Colasoft®
Maximize Network Value

Capsa

Real-time Portable Network Analyzer

ユーザーガイド

著作権所有© 2022 Colasoft. すべての権利を留保する。本書の内容は、予告なしに変更されるこ とがあります。本書の全ての内容は、Colasoft の書面による明確な許可無しに、いずれの目的のため にも、複写を含む電子または機械によるいかなる形式または手段によっても、転載、または拡散をして はならない。

Colasoft は、ユーザーへの予告や通知なしに製品デザインを変更する権利を留保します。

お問い合わせ

電話番号

03-4360-9364

Sales

sales@colasoft-japan.com

技術サポート

support@colasoft-japan.com

ウェブサイト

https://www.colasoft-japan.com

目次

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

1 Capsa の概要

Colasoft Capsa は、データパケットの収集、デコード、プロトコル分析、統計、チャート、レポート、その他の機能を統合した包括的なネットワーク分析プラットフォームです。 これは、ネットワーク管理者がネットワークを監視し、ネットワーク障害を特定し、ネットワーク内のセキュリティリスクをトラブルシューティングするのに役立ちます。

Colasoft Capsa は、Colasoft ネットワークによって作成された新しいネットワーク分析システムであり、Colasoft ネットワーク分析プラットフォームの重要な部分です。 完全に独立して設計および開発された第 2 世代のネットワーク分析エンジンを採用し、大量のデータ収集と高性能のリアルタイム診断および分析を提供し、企業イントラネットのパノラマ情報を包括的に表示し、ネットワーク管理者がネットワーク障害を正確に特定できるようにします。隠れた危険性、多方向のパフォーマンス監視と最適化、およびエンタープライズネットワーク使用の価値を包括的に向上させます。

Colasoft Capsa は、中国で最高のネットワーク分析製品です。モバイルラップトップにインストールして、問題が発生した場所でネットワークデータを即座に分析できます。さまざまな方法でネットワークデータパケットを収集して、リアルタイムで障害を診断したり、アーカイブされたデータパケットを再生してネットワークの履歴問題の遡及的分析を実行したりします。分析設定を適用して正確な分析を実現することで、ユーザーがネットワークで見つかった問題をより効果的に解決し、正確なポジショニングと効率的な分析を実現できます。このシステムは、まったく新しい UI インターフェース設計を採用しており、統計および診断ネットワーク情報を最も簡潔で直感的な方法でユーザーに提示するよう努めています。強化されたエキスパート診断、要約統計、プロトコルレイヤー統計、およびノード統計は、詳細なネットワーク障害、パフォーマンス、およびセキュリティ分析データを提供し、ネットワーク管理者が問題をすばやく見つけて解決するのに役立ちます。新しいアラームとカスタムプロトコル機能により、マネージャーは理解できます。ネットワークの稼働状況とネットワークの詳細なアプリケーション条件をリアルタイムで確認できます。元のノードブラウザナビゲーション、エキスパート診断ナビゲーション、チャートとレポートのナビゲーションビュー、豊富なチャートとレポートのコンテンツにより、ユーザーはいつでもネットワークデータを監視およびマスターできます。

革新的な第 2 世代ネットワークデータ収集エンジンにより、Capsa は、100M

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ネットワークでも 1000M ネットワークでも、大規模なトラフィックのネットワーク環境をサポートできます。その高性能で信頼性の高いデータ収集と分析により、ネットワークに次のようなサービスを提供できます。効率的で完全なデータ収集と分析。Web 分析ソリューション。 Colasoft Capsa は、エンタープライズネットワークが次のタイプの作業を完了するのに役立ちます。

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

Colasoft Capsa は、ネットワークの最下層から開始し、基本的にネットワーク内のさまざまな問題を検出し、他のさまざまなネットワーク管理ツールの使用を調整およびサポートし、完全なネットワーク管理を最大化します。

1.1 バージョン情報

製品バージョン情報を表示します：機能領域、システムページ>バージョン情報> Colasoft Capsa について。

1.2 ライセンス契約

重要な説明：ダウンロード、インストール、コピー、または使用する前に、製品アプリケーションに関する以下の条件を丁寧にお読みください。 ソフトウェアをダウンロード、インストール、コピー、または使用することにより、これらの条件に同意したことになります。

この最終ユーザーライセンス契約（以下「契約」という）は Colasoft 会社およびその子会社完（完全子会社および持株子会社を含む）が、自然人または法人であるあなた（以下「あなた」または「最終ユーザラー」という）と締結するものです。契約ですは本書で 1 番目に定義したソフトウェアをご使用されることを許可します。本書で 1 番目に定義したソフトウェアはデータキャリアに付けられ、電子メールで送って、インターネットからダウンロードされ、Colasoft のサーバからダウンロードされ、または次の条項に従って他のソース

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

から取得される可能性があります。

これは購入契約ではなく、最終ユーザーの権利に関する契約です。このソフトウェア自体、またはソフトウェアのコピー、または商業的にパッケージされたこのソフトウェアを含む物理メディア、または本契約に基づいて最終ユーザラーが使用する権利を有する他のコピーにかかわらず、所有権はすべて Colasoft 会社に所有します。

ソフトウェアのインストールやダウンロードやコピー、または使用中に「同意」ボタンをクリックすると、本契約条件にご同意なさることを示します。本契約の条項と条件にご同意しない場合は、すぐに「閉じる」オプションをクリックし、インストールまたはダウンロードをキャンセルし、本ソフトウェアやインストールメディア、および添付ドキュメントを破棄てください。

ソフトウェアを使用することに同意するということは、この契約を読み済み、この契約の条件を理解し、それに従うことに同意することを意味します。

1.ソフトウェア

本契約の“ソフトウェア”とは:

(i)コンピュータプログラム、そのすべての構成部分を含めます;

(ii)ディスク、CD-ROM、DVD、電子メールや任意の添付ファイル、および本契約に添付されたその他のメディアのすべての内容である，データベアラツールで提供され、電子メールまたはインターネットでダウンロードされたオブジェクトコードの形式のソフトウェアを含めます;

(iii)本ソフトウェアについてのすべての説明材料と他の関するファイルである，ソフトウェア説明、ソフトウェア仕様、ソフトウェア特徴または操作、ソフトウェアを使用についての操作環境や使用やソフトウェアのインストールの説明或はソフトウェアの使用方法に関する説明です（以下「ドキュメント」という）；

(iv)ソフトウェアのコピー、ソフトウェアエラー(エラーがある場合)の修正プログラム、ソフトウェアに添付されたプログラム、ソフトウェアの拡張、ソフトウェアの修正バージョン、およびソフトウェアコンポーネントの更新(ある場合)については、本契約第 3 項に従ってライセンスを付与します。ソフトウェアは、実行可能なオブジェクトコードのみで提供されます。

2.インストール

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

データキャリアに付けられ、電子メールで送って、インターネットからダウンロードされ、Colasoft のサーバからダウンロードされ、または他のソースで入手したソフトウェアをインストールしなければなりません。正しく配置したコンピューター / サーバにソフトウェアをインストールしなければならなくて、そのドキュメントにリストされている少なくとも要件を満たす必要があります。ドキュメントにインストール方法が指定されています。本ソフトウェアに悪影響を及ぼす可能性のあるコンピュータプログラムまたはハードウェアは、本ソフトウェアをインストールするコンピュータにインストールできません。

3.許可

本契約の条項にご同意なさると，許可費用の支払いを完了して本契約の規定されたすべての条項を遵守した場合，Colasoft は次の権利を与える(「許可」):

(a) インストールと使用の許可である。コンピュータのハードディスク（ＨＤＤ）やその他の永続的なメディアにソフトウェアをインストールして、データストレージをして、コンピュータシステムのメモリにソフトウェアをインストールおよびストレージし、実施やストレージやソフトウェアを表示するなどの非独占的で、そして譲渡できない権利があります。

(b) 数量規定の許可である。ソフトウェアの使用権は最終ユーザー数によって制約されます。一人の最終ユーザーとは１個のコンピュータシステムにソフトウェアをインストールすることで、複数のコンピュータで同じライセンスを同時に使用することはできないのです。

(c) 許可条項である。ソフトウェアの使用権は時間にによって制約されます。

(d) 許可終了である。許可は付与された期限が終了すると、自動的に終了します。本契約のいかなる条項を守らなければ、Colasoft は契約を取り消す権利があります。もし契約を取り消す場合、ソフトウェアをすぐに削除し、破棄し、または自己負担でソフトウェアおよびすべてのバックアップコピーを Colasoft 会社やまたはソフトウェアを購入した場所にご返却ください。許可が終了すると、Colasoft は最終ユーザーがソフトウェアを使用する権利を取り消す権利もあります。

4.最終ユーザーの権利を執行

お客様自身または従業員を通じて最終ユーザーの権利を執行する必要があります。ソフトウェアは操作の安全性と保護を確保した許可を購入したコンピュータシステムにのみ使用できます。

5.権利の制限

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

コンポーネントをコピーや配布や抽出すること、、またはソフトウェアの派生バージョンを作成するのは禁止です。ソフトウェアを使用する時、次の制限を守ってなければなりません:

(a) バックアップコピーとして，永続的なストレージメディアにソフトウェアのコピーを作ることができます。この前提は他のコンピュータにそのバックアップコピーをインストールまたは使用されません。ソフトウェアを作成する他のコピーは、本契約に違反するとみなされます。

(b) 本契約で提供される方法以外のいかな方式でソフトウェアを修正や翻訳やコピーし、或はソフトウェアとソフトウェアコピーの使用権を譲渡しません。

(c) ソフトウェアを販売することや依存許可を付与することやソフトウェアを他人に貸すこと、或は他人からソフトウェアを借りたり、ソフトウェアを他人に貸したりするは禁止です。

(d) 法律が制限を明確に禁止する範囲外で、いかなる方式でリバースエンジニアリングやリバースコンパイルやリバースアセンブリソフトウェアして、或はソフトウェアのソースコードを取得しようとしたりしてはいけません。

(e) ご同意したソフトウェアの使用方法はソフトウェアの使用に関する法律のすべての適用法規に合致しなければならないのです。著作権法およびその他の知的財産権に適用される制限を含めますが、これに限定されません。

6.著作権

ソフトウェアとすべての権利は所有権と知的財産権を含めるが、それに限らず、Colasoft に属し、それに中国の関連法律法規と国際条約条項によって保護されます。ソフトウェアの構造、構成、およびコードは、Colasoft の重要な企業秘密および機密情報です。 セクション 5（a）で指定されている場合を除き、ソフトウェアをコピーすることはできません。 本契約に基づいて作成されたコピーには、本ソフトウェアに表示されるものと同じ著作権およびその他の所有権に関する通知を含めることが許可されています。 リバースエンジニアリング、逆コンパイル、ソースの逆アセンブル、またはソフトウェアのソースコードの取得を試みる場合、そのような行為の開始から取得した情報は、自動的かつ不可逆的に Colasoft に転送され、Colasoft が所有することに同意するものとします

7.権利の保留

本契約書でソフトウェアの最終ユーザーとして、明確に付与された権利を除き，Colasoft はこれに基づいて他のすべてのソフトウェア権利を保留します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

8. 複数言語バージョン、デュアルメディアソフトウェア、複数のコピーバージョン

ソフトウェアが複数のプラットフォームまたは複数の言語をサポートしている場合、またはそちらが複数のソフトウェアのコピーを取得している場合は、ソフトウェアは許可が購入したコンピュータシステムの数とバージョンにのみ使用できます。使用しないソフトウェアのバージョンまたはコピーを販売、レンタル、借り、依存ライセンスの付与、貸し出し、または他の人に譲渡することはできません。

9.契約の開始と終了

本契約は、本契約の条項にご同意なさる日から発効します。本契約はいつでもソフトウェアやすべてのバックアップコピーやおよび Colasoft またはそのビジネスパートナーが提供するすべての関連資料を永久にアンインストール、破棄または返却(費用自己負担)することによって、終了できます。本契約の終了方式を考慮しないで、第 6、7、10、12、19 と 20 項の条項は無期限で有効であるべきです。

10.最終ユーザーの声明

最終ユーザーとして、ソフトウェアが「契約に従って」提供されることをご存じで、明示的または暗示的な陳述または保証は一切ありません。適用法律が許容する最大の範囲内で、Colasoft やその代理店または支店または著作権所有者はこれらに限定されない販売性や特定の用途適用性を含む保証についての、明示的または暗示的な陳述と保証を提供しません。Colasoft 或は他の方はソフトウェアの操作がスムーズで間違いないことを保証していません。目的を達成するために、このソフトウェアを選択し、このソフトウェアのインストールと使用とアプリケーション結果をインストール、使用するすべての責任とリスクは、お客様が負担します。

11.他の義務なし

本契約書に特に記載された義務を除き、本契約書は Colasoft にいかなるその他の義務を加えません。

12.責任の制限

法律が許容する最大の範囲内で、いかなる場合でも、Colasoft やその従業員または代理店は以下の損失に責任を負わないのです。いかなる形式による利益、収入または売上高の損失、いかなるデータの損失、予備品またはサービスを得るために支払う追加費用、財産の損失、人身傷害、営業中断、商業情報の損

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

失、またはいかなる特殊、直接、間接、意外、経済、カバー、犯罪、特殊または後続の損失などです。これらの損失が契約の破棄、故意の誤操作、不注意、またはその他の責任理論によるものであっても、ソフトウェアの使用または使用不能によるものであっても、Colasoft またはその代理店または支店にこのような損失の可能性を通知しても責任を負いません。

13. 本契約のいかなる条項は法律が認められた消費者の権利と地位一方の権利に影響を与えないのです

14.技術のサポート

Colasoft または Colasoft が委託した第三者は自ら考慮して技術サポートを提供し、いかなる保証や声明を持ちません。技術のサポートを提供する前に、最終ユーザーは既存のデータやソフトウェアやプログラムツールをすべてバックアップしなければなりません。Colasoft または Colasoft が委託した第三者は技術サポートの提供によって、データや財産やソフトウェアと使ハードウェアの破壊、損失、または利益などの損失を負担されません。Colasoft または Colasoft が委託した第三者は自ら考慮して技術サポートの拒否や停止または終了する権利を保留します。

15.許可の譲渡

契約条項に違反しない限り、ソフトウェアは異なるコンピュータシステム間で移行できます。契約条項に違反しない場合、最終ユーザーは科来の書面同意で、許可と本契約から発生したすべての権利を他の最終ユーザーに譲渡し、以下の条項の制約を受ける権利しかありません。

(i) 元の最終ユーザーはソフトウェアのコピーを保留することができません;

(ii)権利の譲渡は元の最終ユーザーから新しい最終ユーザーに渡さなければなりません。

(iii) 新しい最終ユーザーは元の最終ユーザーが本契約の条項で負うすべての権利と義務を負わなければなりません。

(iv) 元の最終ユーザーは新しい最終ユーザーにドキュメントを提供しなければならなくて、第 16 項で指定したソフトウェアの正規性を証明するためのです。。

16.ソフトウェアの正規性を証明

最終ユーザーは次のいずれかの方法でソフトウェアの使用権を証明できます:

(i) Colasoft または Colasoft が委託した第三者が発行した許可書によって;

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

(ii)書面による許可協議を通じて，このような協議が締結された場

(iii) Colasoft が送信される詳しい許可情報(ユーザー名とパスワード)を含む E メールを通じること。

17.輸出と再輸出の制御

ソフトウェアやドキュメントまたはその中の各部分(ソフトウェアおよびその各部分の関連情報を含む)は政府が発表した関連法律法規での輸入と輸出規則によって制御されます。ここで政府は適用法律の公布を担当する政府機関を指し、中国の輸出管理法規および中国政府とその他の政府が公布した最終ユーザー、最終使用と目標制限を含るのです。適用されるすべての輸入および輸出規制を厳格に遵守することをご同意なさって、それにソフトウェアの輸出、再輸出、輸送、または輸入の許可を取得すことを承認します。

18.お知らせ

すべてのお知らせと返却されたソフトウェアおよびドキュメントは Colasoft に渡さなければなりません。

19.法律の適用

本契約は中華人民共和国の関連法律法規に管轄され、それに中華人民共和国の関連法律法規によって解釈されます。

20.通用条項

本契約の条項が無効または実行できない場合，本契約の他の条項の有効性には影響しません。ここに規定された条件に従って、これらの条項は依然として有効で実行可能です。本契約は書面でのみ修正でき、それにこの操作を実行することを担当者または明確に授権した者が授権依頼書の条項の下でこのような修正する必要があります。

Colasoft と署名した本契約は本フトウェアに関する唯一の完全な契約であり、これまでのソフトウェアに関するいかなる記述、議論、承諾、コミュニケーション、広告に完全に取って代わります。

1.3 購入情報

購入

製品を購入する必要がある場合、または製品購入の関連情報を知る必要がある

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

場合は、support@colasoft-japan.com までご連絡ください。

製品付属品

製品外箱、CD ボックス、製品 CD、ユーザー情報カード、ユーザーガイド。

1.4 サービスと技術サポート

サービス

弊社はユーザーに完全なプレセールサービスとアフターサービスを提供し、ユーザーが安心して弊社の製品を使用できるようにします。

プレセールサービス

- 製品コンサルティング

  ユーザーのニーズを理解し、ソリューションを提供し、製品の機能と使用法をユーザーに紹介します。

- トライアルを提供

ユーザーに製品のトライアル版を提供し、技術的なガイダンスを提供します。

アフターサービス

- 技術サポート

  ユーザーに技術的なアドバイスを提供し、製品のソリューションを使用します。

- アップグレードサービス

  通常のユーザーには、1 年間の無料アップグレードが提供されます。

- トラブルシューティング

  リモートテクノロジーまたは障害レポートを通じてトラブルシューティングするようにユーザーをガイドします。

技術サポート

注：許可されたユーザーのみが技術サポートサービスを受ける資格があります。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

一般的な質問について、 この製品の FAQ 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。

ウェブサイトサポート

当社のウェブサイトから一般的な問題の解決策を見つけてください。

最新 FAQ や専門用語のほかに、 http://www.colasoft-japan.com/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。

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@colasoft-japan.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。

ファックス技術サポート

緊急時に迅速な解決策を得るには、ファックスで 03-4360-9364 までご連絡ください。 ファックスするときは、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。

電話サポート

ソリューションについてお問い合わせください。休日を除き、毎日午前 9 時から午後 5 時まで電話：03-4360-9364 でお問い合わせください。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

2 機能と特徴

Colasoft Capsa は、製品に大幅な改善を加え、多くの新機能も追加しました。以下は、いくつかの重要な機能と特徴です。製品の最新機能については、当社の Web サイト（http://www.colasoft-japan.com）にアクセスすることもできます。

2.1 新機能

- 新しいインターフェースと新しいレイアウト、ユーザー操作の簡素化、より便利なデータマイニングとデータフィルタリング。
- まったく新しい分析モードと分析設定により、ユーザーは分析タスクをすばやく完了することができます。
- 分析設定をカスタマイズして、より的を絞った方法でネットワークの問題を分析します。
- 新しいチャートビュー（My Chart）、強力なチャートカスタマイズ機能、柔軟なインターフェイスパフォーマンス。
- ネットワークの問題をすばやく明らかにするための、まったく新しい専門家による診断とビューのレイアウト。
- 新しいプロトコルビュー。
- 新しい物理エンドポイント/IP エンドポイントビュー。
- 新しい物理セッション/IP セッション/TCP セッション/UDP セッションビュー。
- カスタム作成されたアラーム、オンラインリアルタイムアラームリマインダー。
- カスタマイズされたプロトコル。

2.2 真新しい UI インターフェース

Colasoft Capsa は、製品インターフェイスにまったく新しいデザインを作成し、6.x シリーズの製品のスタイルを継続しなくなりましたが、最新の Microsoft Office2007 スタイルを完全に採用して、ユーザーに最新のインターフェイスエクスペリエンスを提供します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

2.3 新しい分析設定

分析設定は、分析エンジンのパラメーター構成、ロードされた高度な分析モジュール、各高度な分析モジュールの詳細なパラメーター設定など、特定の分析要件の構成情報を保存するために使用されます。

分析設定は、ネットワークビジネスアプリケーションの問題に対するソリューション分析ソリューションです。 これは、ネットワークオブジェクトデータ統計設定、分析モジュール設定、診断設定、ログ設定、チャート設定など、いくつかの分析設定で構成されています。 ユーザーは、実際の分析タスクに応じて適切な分析設定を選択できます。これにより、システム分析のパフォーマンスが向上するだけでなく、ユーザーの分析効率も向上します。

分析設定は複数の分析モジュールで構成されており、カスタム分析設定機能を備えており、実際の分析要件に応じて新しい分析設定を作成したり、システムの初期分析設定を変更したりできます。 分析設定内で、さまざまな分析モジュールをカスタマイズして追加または削除し、最良の分析結果を得ることができます。

分析設定の詳細については、「分析設定」を参照してください。

2.4 新しい分析とガイダンスの経験

プログラムの最初のスタートページは、新鮮な視点でネットワーク分析タスクをユーザーに案内します。 分析タスクは通常、次の 4 つのステップで完了します:

1. 分析モードの選択
   - リアルタイム分析と再生分析の 2 つのデータ収集および分析モードを提供します
   - リアルタイム分析モードでは、ネットワークアダプタの設定を選択できます
   - 再生分析モードではファイルと再生速度を選択できます
   - どちらのモードでも、パケットキャプチャフィルタを追加で設定できます
2. ネットワークアダプタの選択

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

有線ネットワークアダプター：データのキャプチャに使用するネットワークアダプターを選択します。 1 つまたは複数のネットワークカードを同時にデータキャプチャ用に選択できます。
ワイヤレスネットワークアダプタ：データキャプチャ用に選択できるネットワークカードは 1 つだけです。 ワイヤレスパケットをキャプチャするには、分析するワイヤレス AP を選択し、正しいパスワードを入力します。システムはマルチチャネル AP の分析をサポートします。選択した AP がマルチチャネル AP の場合、分析用の補助ネットワークカードを選択する必要があります。

3. [分析設定] の選択

   実際のニーズに応じて、最適な分析アプリケーションを実現するために、関連する分析設定がターゲットを絞って選択されます。

4. 分析を開始

2.5 リアルタイム分析

分析ガイドエクスペリエンスには、2 つの分析モードがあります。リアルタイム分析では、データ収集ソースとしてネットワークアダプターを使用し、対応する分析設定を選択して分析タスクを完了します。 リアルタイム分析により、アダプタのトラフィックステータスが直感的に表示されます。

2.6 再生分析

再生分析モードは、データパケットストレージファイルを分析用の 2 番目の分析データソースとして使用し、履歴問題の遡及的分析を提供し、元の速度の再生と高速再生の 2 つの再生速度をサポートします。

2.7 タイミング分析

Colasoft Capsa は、新しいタイミング分析機能を提供します。 特定の期間のデータパケットを自動的にキャプチャする必要がある場合は、タイミング分析機能を有効にして、分析時間、分析設定、およびその他の予備設定を事前設定できます。指定された時間に達すると、システムは自動的にデータパケット収集と分析を開始します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

2.8 オンラインリアルタイムアラーム

リアルタイムのグローバルアラートを提供して、管理者に現在のイベントを目立つ方法で警告します。 そして、メインビューの右下隅に現在トリガーされているアラームの数を表示します。

ユーザー定義のアラーム機能を提供します。ユーザーは、複数のビューから選択したネットワークオブジェクトのアラートを作成できます。

各アラートには、次のプロパティがあります:

- アラートオブジェクト
- アラートの種類（セキュリティ、パフォーマンス、障害）、重大度（情報、通知、アラート、エラー）
- アラーム統計の豊富なソース
- アラーム入力条件を設定
- アラーム解除条件を設定

Capsa リアルタイムアラームの作成と管理については、「アラームブラウザ」の紹介を参照してください。

2.9 カスタムプロトコル

Colasoft Capsa 専門家強化版には、強力なカスタムプロトコル機能があり、ユーザーは次の 2 種類のフィールドに従って、実際の状況に応じてプロトコルをカスタマイズできます。

- TCP
- UDP

プロトコルをカスタマイズする方法については、Capsa 構成の「プロトコルのカスタマイズ」の概要を参照してください。

2.10 新しい専門家の診断

専門家診断はインテリジェントなネットワーク障害診断機能です。6.x シリーズに基づいて、多くの新しい機能が強化されました。 Colasoft Capsa は、診断イベントの統計情報、診断イベントをトリガーするホストアドレス、および診断イベントの詳細な説明を個別のウィンドウで視覚的に表示する新しい診断ビューレイアウトを採用しています。イベントの場合、診断イベントをトリガ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ーするホストアドレスは自動的にフィルタリングされます。ホストアドレスを選択すると、ホストの診断ログが詳細に表示されます。

Capsa は、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の 4 つのレベルの障害診断をサポートします。

新しい診断ビューを使用すると、ユーザーは次の情報をすばやく理解できます:

- 各診断の参考情報を学び、診断の説明、原因、解決策を提供することができます。
- 各診断情報は、関連する TopN ホストのランキング表示を提供します。 どのホストが各診断イベントをトリガーするかを視覚的に取得できます。
- ホストに関連付けられている診断イベントログを学習して、ユーザーが問題のあるホストをより迅速に見つけるのに役立てることができます。
- イベントに関連するデータパケットマイニングについて知ることができます。これは、ダブルクリックすることで新しいウィンドウに表示できます。

専門家による診断の詳細については、「専門家による診断」を参照してください。

2.11 柔軟なチャートのカスタマイズ

Colasoft Capsa は、強力なチャートカスタマイズ機能を提供し、ユーザーにトラフィックの豊富なグラフィカルなリアルタイム監視ビューを提供します。 チャートパネルは簡単にカスタマイズおよび追加でき、各チャートパネルはさまざまなタイプのチャートを自由に追加できます。

Capsa は、グローバルチャート設定をサポートするだけでなく、特定のネットワークオブジェクトのチャートを作成および追加し、TCP セッションの詳細データ情報、アプリケーショントラフィック情報、アラームデータ情報などを含むリアルタイムのチャート監視を作成できます。さまざまなネットワークパラメータのリアルタイムの実行データをより直感的に確認できます。 新しいチャートビューには、次の機能があります。

- 新しいバージョンのチャートコントロールを使用すると、グラフィック表示がより美しく直感的になります。
- 基本的な分析といくつかのアプリケーション分析によってグループ化された、より多くのチャートタイプを提供します。 アプリケーション分析チャ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ートは、対応するアプリケーションプロトコル分析が有効な分析設定に含まれているかどうかから導き出されます。

- ユーザー定義のチャート機能を提供します。 ユーザーは、複数のビューから選択したネットワークオブジェクトの図を作成できます。

チャート統計の詳細については、「チャートの概要」を参照してください。

2.12 分析メインビュー管理

さまざまなネットワーク分析データを出力し、メインビュー領域から表示する必要があります。Colasoft Capsa は、柔軟な分析ビュー管理設定を提供します。 ユーザーは、表示する必要のないビュー領域を閉じたり、分析要件に応じて分析ビューの表示順序を任意に調整したりできるため、製品の使いやすさと柔軟性が大幅に向上します。

2.13 より多くのプロトコルをサポート

Colasoft Capsa は、次のようなほとんどすべての一般的なプロトコルを含む、多くのプロトコルをサポートしています: AARP, AARP Prbe, AARP Request, AARP Response, ACNET, AFP, AH, AIM, ARP, ARP Request, ARP Response, Auditd, BFTP, BGP, BOOTP, Biff, BitTorrent, CDC, CDP, CFS, CFTP, CGMP, CIFS, CMIP-Agent, CMIP-Man, COPS, CRIP, CRTP, CRUDP, CTF, Cisco-fna, Cisco-sys, Cisco-tna, Citrx ICA, DCCP, DCP, DDP,DECnet, DHCP, DIAG, DNS, DNS Error, DNS Query, DSR, Daytime, Discard, EGP, EIGRP, EIGRP Hello, EIGRP Query, EIGRP Reply, EIGRP Update, ESP, Echo, Emfis-cntl, Emfis-data, Ethernet - Other, Ethernet 802.2, Ethernet 802.3, Ethernet II, Ethernet SNAP, Ethernet SNAP - Other, eMule, FC, FCoE, FCP, FTP, FTP Ctrl, DTP Data, Finger, GDP, GGP, GRE, GTP, Gopher, H.225, H.323, HMP, HSRP, HTTP, HTTP Proxy, HTTPS, Http-mgmt, IBM-app, ICMP, ICMP DestUnreach, ICMP Echo Reply, ICMP Echo Req, ICMP Redirect, ICMP Time Ex, ICMPv6, ICP, IDFP, IDPR, IDRP, IGAP, IGMP, IGRP, IMAP, IAMP3, IAMP4, IMAP4/SSL, IP, IP - Other, IP Fragment, IPX, IPv6, IRC, IRC/SSL, IRTP, ISL, ISMP, ISO-IP, ISO-TP0, ISO-TP4, Kerberos, L2F, L2TP, LDAP, LDAPS, LPD, La-maint, Login, Loopback, MGCP, MPLS, MPLS Etype2, MPM, MPM-snd, MPP, MSN, MSP, MSRDP, MSSQL, Mcidas, Mit-ml-dev, Mnet-discovery, Mobile IP, Msg-auth, NAMP, NARP, NBDGM, NBIPX, NBNS, NBSSN, NCP, NETBLT, NFS, NLSP, NMSP, NNTP, NNTP/SSL, NPP, NSRMP, NTP, Nameserver, NetBEUI, NetBIOS, Ni-ftp, OSPF, OSPF DDs, OSPF Hello, OSPF LSA, OSPF LSR, OSPF LSU, PIM, PIP, PIPE, POP2, POP3, POP3/SSL, PPP, PPP CHAP, PPP FCC, PPP IPCP, PPP LCP, PPP LQP, PPP PAP, PPP Padding, PPPoE, PPPoE Discovery, PPPoE Session, PPTP, PPlive, PRM, PTP, PUP, PVP, Password-chg, Pdap, Pwdgen, Q.931, QQ, QQ keep Alive, QQ Login, QQ Logout, QQ Other, QQ Recv Msg, QQ Send Msg, Qotd, RAMP, RAP, RARP, RARP Request, RARP Response, RCP, RDP, RGMP, RIP, RIP Reply, RIP Request, RIPX, RIPv1, RIPv2, RIPv3, RIPv4, RIS, RJE, RLOGIN, RLP, RPC, RSH, RSVP, RSVP_tunnel, RTCP, RTELNET, RTP, RTP AV, RTP Audio, RTP

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

CelB, RTP DVI4, RTP Dynamic, RTP G.711, RTP G.723, RTP G.728, RTP G.729, RTP GSM, RTP H.261, RTP H.263, RTP JPEG, RTP MP2T, RTP MPV, RTP Video, RTSP, Radius, Radius-acct, Radius-dynauth, Re-mail-ck, Rexec, Rtsps, Rwhois, SAP, SAP, SAP Reply, SAP Request, SCC Security, SCCP, SCTP, SDRP, SER, SFTP, SGMP, SGMP-traps, SIP, SKIP, SLP, SMB, SMTP, SMTP/LSA, SMTP/SSL, SNMP, SNMP Trap, SNP, SNPP, SPS, SPX, SQL, SSDP, SSH, SShell, STP, Send, Sflow, Statsrv, Submission, Supdup, Swift-rvf, Systat, T.120, TCP, TCP - Other, TELNET, TFTP, TLSP, TNS, TRIP, Tacacs, Tacacs-ds, Tacnews, Time, Tunnel, UDP, UDP - Other, ULS, UMA, VLAN, VLAN EType2, VRRP, WINS, Who, WhoIs, Windows NLB, X-Window, X.400, XDAS, XNS, XNS-auth, XNS-ch, XNS-mail, XNS-time, Yahoo Messenger

2.14 強化されたトリックスビュー

新しいマトリックスビューは、以前のバージョンの設計原則に従いますが、詳細に多くの改善が加えられています:

- ノードとラインはエッジスムージングを提供します。
- フォーカスされたノードまたは接続に基づいてプロンプトを強調表示します。
- TOPN セッションと TOPN ノードマトリックスタイプを定義および作成できます。

マトリックスビューの詳細については、「マトリックスの概要」を参照してください。

2.15 プロトコル統計ビュー

プロトコルビューは、通信トラフィック、通信データパケット、送信トラフィック、受信トラフィックなど、現在のネットワーク通信プロトコルの動作パラメータに関する詳細な統計を提供し、プロトコルの実際のカプセル化順序に従って通信プロトコルを階層的に表示します。 プロトコルごとに色が異なります。ユーザーは、ネットワーク通信の現在のプロトコル動作を直感的に確認できます。

新しいプロトコルビューでは、物理エンドポイントと IP エンドポイントのサブビューが追加されます。プロトコルを選択すると、プロトコルを使用する物理アドレスまたは IP アドレスがサブビューに表示され、ユーザーがデータの関連付けを分析するのに便利です。

プロトコル統計ビューの詳細については、「プロトコルビューの概要」を参照

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

してください。

2.16 新しい IP エンドポイント統計ビュー

Colasoft Capsa は、新しい IP エンドポイント統計ビュー、ネットワーク内の各 IP アドレスの通信情報の詳細な統計を提供します。 Capsa には、IP アドレス通信用に最大 46 の統計パラメータがあり、カウントする必要のあるパラメータをカスタマイズできます。 これらのパラメータを使用すると、現在最も多くのトラフィックを占有している IP アドレス、最も多くのトラフィックを送信する IP アドレス、最も多くのトラフィックを受信する IP アドレスなどのさまざまな情報を簡単に知ることができます。 同時に、IP エンドポイントビューには、IP セッション、TCP セッション、UDP セッションの 3 つの個別のサブポートがあります。IP エンドポイントリストで IP アドレスを選択すると、システムはそのすべてのセッション情報を自動的に除外します。アドレス。これは、データの関連付け分析に非常に便利です。

2.17 新しい物理エンドポイント統計ビュー

IP エンドポイントビューに加えて、Capsa は、ネットワーク内の各 MAC アドレスの通信情報を詳細に示す新しい物理エンドポイント統計ビューも提供します。 Capsa は、MAC アドレス通信パラメータの詳細な統計を提供します。これらのパラメータを通じて、現在のトラフィックが占める MAC アドレス、最大の送受信トラフィックを持つ MAC アドレス、および最大の送受信データパケットを持つ MAC を簡単に知ることができます。 アドレスおよびその他の情報。 同時に、物理セッション分離サブポートを含む物理エンドポイントビューで、物理エンドポイントリストで物理アドレスを選択すると、システムはこのアドレスと他のアドレスとの間の通信セッション情報を自動的に除外します。詳細なデータ分析に便利です。

2.18 新しい IP セッションビュー

Capsa は詳細な IP セッション統計を提供し、現在のネットワークの各 IP セッションについて、セッションの送信元アドレス、宛先アドレス、セッショントラフィック、セッションの送受信データパケット、セッション期間、およびその他のパラメータを詳細に分析します。ウィンドウには、現在選択されている IP アドレスに関連付けられている TCP および UDP セッション。これらのセッ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ション情報を通じて、ネットワーク内の現在の IP アドレスセッションをすばやく理解できます。

2.19 新しい物理セッションビュー

物理セッションには、ネットワーク内の物理アドレス間のセッションに関する情報が表示されます。送信元物理アドレス、宛先物理アドレス、セッションで送受信されるデータパケット、およびこれらのデータパケットのサイズをカウントできます。MAC アドレス間のセッションを分析することにより、ネットワーク内のレイヤ 2 通信情報をすばやく分析および表示できます。

2.20 新しい TCP セッションビュー

TCP セッションビューでは、ネットワーク内の TCP 接続の通信セッション情報が詳細に表示されます。 TCP セッションごとに、送信元アドレス、宛先アドレス、合計セッショントラフィック、セッションの受信/送信トラフィック、セッションの受信/送信データパケット、およびこれらのデータパケットのサイズなどのさまざまな統計パラメータをカウントできます。 さらに、現在選択されている TCP 接続の元のデータパケット情報、TCP データストリームの再構成情報、および TCP セッションシーケンス図が TCP セッションサブウィンドウに表示されます。 TCP 通信セッションの分析を通じて、ワーム、ポートスキャン、SYN フラッドなどのさまざまなネットワーク攻撃の動作を分析するのに役立ちます。

2.21 新しい UDP セッションビュー

UDP セッションビューには、ネットワーク内の UDP 通信セッションに関する詳細情報が表示されます。 UDP セッションごとに、送信元アドレス、宛先アドレス、合計セッショントラフィック、セッション送信/受信トラフィック、セッション送信/受信データパケット、およびこれらのデータパケットのサイズをカウントできます。 また、現在選択されている UDP セッションの元のデータパケット情報と UDP データフロー情報が下のサブウィンドウに表示されます。 この情報を通じて、ネットワーク内の UDP 通信の現在の状況をすばやく分析できます。

2.22 包括的な要約統計ビュー

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

Colasoft Capsa の統計機能は非常に強力です。100 近くの統計カウンターが非常に詳細な統計情報を提供します。要約統計はグローバルであるだけでなく、各ネットワークプロトコルとネットワークエンドポイントに独自の要約統計があります。別のネットワークを選択してください。ノードブラウザのオブジェクト（IP アドレス/ MAC アドレス、プロトコルノード）。システムは自動的にオブジェクトの要約統計をフィルタリングして表示します。

要約統計ビューには、アラーム統計、診断統計、トラフィック統計、パケットサイズ分布、アドレス統計、プロトコル統計、データフロー統計、TCP 統計、DNS 分析、電子メール分析、FTP 分析、および HTTP 分析の 12 種類の異なるデータ統計値を提供します。

要約統計量ビューの詳細については、「要約統計量の概要」を参照してください。

2.23 強化されたグラフィカルフィルター

Colasoft Capsa は、強化されたグラフィカルフィルター設定と直感的なデータ分析フィルタープロセス表示を提供します。 フィルタの設定では、より直感的で便利であり、各フィルタエントリはスリーステート操作（受け入れ、拒否、有効化しない）をサポートします。 右側のフィルターフローチャートでは、分析プロセスにおける各フィルターの役割を視覚的に確認できます。

フィルタの詳細については、「フィルタ」の詳細を参照してください。

2.24 複数のネットワークカードの同時分析をサポート

実際のアプリケーションでは、管理するコンピューターに複数のネットワークインターフェイスカード（NIC）がインストールされている場合があります。次に、Colasoft Capsa を使用して複数のネットワークカードのデータを同時に分析できます。また、さまざまなプロジェクトを使用して分析することもできます。データは個別に。データ分析はネットワークカードごとに実行されます。

2.25 ログ分析モジュール

Colasoft Capsa は、基本的なデータ分析モジュールに加えて、HTTP リクエスト（Web ページの閲覧）、メール情報（SMTP / POP3 を介したメールの送受

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

信）、DNS クエリ（ドメイン名の解決）、FTP 送信、MSN ログ、Yahoo ログ、システムグローバルログの 7 種類のログ分析モジュールもサポートしています。これらの高度なログ分析モジュールはすべて、TCP データストリーム再編成機能を備えており、システムはこれを介してネットワーク内のデータ送信をリアルタイムで復元できます。

2.26 TCP セッションシーケンス図

TCP シーケンス図の表示が TCP タイプのセッションビューの個別のサブビューに追加され、TCP 接続と通信の両方の当事者の SYN および ACK 応答ステータスが効果的に表示され、ユーザーが TCP 通信の内容を理解するのに役立ちます。より簡単に、より直感的にコミュニケーションの問題を発見します。

2.27 ノードブラウザナビゲーション

ノードブラウザを使用すると、ユーザーはノードをすばやく見つけてデータをフィルタリングできます。 ノードを選択することにより、ユーザーはノードに対応するネットワークデータを表示できます。 ノードブラウザは、プロトコルノード、物理ノード、IP ノードの 3 つのクラスで構成されています。 ユーザーは、ネットワーク全体を簡単に見つけたり、特定の IP セグメントまたは特定の IP を見つけたりすることができます。 右側の表示領域には、選択したノードに応じた関連データが表示され、Kelai ネットワーク分析システムのノードブラウザがナビゲーションの方法で表示され、ノードブラウザの表示および測位機能が強化されます。 詳細については、ノードブラウザを参照してください。

2.28 付属ガジェット

Colasoft Capsa は、ユーザーが無料で使用できる 7 つの小さなツール、つまりコーデック変換ツール、IP アドレス属性クエリ、デコードスクリプトエディター、Colasoft ping ツール、MAC Scanner、Colasoft Packet player、Colasoft Packet Builder を提供します。ユーザーが一般的に使用されるネットワークツールをカスタマイズして、Colasoft Capsa に追加できるようにします。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

3 製品導入の説明

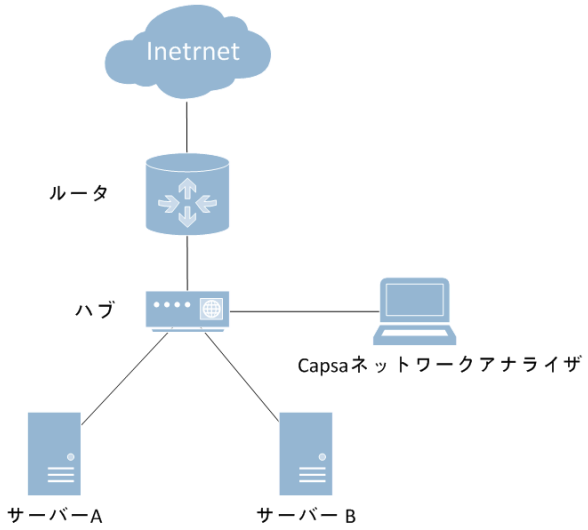
ポータブルネットワーク分析システムとして、Colasoft Capsa は引き続きスニッフィングモードで動作し、バイパスモードを介してデータ収集のためにネットワークに接続されます。展開方法はシンプルで柔軟です。 イントラネット、イントラネット、エクストラネットでデータの検出と分析を実行し、ネットワークセグメントと VLAN 全体のデータを監視できます。 ローカルエリアネットワーク内のすべてのマシンではなく、1 台の管理マシンにのみインストールできます。 管理者は、必要に応じてネットワークのインストール場所を決定できます。インストール場所が異なれば、ネットワーク通信データも異なります。 したがって、ネットワークデータをより包括的に監視するには、製品に導入されている機器を中央スイッチング機器に直接接続して、より多くのデータ情報を収集および分析できるようにすることをお勧めします。ネットワークタップを使用して分析することもできます。ネットワークセグメントデータ。 以下に、いくつかの一般的な製品展開を紹介します。

3.1 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:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

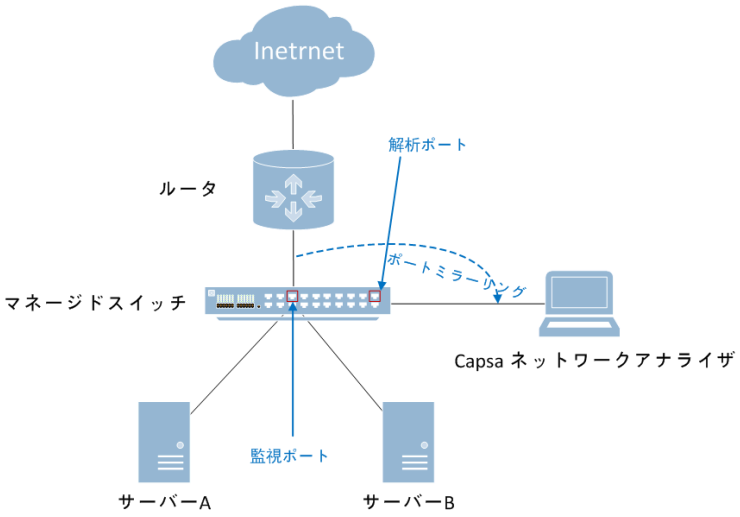


3.2 スイッチドネットワーク – マネージドスイッチ (ポートミラーリング)

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。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



上の図で、ネットワーク内のスイッチがポートミラーリングをサポートしている場合は、次の手順に従うことができます（ここでは、Cisco Catalyst 4000 シリーズスイッチのポートミラーリングを例として取り上げます）。

スイッチのアップリンクポートが f5/48 の場合、つまりこのポートがルーターに接続されている場合、ネットワーク全体のデータ通信をキャプチャするには、このポートをミラーポートとして使用する必要があります（つまり、監視対象ポート）、このポートのデータを指定した監視ポートにコピーします。ここでは、例として f5 / 1 を取り上げます。つまり、f5 / 1 をミラーポート（監視ポート）として使用し、次にホストを使用します。 Colasoft Capsa がインストールされている場合は、f5/1 ポートに接続できます。 上記の要件に基づいて、ポートミラーリングの構成は次のようになります:

ミラーリングされたポートを構成:

```
Switch(config)# monitor session 1 source interface fastethernet 5/48
```

ミラーポートを構成:

```
Switch(config)# monitor session 1 destination interface fastethernet 5/1
```

構成が完了し、構成を表示できます:

```
Switch# show monitor session 1
```

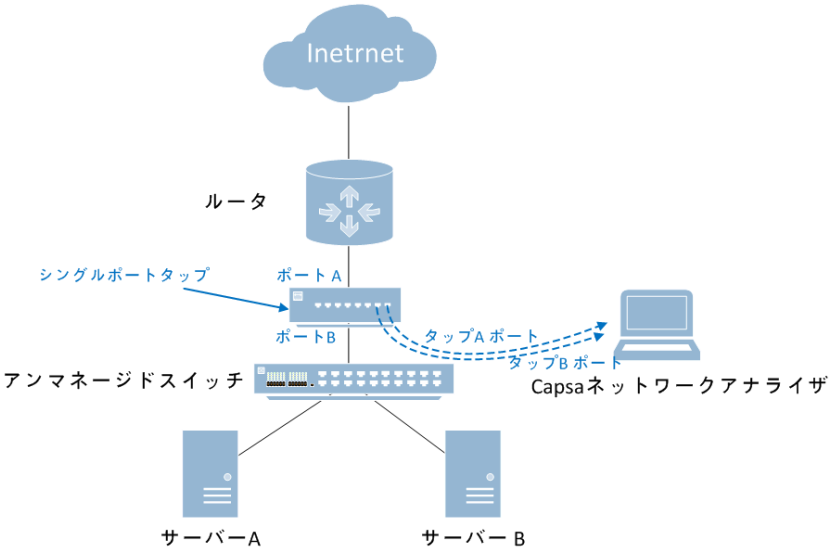
3.3 スイッチドネットワーク - アンマネージドスイッチ

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。以下に示すように、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。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ネットワークタップの使用（タップ）

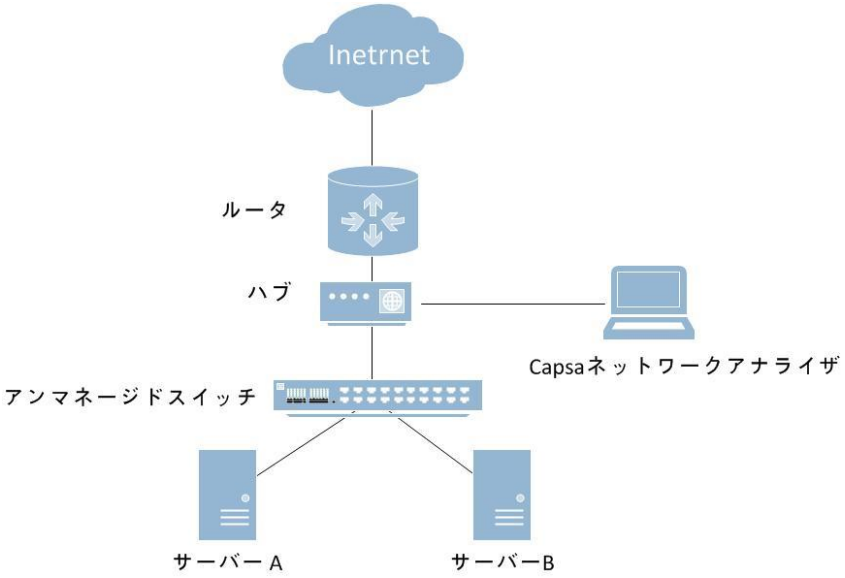
Tap を使用する場合、コストが高く、デュアルネットワークカードをインストールする必要があり、管理マシンはインターネットにアクセスできません。インターネットにアクセスする場合は、別のネットワークカードをインストールする必要があります。



ハブの使用（ハブ）

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。

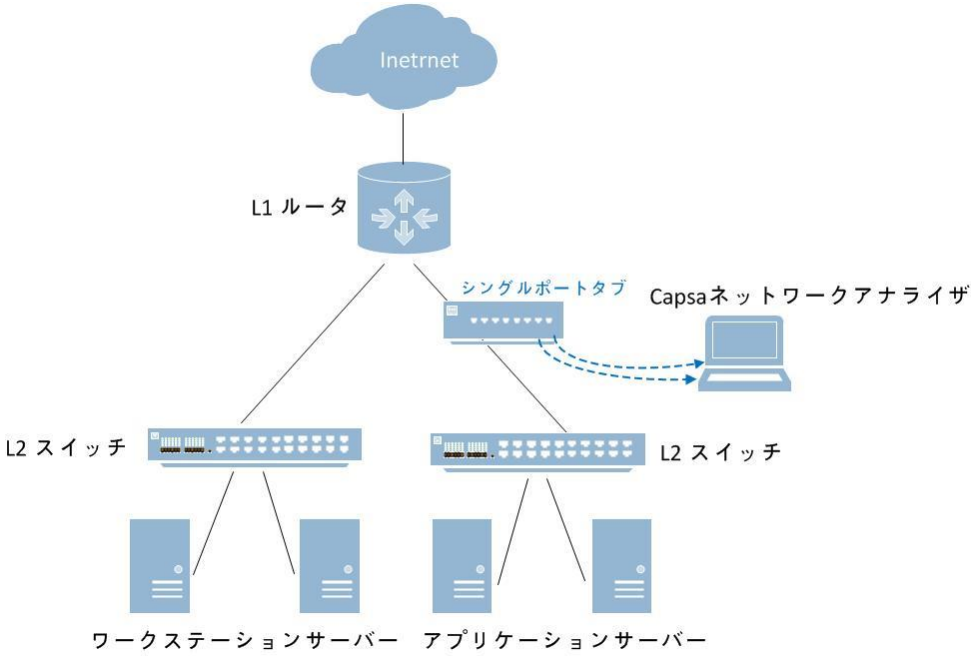
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



3.4 ネットワークセグメントの定点分析

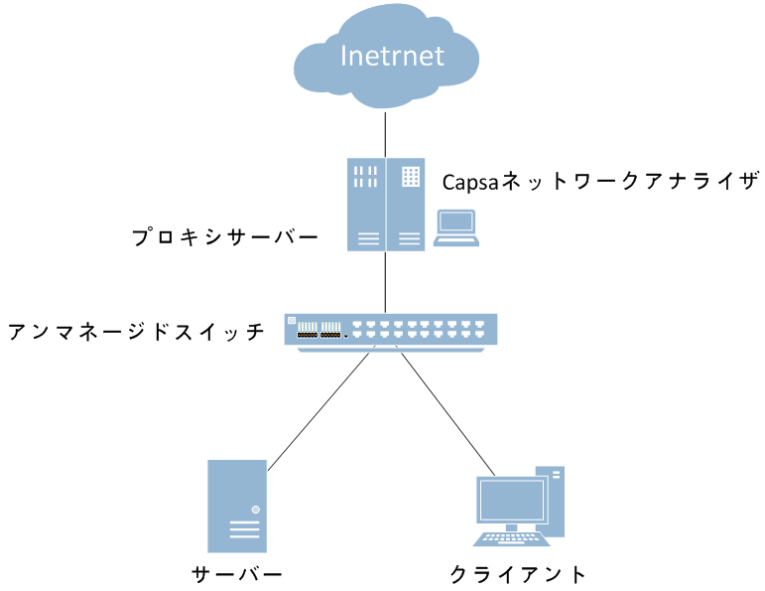
多数のネットワークノードを持つ一部のユーザーの場合、ネットワークトポロジは比較的複雑になる可能性があります。実際のネットワーク分析および監視では、ネットワーク全体を分析する必要がない場合があります。この場合、特定のネットワークのみを分析する必要があります。異常分析用の部門またはVLAN。 そのため、モバイルコンピュータにケライネットワーク解析システムをインストールし、タップやハブを接続することで、あらゆる部門やネットワークセグメントのデータキャプチャを簡単に実現できます。インストールは簡単です。写真は次のとおりです。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



3.5 プロキシサーバーの使用

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。



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

3.6 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、https://www.colasoft-japan.com

をご参照ください。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

4 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、以前のバージョンを完全にアンインストールしてください。製品をインストールするときは、システム要件と Readme.txt ファイルをよくお読みください。

4.1 インストール

インストールする前に、実行中の他のすべてのプログラムを閉じてください。インストールプログラムは.exe 実行可能ファイルです。このファイルをダブルクリックして、製品のインストールウィザードに入ります。

1. 使用許諾契約をよくお読みください。インストールを続行するには、使用許諾契約に同意する必要があります。続行するには、[次へ]をクリックしてください。
2. プログラムのインストールパスを指定し、[次へ]をクリックして続行してください。
3. ンストーラーがスタートメニューにショートカットを作成し、[次へ]をクリックして続行します。
4. デスクトップアイコンとクイック起動アイコンを作成するかどうかを選択し、[次へ]をクリックして続行します。
5. インストールウィザードがインストール構成を作成しました。正しいかどうかを確認し、正しいことを確認して、[インストール]ボタンをクリックすると、プログラムがコンピューターに自動的にインストールされます。
6. プログラムのインストール後、Readme.txt ファイルが表示され、Colasoft Capsa を起動するかどうかのプロンプトが表示されます。

4.2 アンインストール

アンインストール実行プログラムを選択し、アンインストールウィザードの指示に従って製品のアンインストールを完了し、コンピュータを再起動します。

次の方法で製品のアンインストールを実行することもできます:

1. Windows のコントロールパネルを開きます。
2. [プログラムの追加と削除]を選択します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

3. リストから「Colasoft Capsa」を選択し、ダブルクリックするか、削除ボタンを選択します。

4.3 システム要件

より高い構成の Windows オペレーティングシステムに製品をインストールすることをお勧めします。最小システム要件を提供します。ネットワークが比較的大きく、大量のネットワークトラフィックを分析する必要がある場合は、推奨される構成を使用して製品をインストールできます。。

最小構成

- CPU：Intel Core2 Duo 2.0GHz
- メモリ：4GB
- ブラウザ：Internet Explorer 8.0

推奨システム要件

- CPU：Intel Core2 Quad 3.2GH
- メモリ： 8GB 以上
- ブラウザ：Internet Explorer 11.0 以上

サポートしている Windows オペレーションシステム

- Windows 7 SP1（KB3033929）(64-bit)
- Windows Server 2012/2012 R2/2016/2019 (64-bit)
- Windows 8.1 (64-bit)
- Windows 10 (64-bit)
- Windows 11 (64-bit)

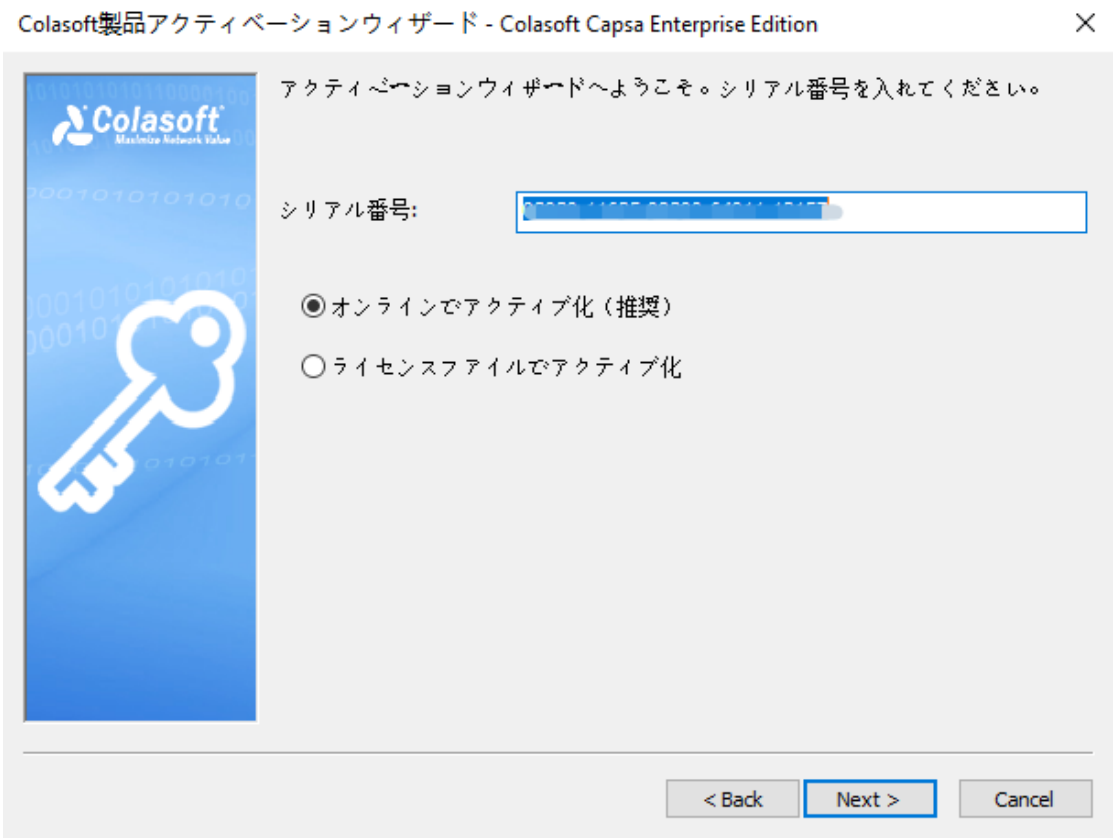
注：Colasoft Capsa をインストールする場合は、Administrator の権限または Administrators グループの権限でインストールする必要があります。

4.4 製品ライセンス

システムをインストールして初めて実行すると、製品のシリアル番号を入力するように求めるダイアログボックスが表示されます。 認証ファイルに従って認証情報を正しく入力し、「OK」をクリックしてください。認証情報が保存され、このダイアログボックスは表示されなくなります。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

認証ファイルは通常、電子メールで送信され、システムの操作と使用に必要なすべての情報が含まれています。 後で使用できるように、認証ファイルを安全な場所に保管してください。 製品のシリアル番号は、製品の外装またはユーザー情報カードに記載されています。認証文書、シリアル番号などに関連するすべての契約条件は、ライセンス契約に準拠しています。



4.5 製品アクティベーション

製品のアクティベーションは、著作権侵害を防止するための手段であり、正当なユーザーの権利と利益を保護するための効果的な手段です。 製品ライセンスは、1 つのサーバー（または PC）にのみバインドできます。製品が正常にアクティブ化された後は、製品を再インストールしても、再度アクティブ化する必要はありません。 ただし、オペレーティングシステムが再インストールされているため、製品を再アクティブ化する必要があります。 Colasoft Capsa は 2 つのアクティベーション方法を提供します:

オンラインでアクティブ化

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

これが最も簡単な方法です。オンラインアクティベーションをクリックする限り、システムは認証検証のために製品サーバーに接続します。 このプロセスは数秒で完了しますが、インターネットに接続するためにマシンをインストールする必要があります。

ライセンスファイルでアクティブ化

この方法は、設置機がインターネットに接続できない場合やオンラインアクティベーションに失敗した場合の操作方法です。 ユーザーは、「製品のシリアル番号」、「製品のインストール番号」、「製品のバージョン番号」を電子メールまたはファックスで送信できます。ユーザーの情報を受け取ったら、製品認証ファイルをユーザーに返し、認証をインポートします。アクティベーションウィザードにファイルして、製品のアクティベーションを完了します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

5 クイック使用

製品のインストールと登録が完了したら、まず、分析モードの選択、ネットワークアダプターの選択、分析設定の選択など、製品の基本的な操作を理解する必要があります。

この章では、次の章で紹介する内容についても説明します:

- 分析プロジェクト
- システム構成
- メインデータビュー
- 解析設定
- エキスパート診断

5.1 起動方法

製品のインストールが完了すると、「デスクトップ」と「スタートメニュー」にシステムショートカットが作成されます。Colasoft Capsa は、以下の方法で起動できます。

- デスクトップアイコンを使用

  デスクトップにショートカットを作成する場合は、オペレーティングシステムのデスクトップにある Colasoft Capsa アイコンをダブルクリックしてプログラムを開始できます。

- クイック起動バーを使用

  クイック起動バーの Colasoft Capsa アイコンを使用して、プログラムを開始します。

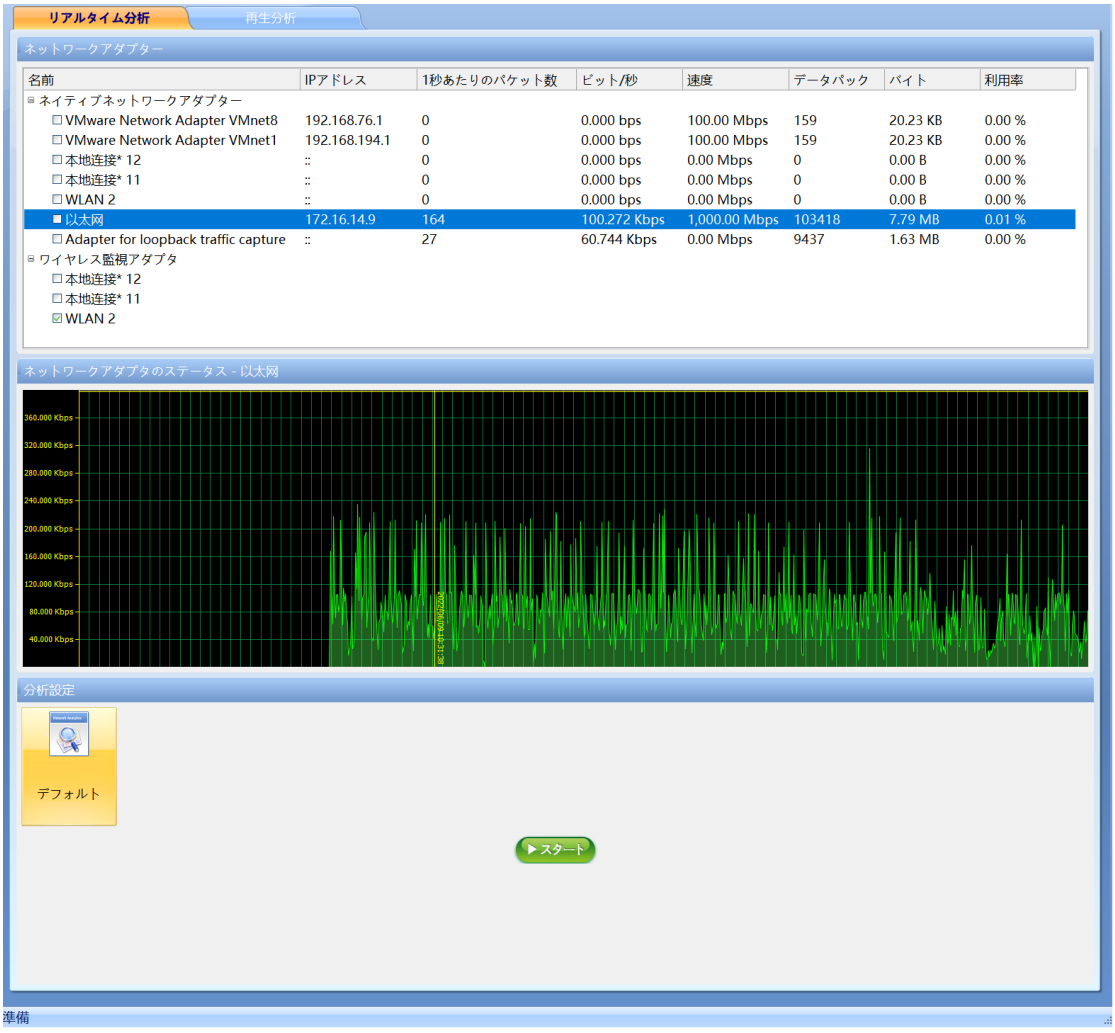
- スタートメニューを使用

  スタートメニューを開き、すべてのプログラムを選択し、Colasoft Capsa をクリックしてプログラムを開始します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

5.2 システムブート

Colasoft Capsa を実行するには、データ収集を開始する前に、システムブートページでデータをキャプチャする前に、関連する設定を実行する必要があります。 次の図に、システムの起動ページを示します:



システムの起動ページには、少なくとも次の 4 つの手順が含まれています。

1. 分析モードを選択
2. ネットワークアダプタを選択
3. 分析設定
4. 分析を開始

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

Tips

分析設定は、フィルター、データストレージ、ログ、診断などの設定を提供します。分析を開始する前に、分析設定のアイコンをダブルクリックできます。

5.3 分析設定の選択

Colasoft Capsa は、デフォルトでネットワークビジネスアプリケーションに共通の分析設定を提供します。 さまざまな分析要件に応じて分析設定を追加または編集し、分析対象のよりターゲットを絞った分析設定を選択できます。

5.4 ネットワークカードを選択

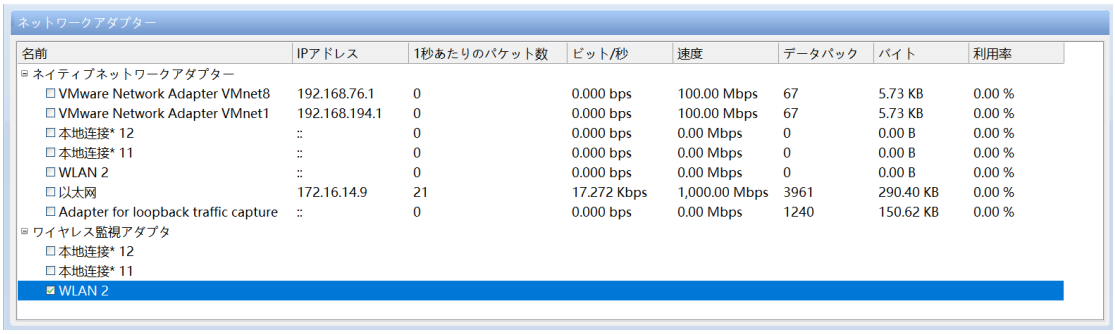
ネットワーク通信データパケットはネットワークカードを介して転送されます。データパケットキャプチャはネットワークカードによって収集される必要があります。データをキャプチャする前に、データを収集するためのネットワークカードを選択する必要があります。

Colasoft Capsa は、現在のシステムにインストールされているネットワークカードと IP アドレス、MAC アドレス、データパケットなどの関連パラメータ情報を自動的に検出および識別できます。ネットワークカードのトラフィックトレンドグラフがグラフィカルに表示されるため、ユーザーはデータのキャプチャに使用するネットワークカードを選択するのに便利です。 また、Colasoft Capsa は、ワイヤレスネットワークカードのデータ収集もサポートしています。

さらに、有線ネットワークカードデータを収集する場合、Colasoft Capsa はデータ収集用に複数のネットワークカードをサポートします。つまり、2 つ以上のネットワークカードを同時に選択してデータをキャプチャし、データ集約分析を自動的に実行できます。

ガイドインターフェイスの[ネットワークアダプタの選択]ボタンをクリックすると、Kelai ネットワーク分析システムが利用可能なすべてのネットワークカードタイプを自動的に一覧表示し、ユーザーは実際の状況に応じて選択できます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



5.5 AP を選択

ユーザーがパケットキャプチャ分析用のワイヤレスネットワークカードを選択した場合は、対応するワイヤレス AP を選択する必要があります。Colasoft Capsa は、近くの AP リストを自動的に検出して識別し、ユーザーは分析要件に従って対応するワイヤレス AP を選択できます。 AP を選択するとき、ユーザーは正しい AP パスワードを入力する必要があります。そうしないと、システムはキャプチャされたデータパケットを復号化できません。

Note

AP がパスワードを設定しない場合は、直接接続でき、システムは暗号化されていないデータを自動的にキャプチャして分析します。

5.6 パケットのキャプチャ

ネットワーク分析を実行するには、ネットワーク内のデータパケットをキャプチャする必要があります。次に、キャプチャされたデータパケットに対して統計分析を実行することにより、現在のネットワーク状態を理解できます。

通常、ガイド付きインターフェースでは、データを収集するネットワークアダプターを選択し、フィルターと対応する分析設定を設定してから、[分析の開始]ボタンをクリックして、ネットワーク通信データの収集と分析を開始できます。

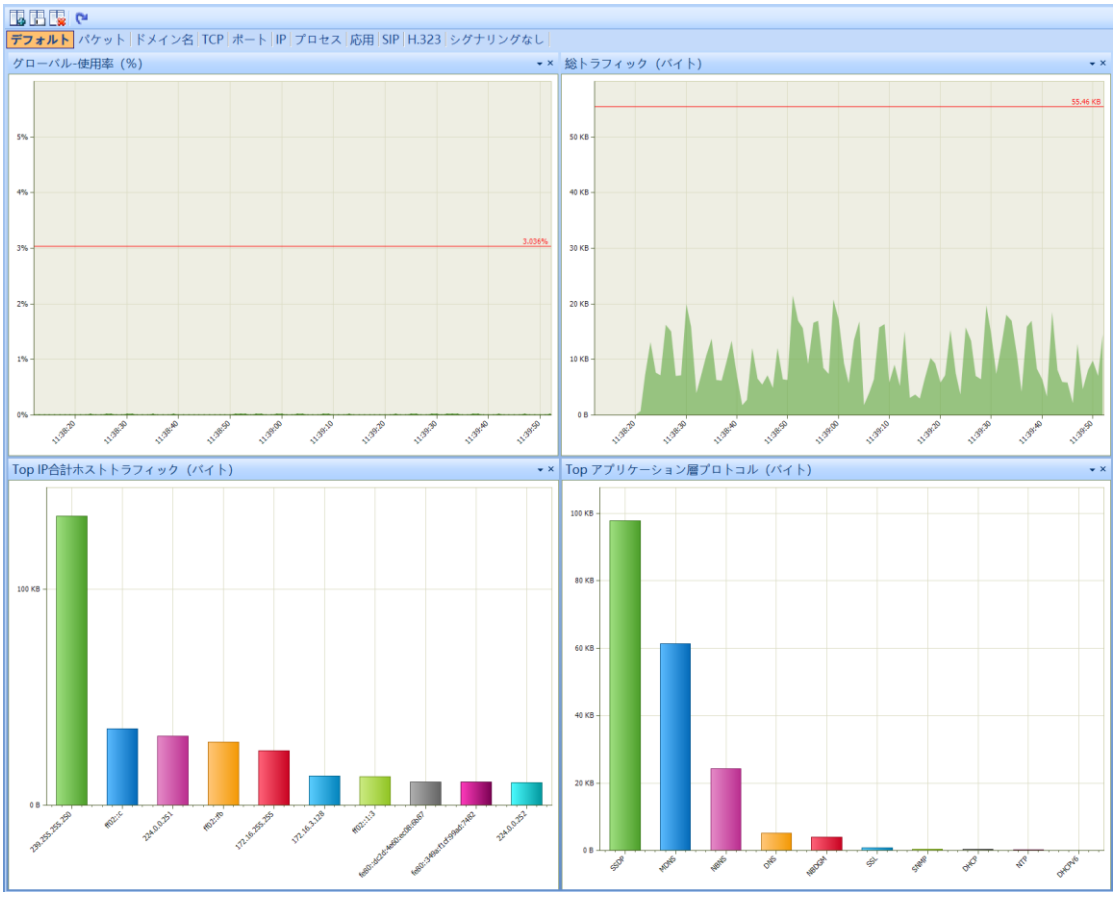
5.7 カスタムチャート

Colasoft Capsa は、まったく新しいチャートビューを提供し、ユーザー定義のチャートの機能を提供します。システムが提供するデフォルトのチャートに加

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

えて、ユーザーはチャートパネルを簡単にカスタマイズおよび追加できます。各チャートパネルは、新しいチャートを自由に追加できます。

チャートビューは、統計分析データをより直感的で読みやすくし、折れ線グラフ、棒グラフ、面グラフ、円グラフなど、ネットワークデータの傾向を簡単に示すことができるさまざまな形式を提供します。



システムはデフォルトで 1 つのチャートパネルと 3 種類のチャート表示を提供します。このビューで新しいチャートパネルを作成し、新しく作成されたパネルに表示されるチャートのタイプを追加できます。システムはリアルタイムの収集チャート監視を提供します。および TOPN シリーズチャートでは、自由に追加することができます。

5.8 カスタムアラート

Colasoft Capsa は、ユーザー定義のアラーム機能を提供します。 アラートビューでグローバルアラートを設定したり、複数のビューで個々のネットワーク

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

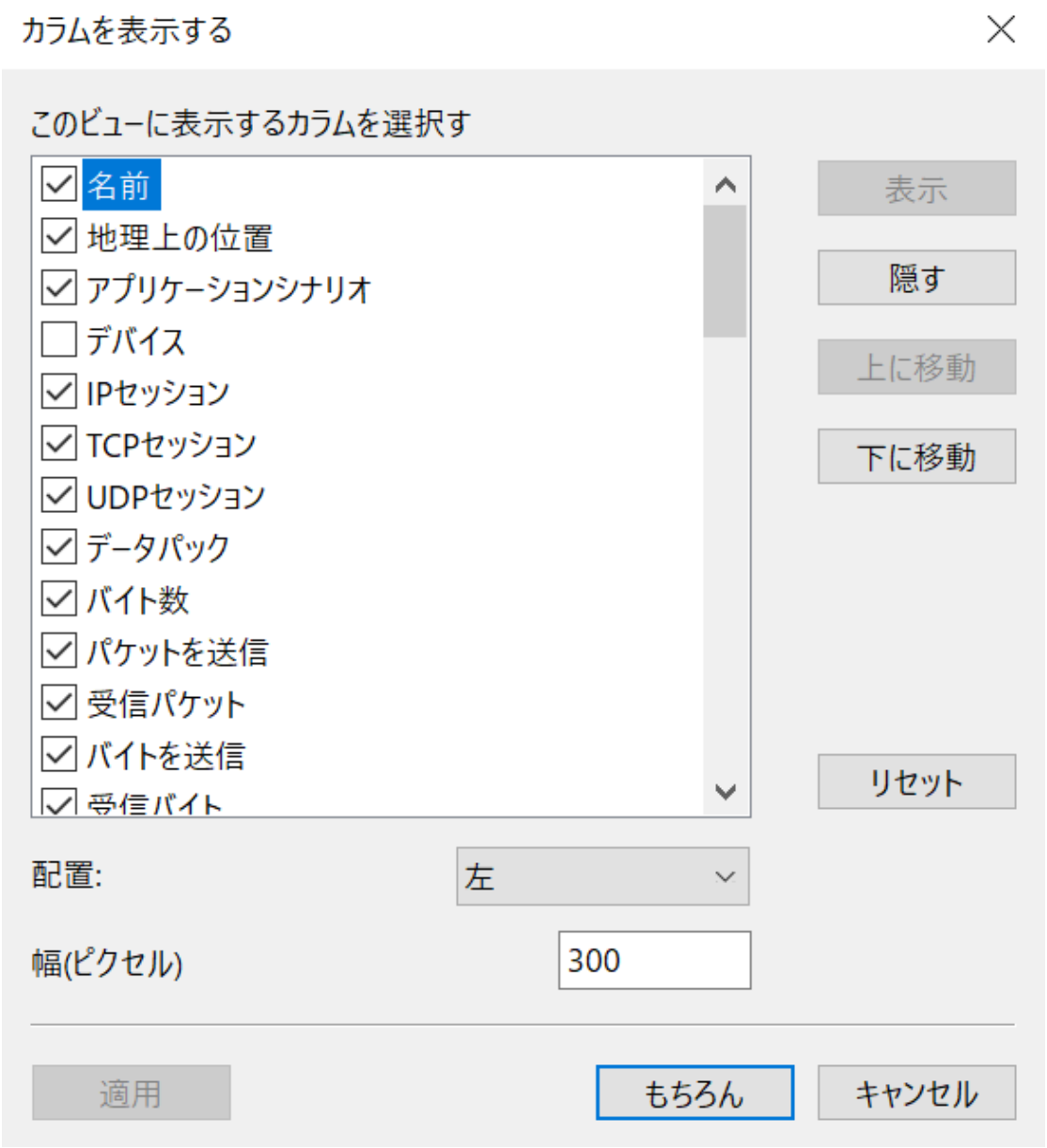
オブジェクトのアラートを作成したりできます。 また、アラームログを自動保存する機能を備えています。

すべてのアラームは、安全性、パフォーマンス、障害に応じて 3 つのカテゴリに分類されます。アラーム統計管理領域は、主にツリーのような階層的方法を採用して、作成したすべてのアラームを効果的にカウントおよび表示します。ここで作成するアラートを管理することもできます。たとえば、アラートプロパティの変更、不要なアラートの却下、新しいアラートの作成などです。

5.9 カスタムビューの表示列

Colasoft Capsa の各分析ビューエリアは、ユーザーに非常に豊富な統計フィールドを提供しますが、表示に適したものにするためにすべてのフィールドが表示されるわけではありません。 ユーザーは、リストオプションを使用して表示データを設定し、各ビューフィールドヘッダーを右クリックして[ビューのカスタマイズ]ダイアログを開くことができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



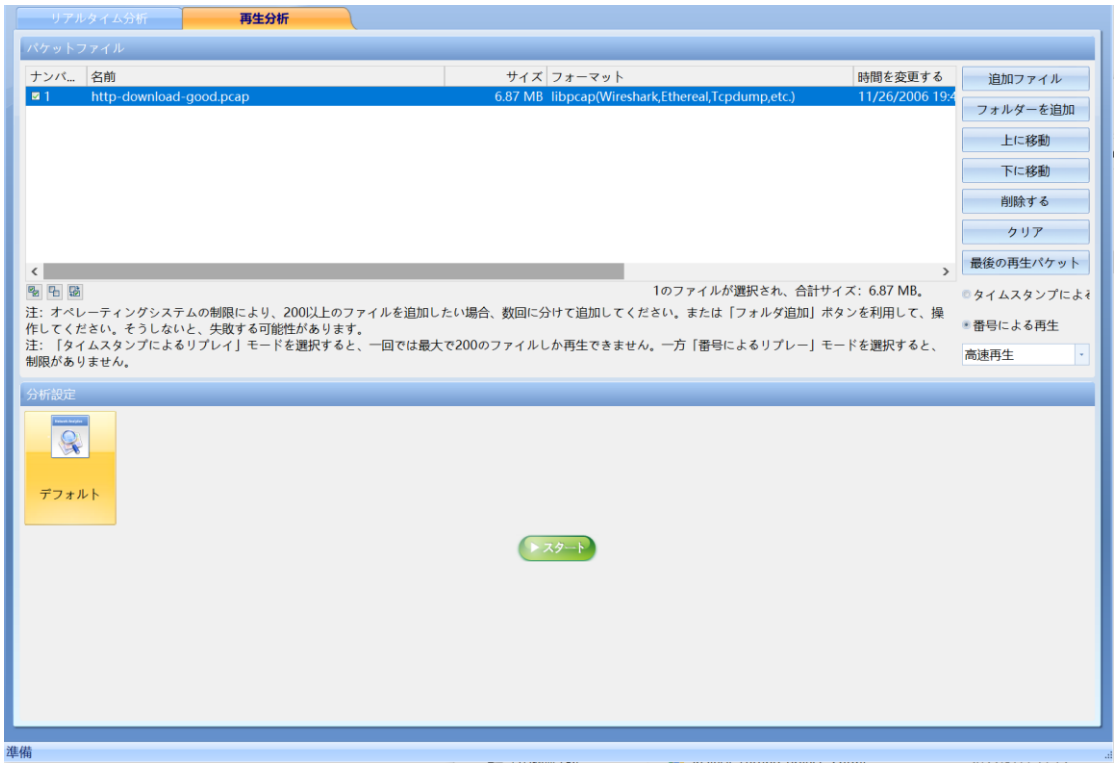
5.10 データの並べ替え

データの並べ替えは、データを表示するときに非常に便利な機能です。 たとえば、特定の種類のデータを表示する必要がある場合、ネットワークトラフィックの IP アドレスを大から小、または小から大に表示する必要があります。リストのフィールドをクリックするだけで、次のことができます。以下に示すように、大きいものから小さいものへ、または小さいものから大きいものへと順番に配置されます。

データの並べ替えを使用して、帯域幅が最も多い IP を検索したり、パケットが

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

最も多い IP を検索したりするのは非常に簡単な方法です



データソート機能は、物理エンドポイントビュー、IP エンドポイントビュー、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 セッションビューのすべての統計パラメータに適用されます。

5.11 データのコピー

データ範囲を選択し、右クリックして、単一行または複数行のコピー、単一列または複数列のコピーなどのコピー方法を選択します。 Colasoft Capsa は、次のようなさまざまなデータ複製方法を提供します。

コマンド	説明
コピー	選択範囲をテキストとしてコピーします。
ツリー構造をコピー	マウスが配置されているツリーのすべてのデータをコピーします。
Hex をコピー	パケットデコードで Hex 形式のコンテンツをコピーします。
テキストをコピー	パケットのデコードされたテキストコンテンツをコピーします。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

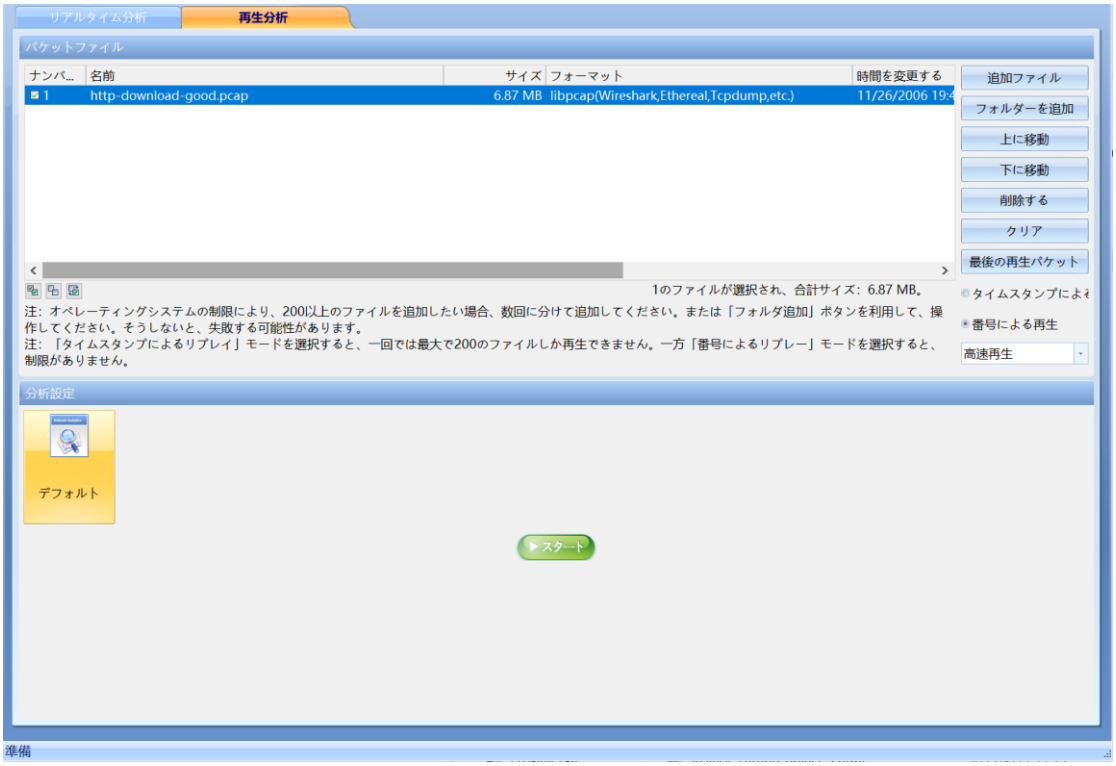
データ列のコピー	指定されたデータ列（フィールドコンテンツ）をコピーします。

ヒント：コピーしたコンテンツは、Excel、Word、およびその他のテキストエディタに貼り付けることができます。

5.12 再生とエクスポート

再生

以下に示すように、Colasoft Capsa は、さまざまな一般的なデータパケット形式の再生インポートと分析をサポートしています。ガイドインターフェイスで[再生分析]モードを選択して、再生分析用のデータパケットファイルをインポートできます:



「追加」ボタンをクリックして、分析のために再生する必要のあるパケットファイルを選択します。再生分析を実行する前に、特定のデータを分析するためのフィルターを設定できます。 さらに、再生分析では、元の速度の再生、高速再生など、さまざまな分析設定とさまざまな再生速度を選択し、関連する条件

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

を設定した後にデータパケットのインポートを開始することもできます。

データパッケージのインポートプロセス中に、ツールバーの[インポートの一時停止]または[インポートの停止]ボタンをクリックして、データパッケージのインポートをいつでも一時停止または停止できます。

Colasoft Capsa でインポートおよび再生用にサポートされているパケット形式は次のとおりです:

- Colasoft Packet File（v6） (*.cscpkt)
- Colasoft Raw Packet File（*.rawpkt）
- Accellent 5Views Packet File（*.5vw）
- EtherPeek Packet File（V9） (*.pkt)
- HP Unix Nettl Packet File（*.TRCO;TRC1）
- Libpcap（tcpdump,Ethereal,etc.） (*.cap)
- Microsoft Network Monitor2.x（*.cap）
- Novell LANalyer（*.tr1）
- Network Instruments Observer v9.0（*.bfr）
- NetXRay2.0,and Windows Sniffer（*.cap）
- Sun_Snoop（*.Snoop）
- Visual Network Traffic Capture（*.cap）

エクスポート

キャプチャしたデータを保存するために、パケットファイルを特定の形式にエクスポートすることもできます。 Colasoft Capsa は、基本的な cscpkt 形式をサポートするだけでなく、Sniffer や Omnipeek などの一般的なツールのファイル形式もサポートしています。 エクスポートをカスタマイズして、パッケージファイルをさまざまな形式で保存できます。

[ファイルの種類]のドロップダウンリストボックスをクリックして、次の種類のパケット形式で保存します:

- Colasoft Packet File（v6） (*.cscpkt)
- Colasoft Raw Packet File（*.rawpkt）
- Accellent 5Views Packet File（*.5vw）
- EtherPeek Packet File（V9） (*.pkt)
- HP Unix Nettl Packet File（*.TRCO;TRC1）

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- Libpcap（tcpdump,Ethereal,etc.）（*.cap）
- Microsoft Network Monitor2.x（*.cap）
- Novell LANalyer（*.tr1）
- Network Instruments Observer v9.0（*.bfr）
- NetXRay2.0,and Windows Sniffer（*.cap）
- Sun_Snoop（*.Snoop）
- Visual Network Traffic Capture（*.cap）

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

6 分析プロジェクト

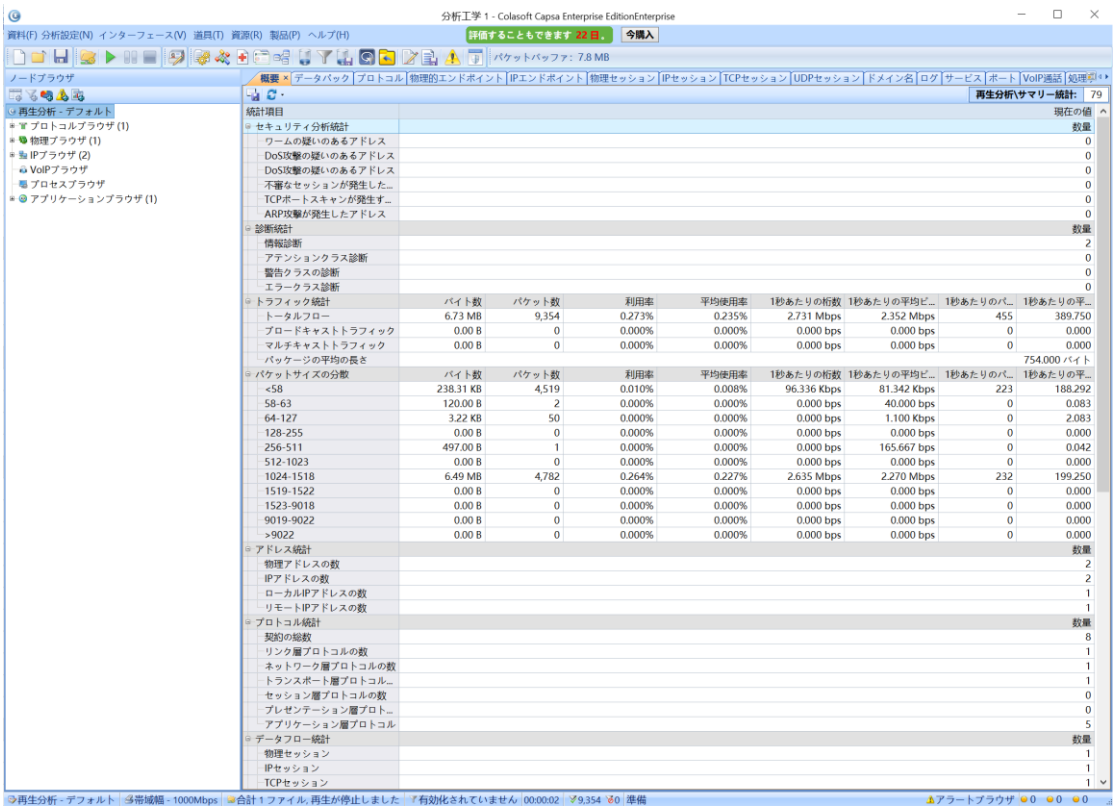
分析プロジェクトは、データソース、ネットワーク環境、フィルター、分析設定、分析結果を含む分析タスクのキャリアです。分析設定は、分析プロジェクト全体の焦点です。 ユーザーは、分析プロジェクトを開始して分析セットアップを実装します。

エンジニアリングは分析タスクとして理解できます。 さまざまな分析タスクに応じてさまざまなフィルターと分析設定を選択し、より的を絞ったネットワーク分析を完了することができます。

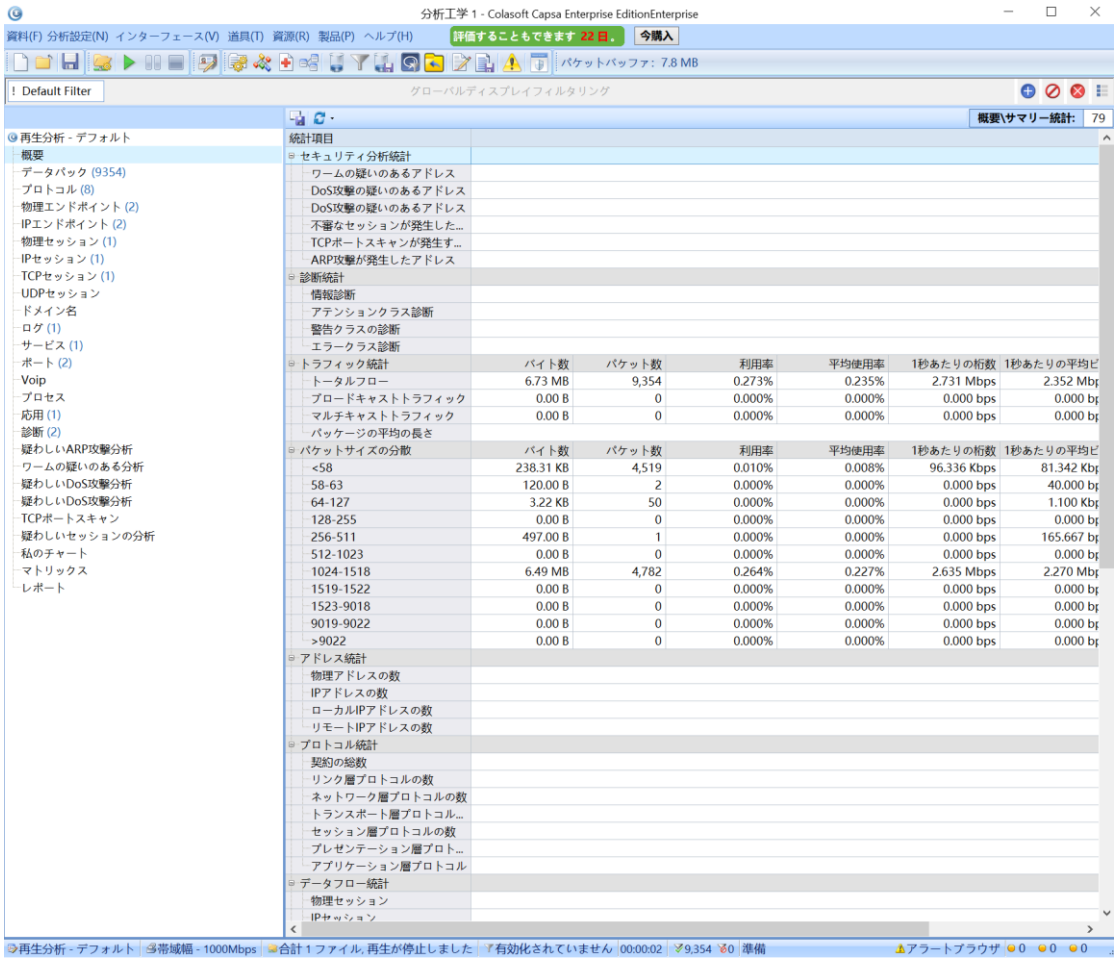
6.1 メインインターフェースの概要

開始データがキャプチャされた後、プログラムのメインインターフェイスは次のようになります。

グローバルフィルターが有効になっていません:



グローバルフィルターを有効にします:



製品のメインインターフェイスは、主にタイトルバー、機能領域、グローバル表示フィルター、ノードブラウザー、メインビュー領域、アラームブラウザー、分析ステータスバーの 6 つの部分で構成されています。

- タイトルバー：分析プロジェクトを表示します。
- リボン：システムメニューとショートカットツールバーを含め、詳細は「**リボン**」の紹介を参照してください。
- グローバル表示フィルター：グローバル表示フィルターを表示および構成します。
- ノードブラウザ：グローバル表示フィルターが有効になっていない場合は、プロトコルエンドポイント、物理エンドポイント、IP エンドポイント、VoIP ブラウザーを提供して、ノードデータのフィルタリングとクイックポジショニングを行います。グローバル表示フィルターを有効にする場合は、グラフ、要約統計、診断、物理エンドポイント、IP エンドポイント、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、プロセス、アプリケーション、クライアント、VoIP コール、ポート、

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

マトリックス、パケット、ログ、およびレポートビューの切り替えを提供します。

- メインビューエリアには、チャート、要約統計量、プロトコル、物理エンドポイント、IP エンドポイント、IP セッションなどの合計 14 のビューエリアが含まれます。
- アラームブラウザ：カスタマイズして、アラームを作成、削除、および管理します。
- 分析ステータスバー：分析ステータスバーには、データキャプチャステータスやトリガーされたアラームの数などの情報がリアルタイムで表示されます。

リボン

機能領域は、[ファイル]、[分析設定]、[詳細設定]、[インターフェイス]、[ツール]、[リソース]、[製品]、[ヘルプ]の 8 つのメニュー項目と、いくつかのショートカットボタンを備えたツールバーに分かれています。

ノードブラウザ

ノードブラウザは主にノードの場所とデータのフィルタリングを提供し、ユーザーがプロトコル、物理アドレス/グループ、IP アドレス/グループ、VLAN などの表示するノードをすばやく選択できるようにします。 ノードブラウザを介してノードを特定することにより、システムはノードの通信データをすばやくフィルタリングします。これにより、障害の原因の特定と分析が容易になります。

メインビューエリア

メインビューエリアは、システム分析結果の出力エリアです。すべての分析、診断、および統計データは、メインビューエリアの各ビューに表示されます。メインビューエリアはウィンドウの右側にあります。分析設定が異なると、出力データの結果も異なります。 メインビュー領域には、主に、チャート、要約統計ビュー、プロトコル、物理エンドポイント、IP エンドポイント、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、マトリックスビュー、パケットデコードなどの 14 のビューが含まれます。 対応する[表示]タブをクリックして、対応するネットワーク分析データを表示します。

アラートブラウザ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

アラームビューエリアでは、アラームタイプ（安全性/パフォーマンス/障害）、アラームトリガー条件、アラームトリガー値、アラームリリース条件、および上位 10 の物理アドレス、IP アドレス、またはプロトコルの設定など、さまざまなタイプのアラームを作成できます。アラームがトリガーされます。 アラームがトリガーされると、このビュー領域にリアルタイムで通知および表示され、管理者は現在トリガーされているアラーム情報を直感的に確認できます。

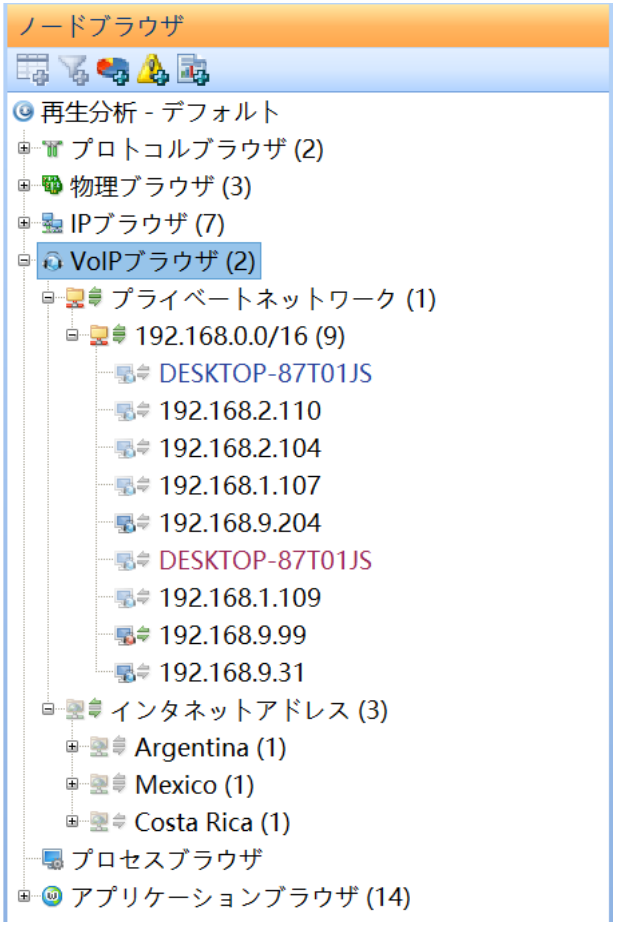
分析ステータスバー

ステータスバーはメインインターフェイスの下部にあり、主に現在使用されている分析モードと分析設定を識別するために使用されます。ここでローカル接続をクリックすると、データのキャプチャに現在使用されているネットワークアダプターを表示および変更することもできます。

6.2 ノードブラウザ

ノードブラウザは、Colasoft Capsa のユニークな機能です。その高速なノードロケーションとデータフィルタリングにより、障害分析が容易になり、ネットワーク分析の効率が大幅に向上します。その最大の目的は、表示するノードをすばやく選択することです。ノードを選択することで、ユーザーはそのノードに対応するネットワークデータを表示できます。 ノードブラウザは、プロトコルノード、物理ノード、IP ノードの 3 つのクラスで構成されています。 ユーザーは、ネットワーク全体を簡単に見つけたり、特定の IP セグメントまたは特定の IP を見つけたりすることができます。 右側の表示領域には、選択したノードに応じた関連データ情報が表示されます。

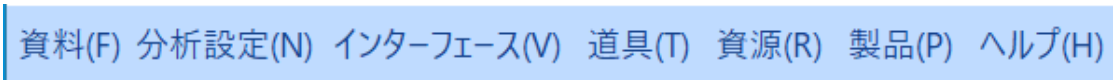
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



6.3 リボン

リボンはメニューバーとツールバーで構成されています。

メニューバー



ファイル

- 新しいプロジェクト：新しい分析プロジェクトを作成します。
- プロジェクトを閉じる：現在の分析プロジェクトを閉じます。
- データパッケージのエクスポート：キャッシュされたデータパッケージをエクスポートします。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- グローバル構成のインポートとエクスポート：グローバル構成をインポートおよびエクスポートします。
- 印刷：ビューの内容を印刷します。
- システムオプション：システム構成ページを開きます。
- メモ：メモを管理します。
- 終了：ソフトウェアを閉じます。

解析設定

- 基本設定：ネットワーク帯域幅、メディアタイプ、分析モジュールの選択などを設定します。
- 分析対象：分析対象データを設定します。
- 診断：診断項目の情報を設定します。
- ビューの表示：表示された分析ビューを管理します。
- ノードのグループ化：IP アドレスのグループ化情報を設定します。
- データパケット表示バッファ：データパケット表示バッファサイズを設定します。
- フィルター：パケットフィルターを管理します。
- データパッケージ保存：データパッケージ保存の構成情報を設定します。
- セッションフィルター：セッションフィルターを管理します。
- 復元：ファイル復元情報を設定します。
- ログ：ログバッファサイズを設定します。
- ログファイルの保存：ログファイルを保存するための情報を設定します。
- アラート：アラート構成を管理します。

インターフェース

- ノードブラウザ：ノードブラウザを表示/非表示します。
- アラームブラウザ：アラームブラウザを表示/非表示します。
- 物理アドレス表示形式：物理アドレスの表示形式を設定します。
- IP アドレスの表示形式：IP アドレスの表示形式を設定します。
- ウィンドウサイズ：ソフトウェアのメインウィンドウのサイズを変更します。

ツール

システムのデフォルトは、コーデック変換ツール、IP アドレスアトリビューションクエリ、デコードスクリプトエディター、Colasoft Ping ツール、Packet Builder、Packet Player 、MAC Scanner の 7 つのネットワークツールであり、サードパーティツールを追加するようにカスタマイズできます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

リソース

これは、Colasoft 関連のオンラインリソースのリンクです。主に、Colasoft ホームページ、CSNA コミュニティ、Colasoft ブログです。

製品

- 製品認証：ソフトウェアの登録と認証を提供します。
- 更新：ソフトウェアの最新バージョンを確認して入手します。

ヘルプ

ローカルヘルプドキュメントへのクイックアクセスを提供します。

ツールバー

次の図に示すように、ツールバーには、一部の操作とパケットキャッシュ情報の表示のショートカットがあります。

ツールバーは、左から新規プロジェクト、プロジェクトのクローズ、パッケージの保存、パッケージファイルの再生、開始、一時停止、停止、名前テーブル、基本設定、解析オブジェクト、診断、解析ビュー、ノードグループ化、パケットキャッシュ、フィルタ、パケット保存、セッションフィルタ、リストア、ログ、ログファイル保存、アラートの順です。

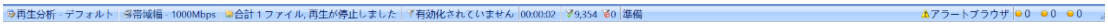
6.4 ステータスバー

システムのメインインターフェースには、リアルタイムのステータスバー表示があります。 ステータスバーから、次の情報を理解して設定できます:

- 分析設定：現在選択されている分析モードと分析設定を表示します。
- ネットワークアダプタ：現在データを収集しているネットワークカードを表示します。ここをクリックしてネットワークアダプタの設定を変更できます。
- フィルター：フィルター情報を表示します。ここをクリックすると、フィルター設定ダイアログボックスがポップアップ表示されます。
- キャプチャステータス：キャプチャ時間とキャプチャされたパケット情報を表示します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

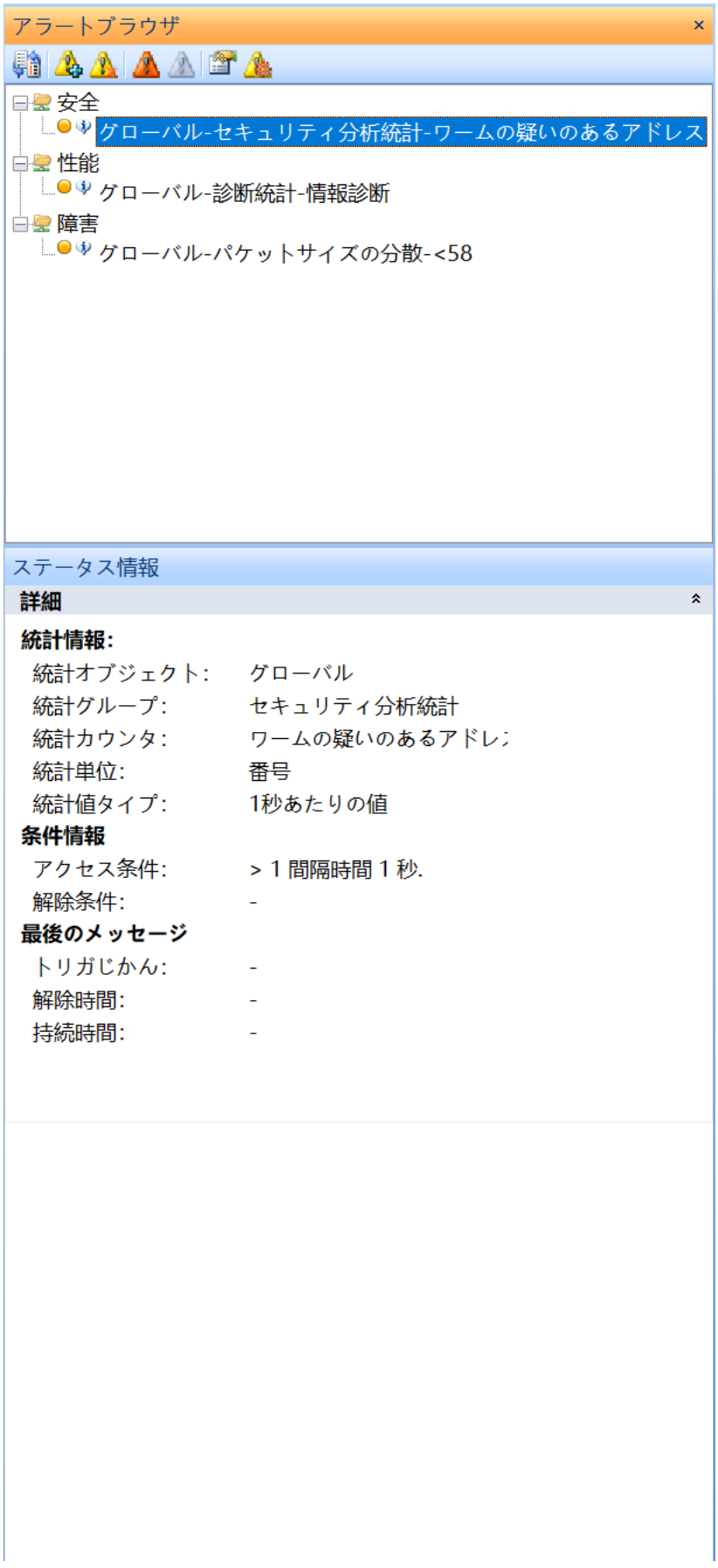
- アラーム情報：システムのアラームビューが最小化され、ここに表示されます。トリガーされた現在のネットワークアラームの数をすばやく表示できます。ここをクリックして、アラーム管理ビュー領域を開きます。



6.5 アラームブラウザ

アラームブラウザは、主にリアルタイムのアラームの作成と管理を提供し、管理者に目を引く方法で現在のアラームイベントを通知し、メインビューの右下隅にある現在トリガーされているアラームの数を最小限に抑えます。 ユーザーは、グローバルアラームを設定できるだけでなく、他のビューからネットワークオブジェクトを選択してアラームを作成することもできます。 アラートブラウザを以下に示します。

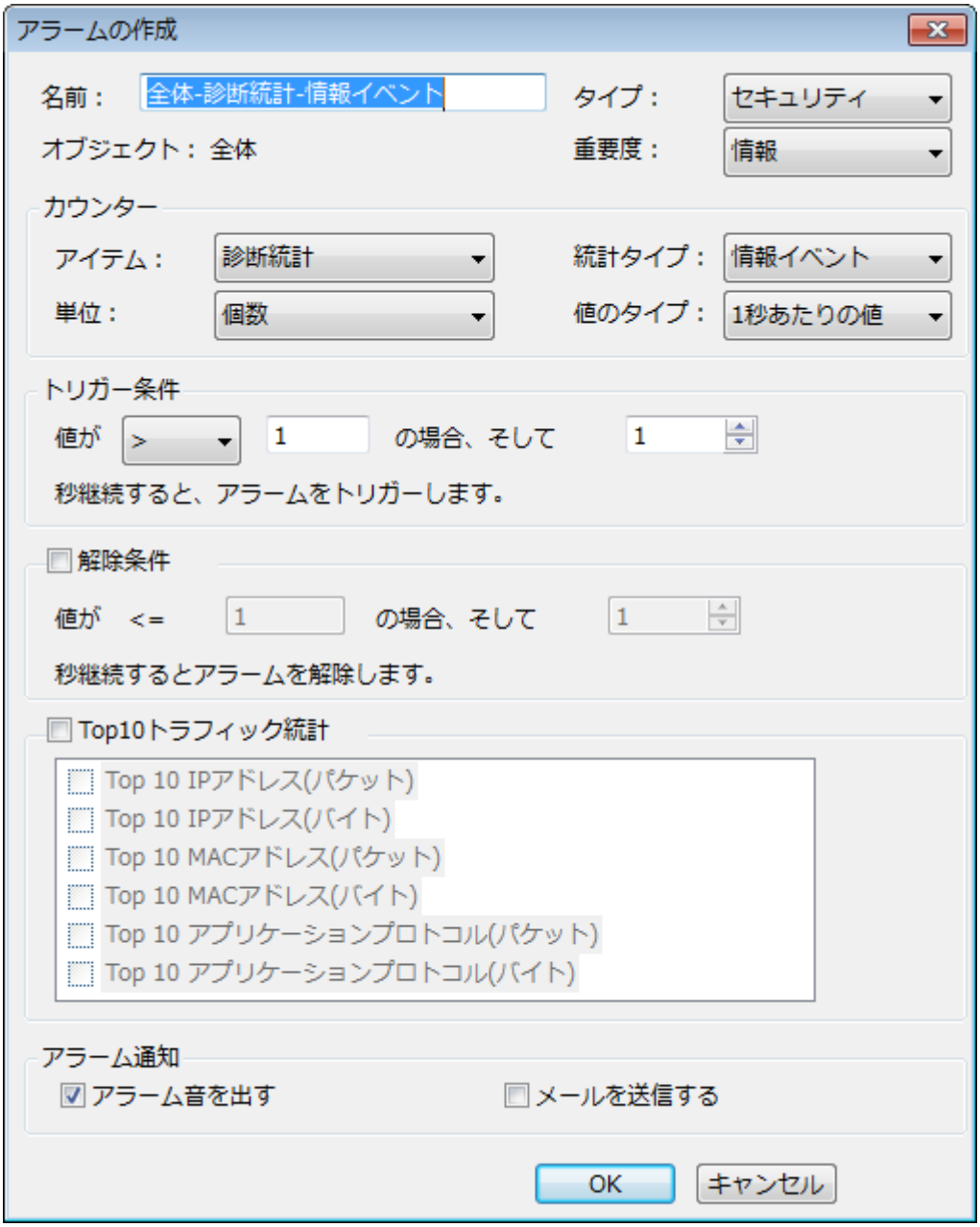
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

システムは、安全性/性能/障害の 3 つのタイプに応じてさまざまなアラームを作成できます。 さらに、アラームの種類ごとに、アラームがトリガーされたときの上位 10 個の物理アドレス、IP アドレス、およびプロトコルをカスタマイズして表示できるため、ユーザーはアラームがトリガーされたときのネットワークステータスを簡単に理解できます。

次の図に示すように、アラームブラウザのツールバーにある[アラームの追加]ボタンをクリックして、さまざまなタイプのアラームをカスタマイズおよび作成します。



このダイアログボックスでは、アラームの種類、重大度、アラーム状態、アラームをトリガーする値を設定し、アラームがトリガーされたときにネットワーク内の上位 10 個の

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

物理アドレス、IP アドレス、およびプロトコルを表示できます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

7 システムオプション

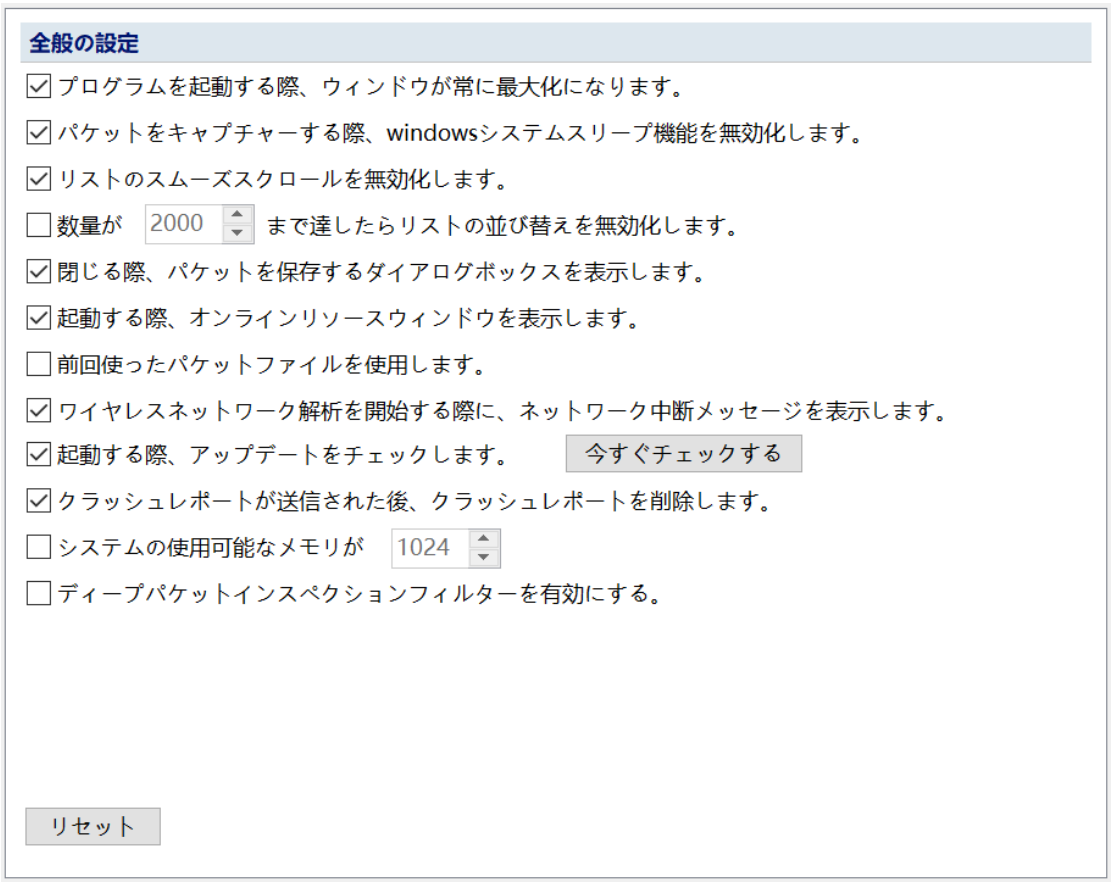
システムオプションには、一般的なシステム全体の設定が含まれています。 ユーザーは、これらの構成ダイアログボックスで事前に対応する設定を行うことができます。これにより、ネットワーク分析タスクを実行する際の分析効率を大幅に向上させることができます。 システムオプションの設定は、システムのメインメニューにあります。 ユーザーは、システムの左上隅にあるメインメニューボタンをクリックしてシステムメニューを開き、メニューの右下隅にある[システムオプション]ボタンをクリックして、システムオプションダイアログボックスを開くことができます。

[システムオプション]ダイアログには、次の 6 つの設定が含まれています:

- 一般：一般構成では、システムのいくつかの一般的な操作構成が提供されます。
- デコーダー：デコーダー構成は、Colasoft Capsa でサポートされるすべてのデコードモジュールを提供します。すべてのデコーダーはモジュラー設計に従って設計されており、ユーザーはさまざまなデコーダーを任意に選択して組み合わせることができます。 デフォルトでは、システムはすべてのデコードモジュールがパケットをデコードできるようにします。
- カスタマイズされたプロトコル：システムの識別と分析に便利な、不明なプロトコルまたはプライベートプロトコルのカスタマイズされた設定を提供します。
- タイミング解析：ネットワークデータのタイミング解析機能を実現するタイミング解析タスク設定を提供します。
- レポート：レポートヘッダー、作成者、作成時間など、システムレポートの一般的な設定を提供します。
- フォーマット：統計データの表示フォーマット設定を提供します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

7.1 一般



- 当运行科来网络分析系统时，系统总是最大化 Colasoft Capsa を実行すると、システムは常に最大化されます

  このオプションを有効にすると、Colasoft Capsa が実行されるたびにシステムが最大化されます。 システムはデフォルトで有効になっています。

- パケットをキャプチャするときに Windows システムのスリープ機能を無効にします

  人工または自動の休止状態とスタンバイを禁止するように Windows を設定します。 システムはデフォルトで有効になっています。

- リストのスムーズなスクロールを無効にします
  システム表示リストをスムーズにスクロールするかどうかを設定します。
  システムはデフォルトで有効になっています。
- 統計データが一定数に達した場合、リストの並べ替えは禁止されます

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

リストを並べ替える数の制限を設定します。システムのデフォルトは 2000 です。つまり、統計データリストが 2000 に達すると、サイズで並べ替えることができなくなり、カスタマイズおよび変更できます。

- 最後に分析されたパケットファイルを自動的にロードします
  このオプションを有効にすると、分析を再生するときに最後に再生されたパケットファイルが自動的にロードされます
- 無線ネットワーク分析を開始すると、ネットワーク中断のプロンプトが表示されます
- 起動時に更新を確認します
  このオプションを有効にすると、ソフトウェアは、ソフトウェアが起動するたびにバージョン更新情報を自動的にチェックします。

- クラッシュレポートを送信した後、クラッシュレポートファイルを削除します
- システムの使用可能なメモリが xx メガバイト未満になったら分析を停止します
  このオプションを有効にすると、分析中にシステムの使用可能なメモリが設定値を下回ると、分析が停止します。
- ディープパケットインスペクションフィルターを有効にします
  このオプションは、デフォルトで有効になっている DPI フィルターを使用するかどうかを制御します。
- 終了時に保存パッケージを表示します

データキャプチャを停止するとき、またはデータキャプチャ中に、システムからログアウトすると、データパケットを保存するかどうかを確認するメッセージが表示されます。これは、デフォルトで有効になっています。

7.2 デコーダー

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

システムでサポートされているすべてのデコーダーモジュールがここに一覧表示され、ユーザーはさまざまなデコーダーを任意に選択して組み合わせることができます。 デフォルトでは、システムはすべてのデコードモジュールがパケットをデコードできるようにします。

7.3 プロトコル設定

プロトコル設定には、HTTPS 復号化、RTP 構成、IEEE 802.11 構成、L2TPv3 構成が含まれます。

7.3.1 SSL/TLS

HTTPS 構成は、HTTPS パケットの復号化方法を構成するために使用されます。 HTTPS 暗号化方式に従って、さまざまな復号化構成を実行できます。 対応する復号化方法が設定された後、システムは対応するキーを使用して暗号化されたデータパケットをデコードできます。 インターフェイスは次のとおりで

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

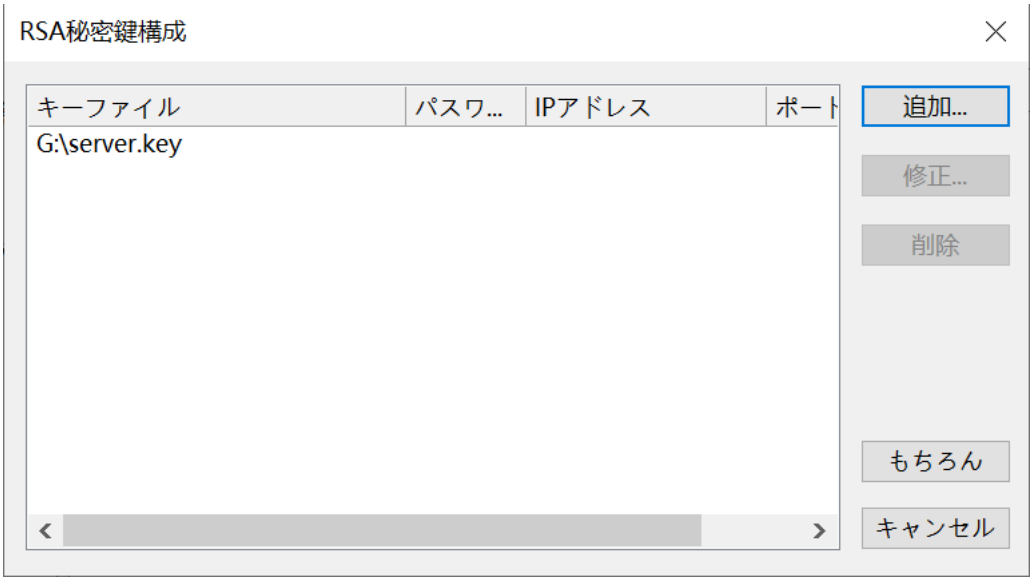
す。

現在、HTTPS の暗号化方式には、主に RSA、PSK、DH が含まれます。

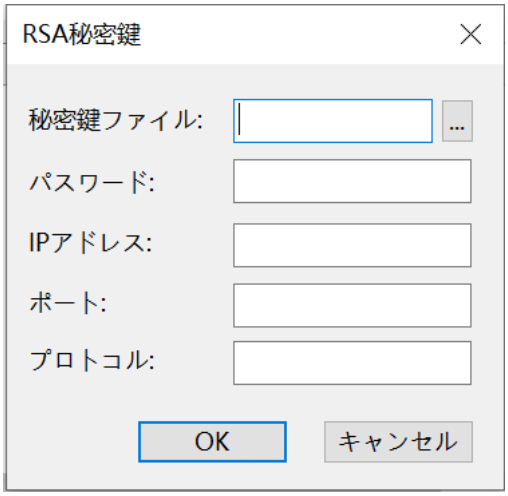
- RSA

以下に示すように、分析するデータパケットが RSA によって暗号化されている場合、「RSA キーファイルリスト」の後ろにある「編集」ボタンをクリックして、RSA キー設定ダイアログボックスに入ることができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



以下に示すように、「追加」をクリックして、ポップアップダイアログボックスに対応するキーファイルをアップロードします:



- キーファイル：RAS のキーファイルをアップロードします。アップロード後、システムはキーファイルに従って対応する HTTPS データパッケージを復号化します。これは必須アイテムです。
- パスワード：キーファイルが 2 回暗号化されている場合、復号化パスワードを入力する必要があります。そうしないと、システムは通常の復号化を実行できません。これは必須ではありません。
- IP アドレス：キーを使用するサーバーの IP アドレス。これは必須ではありません。
- ポートは、HTTPS サービスを提供するサーバー上のポートです。これは必須ではありません。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- プロトコル：データパケットの復号化後のプロトコル形式。現在は http のみをサポートしています。これは必須ではありません。

- PSK

分析するデータパケットが PSK で暗号化されている場合、「事前共有鍵」に 16 進パスワードを入力して復号化できます

- DH

分析するデータパケットが DH で暗号化されている場合は、「（プレ）マスターキーログファイル」の横にある「参照」ボタンをクリックして、キーログファイルをアップロードできます。

「MAC 失敗」を無視する：チェック後、「MAC 失敗」エラーが発生した場合でも、システムは対応するデータをデコードします。 無視しない場合、このデータセグメントはデコードされません。

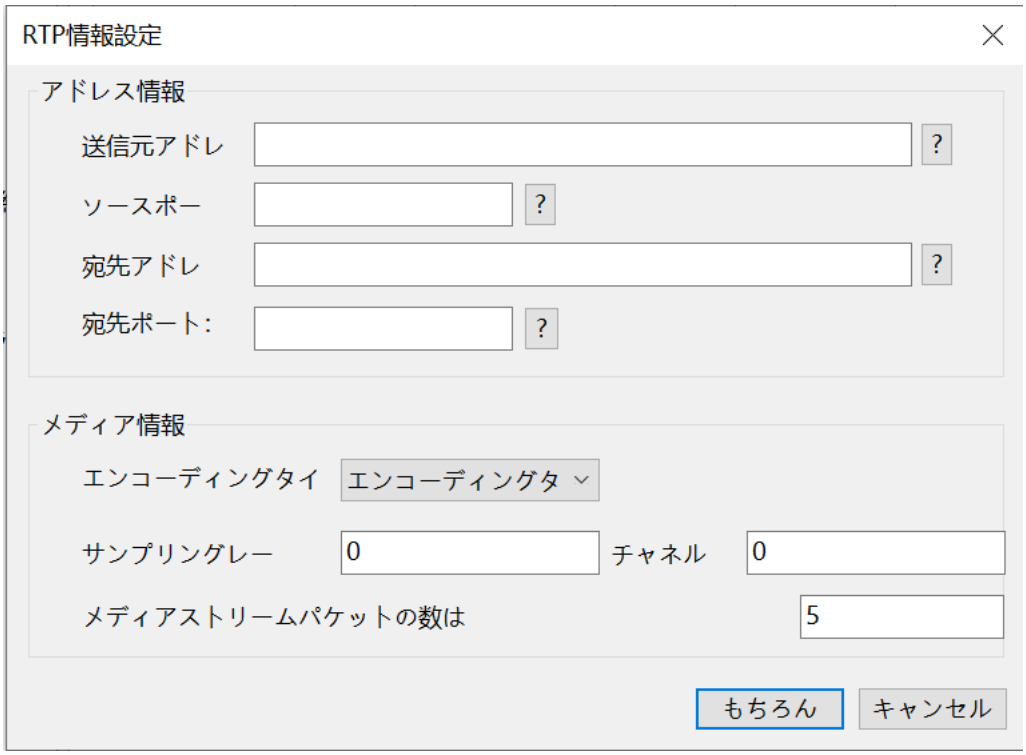
セットアップが完了すると、パケット分析ビューで https パケットのデコード結果を表示できます。

7.3.2 RTP

オーディオとビデオのデコード方法はすべてシグナリングデータパケットに含まれています。シグナリングがない場合、RTP の復元に使用されるエンコード方法を特定することはできず、オーディオファイルとビデオファイルを復元することもできません。 したがって、VoIP でシグナリングせずに RTP プロトコルデータパケットのオーディオとビデオを復元する場合は、RTP の関連情報を設定する必要があります。設定インターフェイスを次の図に示します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

[追加]ボタンをクリックして、RTP 関連のカスタム設定を行います:



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

4 つが RTP ストリームであると判断された場合は、上図のアドレス情報に対応する 4 つ情報を入力し、エンコードタイプを選択し、サンプリングレートとチャネル数を設定してから、オーディオとビデオファイルを復元することができます。

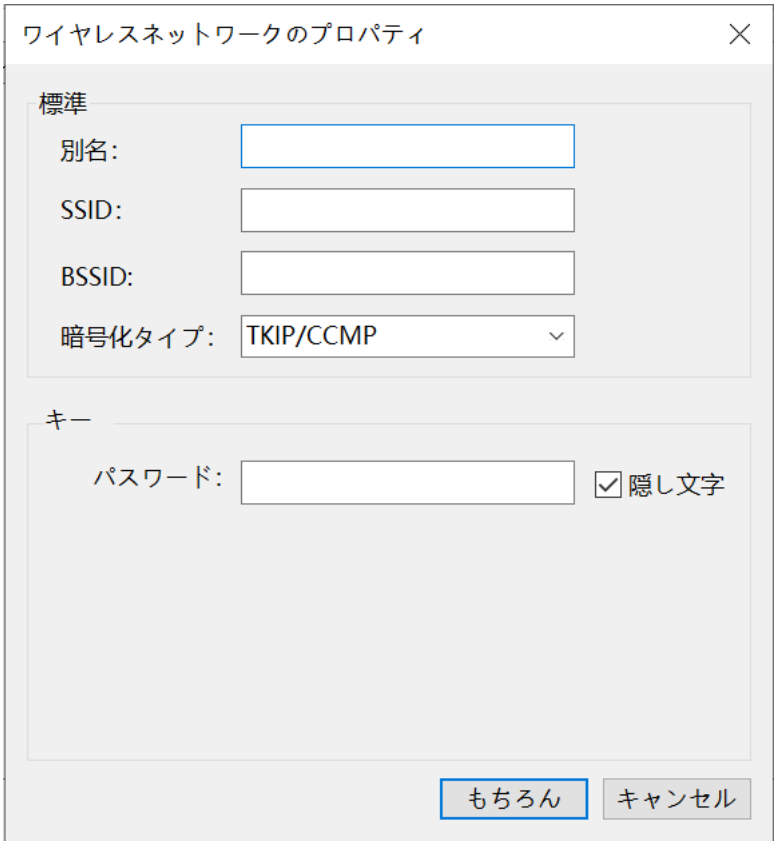
4 タプルの情報がわからない場合は、送信元アドレス、送信元ポートまたは宛先アドレス、および宛先ポートの両端の情報のみを設定でき、もう一方の端はすべて一致します。

7.3.3 IEEE 802.11

ワイヤレスネットワーク構成は、ワイヤレスネットワークの構成に使用されるキーです。 ワイヤレスネットワークの暗号化タイプに応じて対応するキーを設定できます。設定が成功すると、データパケット分析の再生中に対応するワイヤレスデータパケットを復号化できます。 インターフェースは以下の通りです。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

[追加]ボタンをクリックして、ワイヤレスネットワーク関連の設定をカスタマイズします。



エイリアス:

ワイヤレスネットワークエイリアス

SSID:

ワイヤレスネットワーク名

BSSID:

ワイヤレスネットワークの MAC アドレス

暗号化のタイプ

ワイヤレスネットワークの暗号化タイプは、TKIP、CCMP、および WEP に分類されます。

パスワード:

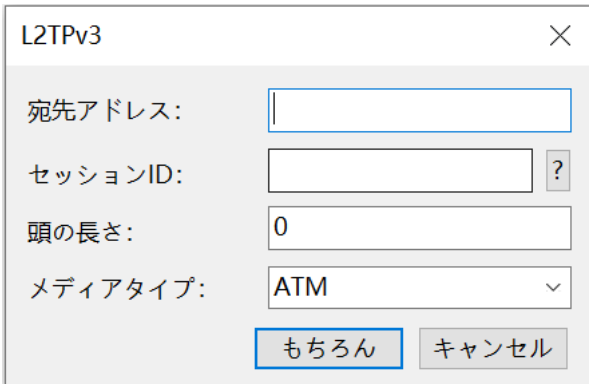
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

TKIP および CCMP 暗号化のパスワードは 1 つだけです。 WEP 暗号化では、複数のパスワードを使用できます。

7.3.4 L2TPv3

L2TPv3 プロトコルのデコードは、独自の構成でカスタマイズできます。構成インターフェイスを次の図に示します。

[追加]ボタンをクリックして、L2TPv3 関連の設定をカスタマイズします。



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

宛先アドレス:

現在、IPv4 アドレスのみがサポートされています。

セッション ID:

10 進表記と 16 進表記の両方がサポートされています。16 進を使用する場合は、「0x」を追加する必要があります。

頭の長さ:

头部长度范围大于等于 4，小于等于 12。ヘッドの長さの範囲は 4 以上 12 以下です。

ミディアムタイプ:

メディアタイプは、ATM、ATM_CELL_TRANSPORT_VCC_MODE、ATM_CELL_TARNSPARENT_PORT_MODE、ATM_CELL_TRANSPORT_VPC_MODE、ETHERNET、ETHERNET_VLAN、HDLC、IP_TRANSPORT、PPP、FRAME_RELAY_DLCI に分類されます。

7.4 カスタムプロトコル

Colasoft Capsa は、カスタマイズされたプロトコル機能を提供します。 多くのネットワークアプリケーションとさまざまなネットワークアプリケーションに関係する多くのネットワークプロトコルがあるため、システムは認識されないプロトコルに対してユーザー定義のネットワーク通信プロトコルをサポートし、ユーザーがネットワーク分析タスクをする時、さまざまなネットワークアプリケーションの関連データ情報をすばやく分析できるようにします。 次の図に示すように、システムオプションメニューの[カスタムプロトコル]をクリックして[カスタムプロトコル]ダイアログボックスを開くと、ユーザーはプロトコル ID をカスタマイズできます。

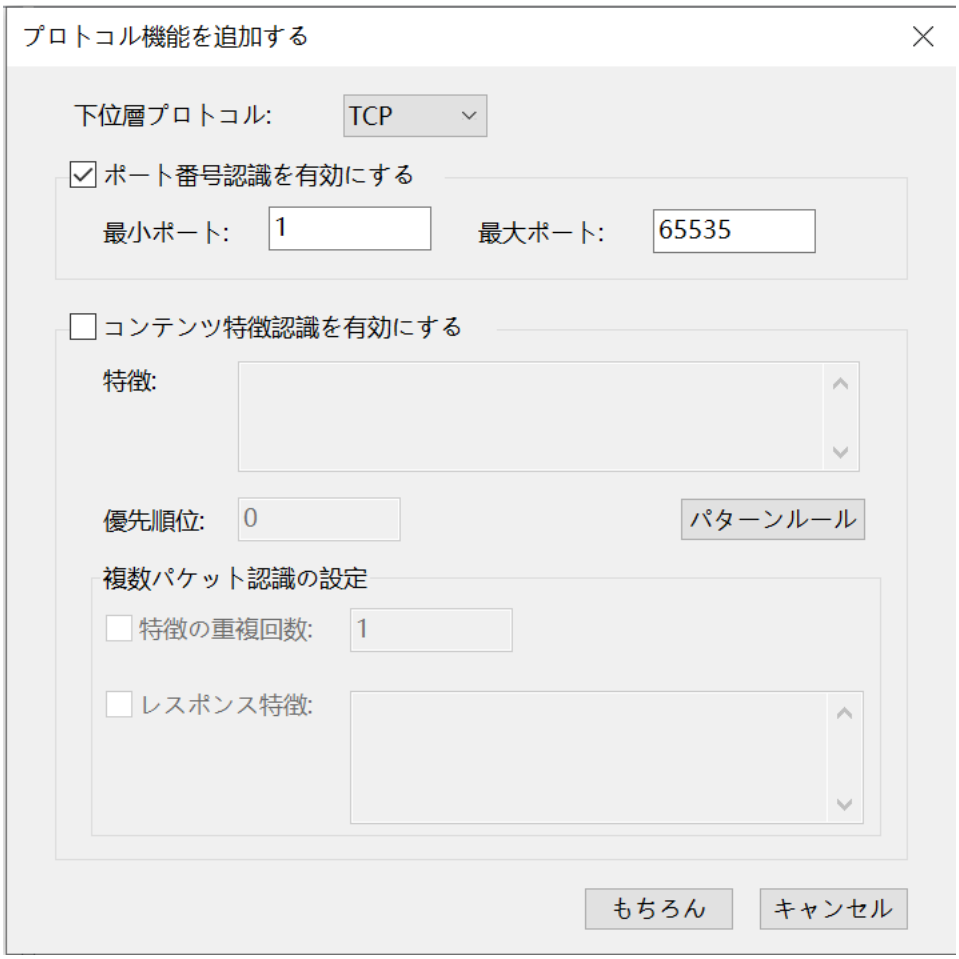
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

次の図に示すように、[プロトコルの追加]ボタンをクリックして、[プロトコルの追加]ダイアログボックスをポップアップします。

ダイアログボックスで、契約名、契約の略語、契約の作成者、契約の説明、および契約の色を設定します。契約番号はシステムによって自動的に生成され、ユーザーが編集することはできません。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

次の図に示すように、プロトコルリストで新しく追加されたプロトコルを選択し、[機能の追加]ボタンをクリックすると、[プロトコル機能の追加]ダイアログボックスがポップアップ表示されます。



プロトコルの特定の特性はダイアログボックスで設定されます。システムがトラフィック識別を実行するとき、識別はプロトコルの特性に基づいています。

プロトコル特性には、ポート特性とコンテンツ特性が含まれます。

- ポート機能の識別：最小ポートと最大ポートを定義します。このポート範囲内のすべてのデータパケットは、定義されたプロトコルとして識別されます。 固定ポート番号の場合、最小ポートと最大ポートは同じに設定されます。
- コンテンツ機能の識別：コンテンツ機能は、単一のパッケージまたは複数のパッケージに固有にすることができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

コンテンツ機能は文字列または 16 進数で表され、設定で使用されるメタ文字は次のとおりです。

- \ ： エスケープキャラクタ
- .: 任意の 1 バイトに一致します
- *: 0 バイトを含む複数の任意のバイトに一致します
- {n} ： n は数値であり、n 個の任意のバイトに一致します

文字列モードの定義規則:

- プロトコル機能は一重引用符（''）で囲まれ、文字列として表されます。
- {n}の中央の数字は、10 進整数である必要があります。整数と'{'、'}'の間にスペースやタブキーはなく、隣り合わせに書き込む必要があります。
- •'*'、'。'、'{'、および'}'のみがメタ文字と見なされます。
- 特別な意味を持つ複数の文字を独自の文字として一致させる必要がある場合は、先頭にエスケープ文字「\」を付ける必要があります。 エスケープ文字は、アスタリスク "\ *"、ピリオド "\。"、開始中括弧 "\ {"、終了中括弧 "\}"、およびスラッシュ"\\"です。
- "\r"、 "\ n"、 "\ t"、キャリッジリターン（13）、ラインフィード（10）、水平タブストップ（9）に対応します。
- エスケープ文字'\'の直後の文字が'*'、'。'、'{'、'}'、'\'、'r'、't'、'n'でない場合、意味がなくて、エラーとしてします。
- プロトコル機能にコロンが表示される場合は、コロンの前にエスケープ文字「\」を追加する必要があります。

16 進モードの定義規則:

- プロトコル機能の各文字を書き込み用の 16 進数に変換します。各 2 桁は文字に対応し、各 16 進数はスペースまたはタブキーで区切る必要があります。
- 0〜9、a〜f、A〜F、'*'、'。'、'{'、'}'のみを表示できます。
- 直接記述された'*'、'。'、'{'、'}'はメタ文字を表し、2A、2E、7B、7D が表示される場合は、文字'*'、'。'、'{'、'}を表します。 '自体なので、16 進表記にはエスケープ文字はありません。
- 16 進数と'*'、'。'、{n}も、スペースまたはタブキーで区切る必要があります。そうでない場合、エラーと見なされます。
- {n}の中央の数字は 10 進整数です。整数と'{'、'}'の間にスペースやタブキーはなく、隣り合わせに書き込む必要があります。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

例:

- 最初の 3 バイトが GET であるパケットを照合します：47 4554*または'GET*'
- 内部に.html を含むパッケージに一致します：* 2e 68 74 6d6c*または'*\。html*'
- 4 番目のバイトがスペースであるパケットに一致します：...20*または{3}20*または'...*'または'{3}*'
- GET で始まり HTTP/が続くパケットを照合します（最初と 3 番目の「。」はワイルドカード文字を表し、2 番目の「。」は前にエスケープ文字があるため文字ドットを表します）：47 45 54 * 48 54 54502f。2e。*または'GET* HTTP/.\..*'

マルチパケット識別の場合は、コンテンツ機能の繰り返し回数を設定したり、応答機能を設定したりできます。

優先度は、プロトコル機能の識別順序を設定するために使用されます。1 つのプロトコルで複数のプロトコル機能を定義でき、優先度の高いプロトコル機能が最初に認識されます。 数字が小さいほど優先度が高くなります。優先度が同じ場合は順番に識別されます。

システムは、カスタムプロトコルのインポートとエクスポートをサポートしています。

7.5 カスタマイズされたアプリケーション

カスタマイズされたアプリケーションは[システムオプション]メニューにあり、主にユーザーがいくつかの特別なアプリケーションをカスタマイズするのを支援するために使用されます。

カスタムアプリケーションは、Dpi フィルタールールをサポートするカスタムアプリケーション（新バージョン）と Dpi フィルタールールをサポートしないカスタムアプリケーション（旧バージョン）に分けられます。デフォルトでは、Dpi フィルタールールをサポートする新しいバージョンのアプリケーションが使用されます。

Note

Dpi フィルターの適用範囲：現在、Dpi フィルターは 64 ビットオペレーティングシステムにのみ適用可能であり、命令セット AVX をサポートしています。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

7.5.1 カスタムアプリケーション（新バージョン）

カスタマイズされたアプリケーションおよびシステムでサポートされているすべての組み込みアプリケーションは、アプリケーションビューでカウントおよび分析でき、アプリケーションビューで表示する必要のあるアプリケーション関連情報を簡単かつ迅速に見つけることができます。 カスタムアプリケーションのインターフェイスを次の図に示します。

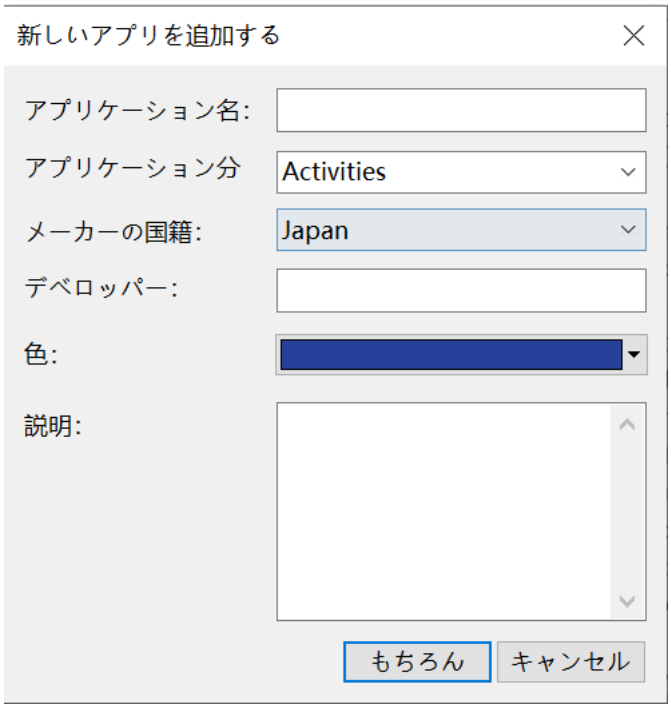
Note

アプリケーションをカスタマイズする場合、開くことができる分析プロジェクトは１つだけであり、プロジェクトはパケットキャプチャの停止状態である必要があります。

アプリを追加

次の図に示すように、[アプリケーションの追加]ボタンをクリックして、[アプリケーションの追加]ダイアログボックスをポップアップします。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



ダイアログボックスで、アプリケーション名、アプリケーション番号、およびアプリケーションの説明を設定します。 アプリケーション番号は整数としてのみ入力でき、保存後に変更することはできません。

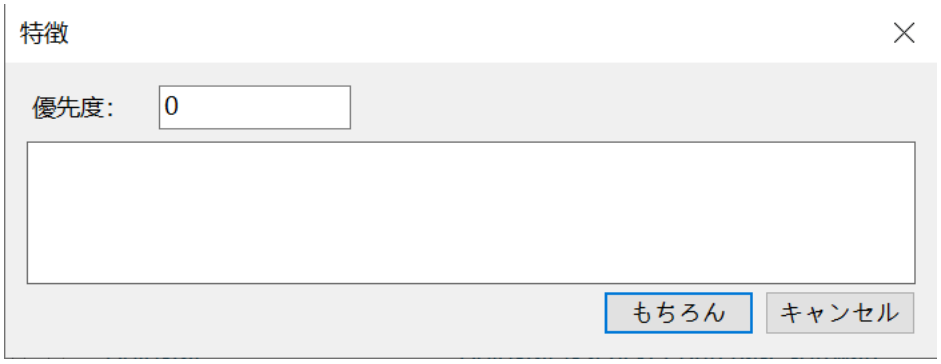
アプリケーション機能を追加

アプリケーションリストで新しく追加されたアプリケーションを選択し、[機能の追加]ボタンをクリックすると、[アプリケーション機能の追加]ダイアログボックスが表示されます。

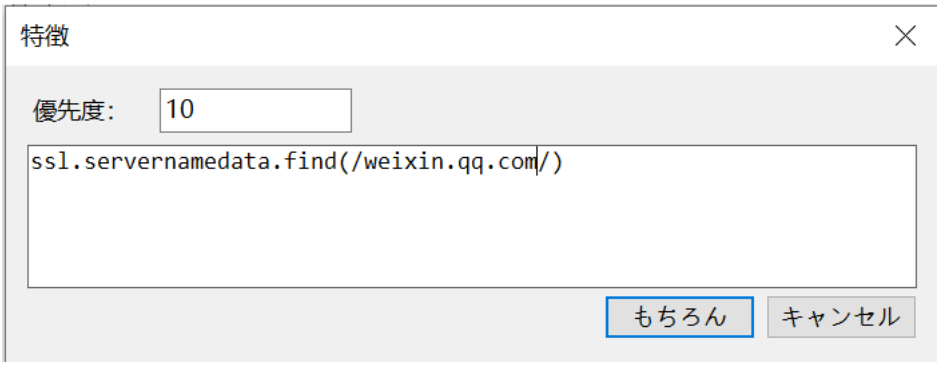
ダイアログボックスでアプリケーションの特定の特性を設定する必要があります。システムがトラフィックの識別を実行する場合、識別はアプリケーションの特性に基づいて行われます。

例 1: プロトコルの特定のフィールド値をカスタマイズし、ヒットした後、このセッションをアプリケーションのトラフィックとしてマークします。 、次の図に示すように、HTTP プロトコルの[ホスト]フィールドまたは SSL プロトコルの[ServerNameData]フィールドに従ってアプリケーション機能を追加します。

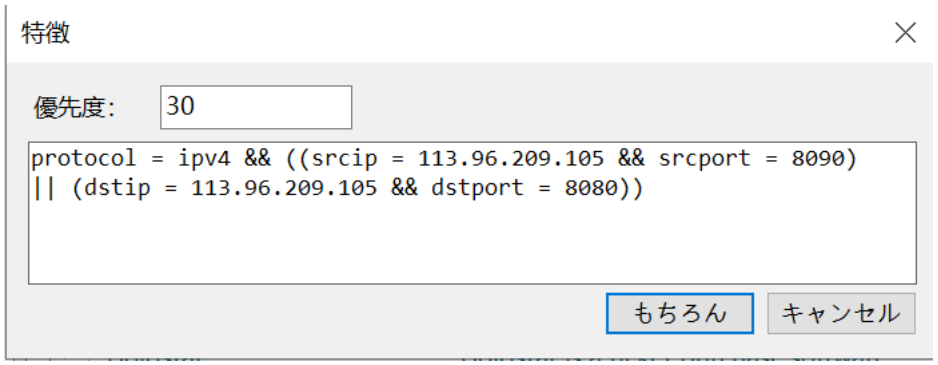
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



例 2：以下に示すように、カスタムロジックの組み合わせルール、「論理と」の関係は「&&」または「と」で表され、「論理または」の関係は「||」または「または」で表され、「論理ではない」の関係は「 ！ 」または「not」は意味します：



例 3：次の図に示すように、識別されたプロトコルに従ってアプリケーション機能を追加します（プロトコルが識別された場合、eMule のプライベートプロトコル Emule などのアプリケーションが存在すると見なされます）。



Note

コンテンツ機能を設定する場合、ユーザーは優先度を設定できます。1 つのプロトコルで複数のコンテンツ機能が定義されている場合、優先度が最

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

も高いプロトコル機能が最初に認識されます。

番号が小さいほど優先度が高くなり、同じ優先度が順番に識別されます。 ユーザー定義のルールは、組み込みの適用ルールよりも常に優先されます。

また、アプリケーションのプロトコル、ポート、アドレス、コンテンツ特性、アドレス+プロトコル、アドレス+ポート、アドレスペア、クライアント+サーバー、アドレス+ポート+コンテンツ特性を使用することもできます。

アプリケーションは複数の機能を定義でき、複数の機能間の関係は OR であり、条件が満たされている限り、アプリケーションとして認識されます。 一般的な例を次の表に示します。

一般的なプロトコルフィールドのユースケース（XXXX：認識条件を示します）	フィルタフィールドの定義
ssl.servernamedata.find(/xxxx/)	ssl リクエストサーバー名データでアプリケーションを特定します
ssl.subjectcommonname.find('xxxx')	SSL 証明書のサブジェクト共通名でアプリケーションを識別します
http.host.find('xxxx')	http 要求サーバーのホスト名でアプリケーションを識別します
http.url.find('xxxx')	http リクエストラインでアプリケーションを特定します
http.useragent.find(/xxxx/)	http の UserAgent フィールドからアプリケーションを識別します
http.cookie.find(/xxxx/)	http の cookie フィールドを介してアプリケーションを識別します
bittorrent.peerid.find(/xxxx/)	bittorrent クライアント ID でアプリケーションを識別します
ip = 192.198.9.51 or ip.in(91.108.56.0/22)	送信元 IP アドレスと宛先 IP アドレスでアプリ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

	ケーションを識別します
Port = 80	送信元ポートと宛先ポートでアプリケーションを識別します
srcip = 192.198.9.51 or srcip .in(91.108.56.0/22)	送信元 IP アドレスでアプリケーションを特定します
srcport = 443	ソースポートでアプリケーションを特定します
dstip = 192.198.9.51 or dstip .in(91.108.56.0/22)	宛先 IP アドレスでアプリケーションを識別します
dstport =443	宛先ポートによるアプリケーションを識別します
protocol = http	プロトコルによるアプリケーションを識別します
payload.find('xxxx')	TCP/UDP ペイロードデータによるアプリケーションを識別します
protocol = tcp && payload.find(/^\x4f\x55\x54\x0d\x0a$/)	TCP/UDP ペイロードデータによるアプリケーションを識別します

アプリケーションのインポート/エクスポート

システムは、カスタムアプリケーションのインポートおよびエクスポート操作をサポートします。

エクスポート

[エクスポート...]ボタンをクリックすると、カスタムアプリケーションをエクスポートできます。 エクスポートすると、システムは「CustomApp.cscapp」と「CustomApp.cscappsig」の 2 つのファイルを生成します。

インポート

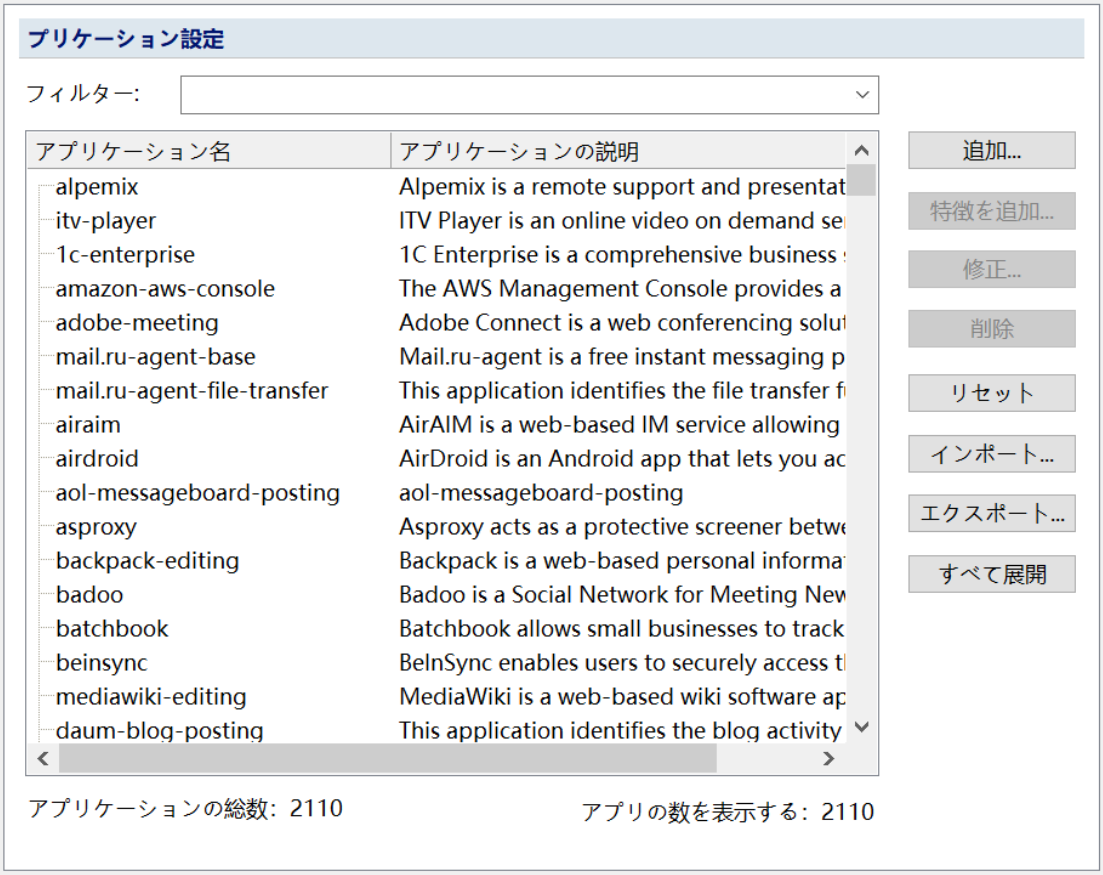
[インポート...]ボタンをクリックして、カスタムアプリケーションをインポートできます。 インポートするときは、「CustomApp.cscapp」ファイルをインポートすることを選択しますが、CustomApp.cscappsig」と「CustomApp.cscapp」が同じ場所にあることを確認する必要があります。同

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

じ場所にないと、カスタムアプリケーションを正しくインポートできません。

7.5.2 カスタムアプリケーション（レガシー）

カスタマイズされたアプリケーションおよびシステムでサポートされているすべての組み込みアプリケーションは、アプリケーションビューでカウントおよび分析でき、アプリケーションビューで表示する必要のあるアプリケーション関連情報を簡単かつ迅速に見つけることができます。 カスタムアプリケーションのインターフェイスを次の図に示します。



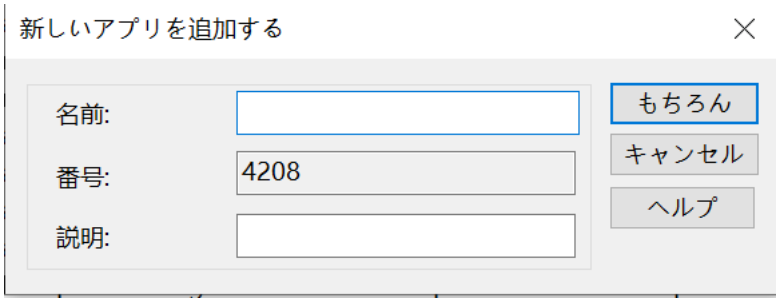
Note

アプリケーションをカスタマイズする場合、開くことができる分析プロジェクトは１つだけであり、プロジェクトはパケットキャプチャの停止状態である必要があります。

アプリを追加

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

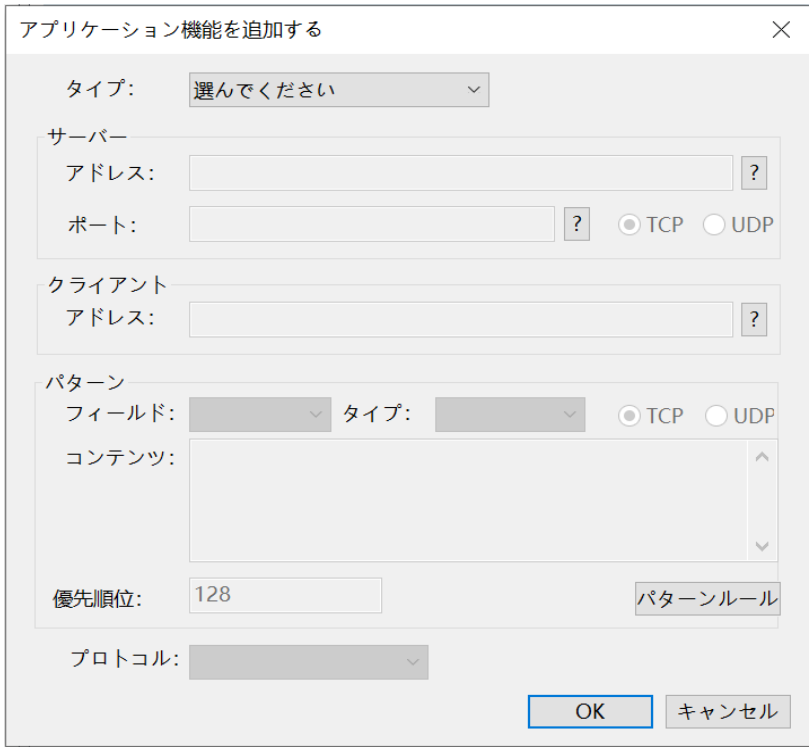
次の図に示すように、[アプリケーションの追加]ボタンをクリックして、[アプリケーションの追加]ダイアログボックスをポップアップします。



ダイアログボックスで、アプリケーション名、アプリケーション番号、およびアプリケーションの説明を設定します。 アプリケーション番号は整数としてのみ入力でき、保存後に変更することはできません。

アプリケーション機能を追加

次の図に示すように、アプリケーションリストで新しく追加されたアプリケーションを選択し、[機能の追加]ボタンをクリックすると、[アプリケーション機能の追加]ダイアログボック。



がポップアップ表示されます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ダイアログボックスでアプリケーションの特定の特性を設定する必要があります。システムがトラフィックの識別を実行する場合、識別はアプリケーションの特性に基づいて行われます。

アプリケーションのプロトコル、ポート、アドレス、コンテンツ特性、アドレス+プロトコル、アドレス+ポート、アドレスペア、クライアント+サーバー、アドレス+ポート+コンテンツ特性を使用できます。

アプリケーションは複数の機能を定義でき、複数の機能間の関係は OR であり、条件が満たされている限り、アプリケーションとして認識されます。

コンテンツ機能を設定する場合、ユーザーは優先度を設定できます。1 つのプロトコルで複数のコンテンツ機能が定義されている場合、優先度が最も高いプロトコル機能が最初に認識されます。 数字が小さいほど優先度が高くなります。優先度が同じ場合は順番に識別されます。

アプリケーションのインポート/エクスポート

システムは、カスタムアプリケーションのインポートおよびエクスポート操作をサポートします。

- エクスポート:

- [エクスポート...]ボタンをクリックすると、カスタムアプリケーションをエクスポートできます。 エクスポートすると、システムは「CustomApp.cscapp」と「CustomApp.cscappsig」の 2 つのファイルを生成します。
- インポート

  [インポート...]ボタンをクリックして、カスタムアプリケーションをインポートできます。 インポートするときは、「CustomApp.cscapp」ファイルをインポートすることを選択しますが、CustomApp.cscappsig」と「CustomApp.cscapp」が同じ場所にあることを確認する必要があります。同じ場所にないと、カスタムアプリケーションを正しくインポートできません。

7.6 名前リスト

名前テーブルの構成では、ネットワークの物理エンドポイントと IP エンドポイ

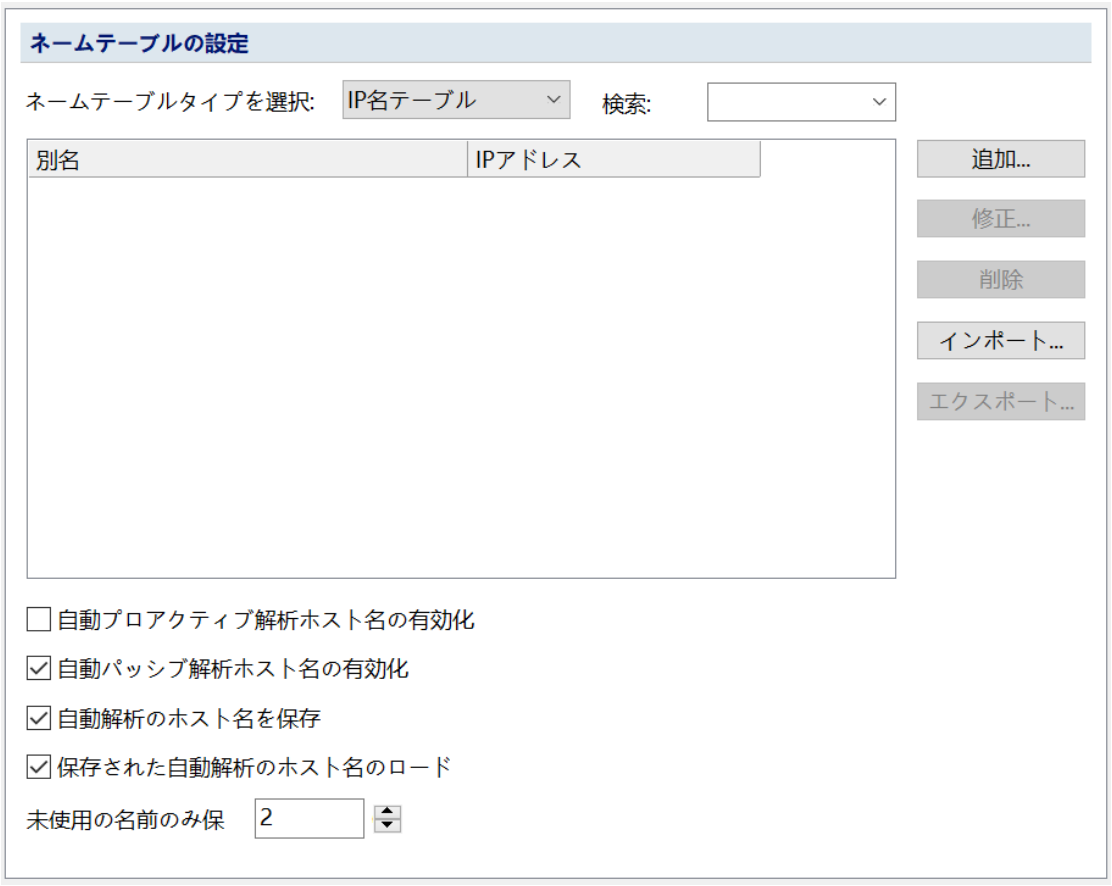
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ントに共通の識別可能な名前を割り当てることができます。これらの名前は、次のビューで IP アドレスと MAC アドレスを置き換えることができます。

- ノードブラウザ
- 物理的なエンドポイント
- IP エンドポイント
- 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
- マトリックスビュー
- パケットビュー

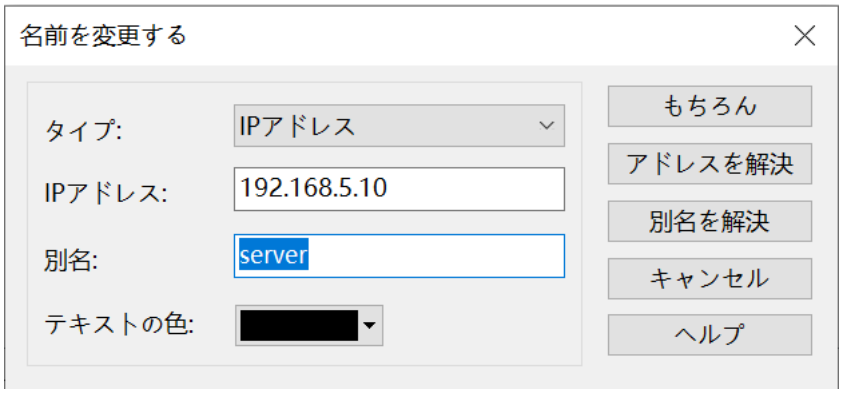
これらのビューから名前テーブルに IP アドレス、MAC アドレスを追加することもできます。 [名前リスト]ダイアログボックスでは、操作を追加、削除、編集、インポート、およびエクスポートすることもできます。

ヒント：アドレスエイリアスを設定した後、システム機能領域の表示ページで物理アドレスと IP アドレスの表示形式を選択できます。

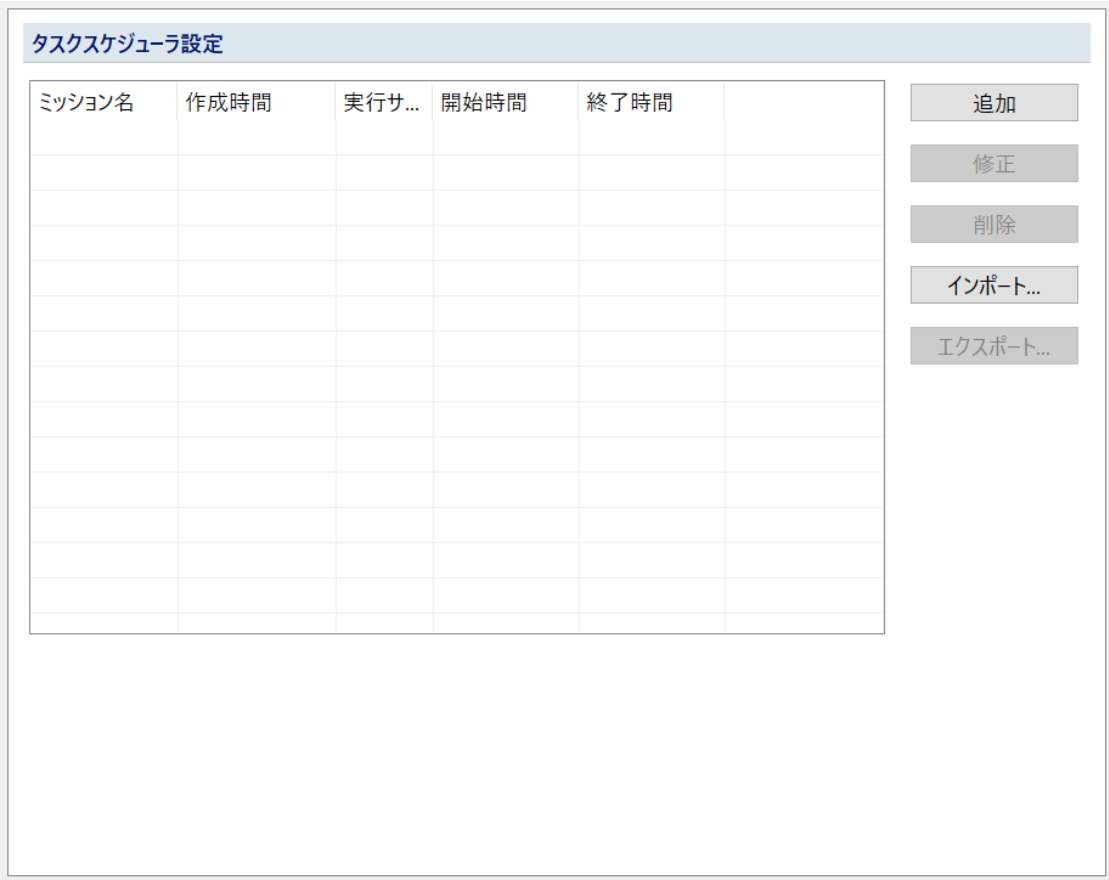


著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

各分析ビュー領域またはノードブラウザで、右クリックして[名前テーブルに追加]メニューを選択すると、名前テーブルをすばやく追加および変更できます。



7.7 タイミング分析

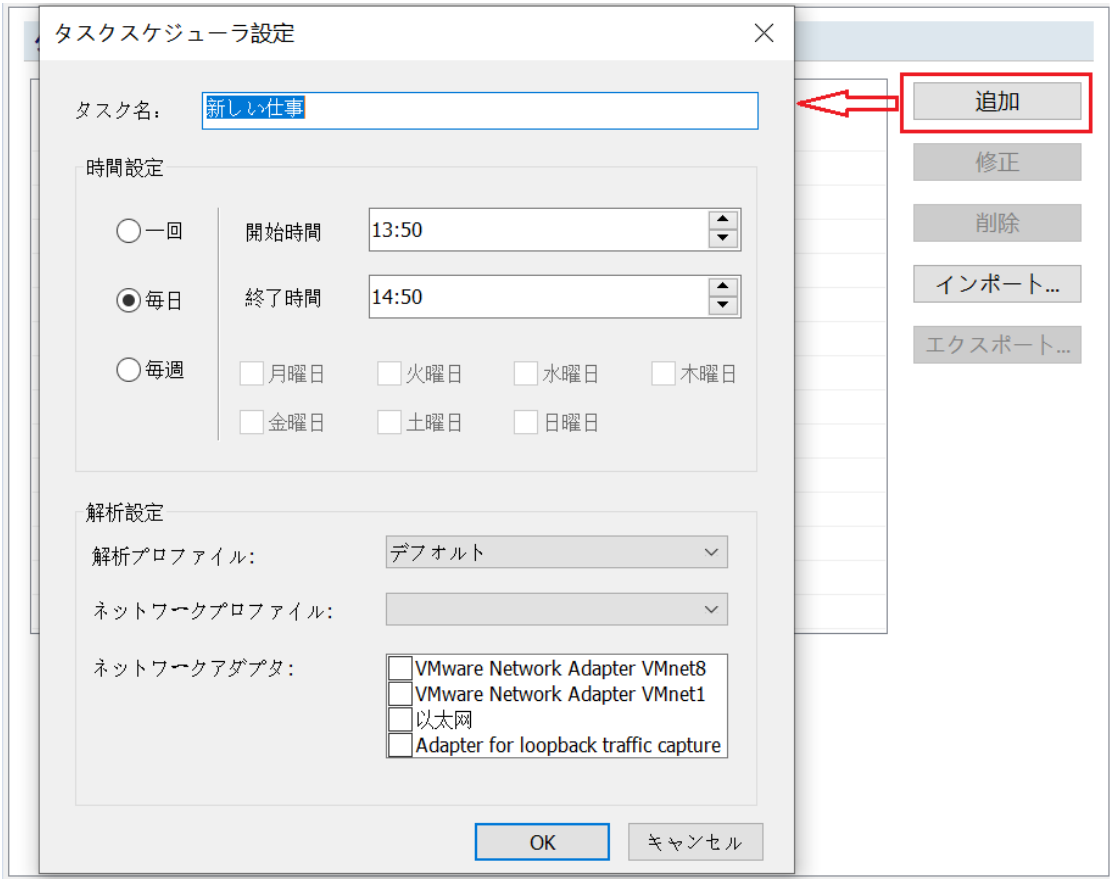


著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

一定期間のネットワーク通信データパケットをキャプチャする必要がある場合は、スケジュール分析機能にスケジュール分析タスクを追加できます。指定時間に達すると、システムは自動的にデータキャプチャを開始します。

タイミング分析は、ユーザーが Colasoft Capsa を使用してタイミング分析タスクを実行するのに役立ちます。 タイミング分析設定はシステムオプションダイアログボックスにあり、ユーザーはシステムオプションでタイミング分析タスク設定を設定できます。

[追加]ボタンをクリックして、時限分析タスクの設定を開始します。



- タスク名：この分析タスクの名前を指定します。
- 時間設定：特定の時間帯に 1 日/週に 1 回データキャプチャを開始するように設定でき、開始時間と終了時間をカスタマイズできます。
- 分析設定：分析には、分析設定とネットワークアダプタを選択する必要があります。システムは、ここの設定に従ってスケジュールされた分析タスクを実行します。
- タイミング分析を有効にした場合：

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- スタートページで停止した場合、指定した分析時間に達すると自動的に分析を開始します。
- システムを分析している場合は、新しい分析プロジェクトを作成し、データの収集と分析を開始します。

7.8 レポート

レポート：レポートダイアログの設定は、主に、レポートタイトル、生成時間、会社のロゴ、作成者名、その他の一般的なレポート表示情報の追加など、レポートオプションをカスタマイズするために使用されます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

7.9 格式 フォーマット

[フォーマット]ダイアログボックスでは、システム内のデータの表示フォーマットを表示または変更するために使用されます。

- 小数点以下の桁数

  小数点以下の桁数を設定します。 システムのデフォルトは 3 桁です。

- パーセンテージの小数点以下に表示される桁数:
  小数点以下の桁数を設定します。 システムのデフォルトは 3 桁です。
- バイト形式:

  システムが表示するバイトフォーマットを設定します。 システムのデフォルト設定では、実際のトラフィックサイズに応じてさまざまなバイト形式（B、KB、MB、GB、TB）が自動的に変換され、ユーザーは常に特定のバイト形式を表示するように選択することもできます。

- ビットフォーマット:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

システムによって表示されるビット形式を設定します。 システムのデフォルト設定では、実際のトラフィックサイズに応じてさまざまなバイト形式（b、Kb、Mb、Gb、Tb）が自動的に変換され、ユーザーは常に特定のバイト形式を表示するように選択することもできます。

- バイト/秒形式

  システムによって表示される 1 秒あたりのバイト数の形式を設定します。システムはデフォルトで、実際のトラフィックサイズに応じてさまざまな毎秒バイト形式（Bps、KBps、MBps、GBps、TBps）を自動的に変換します。また、ユーザーは常に特定の毎秒バイト形式を表示するように選択することもできます。

- ビット/秒形式

  システムによって表示されるビット/秒形式を設定します。 システムのデフォルト設定では、実際のトラフィックサイズに応じて、さまざまなビット/秒形式（bps、Kbps、Mbps、Gbps、Tbps）が自動的に変換されます。また、ユーザーは常に特定のビット/秒のフォーマットを表示するように選択することもできます。

- 時間精度
  システムによって表示される時間精度を設定します。 システムのデフォルトはナノ秒（ns）であり、ユーザーは他の時間精度（s、ms、us）を選択することもできます。
- 期間の形式
  期間の表示形式を設定します。 システムのデフォルトは、N 日、N 時間、N 分、N 秒、N ミリ秒、N マイクロ秒、および N ナノ秒です。ユーザーは hh：mm：ss.000000000 形式を選択することもできます。
- デフォルトに戻す

  ボタンを使用すると、システムのデフォルトのフォーマット構成に戻ります。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

8 分析設定

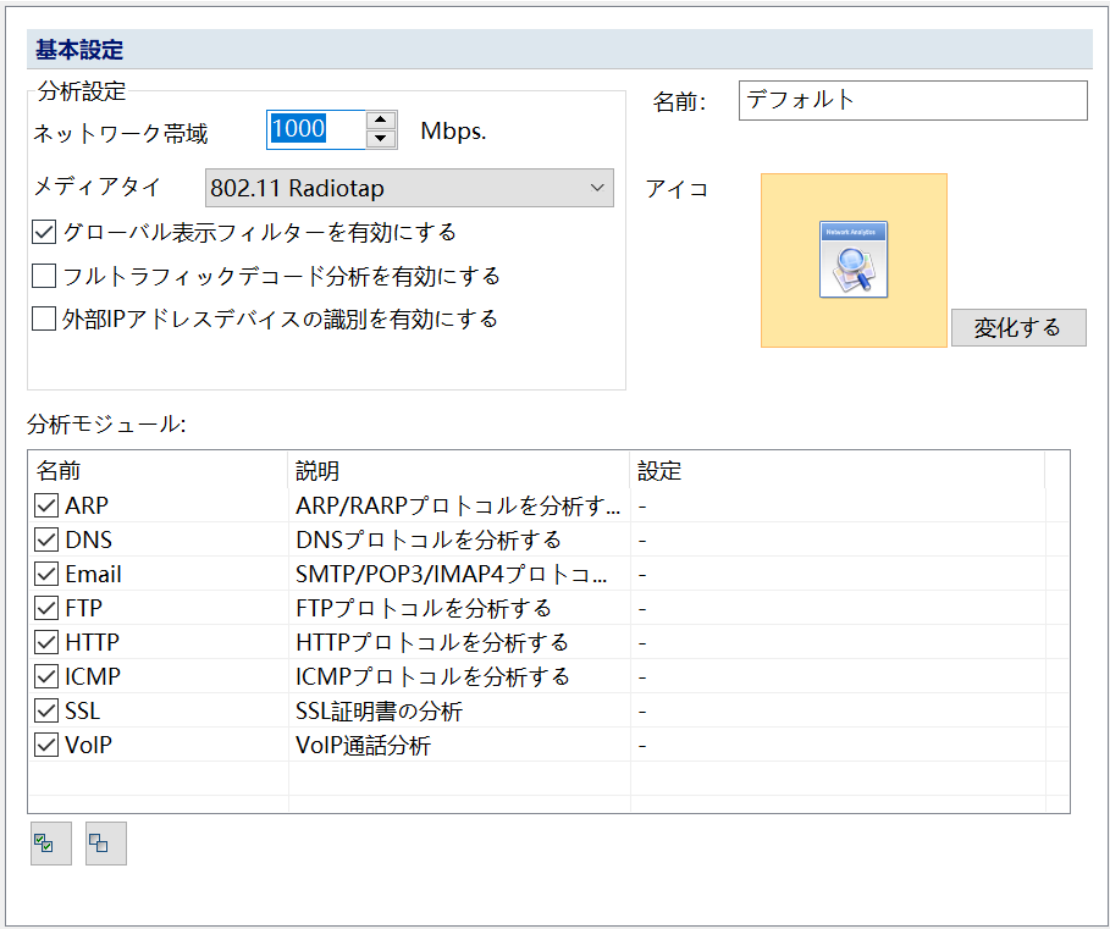
分析設定は、ネットワークデータをキャプチャする前に、キャプチャ条件およびその他の一般的な設定を提供します。 パケットをキャプチャするとき、ユーザーは分析オブジェクト設定、パケット表示キャッシュ設定、フィルター、ネットワークイベント診断設定、ログ設定、ログストレージ、パケットストレージ、および分析ビュー表示設定をカスタマイズできます。 分析設定には、主に次のものが含まれます。

- 基本設定–ネットワーク帯域幅、メディアタイプ、分析モジュールを設定します
- 分析オブジェクトの設定–主な設定は、分析とカウントが必要なネットワークオブジェクトを有効にするかどうかです。
- 診断設定–診断が必要なネットワークイベントをカスタマイズし、ネットワーク内のエラー情報または障害情報を自動的に確認します
- 分析ビュー設定–メインビュー領域のクローズ/表示設定と表示順序設定を分析します
- ノードのグループ化–ノードブラウザで IP ノードと MAC ノードをカスタマイズします
- データパケット表示キャッシュ設定-主にデータパケット表示バッファのサイズを設定します
- パケットフィルター–パケットキャプチャフィルターを設定します
- パケット保存–データパケットの自動保存を設定します
- セッションフィルター–セッションフィルターを設定します
- 復元設定–ファイル復元オプションを設定します
- ログ設定–ログ分析モジュールが一般的なアプリケーションログをカウントおよび分析できるようにするかどうかを設定します
- ログ保存–Web アプリケーションログの自動保存を設定します
- アラート–カスタムアラートメッセージ
- アラームアクションのトリガー–アラームがトリガーされたときのアクションを設定します

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

8.1 基本設定

基本設定ページで、分析設定、ネットワーク帯域幅設定、およびメディアタイプ設定によってロードされた分析モジュールのカスタム設定を提供します。



この設定ページは上級ユーザーにのみお勧めします。通常、システムのデフォルト設定を使用できます。

注：この設定ページは、データキャプチャを開始する前にのみ表示されます。つまり、システムスタートページで分析設定を編集および変更する場合に有効です。システムがすでにデータのキャプチャを開始している場合は、の分析設定をクリックすると有効になります。メインインターフェース、分析設定の分析モジュールは変更できません。

8.2 分析オブジェクト

分析オブジェクト設定ダイアログボックスでは、分析オブジェクトの統計と分

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

析、分析オブジェクトのプロトコル詳細統計、および分析オブジェクトの数の設定を有効にするかどうかを選択できます。 分析オブジェクトには、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、および UDP セッションが含まれます。

[分析オブジェクトの設定]ダイアログボックスで、分析する必要のない分析オブジェクトと分析オブジェクトのプロトコル統計の詳細を有効または無効にすることを選択でき、各分析オブジェクトの最大数を設定できます。たとえば、分析オブジェクトオプションで IP アドレスグループの統計をオフにすると、システムはすべての IP アドレスグループの通信情報をカウントしません。つまり、ノードブラウザで IP エンドポイントで IP アドレスグループを選択した場合です。ビューでは、IP アドレスグループのすべての通信パラメータは 0 です。IP アドレスグループオプションをオンにして分析プロトコルの詳細をオフにすると、IP アドレスグループのプロトコルの詳細はカウントされません。ノードブラウザの IP アドレスグループ分析オブジェクトで物理セッションを閉じると、

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

システムはネットワーク内のすべての物理セッションをカウントおよび分析しません。物理セッションを開いて、物理セッションの分析プロトコルの詳細を閉じると、の場合、通信プロトコルの物理セッションの詳細はカウントされません。つまり、ノードブラウザでレイヤ 2 通信プロトコル（ARP など）を選択すると、物理セッションビューは空になります。

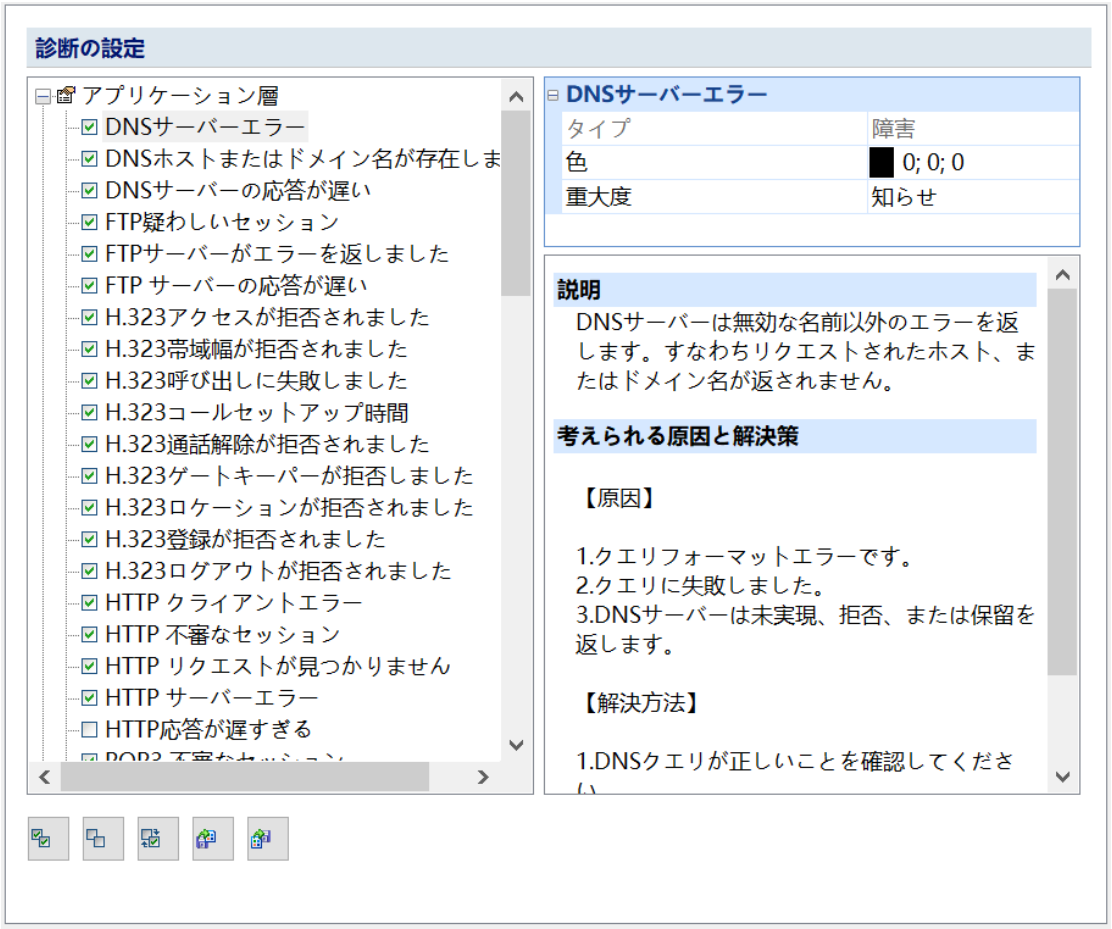
8.3 診断設定

診断設定には、システムに組み込まれているすべての診断イベントが含まれます。ユーザーは、自分のネットワーク状態に応じて、タイプ、色、重大度、状態しきい値などの診断イベントの設定を変更できます。 イベントを診断したくない場合、ユーザーはリスト内のイベントの診断アプリケーションをキャンセルすることもできます。

診断設定では、すべての診断イベントはプロトコル層、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によって分類されます。 このようにして、ネットワークの障害について、ネットワークのどの層に問題があるかをすばやく特定できます。 システムは、診断イベントごとに、イベントの説明、考えられる原因、および考えられる解決策を提供します。これらは、トラブルシューティングに非常に役立ちます。

診断設定の構成については、インポートおよびエクスポートすることで他の人と共有できます。設定がわかりにくい場合は、デフォルト値に戻すこともできます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



[診断設定]ダイアログボックスでは、システムでサポートされているすべての診断イベントが OSI モデルに従って階層的に一覧表示されます。ユーザーは、このダイアログボックスで各イベントのプロパティを設定し、各イベントの説明を表示して、参照ソリューションを提供できます。

8.4 分析ビューの設定

下図のように、Colasoft Capsa には、ネットワーク統計、分析、診断データの出力表示用にデフォルトで 20 のメインビュー領域があります。ユーザーは、に示すように、使用習慣に応じて、表示の開閉順序をカスタマイズしたり、表示順序を調整したりできます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- ビュー表示のオン/オフを切り替える

  特定の種類のデータ出力を気にしない場合は、このダイアログボックスで対応するチェックボックスをオフのままにしておくと、ビューはシステムのメインインターフェイスに表示されません。システムはデフォルトですべての分析ビューを開きます。

- ビュー表示順序の設定

分析ビューの表示順序は、ご自身の使用習慣に合わせて調整し、ビューを選択し、「上に移動」または「下に移動」ボタンをクリックして、ビューの表示順序を調整できます。

システムのメインインターフェイスでは、特定のビューの表示を直接閉じることができます。もう一度開く必要がある場合は、このダイアログボックスを開いて、再度チェックする必要があります。

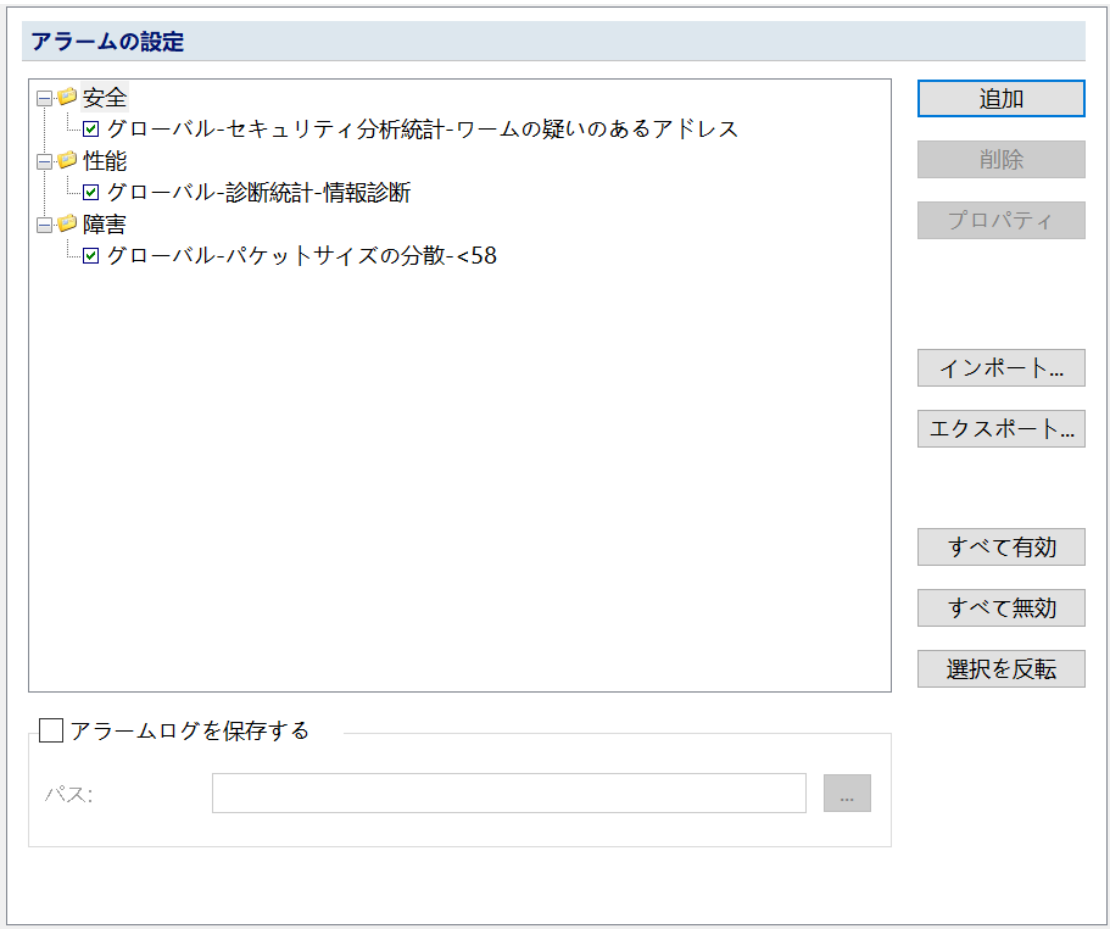
注：分析設定が異なれば、ロードされる分析メインビューも異なります。実際に選択された分析設定を参照してください。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

8.5 ノードのグループ化

ネットワークノードのグループ化構成は、主にノードブラウザの IP ノードと MAC ノードをカスタマイズするためのものです。 IP ノードと MAC ノードは、ローカルネットワークセグメント、ローカルサブネット、プライベートネットワークなど、ネットワークデータの種類に応じて異なるグループを定義します。ユーザーは、ローカルデータ、リモートデータ、ブロードキャストデータ、およびマルチキャストデータを簡単に表示できます。 ユーザーは、必要に応じて追加および削除して、独自のネットワーク構造を計画することもできます。 たとえば、さまざまなネットワークセグメントをさまざまな IP グループに分割したり、部門に応じてさまざまな IP グループを確立したりできます。

Colasoft Capsa にはすでにデフォルト構成があります。[自動検出]をクリックすると、システムはネットワークを自動的にスキャンし、IP ノードと MAC ノードのグループ化構造を自動的に検出します。



8.6 パケット表示キャッシュ

データパケット表示キャッシュ設定ダイアログボックスは、主にデータパケット表示キャッシュのサイズ用であり、そのインターフェースは下図のようになります。

ダイアログボックスの設定について詳しく説明します。

キャプチャされたデータパケットを分析した後、システムはデータパケットをバッファに保存し、データパケットバッファリングはネットワーク分析で高速データストレージの役割を果たすことができます。 キャッシュサイズの設定は、必要なデータの量とコンピュータのメモリの量によって異なります。

パケット表示キャッシュサイズを設定します。「パケット表示キャッシュ最大値」をチェックすると、パケット表示キャッシュの最大値を指定できます。最

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

大値を指定しないと、ソフトウェアは再割り当てできなくなるまでパケットを自動的に割り当ててキャッシュサイズを表示します。

キャッシュがいっぱいになると、次の処理方法を選択できます:

- 古いパケットを廃棄する（リサイクル）

  キャプチャされたデータパケットの数が設定した最大値に達すると、システムはキャッシュに保存されている最も古いデータパケットを破棄し、新しいデータパケットを追加します。

- キャプチャされたパケットの数が設定された最大値に達すると、新しくキャプチャされたパケットは分析モジュールによって分析された後に破棄され、キャッシュに保存されません
- 古いパケットをすべて破棄する

  キャプチャされたデータパケットの数が設定した最大値に達すると、システムはキャッシュをクリアしてから、新しいデータパケットを追加します。

- キャプチャまたは再生を停止する

  バッファがいっぱいになったら、データのキャプチャまたは再生を停止します。

デフォルトでは、バッファがいっぱいになると、システムは処理方法として最も古いデータパケットを破棄します。したがって、データパケット表示バッファのサイズは、データパケットビューでのデータパケット表示に影響します。キャプチャされたデータが表示バッファを超える場合サイズ、最も早いキャプチャされたデータパケットが表示されます。破棄され、パケットビューには最新のキャプチャされたデータのみが表示されます。

8.7 パケットフィルター

データキャプチャを開始する前に、パケットキャプチャフィルタを設定して、特定のトラフィックデータをキャプチャおよび分析できます。 フィルタは、レガシーフィルタと DPI フィルタフィルタに分けられます。 パケットフィルタの詳細な設定については、次の章のフィルタ設定を参照してください。。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

レガシーフィルター

コンピューターのハードウェアが DPI フィルターをサポートしていない場合、ソフトウェアは以下に示すようにレガシーフィルターを使用します。

DPI フィルター

コンピュータハードウェアが DPI フィルタをサポートしている場合、次の図に示すように、ソフトウェアは DPI フィルタを使用します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

8.8 パケット保存

デフォルトでは、システムはデータパケット保存機能を有効にしません。データパケットを自動的に保存する必要がある場合は、分析設定の[データパケット保存設定]ダイアログボックスで事前に設定してください。

次の図に示すように、[パッケージファイルを自動的に保存する]チェックボックスをオンにして、パッケージファイルのストレージを設定します。

- データパケットを XX バイトに制限する：設定をカスタマイズして、各データパケットの XX バイトのサイズのみを保存できます。
- 単一ファイル：データパッケージを単一ファイルとして保存します。
- 複数の分割ファイル：時間またはサイズに応じてデータパケットを分割して保存します。　（おすすめされた）

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

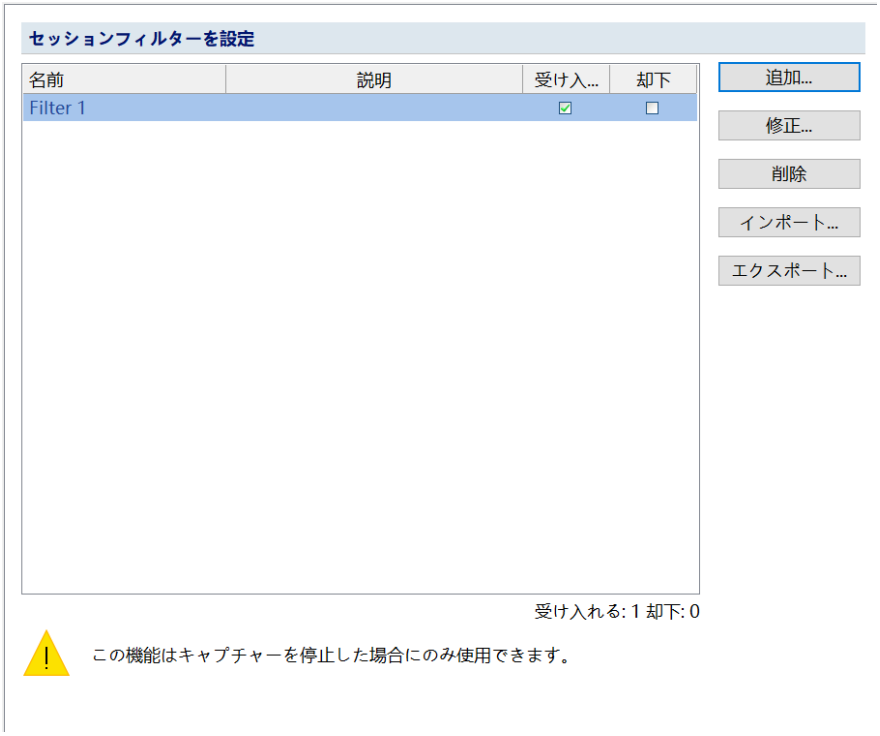
- ファイル保存パス：データパッケージファイル保存パスの設定はここでは変更できません。パスを変更する必要がある場合は、分析サーバーで変更する必要があります。
- 基本ファイル名：データパッケージファイルを保存するための基本ファイル名を設定します。
- ファイル分割間隔：時間（日/時/分）またはファイルサイズ（GB / MB / KB）で保存します。
- 保存ファイル数：分割ファイルの全部または一部を保持するように設定します。
- データパケットは分析せずにのみ保存します。データパケットを分析せずに直接保存します。

8.9 セッションフィルター

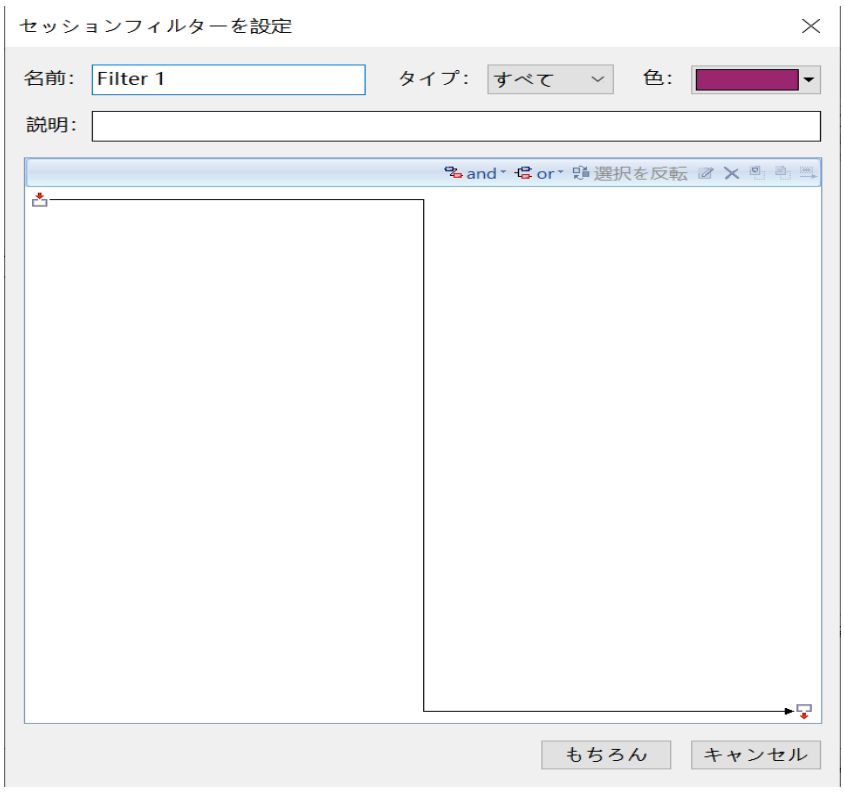
次の画像に示すように、データキャプチャを停止した状態で、セッションフィ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ルタを設定して、アナリティクス固有のセッションデータをキャプチャできます。



以下に示すように、[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できます。



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

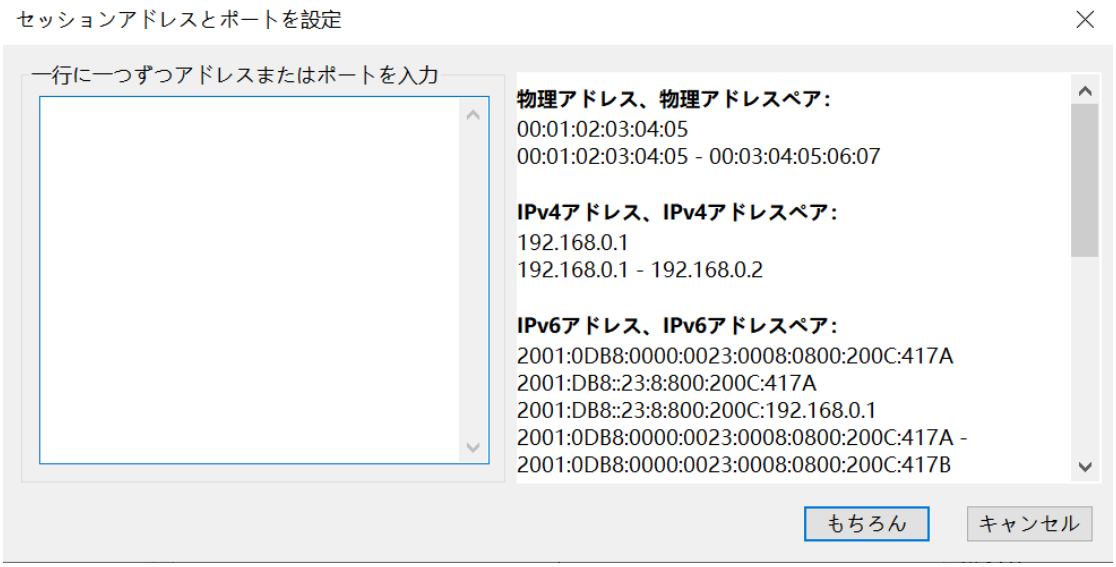
セッションフィルターでは、以下を設定できます。

フィールド名	説明
名前	フィルタに特定の名前を付けます
タイプ	システムは、物理セッション、IP セッション、TCP セッション、および UDP セッションのフィルタリングをサポートしています。これらのセッションの 1 つだけをフィルタリングするか、すべてのセッションをフィルタリングするかを選択できます。
色	フィルタの名前を色付けできます
説明	ここに簡単な説明を入力できます
フィルター	1.システムは、複数の条件の設定とフィルタリングをサポートし、複数の条件間の AND または OR 関係をサポートします。 2.各フィルタ条件は、アドレスとポート、セッションプロトコル、セッションデータパケット、セッションコンテンツ、セッション属性の 5 つの方法で設定できます。各条件の具体的な設定方法については、フィルタ条件の説明を参照してください。

フィルタ条件

- アドレスとポートセッションのアドレスとポートを入力して、特定のアドレスまたはポートのセッションをフィルタリングします。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



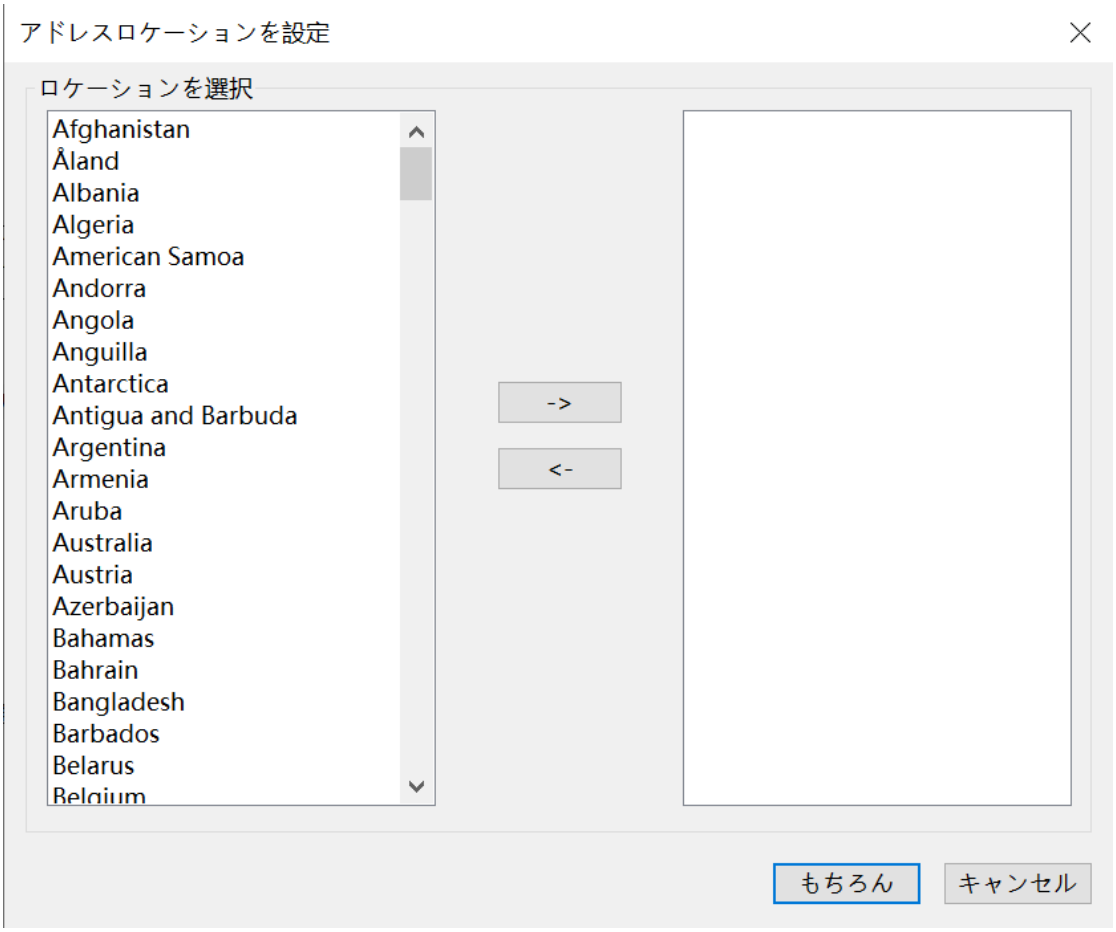
上の図に示すように、システムはアドレスとポートのフィルタリングの複数の方法をサポートしており、フィルタリングの各方法は異なるセッションを対象としています:

- 物理アドレス、物理アドレスのペア：物理アドレスによるセッションフィルタリングします。
- IP アドレス、IP アドレスペア：IP セッション、TCP セッション、および UDP セッションに有効です。
- 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 セッションの場合、システムは IP アドレスポート/ IP アドレスポートペアを使用してフィルタリングします。IP セッションの場合、システムは構成された IP アドレス/IP アドレスペアに従ってのみフィルタリングします。
- ポート、ポートペア：TCP セッションと UDP セッションに有効です。

- 帰属地

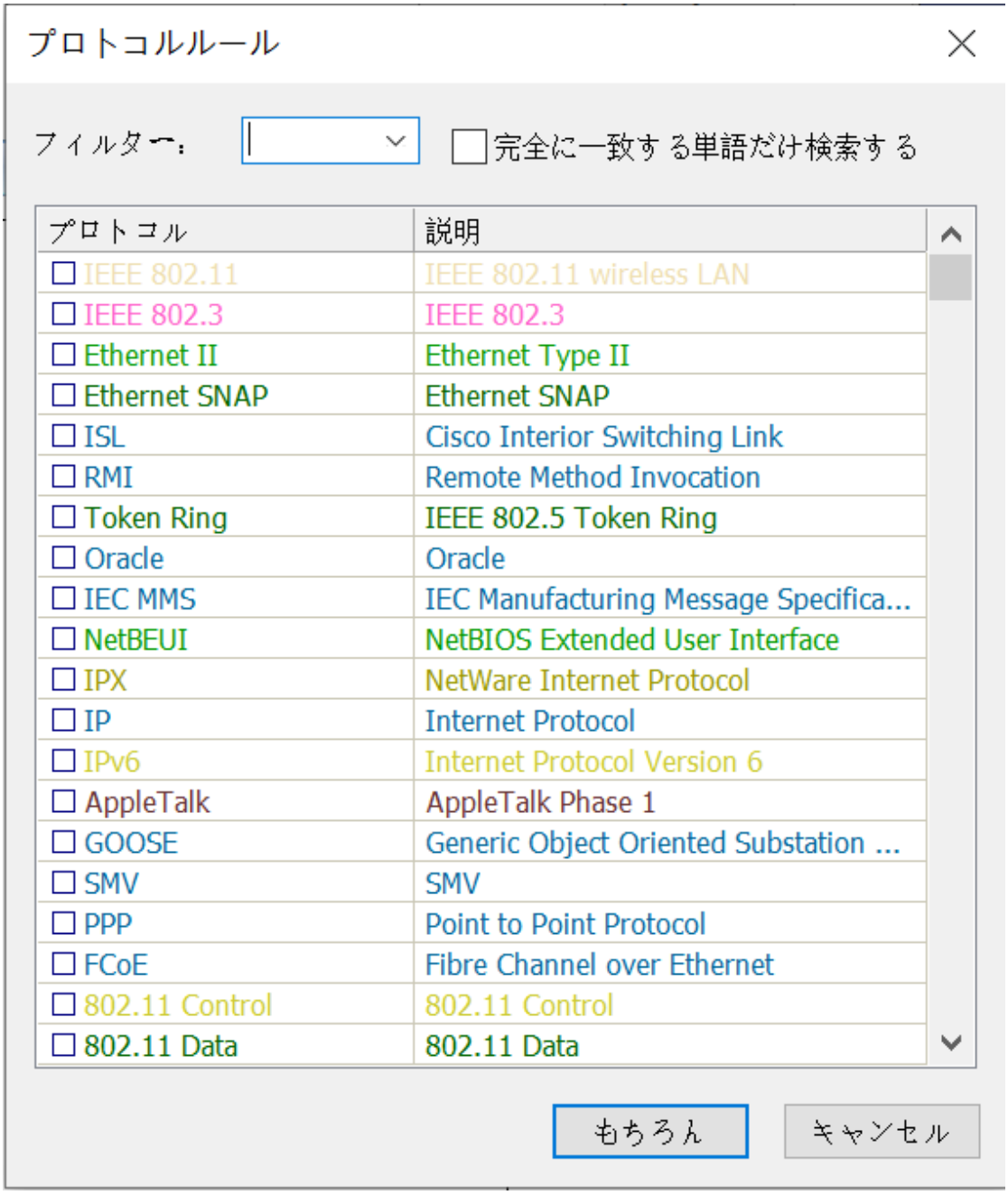
  システムはセッションの IP アドレスによるセッションフィルタリングをサポートしていますが、物理セッションはホームによるフィルタリングをサポートしていません。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



- セッションプロトコル
  1 つ以上のプロトコルを選択すると、システムはプロトコル情報に基づいてセッションをフィルタリングして表示します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

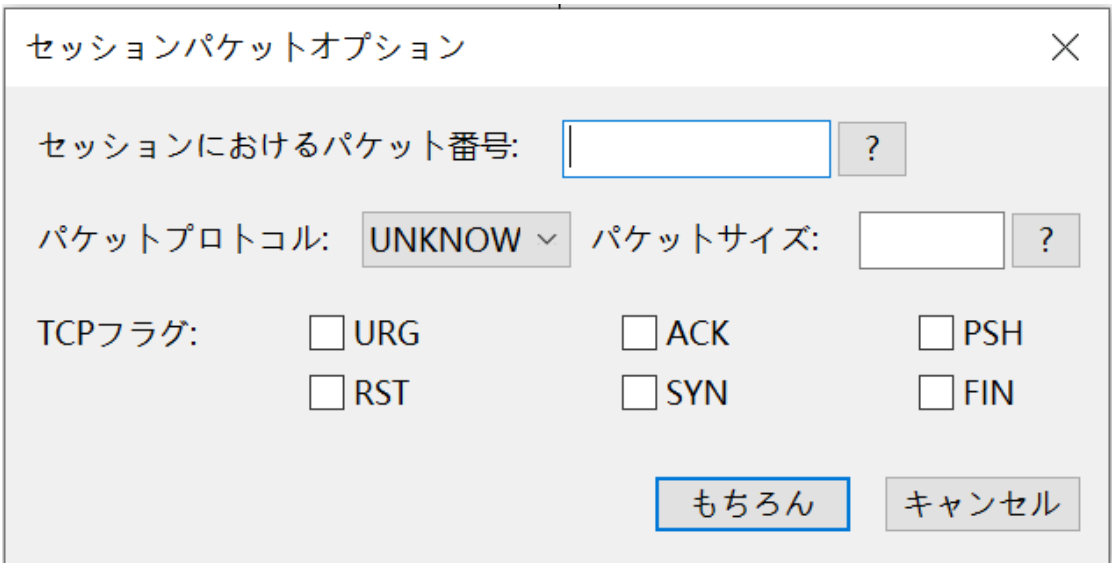


- セッションパケット
  セッション内のデータパケットのシーケンス番号：独立したセッション内のデータパケットのシーケンス番号を設定します。
  パケットプロトコル：パケットプロトコルタイプを選択します。
  パケットサイズ：このシーケンス番号のデータパケットのサイズを設定します。
  TCP フラグビット：このシーケンス番号を持つパケットのフラグビットをチェックするには、条件を満たす必要があります。 この設定は TCP セッションでのみ有効です

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- Note

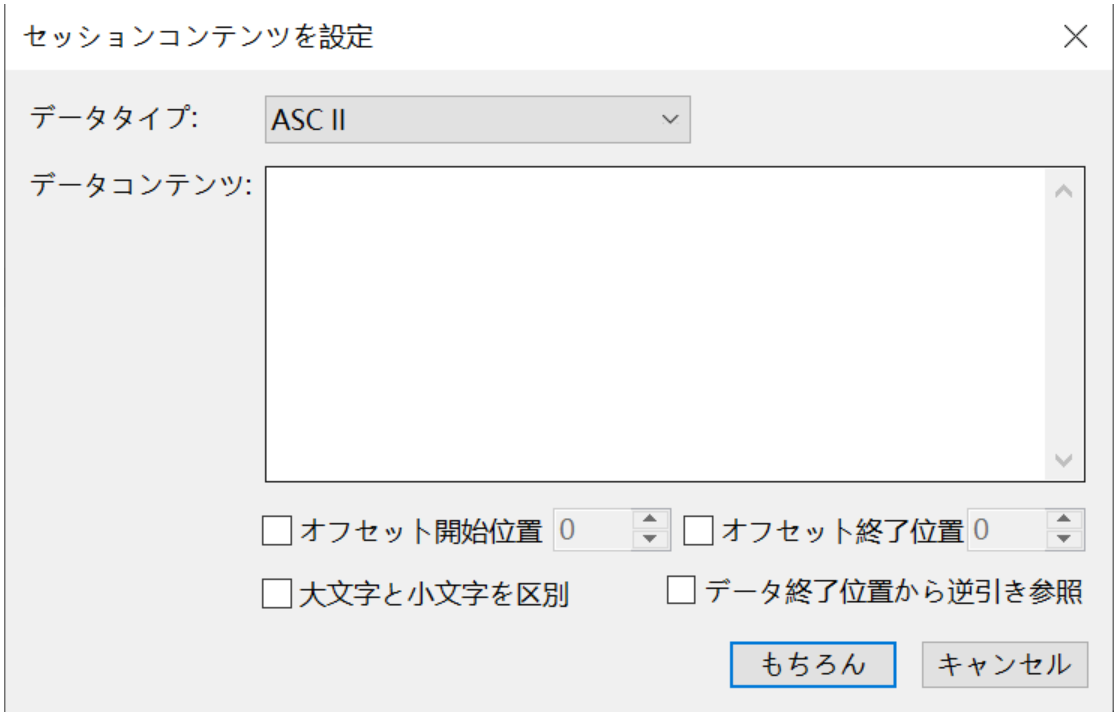
「セッション内のデータパケットのシーケンス番号」は、この条件の必須情報であり、1 つ以上のデータパケットサイズと TCP フラグを選択できます。



- セッションコンテンツ

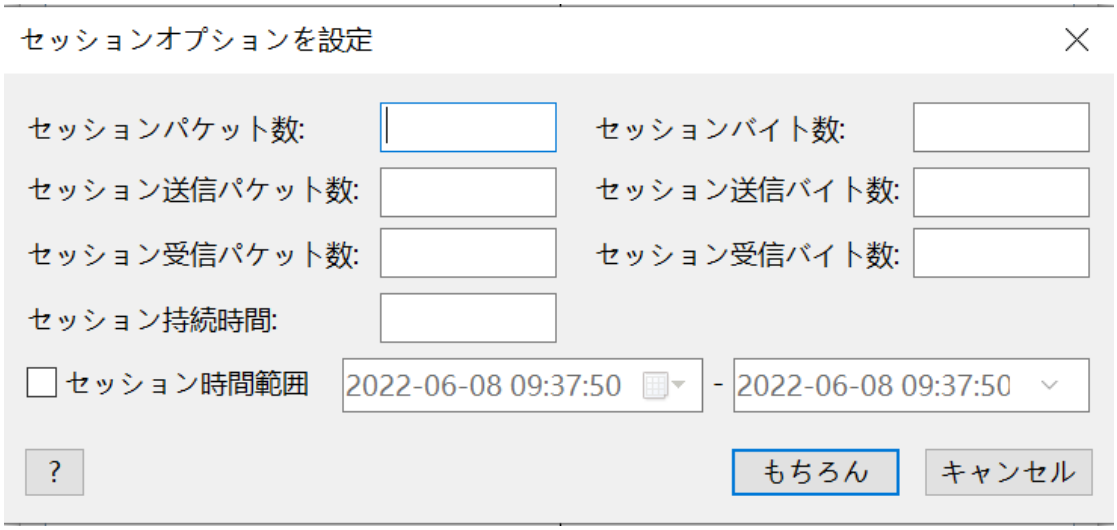
  システムは、セッションコンテンツによるセッションのフィルタリングをサポートしています。 セッションコンテンツを設定するときに、ASCII、HEX、UTF-8、UTF-16 などのセッションコンテンツのデータタイプを選択できます。 同時に、セッションコンテンツマッチングのオフセット位置とマッチング方法を設定することもできます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



- セッションプロパティ
  システムは、セッションの主要な属性によるフィルタリングをサポートしています。
  - セッションパケットの数：セッションに含まれるパケットの数。
  - セッションバイト数：セッションの合計通信バイト数.
  - セッションによって送信されたバイト数：このセッションによって送信されたバイト数
  - セッション受信バイト数：このセッションによって受信されたバイト数
  - セッションによって送信されたパケットの数：このセッションによって送信されたパケットの数。
  - セッション受信パケット数：このセッションで受信されたパケットの数。
  - セッション継続時間：セッションが継続した時間。
  - セッション時間範囲：特定の時間範囲内のセッションをフィルタリングします。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



フィルタの有効化

フィルタを設定した後、フィルタを受け入れるか拒否するかを選択できます。

- 承認：フィルター基準を満たすセッションのみがセッション統計に表示されます。
- 拒否：フィルター基準を満たすセッションは、セッション統計に表示されません

フィルタのインポート/エクスポート

[エクスポート]ボタンをクリックして、作成したフィルターをローカルにエクスポートできます。エクスポート形式は「.csconvflt」です。 [インポート]ボタンをクリックして、ローカルの「.csconvflt」ファイルをシステムにインポートし、セッションフィルターをすばやく追加することもできます。

8.10 設定を復元する

[ファイル復元設定]ダイアログボックスを以下に示します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ファイル復元設定

システムは、FTP 転送ファイル、TFTP 転送ファイル、HTTP 転送ファイ　ル、電子メールコピー、および SSL 証明書の抽出と完全な復元を提供します。

「ファイルをディスクに復元する」にチェックを入れると、復元するファイルの種類を設定したり、復元したファイルの保存パスを設定したりできます。チェックを外すと、ファイル復元機能が有効になりません。

Note

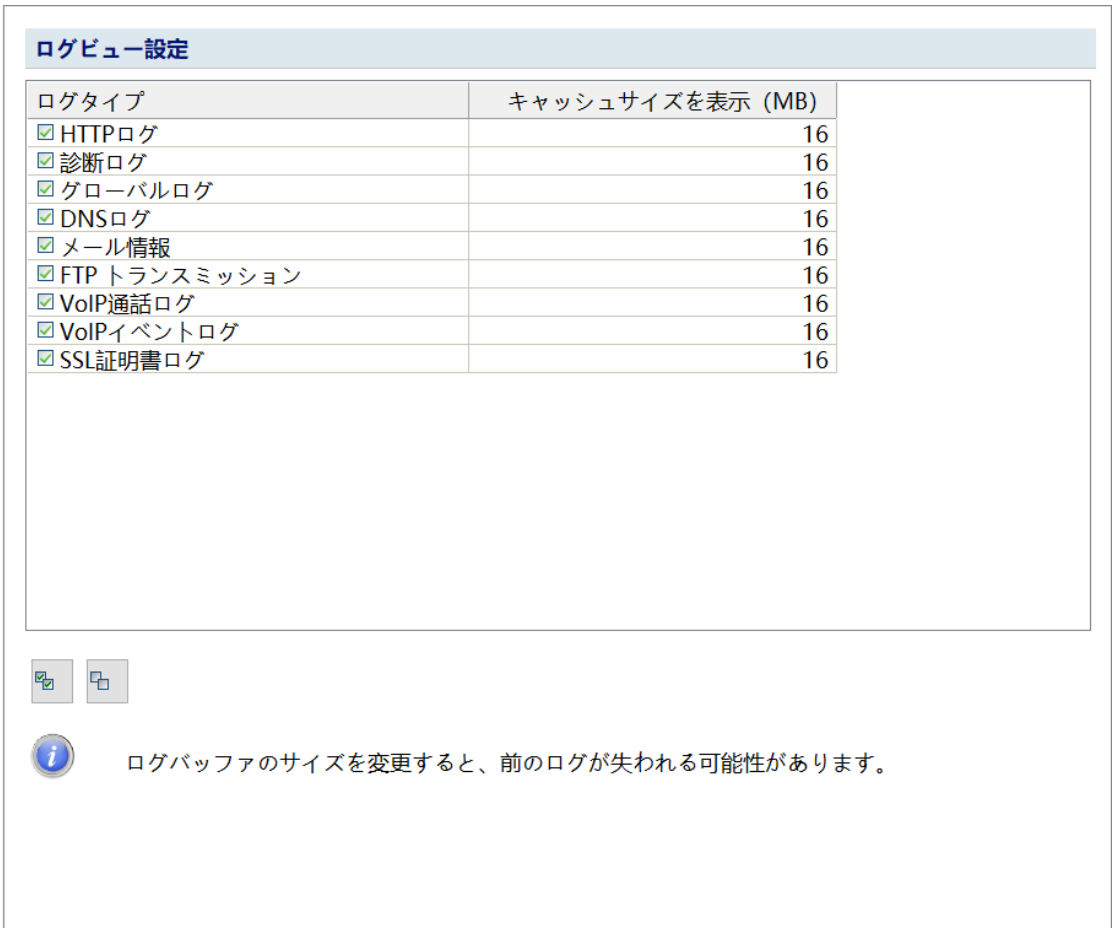
ファイル復元機能を有効にすると、システムの分析パフォーマンスに一定の影響があります。

8.11 ログ設定

Colasoft Capsa は、HTTP ログ、診断ログ、グローバルログ、DNS ログ、電子メール情報ログ、FTP 転送ログ、SSL 証明書ログ、VOIP 通話ログ、VOIP 時間

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ログログなど、さまざまな一般的なネットワークアプリケーションのログと保存をサポートしています。 このダイアログボックスで、ユーザーは有効にして記録する必要のあるログの種類を選択できます。次の図に示すように、さまざまな分析設定で有効になっているログオブジェクトは異なります。すべてのログはデフォルトで有効になっています。



さらに、ログタイプごとに表示キャッシュサイズとエクスポートログ設定を設定できます。ログオブジェクト設定で特定のタイプのログを選択しない場合、システムはログの統計と分析を実行しません。ログ内ビュー、このログの出力を表示できません。エクスポートログ設定で、MSN メッセージログなどの特定の種類のログを選択しない場合、ログファイルが自動的に保存されるときに MSN メッセージログは保存されません。

8.12 ログ保存

システムは、診断ログ、メールログ、HTTP Apache ログ、HTTP 拡張ログ、フ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ファイル転送ログなど、10 種類のログ分析とストレージを提供します。 特定の種類のログを保存する必要がある場合は、事前に[ログ設定]ダイアログボックスの[ログ設定のエクスポート]でそれらを選択する必要があります。

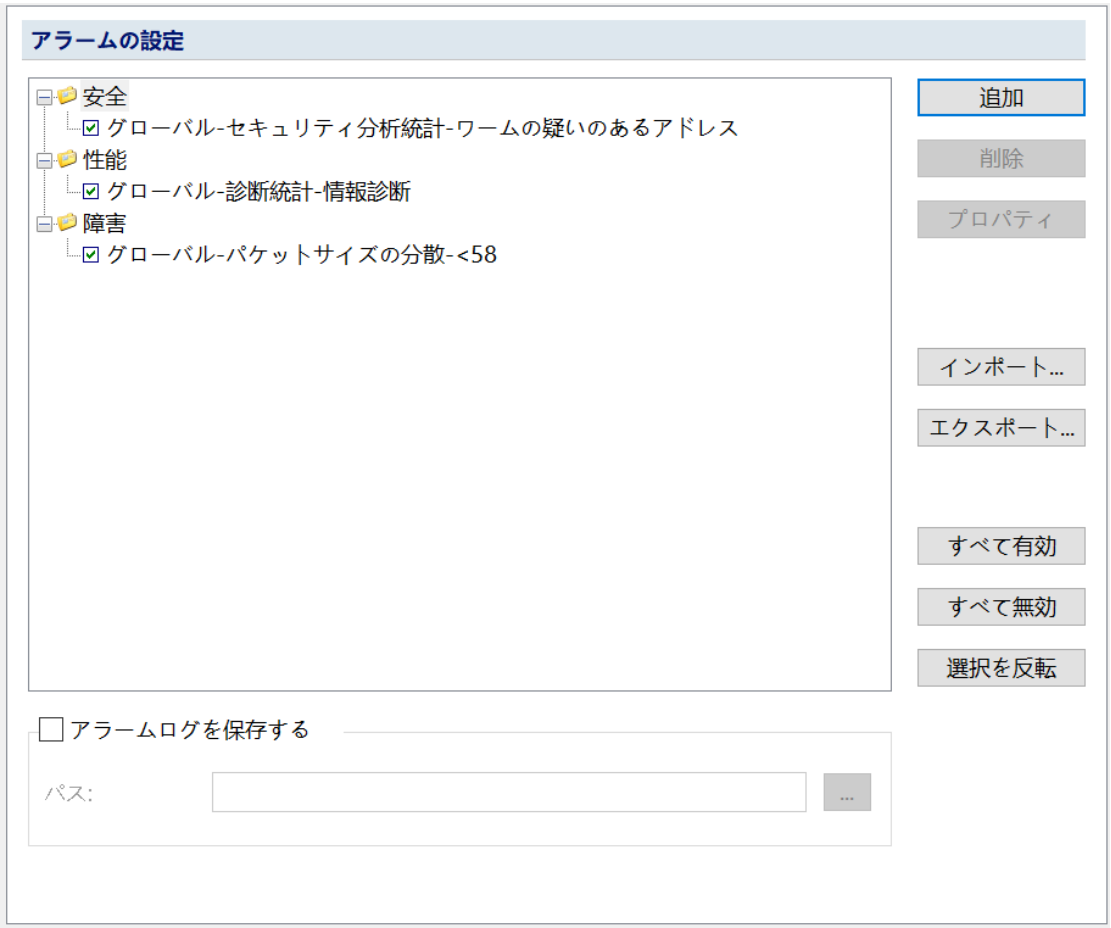
- ストレージパス：データパッケージストレージと同様に、ストレージパスをカスタマイズおよび変更でき、ストレージファイルをログファイルまたは csv ファイルに設定できます。
- ファイル分割間隔：ファイルサイズ（MB / KB）または時間（日/時間/分）で分割します。
- 保存ファイル数：分割ファイルの全部または一部を保持するように設定します。

設定が成功すると、対応するログフォルダがストレージパスの下に自動的に作成され、ログファイルが自動的に保存されます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

8.13 アラーム

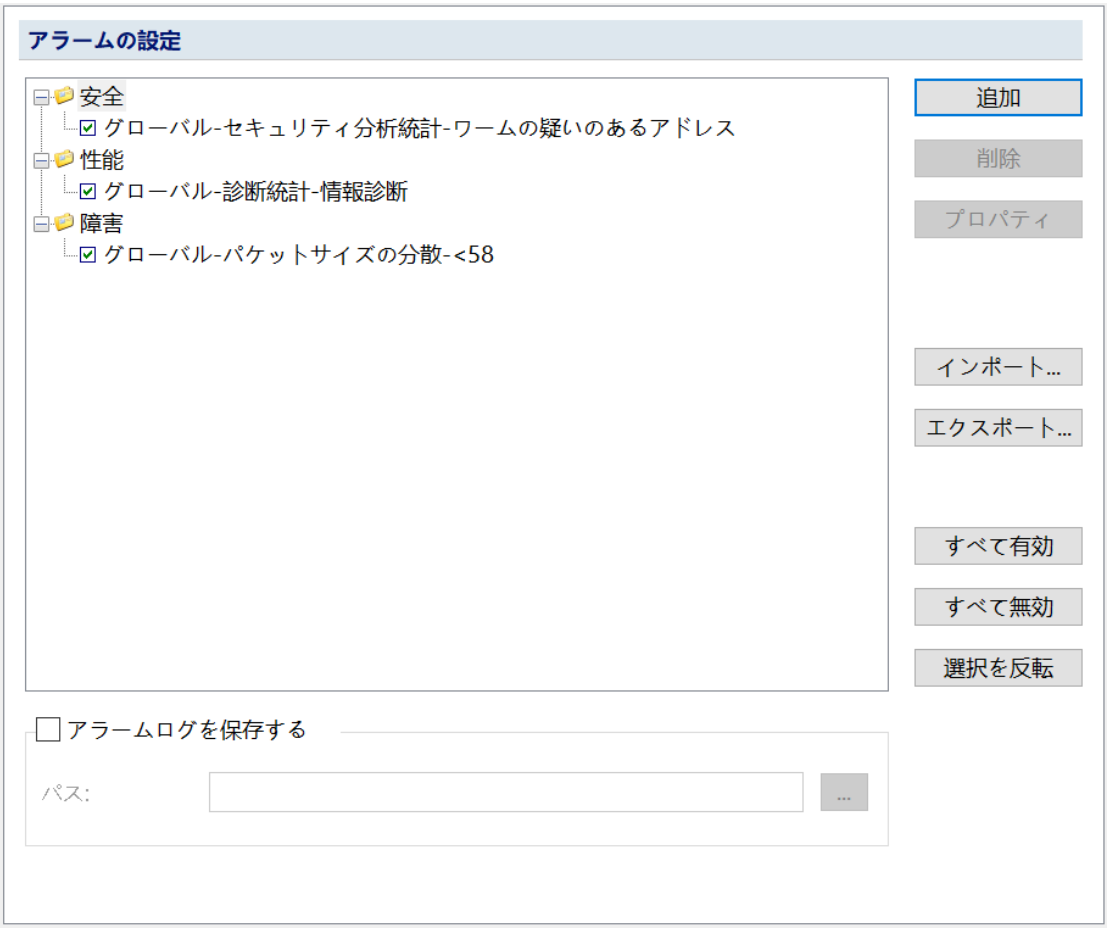
Web プロファイルの[アラート設定]ダイアログボックスには、作成したすべてのアラート情報が表示され、アラート条件を有効、無効、または編集したり、インポート/エクスポート操作を実行したりできます。 また、アラームログを自動保存するように設定することができ、アラームがトリガーされると、設定に応じてアラームがトリガーされたときの関連情報が自動的に保存されます。



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

8.14 アラームトリガーアクション

アラームがトリガーされたときに、アラームリマインダーの電子メールまたはサウンドを送信することを選択できます。ネットワークファイル構成では、事前にアラーム電子メールパラメータまたはアラームサウンドを設定する必要があります。 アラームトリガーアクション設定インターフェースを次の図に示します。



アラームメールパラメータ設定

送信者情報

- 送信者のアドレス：電子メールの送信者の電子メールアドレスを入力します。
- あなたの名前：送信者の名前を設定します。
- ユーザー名：送信者のログインメールボックスのユーザー名を設定するために使用されます。
- パスワード：送信者のログインメールボックスのパスワードを設定するために使用されます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

受信者情報

- 電子メールの件名：アラート電子メールの件名を設定するために使用されます。
- 受信者のアドレス：アラート受信者の電子メールアドレス。複数の受信者を同時に入力でき、複数の受信者は「;」で区切られます。

サーバー情報

- メールサーバー：メールサーバーのアドレスを設定するために使用されます。
- 暗号化：暗号化方式を設定するために使用されます。システムでサポートされている暗号化方式には、TLS と SSL が含まれます。
- ポート：メールサーバーのポートを設定するために使用されます。暗号化方式が SSL の場合、デフォルトのポートは 465 です。暗号化方式が TLS の場合、デフォルトのポートは 25 です。

アラーム音の設定

アラームがトリガーされたときのアラーム音をカスタマイズできます。アラーム音の形式は wav です。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

9 メインビュー領域

ネット通信パケットの深度診断分析を行った後、すべてのネット分析結果がメインビュー領域に表示されます。Capsa には以下のメインビューが含まれており、各ビューは異なる分析結果を示している。

ビュー	機能の説明
マイグラフ	グラフビューは、ユーザーに強力で多様なリアルタイムグラフ監視とカスタムグラフ設定を提供します。
概要統計	百近くの統計カウンタを提供して、ユーザーに非常に詳細なネットワーク統計情報を提供して、グラフィカルなインタフェース表示はユーザーがより直感的にネットワークの全体的な実行情報を表示するのを助けることができます。
診断	アプリケーション層/トランスポート層/ネットワーク層/データリンク層ネットワークイベントのリアルタイム診断と分析を提供し、ネットワーク障害イベントを自動的に提示し、ユーザーの直感的なネットワーク通信障害の発見を支援する。
プロトコル	OSI 7 層プロトコルに従い、実際のネットワークプロトコルのカプセル化順序に基づいて、階層化がユーザーに現れ、ユーザーがネットワークプロトコルの使用状況を迅速に位置付けし、表示するのに便利である。グローバルなプロトコル統計に加えて、各ネットワークのエンドポイントにおけるプロトコル統計も提供できます。
物理エンドポイント	ネットワーク中の物理エンドポイントの詳細な通信状況を提供し、各物理エンドポイントに対して、その総流量、パケット、送信流量、受信流量など 20 種類以上のパラメータ統計を詳細に統計する。
IP エンドポイント	ネットワーク中の IP エンドポイントの詳細な通信状況を提供し、各 IP エンドポイントに対して、その総流量、パケット、送信流量、受信流量などの多種のパラメータ統計を詳細に統計する。
物理セッション	ネットワーク内の物理アドレス間の通信セッションの状況を指定します。システムは、各セッションのソースアドレス、宛先アドレス、セッション総トラフィック、送信トラフィック、送信パケット、受信トラフィックなどのデータを詳細に統計する。
IP セッション	ネットワークにおける IP アドレス間の通信セッションの状況を提供する。システムは、各 IP セッションのソースアドレス、宛先アドレス、セッション総トラフィック、送信トラフィック、受信トラフィックなどのデータを詳細に統計する。
TCP セッション	詳細な TCP 接続通信セッション情報を提供します。また、TCP セッション関連パケット、データストリーム再編、TCP シーケンス図などを提供し、ユーザーが TCP 通信状況を迅速に分析するのに便利である。
UDP セッション	詳細な UDP 通信セッションの状況を提供します。ユーザは、ネットワーク内の UDP 通信を直感的かつ容易に分析することができる。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

矩阵	マトリックスビューは、ネットワーク内で通信されているノードとセッションを詳細に統計し、マトリックスを介してネットワーク全体の通信のノード/セッション情報、物理ホスト/IP ホストの通信ノード/セッション情報、セッションのホスト情報を理解することができます。
パケット	パケットサマリー復号、フィールド復号、16 進復号を提供する。パケットの内容を見ることで、ネットワーク上の問題を正確に特定することができ、アプリケーションのソースやその他の詳細を明確に理解することができ、複雑なデータストリームの中で存在する可能性のある問題を見つけることができます。
ログ	HTTP 要求、メール情報、DNS クエリ、FTP 転送など、一般的なネットワークアプリケーションログを提供します。ユーザーは、これらの詳細なログ情報の表示と保存をカスタマイズできます。
レポート	システムは、サマリー統計レポート、診断統計レポート、プロトコル統計レポート、TOP N シリーズレポートなどの様々なタイプのレポート出力を提供し、カスタムレポート生成時間、会社 ID、作成者などのパラメータをサポートします。

次に、各ビューには独自のツールバーがあり、ユーザーはこれらのビューツールを使用してデータのフィルタリング、フィルタリング、コピーなどの操作を行うことができます。

分析結果を表示する際には、データのソートを使用してデータの高速フィルタリングを行うことができます。帯域幅が最大またはネットワークが最もアクティブなホストを分離するのは、非常に容易なことです。

ビューに表示されるコンテンツについても、ユーザは自分の必要に応じて、データ表示を設定することができる。

科来ネットワーク分析システムの各ビューは、ユーザーに非常に豊富な統計フィールドを提供しており、表示に適したためにすべてのフィールドを表示していません。ユーザーは、リストオプションを使用して表示されるデータを設定し、各ビューフィールドのタイトルを右クリックすると、表示オプションを開くことができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

各セッションビューでは、管理者は次のこともできます:

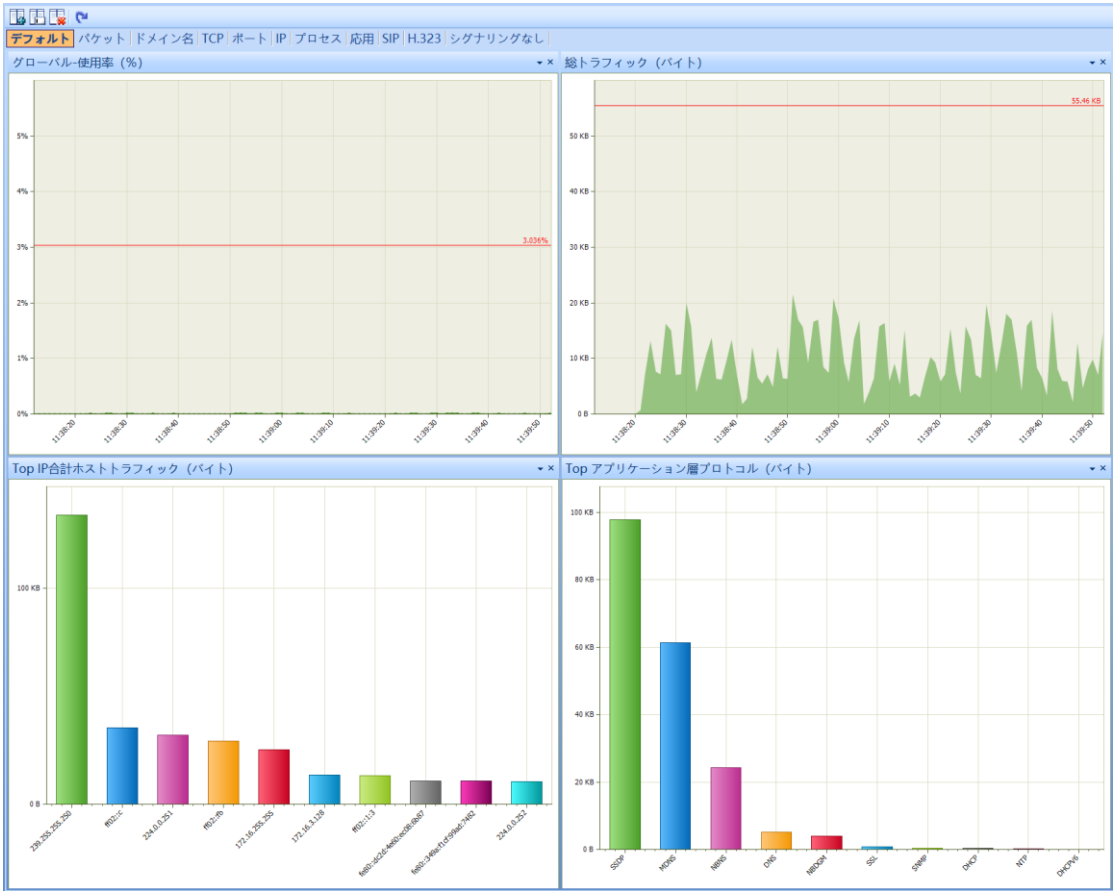
- 検索条件を設定し、表示データを素早く検索する
- 表示オプションを設定し、表示するデータ列をカスタマイズする
- ダブルクリックして新しいウィンドウを開き、セッションの詳細を見る
- 保存セッション情報のエクスポート
- セッションによるフィルタの生成
- セッション通信ノードをノードブラウザにナビゲートする
- 名前テーブルに MAC アドレスまたは IP アドレスを追加する
- ビューのリフレッシュ時間を調整し、最新のセッションを素早く表示する
- データ関連サブウィンドウビューを表示し、関連付けられたデータを迅速に分析する

9.1 グラフ（マイグラフ）

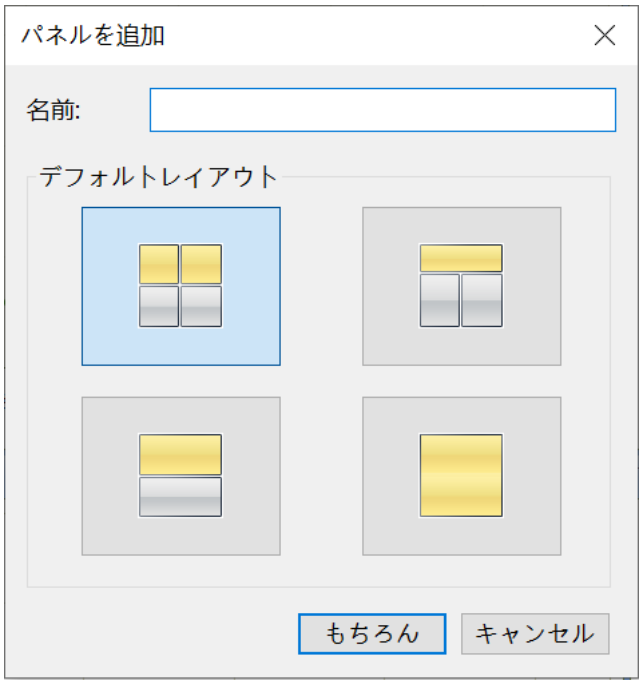
Caspa システムは強力なグラフビューを提供し、統計分析データをより直感的に読みやすく表現し、折れ線図、棒グラフ、面積図、円グラフなどの多種の形式を提供し、ネットワークデータの動きを便利に表現することができる。

ユーザーはグラフビューに新しいグラフパネルをカスタマイズして追加することができ、このパネルに様々な種類のグラフを作成することができ、ネットワークグローバルグラフを作成することができるだけでなく、様々なネットワークオブジェクトに対して簡単にグラフ表示をカスタマイズすることができ、非常に柔軟で便利で、管理者がネットワークに対する応用分析管理をネットワーク全体、各ホストまで大きくすることができ、様々なネットワークデータ情報をより直感的に表示することができる。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

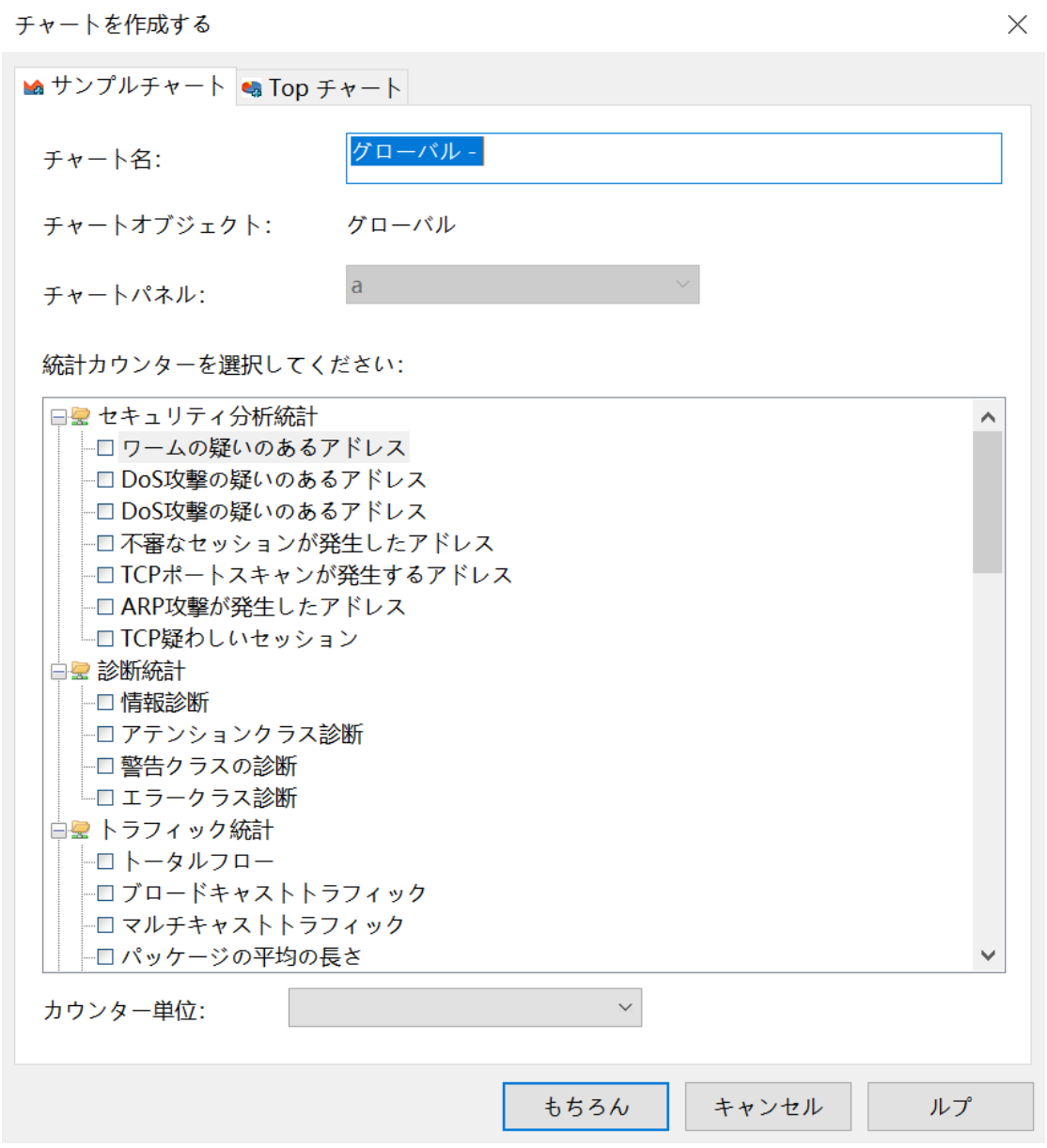


ビューツールバーの[新規パネル]ボタンをクリックして、次の図のようにグラフサブパネルを新規作成します。：



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

新規パネルのタイトルを入力し、グラフのレイアウトを選択し、[OK]をクリックすると、新しいグラフパネルが作成され、新規グラフパネルで、[グラフを追加]をクリックして、次のダイアログボックスが表示されます:



ユーザーは、このダイアログボックスで作成するグラフの種類を選択できます。

グラフビューは、ユーザーに複数のデータ型の統計を提供します:

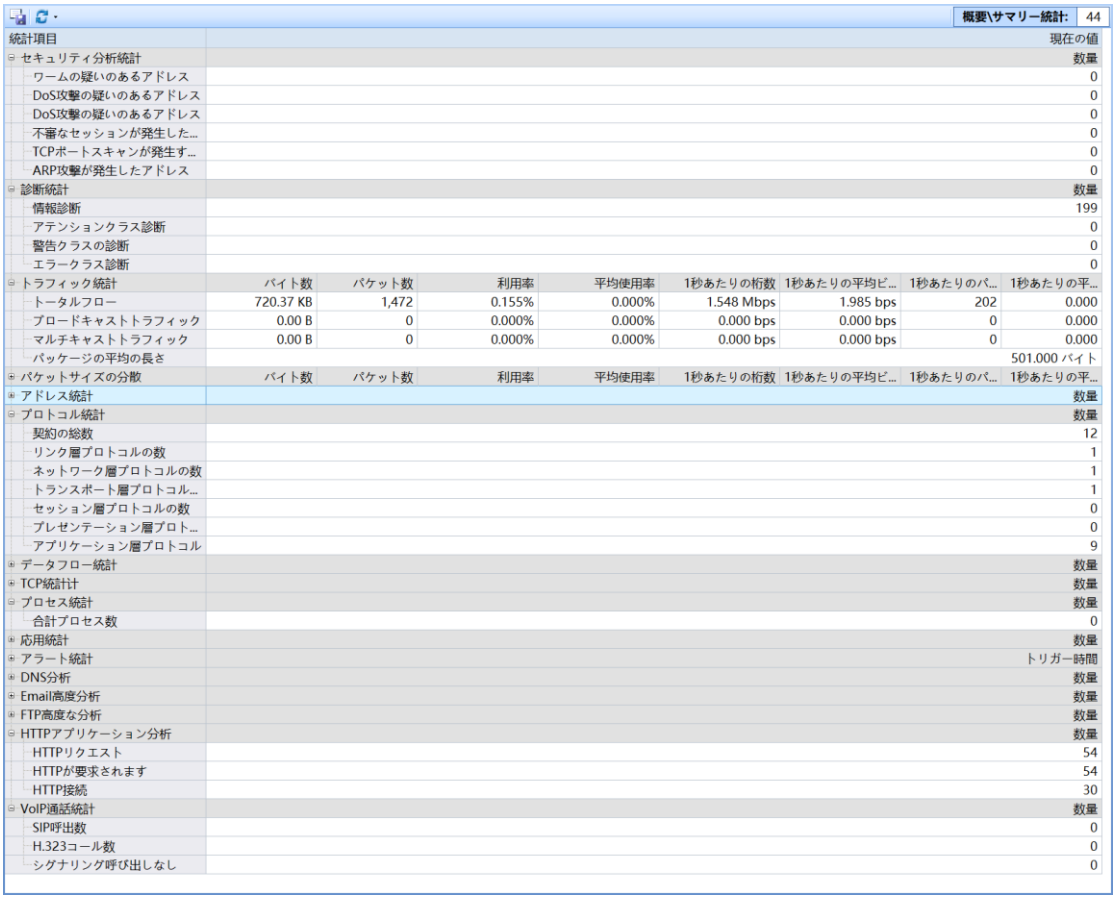
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

グラフ	説明
サンプリンググラフ	アラート統計、診断統計、トラフィック統計、パケットサイズ分布、アドレス統計、プロトコル統計、データフロー統計、TCP 分析、DNS 分析、HTTP 分析、FTP 分析などの多種のサンプリングチャートの種類を含む。これらの情報により、ネットワークの動作状態が合理的であるか、ネットワークトラフィックが大きすぎるか、ネットワークブロードキャストトラフィックが異常であるか、ブロードキャスト嵐が存在するか、ネットワーク中のパケットのサイズ分布が合理的であるか、破片攻撃が存在するかなどの不審な行為が直感的にわかる。
TOP N グラフ	ネットワークにおける物理アドレス総流量、物理アドレス受信流量、物理アドレス送信流量、IP アドレス総流量、IP アドレス送信流量、IP アドレス受信流量、遠隔 IP アドレス総流量、遠隔 IP アドレス送信流量、遠隔 IP アドレス受信流量及び物理アドレス群、IP アドレス群などの流量パラメータ TOP N 統計グラフに対して、それぞれパケット及びバイト数の 2 種類の単位で統計することができ、システムのデフォルト統計値は TOP 10 で、統計の TOP 数をカスタマイズできます。これらの情報により、ネットワーク内で TOP 10 にランクインしているホストの動作状態が異常またはビジー状態であるかどうかを判断することができます。

9.2 概要統計

Capsa システムの統計機能は非常に強力で、百近くの統計カウンタはユーザーに非常に詳細な統計情報を提供し、ユーザーがネットワークの全体的な運行状況をより直感的に見ることができるようにする。「≪サマリー統計|SummaryStatistics|emdw≫」ビューでは、ネットワーク・グローバルの実行情報を表示するだけでなく、ネットワーク・プロトコルとネットワーク・ノードごとに独自のサマリー統計が表示されるため、各プロトコルまたはノードのサマリー統計を簡単に表示できます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



概要\サマリー統計: 44

統計項目								現在の値
セキュリティ分析統計								数量
ワームの疑いのあるアドレス								0
DoS攻撃の疑いのあるアドレス								0
DoS攻撃の疑いのあるアドレス								0
不審なセッションが発生した...								0
TCPポートスキャンが発生す...								0
ARP攻撃が発生したアドレス								0
診断統計								数量
情報診断								199
アテンションクラス診断								0
警告クラスの診断								0
エラークラス診断								0
トラフィック統計	バイト数	パケット数	利用率	平均使用率	1秒あたりの桁数	1秒あたりの平均ビ...	1秒あたりのパ...	1秒あたりの平...
トータルフロー	720.37 KB	1,472	0.155%	0.000%	1.548 Mbps	1.985 bps	202	0.000
ブロードキャストトラフィック	0.00 B	0	0.000%	0.000%	0.000 bps	0.000 bps	0	0.000
マルチキャストトラフィック	0.00 B	0	0.000%	0.000%	0.000 bps	0.000 bps	0	0.000
パッケージの平均の長さ								501.000 バイト
パケットサイズの分散	バイト数	パケット数	利用率	平均使用率	1秒あたりの桁数	1秒あたりの平均ビ...	1秒あたりのパ...	1秒あたりの平...
アドレス統計								数量
プロトコル統計								数量
契約の総数								12
リンク層プロトコルの数								1
ネットワーク層プロトコルの数								1
トランスポート層プロトコル...								1
セッション層プロトコルの数								0
プレゼンテーション層プロト...								0
アプリケーション層プロトコル								9
データフロー統計								数量
TCP統計計								数量
プロセス統計								数量
合計プロセス数								0
応用統計								数量
アラート統計								トリガー時間
DNS分析								数量
Email高度分析								数量
FTP高度な分析								数量
HTTPアプリケーション分析								数量
HTTPリクエスト								54
HTTPが要求されます								54
HTTP接続								30
VoIP通話統計								数量
SIP呼出数								0
H.323コール数								0
シグナリング呼び出しなし								0

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

次は、概要統計の統計情報の説明です：

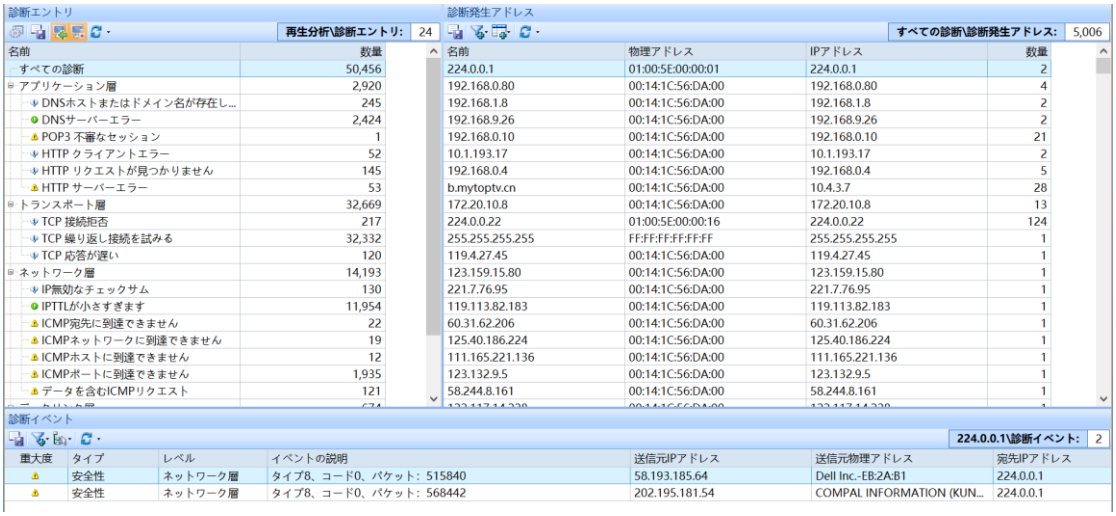
ネーム	説明
診断統計	現在のネットワークで発生しているネットワークイベントを情報/注意/警告/エラーの 4 種類で集計します。
トラフィック統計	ネットワークの総トラフィック、ブロードキャストトラフィック、マルチキャストトラフィックなどを詳細に統計し、ユーザーは現在のトラフィックが正常であるかどうかを迅速に確認することができます。
パケットサイズ分布	現在のネットワーク通信のパケットサイズ分布状況を詳細に統計し、ユーザーは各タイプのパケットの流量、パケット数、毎秒パケット数などを直感的に見ることができる。
アドレス統計	ネットワーク通信の物理アドレス数、IP アドレス数、ローカル IP アドレス数及びリモート IP アドレス数を統計する。
プロトコル統計	ネットワーク通信の総プロトコル数を統計し、OSI モデル別に階層的に統計する。
数据流統計	ネットワーク通信の物理セッション数、IP セッション数、TCP セッション数及び UDP セッション数を統計する。
TCP 統計	TCP 同期送信パケット、TCP 同期確認送信パケット、TCP 終了接続送信パケット及び TCP リセット送信パケットの個数を集計する。
アラート統計	現在トリガーされているアラートの数は、パフォーマンス/セキュリティ/障害の 3 種類で個別に集計されます。
DNS 統計	DNS クエリとレスポンスのそれぞれのパケット数を統計します。
E-mail 分析	SMTP 接続と POP 3 接続の通信数をそれぞれ集計する。
FTP 分析	FTP アップロードと FTP ダウンロードの数を集計します。
HTTP 分析	HTTP 要求と HTTP 接続の数を統計します。

9.3 診断

専門家診断は Caspa システムの重要な機能であり、新しい診断ビューレイアウトを提供し、診断階層、診断発生アドレス、詳細なイベント記述ウィンドウを含む 3 つの分割サブウィンドウを採用し、各ウィンドウに異なるデータ情報を表示し、リアルタイムのデータフィルタリングを提供する。診断階層ウィンドウでイベントを選択すると、イベントをトリガーするホストアドレスが自動的にフィルタリングされ、イベントウィンドウにイベントの詳細な説明が表示されます。各診断情報がどのホストによってトリガーされたのか、各診断イベントの詳細な説明が非常に直感的に表示され、パケットの詳細を理解する必要なく、エキスパート診断モジュールからネットワーク内のエラーとトラブルシューティングを取得できます。。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

診断モジュールはそれぞれ OSI 7 層プロトコルとタイプに基づいてエラー情報をグループ化することができ、現在、製品は 4 つの階層の故障診断をサポートしている：応用層、伝送層、ネットワーク層、データリンク層、一方、タイプ別には、障害、パフォーマンス、セキュリティの 3 種類の障害情報が表示され、異なるプロトコル・レベルまたは異なるタイプのネットワーク・エラーと障害をそれぞれ表示できます。



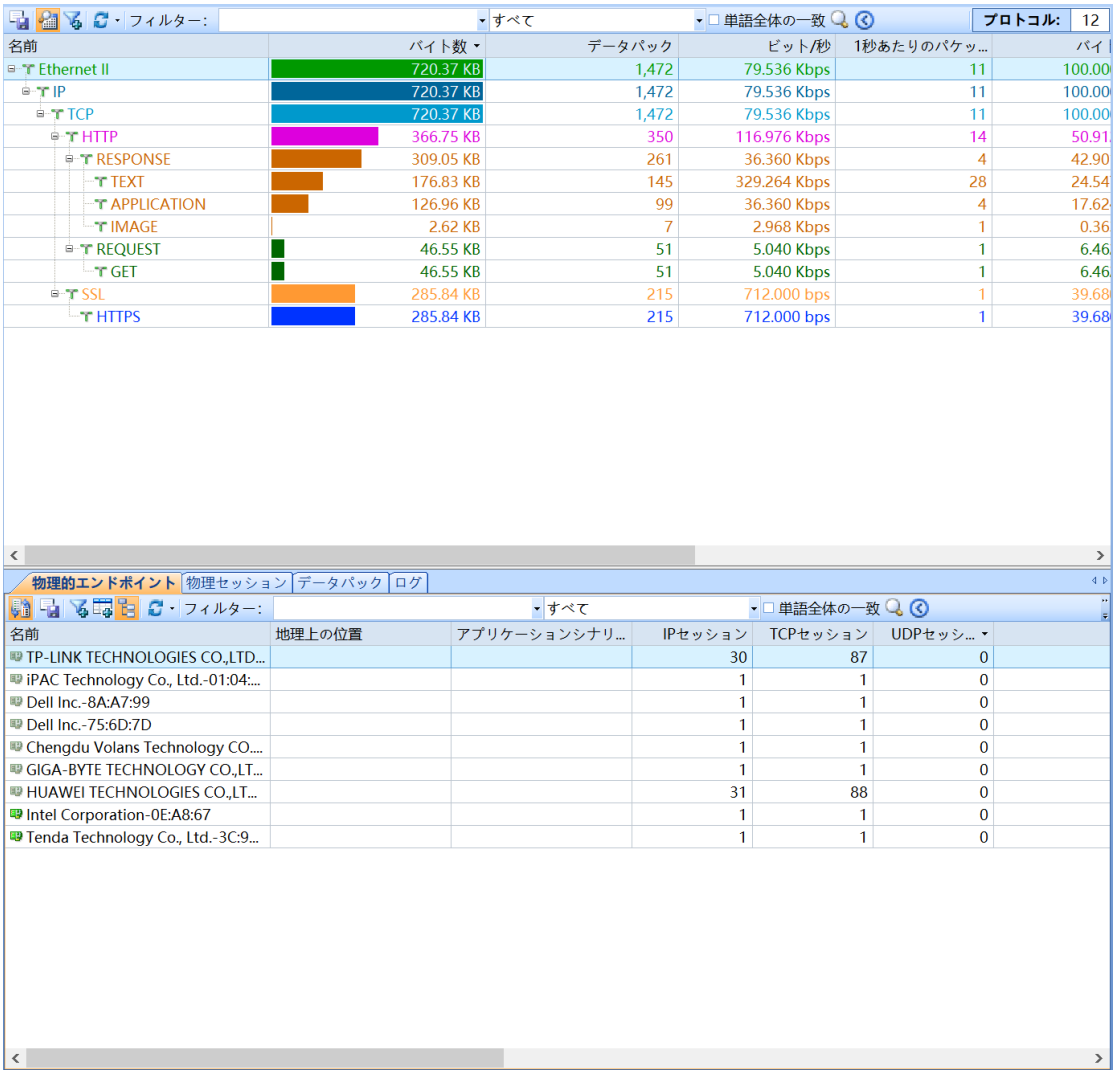
ネットワークエラーと障害には、通常の情報ヒント、重大なエラー警告の 4 つのセキュリティレベルがあります、次の表に示すように：

セキュリティレベル	アイコン	説明
メッセージ		通常の情報通知は、イベントを記録するために使用されるだけで、ネットワークエラーはありません。
注意		ネットワークイベントや特定のイベントを提示するには、ユーザーが重視するコンテンツが必要です。
警告		エラーや障害に対する警告メッセージは、ユーザーがタイムリーに処理する必要があります。
重大		これは重大なエラーや重大な障害に関するヒントであり、ユーザーはタイムリーに処理する必要があります。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

9.4 プロトコル統計

OSI 7 層プロトコルの分析に従い、実際のネットワークプロトコルのカプセル化順序に基づいて、ユーザーに階層化され、グローバルなプロトコル統計のほか、各ネットワークノードの下のプロトコル統計データを提供することができる。



プロトコルビューはネットワークでデータ通信に使用されるプロトコルを効果的に表示することができ、プロトコルはツリーレベルで表示され、各プロトコルに対して、使用されているトラフィック、このプロトコルを使用しているパケット数、このプロトコルのトラフィックの総トラフィックにおける割合、およびこのプロトコルを使用しているパケットの総パケットにおける割合を統計し、図に示されています。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

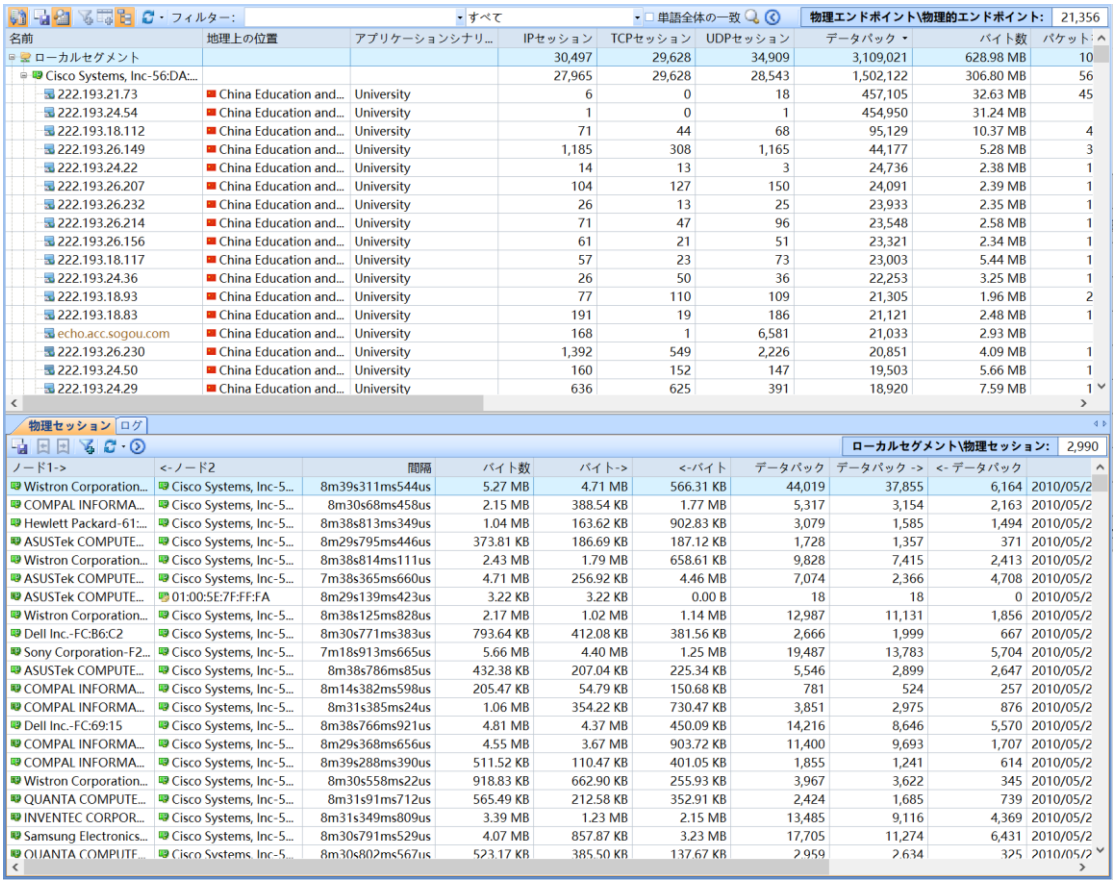
プロトコルビューによる各ビューの占有流量とパーセンテージの統計により、ユーザーは現在のネットワークで最も占有流量の多いプロトコル、すなわち現在のネットワークで最も占有量の多いサービスタイプを得ることができ、また、ネットワーク速度が遅い、メールワームウイルス攻撃、ネットワーク時間が途切れている、ユーザーがインターネットに接続できないなどのネットワーク障害を調査するのに役立ちます。

プロトコル・ビュー・ツールバーの「詳細表示」ボタンをクリックすると、プロトコル・リストでプロトコルを選択すると、プロトコル通信を使用して物理アドレスまたは IP アドレス情報が自動的にフィルタリングされ、データの関連付け分析が容易になります。

9.5 物理エンドポイント

ネットワークエンドポイントはネットワーク通信における重要な構成部分であり、科来ネットワーク分析システムはネットワークエンドポイントを物理エンドポイントと IP エンドポイントに分け、ネットワークエンドポイント統計分析機能を通じて、ユーザーは通信量が最大の IP エンドポイントと物理エンドポイントを迅速に位置決めすることができる。物理的なポイントのビューでは、システムは物理的なエンドポイントの詳細な通信解析を提供し、データリンク層のネットワーク通信状況をよりよく分析するのに役立ちます。物理エンドポイントビューには最大 20 種類以上のパラメータ統計があり、統計と表示が必要なパラメータをカスタマイズできます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



物理的なエンドポイントのビューを通じて、ユーザーは現在のネットワーク中のすべての物理アドレスの通信情報を非常に明確に見ることができて、物理アドレスグループまたは単一の物理アドレスの具体的な流量占有状況、例えば総流量が最大の MAC アドレス、送信流量が最大の MAC アドレス、受信流量が最大の MAC アドレス、送受信パケット数が最も多い MAC アドレスなど、統計パラメータの列ヘッダーを右クリックして、より多くの統計パラメータを表示することができます。

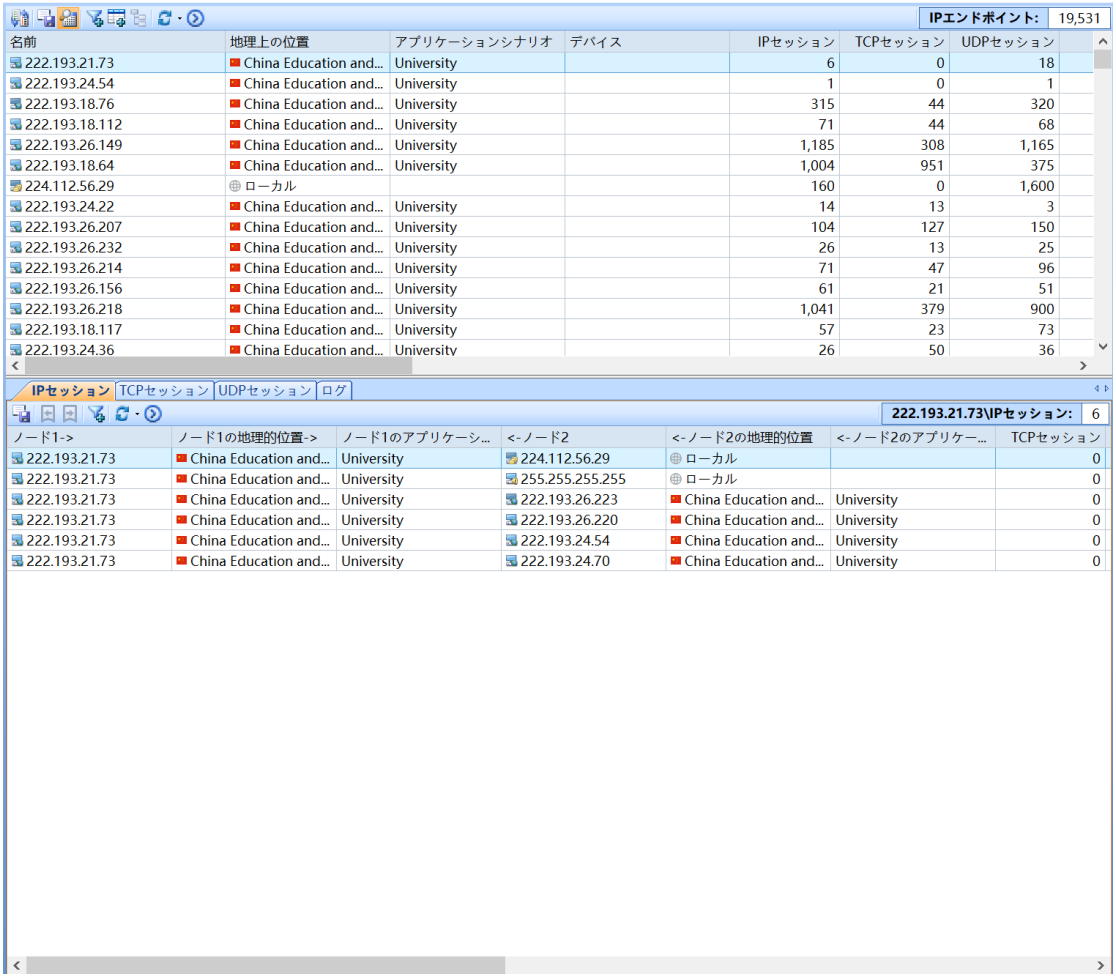
物理エンドポイント表示ツールバーで、「詳細表示」ボタンをクリックして、現在選択されている物理アドレスの通信セッション情報をすばやく表示するための物理セッション区切りサブウィンドウを自動的に表示または非表示にします。

9.6 IP エンドポイント

IP エンドポイントビューでは、システムは IP アドレスの詳細な通信解析と統計を提供している。IP エンドポイントの統計解析機能により、ユーザーは通信

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

トラフィックが最も大きい IP アドレスまたは IP アドレスグループを迅速に特定することができる。これらの情報により、ネットワークにブロードキャスト/マルチキャストの嵐が存在するかどうかを特定し、ネットワーク速度が遅い、ネットワーク時間が途切れている、ワームウイルス攻撃、DOS 攻撃、ユーザーがインターネットに接続できないなどのネットワーク障害を調査するのに役立てることができます。



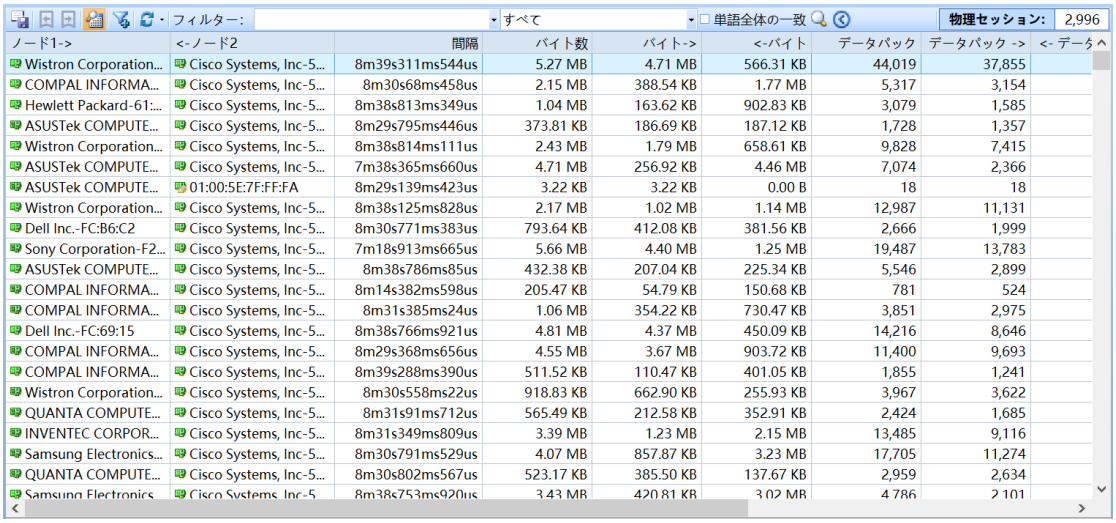
IP エンドポイントビューには、IP セッション、TCP セッション、UDP セッションのサブウィンドウが含まれており、IP エンドポイントリストで IP アドレスを選択すると、その IP アドレスを表示するすべての通信セッション情報が自動的にフィルタリングされ、操作分析ステップが簡略化され、分析効率が向上します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

9.7 物理セッション

Capsa システムはネットワーク通信セッションの分析と統計を強化し、ネットワーク中の物理セッション、IP セッション、TCP セッション及び UDP セッションを独立したビューとしてユーザーに異なるセッション情報を見せる。

各セッション情報は、ソースアドレス、宛先アドレス、セッションの総トラフィック、送受信されたパケット、およびこれらのパケットのサイズなど多くのパラメータを詳細に統計し、物理セッションビューを通じて現在のネットワークにおける物理アドレス間の通信セッションの状況を知ることができます。以下の図に示します:

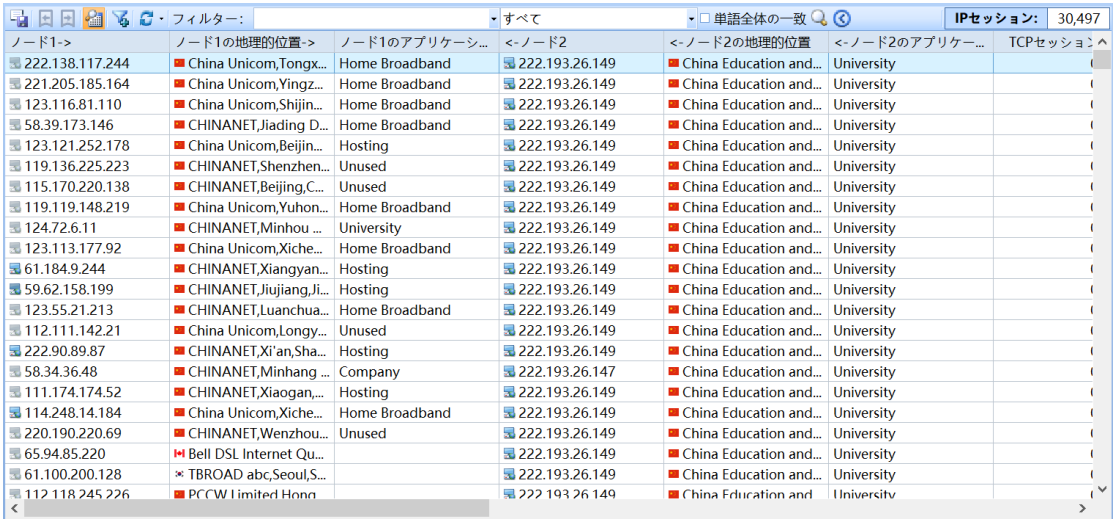


ノード1->	<-ノード2	間隔	バイト数	バイト->	<-バイト	データパック	データパック ->	<- データ
Wistron Corporation...	Cisco Systems, Inc-5...	8m39s311ms544us	5.27 MB	4.71 MB	566.31 KB	44,019	37,855	
COMPAL INFORMA...	Cisco Systems, Inc-5...	8m30s68ms458us	2.15 MB	388.54 KB	1.77 MB	5,317	3,154	
Hewlett Packard-61:...	Cisco Systems, Inc-5...	8m38s813ms349us	1.04 MB	163.62 KB	902.83 KB	3,079	1,585	
ASUSTek COMPUTE...	Cisco Systems, Inc-5...	8m29s795ms446us	373.81 KB	186.69 KB	187.12 KB	1,728	1,357	
Wistron Corporation...	Cisco Systems, Inc-5...	8m38s814ms111us	2.43 MB	1.79 MB	658.61 KB	9,828	7,415	
ASUSTek COMPUTE...	Cisco Systems, Inc-5...	7m38s365ms660us	4.71 MB	256.92 KB	4.46 MB	7,074	2,366	
ASUSTek COMPUTE...	01:00:5E:7F:FF:FA	8m29s139ms423us	3.22 KB	3.22 KB	0.00 B	18	18	
Wistron Corporation...	Cisco Systems, Inc-5...	8m38s125ms828us	2.17 MB	1.02 MB	1.14 MB	12,987	11,131	
Dell Inc.-FC:B6:C2	Cisco Systems, Inc-5...	8m30s771ms383us	793.64 KB	412.08 KB	381.56 KB	2,666	1,999	
Sony Corporation-F2...	Cisco Systems, Inc-5...	7m18s913ms665us	5.66 MB	4.40 MB	1.25 MB	19,487	13,783	
ASUSTek COMPUTE...	Cisco Systems, Inc-5...	8m38s786ms85us	432.38 KB	207.04 KB	225.34 KB	5,546	2,899	
COMPAL INFORMA...	Cisco Systems, Inc-5...	8m14s382ms598us	205.47 KB	54.79 KB	150.68 KB	781	524	
COMPAL INFORMA...	Cisco Systems, Inc-5...	8m31s385ms24us	1.06 MB	354.22 KB	730.47 KB	3,851	2,975	
Dell Inc.-FC:69:15	Cisco Systems, Inc-5...	8m38s766ms921us	4.81 MB	4.37 MB	450.09 KB	14,216	8,646	
COMPAL INFORMA...	Cisco Systems, Inc-5...	8m29s368ms656us	4.55 MB	3.67 MB	903.72 KB	11,400	9,693	
COMPAL INFORMA...	Cisco Systems, Inc-5...	8m39s288ms390us	511.52 KB	110.47 KB	401.05 KB	1,855	1,241	
Wistron Corporation...	Cisco Systems, Inc-5...	8m30s558ms22us	918.83 KB	662.90 KB	255.93 KB	3,967	3,622	
QUANTA COMPUTE...	Cisco Systems, Inc-5...	8m31s91ms712us	565.49 KB	212.58 KB	352.91 KB	2,424	1,685	
INVENTEC CORPOR...	Cisco Systems, Inc-5...	8m31s349ms809us	3.39 MB	1.23 MB	2.15 MB	13,485	9,116	
Samsung Electronics...	Cisco Systems, Inc-5...	8m30s791ms529us	4.07 MB	857.87 KB	3.23 MB	17,705	11,274	
QUANTA COMPUTE...	Cisco Systems, Inc-5...	8m30s802ms567us	523.17 KB	385.50 KB	137.67 KB	2,959	2,634	
Samsung Electronics	Cisco Systems, Inc-5	8m38s753ms920us	3.43 MB	420.81 KB	3.02 MB	4,786	2,101	

9.8 IP セッション

IP アドレスセッションビューでは、ネットワーク内の IP アドレスの通信セッション情報を詳細に解析して表示します。IP アドレスセッションごとに、ソースアドレス、宛先アドレス、セッショントラフィック、セッション送受信のパケット、およびこれらのパケットのサイズなどの統計パラメータを統計することができます。そして、現在選択されている IP アドレスに関連付けられている TCP および UDP セッションを下のサブウィンドウに表示します。これらのセッション情報により、現在のネットワークにおける IP アドレスセッションの状況をすばやく知ることができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



ノード1->	ノード1の地理的位置->	ノード1のアプリケーシ...	<-ノード2	<-ノード2の地理的位置	<-ノード2のアプリケー...	TCPセッション
222.138.117.244	China Unicom,Tongx...	Home Broadband	222.193.26.149	China Education and...	University	
221.205.185.164	China Unicom,Yingz...	Home Broadband	222.193.26.149	China Education and...	University	
123.116.81.110	China Unicom,Shijin...	Home Broadband	222.193.26.149	China Education and...	University	
58.39.173.146	CHINANET,Jiading D...	Home Broadband	222.193.26.149	China Education and...	University	
123.121.252.178	China Unicom,Beijin...	Hosting	222.193.26.149	China Education and...	University	
119.136.225.223	CHINANET,Shenzhen...	Unused	222.193.26.149	China Education and...	University	
115.170.220.138	CHINANET,Beijing,C...	Unused	222.193.26.149	China Education and...	University	
119.119.148.219	China Unicom,Yuhon...	Home Broadband	222.193.26.149	China Education and...	University	
124.72.6.11	CHINANET,Minhou ...	University	222.193.26.149	China Education and...	University	
123.113.177.92	China Unicom,Xiche...	Home Broadband	222.193.26.149	China Education and...	University	
61.184.9.244	CHINANET,Xiangyan...	Hosting	222.193.26.149	China Education and...	University	
59.62.158.199	CHINANET,Jiujiang,Ji...	Hosting	222.193.26.149	China Education and...	University	
123.55.21.213	CHINANET,Luanchua...	Home Broadband	222.193.26.149	China Education and...	University	
112.111.142.21	China Unicom,Longy...	Unused	222.193.26.149	China Education and...	University	
222.90.89.87	CHINANET,Xi'an,Sha...	Hosting	222.193.26.149	China Education and...	University	
58.34.36.48	CHINANET,Minhang ...	Company	222.193.26.147	China Education and...	University	
111.174.174.52	CHINANET,Xiaogan,...	Hosting	222.193.26.149	China Education and...	University	
114.248.14.184	China Unicom,Xiche...	Home Broadband	222.193.26.149	China Education and...	University	
220.190.220.69	CHINANET,Wenzhou...	Unused	222.193.26.149	China Education and...	University	
65.94.85.220	Bell DSL Internet Qu...		222.193.26.149	China Education and...	University	
61.100.200.128	TBROAD abc,Seoul,S...		222.193.26.149	China Education and...	University	
112.118.245.226	PCCW Limited Hong		222.193.26.149	China Education and	University	

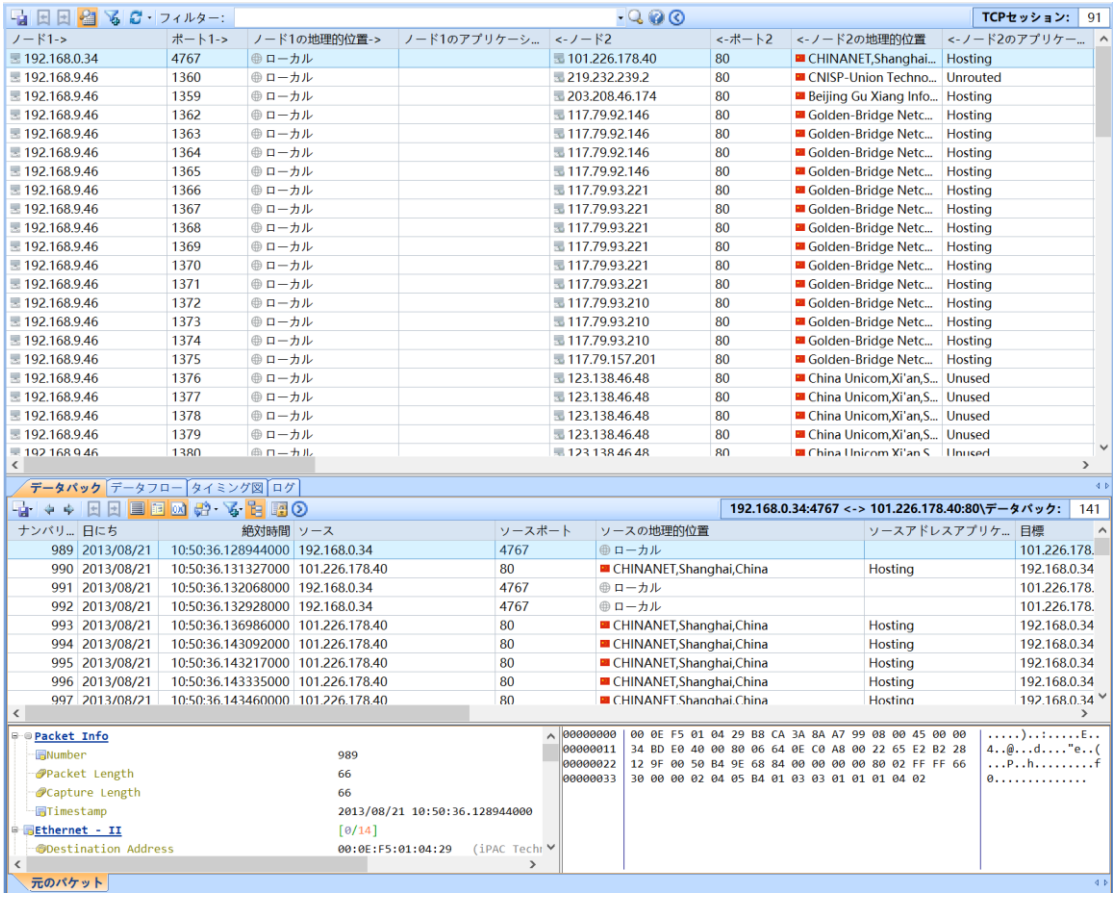
IP セッションビューツールバーの「詳細表示」ボタンをクリックして、分割サブウィンドウを表示または非表示にします。つまり、IP アドレスに関連付けられた TCP セッションと UDP セッションを表示して、データ関連付け分析を容易にすることができます。

9.9 TCP セッション

TCP 通信は、現在のイーサネットにおける主要な転送通信プロトコルの 1 つであり、科来ネットワーク分析システムはネットワークにおける TCP 通信状況を詳細に分析し、各セッションのソースアドレス、宛先アドレス、セッション持続時間、セッション総流量、送信流量、送信パケット、通信に使用される上位プロトコルなど 10 種類以上のセッションパラメータを深く分析することができる。また、再編成 TCP 通信におけるパケット乱数状況を自動的に分析し、乱数が発生したセッションを完全なデータストリームに再編成する。

TCP セッションには、パケット、データストリーム、タイミングチャートの 3 つの分割サブウィンドウビューが含まれており、ユーザーは各通信セッションのオリジナルパケット、完全なセッションデータストリーム、および通信中にグラフィカル化された SYN、ACK 状態、マイクロ秒レベルの時間パラメータを迅速に見ることができ、ユーザーの TCP 伝送性能のより良い分析を支援する。TCP セッションビューを下図に示す:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



TCP セッションの分析を通じて、現在のネットワークにおける TCP 接続の状況を特定することができます、例:

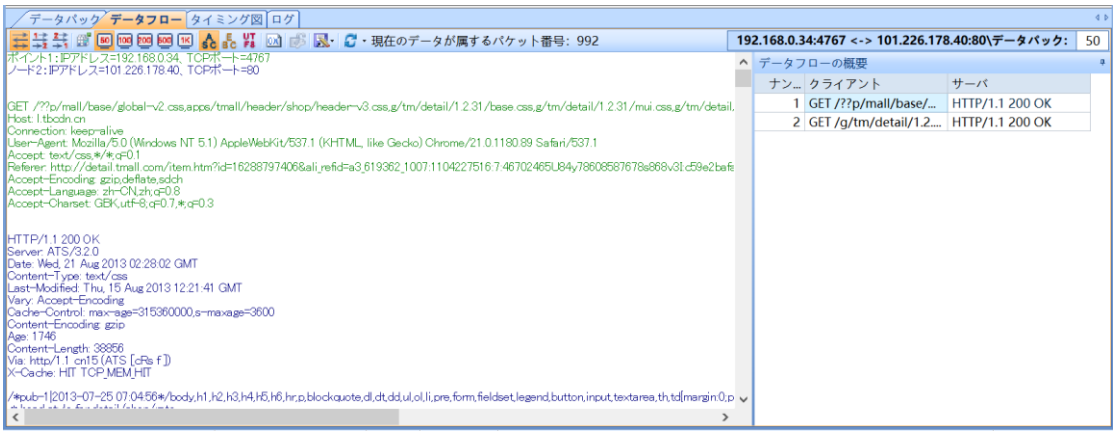
- 2 台のホスト間の通信内容を表示します。
- ネットワークに TCP ポートスキャン攻撃が存在するかどうか。
- ネットワークに TCP プロトコルに基づくサービスのアカウントユーザ名暗号解読攻撃が存在するかどうか。
- ネットワークにメールワームウイルス攻撃が存在するか。
- ネットワークに長時間接続され、トラフィックの少ない TCP 接続が存在するか（QQ/MSN などのプログラムが HTTP エージェントを使用するのはこの現象）。

TCP データストリーム再編成

TCP セッションビュー領域の下には、通信のパケットを表示するほか、TCP データストリーム再編成ビューもあり、ユーザーは現在選択されている接続の元の操作情報を簡単に理解でき、TCP 接続の元の情報を通じて、これらの TCP

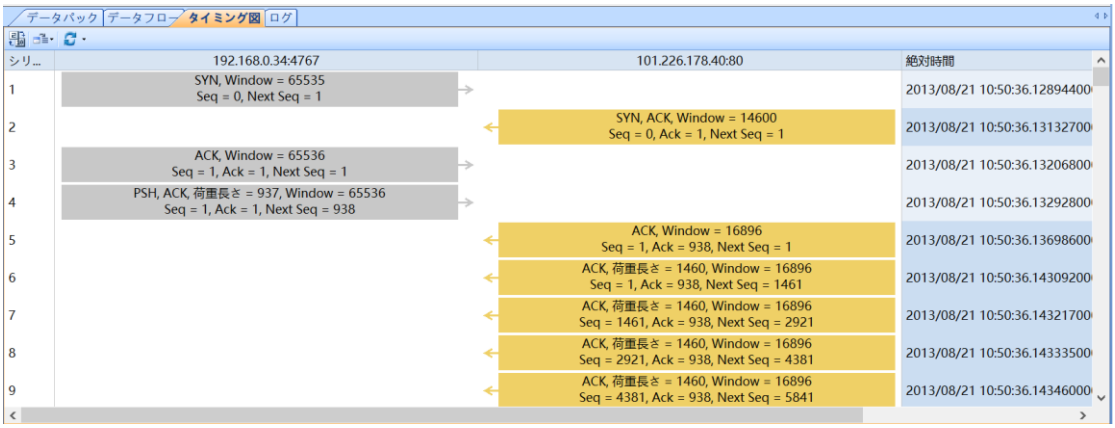
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

通信の内容、手順を特定し、この接続が正常であるかどうかを判断することができる。そのインタフェースを図に示します:



TCP セッションシーケンス図

TCP セッションシーケンス図では、通信双方の各種通信状態と応答時間をグラフィカルに表示し、ユーザーが TCP 通信内容を理解しやすくし、TCP 伝送性能の問題を直感的に発見するのを支援する。次の図に示します:

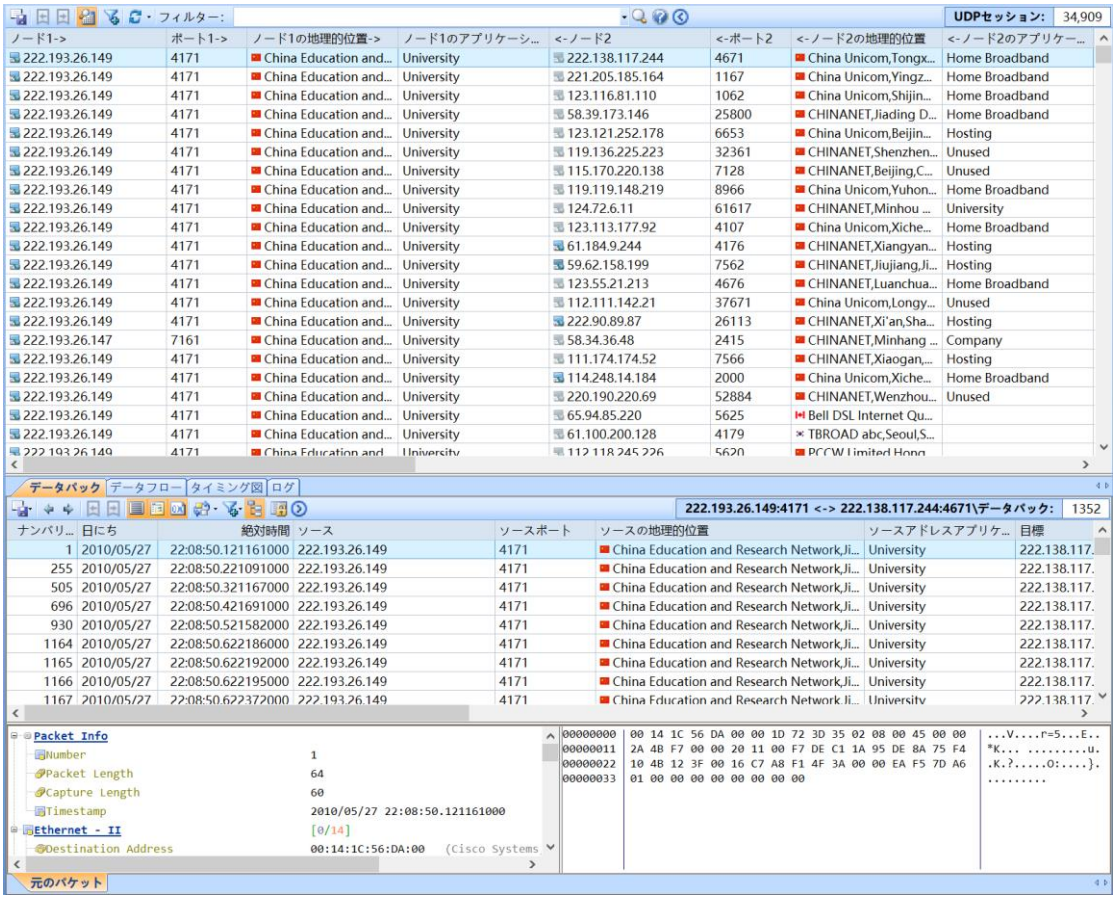


9.10 UDP セッション

UDP セッションビューには、ネットワーク内の UDP の通信セッション情報が詳細に表示されます。UDP セッションごとに、ソースアドレス、宛先アドレス、セッション総トラフィック、セッション送受信トラフィック、セッション送受信パケット、およびこれらのパケットのサイズなどの情報を詳細に統計します。そして、現在選択されている UDP セッションの元のパケット情報、

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

UDP データストリーム情報を下のサブウィンドウに表示します。これらの情報により、現在のネットワークにおける UDP 通信の状況を迅速に分析することができます。



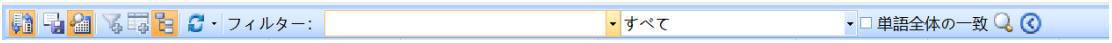
9.11 ドメイン名

ドメイン名ビューでは、ネットワーク内のドメイン名に対応する IP アドレスの通信情報を詳細に解析して表示します。ドメイン名ごとの IP アドレスに対して、その IP セッション数、TCP セッション数、UDP セッション数、パケット、送受信されたパケット及びこれらのパケットのサイズなどの多種の統計パラメータを統計することができる。そして、現在選択されているドメイン名に関連する IP セッション、TCP セッション、UDP セッションを下のサブウィン

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ドウに表示します。これらのセッション情報により、現在のネットワークにおけるドメイン名セッションの状況をすばやく知ることができます。

ドメイン名の表示ツールバーは次の図のとおりです:

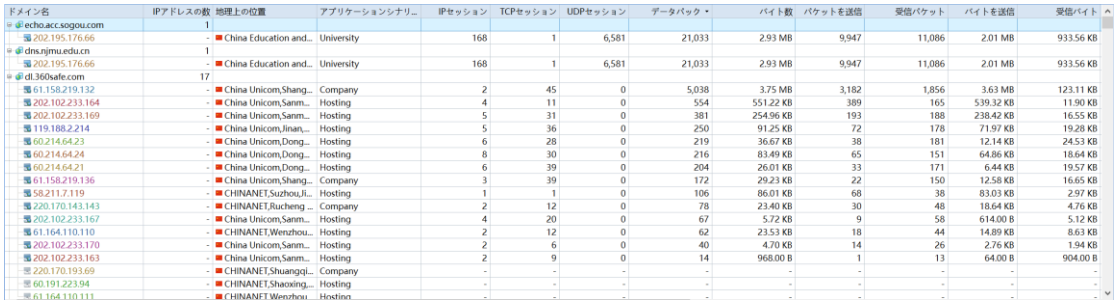


ドメイン名ビューのツールバーの左から右の機能を次の表に示します:

機能ネーム	詳しい説明
エクスポート	エクスポートリスト表示領域のすべてのデータをローカルディスクに csv 形式で保存することで、履歴としての表示と保存が容易になります。
詳細表示	IP/TCP/UDP 会话分隔子视图显示，点击此按钮可显示/隐藏与域名关联的 IP/TCP/UDP 会话分隔子视图。
フィルタに追加	特定の IP アドレスを選択してフィルタに追加し、新しいフィルタを生成します。
ネーム表に追加	特定の IP アドレスを選択してネーム表に追加し、ネーム表に新しいレコードを生成して保存します。
すべて展開	ドメイン名ビュー内のすべてのノードを展開/縮小します。
リフレッシュ	ビューリフレッシュ間隔を設定します。
フィルタリング	条件入力をフィルタし、任意の条件を入力してデータをすばやく検索できます。
全部	このドロップダウンメニューで特定のパラメータを指定すると、データの検索が高速になり、検索効率が向上します。
全文字マッチング	全文字マッチングとは、検索条件に完全に一致する単語に遭遇した場合にのみ検索結果として表示され、検索結果をより正確にすることができます。システムのデフォルトでは、全文字マッチングは有効になっていません。

ドメイン名の統計ビューを次の図に示します:

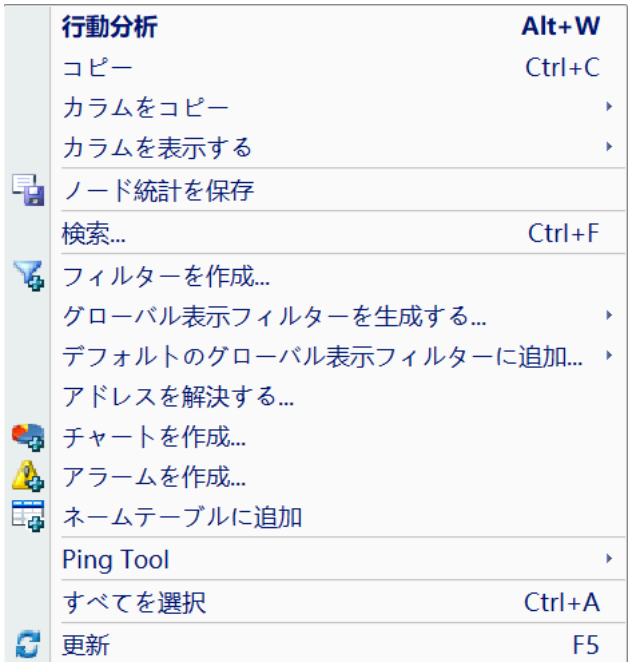
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



ドメイン名	IPアドレスの数	地理上の位置	アプリケーションシナリ...	IPセッション	TCPセッション	UDPセッション	データパック	バイト数	パケットを送信	受信パケット	バイトを送信	受信バイト
echo.acc.sogou.com	1											
202.195.176.66	-	China Education and...	University	168	1	6,581	21,033	2.93 MB	9,947	11,086	2.01 MB	933.56 KB
dns.njmu.edu.cn	1											
202.195.176.66	-	China Education and...	University	168	1	6,581	21,033	2.93 MB	9,947	11,086	2.01 MB	933.56 KB
dl.360safe.com	17											
61.158.219.132	-	China Unicom,Shang...	Company	2	45	0	5,038	3.75 MB	3,182	1,856	3.63 MB	123.11 KB
202.102.233.164	-	China Unicom,Sanm...	Hosting	4	11	0	554	551.22 KB	389	165	539.32 KB	11.90 KB
202.102.233.169	-	China Unicom,Sanm...	Hosting	5	31	0	381	254.96 KB	193	188	238.42 KB	16.55 KB
119.188.2.214	-	China Unicom,Jinan,...	Hosting	5	36	0	250	91.25 KB	72	178	71.97 KB	19.28 KB
60.214.64.23	-	China Unicom,Dong...	Hosting	6	28	0	219	36.67 KB	38	181	12.14 KB	24.53 KB
60.214.64.24	-	China Unicom,Dong...	Hosting	8	30	0	216	83.49 KB	65	151	64.86 KB	18.64 KB
60.214.64.21	-	China Unicom,Dong...	Hosting	6	39	0	204	26.01 KB	33	171	6.44 KB	19.57 KB
61.158.219.136	-	China Unicom,Shang...	Company	3	39	0	172	29.23 KB	22	150	12.58 KB	16.65 KB
58.211.7.119	-	CHINANET,Suzhou,Ji...	Hosting	1	1	0	106	86.01 KB	68	38	83.03 KB	2.97 KB
220.170.143.143	-	CHINANET,Rucheng ...	Company	2	12	0	78	23.40 KB	30	48	18.64 KB	4.76 KB
202.102.233.167	-	China Unicom,Sanm...	Hosting	4	20	0	67	5.72 KB	9	58	614.00 B	5.12 KB
61.164.110.110	-	CHINANET,Wenzhou...	Hosting	2	12	0	62	23.53 KB	18	44	14.89 KB	8.63 KB
202.102.233.170	-	China Unicom,Sanm...	Hosting	2	6	0	40	4.70 KB	14	26	2.76 KB	1.94 KB
202.102.233.163	-	China Unicom,Sanm...	Hosting	2	9	0	14	968.00 B	1	13	64.00 B	904.00 B
220.170.193.69	-	CHINANET,Shuangqi...	Company	-	-	-	-	-	-	-	-	-
60.191.223.94	-	CHINANET,Shaoxing,...	Hosting	-	-	-	-	-	-	-	-	-
61.164.110.111	-	CHINANET,Wenzhou...	Hosting	-	-	-	-	-	-	-	-	-

ドメイン名ビューはネットワークにおけるドメイン名対応 IP アドレスの通信状況を詳細に統計し、ビューのサブウィンドウには、現在選択されているドメイン名対応 IP セッション、TCP セッションなどの情報が関連して表示され、これらの情報を通じて、現在のネットワークにおけるドメイン名の通信状況を特定することができる

ドメイン名の統計は、次の図に示すように右クリックメニュー機能をサポートしています:



具体的な機能は次の表のとおりです:

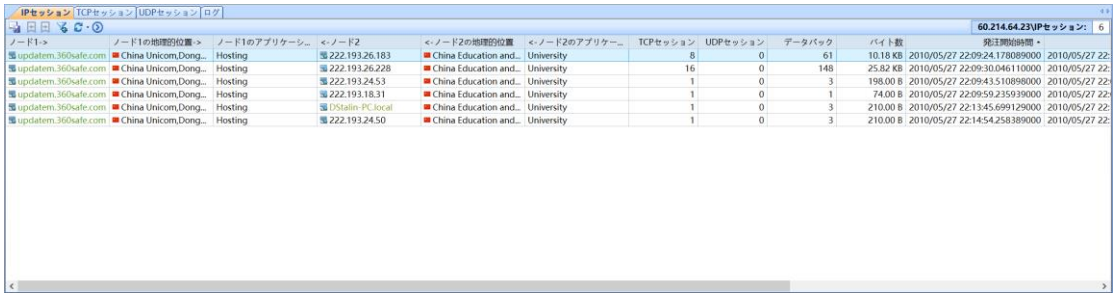
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

機能ネーム	詳しい説明
新しいウィンドウにパケットを表示	物理アドレス間で通信する元のパケットを新しいウィンドウで開きます。
コピー	選択したセッションのリストから情報をコピーします。
列のコピー	ノード 1、ノード 2、パケット数などのフィールドをコピーする場合に選択します。
カスタム列	ノードの関連情報を表示するには、希望するフィールドを追加します（秒当たりのパケット数、秒当たりのバイト数など）。
ノード統計の保存	ツールバーのエクスポート機能と同様に、ノードリスト表示領域のすべてのデータをテキスト形式（*txt）でローカルディスクに保存し、履歴としての表示と保存を容易にします。
検索	検索するセッションを入力します。ファジィルックアップとルックアップ統計をサポートします。
解析フィルタの生成	特定の IP アドレスを選択して分析フィルタに追加し、新しい分析フィルタを生成します。
グローバル表示フィルタの生成	特定の IP アドレスを選択してグローバル表示フィルタに追加し、新しいグローバル表示フィルタを生成します。
アドレス解析	IP アドレスのホスト名を解析し、ホスト名を解析することで、IP ホストをすばやく識別することができます。
名前テーブルに追加	特定のノードを選択するか、名前テーブルに追加して、名前テーブルに新しいレコードを生成して保存します。
すべて選択	セッション統計リストのすべてのセッションを選択します。
リフレッシュ	セッション統計リストをすぐに更新します。

ドメイン名ビューツールバーの「詳細表示」ボタンをクリックして、セパレータサブウィンドウを表示または非表示にします。すなわち、次の図に示すよう

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

に、ドメイン名に関連付けられた IP セッション、TCP セッション、UDP セッションを表示して、データ関連付け分析を容易にすることができます:



9.12 サービス

サービスビューでは、IP アドレス、ポート、地理的位置、パケット、バイト数、ロードなどのさまざまなパラメータに基づいて各サービスの通信状況を統計的に分析し、各サービスの通信状態を詳細に知ることができます。

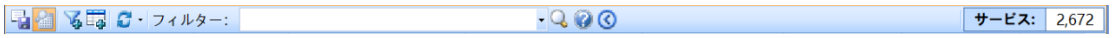
概要

サービスの概要統計ビュー統計はサービスの総数とポート総数を示し、またグラフで内外ネットアクセス TOP 10 サービス、累計通信量最大 TOP 10 サービス、累計サービス最長時 TOP 10 サービス、セッション数 TOP 10 サービスを示し、下図のように:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ツールバー

アプリビューツールバーを次の図に示します:



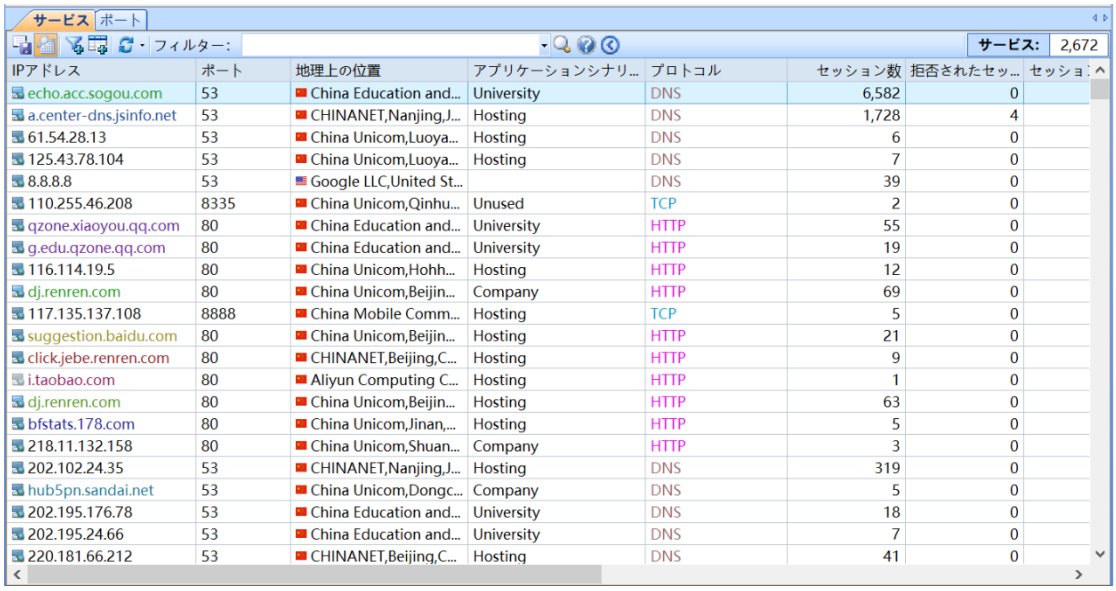
ツールバーの左から右への機能を次の表に示します:

機能ネーム	詳しい説明
エクスポート	セッションリスト表示領域のすべてのデータをエクスポートし、ローカルディスクに csv 形式で保存することで、履歴としての表示と保存が容易になります。
フィルタに追加	特定のノードを選択してフィルタに追加し、新しいフィルタを生成します。
ネーム表に追加	特定のノードを選択してネーム表に追加し、ネーム表に新しいレコードを生成して保存します。
リフレッシュ	ビューリフレッシュ間隔を設定します。
フィルタリング	条件入力をフィルタし、任意の条件を入力してデータをすばやく検索できます。
すべて	このドロップダウンメニューで特定のパラメータを指定すると、データの検索が高速になり、検索効率が向上します。
全文字マッチング	全文字マッチングとは、検索条件に完全に一致する単語に遭遇した場合にのみ検索結果として表示され、検索結果をより正確にすることができます。システムのデフォルトでは、全文字マッチングは有効になっていません。

サービス統計リスト

サービス統計リストの表示は次の図の通りです:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



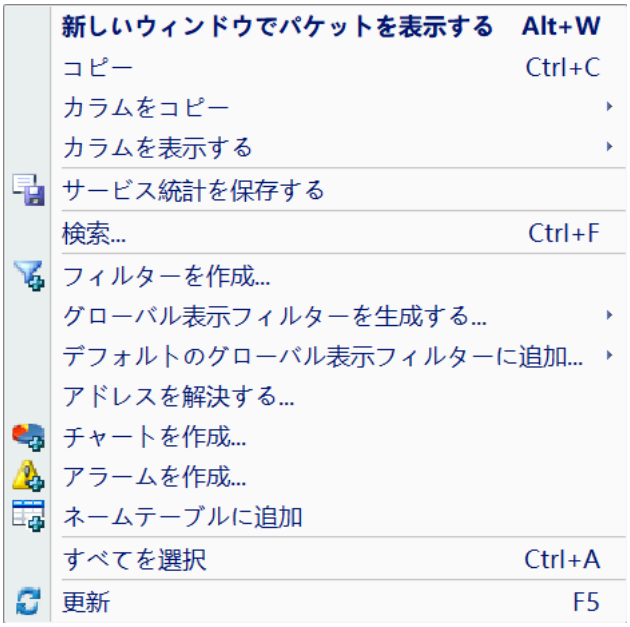
IPアドレス	ポート	地理上の位置	アプリケーションシナリ...	プロトコル	セッション数	拒否されたセッ...	セッショ
echo.acc.sogou.com	53	China Education and...	University	DNS	6,582	0	
a.center-dns.jsinfo.net	53	CHINANET,Nanjing,J...	Hosting	DNS	1,728	4	
61.54.28.13	53	China Unicom,Luoya...	Hosting	DNS	6	0	
125.43.78.104	53	China Unicom,Luoya...	Hosting	DNS	7	0	
8.8.8.8	53	Google LLC,United St...		DNS	39	0	
110.255.46.208	8335	China Unicom,Qinhu...	Unused	TCP	2	0	
qzone.xiaoyou.qq.com	80	China Education and...	University	HTTP	55	0	
g.edu.qzone.qq.com	80	China Education and...	University	HTTP	19	0	
116.114.19.5	80	China Unicom,Hohh...	Hosting	HTTP	12	0	
dj.renren.com	80	China Unicom,Beijin...	Company	HTTP	69	0	
117.135.137.108	8888	China Mobile Comm...	Hosting	TCP	5	0	
suggestion.baidu.com	80	China Unicom,Beijin...	Hosting	HTTP	21	0	
click.jebe.renren.com	80	CHINANET,Beijing,C...	Hosting	HTTP	9	0	
i.taobao.com	80	Aliyun Computing C...	Hosting	HTTP	1	0	
dj.renren.com	80	China Unicom,Beijin...	Hosting	HTTP	63	0	
bfstats.178.com	80	China Unicom,Jinan,...	Hosting	HTTP	5	0	
218.11.132.158	80	China Unicom,Shuan...	Company	HTTP	3	0	
202.102.24.35	53	CHINANET,Nanjing,J...	Hosting	DNS	319	0	
hub5pn.sandai.net	53	China Unicom,Dongc...	Company	DNS	5	0	
202.195.176.78	53	China Education and...	University	DNS	18	0	
202.195.24.66	53	China Education and...	University	DNS	7	0	
220.181.66.212	53	CHINANET,Beijing,C...	Hosting	DNS	41	0	

サービスビューでは、各サービスの通信状況と対応するポートの通信状況を詳細に統計しています。

Tips

フィールド列を選択して右クリックするか、右クリックメニューのカスタム列を直接クリックして、 詳細については、「リセット」を選択するとデフォルト設定に戻ります。

サービス統計は、次の図に示すように右クリックメニュー機能をサポートします:



具体的な機能は次の表の通りです:

機能ネーム	詳しい説明

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

動作分析	新しいウィンドウに対応する IP のネットワーク動作、TCP セッション、ログ、およびパケットを表示する。
コピー	選択したセッションのリストから情報をコピーします。
列のコピー	ノード 1、ノード 2、パケット数などのフィールドをコピーする場合に選択します。
カスタム列	ノードの関連情報を表示するには、希望するフィールドを追加します（秒当たりのパケット数、秒当たりのバイト数など）。
サービス統計の保存	ツールバーのエクスポート機能と同様に、セッション統計リスト表示領域のすべてのデータを CSV 形式でローカルディスクに保存し、履歴として表示して保存するのに便利です。
検索	検索するセッションを入力します。ファジィルックアップとルックアップ統計をサポートします。
解析フィルタの生成	特定のノードを選択して分析フィルタに追加し、新しいフィルタを生成します。
グローバル表示フィルタの生成	特定のノードを選択してグローバル表示フィルタに追加し、新しいフィルタを生成します。
アドレス解析	選択したセッションをプロアクティブに解析し、ノードの IP アドレスを取得することで、この IP ノードがネットワーク内のどのホストであるかを正確に判断します。
脅威情報の表示	特定のノードを選択し、ノード IP またはドメイン名に従って詳細な脅威情報を表示します。
グラフの作成	特定のノードまたはネットワークセグメントを選択してグラフビューに追加し、新しいグラフを生成して解析を表示します。
アラートの生成	特定のノードまたはネットワークセグメントを選択してアラートビューに追加し、ネットワーク内の新しい問題をタイムリーに検出するための新しいアラートを生成します。
ネーム表に追加	特定のノードを選択してネーム表に追加し、ネーム表に新しいレコードを生成して保存します。
ノードブラウザにナビゲート	クリックすると、アプリケーションノードブラウザで現在のアプリケーションが自動的に選択されます。

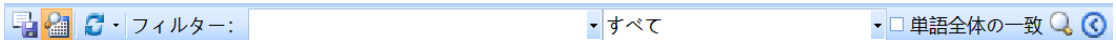
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

すべて選択	統計リストのすべてのアプリを選択します。
リフレッシュ	セッション統計リストを更新します。

9.13 アプリケーション

アプリビューは流量、パケット数、送信流量、受信流量、送信パケット数、受信パケット数などの多種のパラメータに基づいてネットワーク中の各アプリの通信状況を統計し、分析し、ネットワーク中のアプリの通信状態を詳しく知ることができる。

アプリビューツールバーを次の図に示します:



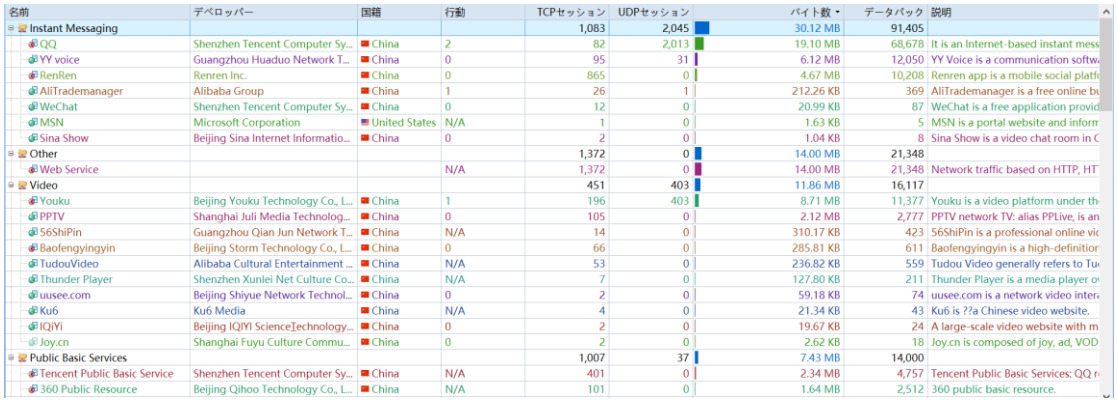
ツールバーの左から右への機能を次の表に示します:

機能ネーム	詳しい説明
エクスポート	セッションリスト表示領域のすべてのデータをエクスポートし、ローカルディスクに csv 形式で保存することで、履歴としての表示と保存が容易になります。
詳細表示	アプリケーション関連のプロトコル、TCP、UDP ウィンドウを非表示または表示にします。
ノードブラウザにナビゲート	クリックすると、アプリケーションノードブラウザで現在のアプリケーションが自動的に選択されます。
リフレッシュ	ビューリフレッシュ間隔を設定します。
フィルタリング	条件入力をフィルタし、任意の条件を入力してデータをすばやく検索できます。
すべて	このドロップダウンメニューで特定のパラメータを指定すると、データの検索が高速になり、検索効率が向上します。
全文字マッチング	全文字マッチングとは、検索条件に完全に一致する単語に遭遇した場合にのみ検索結果として表示され、検索結果をより正確にすることができます。システムのデフォルトでは、全文字マッチングは有効になっていません。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

アプリ統計リスト

アプリ統計リストビューを次の図に示します:



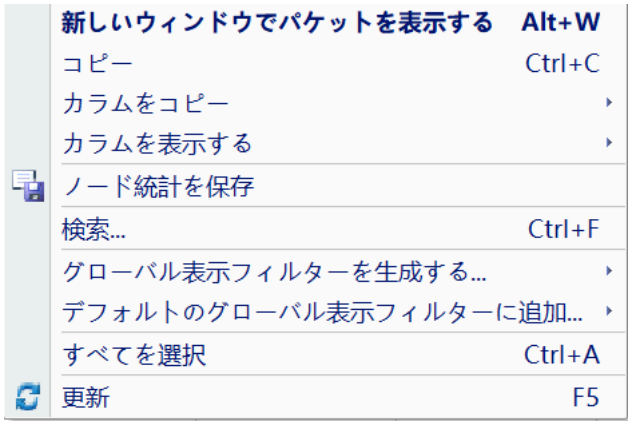
名前	デベロッパー	国籍	行動	TCPセッション	UDPセッション	バイト数	データパック	説明
Instant Messaging				1,083	2,045	30.12 MB	91,405	
QQ	Shenzhen Tencent Computer Sy...	China	2	82	2,013	19.10 MB	68,678	It is an Internet-based instant mess
YY voice	Guangzhou Huaduo Network T...	China	0	95	31	6.12 MB	12,050	YY Voice is a communication softw
RenRen	Renren Inc.	China	0	865	0	4.67 MB	10,208	Renren app is a mobile social platf
AliTrademanager	Alibaba Group	China	1	26	1	212.26 KB	369	AliTrademanager is a free online bu
WeChat	Shenzhen Tencent Computer Sy...	China	0	12	0	20.99 KB	87	WeChat is a free application provid
MSN	Microsoft Corporation	United States	N/A	1	0	1.63 KB	5	MSN is a portal website and inform
Sina Show	Beijing Sina Internet Informatio...	China	0	2	0	1.04 KB	8	Sina Show is a video chat room in C
Other				1,372	0	14.00 MB	21,348	
Web Service			N/A	1,372	0	14.00 MB	21,348	Network traffic based on HTTP, HT
Video				451	403	11.86 MB	16,117	
Youku	Beijing Youku Technology Co., L...	China	1	196	403	8.71 MB	11,377	Youku is a video platform under th
PPTV	Shanghai Juli Media Technolog...	China	0	105	0	2.12 MB	2,777	PPTV network TV: alias PPLive, is an
56ShiPin	Guangzhou Qian Jun Network T...	China	N/A	14	0	310.17 KB	423	56ShiPin is a professional online vic
Baofengyingyin	Beijing Storm Technology Co., L...	China	0	66	0	285.81 KB	611	Baofengyingyin is a high-definition
TudouVideo	Alibaba Cultural Entertainment ...	China	N/A	53	0	236.82 KB	559	Tudou Video generally refers to Tu
Thunder Player	Shenzhen Xunlei Net Culture Co...	China	N/A	7	0	127.80 KB	211	Thunder Player is a media player o
uusee.com	Beijing Shiyue Network Technol...	China	0	2	0	59.18 KB	74	uusee.com is a network video inter
Ku6	Ku6 Media	China	N/A	4	0	21.34 KB	43	Ku6 is ??a Chinese video website.
IQiYi	Beijing IQIYI Science&Technology...	China	0	2	0	19.67 KB	24	A large-scale video website with m
Joy.cn	Shanghai Fuyu Culture Commu...	China	0	2	0	2.62 KB	18	Joy.cn is composed of joy, ad, VOD
Public Basic Services				1,007	37	7.43 MB	14,000	
Tencent Public Basic Service	Shenzhen Tencent Computer Sy...	China	N/A	401	0	2.34 MB	4,757	Tencent Public Basic Services: QQ r
360 Public Resource	Beijing Qihoo Technology Co., L...	China	N/A	101	0	1.64 MB	2,512	360 public basic resource.

アプリビューはネットワーク内のさまざまなアプリケーションの通信状況を詳細に統計し、ビューのサブウィンドウには、現在選択されているアプリケーションで使用されているプロトコルと、TCP、UDP セッション情報が含まれていることが関連付けられて表示されます。

Tips

フィールド列を選択して右クリックするか、右クリックメニューのカスタム列を直接クリックして、表示したいフィールド情報をさらに選択し、リセットを選択するとデフォルト設定に戻ります。

アプリケーション統計は、次の図に示すように右クリックメニュー機能をサポートします:



具体的な機能は次の表の通りです:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

機能ネーム	詳しい説明
新しいウィンドウにパケットを表示	物理アドレス間で通信する元のパケットを新しいウィンドウで開きます。
コピー	選択したセッションのリストから情報をコピーします。
列のコピー	ノード 1、ノード 2、パケット数などのフィールドをコピーする場合に選択します。
カスタム列	ノードの関連情報を表示するには、希望するフィールドを追加します（秒当たりのパケット数、秒当たりのバイト数など）。
ノード統計の保存	ツールバーのエクスポート機能と同様に、セッション統計リストの表示領域のすべてのデータは、履歴として表示および保存するのに便利なテキスト形式（*txt）でローカルディスクに保存されます。
検索	検索するセッションを入力します。ファジィルックアップとルックアップ統計をサポートします。
ノードブラウザにナビゲート	クリックすると、アプリケーションノードブラウザで現在のアプリケーションが自動的に選択されます。
すべて選択	統計リストのすべてのアプリを選択します。
リフレッシュ	セッション統計リストを更新します。

サブビュー表示領域

サブビュー表示領域インタフェースは、次の図のようになります:

ツールバーで「詳細表示」ボタンをクリックすると、選択したアプリケーションのプロトコル、物理セッション、IP セッション、TCP セッション、UDP セ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

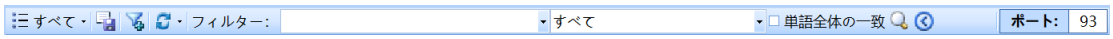
ッション、動作を詳細に統計したアプリケーション関連のサブビューを表示ま

たは非表示にできます。

9.14 ポート

ポートビューでは、ネットワーク内のポート情報を詳細に解析して表示します。各ポートについて、ポート番号、ポートタイプ、プロトコルタイプ、パケット数、バイト数、一般的なサービスなど、さまざまなパラメータを統計できます。そして、現在選択されているポートに関連付けられている TCP セッションまたは UDP セッションを下のサブウィンドウに表示します。これらのセッション情報により、現在のネットワークにおけるポートの使用状況をすばやく知ることができます。

ポートビューツールバーは次の図の通りです:



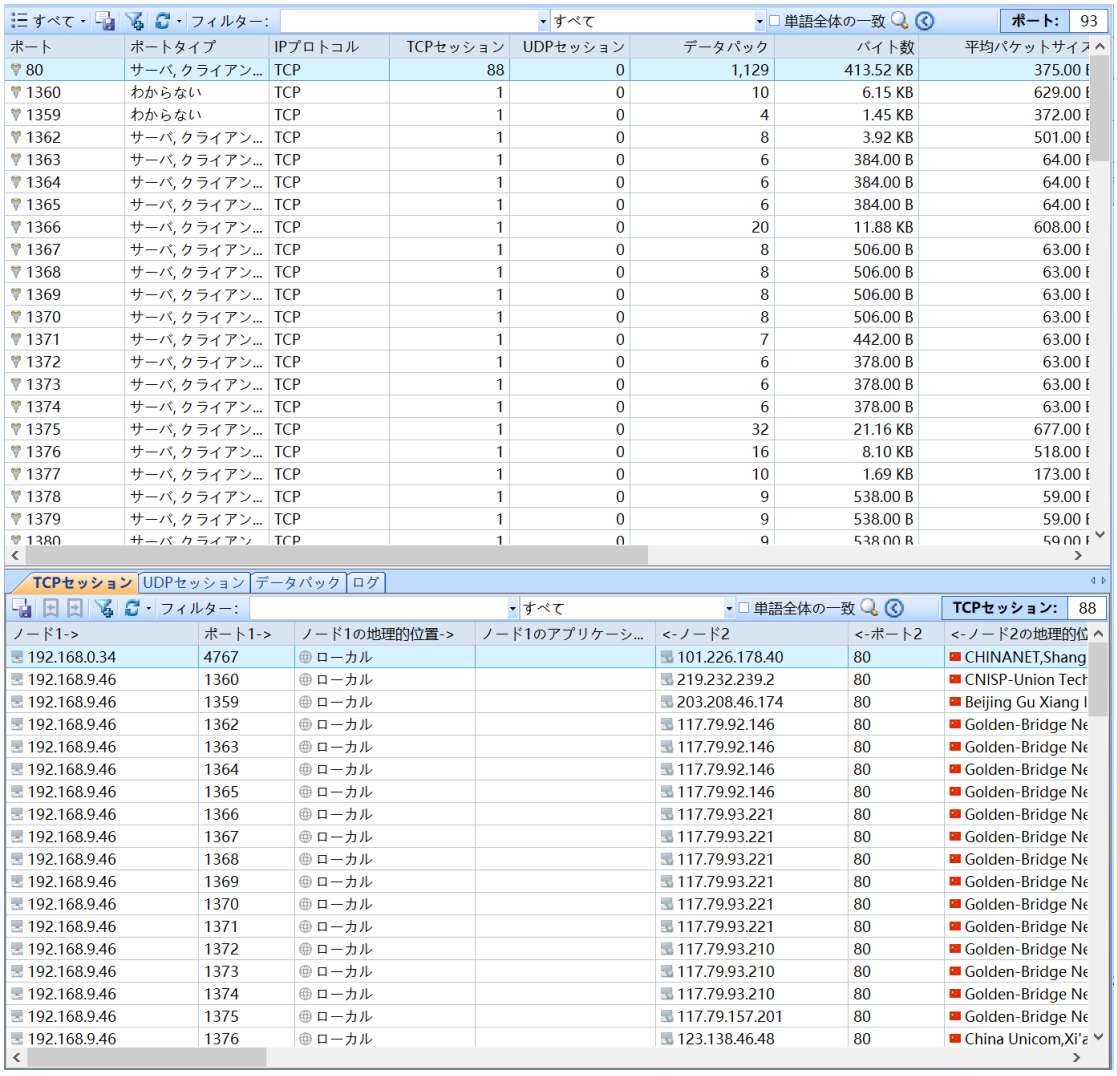
ポートビューのツールバーの左から右の機能を次の表に示します:

機能ネーム	詳しい説明
エクスポート	セッションリスト表示領域のすべてのデータをエクスポートし、ローカルディスクに csv 形式で保存することで、履歴としての表示と保存が容易になります。
フィルタに追加	特定のセッションを選択してフィルタに追加し、新しいフィルタを生成します。
リフレッシュ	ビューリフレッシュ間隔を設定します。
フィルタリング	条件入力をフィルタし、任意の条件を入力してデータをすばやく検索できます。
すべて	このドロップダウンメニューで特定のパラメータを指定すると、データの検索が高速になり、検索効率が向上します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

全文字マッチング	全文字マッチングとは、検索条件に完全に一致する単語に遭遇した場合にのみ検索結果として表示され、検索結果をより正確にすることができます。システムのデフォルトでは、全文字マッチングは有効になっていません。

ポートビューは次の図のようになります:



- ポートタイプにはクライアント、サーバ、不明が含まれ、ポートがクライアントまたはサーバタイプに属しているかどうかを判断できない場合は不明と定義されます。1 つのポートが複数のセッションに存在する可能性があるため、複数のタイプに属する可能性があります。
- 共通サービス列に表示されるサービス名は、ポート番号と IP プロトコル・タイプに基づいて識別され、識別できない場合は NULL として表示されます。

ポートビューはネットワーク内のポートの使用状況を詳細に統計し、ビューの

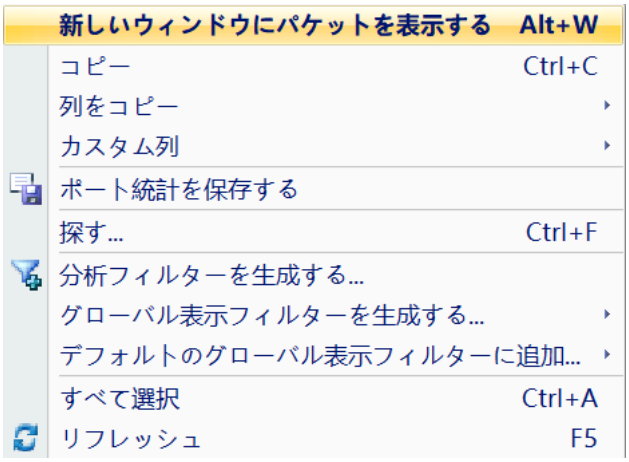
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

サブウィンドウには、現在選択されているポートに対応する TCP セッションまたは UDP セッション情報が関連付けて表示されます。

Tips

フィールド列を選択して右クリックするか、右クリックメニューのカスタム列を直接クリックして、表示したいフィールド情報をさらに選択し、リセットを選択するとデフォルト設定に戻ります。

ポートビューは、次の図に示すように右クリックメニュー機能をサポートしています:



具体的な機能は次の表のとおりです:

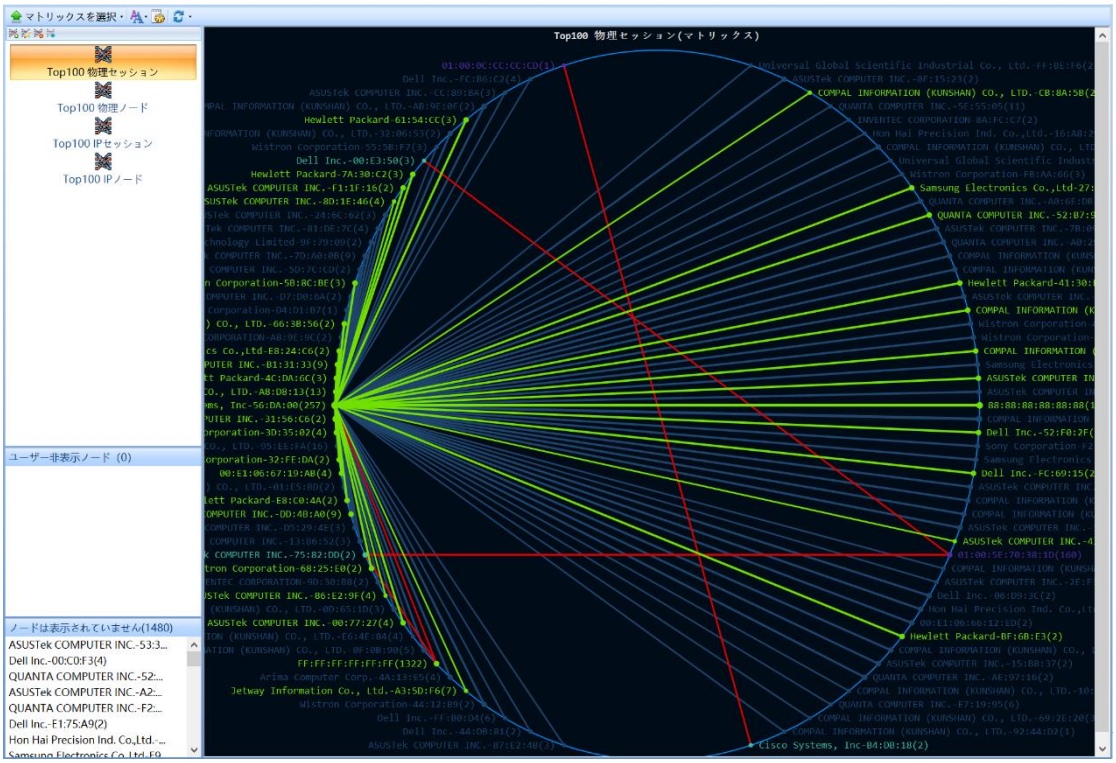
機能ネーム	詳しい説明
コピー	選択したセッションのリストから情報をコピーします。
列のコピー	ノード 1、ノード 2、パケット数などのフィールドをコピーする場合に選択します。
カスタム列	ノードの関連情報を表示するには、希望するフィールドを追加します（秒当たりのパケット数、秒当たりのバイト数など）。
ポート統計の保存	ツールバーのエクスポート機能と同様に、ポート統計リスト表示領域のすべてのデータは、履歴として表示および保存するのに便利なテキスト形式（*txt）でローカルディスクに保存されます。
検索	検索するセッションを入力します。ファジィルックアップとルックアップ統計をサポートします。
生成フィルタ	特定のセッションを選択してフィルタに追加し、新しいフィルタを

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

	生成します。
すべて選択	セッション統計リストのすべてのセッションを選択します。
リフレッシュ	セッション統計リストをすぐに更新します。

9.15 マトリックス

Capsa システムのマトリックスビューは、ネットワークにおける通信のノードとセッションを詳細に統計することができ、そのインタフェースは下図のようになる。



マトリックスビューを使用して、次の情報を知ることができます:

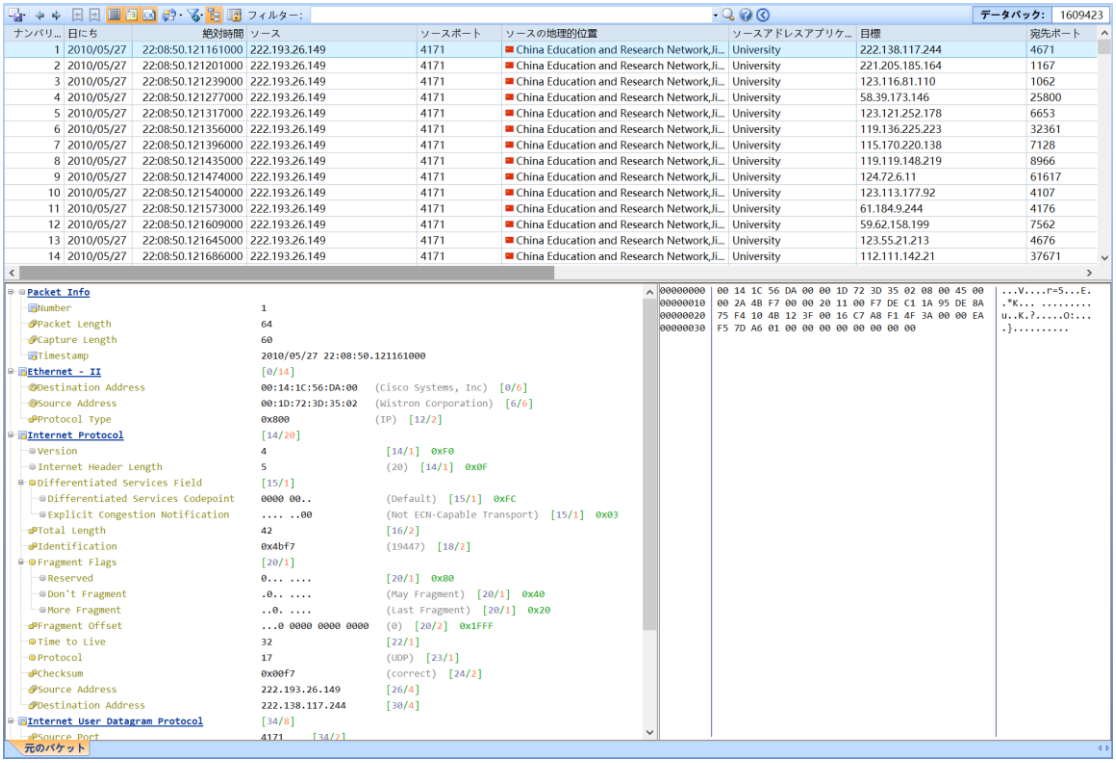
- ネットワーク通信全体のノード情報。
- ネットワーク通信全体のセッション情報。
- ある物理ホストの通信ノード情報。
- ある IP ホストの通信セッション情報。
- ある物理ホストの通信ノード情報。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- ある IP ホストの通信セッション情報。
- あるセッションのホスト情報。

9.16 パケット

パケット復号は概要復号、フィールド復号、16 進復号から構成され、概要復号は自動的に行われ、ユーザーも概要復号のプロトコル層を選択することができ、ユーザーが不審なネットワークパケットを迅速に特定するのを助けることができ、ユーザーはまた単一のパケットを選択して詳細な復号を行うことができ、詳細復号フィールドはパケットのオリジナルデータと相互作用することができ、たとえ入念に偽造されたサイバー攻撃であっても、詐欺パケットはこのモードでも逃げ場がない。



説明：パケットビューツールバーで、「エクスポート」ボタンをクリックして、現在キャッシュされているパケットをさまざまな形式のパケットファイルエクスポートでローカルディスクに保存します。

パケット復号により、次の情報を知ることができます：

- パケットの概要情報と詳細な復号。
- パケットがスライスされているかどうか。

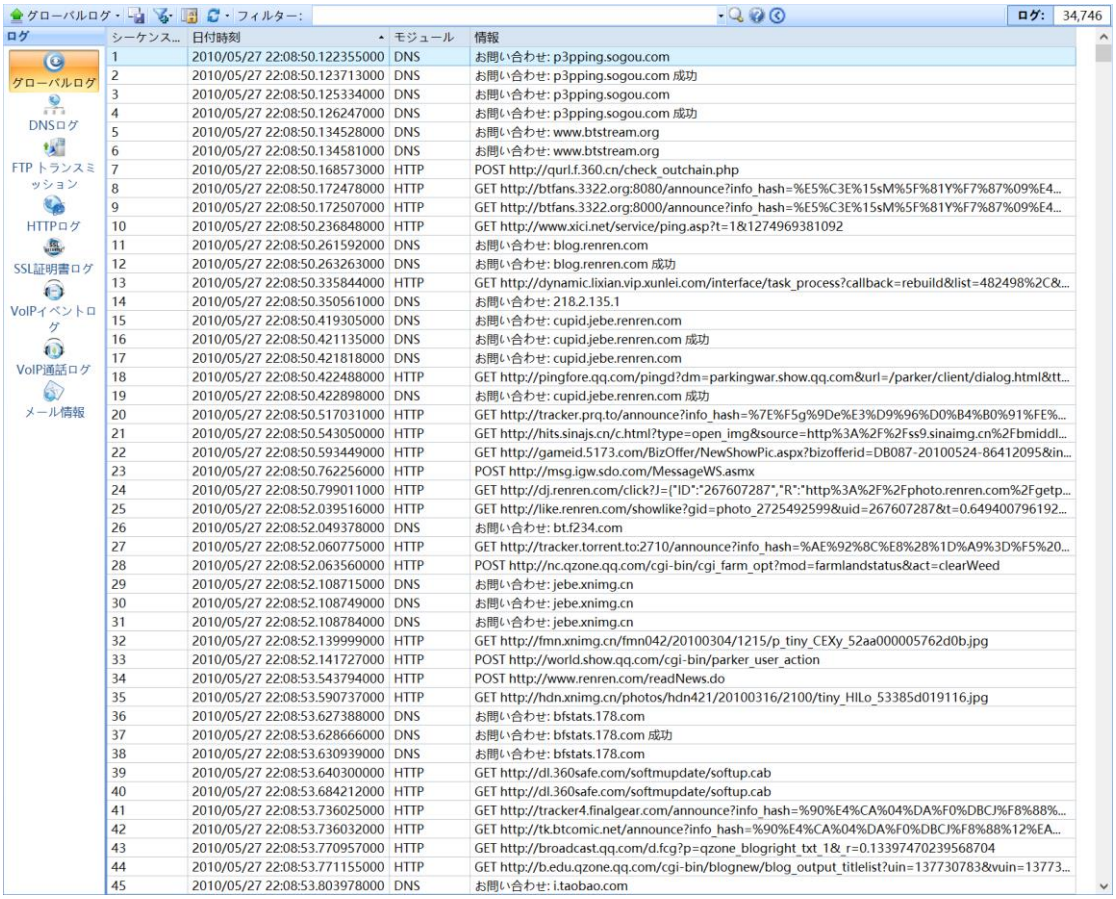
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- ネットワーク内のパケットのタイプ。
- ネットワークで転送されたパケットが正しいかどうか。
- ネットワーク内の IP パケットのバージョン。
- ターゲットホストがクライアントホストから要求されたサービスを実行しているかどうか。
- ソースホストからターゲットホストへのルーティング時間（つまりリンク長）。
- クライアントホストから要求されたサービスに対するターゲットホストの応答時間。
- ネットワークで転送されたデータは緊急データであるかどうか。
- ネットワーク上をパケットが通過するルーティングホップの数。
- ネットワークにループ現象が存在するかどうか。
- ユーザーがターゲットホストのサービスにアクセスするための元の手順。
- 攻撃や偽造パケットが存在するかどうか、すなわち正常ではないデータ通信。

9.17 ログ

ログビューは、HTTP 要求（Web ブラウズ）、メール情報（SMTP/POP 3 によるメール送受信）、DNS クエリ（ドメイン解析）、FTP 転送（FTP を用いた転送に関する情報）などのネットワークアプリケーションログを含む、ネットワーク内のアプリケーション層通信情報を記録する。システムはデフォルトですべてのタイプのログ解析モジュールを有効にし、ユーザーは解析設定のログ設定ダイアログボックスで実際の解析状況に応じて適切なモジュールをオンまたはオフにし、ログ情報をローカルディスクに保存することができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



ログビューでは、一般的なネットワークアプリケーションの通信状態をすばやく表示するために、任意の特定のタイプのログを表示することができます。

ヒント: ログ統計解析は解析設定のログ設定に依存します。ログ設定にログの種類がチェックされていない場合、ログは解析されず表示されません。

9.18 レポート

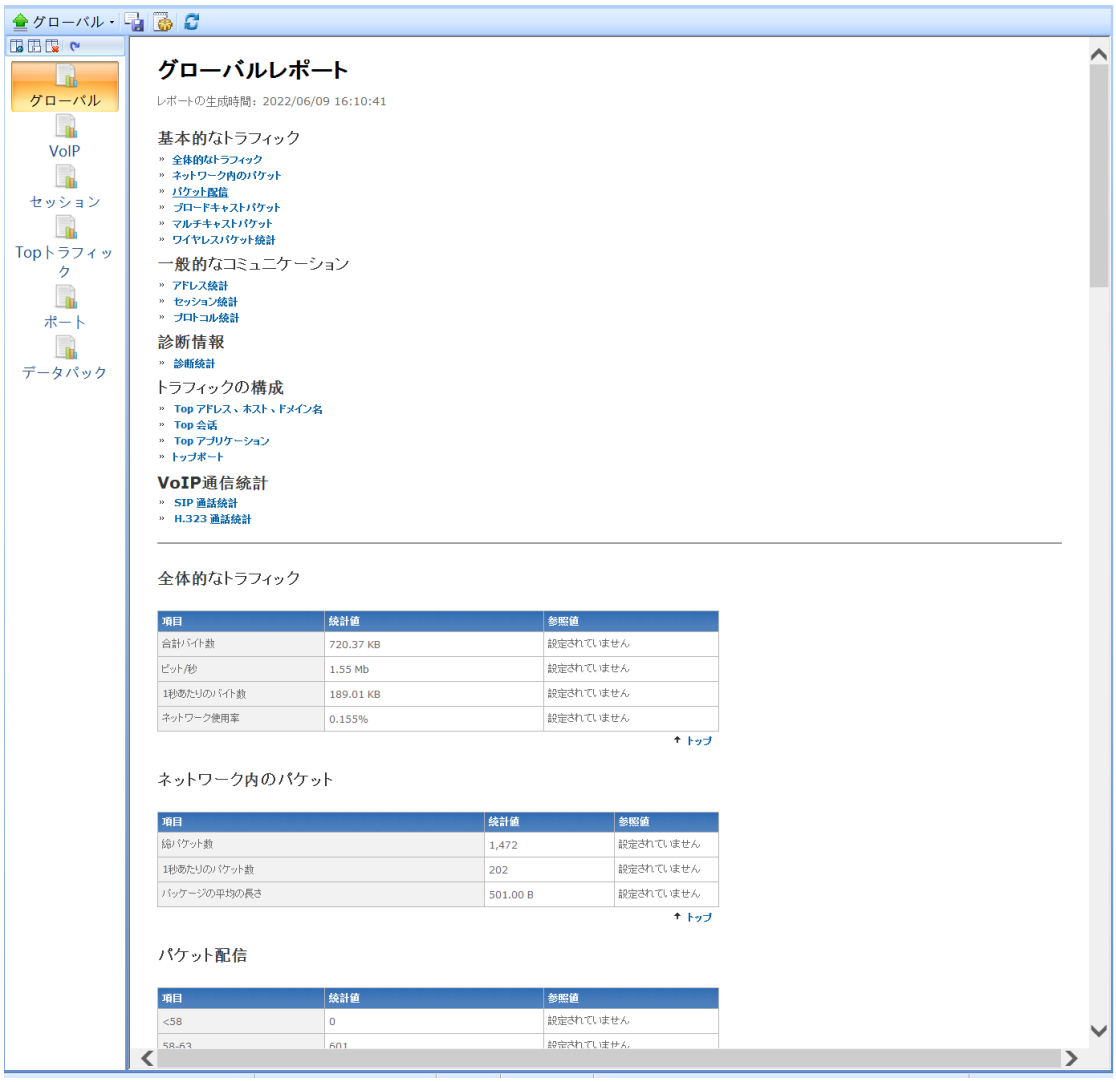
レポートでは、データ統計と分析結果を直感的に出力することができます。ユーザーは、次のレポート・タイプをすばやく表示できます:

- 概要統計レポート
- 診断統計レポート
- プロトコル統計レポート
- TOP N アプリケーション層プロトコルのレポート
- TOP N 物理アドレスレポート
- TOP N IP アドレスレポート
- TOP N ローカル IP アドレスレポート

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- TOP N リモート IP アドレスレポート

レポート機能により、統計的な分析結果をレポート形式でいつでも出力できます。ユーザーはレポートのデータに基づいて、現在のネットワーク状況を完全に把握することができます。



Capsa システムのレポート機能は以下のとおりである：

- レポートの内容のカスタマイズ
- レポートの一般設定
- レポートのエクスポート保存

カスタム・レポート・パネルでは、レポートの内容をカスタマイズし、レポートを*.htm/*.html 及び*.pdf 3 種類のフォーマットをエクスポートして保存し、「システム・オプション」のレポート・ダイアログ・ボックスでレポートの関

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

連情報を設定し、レポート内の会社 ID、名前、レポートの接頭辞、作成者、生成時間などのオプションを指定したり、レポート統計の TOP-N 表示を指定したりできます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

10 統計分析

統計分析はネットワークをリアルタイムに監視し、リアルタイムに分析し、統計結果を自動的に各ビューに表示し、ユーザーは統計分析結果をコピー、エクスポート、印刷、ログ生成、レポート生成などの操作を行うことができる。

Capsa システムは、統計分析が大幅に強化された。主な表現：ネットワークカウンタは数百種類に達し、ネットワークエラーのモニタリングを増加し、パケットサイズ分布の統計を増加し、利用率の分析を押し付け、プロトコルツリーの拡張分析を増加し、図形化統計を増加した。

統計分析には、サマリー統計、エンドポイント統計、プロトコル統計、セッション統計、マトリックス統計、グラフ統計、レポート統計が含まれます。

概要統計

概要統計によって提供される 100 近くの統計カウンタは、ユーザーに非常に詳細な統計情報を提供し、スナップショット機能は、ユーザーが特定の期間のデータ変化を比較できるようにします。概要統計はグローバルだけでなく、ネットワークプロトコルとネットワークエンドポイントごとに独自の概要統計があり、ユーザーは複数のウィンドウを開き、異なるプロトコルまたはエンドポイント間の概要統計を比較することができます。

エンドポイント統計

エンドポイント統計はネットワーク分析の重要な構成部分であり、科学的ネットワーク分析システムは物理エンドポイントと IP エンドポイントに分け、独立したビューで物理アドレスと IP アドレスの通信情報をそれぞれ表示する。ネットワークエンドポイント統計解析機能により、ユーザーは通信量が最大の IP エンドポイントと物理エンドポイントを迅速に位置特定することができる。システムはまた、HTTP プロトコルを使用してトラフィックが最大となる上位 5 つの IP エンドポイントを知ることができるなど、各ネットワークプロトコルのエンドポイントトラフィックの明瞭な統計ランキングをサポートする。

プロトコル統計

プロトコル統計は OSI 七層プロトコル分析に従い、実際のネットワークプロトコルのカプセル化順序に基づいて、階層化はユーザーに現れ、各プロトコルは

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

独自の色を持ち、グローバルなプロトコル統計のほか、各ネットワークエンドポイント下のプロトコル統計データを提供することができる。

セッション統計

セッション統計はネットワーク内のセッション情報を統計する物理アドレス、IP アドレス、TCP 接続、UDP セッションを提供し、現在選択されているセッションのパケットなどの情報を下のサブウィンドウに表示します。各セッションを表示することで、ソースアドレス、宛先アドレス、セッションで送受信されたパケット、およびこれらのパケットのサイズなどの情報を統計できます。これらの情報から、現在のネットワーク内のセッションの通信状況を特定できます。

マトリックス統計

マトリックス統計により、ネットワーク内で通信されているノードとセッションの詳細な統計をとることができ、ユーザーは異なる統計タイプを使用してマトリックスビューを表示することができ、また、ユーザーは表示オプションをカスタマイズすることもできます。

グラフ統計

グラフ統計はユーザーに柔軟なグラフカスタマイズ機能を提供し、ユーザーは様々なタイプのグラフをカスタマイズして作成することができ、グローバルグラフのほか、各プロトコルとネットワークエンドポイントのグラフデータ収集表示もサポートする。

レポート統計

レポート統計は、サマリー統計、診断統計、TOP N 統計など、さまざまなタイプのレポートを自動的に生成します。ユーザーはレポート・オプションを使用して、表示と統計のレポート・アイテムを決定でき、レポートを生成した後、生成したレポートを html、htm、pdf 形式でディスクに保存することもできます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

11 専門家診断

専門家診断は科学技術ネットワーク分析システムの重要な機能であり、捕捉されたデータをインテリジェント化した分析を行い、ネットワーク内のエラー情報または障害情報に対して、自動的に提示することができ、ユーザーはパケットの詳細を理解する必要はなく、専門家診断モジュールからネットワーク内のエラーと障害分析を得ることができる。

11.1 診断の参考

各診断イベントに対応して、専門家診断モジュールはイベントの解釈、原因、および採用可能なソリューションを提供し、管理者は現在のネットワーク状況を迅速に理解しやすく、診断の参考情報に基づいて迅速に応答し、ネットワークエラーと障害問題をタイムリーに排除することができます。

診断イベントの情報の説明、障害の原因、および推奨される解決方法については、解析設定の“診断設定” で確認できます。

11.2 参照情報-アプリケーション層

次に、アプリケーション層のイベント診断の対応情報を示します。イベント名、イベントの説明、重要度レベル、考えられる原因、および解決方法を含む:

イベント	説明	重要度レベル	可能な原因と解決方法
DNS ホストまたはドメイン名は存在しません	ユーザーが要求したドメイン名は存在しません	情報	要求されたドメイン名が存在しないか、ドメイン名入力エラーが発生しました。
DNS ホストの遅い応答	DNS サーバの平均応答時間は、DNS ホストの遅い応答閾値以上である。	注意	DNS サーバーの過負荷。
DNS エラー	ユーザーが要求したホストまたはドメイン名が正常に返されませんでした	注意	クエリ形式のエラー、サーバの失敗、実装されていない、拒否、予約。
HTTP サーバの応答	HTTP サーバの平均応答時間は	注意	Web サーバの過負荷。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

イベント	説明	重要度レベル	可能な原因と解決方法
が遅すぎる	HTTP スロー応答プリセット閾値以上である。		
HTTP 検証に失敗	HTTP クライアントによる認証要求が失敗したため、認証が拒否されました。	警告	ログイン時に間違ったユーザー名またはパスワードが使用されました。
HTTP ポートを用いた通信の非 HTTP トラフィック	HTTP（80）ポートを用いた通信の TCP 接続非 HTTP を含むトラフィック	警告	アプリケーションはTCP 80 ポートを使用して動作しますが、HTTP 以外のトラフィックを転送します 。ソースと宛先から送信されるトラフィックの内容を確認します。クライアントが要求したページが見つからない場合、HTTP サーバはこのエラーを返す（404）。
HTTP 要求ページが見つかりません	クライアントが要求したページが見つからない場合、HTTP サーバはこのエラーを返す（404）。	消息	ユーザーは無効な Web アドレスを入力した。Web サーバ接続が中断されました。HTTP サーバは、クライアント要求ページが見つからないことを示す 404 以外の 4 xx コードを返してクライアントエラーを識別します。
HTTP クライアントエラー	HTTP サーバは、クライアント要求ページが見つからないことを示す 404 以外の 4 xx コードを返してクライアントエラーを識別します。	消息	サーバは 5 XX のコード識別サーバエラーを返し、クライアントの要求は通常正しい。
HTTP サーバエラー	HTTP サーバは 5 XX のコード識別サーバエラーを返し、クライアントの要求は通常正しい。	警告	POP 3 クライアントがサーバにログインできませんでした。
POP3 ログイン失敗	POP3 クライアントがサーバにログインできませんでした。	警告	ユーザー名またはパスワードが間違っています。
POP3 サーバの応答が遅すぎる	POP3 サーバの平均応答時間は、POP 3 スロー応答プリセットしきい値以上である。	注意	POP3 サーバーが過負荷になっています。
POP 3 ポートを使用した非 POP 3 トラフ	POP 3（110）ポートを使用した通信の TCP 接続非 POP 3 を含	警告	アプリケーションは TCP 110 ポートを使用して動作しているが、非

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

イベント	説明	重要度レベル	可能な原因と解決方法
ィック	むトラフィック		POP 3 トラフィックが転送されている。 ソースと宛先から送信されるトラフィックの内容を確認します。
POP3 サーバリターンエラー	POP3接続または要求は、TCP接続が正常に確立された後、POP 3サーバによって拒否されます。	ピンチ	クライアントは間違ったコマンドを実行しました。 サーバがビジーです。 SMTP クライアントがサーバにログインできませんでした。
SMTP ログインに失敗	SMTP クライアントがサーバにログインできませんでした。	警告	ユーザー名またはパスワードが間違っています。
SMTP サーバの応答が遅すぎる	SMTP サーバの平均応答時間はSMTP スロー応答プリセット閾値以上である。	注意	SMTP サーバーの過負荷。
SMTP ポートを使用した通信の非 SMTPトラフィック	SMTP (25) ポートを使用して通信する TCP 接続は、SMTP 以外のトラフィックを含む。	警告	アプリケーションはTCP 25 ポートを使用して動作していますが、SMTP 以外のトラフィックが転送されます。 ソースと宛先から送信されるトラフィックの内容を確認します。
SMTP サーバリターンエラー	SMTP 接続または要求は、TCP接続が確立された後に SMTP サーバによって拒否される。	ピンチ	クライアントは間違ったコマンドを実行しました。 サーバがビジーです。 FTP クライアントがサーバにログインできませんでした。

11.3 参照情報-トランスポート層

次に、トランスポート層のイベント診断の対応情報を示します。イベント名、イベントの説明、重要度レベル、考えられる原因、および解決方法を含む:

イベント	説明	重要度レベル	可能な原因と解決方法
TCP 重複接続試行	クライアントは TCP 接続を確立しようと複数回試みた。	警告	クライアントからサーバへ送信されたSYN パケットとサーバから返されたACK パケットはファイアウォールに

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

イベント	説明	重要度レベル	可能な原因と解決方法
			よってブロックされる。 クライアントはサーバが提供していないサービスを要求しました。
TCP 接続が拒否されました	クライアントは TCP 接続の初期化を試みたが、ターゲットホストによって拒否された。	警告	クライアントはサーバが提供していないサービスを要求しました。 サーバには新しい接続を受け入れるための十分なリソースがありません。
TCP 再送パケット	TCP 再送は、送信側が受信側からあるパケットの ACK 確認を受けていない場合に再送される。	注意	ACK は、より遅いルーティングによりパケットが伝送されることを確認する。 ネットワーク負荷が大きすぎる。 受信側またはルータが過負荷です。
TCP チェックサムエラー	TCP ヘッダ和 (または) データチェックサムに誤りがある。送信側はパケットを送信する前にチェックサムを計算し、チェックサムの値をパケットに書き込み、受信側はパケットを受信した後にパケットのチェックサムを再計算し、2 つの値が異なるとエラーを表します。	警告	ネットワーク上のデバイスに障害がある 。 すべてのローカルパケットのチェックサムがエラーとして表示されている場合、チェックサムを計算しない機能が有効になっている可能性があります。この機能が使用可能になると、アダプタは CRC を計算するプロセスを実行します。Windows の TCP/IP スタックは IP と TCP チェックサムを計算せず、0 x 0000 で識別されます。科来ネットワーク分析システムは、各出力パケットがアダプタに到着する前にコピーを収集します。 この問題を解決するには、ネットワークアダプタの詳細設定ダイアログボックスでアダプタの転送 TCP チェックサムを無効にする必要があります。
TCP スローレスポンス	TCP 接続における ACK パケットの応答時間は、TCP 接続の遅い応答閾値 + 平均応答時間を超える。	警告	遅いルーティングでパケットが転送されることを確認します 。 ネットワーク負荷が大きすぎる。 受信側またはルータの過負荷。
TCP 重複の確認	ある TCP の確認番号とシリアル番号は同時に 3 回以上	性能	TCP ベースの DOS/DDOS 攻撃は、TCP SYN を使用してサーバに複数の

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

イベント	説明	重要度レベル	可能な原因と解決方法
	繰り返され、同じ TCP ヘッダを持つ。		半開 TCP 接続の作成と維持を強制し、リソースの枯渇、サービスの拒否を招いた。
TCP ポートスキャン	ローカルまたはリモートのワークステーションがネットワークで開いている TCP ポートをスキャンします。	警告	ポートスキャンはネットワーク侵入のフラグです。ローカルホストがワームウイルスに感染するか、スキャンソフトウェアを使用してポートスキャンを人為的に実行します。
TCP SYN ストーム	大量の TCP 同期パケットが閾値を上回るレートで送信される。	安全	TCP ベースの DOS/DDOS 攻撃は、TCP SYN を使用してサーバに複数の半開 TCP 接続の作成と維持を強制し、リソースの枯渇、サービスの拒否を招いた。
TCP ヘッダオフセットエラー	5 未満の TCP ヘッダオフセット値が発生した。	安全	ホストは間違った TCP パケットを送信しています。

11.4 参照情報-ネットワーク層

ネットワーク層のイベント診断の対応情報を次に示します。イベント名、イベントの説明、重要度レベル、考えられる原因、および解決方法を含む:

イベント	説明	重要度レベル	可能な原因と解決方法
ICMP 目標到達不可	ワークステーションに ICMP ターゲット不達メッセージが受信されました	警告	ターゲットネットワークが存在しません
ICMP ホスト到達不可	ワークステーションは ICMP ホスト不達メッセージを受信しました	警告	ターゲットホストは存在しません.
ICMP ネットワーク到達不可	ワークステーションは ICMP ネットワーク不達メッセージを受信する	警告	ターゲットネットワークは存在しません.
ICMP パラメータエラー	ワークステーションが ICMP メッセージを送信しましたパラメータエラーを示します	警告	

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

イベント	説明	重要度レベル	可能な原因と解決方法
ICMP ポート到達不可	ワークステーションに ICMP ポート不可メッセージが受信されました	警告	ワークステーション要求のターゲットポートがターゲットホストで開かれていない
ICMP ホストのリダイレクト	ワークステーションは、コード 1 の ICMP リダイレクトメッセージを受信しました（リダイレクトデータはホストにレポートされます)	警告	ルータがメッセージを送信してワークステーションに目的地に到着するより良いルートが存在することを通知する
ICMP ネットワークのリダイレクト	ワークステーションはコード 0 の ICMP リダイレクトメッセージを受信しました（リダイレクトデータはネットワークに送信されます)	警告	ルータがメッセージを送信してワークステーションに目的地に到着するより良いルートが存在することを通知する
ICMP ソース抑制	ワークステーションに ICMP ソース抑制メッセージが受信されました	警告	メッセージを送信したワークステーションがハングアップしたり、再起動したりする可能性があります.
IP ヘッダの無効なチェックサム	IP ヘッダチェックサムに誤りがある。 送信側はパケットを送信する前にチェックサムを計算し、計算結果をパケットに書き込み、受信側がパケットを受信した後にパケットの IP ヘッダチェックサムを再計算し、2 つの値が異なるとエラーを示します。	警告	ネットワーク上のデバイスに障害がある.
IP 生存期間が短すぎる	IP パケットの TTL フィールドの値が 0 または 1 であることは、パケットが期限切れになり、破棄されることを意味します。	注意	ネットワーク上のルータのルーティングテーブルに誤りがある ネットワークループ ソースホストはパケットの転送を開始する際に低い TTL 値を使用している 元のパケット・ソースの検索を試みることができます
IP アドレス競合	典型的な IP アドレス衝突は、無料 ARP を発行して IP アドレスと MAC アドレスの対応	安全	ネットワーク内のデバイスは、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。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

イベント	説明	重要度レベル	可能な原因と解決方法
	関係を公表することによって、あるIPアドレスの元使用者は他のデバイスが自分が使用しているIPアドレスを使用しようとしていることを検出し、衝突が発生し、ARP情報を使用して試行者に通知する。		

11.5 参考情報-データリンク層

次に、データリンク層のイベント診断の対応情報を示します。イベント名、イベントの説明、重要度レベル、考えられる原因、および解決方法を含む：

イベント	説明	重要度レベル	可能な原因と解決方法
ARP フォーマット違反	Ethernet ネットワークで正しく動作しない、ソース MAC アドレスがマルチキャストアドレスである、または ARP ヘッダ中のアドレス情報が MAC ヘッダ中の情報と一致しないなど、RFC 定義のフレームフォーマットに違反する場合。	安全	データパケットの改ざんや偽造を利用して、仲介者の詐欺などの特殊な目的地に到達する。
要求されていない ARP 応答が多すぎる	ある物理ノードからの ARP 応答が要求されていない応答閾値プリセットのパーセンテージを超えるか等しい場合、科学技術ネットワーク解析システムはこの警告を発行する。	警告	ソース側と宛先側の物理ノードに ARP 詐欺が存在する可能性があることを確認します。
ARP 要求嵐	ARP 要求パケット数が ARP 要求閾値設定の値を超えていることは、ネットワークに ARP 要求嵐が発生している	警告	ARP パケットのソースホストプログラムが ARP 要求を大量に送信しているかどうかをチェックします。

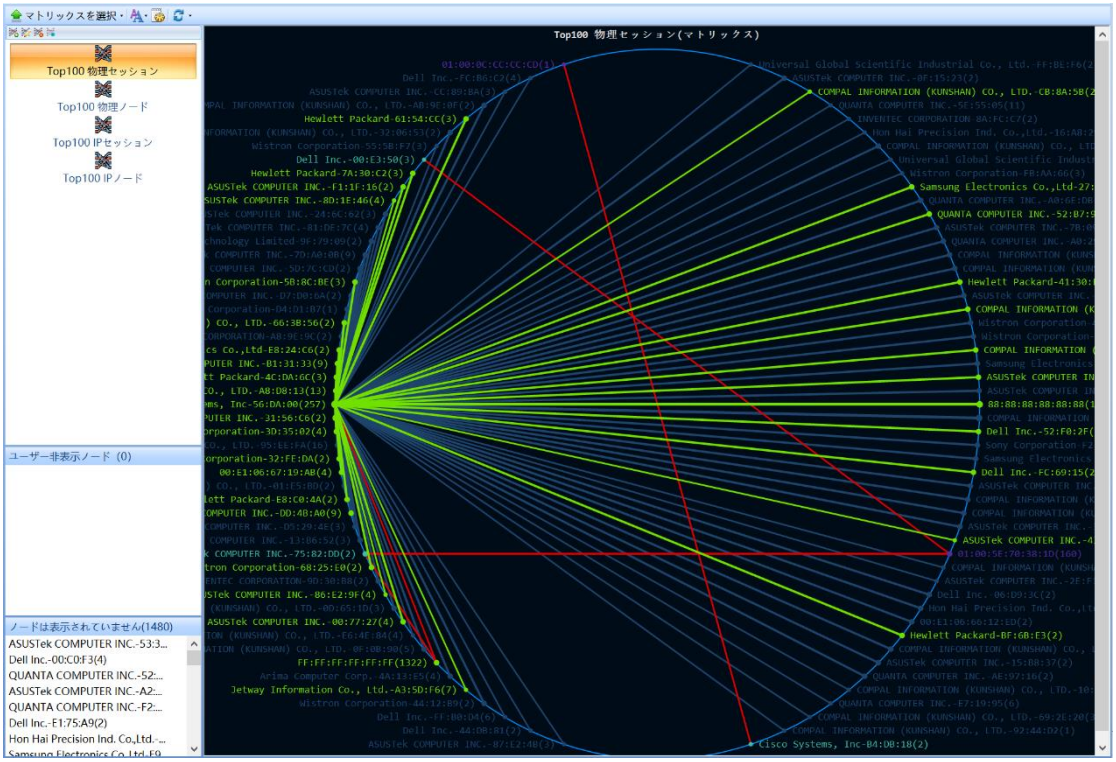
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

イベント	説明	重要度レベル	可能な原因と解決方法
	ことを示す。		
ARP スキャン	ワークステーションは ARP を介してネットワークアドレスのスキャンを要求する。	警告	ARP パケットを送信したソースホストにプログラムがスキャンされているかどうかをチェックします。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

12 マトリックス

Capsa システムが提供するマトリックスビューは、ネットワーク内で通信するノードとセッションを詳細に統計することができ、そのインタフェースは下図のようになる。



システムには最初は 4 種類のマトリックスがあり、ユーザーは新しいマトリックスを追加したり、既存のマトリックスを編集したりすることができます。マトリックスは次のとおりです:

- 物理セッションマトリックス
- 物理ノードマトリックス
- IPv 4 セッションマトリックス
- IPv 4 ノードマトリックス

マトリックスビューを使用して、次の情報を知ることができます:

- ネットワーク通信全体のノード情報。
- ネットワーク通信全体のセッション情報。
- ある物理ホストの通信ノード情報。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

- ある IP ホストの通信セッション情報。
- ある物理ホストの通信ノード情報。
- ある IP ホストの通信セッション情報。
- あるセッションのホスト情報。

マトリックスビューでは、ユーザーはカスタムでマトリックスを追加または削除できます。マトリックスビューツールバーの「マトリックスを追加」ボタンをクリックして、次のダイアログボックスをポップアップします:

- マトリックス名: 追加したマトリックス名をカスタマイズします。
- 最大個数: カスタムマトリクス表示のノード数。
  マトリックスタイプ: 物理アドレスと IP アドレスの 2 種類があり、同時に選択できるのは 1 種類のマトリックスのみを表示することです。
  IP アドレス: IP アドレスノードに基づいてマトリックスコンテンツを表示します。
- トラフィックタイプ: ユニキャスト、マルチキャスト、ブロードキャストの 3 種類があり、1 種類以上のトラフィックを同時に選択して表示することができ、システムはデフォルトで 3 種類のトラフィックをすべて選択します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

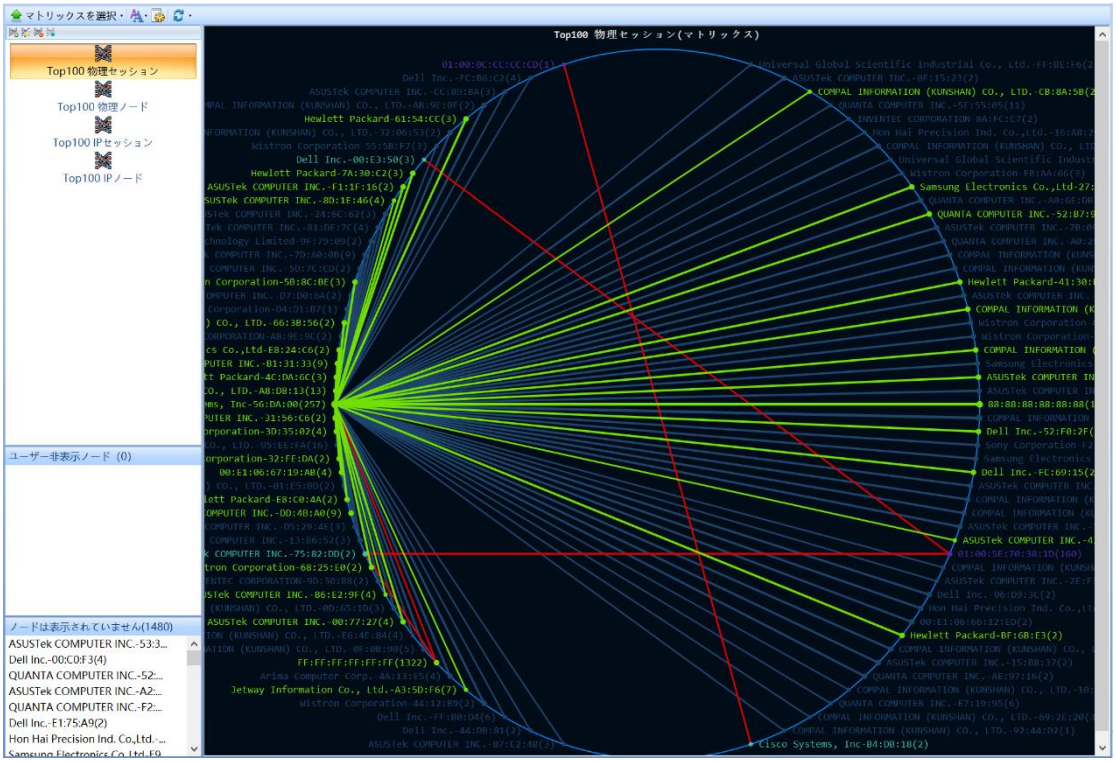
ユニキャスト：ターゲットアドレスとソースアドレスはすべてユニキャストアドレスの流量で、ユニキャスト流量と呼ばれ、ユニキャストを選択すると、右のマトリックスコンテンツ表示領域にネットワーク中のユニキャスト流量のマトリックス情報が表示されます。
マルチキャスト：ターゲットアドレスまたはソースアドレスはマルチキャストアドレスのトラフィックであり、マルチキャストトラフィックと呼ばれ、マルチキャストトラフィックと呼ばれることもあります。マルチキャストを選択すると、右側のマトリックスコンテンツ表示領域にネットワーク中のマルチキャストトラフィックのマトリックス情報が表示されます。
ブロードキャスト：ターゲットアドレスまたはソースアドレスはブロードキャストアドレスのトラフィックであり、ブロードキャストトラフィックと呼ばれ、ブロードキャストを選択すると、右側のマトリックスコンテンツ表示領域にネットワーク内のブロードキャストトラフィックのマトリックス情報が表示されます。

- ソート方法：ノードまたはセッション情報を表示し、降順または昇順で表示します。

12.1 物理マトリックス

物理マトリックスは物理アドレス（MAC アドレス）ノードに基づいてマトリックスの内容を表示し、インタフェースは下図のようになる。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



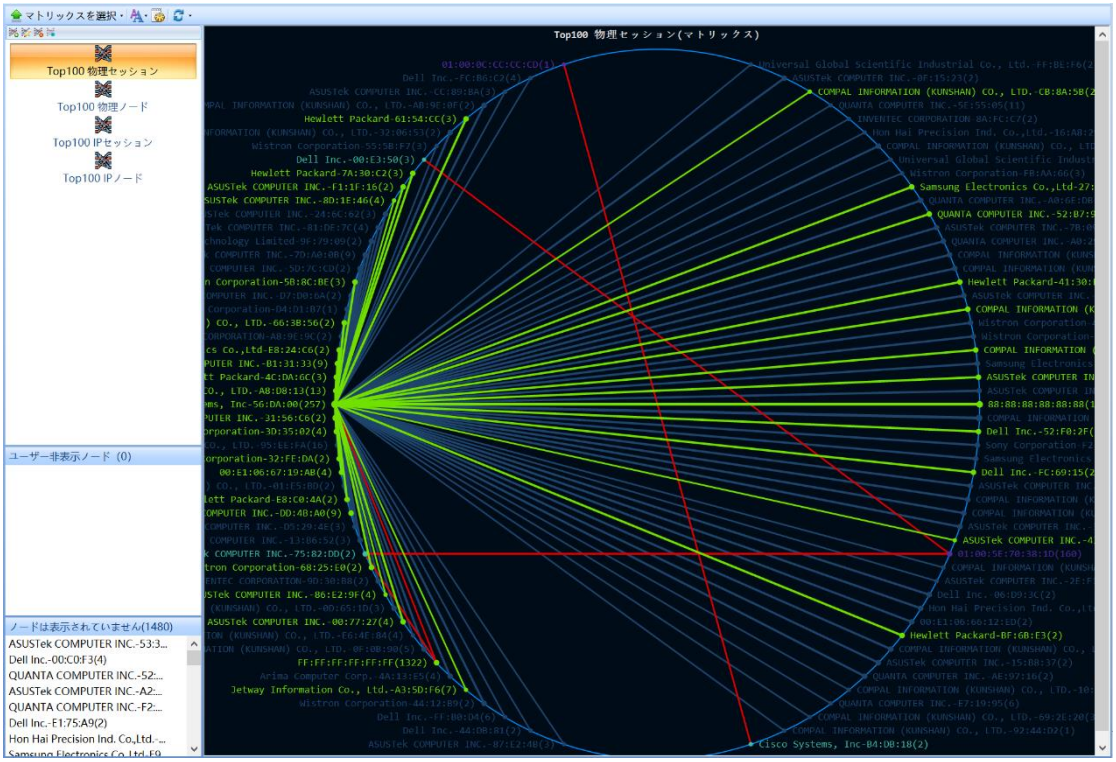
図では、マトリックスタイプは物理を選択しているため、マトリックス内のノードはすべて物理アドレスノードであり、つまりネットワークカード間の通信を表示しています。

このとき、隠れているノードと表示されていないノードの中のノード情報（あれば）も物理アドレスである。

12.2 IP マトリックス

IP マトリックスは IP アドレスノードに基づいてマトリックスの内容を表示し、インタフェースは下図のようになる。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



図では、行列タイプが IP を選択しているため、行列中のノードはすべて IP アドレスノードであり、つまり IP アドレス間の通信を表示している。

このとき、隠れているノードと表示されていないノードの中のノード情報（あれば）も IP アドレスである。

マトリックスビューツールバーには、マトリックス背景色設定、送受信トラフィックの色設定などのマトリックス表示をカスタマイズし、一方向トラフィック、双方向トラフィックなどのさまざまな通信状態の MAC アドレスと IP アドレスを迅速に識別するためのマトリックスオプション機能が提供されています。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

13 パケット復号

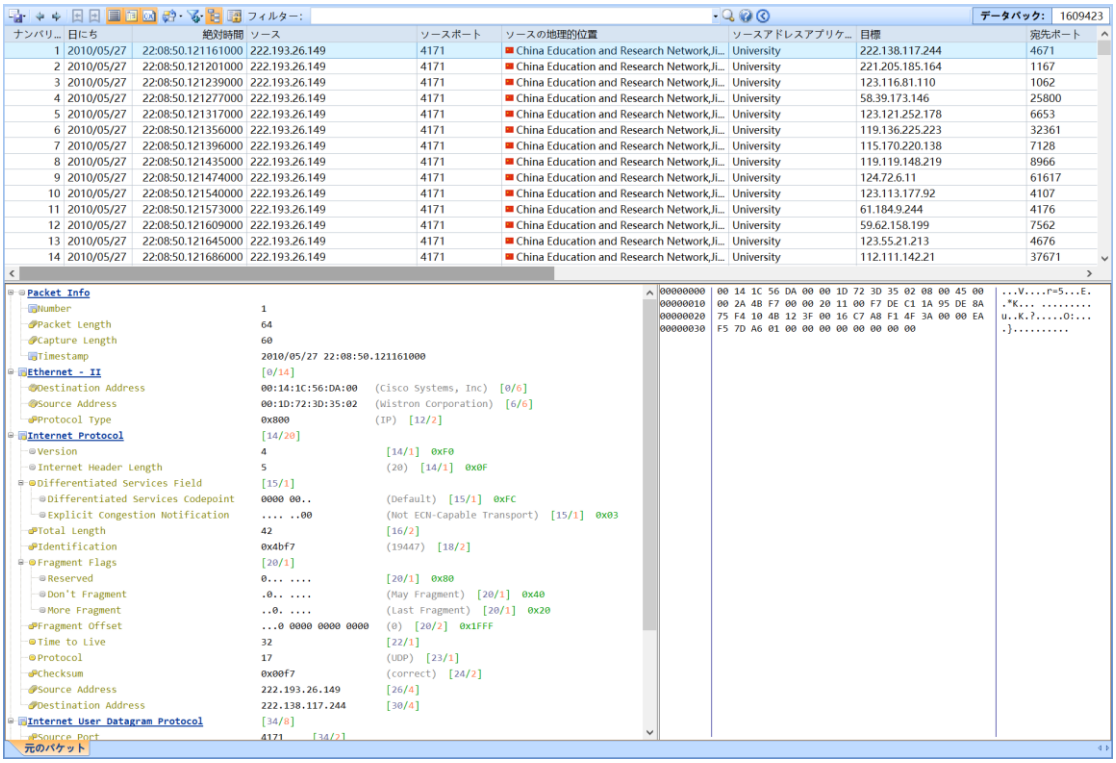
Capsa システムは、デコーダを介して、捕捉されたパケットを自動復号する。復号化は、パケットのレイヤごとの情報を詳細に解釈して分析し、ネットワークの最も細分化された分析を達成することです。

ネットワーク分析が細分化されるほど、ネットワークの管理者はネットワークに存在する異常をより容易に発見できることを意味する。より正確なデータサンプルを収集し、診断と分析を行い、対応策をタイムリーに作成します。同時に、パケット復号分析はネットワークアプリケーションの識別能力を大幅に向上させることができ、ユーザーはネットワーク性能やネットワーク攻撃を低下させる可能性のある潜在的な要素を迅速に見つけることができる。

同時に、「高精細なパケット解析」機能も既存のネットワーク管理システムの不足をカバーしている。現在のネットワークにおけるデータ転送の種類が増加し、ネットワークトラフィックが加速し、ネットワーク構造がますます複雑になっている状況では、ネットワークにおける異常は一瞬にして消失する可能性が高く、従来のネットワーク管理手段を通じてネットワーク障害、ネットワーク攻撃の正確な位置付け、捕捉、分析を行うことは困難である。しかし、「高精細なパケット解析」により、ネットワークの管理者はパケットのキャプチャを通じて各パケットの内容を見ることができ、アプリケーションのソース、目的、役割、その他の詳細を明確に理解することができ、それにより、複雑なデータストリームの中で存在する可能性のある問題を見つけることができる。

パケット復号は概要復号、フィールド復号、16 進復号からなり、3 つのビューボックスからなり、ユーザは復号ビューボックスの配置方法と組み合わせ方法を変更することができる。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



復号化により、次の情報を知ることができます:

- パケットの概要情報（役割、および抽出された重要な値）。
- ネットワーク内のパケットのタイプ。
- ネットワークで転送されたパケットが正しいかどうか。
- ネットワーク内の IP パケットのバージョン。
- ターゲットホストがクライアントホストから要求されたサービスを実行しているかどうか。
- ソースホストからターゲットホストへのルーティング時間（つまりリンク長）。
- クライアントホストから要求されたサービスに対するターゲットホストの応答時間。
- ネットワークで転送されたデータは緊急データであるかどうか。
- ネットワーク上をパケットが通過するルーティングホップの数。
- ネットワークにループ現象が存在するかどうか。
- ユーザーがターゲットホストのサービスにアクセスするための元の手順。
- 偽造パケットが存在するかどうか、すなわち異常なデータ通信である。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

13.1 概要復号

概要復号行ごとに、各取得パケットの概要情報が表示されます。

概要情報は主に、パケットがキャプチャされた絶対時間、ソース IP 及び使用ポート、送信されたターゲット IP 及びポート、使用されたプロトコル、パケットのサイズ、概要内容などを含む。

パッケージを表示するには、管理者は次のことができます:

- 表示オプションを設定し、表示するデータ列をカスタマイズする
- ダブルクリックして新しいウィンドウを開き、パケット復号のすべてを表示します
- 選択したパケットをハイライト表示
- 関心のあるパケットへのコメントの追加
- 関連するパケットの選択
- パケット生成フィルタ
- パッケージのエクスポート
- パケットが存在するノードの位置付け
- ネーム表に MAC アドレスまたは IP アドレスを追加する
- 画面スクロール機能を使用して常に最新のパケットを表示する

13.2 フィールド復号

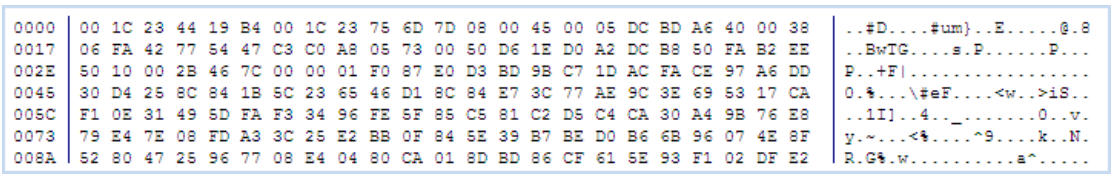
フィールド復号は詳細復号とも呼ばれ、パケットの詳細を見ることができます。デフォルトでは、コーレネットワーク解析システムは、フィールド復号ボックスでプロトコルレイヤのコンテンツをレイヤごとに展開し、ツリー構造に従って表示します。表示スペースを節約するには、プロトコルのサブレベルの前にあるマイナス記号（-）をクリックします。プロトコル表示を再度展開するには、プラス記号（+）をクリックします。プロトコルサブレイヤのデータをクリップボードにコピーするには、右クリックした[ツリー構造をコピー]をクリックします。

フィールドの詳細については、Web サイトで提供されている共通プロトコルの詳細な復号情報を参照してください。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

13.3 16 進復号

16 進復号は、選択したパケットを 16 進法および ASCII（または EBCDIC）フォーマットで表示するものです。「サマリー復号」でパケットを選択するか、「フィールド復号」でプロトコルフィールドを選択すると、図に示すように、対応する 16 進バイト（Hex フォーマット）が「16 進復号ビューボックス」でハイライト表示されます。これにより、プロトコルフィールドとパケット内の対応するバイトの対応関係をすばやく理解することができます。



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

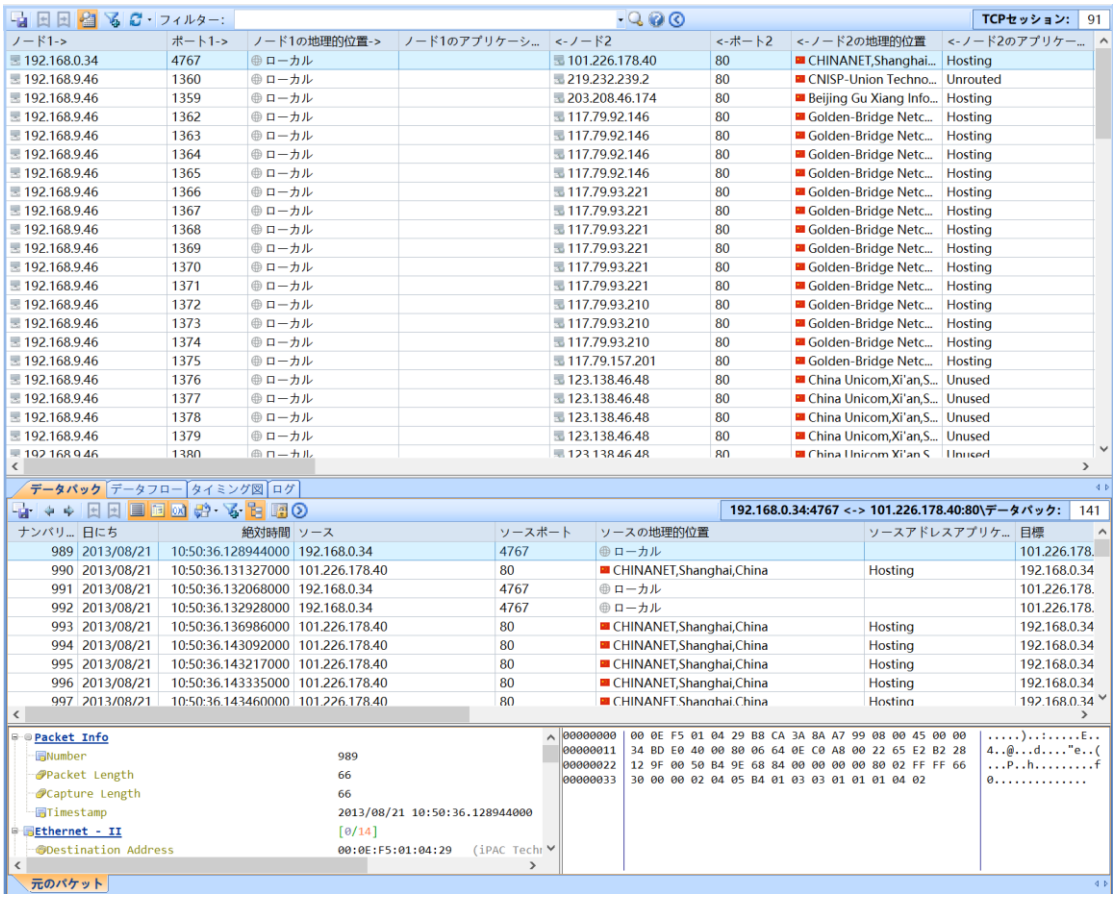
14 TCP セッション分析

14.1 TCP データストリームの再編成

Capsa システムは、取得したネットワークデータを正しい順序で TCP フローに再編成することができる。TCP データストリームにより、管理者はデータの通信状況を完全に把握することができる。TCP データストリーム内のセッション情報を使用すると、クライアントとサーバ側との間の要求と応答を含む、ネットワークセッションごとのプロセス全体を容易に追跡することができます。

Capsa システムは主要な TCP 応用の再編をサポートし、以下を含む：WEB（HTTP）、Email（SMTP/POP 3）、FTP、MSN など。

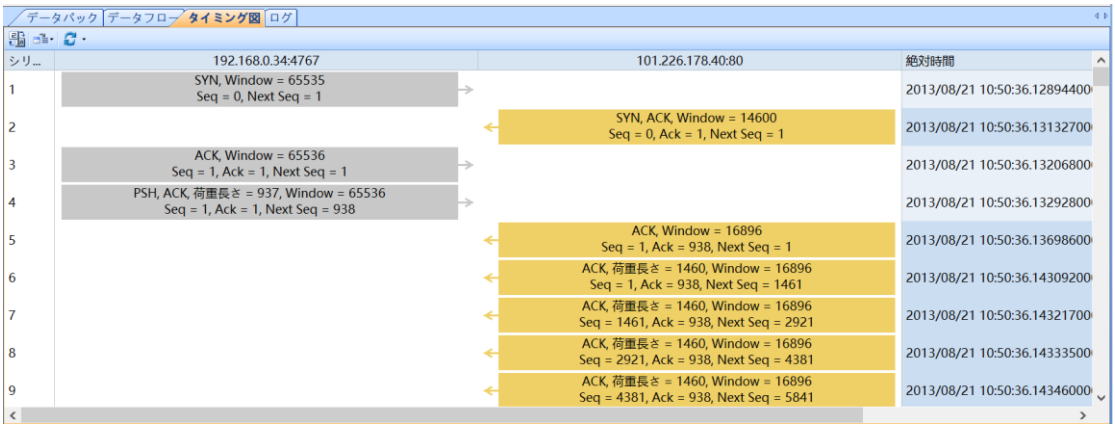
次の図は、クライアントとサーバ側の間のセッションの詳細なプロセスを見ることができる HTTP のデータストリーム再編成結果を示しています。



14.2 TCP セッションシーケンス図

Capsa システムの TCP セッション統計において、TCP セッションビューが区切られたサブビューの下で、TCP データストリーム再編成のほか、TCP セッションシーケンス図も含まれており、TCP セッションの分析を通じて、TCP 接続通信双方の SYN と ACK 応答状態を図形化して示し、ユーザーが TCP 通信内容を理解しやすく、通信中に存在する問題をより直感的に発見するのを助けることができる。

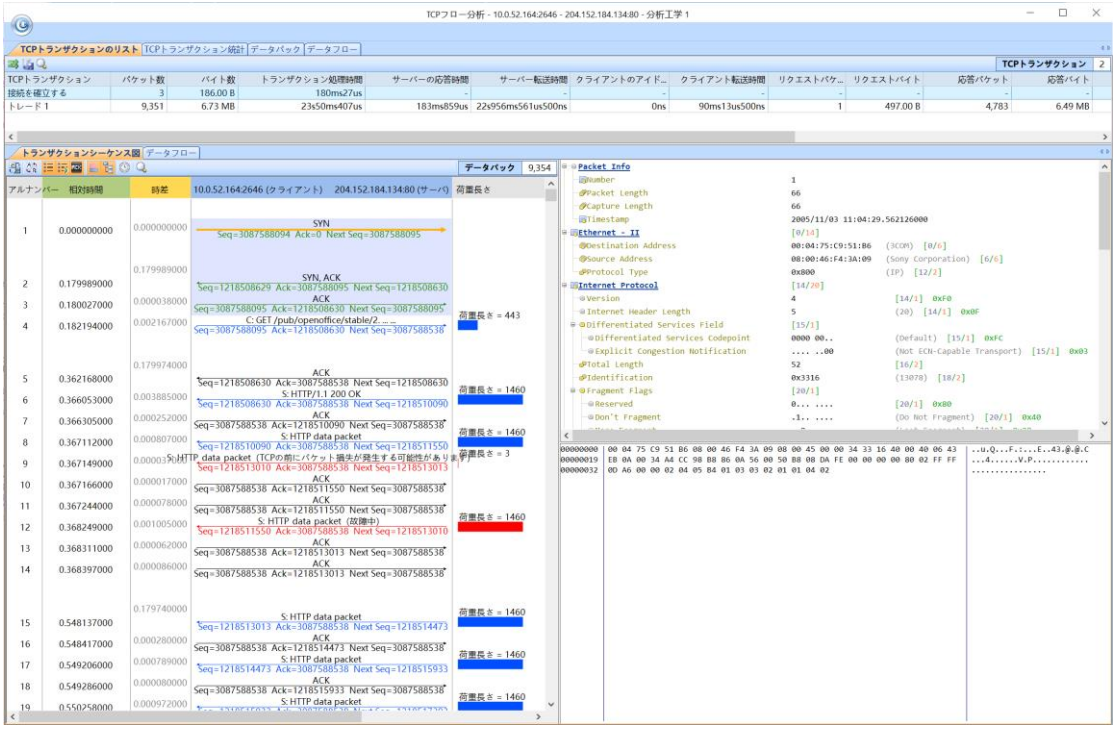
TCP セッションシーケンス図の表示により、ユーザーはネットワークの伝送性能、TCP スキャンなどのネットワークのよくある問題を直感的に分析することができ、TCP セッションシーケンス図インタフェースは下図のように:



14.3 TCP データストリーム分析

TCP セッションビューは、すべての TCP フローを統計的に表示し、クライアントとサーバの詳細な TCP トランザクション詳細を分析する必要がある場合は、ビュー内のセッションをダブルクリックすると、次の図のように 2 つのエンドポイント間の詳細な TCP フロー分析が開きます:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

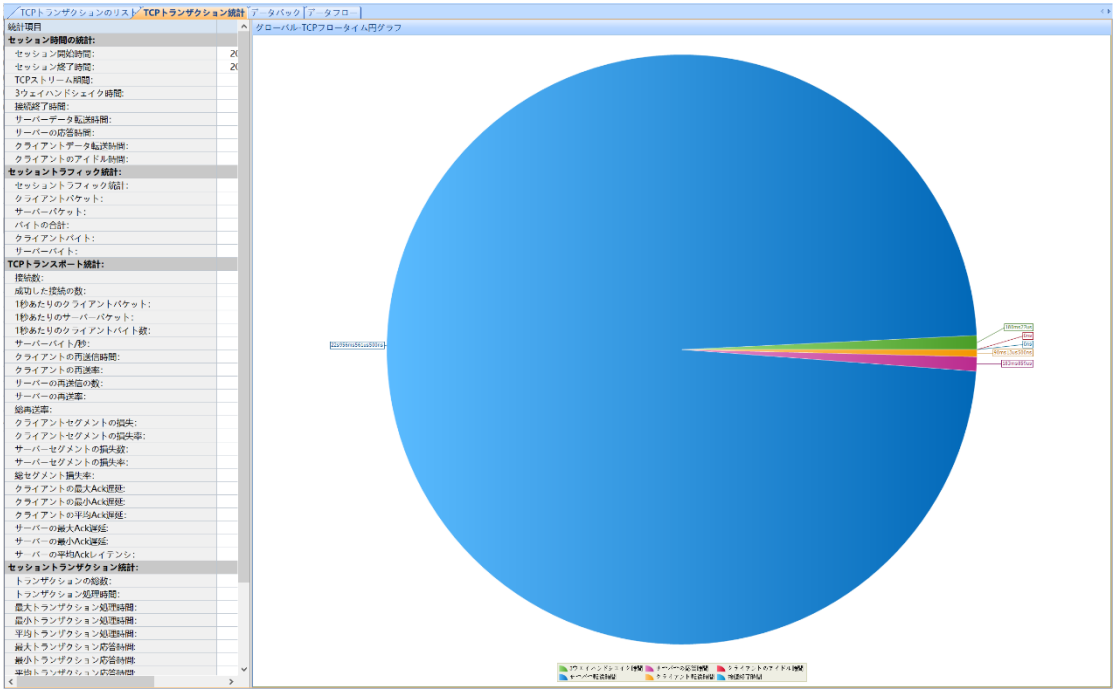


上図から見ると、TCP フロー分析は TCP 取引リストと TCP 取引統計の 2 つのページを含み、クライアント（192.168.5.115）とサーバー端末（121.14.1.12）の間の TCP 伝送詳細を詳細に統計し、接続の確立、伝送詳細、接続の停止のリスト統計、タイミングチャート、パケットなどの情報を含み、ユーザーの直感的な TCP の伝送性能、例えば接続時間の確立、伝送時間、伝送遅延などの分析を助けることができる。

TCP 取引統計ページには、この TCP フローの各種統計データが表示され、セッション時間統計、セッションフロー統計、TCP 転送統計などを含み、各種時間が占める割合を円グラフで表示し、ユーザーは TCP の各種転送詳細を一目で見ることができる。

TCP データストリーム分析を利用して、ユーザーがネットワーク業務の使用、中断、性能などの障害を迅速に解決するのを助けることができる。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。


TCPトランザクションのリスト
TCPトランザクション統計
データパック
データフロー
統計項目
セッション時間の統計:
セッション開始時間:
セッション終了時間:
TCPストリーム時間:
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:
サーバーの応答時間:
クライアントデータ転送時間:
クライアントのアイドル時間:
セッショントラフィック統計:
セッショントラフィック統計:
クライアントパケット:
サーバーパケット:
バイトの合計:
クライアントバイト:
サーバーバイト:
TCPトランスポート統計:
接続数:
成功した接続の数:
1秒あたりのクライアントパケット:
1秒あたりのサーバーパケット:
1秒あたりのクライアントバイト数:
サーバーバイト/秒:
クライアントの再送信時間:
クライアントの再送率:
サーバーの再送信の数:
サーバーの再送率:
総再送率:
クライアントセグメントの損失:
クライアントセグメントの損失率:
サーバーセグメントの損失数:
サーバーセグメントの損失率:
総セグメント損失率:
クライアントの最大Ack遅延:
クライアントの最小Ack遅延:
クライアントの平均Ack遅延:
サーバーの最大Ack遅延:
サーバーの最小Ack遅延:
サーバーの平均Ackレイテンシ:
セッショントランザクション統計:
トランザクションの総数:
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:
最小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応答時間:
最小トランザクション応答時間:
グローバル-TCPフロータイム円グラフ

15 フィルタ

ユーザーは、システムリボンのメニューバー解析設定で「フィルタ」ボタンをクリックしてフィルタ設定ダイアログボックスを開くことができます。科来ネットワーク解析システムはデフォルトのフィルタリストを提供している。これらのフィルタはプロトコルに従ったフィルタです。また、フィルタを任意に組み合わせてパケットの取得範囲を設定することもできます。

「パケットフィルタリスト」ページでは、パケットをキャプチャするフィルタをカスタマイズできます。フィルタが設定されていない場合、科来ネットワーク解析システムはすべてのパケットをキャプチャして解析します。

15.1 旧版フィルタ

フィルタはコーレネットワーク解析システムにおいて単純フィルタと高級フィルタに分けられる。ユーザは、IP、ポート、プロトコル、パケット値などの条件を設定することでパケットをフィルタリングすることができる。フィルタリストでは、フィルタ設定を組み合わせるために、「承認」、「除外」などの論理関係を使用できます。

フィルタを設定することは、取得データの範囲を変更するための重要な手段です。フィルタにより、必要な特定のパケットだけをキャプチャし、重要なデータを分離することができます。これにより、ユーザは、大量のデータの中から1つ1つ探すのではなく、ネットワーク障害やサイバー攻撃が存在するデータ情報だけに注目することができます。

ユーザーが興味を持っている場合は、ウイルスを探すフィルタ、BT パケットを探すフィルタなどを設定することができます。直感的には、フィルタの設定を「単純フィルタ」と「高度フィルタ」に分けています。高度なフィルタリングのフィルタ条件は単純なフィルタリングよりも多いため、単純なフィルタを高度なフィルタに変換できますが、高度なフィルタを単純なフィルタに変換するとフィルタ条件が失われます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

フィルタダイアログボックスでは、グラフィカルなフィルタ設定インタフェースが提供されます。左側のフィルタライブラリには、システムがデフォルトで追加したプロトコルフィルタのコレクションが表示されており、ユーザーはフィルタライブラリでフィルタを直接選択でき、「受信」、「拒否」、および 3 つのフィルタステータスを有効にしないことができます。

このダイアログボックスで「追加」ボタンをクリックして、新しいフィルタの追加をカスタマイズすることができます。追加されたフィルタはダイアログボックスの左側のフィルタセットに自動的に保存され、後で簡単に選択できます。

15.1.1 簡易フィルタ

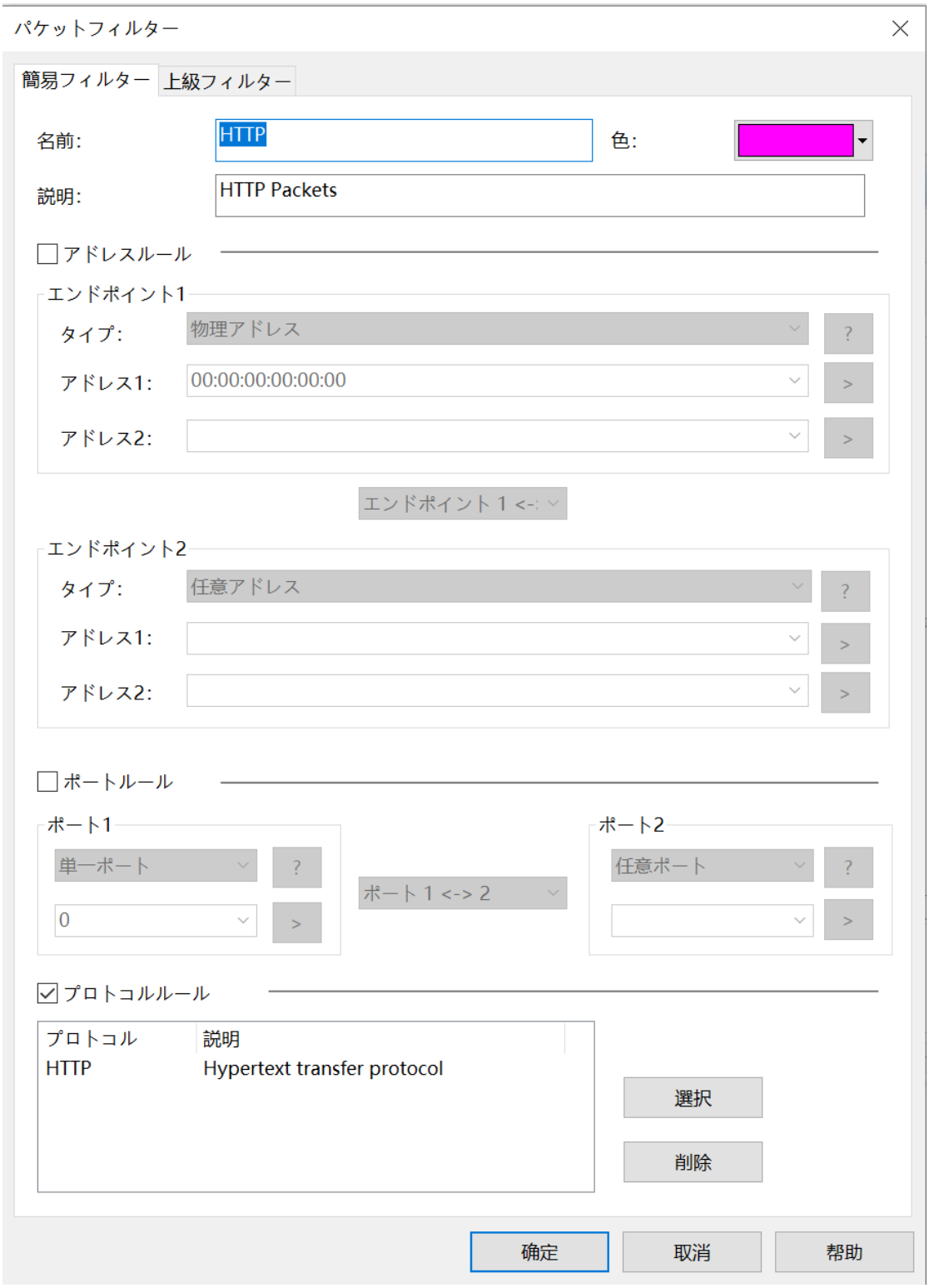
簡易フィルタを使用すると、IP アドレス、MAC アドレス、ポート、プロトコルなどの一般的なフィルタ条件を使用することができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

IP アドレス、MAC アドレス、ポートなどの条件を設定する際に、パケット送信の方向を選択することができます。これにより、データのフィルタリングを正確に行うことができます。一方、プロトコル条件を設定する場合は、フィルタリングのために 1 つ以上のプロトコルを選択することができます。

簡易フィルタリングのフィルタ条件は任意に組み合わせることができ、表示を容易にするために、プロトコルの色を指定して他のプロトコルを区別することができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



アドレスフィルタリング

アドレスを選択してフィルタリングする場合、物理アドレス、IP アドレス、IP

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

範囲、IP マスクを指定して両方のアドレスを定義することができます。同時に、パケットの転送方向を制御することもでき、一方向または双方向のデータを設定することができます。アイコン  クリックすると、入力したすべての履歴が削除され、アイコン  をクリックすると、アドレスフィルタリングされた入力フォーマットが表示されます。

ポートフィルタリング

ポートフィルタリングにもさまざまな方法があり、ユーザーは単一のポート、または 1 つのポート範囲、または複数のポートを選択できます。

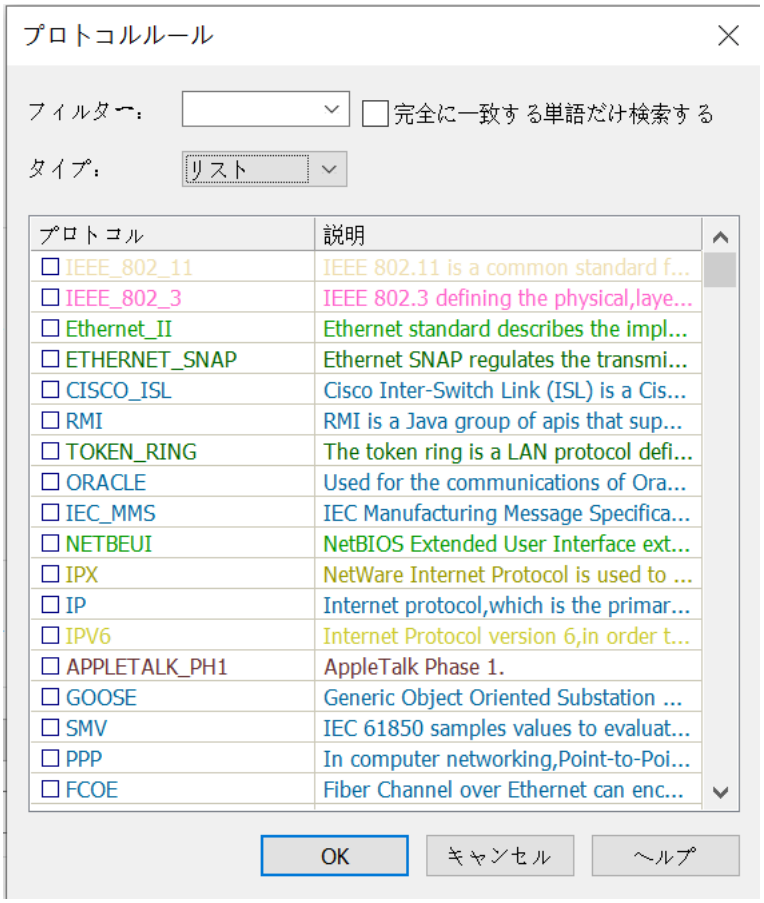
プロトコルフィルタリング

プロトコルフィルタリングは、次の図に示すように、1 つ以上のプロトコルを選択してフィルタ条件を定義できる完全なプロトコルツリーを提供します:

プロトコルフィルタでは、システムは 2 つのプロトコル表示方法を提供します:

- リスト: システムでサポートされているすべてのプロトコルを詳細にリストします。
- 階層化: OSI 標準モデルに従ってプロトコルの作業階層で表示されます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

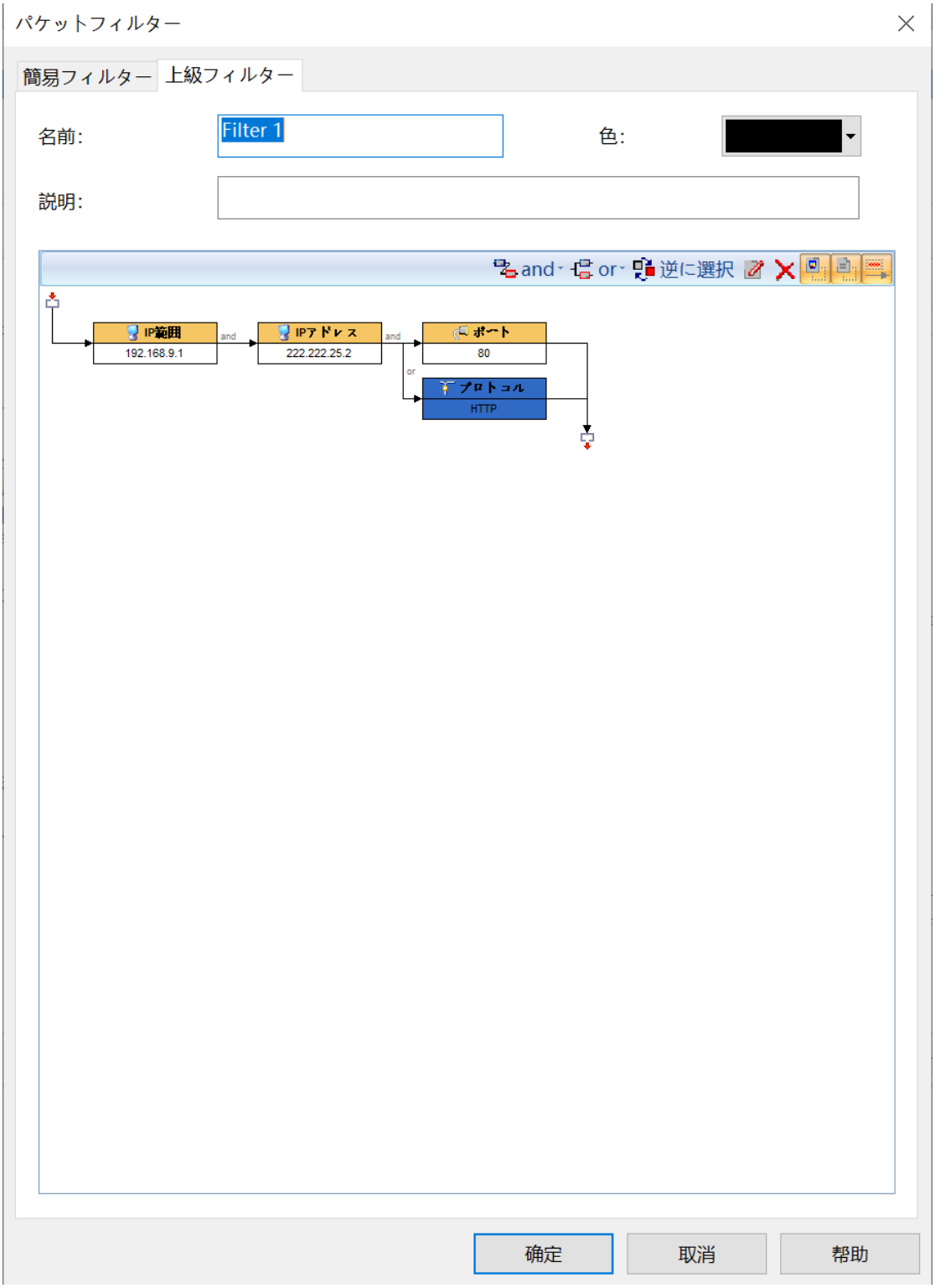


15.1.2 高級フィルタ

簡易フィルタと比較すると、拡張フィルタにより、「パケット値」フィルタ、「パケットサイズ」フィルタ、「パケットモード構成」フィルタ条件が追加され、さまざまな条件を組み合わせるためのさまざまな論理関係が提供されます。

高級フィルタ設定では、設定されたフィルタ条件の論理関係を示す非常に直感的なフィルタ関係図を提供し、ネットワークカードからホストへの過達経路を通じて、フィルタの条件関係を簡単に見ることができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



高級フィルタを作成する場合は、フィルタのツールバーを使用してさまざまな条件を組み合わせることができます。上図は、ネットワーク範囲を監視する BT を使用したフィルタ設定です。

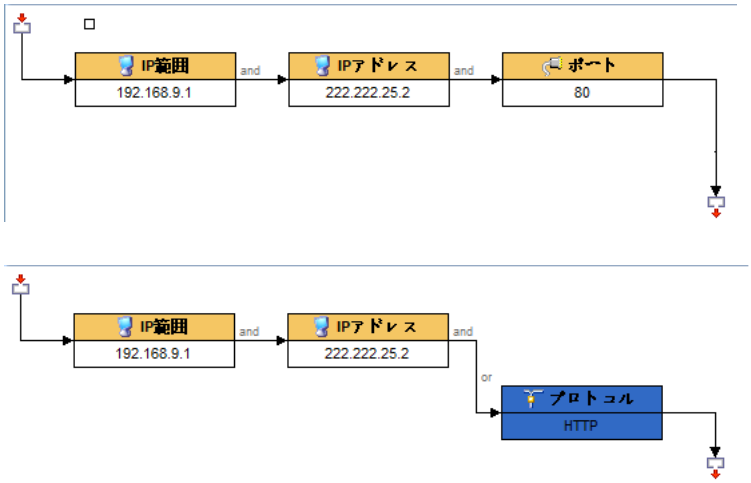
著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

最初の条件：ネットワークセグメント範囲を満たす、192.168.0.1-192.168.0.200

2 番目の条件：IP を 1 つ除外する、192.168.0.10

3 番目の条件：BitTorrent プロトコルを使用して設定された条件の 1 つを満たすこと、またはポート範囲が 6881～6889 のパケットです。

設定された各フィルタ条件の中で右クリックして、関連する属性設定があり、フィルタ条件を編集または削除することができ、新しいフィルタ条件を追加することができ、フィルタ条件の詳細情報を表示または非表示にすることができ、インタフェースは下図のようになります。



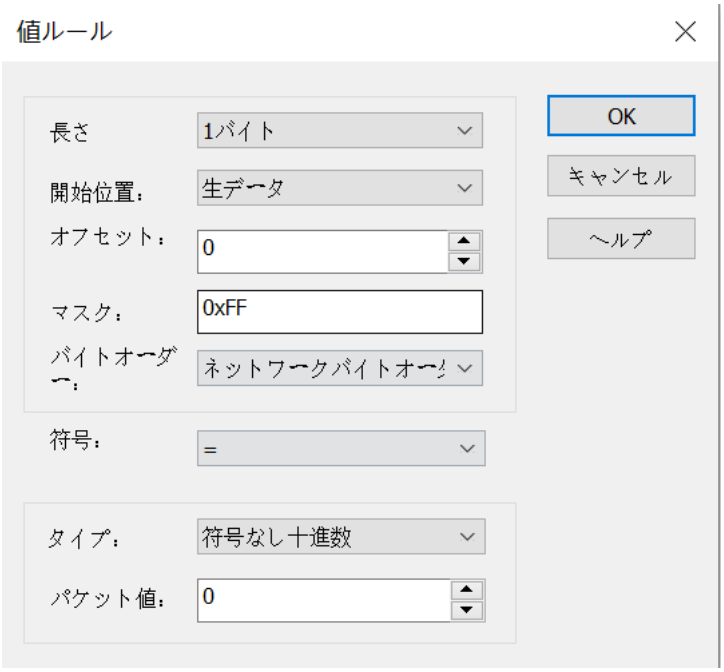
フィルタのツールバーを見てみましょう：

コマンド	説明
と(And)	「と」関係を提供し、関連する 2 つの条件を同時に満たす必要があります。
また(Or)	「また」関係を提供し、少なくともいずれかの条件を満たす。
非(Not)	「非」関係を提供し、設定した条件とは逆の条件を満たす。
Edit	選択したフィルタ設定の編集
Delete	選択したフィルタ条件の削除
アイコン表示	フィルタのアイコンを表示
詳細表示	フィルタの詳細を表示

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

簡易フィルタリングを含む条件に加えて、高級フィルタリングは、より正確な条件でフィルタリングすることができ、次のような条件のいずれかのパケットにほぼ一致することができます:

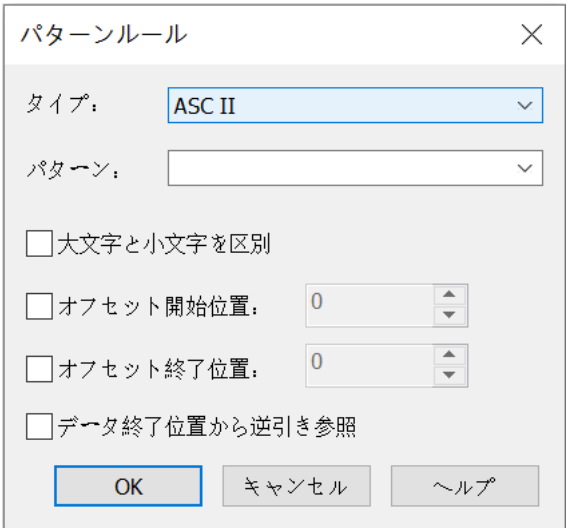
パケット値フィルタ



パケットサイズフィルタリング

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

パケット内容フィルタ



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

15.2 DPI Filter フィルタ

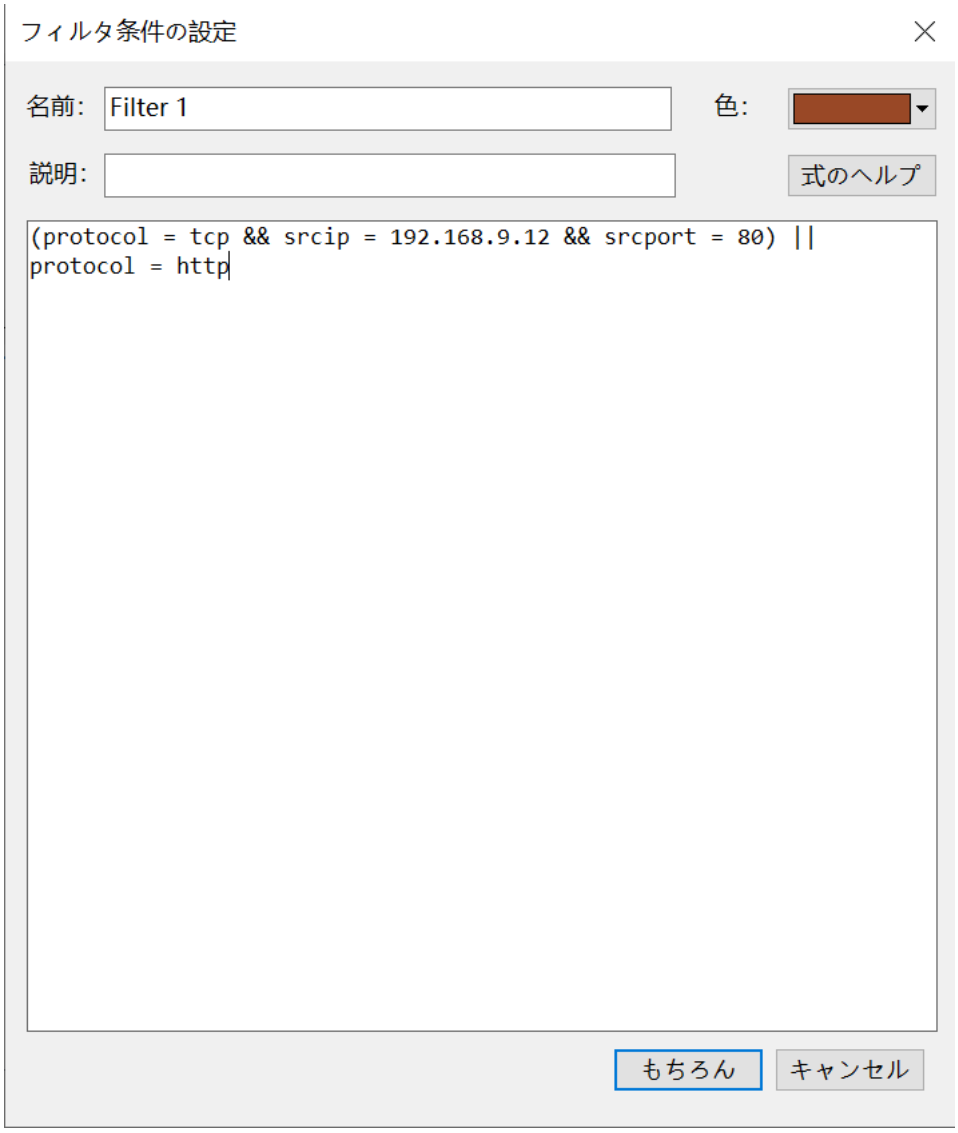
現在、Dpi フィルタは 64 ビットオペレーティングシステムにのみ適用され、命令セット AVX をサポートしている。

フィルタリストでは、フィルタをチェックすることでフィルタ設定を組み合わせることができます。次の図に示します:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

15.2.1 フィルタ設定

DPI Filter フィルタは、フィルタ条件を表す式の形式を使用できます。DPI Filter フィルタ設定の画面を下図に示します:



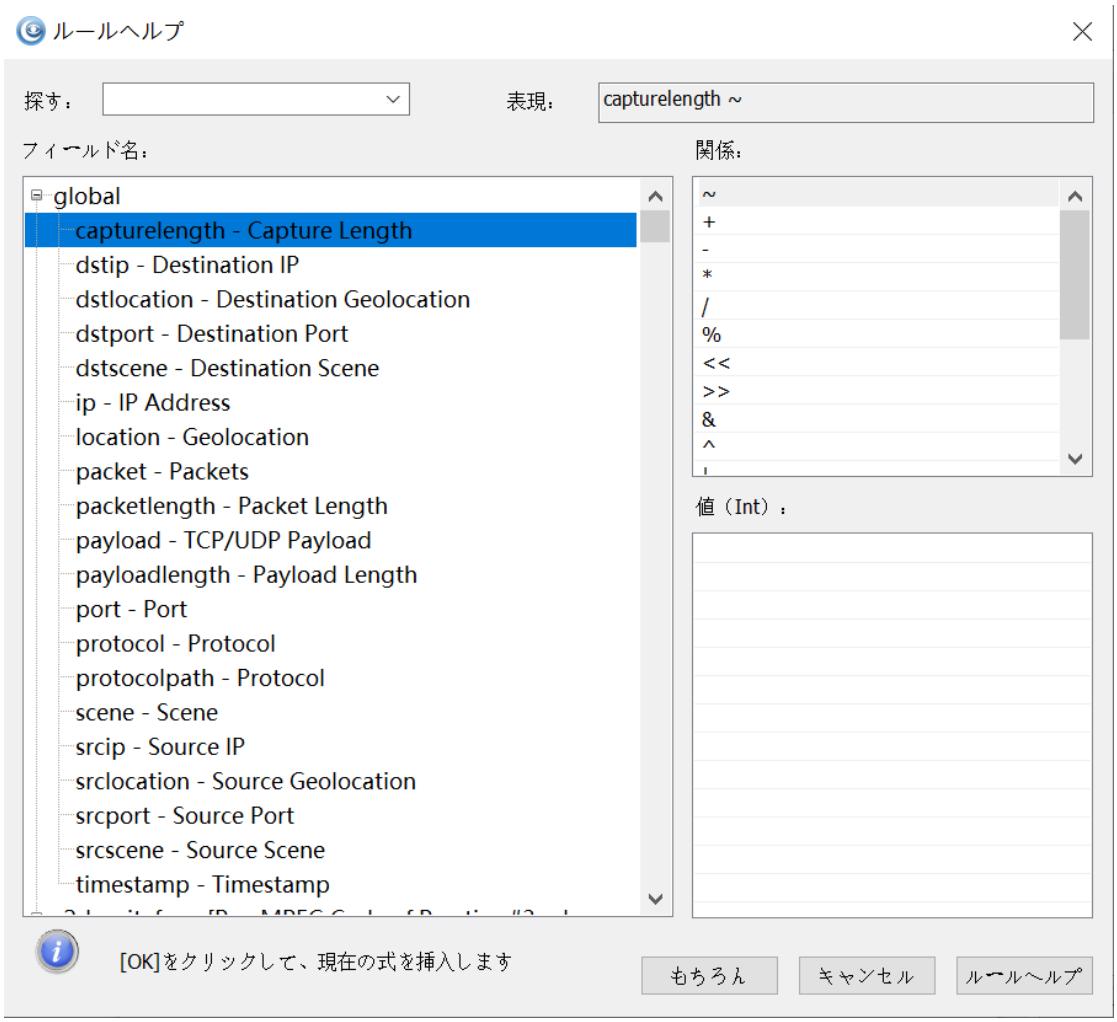
Note

式の構成は、フィールド名、オペレータ、値、論理演算子で構成されています。式の詳細については、 “式のヘルプ” を参照してください。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

15.2.2 フィルタヘルプ

式ヘルプインタフェースには、現在サポートされているすべてのプロトコルとフィールド、フィールドに対応するオペレータ、フィールドの値タイプ、特定のフィールド値の一部の書き方が列挙されています。式ヘルプインタフェースは次の図のようになります:



Note

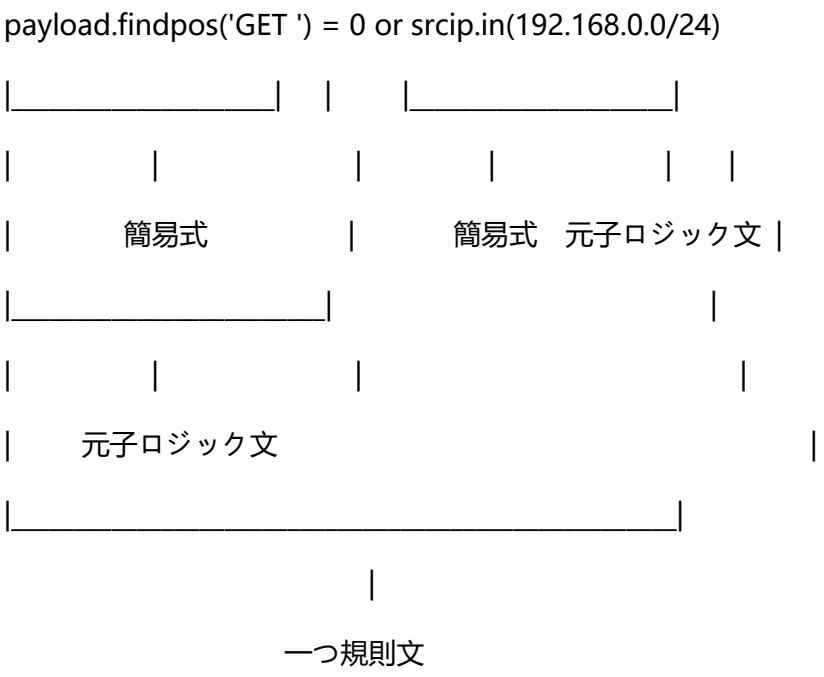
フィールド情報を知りたい場合は、エクスプレッションインタフェースの上にある検索ボタンを使用して、検索フィールドの完全なフィールド名を入力して検索することができます。または、フィールドツリーを展開して表示することで、フィールドでサポートされているオペレータ、タイプ、値が右側の適切な位置に表示されます。

式規則の説明

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

規則と規則グループ

1.DPI Filter 規則はロジック式で構成され、各ロジック文は簡易式で構成されています。例:



2. 規則グループは複数の規則文で構成されています。次の規則には、ID=0、1、2（ロジック的または関係）の 3 つの規則があります:

payloadlength <= 30 && payload[0,6].find('https:')

!(payload[3,20].find(HEX'00 00 00 0A 00 00 00 00')) || dstport >=1000

payload[0,4] = HEX'03 00 00 00' and (payload.find(HEX'10 00 00 0C 0A 83 86 7C') or packetlength <= 2000)

タイプ表現規則

String タイプの表示規則

String	規則
一対の一重引用符 ''	エスケープはサポートされていません。コレクション: 一重引用符''を除くすべての表示される ASCII 文字
16 進 String	HEX'00 A'など、一重引用符の前に HEX 接頭辞修飾を追加します

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

詳細な例は“String タイプ式“を参照してください。

2.DateTime タイプの表示規則

DateTime には、秒レベル（DTSec）とナノ秒レベル（DTNanoSec）の 2 種類の経度タイプがあります。DT'2022-01-01 07:59:60+0800'などのうるう秒をサポートします。

書式	説明
DT 'year month mday hour min sec'	タイムゾーンなし、秒レベル DT タイプ、ホストローカルタイムゾーン
DT 'year month mday hour min sec .nanosec'	タイムゾーンなし、ナノ秒レベル DT タイプ、ホストローカルタイムゾーン
DT 'year month mday hour min sec ±timezone'	タイムゾーン付き秒レベル DT タイプ
DT 'year month mday hour min sec .nanosec ±timezone'	タイムゾーン付きナノ秒レベル DT タイプ

また、次の制約を満たします：
•字面値は DT'と'で修飾しなければならない；
•year 年、連続する 4 文字の数字で構成され、1970 未満の数字は使用できません；
•month 月、連続する 2 つの数字文字から構成され、2 桁未満は前にゼロを補う必要があり、合法的な範囲[01、12]；
•mday day of the month、連続する 2 つの数字文字からなり、2 桁未満は前にゼロを補う必要があり、合法範囲[01、31]；
•hour 時，連続した 2 つの数字文字からなり、2 桁未満の場合は前にゼロを補う必要があり、合法的な範囲[00、23]；
•min 分，連続する 2 つの数字文字から構成され、2 桁未満は前にゼロを補う必要があり、合法範囲[00、59]；
•sec 秒，連続する 2 つの数字文字から構成され、2 桁未満は前にゼロを補充し、合法的な範囲[00、60]、うるう秒をサポートする；

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

•nanosec ナノ秒，連続する 9 つの数字文字から構成され、9 桁未満は前にゼロを補う必要がある、必要があります。接頭辞が一緒に表示され、ナノ秒と接頭辞の間に他の文字を挟むことはできません。ナノ秒ビットの有無は DT タイプの精度を判定する唯一の識別である：ナノ秒の有無は DTSec タイプである、ナノ秒があれば DTNanoSec タイプ;
•timezone タイムゾーンの修正、GMT/UTC との時差は、連続する 4 つの数字文字から構成され、最初の 2 つの数字は時間後の 2 つの数字は分で、足りない桁は前にゼロを補充しなければならない、接頭辞+または-とともに表示されなければならず、他の文字を挟むことはできません。+は UTC より前、-は UTC より後;
•その他
1.DT 字面値 空白の文字'''、' t'、' n'などをすべて無視します。
2.year、month、mday の間には、合法的な空白文字以外の文字を分割することができます。
4. 合法的な空白以外の分割文字は（限定されない）を含む !"#$%&*+,-./:;@^_|~。

合法的な書き方の例:

分類	例
タイムゾーン接尾辞なし：デフォルト localtime タイムゾーン	DT'2022-09-26 11:02:59' DT'2022/09/26 11:02:59' DT'2022-09-26 11:02:59.981815000' DT'2022/09/26 11:02:59.981815000'
UTC	DT'2022-09-26 11:02:59+0000' DT'2022/09/26 11:02:59+0000' DT'2022-09-26 11:02:59.981815000+0000' DT'2022/09/26 11:02:59.981815000+0000'
東京時間 CST	DT'2022-09-26 11:02:59+0800' DT'2022/09/26 11:02:59+0800' DT'2022-09-26 11:02:59.981815000+0800' DT'2022/09/26 11:02:59.981815000+0800'
太平洋標準時 PST	DT'2022-09-26 11:02:59-0800' DT'2022/09/26 11:02:59-0800' DT'2022-09-26 11:02:59.981815000-0800' DT'2022/09/26 11:02:59.981815000-0800'
その他の合法的なフォーマット	DT'20220926 11:02:59-0800' DT'20220926110259' DT'20220926110259+0800'

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

	DT'2022/09/26 110259-0800' DT'2022 09 26 11 02 59 +0800' DT'2022-09-26 110259-0800' DT'20220926110259.055000000+0800'

詳細な例は“DateTime タイプ式“を参照してください

3. 正規表現式のタイプ表現規則

正規表現式は find()関数でのみ使用されます。正規文法は pattern と modifiers の 2 つの部分が構成され、書き方：/pattern/modifiers、ここで modifiers はデフォルトにできます。

pattern：Perl/POSIX スタイルの正規表現式。

pattern 中単一 \ 文字のエスケープを表します。

pattern 中 \ および / 特徴文字として，エスケープが必要：\\ および \/

modifiers：マッチング方式（モード修飾子）

1 つの modifiers は、i、m、s、V、ゼロまたは複数の modifier から構成される

特定の modifier は設定されておらず、関連する機能は使用できません

modifier は重ねて使用できます

複数の modifier 複数のモディファイヤ間は接続されている必要があり、他の文字は使用できません，例 /abc/i m 中の modifiers の間にスペースがあり、間違った書き方です

modifiers の説明

modifier	説明
i	大文字と小文字が不敏感
m	^ ^ 行頭に一致可能;$一致可能な行末 注意：payload の最初のバイトの位置は行頭ではありません
s	. 新しい行を含むすべての文字を一致させることができます
V	空のストリングを許可します（a | ）

Note

正規表現は完全にサポートされていません。たとえば、いくつかの高度な使用法のサポート状況は次のとおりです：

高級	サポート状況	例
(?:pattern)	サポート	/(?:45|56)123/

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

Zero-width assertions	サポートしません	ゼロ幅アサーション：/(?!abc)def/
Back-references	サポートしません	遡及参照：　/.*?<\/[hH]\1/s
Conditional references	サポートしません	/(?(1)foo|bar)/

詳細な例は“正規表現式タイプ式“を参照してください

4.Int タイプ，集合：8 バイトの符号付き整数

詳細な例は“Int タイプ式“を参照してください

5. IPv 6 ルールを設定するには String タイプを使用して、**IPv 4 のみ**をサポートしている IP タイプ

(1). IPv 4 ワード字面表記は、ポイント 10 進法とポイント 16 進法、およびそれらの混合（wiki-IPv 4）、10 進法と 16 進法のデジタル IP も限定的にサポートされています。例えば、合法的な IPv 4 ワード字面値:

書式	値	IP 範囲（セグメント/サブネット）の書き込みに使用できるかどうか
点分 10 進法	192.0.2.235	是
点分 16 進法	0xC0.0x00.0x2.0xeB	是
混用	192.0.0x2.235	是
16 進法	0xC00002EB	非
10 進法	3221226219	非

(2). IP 範囲（セグメント/サブネット）

IP 範囲（セグメント / サブネット）は、左閉じ右閉じの IP 区間を表す。

すべての合法的な形式	コメント
192.168.1.0-192.168.1.255	IPv4 範囲，　普通
192.168.1.0/24	IPv4 サブネット，　普通
192.168.0x01.0-192.168.1.255	
192.168.0x01.0-192.168.1.0xff	
192.168.0x01.0/24	

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

192.168.0x01.0/0x18	

詳細な例は“IP タイプ式“を参照してください

タイプメンバー関数

String タイプメンバー関数

関数名	例	説明
find	payload.find('HTTP 1.')	固定フィーチャー列の一致。親列に変更特徴列がある場合、式の値は true、逆は false
find	payload.find(/[hc]at<\/tag>/i)	正規表現式バージョンの一致。特に、payload[2,10].find(/a[0-9]*c/)はパケット全体を a[0-9]*c を検索し、「c」の落下点が payload の[2、10]区間にあることを保証し、「a」が payload に現れなくても

Int タイプメンバー関数

関数名	例	説明
findpos	payload.findpos('ABC')	親列 payload における特徴列'ABC'のオフセット値を返します。オフセット値は 0 から開始します。親ストリングに特徴ストリングが存在しない場合、その論理式の値は例外です。findpos()の照合値は 0 未満にすることはできません
N2H16	payload.N2H16()	payload の最初の 2 バイトを返すネットワーク順序は、小端バイト順序の正の整数に変換される

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

N2H32	payload[30,100].N2H32()	親ストリングの最初の 4 バイトを返すネットワーク順序は、小端バイト順序の正の整数に変換される
N2H64	payload.N2H64()	親ストリングの最初の 8 バイトを返すネットワーク順序は、小端バイト順序の正の整数に変換される
isnull	!payload.isnull()	isnull は常に論理演算子「! 」一緒に使用します。戻り値が NULL でないことを示します。
length	payload.length() > 10	length は、リレーショナル演算子">", "<", ">=", "<=", "! ="などとともに使用され、フィールド値の長さ範囲に一致する内容を返すことを示します。
U8	payload.U8 > 10	payload の前のバイトを比較する
U16	payload.U16() > 10	payload の最初の 2 バイトを比較する
U32	payload.U32() > 10	payload の最初の 4 バイトを比較する
U64	payload.U64() > 10	payload の最初の 8 バイトを比較する

IP タイプメンバー関数

関数名	例	説明
in	srcip.in(192.168.1.0-192.168.1.30)	srcip が連続する IP 範囲に属しているかどうかを判断する
in	dstip.in(192.168.1.1/24)	dstip がある IP サブネットに属しているかどうかを判断する
in	srcip.in('192.168.9.2,192.168.1.0-192.168.1.30,192.168.10.1/24')	srcip が集合に属しているかどうかを判断し、集合内の各要素間をカンマで区切る

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

オペレータ（演算子、修飾子など）

算術演算子+-などはしばらく提供されません

オペレータタイプ	説明
Relation	関係演算子
Logic	ロジック演算子
Grouping	グループ化演算子
modifier	修飾子

優先度：Grouping > Modifier > Relation > Logic

1. 関係演算子

関係演算子	説明
=	等しい
<	より小さい
>	より大きい
!=	等しくない
>=	以上
<=	以下
+	加算
-	減算
*	乗算
/	除算
%	余剰を求める
>>	左へ移動

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

>>	右へ移動
&	ビットと
^	ビット別
|	ビットまたは
~	はんてん

2. ロジック演算子

ロジック演算子	説明	優先度	方向
! not	非	高	右から左へ
&& and	と	中	左から右へ
|| or	または	低	左から右へ

3.分组控制符

グループ化演算子	説明	優先度	例
()	グループ	最高	例：!(bool_expr1||bool_expr2); (bool_expr1||bool_expr2) && bool_expr3 など

4. 修飾子

修饰符	説明	説明/例
()	関数呼び出し	find()
[a, b]	文字列境界修飾子。a、b は、すべて整数型である所望の最大境界を示すために使用される。	String 式では、SubString が得られます。SubString は境界修飾の使用を禁止します

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

.	メンバー・アクセス	HTTP.url ; payload.find('str')
.	タイプに使用される字面値	192.168.0.1
"	String ワード字面修飾	空の文字列"の文字面値は許可されていません。エスケープは許可されていません
HEX"	16 進数文字列接頭辞修飾、単引用符のみサポート、HEX と最初の単引用符'の間に他の文字の存在を許可しない	一重引用符の内部大文字と小文字の両方が可能で、大文字と小文字の混用を許可します。ただし、バイトとバイトの間は空白文字で区切らなければならず、シングルバイトの幅は 2 で、幅はゼロ（0）を補う必要がありません。連続する複数の空白文字を分割として許可する
/pattern/modifiers	正規表現式	modifiers はデフォルトであり、正規表現は find()でのみ使用できます

境界修飾子［a，b］についての補足説明:

• a は左境界、b は右境界を望む。［a，b］は左閉じ右開きの区間を示す。

• 値域:　a, b ∈ { -2147483648, ..., -2, -1, 0, 1, 2, ..., 2147483647 }。

• a < b，且 a × b >= 0 厳格に成立する。

親ストリング'helloworld'の場合は、次の 2 つだけです:

(1) 0 <= a < b:

	0	1	2	3	4	5	6	7	8	9	10
	h	e	l	l	o	w	o	r	l	d	

(2) a < b <= 0:

-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0

例の［1，4］は「ell」、［−4，0］は「orld」になります

所望の境界であるため［1，200］は「elloworld」を得る

例では、「hellowod」を[200,300]で修飾すると、例外ストリング nullstr が得られます。

• 値取り戦略: 文字列と範囲修飾の間、交差があれば交差をとり、交差がなければ異常列 nullstr を得る。

0 の長い空の列を修飾すると異常な列が得られます;

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

異常列を修飾しても異常列が得られます;

• a デフォルト：左端境界、b デフォルト：最右境界、a と b は同時にデフォルトを許可しません。 [0，] は [，0] と等価であり、親列自体を表現するために使用することができる。

• 次の書き方はすべて合法:

[1, 2] , [1,] , [, -20] , [-10, -1] , [-10,] , [0,] , [, 0] , [, -1] , [, 10]

メタデータフィールド

メタデータフィールドの 2 つの書き方:

1.一般形式：データソース.フィールド

2. 組み込みグローバルフィールドの書き方：フィールド

組み込みメタデータフィールド	説明
packet	データパッケージ
capturelength	パケット取得長さ
packetlength	パケット長さ
payload	TCP または UDP 負荷
payloadlength	負荷長さ
ip	IP アドレス
srcip	ソース IP
dstip	宛先 IP
port	ポート
srcport	ソースポート
dstport	宛先ポート
location	ホーム（技術交流版ではこのフィールドはサポートされていません）
srclocation	ソースエンドポイントホーム（技術交流版ではこのフィールドはサポートされていません）

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

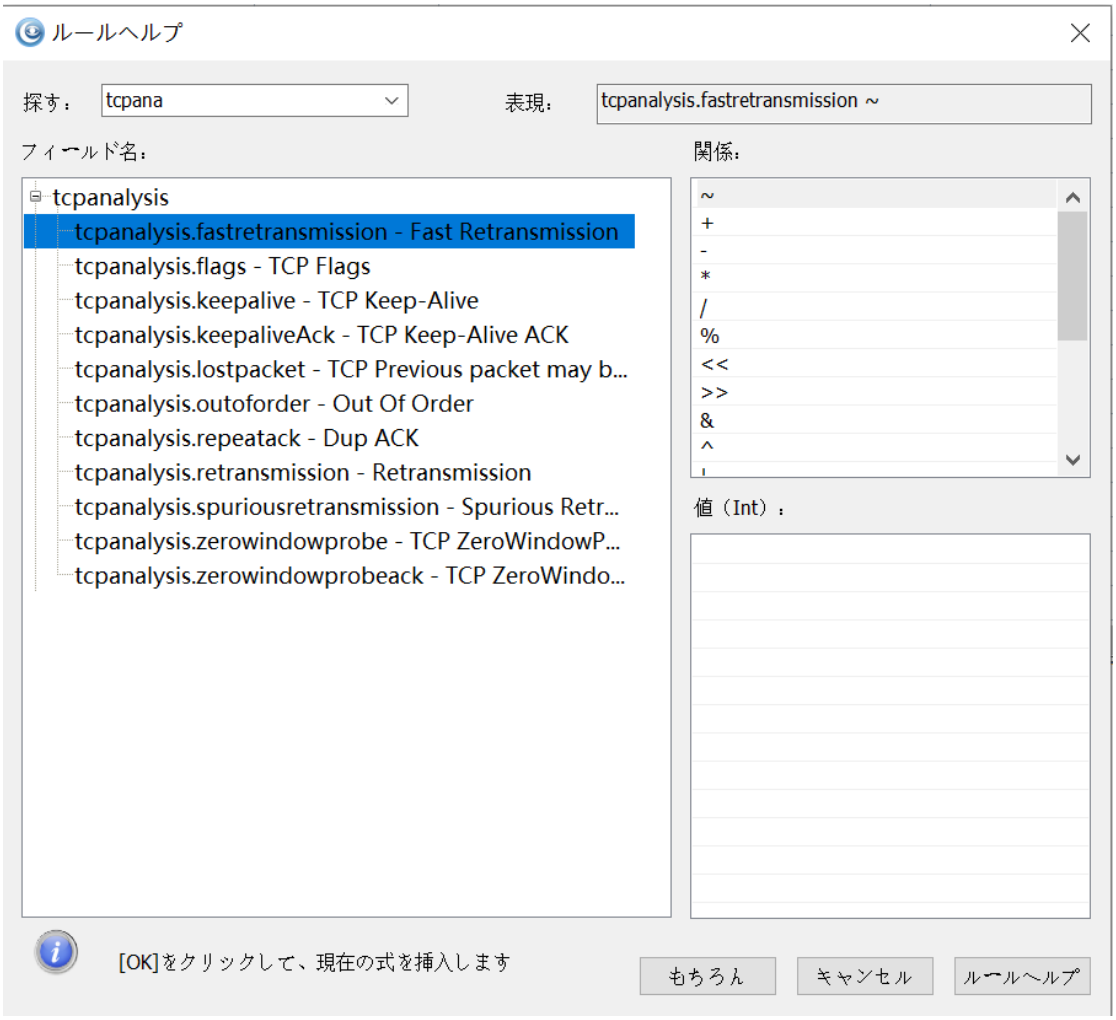
dstlocation	デスティネーションエンドポイント帰属地（技術交流版ではこのフィールドはサポートされていません）
protocol	プロトコル
protocolpath	プロトコルパス
timestamp	タイムスタンプ
alias	アドレス別名（物理アドレスと IP アドレスを含む）
srcalias	ソースアドレス別名（物理アドレスと IP アドレスを含む）
dstalias	宛先アドレス別名（物理アドレスと IP アドレスを含む）

組み込みフィールドでサポートされるオペレータとタイプメンバー関数

フィールド	データ型	サポートされるオペレータとタイプメンバー関数
packet / payload / protocolpath / location / srclocation / dstlocation / alias / srcalias / dstalias	String	[a, b] . = != String タイプメンバー関数と Int タイプメンバー関数
capturelength / packetlength / payloadlength / port / srcport / dstport / timestamp / protocol	Int	すべての関係演算子 isnull
ip / srcip / dstip	IP	= != . IP タイプメンバー関数

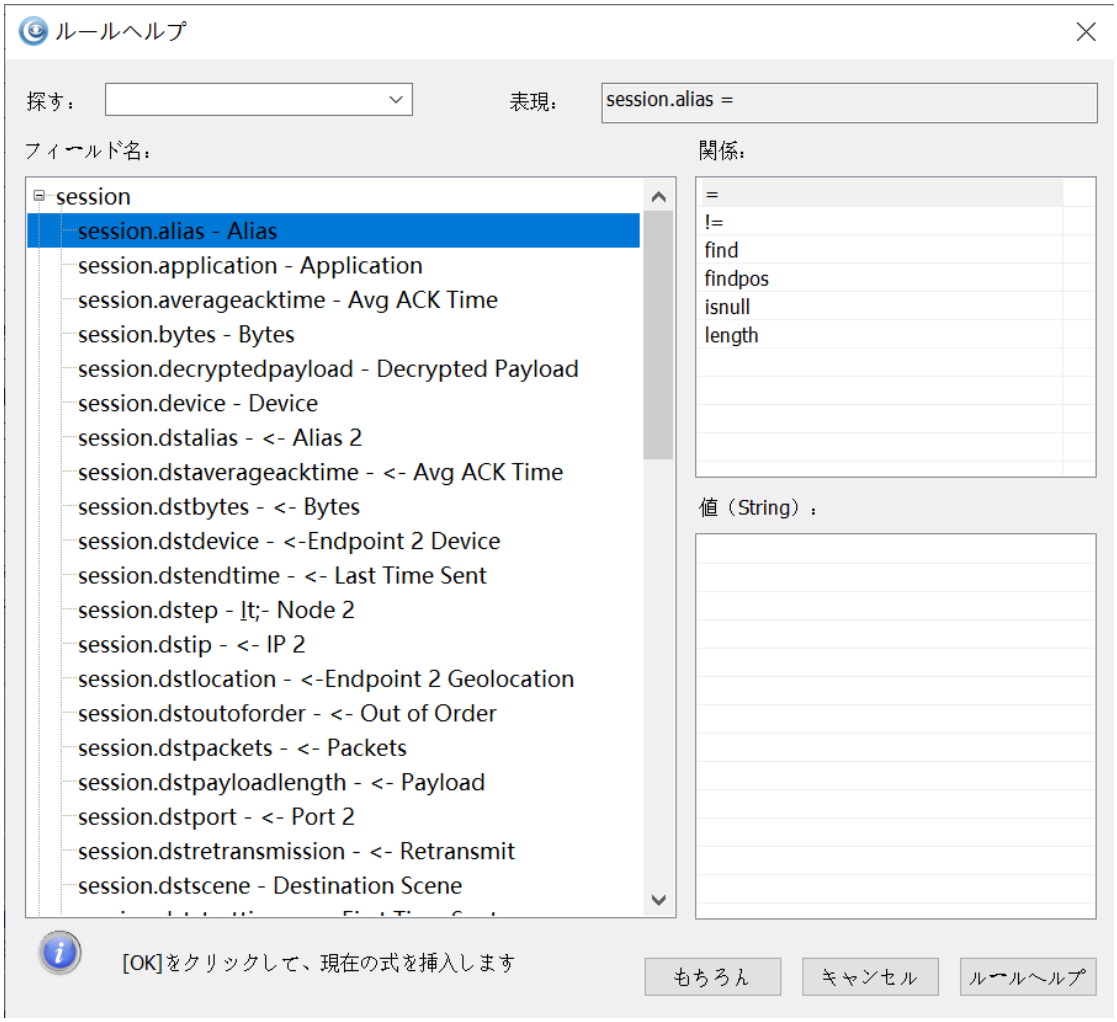
その中で、パケットビュー表示フィルタと分析フィルタはメタデータフィールドを含むのが少し異なり、表示フィルタは内蔵フィールド、プロトコルフィールドのほか、TCP 分析フィールド（tcpanalysis）を追加し、このフィールドはパケット分析後にのみ適用され、TCP 分析フィールドの具体的な内容は以下の図である

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



セッションビューの表示フィルタは**セッションフィールド（session）**のみで、このフィールドはセッションの統計データのみをフィルタリングします。詳細は次の図の通りです：

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



Note

セッションフィールドのバイト数関連フィールドと時間関連フィールドは、異なる精度のフィルタリングをサポートし、これらのフィールドはすべて int タイプフィールドであり、浮動小数点数の書き方はサポートされていません:

1. バイト数関連フィールド：**session.bytes**, **session.ep1bytes**, **session.ep2bytes**

バイトサイズの単位はデフォルトで **b(byte)** が使用され、**k/kb**，**m/mb**，**g/gb**，**t/tb** もサポートされています。例：session.bytes > 1024k と表すこともできる session.bytes > 1mb;

2. 時間関連フィールド：**session.duration**, **session.averageacktime**, **session.ep1averageacktime**, **session.ep2averageacktime**, **session.maxacktime**

時間の単位は**納秒（ns）**がデフォルトで使用され、**微秒（us）**，**毫秒（ms）**，**秒（s）**，**分（m）**，**时（h）**もサポートされています。例:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

session.duration > 60s と書くこともできる session.duration > 1m;
3.String タイプフィールド：**session.payload**， **session.payload，session.uncompressedpayload，session.decryptedpayload は、session.payload** は TCP と UDP のセッション内容フィルタリング、**session.uncompressedpayload** は HTTP セッションデータの解凍後のコンテンツフィルタリングであり。技術交流版では、上記のフィールドタイプのフィルタリングはサポートされていません。

計算中に発生した例外

ロジック式の計算中に例外が発生すると、そのロジック式の値も例外になります。異常状態は非真非偽の第 3 状態であり、多値ロジックでは非真すなわち偽ではない。原子ロジック式の計算値は、{true、false、abnormal}です。
例外的に関与する述語演算とロジック演算の規則は次の通りである（3 つの状態ブール、ここでは 3 つ目の状態を abnormal と規定する）：
1. abnormal オペランドが関与する述語演算では、その論理式の結果は abnormal である。すべての関係比較を含む:=!=>>=<=。
2. abnormal との論理的または演算（｜｜）は、true との演算結果のみ true であり、その他は abnormal である。
3. abnormal との論理と演算（&&）、false との演算結果のみ false であり、その他は abnormal である。
4. abnormal の論理非動作（！）、その結果はまだ abnormal である。

原子論理式の命中の定義とは、その原子論理式の値が true であること、ルール・ヒットの定義は、ルールの値が true であることです。

異常を引き起こす可能性がある場合の例:
1. String の範囲修飾は交差境界がないため、オペランドが例外列 nullstr になります。
2. グローバルデータソースには特別なフィールド payload があり、その長さが 0（payloadlength＝0）の場合、payload は異常列 nullstr であり、その直観的意味では「負荷がない」。ただし、長さが 0 の String フィールドがすべて例外列であるわけではありません。このフィールドの登録ポリシーによって異なります。
3. 内蔵された findpos 関数は、特徴列が見つからない場合に異常を引き起こす。ルール StringOperand.findpos('abc') < 20 || !（StringOperand.findpos('abc')<20）、StringOperand で'abc'が見つからな

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

い場合、ルールはヒットしません。
4. その他異常を誘発した場合。

15.2.3 式の例

String タイプ式

(1) payload の文字列「abcd」に一致する：payload.find('abcd')

(2) 検索内容を 16 進数で表し、payload 中の文字列「abcd」：
payload.find(HEX'61 62 63 64')

(3) 境界修飾子を使用してコンテンツを検索し、payload 内の文字列「abcd」に一致させる：
payload[2,50].find（「abcd」）は、payload オフセット 2～50 のデータのうち「abcd」に一致する
payload[,50].find（「abcd」）は、payload オフセット 0 から 50 のデータのうち「abcd」に一致する
payload[10,].find（「abcd」）は、payload オフセット 10 の開始におけるデータの「abcd」との一致する
payload[-10,-1].find（「abcd」）は、payload オフセットの最後から 10 番目から最後から 1 番目の部分のデータに「abcd」に一致する

(4) payload 中の文字列「abcd」に一致するオフセット位置が 10 より大きい：payload.findpos('abcd') > 10

(5) マッチングは http が存在しない.url フィールドのパケット：
http.url.isnull()

(6) マッチング payload 長が 100 を超えるもの：payload.length() > 100

(7) マッチング payload の最初のバイトは 10：payload.U8() > 10

DateTime タイプ式

timestamp = DT'2022-9-10 13:00:10'，一致するタイムスタンプが“2022-9-10 13:00:10”；
timestamp = DT'2022-9-10 13:00:10.981815000'，ナノ秒レベルのタイムスタンプ一致を表す；

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

timestamp = DT'2022-09-26 11:02:59+0900'，タイムゾーンを持つ秒レベルのタイムスタンプの一致を示します;+0900 は東九区時間、すなわち東京時間を表す;-0900 は西九区の時間を表し、0000 は UTC 時間を表し

正規表現式タイプ式

(1) payload 内の文字列「aBCd」に一致し、大文字と小文字が敏感ではない：payload.find(/aBCd/i)

(2) payload 内の文字列「ab c d」に一致し、大文字と小文字が敏感ではない：payload.find(/ab\\c\\d/i)

(3) payload の文字列「ab[任意の 1 文字]d」に一致：payload.find(/ab.d/s)

(4) payload の文字列「ab[任意の複数文字]d」に一致：payload.find(/ab.*d/s)

(5) payload の文字列「ab[任意の 1 文字]D」に一致し、大文字と小文字が敏感である：payload.find(/ab.D/is)

Int 类型表达式

payloadlength = 100；payloadlength > 100；payloadlength < 100；分别表示匹配 payloadlength 等于 100，大于 100，小于 100

IP タイプ式

(1) 単一 ip に一致：ip = 192.168.9.12

(2) IP 範囲に一致：ip.in(192.168.9.1-192.168.9.15)

(3) IP サブネットに一致：ip.in(192.168.1.1/24)

(4) 集合内の IP に一致，集合内の要素は単一の ip、ip 範囲、ip サブネット：ip.in(192.168.9.20,192.168.9.1-192.168.9.15,192.168.1.1/24)

多値型式

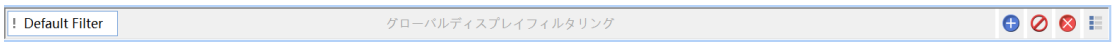
多値タイプが一致している場合、「! =」と「! 」は等しくありません。の結果は異なります。例:
ip != 192.168.9.12 与(srcip != 192.168.9.12 || dstip != 192.168.9.12)等しい;
!(ip=192.168.9.12)与(srcip != 192.168.9.12 && dstip != 192.168.9.12)等しい;

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

protocol != TCP 与 !(protocol = TCP) 等しくない
port != 80 与 !(port = 80) 等しくない
これは、パケットにおいて、ip はソース IP と宛先 IP を表し、port はソースポートと宛先ポートを表し、protocol はデータリンク層、トランスポート層、アプリケーション層などの異なる階層のプロトコルを表す。
現在、DPI Filter の多値タイプには、**ip、port、protocol、すべてのプロトコルのすべてのフィールド**があります。

15.3 グローバル表示フィルタ

グローバル表示フィルタは、すべての分析ビューの表示フィルタであり、グローバル表示フィルタが設定されていると、すべてのビューはグローバル表示フィルタのフィルタ条件を使用してデータ表示フィルタリングされます。次の図のようにフィルタインタフェースをグローバルに表示します:



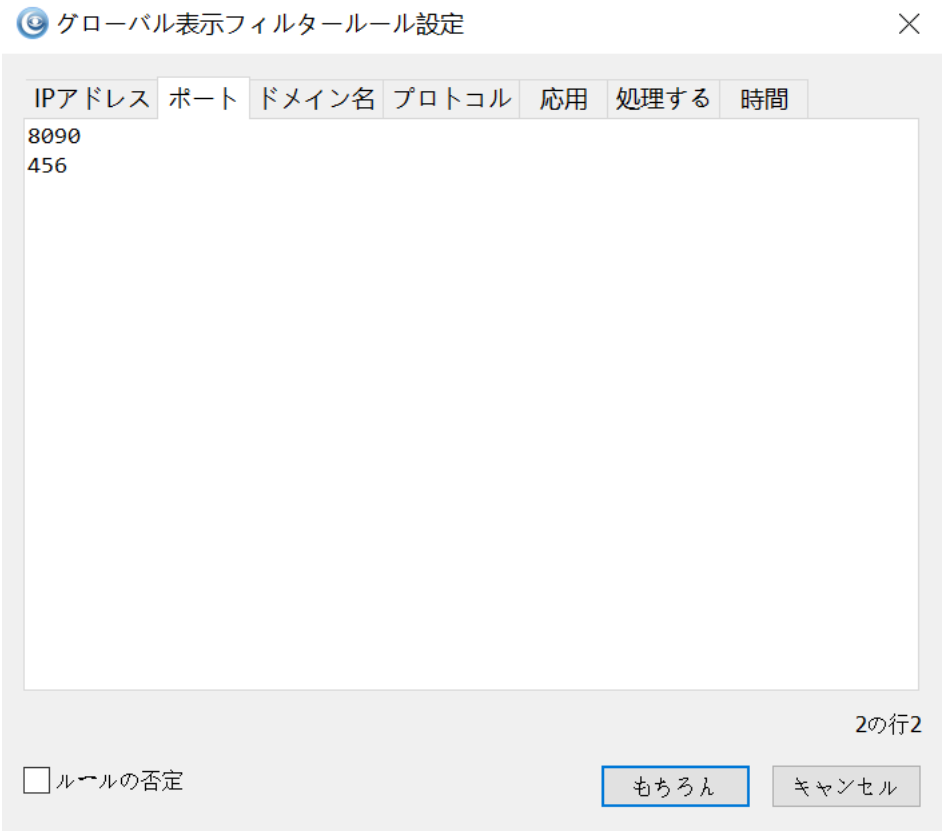
グローバル表示フィルタの追加

分析インタフェースで  ボタンをクリックするか、ショートカット **Alt+G** を使用してグローバル表示フィルタ設定ウィンドウを開くことができます。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

ポートの追加

フィルタ編集画面でポート Tab をクリックし、編集ボックスにフィルタリングが必要なポートを入力します。各行に 1 つのポート、複数のポートを改行して入力します。構成インタフェースは次のとおりです:



ドメイン名の追加

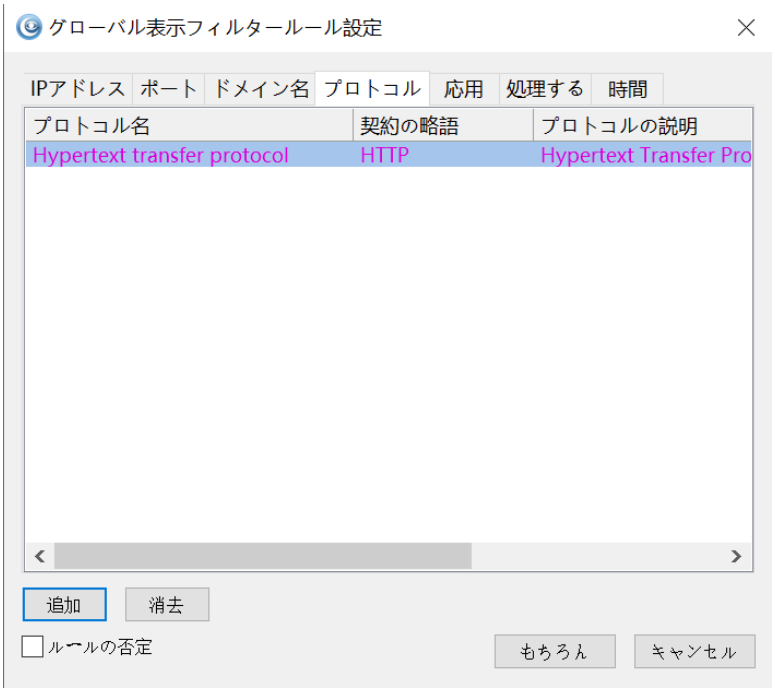
フィルタ編集画面でポート Tab をクリックし、編集ボックスにフィルタリングが必要なポートを入力します。各行に 1 つのポート、複数のポートを改行して入力します。

プロトコルの追加

フィルタ編集画面でプロトコル Tab をクリックし、下にある追加ボタンをクリックして、ポップアップダイアログボックスでフィルタリングが必要なプロトコルを選択します。プロトコルが必要でない場合は、削除するプロトコルを選択し、削除ボタンをクリックします。

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

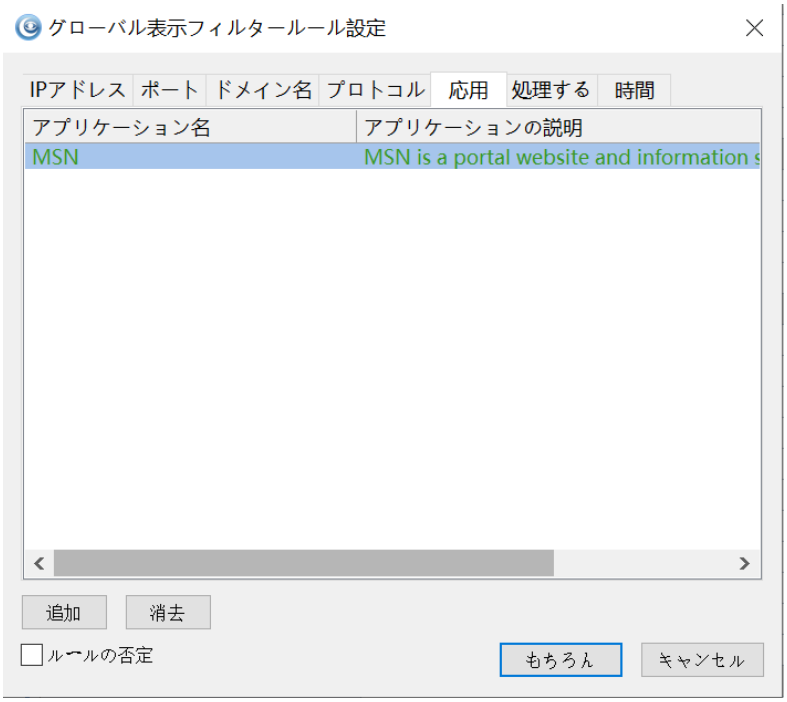
構成インタフェースは次のとおりです:



アプリケーションの追加

フィルタ編集画面でアプリケーション Tab をクリックし、下の追加ボタンをクリックして、ポップアップダイアログボックスでフィルタリングが必要なアプリケーションを選択します。アプリケーションが必要でない場合は、削除するアプリケーションを選択し、削除ボタンをクリックすればよい。

構成インタフェースは次のとおりです:



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

プロセスの追加

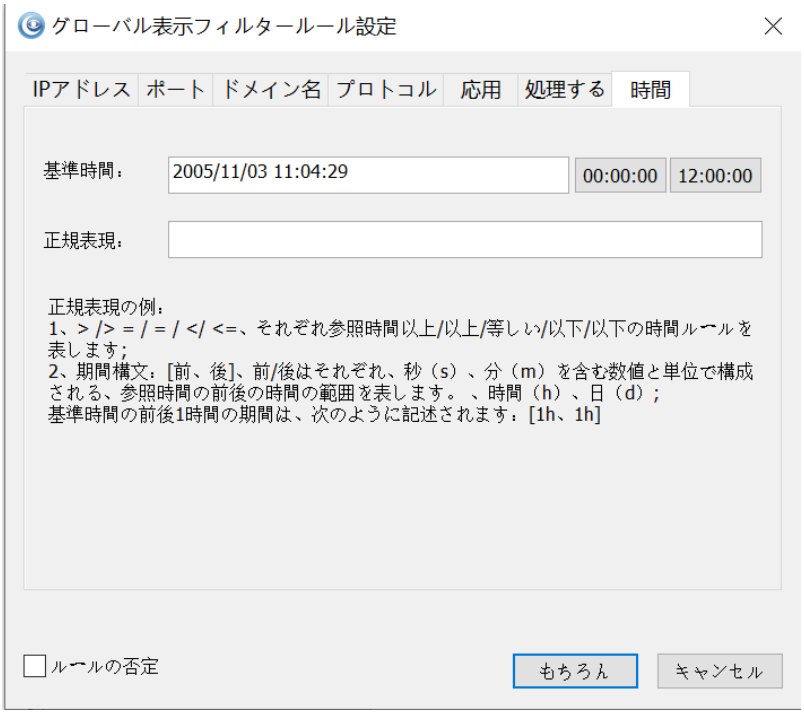
フィルタ編集画面でプロセス Tab をクリックし、下にある追加ボタンをクリックし、ポップアップダイアログボックスにアプリケーションの exe ファイルパスとプロセス ID を配置します。プロセスが必要でない場合は、削除するプロセスを選択し、削除ボタンをクリックします。

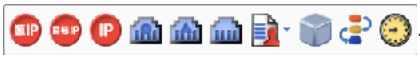
構成インタフェースは次のとおりです:

タイムスタンプの追加

フィルタ編集画面で時間 Tab をクリックし、画面に基準時間を入力し、ルール式に具体的なルールを記入する（ルール表記は下の例を参照）。構成インタフェースは次のとおりです:

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。



各分析ビューの右クリックメニューで、現在のビューに追加可能なグローバル表示フィルタ条件がある場合に表示されます。ツールバーの上にある対応する  アイコンをクリックすると、現在選択されているアイテムのデータをグローバル表示フィルタとしてすばやく追加できます。ツールバーのアイコンは、それぞれソース IP アドレス、ターゲット IP アドレス、ソース IP アドレス、ターゲット IP アドレス、ソースポート、ターゲットポート、ソースポート、ターゲットポート、プロトコル、アプリケーション、プロセス、タイムスタンプを表します。

フィルタ条件を設定すると、グローバル表示フィルタインタフェースにすべてのフィルタラベルが表示され、ラベルを選択するとフィルタが実行されます。複数のフィルタを選択する必要がある場合は、Ctrl+マウスの左ボタンを使用すると、選択したフィルタラベルがハイライト表示されます。下図に示すように：

グローバル表示フィルタの削除

フィルタを削除したい場合は、フィルタラベルの「x」をクリックして削除するか、グローバル表示フィルタ管理インタフェースに入って削除することができ

著作権所有© 2022 Colasoft Japan. すべての権利を留保します。

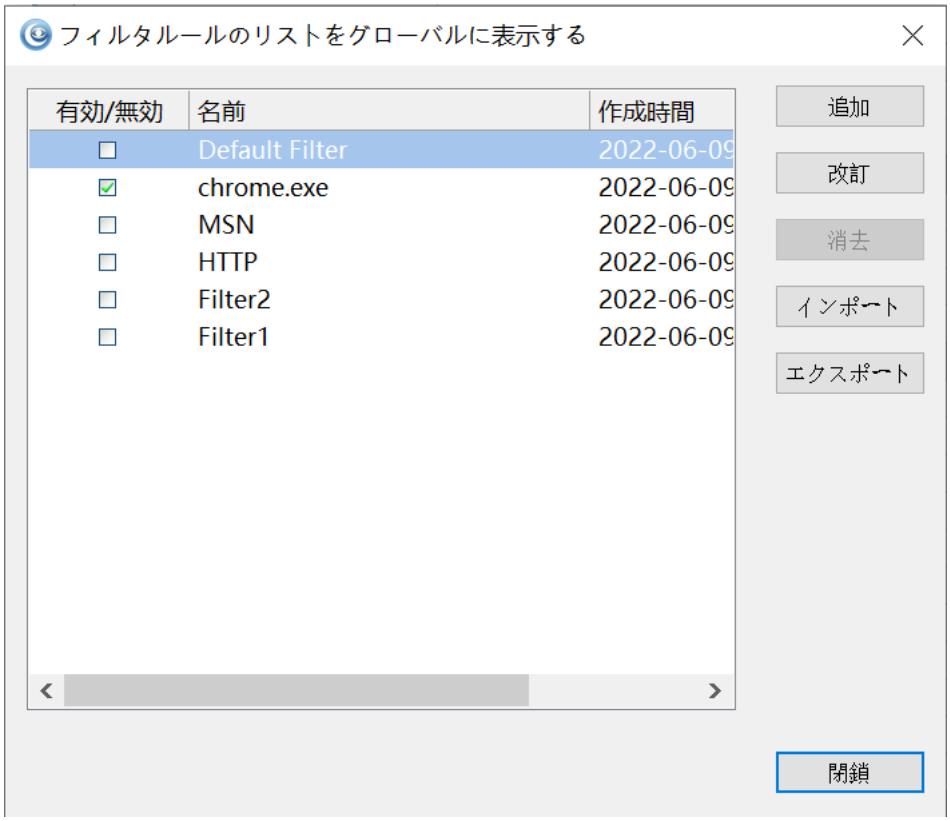
ます。分析画面で  ボタンをクリックすると、すべてのフィルタが削除されます。

グローバル表示フィルタを無効にする

グローバル表示フィルタ機能を無効にしたい場合は、ハイライトされたフィルタラベルをクリックするか、グローバル表示フィルタ管理インタフェースに入ってチェックされたフィルタを除去することができます。解析インタフェースで  ボタンをクリックすると、すべてのフィルタが無効になります。

グローバル表示フィルタ管理

分析インタフェースで  ボタンをクリックしてグローバル表示フィルタ管理インタフェースを開くことができます。管理インタフェースですべてのグローバル表示フィルタを追加、削除、変更、インポート、エクスポート、選択などの操作を行うことができます。インタフェースは以下の通りです:



著作権所有© 2022 Colasoft Japan. すべての権利を留保します。