用して、プログラムは特定の時間帯でパケットをキャプチャーするために、新しい解析プロジェクトを開始します。

プロジェクトをスケジュールするには、

1. **メニュー**ボタン  をクリックし、メニューの右下で**システムオプション**をクリックして、開かれるダイアログボックスで**タスクスケジューラ**タブをクリックします。



2. **追加**をクリックして、開かれたダイアログボックスでタスク名を入力し、プロジェクトの実行頻度を設定し、適切な解析プロファイル、ネットワークプロファイル、ネットワークアダプタを選択します。
3. **OK** をクリックして、**タスクスケジューラ設定**ダイアログボックスを閉じます。

タスクスケジューラタブは、スケジュールされたプロジェクトリストと五つのボタンから構成されています。プロジェクトリストには、名前、作成時間、実行周期、開始時間、終了時間という五つのカラムが含まれています。**名前**はプロジェクトタスクの名前で、**作成時間**はスケジュールプロジェクトが作成された時間で、**実行周期**はスケジュールされたプロジェクトの実行頻度で、**開始時間**はスケジュールされたプロジェクトの実行開始時間で、**終了時間**はスケジュールされたプロジェクトの実行終了時間です。

以下は**タスクスケジューラ**タブにおけるボタンについて説明しています。

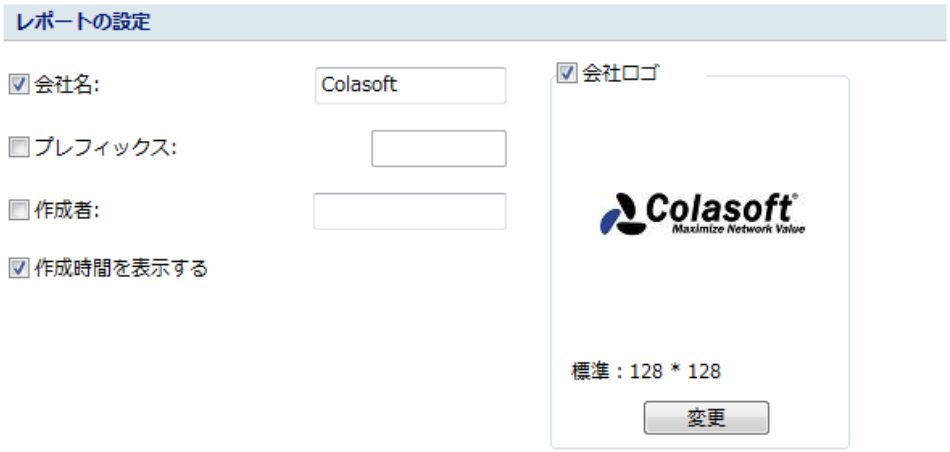
- **追加**:新しい解析プロジェクトをスケジュールします。
- **修正**:選択されたプロジェクトを修正します。
- **削除**:選択されたプロジェクトを削除します。
- **インポート**:保存されたスケジュールタスクをインポートします。インポートされるタスクの名前が既存タスクと同じ場合、既存タスクは上書きされます。
- **エクスポート**:リストにおけるすべてのプロジェクトタスクを.cscta ファイルにエクスポートします。

タスクスケジューラ設定ダイアログボックスは以下のように表示されます。

以下はこのダイアログボックスにおける各オプションについて説明しています。

- **タスク名**:スケジュールするプロジェクトタスクの名前です。デフォルトでは、**新規タスク**となります。
- **時間設定**:スケジュールプロジェクトタスクを実行する頻度を設定します。タスクを実行する頻度を一回、毎日、または毎週に設定することができます。設定された時間は、タスクを実行するコンピューターで設定されたタイムゾーンを基準としています。
- **一回**を選択した場合、タスクは設定された開始時間と終了時間の間で一回だけ実行されたます。
- **毎日**を選択した場合、タスクは設定された開始時間と終了時間の間で毎日実行されます。
- **毎週**を選択した場合、タスクは指定された曜日の時間帯で毎週実行されます。
- **解析設定**:スケジュールプロジェクトタスクの解析プロファイル、ネットワークプロファイル、ネットワークアダプタを選択します。

レポート



以下はレポートタブにおける各オプションについて説明しています。

- **会社名:** このオプション（デフォルトでは無効にされています）を有効にして、会社名を入力します。会社名はレポートの右上に表示されます。
- **プレフィックス:** このオプション（デフォルトでは無効にされています）を有効にして、すべてのレポートタイトル前に表示されるプレフィックスを入力します。
- **作成者:** このオプション（デフォルトでは無効にされています）を有効にして、レポートを作成する人の名前を入力します。作成者は、レポートの右下に表示されます。
- **作成時間を表示する:** このオプションが有効にされると、レポートが作成された時間はレポートの左上に表示されます。デフォルトでは、無効にされています。
- **会社ロゴ:** このオプション（デフォルトでは無効にされています）を有効にして、会社ロゴとして、イメージファイルを指定します。会社ロゴはレポートの右上に表示されます。

フォーマット

フォーマットタブは、小数点以下の桁数、バイト、ビット、毎秒バイトとビットを含め、データ表示のフォーマットを定義することができます。

以下はこのタブにおける各アイテムについて説明しています。

- **小数点以下の表示桁数:**値の小数点以下の表示桁数です。デフォルトでは 3 となり、1 から 6 まで入力することができます。
- **パーセンテージ小数点以下の表示桁数:**パーセンテージ値の小数点以下の表示桁数です。デフォルトでは 3 となり、1 から 6 まで入力することができます。
- **バイトのフォーマット:**デフォルトでは、プログラムは適切な単位、例えば B、KB、MB、 GB、または TB でパケットサイズとトラフィックを表示します。どの単位で表示するかは、パケットとトラフィックのサイズによります。表示単位を指定した場合、すべてのバイトは指定されたフォーマットで表示されます。
- **ビットのフォーマット:**デフォルトでは、プログラムは適切な単位、例えば b、 kb、Mb、Gb または Tb でパケットサイズとトラフィックを表示します。どの単位で表示するかは、パケットとトラフィックのサイズによります。表示単位を指定した場合、すべてのビットは指定されたフォーマットで表示されます。
- **バイト/秒のフォーマット:**毎秒バイトの単位で、Bps、KBps、 MBps、GBps、および TBps から選択することができます。それぞれ毎秒バイト数、毎秒キロバイト数、毎秒メガバイト数、毎秒ギガバイト数、および毎秒テラバイト数を表します。表示単位を指定した場合、すべての毎秒バイトの単位は指定されたフォーマットで表示されます。
- **ビット/秒のフォーマット:**毎秒ビットの単位で、bps、Kbps、 Mbps、Gbps、および Tbps から選択することができます。それぞれ毎秒ビット数、毎秒キロビット数、毎秒メガビット数、毎秒ギガビット数、および毎秒テラビット数を表します。表示単位を指定した場合、すべての毎秒ビットの単位は指定されたフォーマットで表示されます。
- **リセット**:このタブにおけるすべての設定をリセットします。

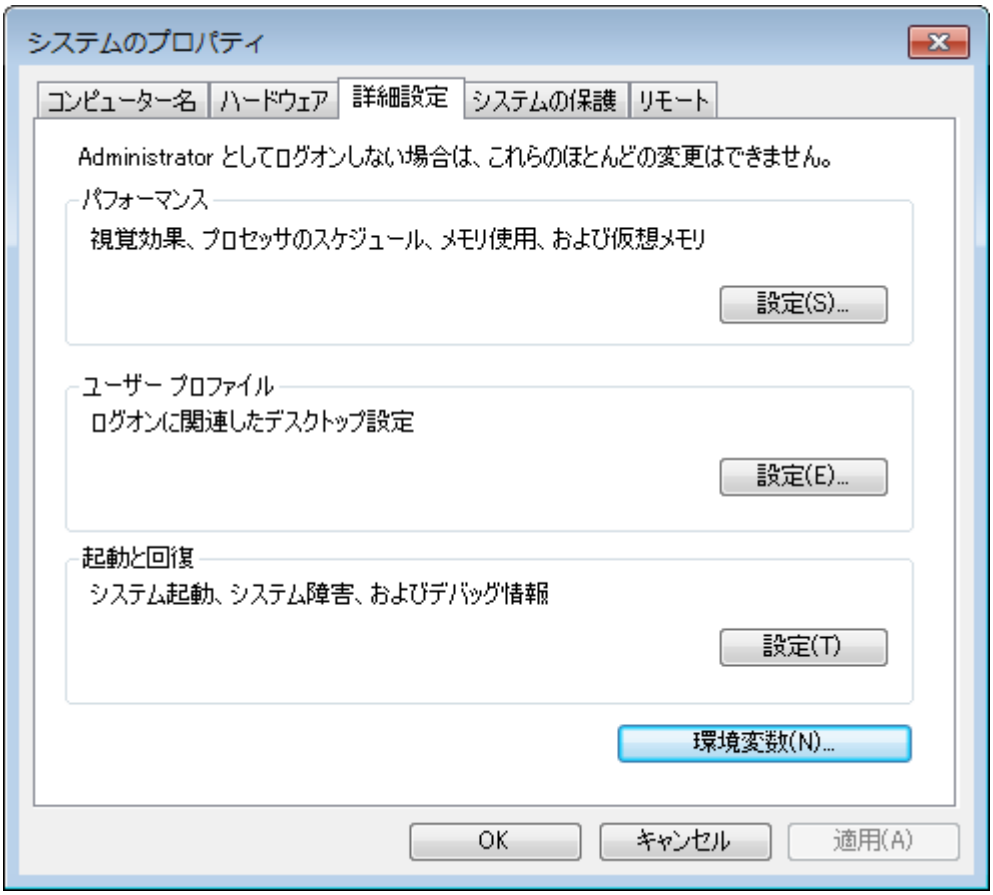
コマンドラインについて

Capsa はコマンドラインを提供します。ユーザーはコマンドラインを介して、リアルタイムに解析したり、パケットをリプレイしたりすることができます。

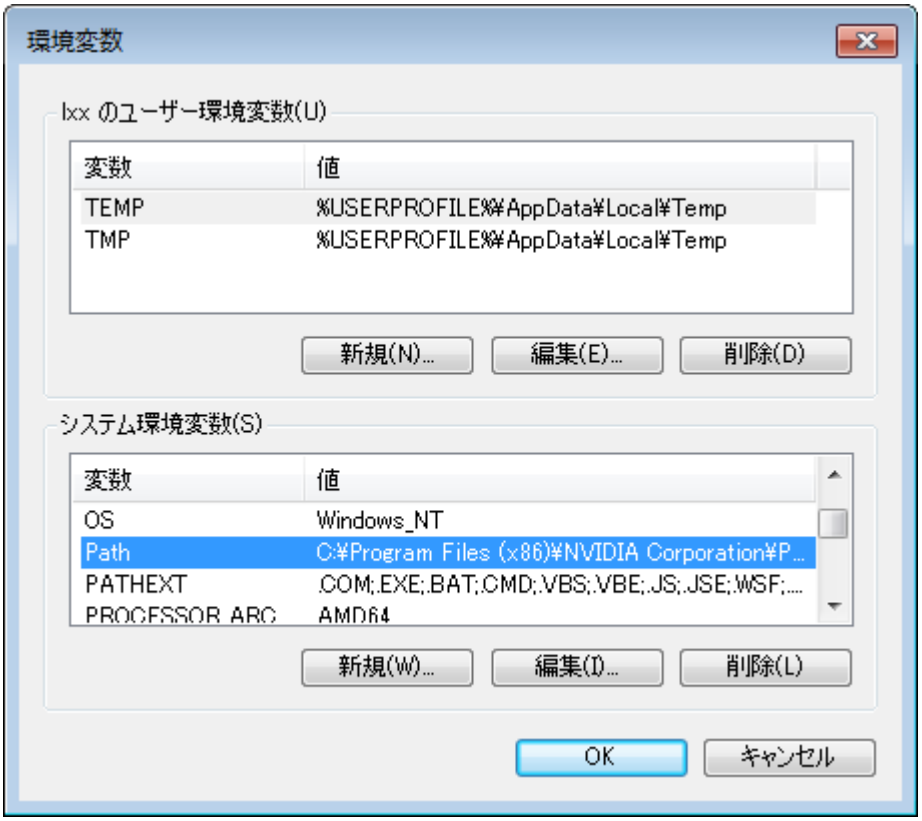
環境変数を設定

コマンドラインを利用する前に、環境変数の設定を行う必要があります。以下のステップに従い、cmdl.exe という名前のファイルのパスを環境変数に追加します（Windows 7 Ultimate を例とする）。

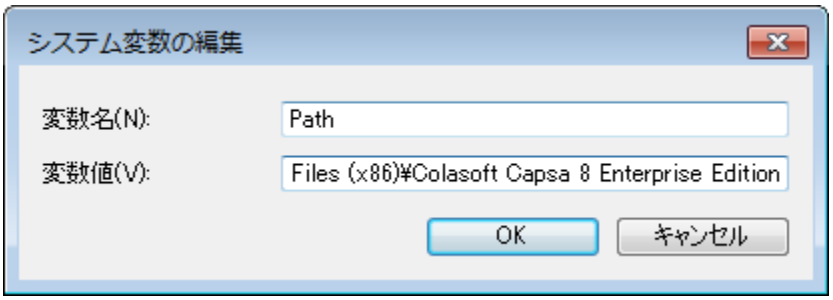
1. デスクトップにおける**コンピューター**を右クリックし、**プロパティ**をクリックすることで、**システム**というポップアップが開かれます。
2. **システム**というポップアップの左側で **システムの詳細設定** をクリックして、下図のように**システムのプロパティ**ダイアログボックスが開かれます。



3. **環境変数**をクリックして、下図のように**環境変数**ダイアログボックスが開かれます。



4. **システム環境変数**で、変数 Path を選択し、**編集**ボタンをクリックして、下図のようにシステム変数の編集ダイアログボックスが開かれます。

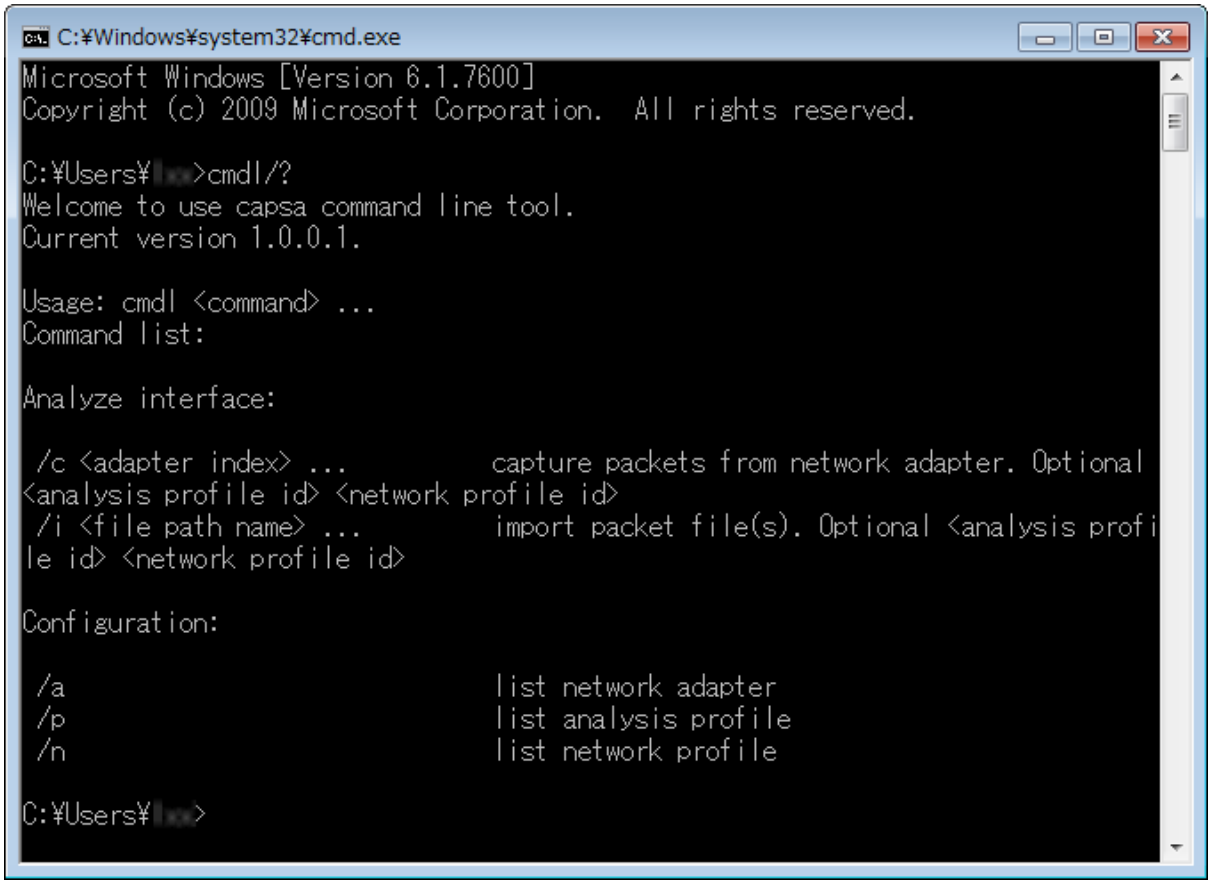


5. **変数値**に"cmdl.exe"という名前のファイルのパス、つまり Capsa のインストールディレクトリを入力します。セミコンで既存のパスと入力されたパスを区切る必要があります。
6. **OK** をクリックして、環境変数の設定を完了します。

環境変数設定を検証

環境変数を設定した後、以下のステップに従い、環境変数設定が成功したかどうかを検証する必要があります（Windows 7 Ultimate を例とする）。

1. **スタート** をクリックして、 **プログラムとファイルの検索** ボックスに"cmd"を入力し、Enter キーをクリックすることで、cmd ウィンドウが表示されます。
2. "cmdl /?"を入力して、Enter キーをクリックします。以下のようなコンテンツが表示される場合、環境変数設定が成功したことを表します。



3. 以上のようなコンテンツが表示されない場合、環境変数設定が正しいかどうかを確認してください。

パラメータについて

コマンドラインで使用されるパラメータについて説明します。

- /? コマンドのヘルプ情報を呼び出します。
- /c リアルタイムにパケットをキャプチャーする機能を有効にします。
- /i パケットをリプレイする機能を有効にします。
- /a システムで検出されたすべてのネットワークアダプタとアダプタの番号をリストします。
- /p システムにおけるすべての解析プロファイルとその番号をリストします。
- /n システムにおけるすべてのネットワークプロファイルとその番号をリストします。

使用例について

設定情報のクエリ

ネットワークアダプタをリスト

C:¥Users¥Administrator>cmdl /a

0. ローカルエリア接続

1. VMware Network Adapter VMnet1
2. VMware Network Adapter VMnet8

解析プロファイルをリスト

C:¥Users¥Administrator>cmdl /p

1. フル解析
2. セキュリティモニター
3. HTTP アプリケーション解析
4. E メールアプリケーション解析
5. DNS アプリケーション解析
6. FTP アプリケーション解析
7. IM アナリシス
8. VoIP 解析

ネットワークプロファイルをリスト

C:¥Users¥Administrator>cmdl /p

0. ネットワークプロファイル 1
1. ネットワークプロファイル 2
2. ネットワークプロファイル 3
3. ネットワークプロファイル 4

リアルタイム解析

ネットワークアダプタを割り当て、デフォルトのシステム設定を使用します。

C:¥Users¥Administrator>cmdl /c 0

ネットワークアダプタ、解析プロファイル、およびネットワークプロファイルを割り当てます。ネットワークアダプタの番号は 2 で、解析プロファイルの番号は 3 で、ネットワークプロファイルの番号は 0 です。

C:¥Users¥Administrator>cmdl /c 2 3 0

リプレイ解析

パケットファイルのパスを割り当て、デフォルトのシステム設定を使用します。

C:¥Users¥Administrator>cmdl /i E:¥

パケットファイルのパス、解析プロファイル、ネットワークプロファイルを割り当てます。パケットファイルのパスはディスク(E:)で、解析プロファイル番号は 1 で、ネットワークプロファイルの番号は 0 です。

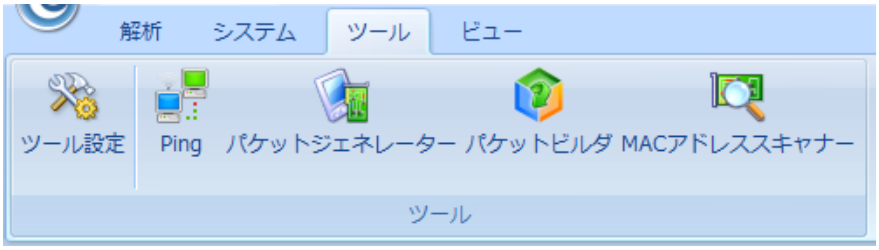
C:¥Users¥Administrator>cmdl /i E:¥ 1 0

ネットワークツール

便利にネットワークを管理するために、Capsa は四つのネットワークツールを提供します。

- ツール設定
- Colasoft Ping Tool
- Colasoft MAC Scanner
- Colasoft Packet Player
- Colasoft Packet Builder

ネットワークツールは、機能エリアのツールタブにあります。

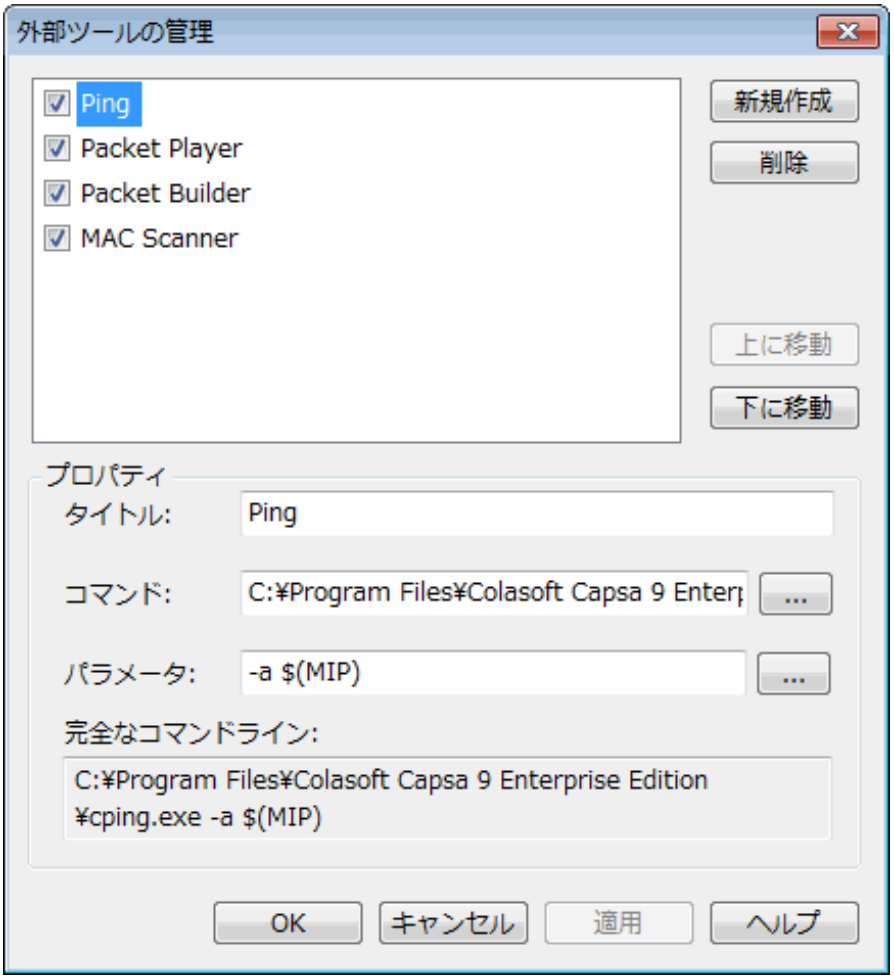


ツール設定

デフォルトで提供されている四つのツールの他に、ユーザーは**外部ツールの管理**ダイアログボックスで *Windows* アプリケーションとツールを Colasoft Capsa に追加することができます。Colasoft Capsa を通じて、追加されたアプリケーションを呼び出すだけでなく、実行することもできます。

外部ツールの管理ダイアログボックスを開くには、**機能エリア**における**ツール**タブの**ツール設定**をクリックします。

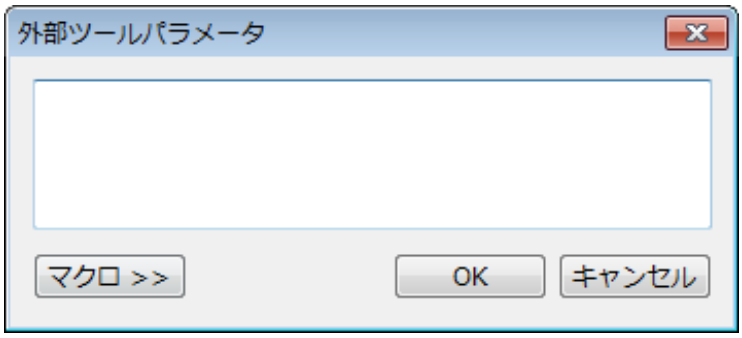
外部ツールの管理ダイアログボックスは以下のように表示されます。



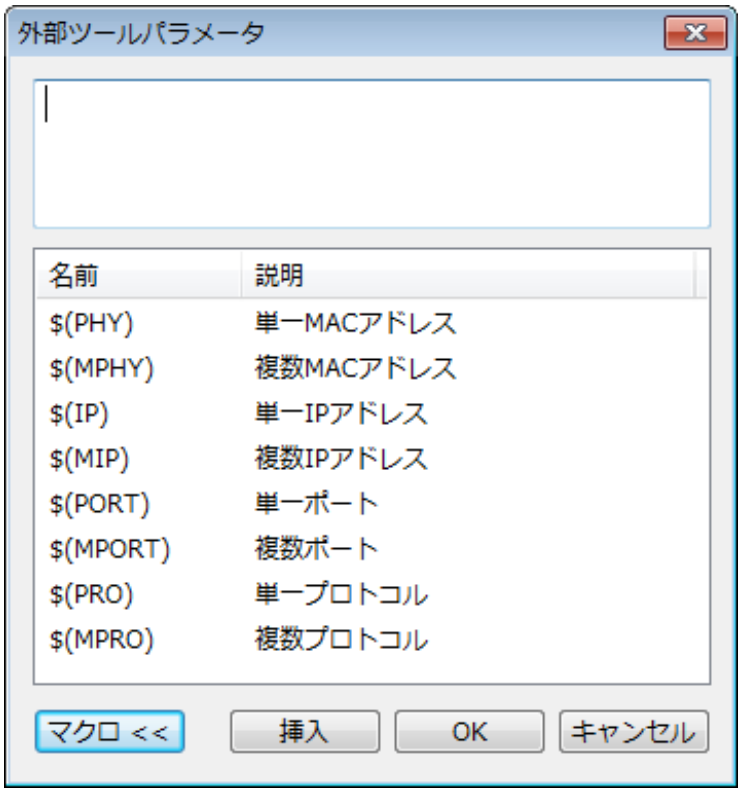
新規作成をクリックして新しいツールを追加したり、**削除**をクリックして左側パネルで選択されたツールを削除したりすることができます。**上に移動**と**下に移動**をクリックして、ツールの表示順序を変更することができいます。

実証するために、以下のステップに従い、Internet Explorer コマンドを Colasoft Capsa に追加することができます。

1. **新規作成**ボタンをクリックして、[New Tool 1]がツールリストに表示されます。
2. タイトルテキストボックスでツール名として、*Iinternet Explorer* を入力します。
3. コマンドでプログラムのパス C:¥Program Files (x86)¥Internet Explorer¥iexplore.exe を入力し、あるいは[...]をクリックしてパスを選択します。
4. パラメータテキストボックスの後にある[...]をクリックして、**外部ツールパラメータ**ダイアログボックスが開かれます。



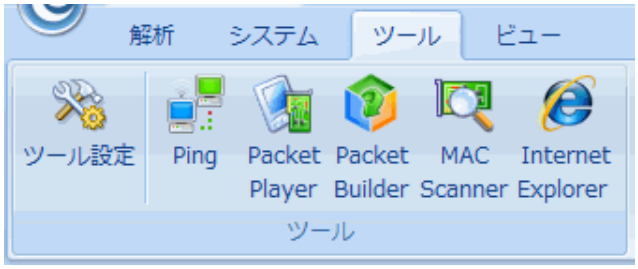
5. **マクロ >>ボタン**をクリックして、パラメータの詳細情報が表示されます。



Colasoft Capsa はパラメータ IP アドレス、MAC アドレス、ポート、およびプロトコルを表示される下側ウィンドウにリストします。パラメータの名前を選択して、挿入ボタンをクリックすることでパラメータを追加することができます。パラメータがリストされていない場合、上側ウィンドウで手動でパラメータを入力することができます。二つのパラメータ間は空白で区切る必要があります。

6. 適切なパラメータを選択し、**挿入**をクリックします。そして OK をクリックし、**外部ツールの管理**ダイアログボックスに戻ります。

追加が終わったら、Internet Explorer は**機能エリア**における**ツール**タブに表示されます。



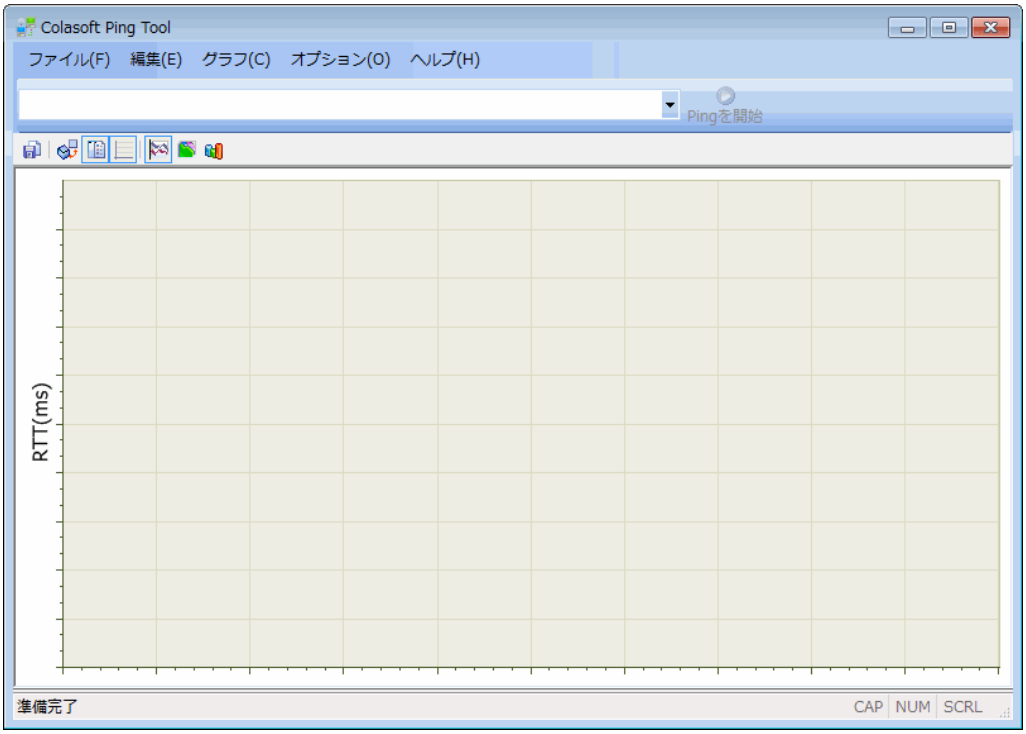
Colasoft Ping Tool

Colasoft Ping Tool は強力なグラフィック Ping ツールで、同時に複数の IP アドレスを Ping したり、グラフィックチャートでレスポンス時間を比較したりすることができます。

以下のいずれに従い、Colasoft Ping Tool を起動します。

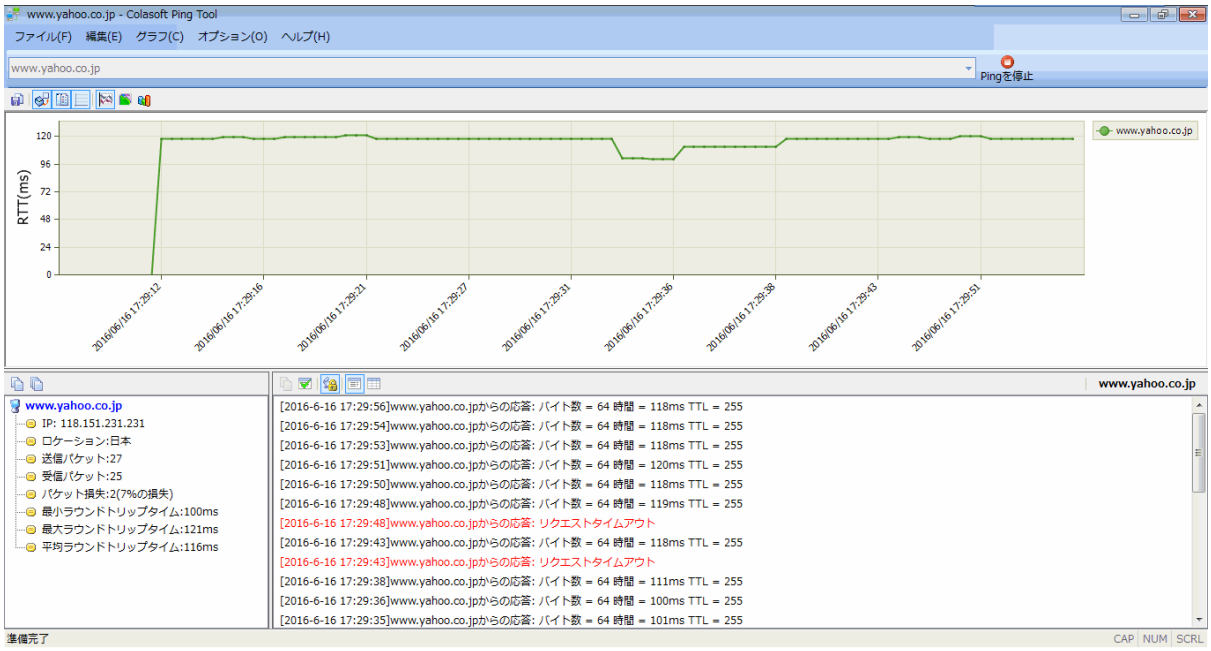
- **機能エリア**における**ツール**タブで **Ping** をクリックします。
- **スタート** > **すべてのプログラム**> **Colasoft Capsa 9** > **ネットワークツールセット** > **Ping Tool** をクリックします。
- **スタート**ボタンをクリックして、表示される**プログラムとファイルの検索**テキストボックスに″ *cping*″を入力し、「Enter」キーを押します。

Ping Tool ウィンドウは以下のように表示されます。

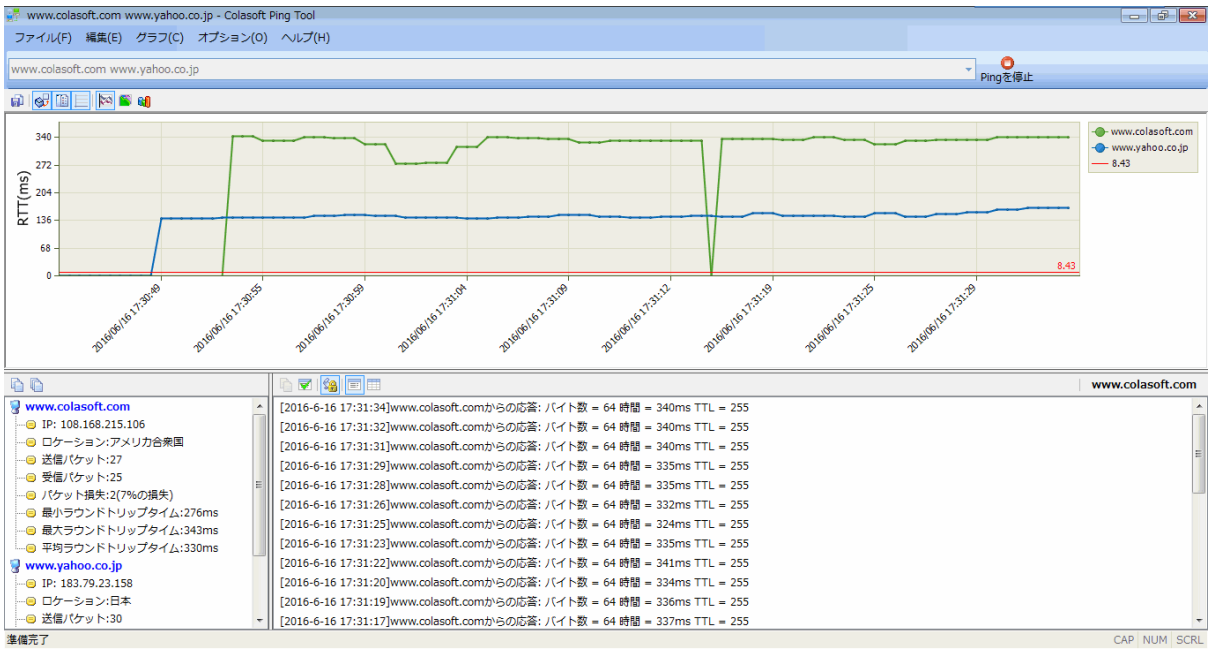


Colasoft Capsa を利用して、単一 IP アドレス（ドメイン名）だけでなく、複数 IP アドレス（ドメイン名）を Ping することができます。IP アドレスまたはドメイン名（複数の場合、カンマで区切ってください）を入力して、**Ping を開始**をクリックすることで、Ping を開始します。

単一ドメイン名を Ping する場合：



複数ドメイン名を Ping する場合：



デフォルトでは、**Ping を停止**をクリックして Ping を停止するまで、 Colasoft Ping Tool はずっとターゲットホストを Ping します。

Ping Tool を利用して、ユーザーは送信元 IP、宛先 IP を含め、Colasoft Capsa でキャプチャーされたパケットにおける IP アドレスを便利に Ping することができます。Ping Tool におけるチャートを*.bmp フォーマットファイルに保存することもできます。

Colasoft MAC Scanner

Colasoft MAC Scanner はローカルネットワークにおける IP アドレスと MAC アドレスをスキャンするために使用されているツールです。指定されたサブネットに ARP クエリを送信し、ARP レスポンスを聞き入れて、高速なスキャンで IP アドレスと MAC アドレスを取得します。より良い効率を得るために、スキャンスレッドの数を変更することもできます。

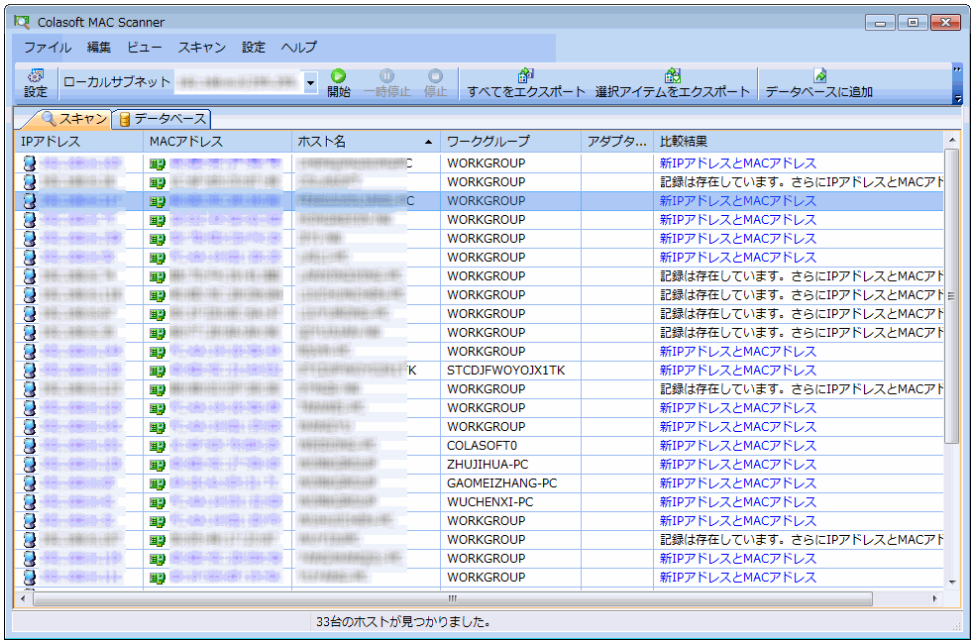
ここに二つの有用な機能があります。

- **データベース**:後で IP アドレスと MAC アドレスの比較のために、スキャン結果をデータベースに保存することができます。
- **ネームテーブルに追加**:直接 IP アドレス、MAC アドレス、または IP アドレスと MAC アドレス両方を**ネームテーブル**に追加することができます。

以下のいずれに従い、Colasoft MAC Scanner を起動します。

- **機能エリア**における**ツール**タブで **MAC Scanner** をクリックします。
- **スタート** > **すべてのプログラム**> **Colasoft Capsa 9** > **ネットワークツールセット** >**MAC Scanner** をクリックします。
- **スタート**ボタンをクリックして、表示される**プログラムとファイルの検索**テキストボックスに" *cmac* "を入力し、「Enter」キーを押します。

Colasoft MAC Scanner は以下のように表示されます。



Colasoft MAC Scanner は以下のコンポーネントが含まれています。

メニュー

ツールバーにおけるすべてのアイテム、ウィンドウを制御するコマンド、および**ヘルプ**が含まれています。

ツールバー

最も一般的に使用されるコマンドのショートカットが含まれています。

スキャンビュー

スキャンビューは、IP アドレス、MAC アドレス、ホスト名、ネットワークカードメーカーなどを含め、スキャン結果を表示します。MAC アドレスに複数の IP アドレスが割り当てられている場合、MAC アドレスに基づいてすべての IP アドレスをグループ分けします。スキャン結果は.*txt* ファイルにエクスポートすることができます。

データベースビュー

データベースビューはスキャン結果を保存することができます。後で他のスキャンを実行する場合、**スキャン**ビューは、データベースに保存された記録と比較して、スキャン結果を表示します。

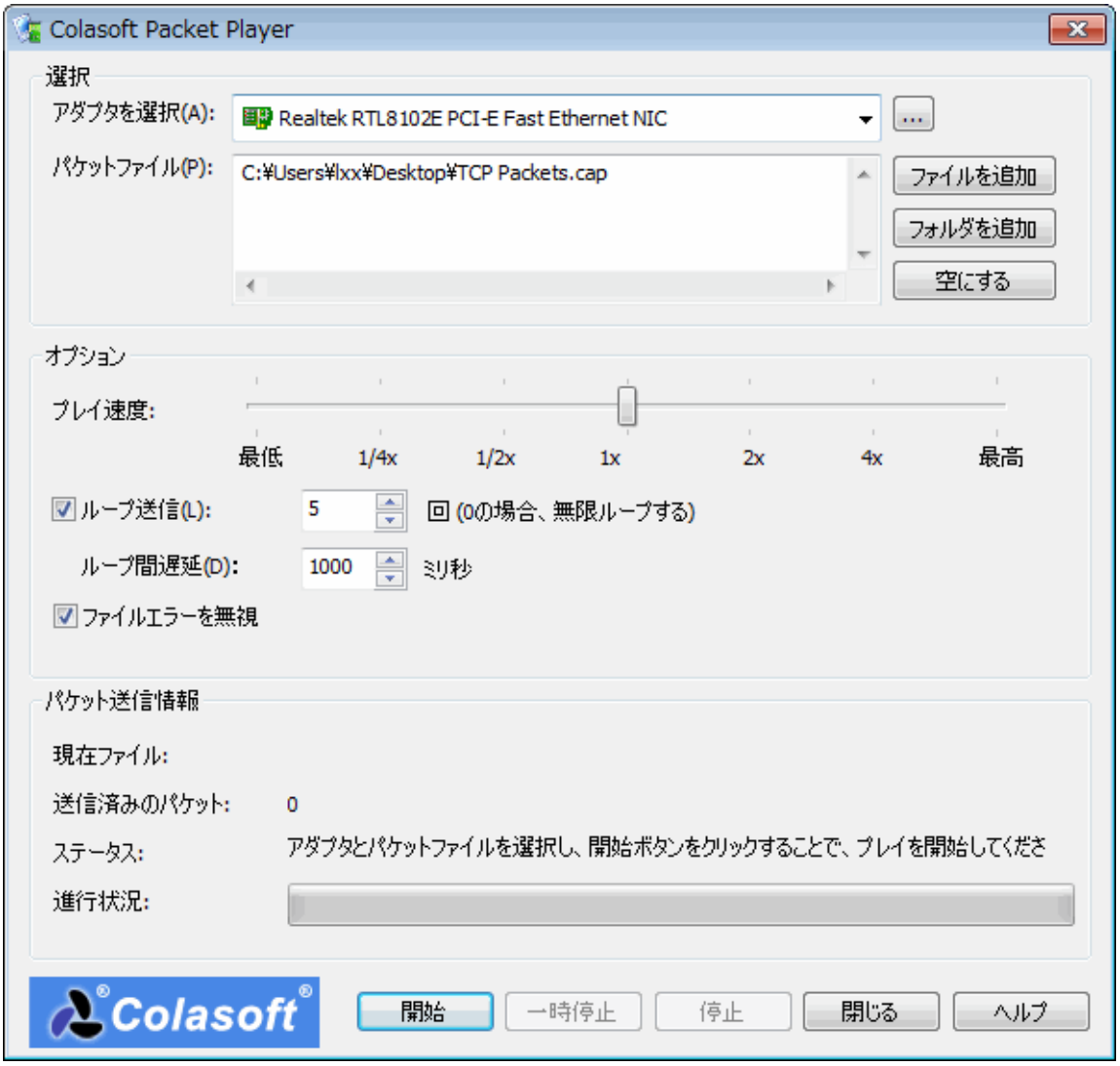
Colasoft Packet Player

Colasoft Packet Player はキャプチャーされたパケットファイルを開き、プレイすることができる再生ツールです。Colasoft Packet Player は Colasoft Capsa、 Wireshark、Network General Sniffer および WildPackets EtherPeek/OmniPeek など様々なスニファソフトウェア製品で作成されたパケットファイルフォーマットをサポートします。ループ送信機能もサポートします。

以下のいずれに従い、Colasoft Packet Player を起動します。

- **機能エリア**における**ツール**タブで **Packet Player** をクリックします。
- **スタート** > **すべてのプログラム**> **Colasoft Capsa 9** > **ネットワークツールセット** > **Packet Player** をクリックします。
- **スタート**ボタンをクリックして、表示される**プログラムとファイルの検索**テキストボックスに″ *pktplayer* ″を入力し、「Enter」キーを押します。

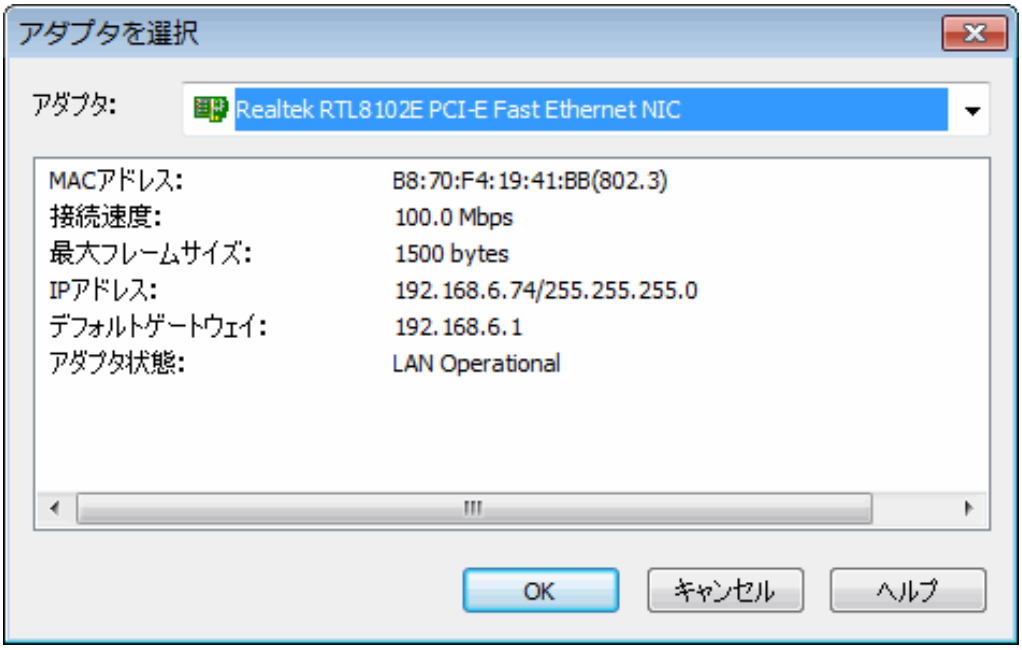
Colasoft Packet Player は以下のように表示されます。



Colasoft Packet Player には以下のアイテムが含まれています。

ネットワークカード

パケットを送信するために、ネットワークカードを一つ選択する必要があります。デフォルトでは、選択されていません。[...]をクリックして、開かれた**アダプタを選択**ダイアログボックスにおけるコンボボックスからアダプタを選択します。コンボボックスの下で選択されたアダプタの詳細情報が表示されます。



パケットファイル

送信したいパケットを選択します。Colasoft Packet Player がサポートしているファイルフォーマットは以下の通りです。**ファイルを追加**、または**フォルダを追加**をクリックして、複数ファイルを追加することができます。コンボボックスから以前送信されたパケットファイルをリプレイすることもできます。

- Colasoft Capsa 5.0 Packet File (*.cscpkt)
- Colasoft Capsa 5.0 Raw Packet File (*.rawpkt)
- Colasoft Capsa 7.0 Packet File (*.cscpkt)
- Accellnt 5Views Packet File (*.5vw)
- EthePeek Packet File(V7) (*.pkt)
- EthePeek Packet File(V9) (*.pkt)
- HP Uinx Nettl Packet File (*.TRC0;TRC1)
- libpcap(tcpdump,Ethereal,etc.) (*.cap)
- Microsoft Network Mintor2.x (*.cap)
- Novell LANalyer (*.tr1)
- Network Instuments Observer V9.0 (*.bfr)
- NetXRay2.0 and WINDWS Sniffer (*.cap)
- Sun_Snoop (*.snoop)
- Visual Network Traffic Capture (*.cap)

アドバイス **空にする**ボタンをクリックして、パケットファイルリストにおけるすべてのアイテムを削除することができます。リストにおけるあるアイテムを削除したい場合、そのアイテムを選択し、**Delete** キーを押せばよいのです。

ループ送信

送信を実行する回数を定義します。デフォルトでは一回となります。一時停止、または閉じるまでずっとパケットを送信したい場合、0 を入力してください。

ループ間遅延:ループ回数が一回以上定義される場合、ループ間の間隔を設定する必要があります。デフォルトでは、Colasoft Packet Player は無間隔でパケットを循環送信します。

ファイルエラーを無視

このオプションにチェックを入れると、 Packet Player はパケットファイルにおけるファイルエラーをスキップして、再生を続けます。

現在ファイル

ファイルのパスを表示します。

送信済みのパケット

成功に送信されたパケットの数を表示します。送信できなかったパケットがある場合でも、Colasoft Packet Player は成功に送信されたパケットの数を表示します。

ステータス

操作のヘントまたは状態を表示します。

進行状況

プロセスバーは実行している送信の現時点の進度を表示します。

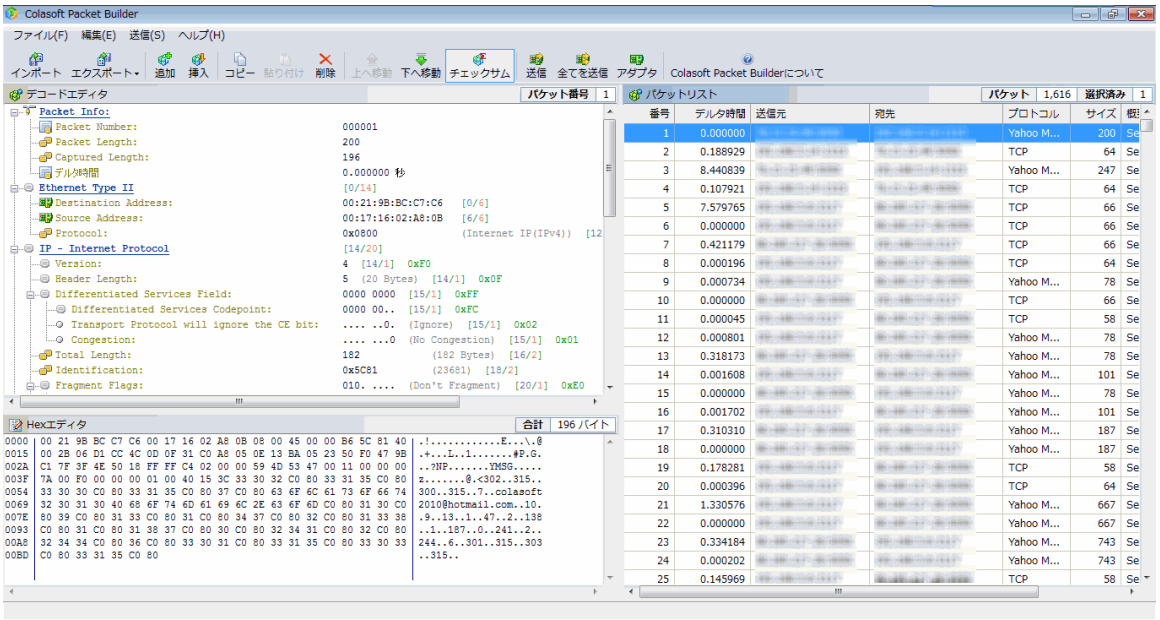
Colasoft Packet Builder

Colasoft Packet Builder は、カスタムネットワークパケットを作成する便利なツールです。このツールを利用して、ネットワーク攻撃と侵入に対する防御能力をチェックすることができます。Colasoft Packet Builder は強力な編集機能を持って、普通の Hex 生データの編集の他に、デコードエディタを搭載し、簡単に特定プロトコルフィールドの値を編集することができます。パケットを作成するほかに、Colasoft Packet Builder では、パケットをパケットファイルに保存したり、パケットをネットワークに送信したりすることができます。

以下のいずれに従い、Colasoft Packet Builder を起動します。

- **機能エリア**における**ツール**タブで **Packet Builder** をクリックします。
- **スタート** > **すべてのプログラム**> **Colasoft Capsa 9** > **ネットワークツールセット** > **Packet Builder** をクリックします。
- **スタート**ボタンをクリックして、表示される**プログラムとファイルの検索**テキスト

ボックスに”*pktbuilder*”を入力し、「Enter」キーを押します。
Colasoft Packet Builder ウィンドウは以下のように表示されます。



Colasoft Packet Builder のメインビューは、三つのパネルからなっています。

- パケットリスト
- デコードエディタ
- Hex エディタ

後の二つのパネルはパケットリストパネルと協力し合います。パケットリストでパケットを選択すると、デコードエディタと Hex エディタはそのパケットをデコードします。ユーザーはこの二つのパネルでパケットを編集することができます。

メインビューにおける三つのパネルのレイアウトを変更するには、パネルヘッダーをドラッグして移動すればよいのです。

Colasoft Packet Builder を利用して、

新しいパケットを追加、または挿入

Colasoft Capsa のパケットタブからパケットを追加、または挿入し、パケットテンプレート（ARP、IP、TCP、および UDP）を追加、挿入することができます。

パケットを編集

デコードエディタパネルと Hex エディタパネルで編集したいアイテムと数字をクリックして、編集すればよいのです。

パケットを送信

ツールバーにおける**送信**、または**すべてを送信**ボタンをクリックして、作成されたパネットをネットワークに送信します。

ヒント 作成されたパケットをディスクに保存することも重要です。エクスポートをクリックして、選択したパケットまたは全てのパケットをディスクに保存することができます。

付録

FAQ

Q: Capsa を利用して何ができますか。

A: Capsa は多くの機能を備えています。

ネットワーク管理者:ネットワーク障害の診断、感染したウィルスの検出、ネットワークトラフィックの監視、ネットワークプロトコルの解析、およびネットワークの脆弱性の検出を行います。

会社 IT 管理者:ネットワーク全体の健康状態とインフラ健康状態をモニターし、統計情報とレポートを確認します。

セキュリティマネージャ:ネットワークアクティビティを監視し、フォレンジック解析で会社セキュリティポリシーに違反していることを検出します。

コンサルタント:ネットワークトラブルを解析し、顧客のためにネットワーク問題を解決して、ネットワーク機能を最適化します。

ネットワークアプリケーション開発者:ネットワークアプリケーションのデバッグ、プログラム性能の最適化、送受信したコンテンツのテスト、およびネットワークプロトコルの調査を行います。

Q:自分自身のためにトラフィックフィルターを設定できますか。

A:はい、できます。Capsa では興味を持っているトラフィックをキャプチャーするために、一連のフィルタールールを設定することができます。フィルターは本当に興味を持っているものに集中させ、パケットの解析と表示をスピードアップします。Capsa はグローバルフィルターとプロジェクトフィルターという二つのフィルターがあります。グローバルフィルターは一般的に使用されるプロトコルフィルターで、現在のプロジェクトに適用することができます。プロジェクトフィルターは現在のプロジェクトにだけ適用されます。

Q: Capsa はネットワークにおけるトラフィック利用率を監視できますか。

A:はい、できます。Capsa は全体ネットワーク、または各ネットワークセグメントの詳細な統計情報、トラフィック利用状況、トップトーカー、ネットワークのビジー状態、MAC/IP アドレスまたはプロトコル、ビット率、および TCP トランザクションなどの統計を提供します。

Q: LAN がハブに接続しているのに、私のマシンのトラフィックだけを検出します。

A:一般的には、NIC がプロミスキャスモードをサポートしている場合、Capsa はうまく機能することができます。考えられる原因の一つは、お使いのデバイスがハブ（例えば、Linksys hubs）と名付けていますが、実際のところスイッチとして機能しているということです。もう一つの原因は、マルチスピードハブを使っているので、お使いの NIC のスピードと異なるスピードで動作するステーションからのトラフィックを見ることができないということです（例えば、10M NIC を使っている場合、100M NIC によって生成されたトラフィックを見ることができません）。

Q:どのようにポートミラーリングを設定するのですか。

A:ポートミラーリングを設定する方法を学習するために、スイッチのマニュアルを読んだり、スイッチのウェブサイトを訪問したりすることができます。または、技術者に助けを求めることも一つの手段でしょう。

Q: Colasoft Capsa を利用して、ラジオを聴いたり、音楽をオンラインでダウンロードしたりする人を確認できますか。

A:はい、できます。メディアプロトコルの標準ポートは RTSP ポート 554、PNM ポート 7070（PNA ポートとも知られている）、MMS ポート 1755 です。**簡易フィルター**におけるポートルールを設定することで、簡単にメディアリソースを訪問している人を見つけることができます。上級フィルターで HTTP 解析の URL フィルターを設定することで、メディアファイル（例えば、.rm）のダウンロードを監視することができます。

Q:マイグラフビューが時には表示されないのはなぜですか。

A:ノードブラウザでルートノードを選択した場合にのみマイグラフビューが表示されます。マイグラフビューはノードブラウザにおける任意の特定ノードに属していないグローバルノードだからです。ノードブラウザでノードが選択された場合、選択されたノートと関連しているビューだけ表示されます。

Q:シリアル番号とライセンスキーを入力したのに、機能しませんでした。

A:弊社からのシリアル番号とライセンスキーをコピーし、貼り付ける場合、不必要な空白があるかどうかを確認してください。シリアル番号とライセンスキーを入力する場合、入力エラーがあるかどうかを確認してください。

フリーエディションユーザーの場合、ライセンス申請をクリックして、シリアル番号を申請する必要があります。シリアル番号はすぐお使いのメールボックスに送付されます。

Q:キャプチャーされたパケット、ログ、レポート、およびチャートを異なるフォーマットでエクスポートすることができますか。

A:はい、できます。Capsa を利用して、パケットを複数のフォーマットでエクスポートしたり、ログ、レポート、およびチャートを複数のファイルフォーマットとイメージフォーマットにエクスポートしたりすることができます。詳しいことは、関連部分を確認してください。

Q: Capsa は RADIUS プロトコルをサポートしますか。

A:はい、Capsa は RADIUS パケットをキャプチャー、解析することができます。

弊社は弊社ウェブサイトでより多くの FAQ を更新します。詳しいことは弊社ウェブサイト http://www.colasoft.com/jp/をご覧ください。

イーサネットタイプコード

Ethernet		Exp. Ethernet		Description
decimal	Hex	decimal	octal	
0000	0000-05DC			IEEE802.3LengthField
0257	0101-01FF	-	-	Experimental
0512	0200	512	1000	XEROX PUP (see 0A00)
0513	0201	-	-	PUP Addr Trans (see 0A01)
	0400	-	-	Nixdorf
1536	0600	1536	3000	XEROX NS IDP
	0660	-	-	DLOG
	0661	-	-	DLOG
2048	0800	513	1001	Internet IP (IPv4)
2049	0801	-	-	X.75 Internet
2050	0802	-	-	NBS Internet
2051	0803	-	-	ECMA Internet
2052	0804	-	-	Chaosnet
2053	0805	-	-	X.25 Level 3
2054	0806	-	-	ARP
2055	0807	-	-	XNS Compatability
2056	0808	-	-	Frame Relay ARP
2076	081C	-	-	Symbolics Private
2184	0888-088A	-	-	Xyplex
2304	0900	-	-	Ungermann-Bass net debugr
2560	0A00	-	-	Xerox IEEE802.3 PUP
2561	0A01	-	-	PUP Addr Trans
2989	0BAD	-	-	Banyan VINES
2990	0BAE	-	-	VINES Loopback
2991	0BAF	-	-	VINES Echo
4096	1000	-	-	Berkeley Trailer nego
4097	1001-100F	-	-	Berkeley Trailer encap/IP
5632	1600	-	-	Valid Systems
16962	4242	-	-	PCS Basic Block Protocol
21000	5208	-	-	BBN Simnet
24576	6000	-	-	DEC Unassigned (Exp.)
24577	6001	-	-	DEC MOP Dump/Load
24578	6002	-	-	DEC MOP Remote Console
24579	6003	-	-	DEC DECNET Phase IV Route
24580	6004	-	-	DEC LAT
24581	6005	-	-	DEC Diagnostic Protocol
24582	6006	-	-	DEC Customer Protocol
24583	6007	-	-	DEC LAVC, SCA
24584	6008-6009	-	-	DEC Unassigned
24586	6010-6014	-	-	3Com Corporation
25944	6558	-	-	Trans Ether Bridging
25945	6559	-	-	Raw Frame Relay
28672	7000	-	-	Ungermann-Bass download
28674	7002	-	-	Ungermann-Bass dia/loop

28704	7020-7029	-	-	LRT
28720	7030	-	-	Proteon
28724	7034	-	-	Cabletron
32771	8003	-	-	Cronus VLN
32772	8004	-	-	Cronus Direct
32773	8005	-	-	HP Probe
32774	8006	-	-	Nestar
32776	8008	-	-	AT&T
32784	8010	-	-	Excelan
32787	8013	-	-	SGI diagnostics
32788	8014	-	-	SGI network games
32789	8015	-	-	SGI reserved
32790	8016	-	-	SGI bounce server
32793	8019	-	-	Apollo Domain
32815	802E	-	-	Tymshare
32816	802F	-	-	Tigan, Inc.
32821	8035	-	-	Reverse ARP
32822	8036	-	-	Aeonic Systems
32824	8038	-	-	DEC LANBridge
32825	8039-803C	-	-	DEC Unassigned
32829	803D	-	-	DEC Ethernet Encryption
32830	803E	-	-	DEC Unassigned
32831	803F	-	-	DEC LAN Traffic Monitor
32832	8040-8042	-	-	DEC Unassigned
32836	8044	-	-	Planning Research Corp.
32838	8046	-	-	AT&T
32839	8047	-	-	AT&T
32841	8049	-	-	ExperData
32859	805B	-	-	Stanford V Kernel exp.
32860	805C	-	-	Stanford V Kernel prod.
32861	805D	-	-	Evans & Sutherland
32864	8060	-	-	Little Machines
32866	8062	-	-	Counterpoint Computers
32869	8065	-	-	Univ. of Mass. @A mherst
32870	8066	-	-	Univ. of Mass. @ Amherst
32871	8067	-	-	Veeco Integrated Auto.
32872	8068	-	-	General Dynamics
32873	8069	-	-	AT&T
32874	806A	-	-	Autophon
32876	806C	-	-	ComDesign
32877	806D	-	-	Computgraphic Corp.
32878	806E-8077	-	-	Landmark Graphics Corp.
32890	807A	-	-	Matra
32891	807B	-	-	Dansk Data Elektronik
32892	807C	-	-	Merit Internodal
32893	807D-807F	-	-	Vitalink Communications
32896	8080	-	-	Vitalink TransLAN III
32897	8081-8083	-	-	Counterpoint Computers

32923	809B	-	-	Appletalk
32924	809C-809E	-	-	Datability
32927	809F	-	-	Spider Systems Ltd.
32931	80A3	-	-	Nixdorf Computers
32932	80A4-80B3	-	-	Siemens Gammasonics Inc.
32960	80C0-80C3	-	-	DCA Data Exchange Cluster
32964	80C4	-	-	Banyan Systems
32965	80C5	-	-	Banyan Systems
32966	80C6	-	-	Pacer Software
32967	80C7	-	-	Applitek Corporation
32968	80C8-80CC	-	-	Intergraph Corporation
32973	80CD-80CE	-	-	Harris Corporation
32975	80CF-80D2	-	-	Taylor Instrument
32979	80D3-80D4	-	-	Rosemount Corporation
32981	80D5	-	-	IBM SNA Service on Ether
32989	80DD	-	-	Varian Associates
32990	80DE-80DF	-	-	Integrated Solutions TRFS
32992	80E0-80E3	-	-	Allen-Bradley
32996	80E4-80F0	-	-	Datability
33010	80F2	-	-	Retix
33011	80F3	-	-	AppleTalk AARP (Kinetics)
33012	80F4-80F5	-	-	Kinetics
33015	80F7	-	-	Apollo Computer
33023	80FF-8103	-	-	Wellfleet Communications
33031	8107-8109	-	-	Symbolics Private
33072	8130	-	-	Hayes Microcomputers
33073	8131	-	-	VG Laboratory Systems
33074	8132-8136	-	-	Bridge Communications
33079	8137-8138	-	-	Novell, Inc.
33081	8139-813D	-	-	KTI
	8148	-	-	Logicraft
	8149	-	-	Network Computing Devices
	814A	-	-	Alpha Micro
33100	814C	-	-	- SNMP
	814D	-	-	BIIN
	814E	-	-	BIIN
	814F	-	-	Technically Elite Concept
	8150	-	-	Rational Corp
	8151-8153	-	-	Qualcomm
	815C-815E	-	-	Computer Protocol Pty Ltd
	8164-8166	-	-	Charles River Data System
	817D	-	-	XTP
	817E	-	-	SGI/Time Warner prop.
	8180	-	-	HIPPI-FP encapsulation
	8181	-	-	STP, HIPPI-ST
	8182	-	-	Reserved for HIPPI-6400
	8183	-	-	Reserved for HIPPI-6400
	8184-818C	-	-	Silicon Graphics prop.

	818D	-	-	Motorola Computer
	819A-81A3	-	-	Qualcomm
	81A4	-	-	ARAI Bunkichi
	81A5-81AE	-	-	RAD Network Devices
	81B7-81B9	-	-	Xyplex
	81CC-81D5	-	-	Apricot Computers
	81D6-81DD	-	-	Artisoft
	81E6-81EF	-	-	Polygon
	81F0-81F2	-	-	Comsat Labs
	81F3-81F5	-	-	SAIC
	81F6-81F8	-	-	VG Analytical
	8203-8205	-	-	Quantum Software
	8221-8222	-	-	Ascom Banking Systems
	823E-8240	-	-	Advanced Encryption Syste
	827F-8282	-	-	Athena Programming
	8263-826A	-	-	Charles River Data System
	829A-829B	-	-	Inst Ind Info Tech
	829C-82AB	-	-	Taurus Controls
	82AC-8693	-	-	Walker Richer & Quinn
	8694-869D	-	-	Idea Courier
	869E-86A1	-	-	Computer Network Tech
	86A3-86AC	-	-	Gateway Communications
	86DB	-	-	SECTRA
	86DE	-	-	Delta Controls
	86DD	-	-	IPv6
34543	86DF	-	-	ATOMIC
	86E0-86EF	-	-	Landis & Gyr Powers
	8700-8710	-	-	Motorola
34667	876B	-	-	TCP/IP Compression
34668	876C	-	-	IP Autonomous Systems
34669	876D	-	-	Secure Data
	880B	-	-	PPP
	8847	-	-	MPLS Unicast
	8848	-	-	MPLS Multicast
	8A96-8A97	-	-	Invisible Software
36864	9000	-	-	Loopback
36865	9001	-	-	3Com(Bridge) XNS Sys Mgmt
36866	9002	-	-	3Com(Bridge) TCP-IP Sys
36867	9003	-	-	3Com(Bridge) loop detect
65280	FF00	-	-	BBN VITAL-LanBridge cache
	FF00-FF0F	-	-	ISC Bunker Ramo
65535	FFFF	-	-	Reserved

HTTP ステータスコード

ステータスコード	説明
100	Continue—継続。クライアントはリクエストを継続できる。

101	Switch protocols--プロトコル切替え。サーバーはリクエストを理解し、遂行のためにプロトコルの切替えを要求している。
200	OK-- OK。リクエストは成功し、レスポンスとともに要求に応じた情報が返される。
201	Created--作成。リクエストは完了し、新たに作成されたリソースの URI が返される。
202	Accepted--受理。リクエストは受理されたが、処理は完了していない。
203	Non-Authoritative Information--信頼できない情報。オリジナルのデータではなく、ローカルやプロキシ等からの情報であることを示す。
204	No Content-- 内容なし。リクエストを受理したが、返すべきレスポンスエンティティが存在しない場合に返される。
205	Reset Content--内容のリセット。リクエストを受理し、ユーザーエージェントの画面をリセットする場合に返される。
206	Partial Content--部分的内容。部分的 GET リクエストを受理したときに、返される。
300	Multiple Choices--複数の選択。リクエストしたリソースが複数存在し、ユーザーやユーザーエージェントに選択肢を提示するときに返される。
301	Moved Permanently-- 恒久的に移動した。リクエストしたリソースが恒久的に移動されているときに返される。Location:ヘッダーに移動先の URL が示されている。
302	Found--発見した。リクエストしたリソースが一時的に移動されているときに返される。Location:ヘッダーに移動先の URL が示されている。
303	See Other--他を参照せよ。リクエストに対するレスポンスが他の URL に存在するときに返される。Location:ヘッダーに移動先の URL が示されている。
304	Not Modified-- 未更新。リクエストしたリソースは更新されていないことを示す。
305	Use Proxy--プロキシを使用せよ。レスポンスの Location:ヘッダーに示されるプロキシを使用してリクエストを行わなければならないことを示す。
306	No Longer Used--将来のために予約されている。ステータスコードは前のバージョンの仕様書では使われていたが、もはや使われておらず、将来のために予約されているとされる。
307	Temporary Redirect --一時的リダイレクト。リクエストしたリソースは一時的に移動されているときに返される。Location:ヘッダーに移動先の URL が示されている。
400	Bad request--リクエストが不正である。定義されていないメソッドを使うなど、クライアントのリクエストがおかしい場合に返される。
401	Unauthorized--認証が必要である。Basic 認証や Digest 認証などを行うときに使用される。
402	Payment required--支払いが必要である。現在は実装されておらず、将来のために予約されているとされる。
403	Forbidden--禁止されている。リソースにアクセスすることを拒否された。リクエストはしたが処理できないという意味。
404	Not found--未検出。リソースが見つからなかった。
405	Method Not Allowed--許可されていないメソッド。許可されていないメソッド

	を使用しようとした。
406	Not Acceptable--受理できない。Accept 関連のヘッダーに受理できない内容が含まれている場合に返される。
407	Proxy Auth Req--プロキシ認証が必要である。プロキシの認証が必要な場合に返される。
408	Request Timeout--リクエストタイムアウト。リクエストが時間以内に完了していない場合に返される。
409	Conflict--矛盾。要求は現在のリソースと矛盾するので完了出来ない。
410	Gone--消滅した。リソースは恒久的に移動・消滅した。どこに行ったかもわからない。
411	Length Required--長さが必要。Content-Length ヘッダーがないのでサーバがアクセスを拒否した場合に返される。
412	Precondition Failed--前提条件で失敗した。前提条件が偽だった場合に返される。
413	Request Entity Too Large--リクエストエンティティが大きすぎる。リクエストエンティティがサーバーの許容範囲を超えている場合に返す。
414	Request URI Too Long--リクエスト URI が大きすぎる。URI が長過ぎるのでサーバーが処理を拒否した場合に返す。
415	Unsupported Media Type--サポートしていないメディアタイプ。指定されたメディアタイプがサーバーでサポートされていない場合に返す。
416	Requested Range Not Satisfiable--リクエストしたレンジは範囲外にある。実リソースのサイズを超えるデータを要求した。
417	Expectation Failed--その拡張はレスポンスできない。またはプロキシサーバーは、次に到達するサーバーがレスポンスできないと判断している。
449	Retry With--再び試みる。要請は、適切な行動を実行した後に再び試みられなければならない。
500	Internal Error-- サーバー内部エラー。サーバー内部にエラーが発生した場合に返される。
501	Not implemented--実装されていない。実装されていないメソッドを使用した。
502	Bad Gateway--不正なゲートウェイ。ゲートウェイ・プロキシサーバーは不正な要求を受け取り、これを拒否した。
503	Service Unavailable--サービス利用不可。サービスが一時的に過負荷やメンテナンスで使用不可能である。
504	Gateway timeout--ゲートウェイタイムアウト。ゲートウェイ・プロキシサーバーは URI から推測されるサーバーからの適切なレスポンスがなくタイムアウトした。
505	HTTP Version Not Supported--サポートしていない HTTP バージョン。リクエストがサポートされていない HTTP バージョンである場合に返される。