

nChronos

Network Forensic Analysis Application

ユーザーガイド

(nChronos 5.0)



著作権所有© 2015 Colasoft LLC. 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

090-7197-9436

Sales

sales.jp@colasoft.com

技術サポート

support.jp@colasoft.com

ウェブサイト

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

目次

はじめに	1
概要	3
nChronos について	3
アーキテクチャー	3
デプロイメント	4
インストール、アクティベーションとアンインストール	8
nChronos サーバーをインストール	8
インストール準備	8
OS RAID パーティション	8
OS をインストール	10
自動インストール手順	10
手動インストール手順	11
nChronos コンソールをインストール	11
nChronos コンソールをアクティブ化	16
オンラインでアクティブ化	17
ライセンスファイルでアクティブ化	18
nChronos コンソールをアンインストール	19
サーバー設定	22
ブラウザからサーバーにログイン	22
ストレージ	23
インターフェース	24
インターフェースタイプの定義	25
キャプチャーインターフェースの設定	25
管理インターフェースの設定	26
ネットワークリンク	27
ライブラリー	30
解析センター	31
SMTP 設定	32
アラーム通知	33
レポート通知	34
ユーザーアカウント	35
デジタル証明書	37

セキュリティポリシー.....	38
監査ログ.....	39
時間同期.....	41
サーバー情報.....	42
サーバー管理.....	43
コンソールユーザーインターフェース	44
メニューバー.....	44
サーバーエクスプローラ	45
スタートページ.....	46
nChronos サーバーの追加と接続	48
nChronos サーバーの追加.....	48
nChronos サーバーに接続.....	49
ネットワークリンクの設定.....	50
キャプチャーフィルター.....	51
シンプルなフィルター.....	52
高度なフィルター.....	55
ストレージフィルター.....	56
ネームテーブル.....	57
ネットワークセグメント.....	59
参考値.....	61
フィールド定義.....	62
解析設定.....	63
標準アプリケーションの追加.....	65
Web アプリケーションの追加.....	67
特徴アプリケーションの追加.....	70
アプリケーションアラーム.....	71
トランザクションアラーム.....	75
トラフィックアラーム.....	77
ミリ秒におけるトラフィックアラーム.....	80
E メールアラーム.....	84
ドメインアラーム.....	86
特徴アラーム.....	89
リンク解析.....	93
ミリ秒解析.....	94

アラーム.....	95
アプリケーションパフォーマンス解析.....	96
アプリケーショントランザクション解析.....	97
ネットワークリンクプロパティをエクスポート.....	97
ネットワークリンクプロパティをインポート.....	98
リンク解析.....	100
ネットワークリンクを遡及的に解析.....	100
リンク解析ウィンドウ.....	100
タイムウィンドウ.....	101
リンク解析のトレントチャート.....	103
解析ビュー.....	104
ツールバーとポップアップメニュー.....	104
概要ビュー.....	106
アプリケーションビュー.....	106
サービスアクセスビュー.....	108
物理アドレスビュー.....	110
物理セッションビュー.....	111
ポートビュー.....	112
ネットワークセグメントビュー.....	114
セグメント間統計ビュー.....	115
VLAN ビュー.....	117
MPLS VPN ビュー.....	118
IP アドレスビュー.....	120
IP セッションビュー.....	122
TCP セッションビュー.....	123
UDP セッションビュー.....	123
アラームビュー.....	124
マルチセグメント解析.....	125
概要解析.....	125
詳細解析.....	126
統計情報をエクスポート.....	127
パケットのダウンロード.....	128
エキスパートアナライザで解析.....	130
一時的なレポートを生成.....	131
統計ビューにおける高度なフィルター.....	132

リンクモニター	135
リアルタイムにネットワークリンクを監視	135
リンクモニターウィンドウ	135
リアルタイムデータパネル	136
トレンドチャートパネル	136
トップセグメントパネル	137
トップ内部ホストパネル	137
トップアプリケーションパネル	137
アラームパネル	138
マトリックスパネル	138
ミリ秒解析	139
タイムウィンドウ	139
概要ビュー	140
ミリ秒におけるトラフィックアラームビュー	140
レポート	141
インスタントレポート	141
システムレポート	143
ユーザー定義のレポート	144
レポートの作成	144
レポートの複製	147
スケジュールの管理	148
レポートをスケジュール	149
レポートモジュール	151
アラーム	152
アプリケーションモニター	153
アプリケーションを監視	153
トレンドチャートパネル	154
リアルタイムデータパネル	154
トップセグメントパネル	154
トップクライアントパネル	154
アラームパネル	154
マトリックスパネル	154

アプリケーション解析.....	156
アプリケーションパフォーマンスを解析.....	156
アプリケーションパフォーマンス解析におけるトレンドチャート.....	156
パフォーマンス解析ビュー.....	158
クライアントビュー.....	158
サーバービュー.....	159
ネットワークセグメントビュー.....	160
IPセッションビュー.....	161
TCPセッションビュー.....	161
パケットサイズ分布ビュー.....	162
アラームビュー.....	162
トランザクションの解析.....	164
クライアントビュー.....	164
サーバービュー.....	165
ネットワークセグメントビュー.....	165
トランザクションビュー.....	166
トランザクションログビュー.....	167
アラームビュー.....	168

はじめに

要約

このユーザーガイドは、nChronos の使用を案内するために作成されたものです。使用状況や難易度に応じて構成されているので、章によって読むことをお勧めします。

対象読者

このユーザーガイドは、すべての nChronos ユーザーを対象として、作成されたものです。

専門用語

このユーザーガイドでよく使用される専門用語は、表 1 に記載されています。

専門用語リスト 表 1

専門用語	説明
nChronos サーバー	nChronos の中核として、目標ネットワーク（ネットワークリンクとも呼ばれる）のトラフィックデータのキャプチャー、解析、または保存に役立ちます。そして、通信ポートを介して nChronos コンソールと通信します。サーバーとも呼ばれます。
nChronos コンソール	データプレゼンテーションプラットフォームとして、nChronos サーバーに接続し、ネットワークトラフィック状況を表示、および解析するためのさまざまな統計情報を提供します。また、遡及的解析、新たな解析とデータのドリルダウンをも提供します。コンソールとも呼ばれます。
解析オブジェクト	プロトコル、アドレス、ポート、セッション、アプリケーション、ホスト、ネットワークセグメント、目標ネットワーク、およびその他の要素を含むネットワーク要素です。
キャプチャーインターフェース	nChronos サーバー上のネットワークインターフェース/ポートで、一般にはミラーポートに接続されています。目標ネットワークトラフィックをキャプチャーします。
管理インターフェース	nChronos サーバー上のネットワークインターフェース/ポートで、一般的にはインターネット接続に使用されています。nChronos コンソールとサードパーティーアプリは、nChronos サーバーに接続して、統計情報と解析データを取得することができます。
ネットワークリンク	nChronos がネットワークトラフィックをキャプチャーし、統計と解析を行うためのネットワークオブジェクトです。

専門用語	説明
バックインタイム解析	遡及的解析とも呼ばれます。詳細な解析プレゼンテーション、データのドリルダウン、新たな解析およびネットワーク履歴データなどさまざまな統計情報が提供されています。
タイムウィンドウ	タイムウィンドウでは、4分、20分、1時間、4時間、および他の時間スパンを選択することができます。時間スパンが短い場合、少ないデータ量と細かいデータが提供されています。タイムウィンドウを使用することによって、ネットワークの履歴データを簡単に特定することができます。
フィルター	カスタムのフィルター条件或いはルールを設定して、指定されるデータを見つけ出します。
IPペア	IPアドレスをペアで表示しますが、送信元アドレスと宛先アドレスを区別しません。
ドリルダウン	アプリケーション、ネットワークセグメント、アドレスおよびセッションを含むネットワークオブジェクトに対するレベルごとの革新的な解析です。
エキスパートアナライザ	パケットレベルの解析システム。さまざまな選択されたネットワークオブジェクトの統計情報およびパケットのオリジナルデコード情報を提供します。
Webアプリケーション	URLベースのアプリケーションで、ホスト名、IPアドレス、ポート番号及ぶURLパラメータによって定義されます。
特徴アプリケーション	データフローの特徴によって、ASCII、Hex、UTF-8またはUTF-16で定義されるアプリケーションです。
パフォーマンス解析	アプリケーションのサービスパフォーマンスに対する解析です。

概要

この章では、アーキテクチャーとデプロイメントを含め、nChronos のことについて説明しています。

nChronos について

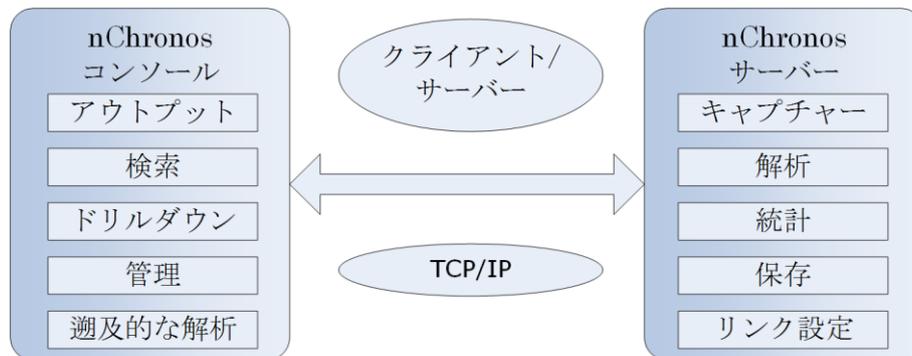
nChronos は nChronos サーバーと nChronos コンソールから構成されています。 nChronos サーバーは、nChronos の中核で、目標ネットワークパケットのキャプチャー、解析、および保存に役立ちます。 nChronos コンソールは、データのプレゼンテーションプラットフォームで、nChronos サーバーに接続して、プレゼンテーションのための統計情報やその他の解析データを取得することができます。データを表示するには、ユーザーはまず nChronos サーバーを設定して、nChronos サーバーをコンソールに接続する必要があります。

アーキテクチャー

nChronos サーバーは、少なくとも 2 つのネットワークインターフェースが含まれています。一つはキャプチャーインターフェースで、もう一つは管理インターフェースと呼ばれています。キャプチャーインターフェースを使って、nChronos サーバーは、スイッチまたはタップのミラーポートを介して目標ネットワーク上のすべてのパケットをキャプチャーします。そして、解析や保存のために、キャプチャーされたパケットを解析モジュールと統計モジュールに配達します。管理インターフェースを使用すると、nChronos サーバーは、LAN またはインターネットを介し nChronos コンソールと通信できます。

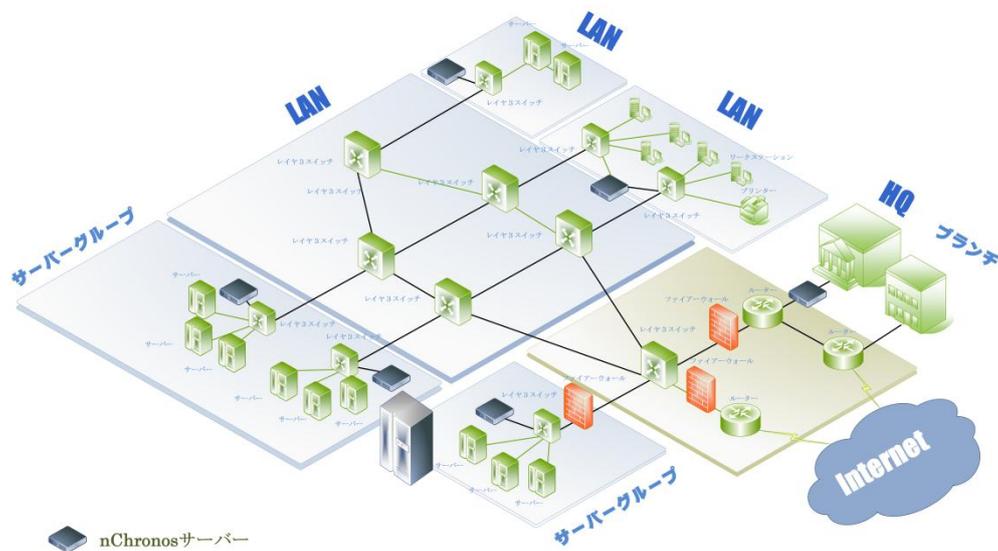
nChronos コンソールは C/S (クライアント/サーバー) 技術を利用して、nChronos サーバーと通信します。 nChronos コンソールはリアルタイムにネットワークリンクを監視する、解析ビューに統計情報を表示する、統計情報をエクスポートする、パケットをダウンロードする、ネットワークオブジェクトをドリルダウンする、および他の通信操作を実行する場合、リクエストコマンドをサーバーに送信します。そしてサーバーは、そのコマンドにレスポンスして、対応のデータを返します。さらに、nChronos コンソールと nChronos サーバーは、指定されたポート番号を通じ、TCP/IP プロトコルを使用してインターネットで通信を行います。

nChronos コンソールと nChronos サーバーの機能アーキテクチャーは下図のようです。



デプロイメント

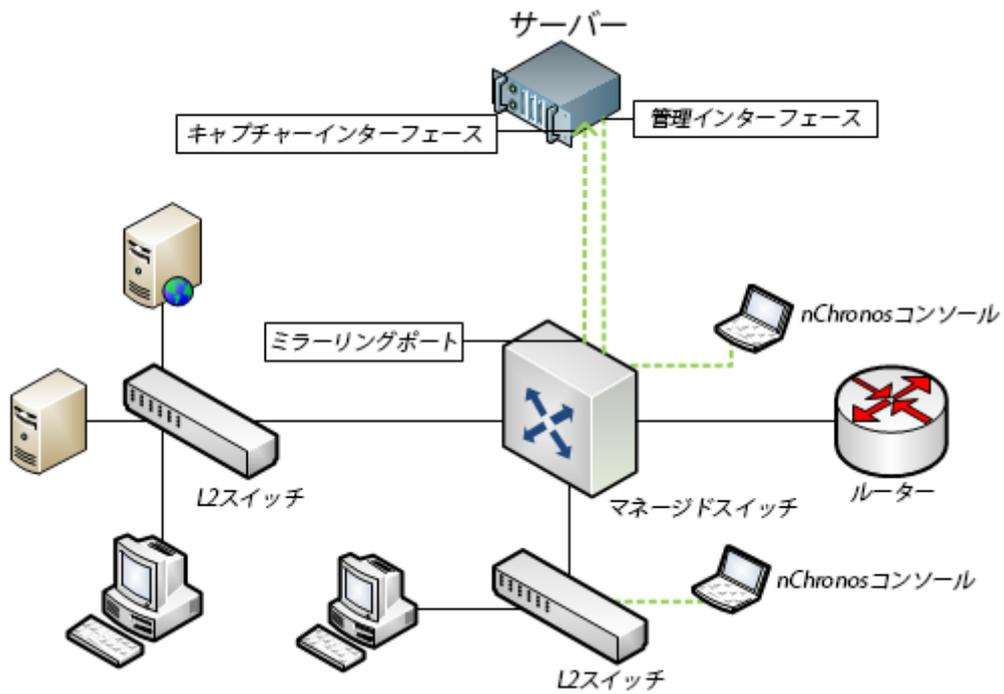
異なるネットワークと複数ネットワークリンクを持つネットワークでは、nChronos はローカルネットワークのネットワークデータをキャプチャーまたは保存するほかに、分散的デプロイメントとリモート監視をもサポートしています。重要なネットワークリンクの場合、複数の nChronos サーバーを配備することができ、ユーザーはデータ解析とネットワーク管理のため、いつでもどこでもリモート nChronos サーバーに接続することができます。さらに、nChronos コンソールを使用して、重要なネットワークリンクのトラフィックをリアルタイムに監視することができ、一旦異常が発生したら報告することもできます。nChronos のデプロイメントは、下図のようです。



トラフィックを効果的にキャプチャーするには、トラフィックソースはマネージドスイッチ、ハブ、及びタップを含む適切なネットワークデバイスから来る必要があります。ポートミラーリング/ SPAN 機能を利用して、パケットを監視ポートにコピーすることができるため、マネージドスイッチが最適です。この機能は、ポートミラーリング (Cisco は SPAN と呼んでいる) と呼ばれています。ポートミラーリングの詳細については、当社のウェブサイトにおける [Switch Management](#) をお読みください。

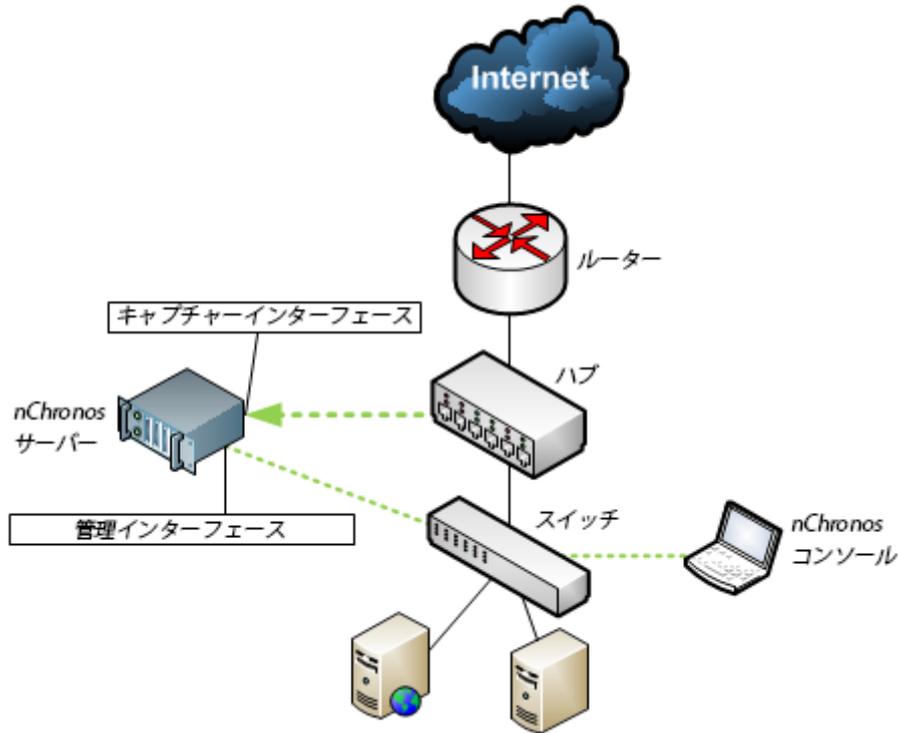
マネージドスイッチ

次の図は、ネットワークにおけるマネージドスイッチのついた、簡略化した nChronos デプロイメントを示しています。



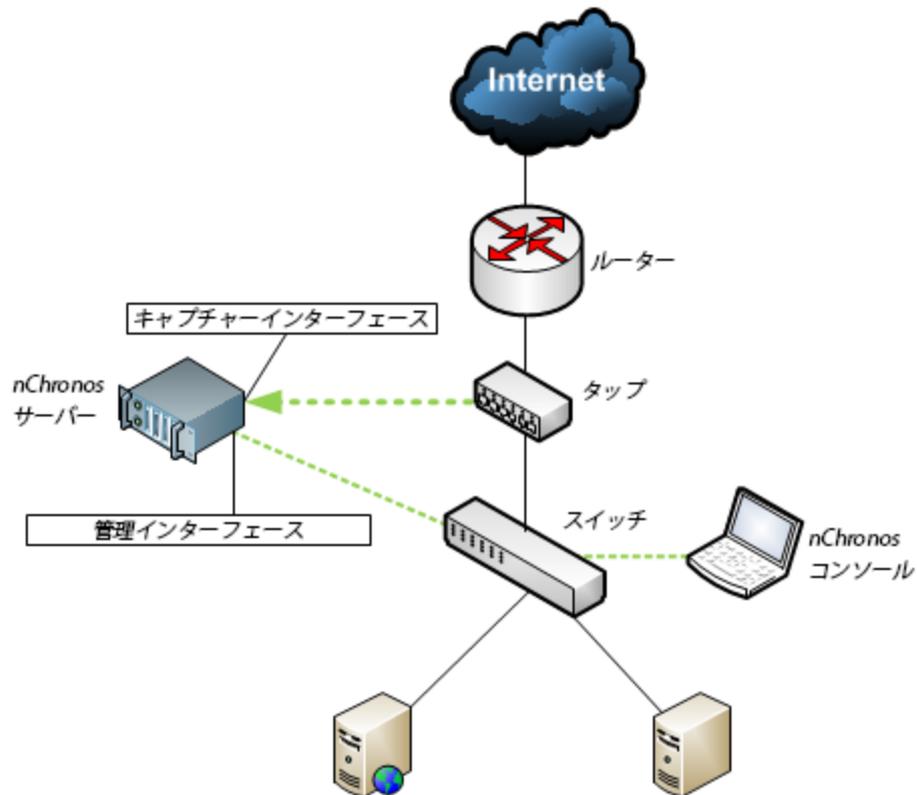
ハブ

マネージドスイッチがネットワークで使用できない場合は、トラフィックソースとしてハブを使用することができます。このようなネットワークでは、キャプチャーインターフェースがハブに接続されています。ハブが 100 Mbps のトラフィックしか処理できないことと、現代ネットワークに適していないことに注意してください。ネットワークトラフィックが少ない場合、ハブはまた経済的な選択です。次の図は、ネットワークにおけるハブのついた、簡略化した nChronos デプロイメントを示しています。



タップ

ハブを使用して、小規模なネットワークからのトラフィックをキャプチャするほかに、使用率の高いケーブルからのトラフィックをキャプチャするために、ネットワークタップは、より賢明な選択です。ネットワークタップは、マネージドスイッチのポートミラーリング機能で動作しています。その機能によって、すべてのパケットをコピーし、サーバーに送信することができます。次の図は、ネットワークにおけるタップのついた、簡略化した nChronos デプロイメントを示しています。



インストール、アクティベーションとアンインストール

この章では、nChronos サーバーとコンソールのインストール、アクティベーションとアンインストールを紹介します。

nChronos サーバーをインストール

nChronosサーバーはバージョン5.0からWindowsからLinuxに移行されます。正常な運行を確保するために、CentOS 6.6にインストールされ、OSが必要に応じてパーティションを設定する必要があります。以下のステップに従い、まずCentOS 6.6をインストールして、nChronosサーバー5.0をインストールします。

 **注意** インストールはもとのOSを上書きします。

インストール準備

nChronos サーバー5.0 をインストールする前に、以下の準備をする必要があります。

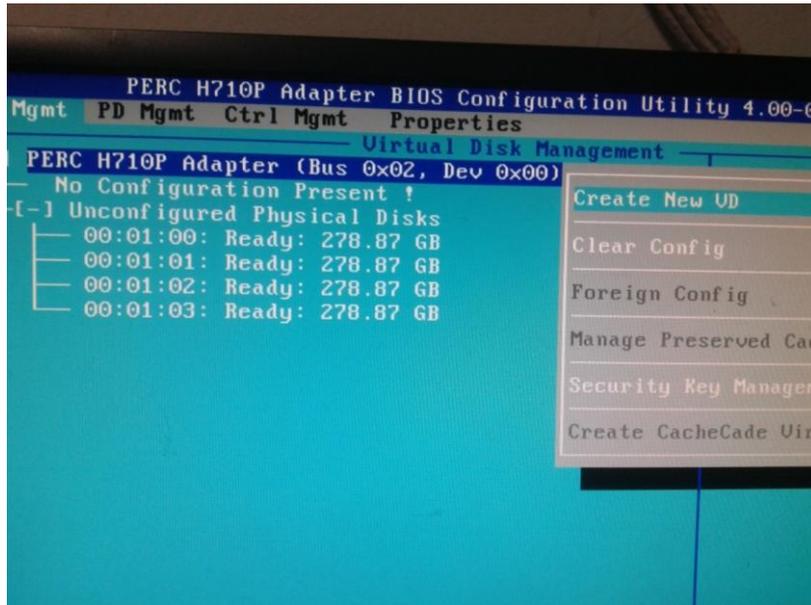
1. ColaOS 6.6 インストールディスク (CentOS 6.6)
2. nChronos サーバーインストールパッケージ: `csras.xxxx.rpm`、他の関連ソフトウェアインストールパッケージ: `lrzrz.xxx.rpm`、`xfsprogos.xxxx.rpm`、及び自動インストールスクリプト: `csrass_install_1.2.sh`
3. OS をインストールするには、二つの RAID パーティションが必要で、データパーティション `sdb` を `/data` にアップロードする必要があります。

OS RAID パーティション

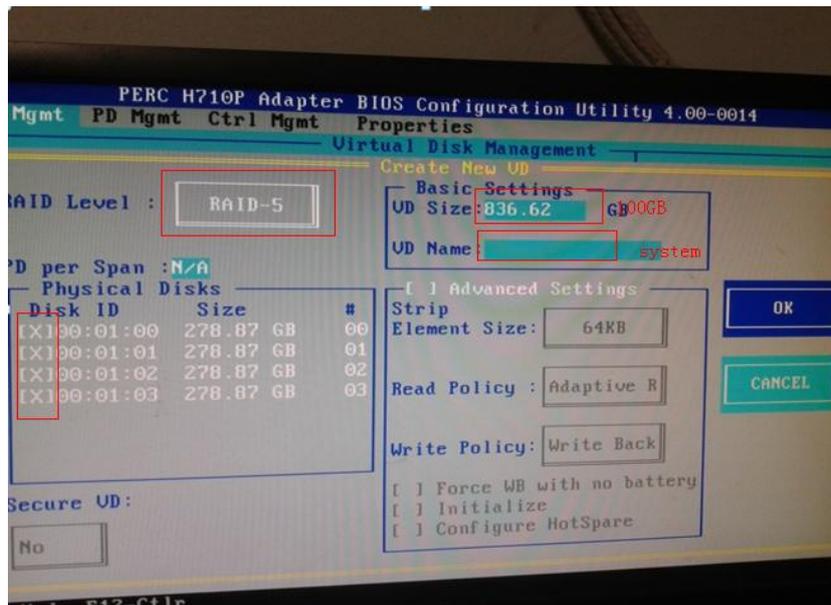
サーバーを起動する際、RAID カードのモデルにより、対応するショートカットキーをクリックすることで、RAID カード設定インターフェースに入ります。

PERC H710P を例とします。サーバーを起動する際、CTRL+R をくりっくして、RAID カード設定インターフェースに入ります。

F2 をクリックし、「Clear Config」を選択することで、デフォルトの設定情報を削除します。



- 1) 「Create New VD」を選択し、「RAID-5」を選択して、すべての物理ディスクにチェックを入れます。Tab キーで切り替えて、VD1 の「VD Size」を 60G に、「VD Name」を system に設定し、OK をクリックします。



- 2) Disk Group で VD2 を追加します。今回は物理ディスクにチェックを入れなくてもいいです。「RAID Level」に RAID-5 を選択し、残りのストレージスペースを選択して、「VD Name」を data に設定します。「Advanced Settings」を選択し、「Element Size」を 1 MB に設定し、OK をクリックします。
- 3) 二つのパーティションを初期化します。パーティションを選択し、F2 をクリックして、「Fast Init」をクリックすることで、クイック初期化します。
- 4) 設定が完了した後、サーバーを再起動します。

OS をインストール

ColaOS ディスクを利用して、OS をインストールするには、サーバーの起動プロセス中にスタートアップ項目を変更し、CD ドライバからサーバーを起動するのを選択する必要があります。そうすると、OS は自動的にインストールされます。（修正済みの ISO でするので、手動で操作する必要がありません。）インストールが完了されると、サーバーは再起動されず。最後にディスクを取り出す必要があります。そうしないと、古いサーバーの場合、OS を再インストールする可能性があります。

OS のインストールが完了した後、デフォルトで、ユーザー名は「root」で、パスワードは「!ColasoftL23」となります。デフォルトでイーサネットポートは eth0 で、IP アドレスは 192.168.5.160 となります。ユーザーはサーバーにログインし、「ethtool -p eth0 9」を入力することで、eth0 の位置を特定することができます。eth0 のランプは 9 秒点滅します。ランプの点滅する時間は必要に応じて設定できます。

自動インストール手順

1. SSH ツールを利用して、リモートでサーバーに接続し、下図のように RPM パッケージ、ソフトウェアインストールパッケージ、及び OS インストールスクリプトをサーバーにおける root という名前のファイルフォルダにアップロードします。

```
-rw-r--r-- 1 root root 58477252 Nov 12 10:24 nchronoss-5.0.2.2802.x86_64.rpm
-rwxr-xr-x 1 root root 5810 Sep 30 14:16 nchronoss_install_1.2.sh
```

2. 「chmod +x nchronoss_install_1.2.sh」を入力して、インストールスクリプトに実行権限を与えます。

```
[root@colasoft ~]# chmod +x nchronoss_install_1.2.sh
```

3. 「./nchronoss_install_1.2.sh」を入力して、スクリプトを実行します。

スクリプトの実行が終わると、インストールが完了します。インストールプロセス中、パッケージ紛失など問題が発生したら、エラーメッセージが出てきます。

```
network restart...
nchronoss file found...
Preparing... ##### [100%]
 1:nchronoss ##### [100%]
starting 'nchronoss' server: [ OK ]
nchronoss rpm installed !
All install completed...
*****
```

ユーザーはブラウザを利用して、サーバーウェブページにログインすることができます。

手動インストール手順

1. SSH ツールを利用して、リモートでサーバーに接続し、下図のように RPM パッケージ、ソフトウェアインストールパッケージなどをサーバーにおける root という名前のファイルフォルダにアップロードします。

```
-rw-r--r-- 1 root root 58477252 Nov 12 10:24 nchronoss-5.0.2.2802.x86_64.rpm
-rwxr-xr-x 1 root root 5810 Sep 30 14:16 nchronoss_install_1.2.sh
```

2. 「chmod +x nchronoss.5.0.2.xxx.rpm」というコマンドを入力して、権限を修正します。
3. 「mkdir /data」というコマンドを入力して、data という名前のファイルフォルダを追加します。
4. 「rpm -ivh nchronoss-5.0.2.xxx.x86_64.rpm」というコマンドを入力して、インストールします。

nChronos コンソールをインストール

システム要件

nChronos コンソールのシステム要件：

- Windows XP (SP3 以上)/Vista/7/8/Server 2003/Server 2008/Server 2012
- 4GB RAM
- Dual-core processor
- Internet Explorer 7.0

nChronos コンソールの推奨システム要件：

- 4-core processor
- 4GB RAM
- Independent network adapter
- Internet Explorer 8.0

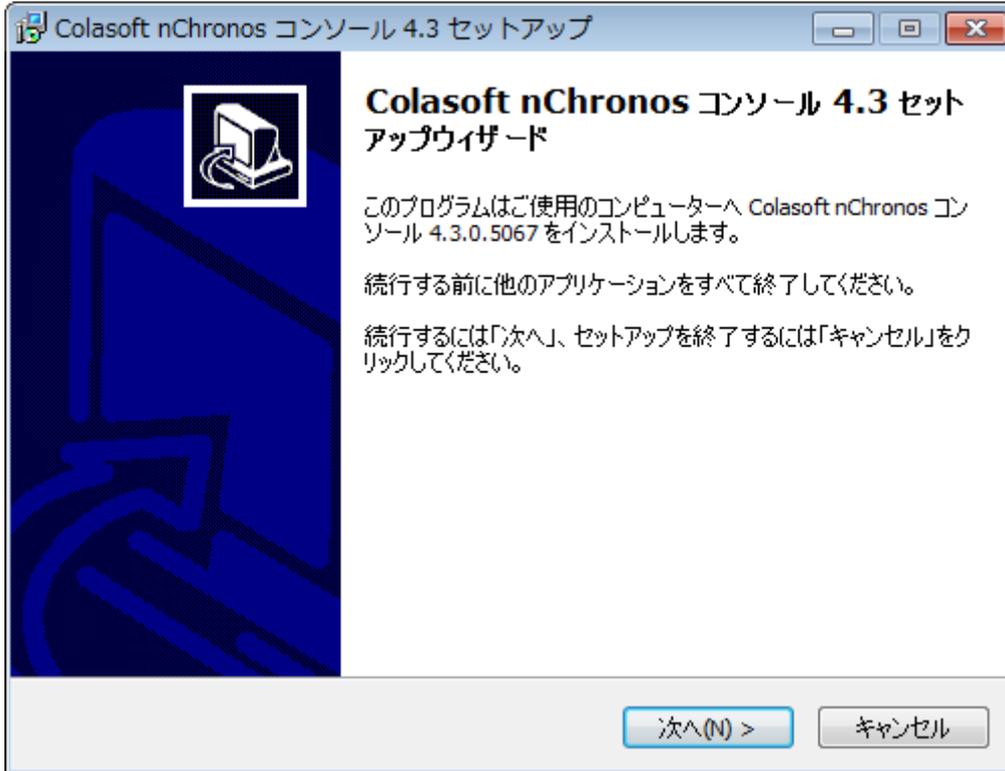
nChronos コンソールをインストール

nChronos コンソールをインストールする前に、以下のことをする必要があります：

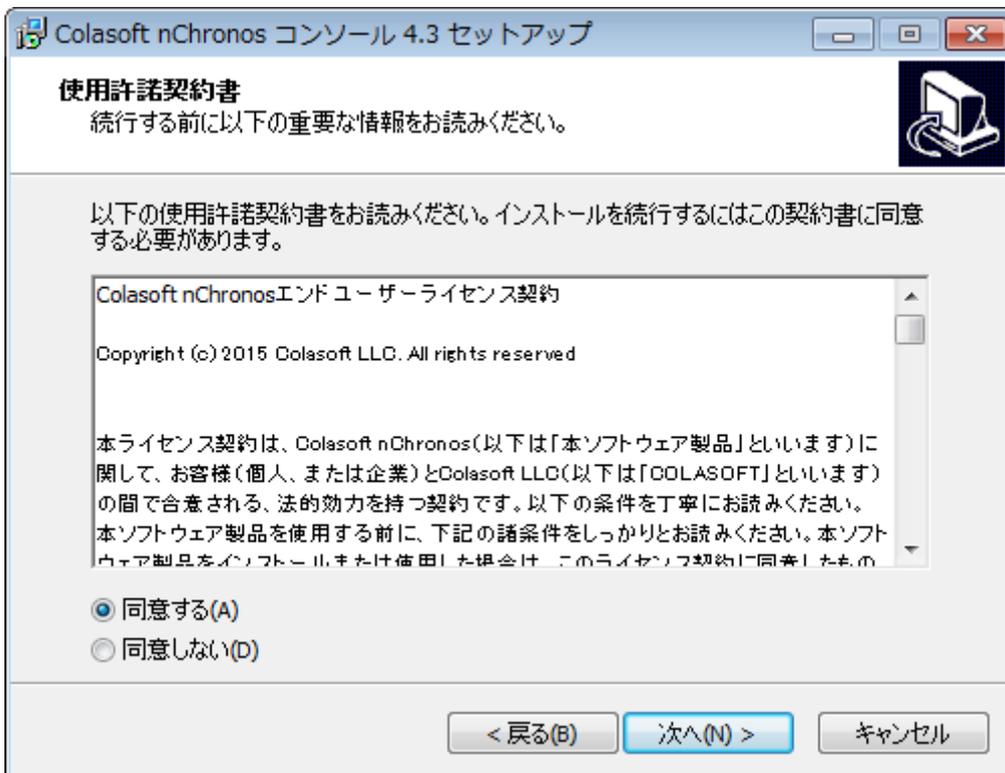
- お使いのマシンが最小システム要件を満たしていることを確認してください。
- お使いのマシンで実行中のすべてのアプリケーションを終了してください。
- 古いバージョン、または試用版の nChronos コンソールをアンインストールしてください。

コンソールをインストールするには、

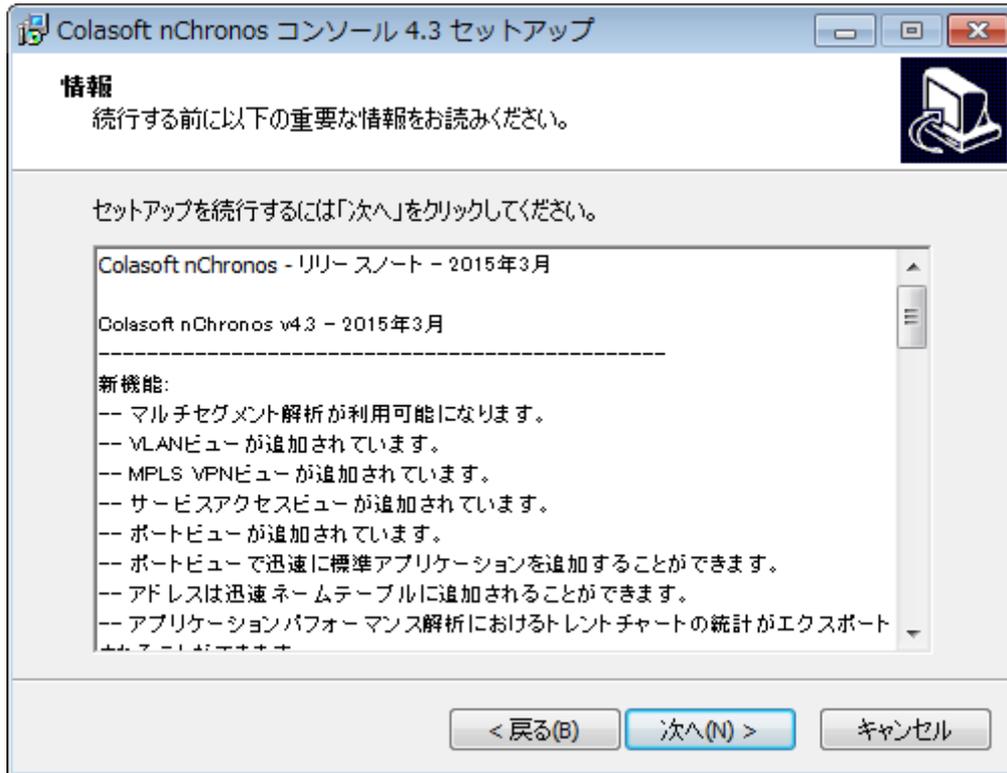
1. nChronos コンソールのインストールファイルをダブルクリックして、セットアップウィザードが下図のように、表示されます。



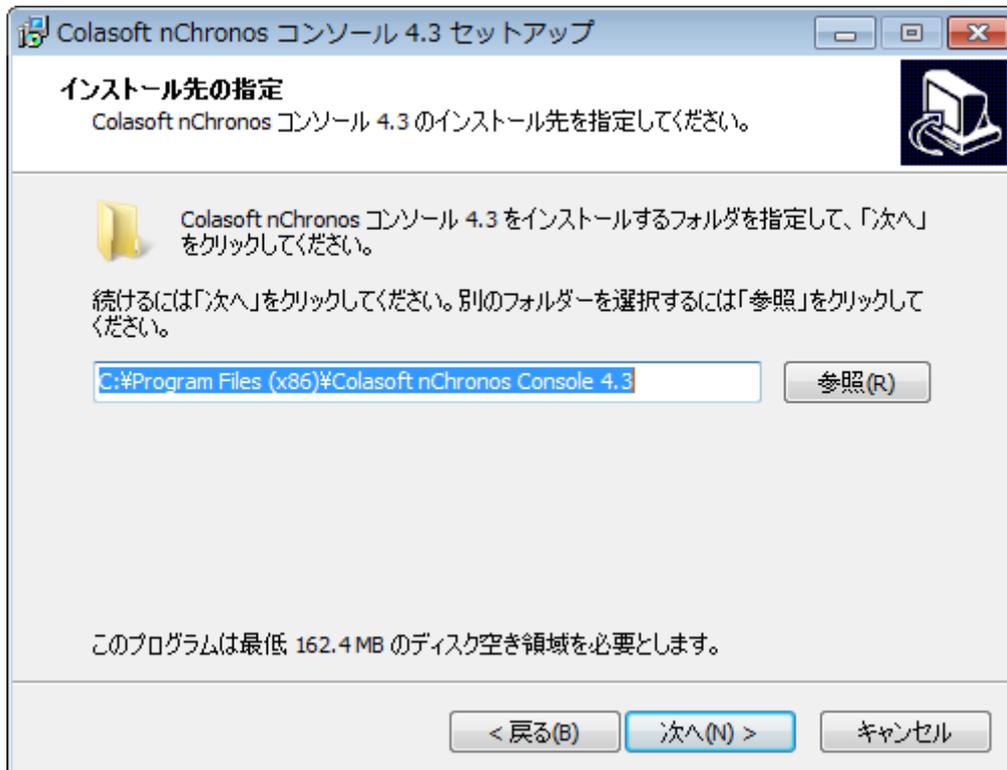
2. 「次へ」をクリックすることによって、下図のように使用許諾契約書ページが表示されます。使用許諾契約書を確認して、同意する場合、「同意する」にチェックを入れてください。



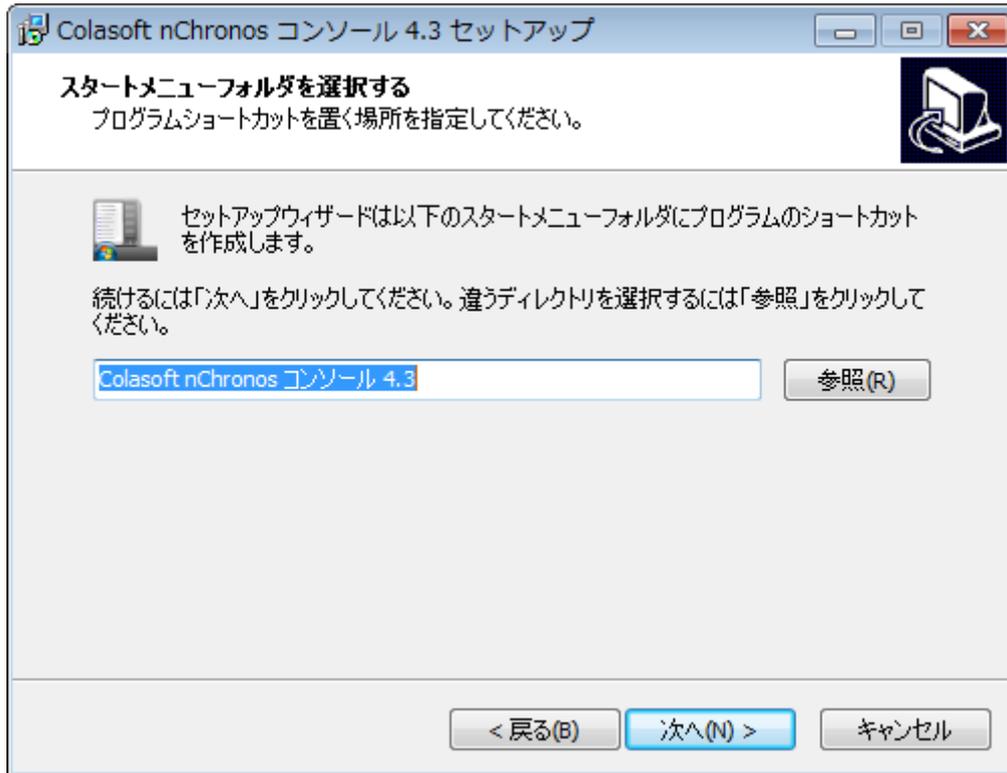
3. 「次へ」をクリックすることによって、下図のようにリリースノートが書いている nChronos 情報ページが表示されます。製品のアップデートを確認します。



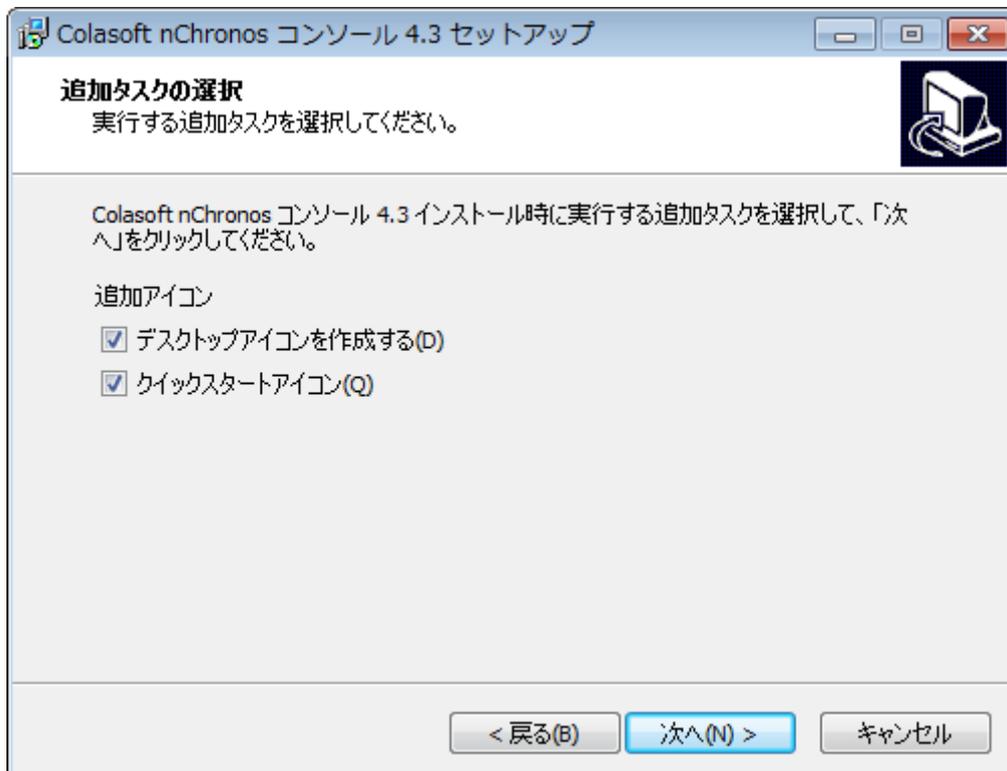
4. 「次へ」をクリックすることによって、インストール先を指定するページが表示されます。デフォルトでは、インストールディレクトリは C:\Program Files\Colasoft nChronos Console 5.0 となっています。ほかのディレクトリを指定するには、下図のように、インストールルートを入力するか、「参照」をクリックして、インストールフォルダを指定することができます。



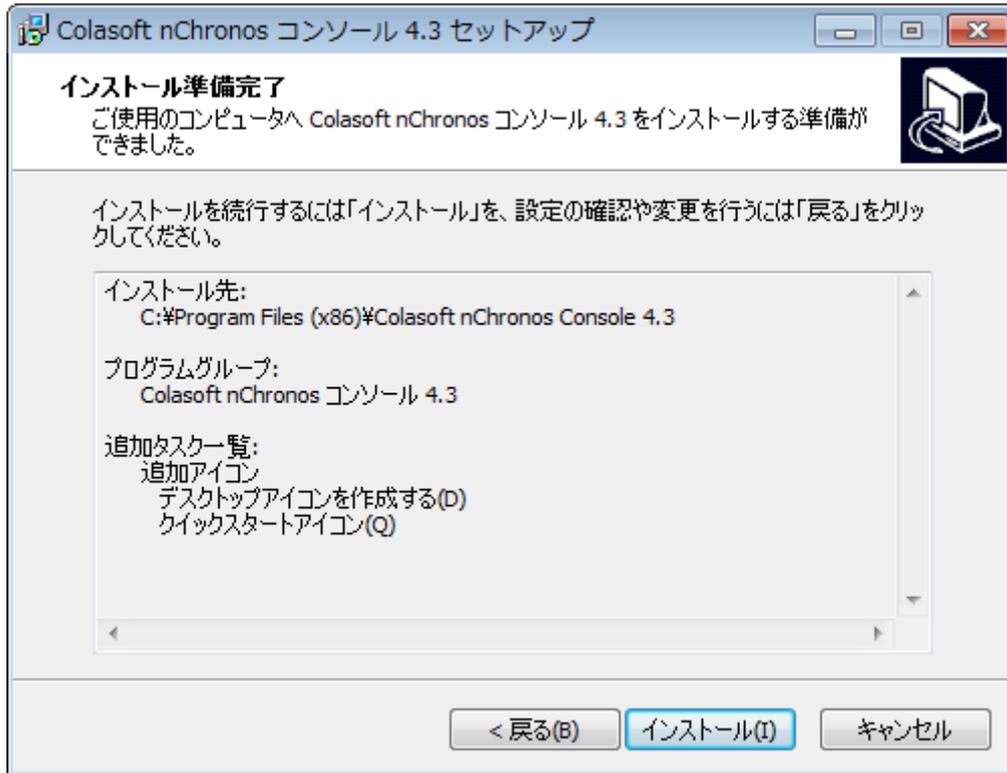
5. 「次へ」をクリックすることによって、下図のようにスタートメニューフォルダが表示されます。スタートメニューフォルダ名を指定します。



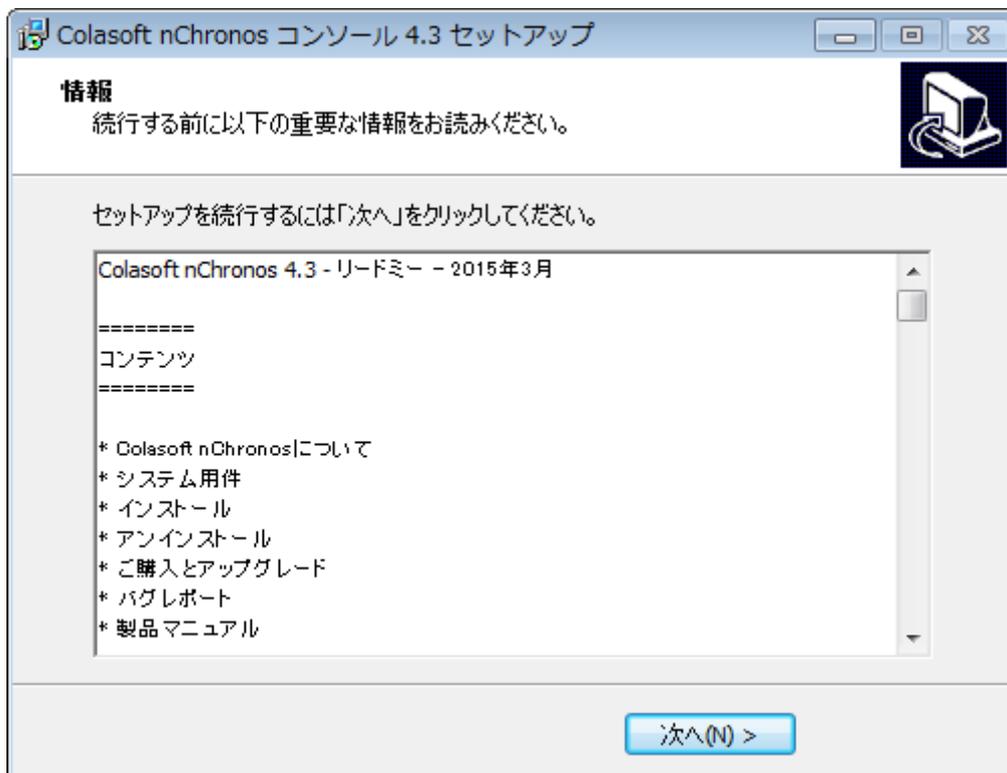
6. 「次へ」をクリックすることによって、追加タスクを選択するページが表示されま
す。下図のように、デスクトップアイコンとクイックスタートアイコンを作成する
かどうかを指定します。



7. 「次へ」をクリックすることによって、インストール準備完了ページが表示されま
す。下図のように、インストール情報を確認して、すべての情報が正しい場合、
「インストール」をクリックして、nChronos コンソールをインストールします。



8. インストール後、リードミーファイル情報を書いている情報ページが表示されます。リードミー情報を確認し、「次へ」をクリックします。

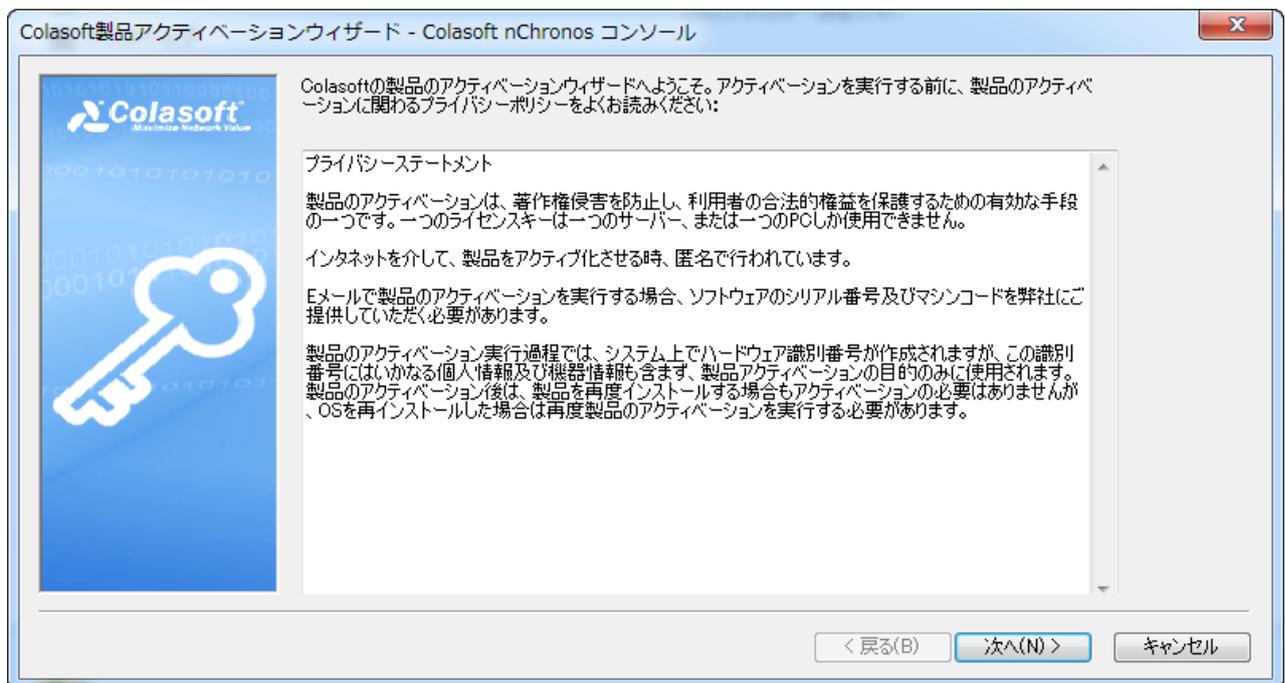


9. インストール完了ページがポップアップされます。「完了」をクリックして、インストールを終了します。



nChronos コンソールをアクティブ化

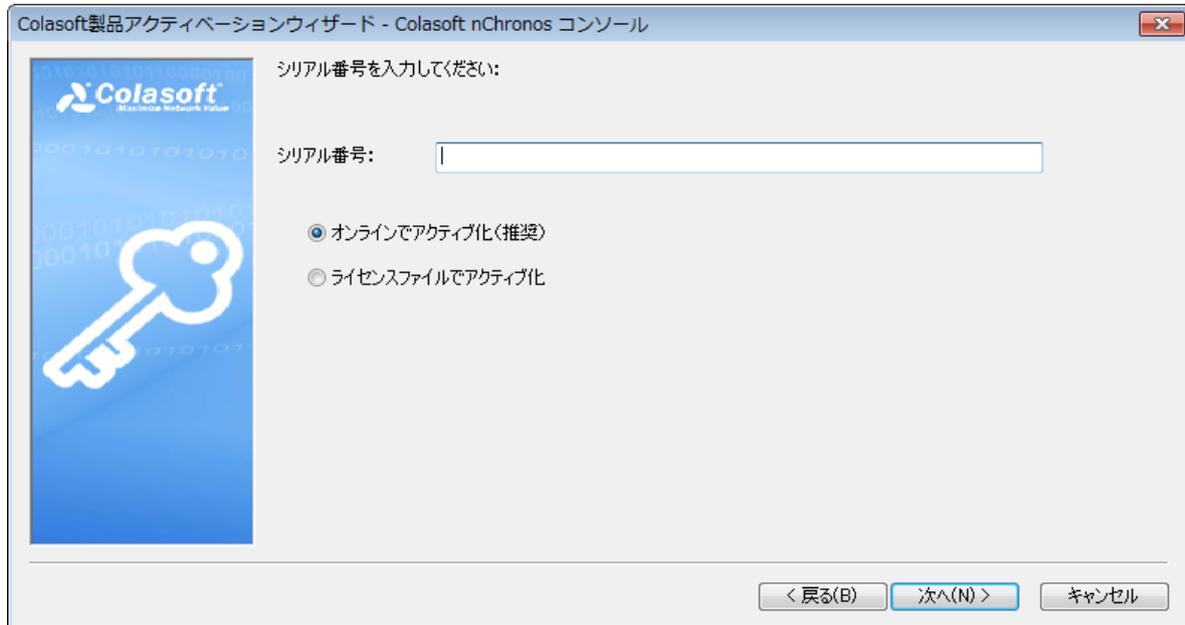
インストール後、アクティベーションウィザードが表示され、ステップごとにアクティベーションをガイドします。



コンソールをアクティブ化するには、オンラインでアクティブ化とライセンスファイルでアクティブ化という二つの方法があります。

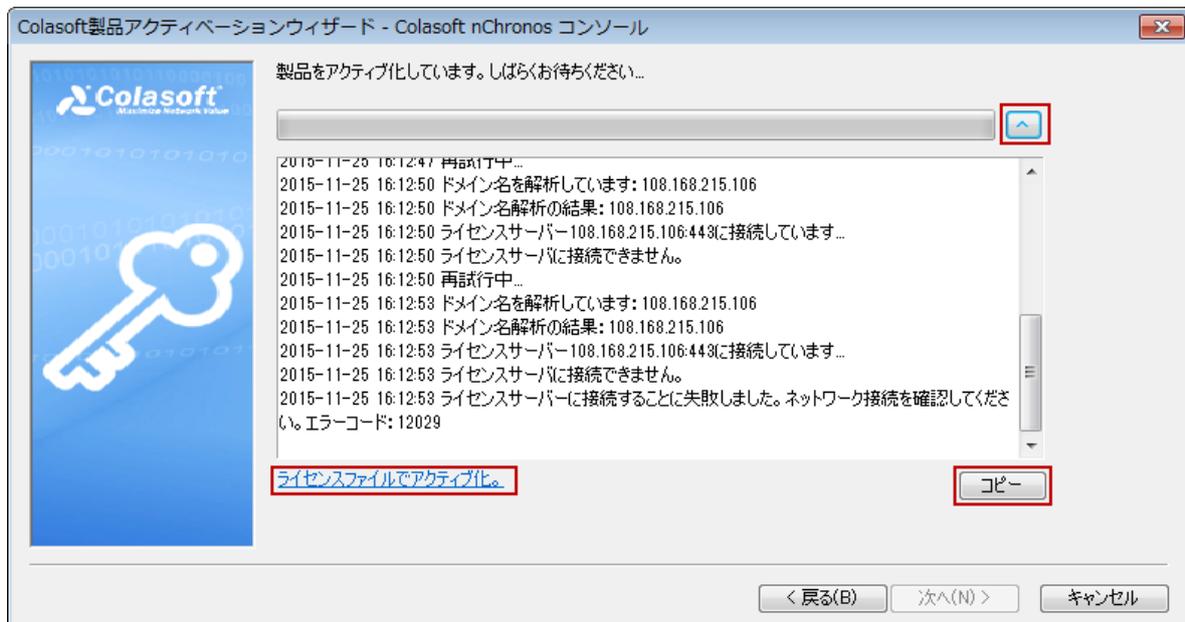
オンラインでアクティブ化

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



オンラインでアクティブ化に失敗した場合、

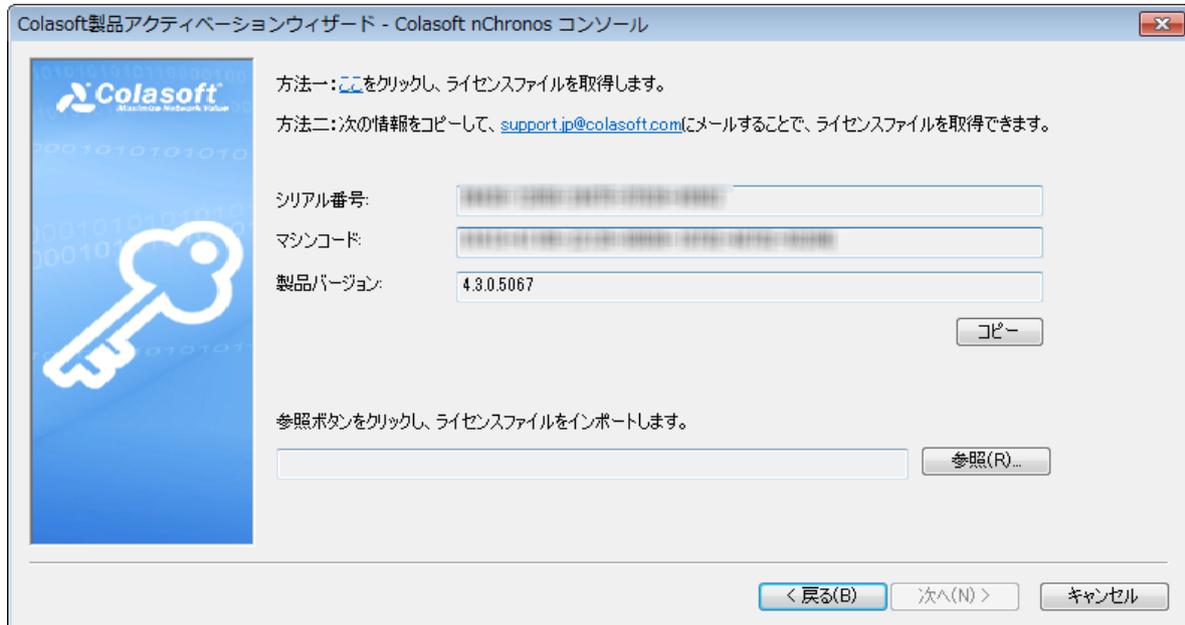
1. アクティベーション詳細を表示する、右側のアクティベーションプログレスバーの横にある二重矢印ボタンをクリックし、「コピー」をクリックします。



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

ライセンスファイルでアクティブ化

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



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

Colasoft ウェブページを介する

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

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



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

Colasoft Support を介する

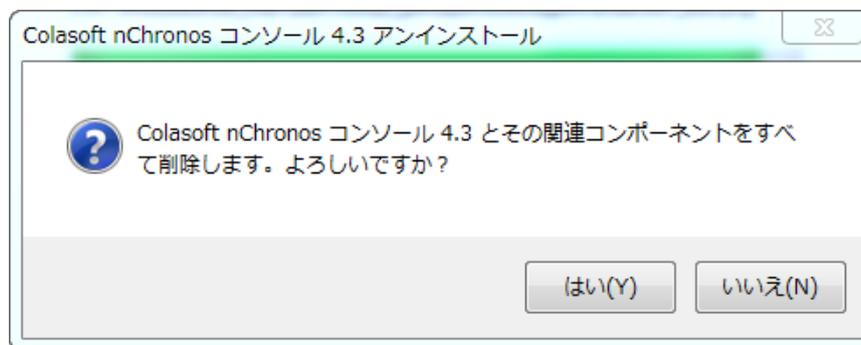
以下のステップに従い、Colasoft Support を介して、ライセンスファイルを取得します。

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

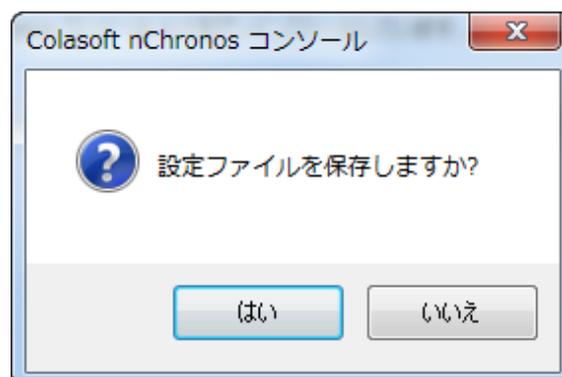
nChronos コンソールをアンインストール

nChronos コンソール 5.0 をアンインストールするには、

1. 以下のいずれを実行します：
 - 「スタート」メニューで nChronos コンソールのフォルダ（デフォルトでは Colasoft nChronos Console 5.0 である）を見つけ出し、Uninstall Colasoft nChronos Console 5.0 をクリックします。
 - 「スタート」メニューで、コントロールパネルをクリックして、コントロールパネルにおける「プロダクトと機能」をクリックします。Colasoft nChronos Console 5.0 を見つけ出して、「アンインストール」をクリックします。
2. 下図のようにアンインストールダイアログボックスがポップアップされます。「はい」をクリックして、アンインストールを続けます。

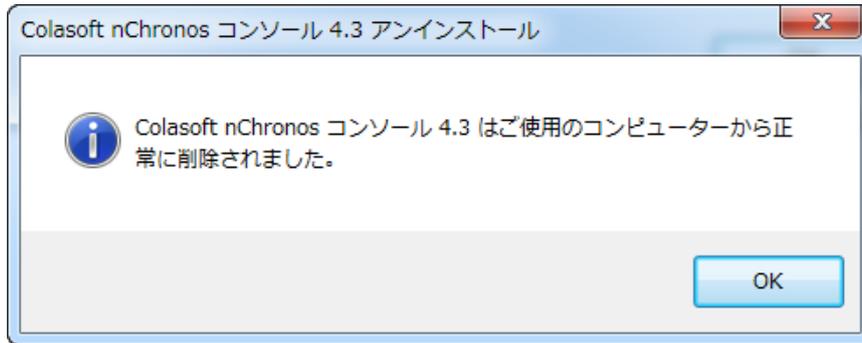


3. 設定を保存するかどうかを確認する大ログボックスがポップアップされます。設定を保存したい場合は、「はい」をクリックして、他の場合は「いいえ」をクリックします。



ヒント この設定はサーバーエクスプローラにおけるサーバーリスト情報です。

4. そして、アンインストールウィザードが自動的に nChronos コンソール 5.0 をアンインストールします。



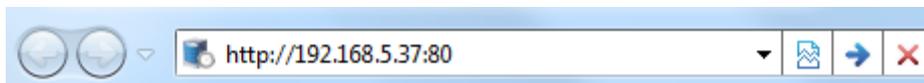
サーバー設定

有用なトラフィックをキャプチャーし、効率的に解析するには、nChronos サーバーを設定する必要があります。この章では、nChronos サーバーの設定について紹介しています。これら全ての設定はウェブページで行われています。だから、まずブラウザから nChronos サーバーにログインする必要があります。

ブラウザからサーバーにログイン

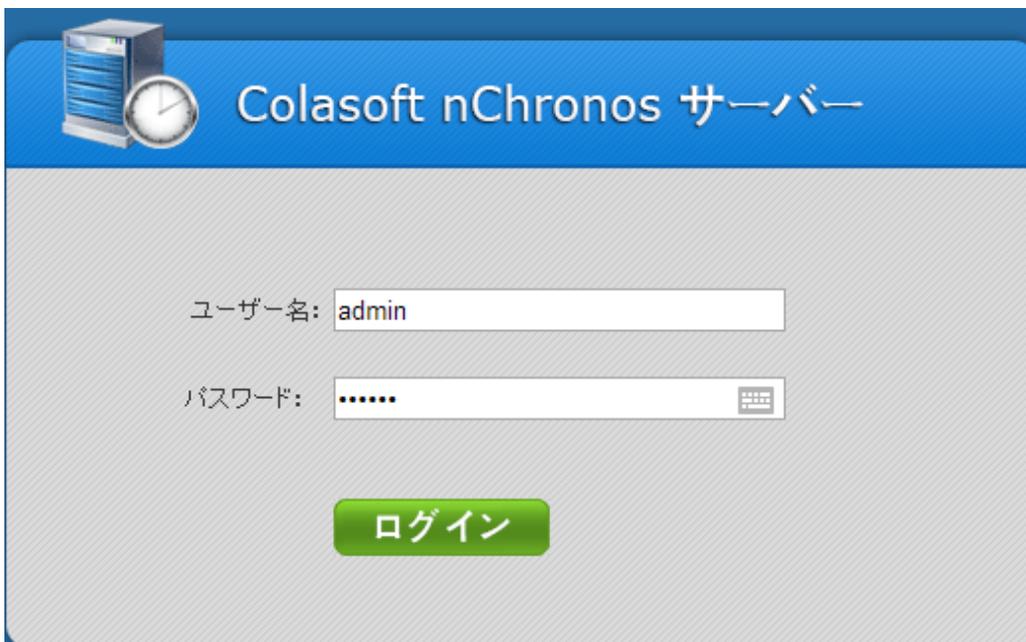
サーバー側とコンソール側の両方を介して、ブラウザから nChronos サーバーにログインすることができます。以下のステップに従い、ブラウザからサーバーにログインします。

1. ブラウザを起動し、アドレスバーに IP アドレスとポート番号を入力して、「Enter」を押します。



IP アドレスは nChronos サーバー上の管理インターフェースです。ポート番号はデフォルトでは 80 となっています。ポート番号を省略して、IP アドレスだけを入力することができます。

2. nChronos サーバーを初期化する時、指定されたユーザー名とパスワードを入力します。



3. 「ログイン」をクリックして、サーバーにログインします。

ストレージ

このページはストレージの設定に利用されています。

[ストレージ設定](#)

有効にする	ハードディスクドライブ	容量	空き領域	配置スペース	使用領域	残りのスペース	利用率
<input type="checkbox"/>	C:	79GB	7GB	<input type="text" value="0"/> GB	0GB	0 GB	0.00%
<input type="checkbox"/>	D:	100GB	87GB	<input type="text" value="0"/> GB	0GB	0 GB	0.00%
<input checked="" type="checkbox"/>	E:	285GB	254GB	<input type="text" value="100"/> GB	0GB	0 GB	0.00%



解析データ

統計情報: % パケット: %

ログデータ

アラームログ: MB トランザクションログ: MB

ディスク容量

ディスク容量は nChronos サーバーのストレージスペースを設定するために設けられています。以下のリストは、上図におけるディスク容量のカラムを説明しています。

- **ディスク**: サーバーで配置されたディスクです。
- **ハードディスクドライブ**: サーバーにおけるディスクのパスです。
- **総容量**: ディスクの総容量です。
- **利用可能な領域**: ディスクの空き領域です。ユーザーは空き領域のすべて、または一部をストレージスペースとして設定することができます。
- **使用領域**: ディスクの配置スペースの中で、すでに使用されている容量です。
- **配置スペース**: 配置されたストレージスペースです。配置スペースは統計データ、パケット、トランザクションログ、アラームログなどの保存に利用されます。

解析スペース

解析スペースは nChronos サーバーのストレージエリアとエクスポートデータが占めている容量を設定するために設けられています。以下のリストは、上図における解析スペースのカラムを説明しています。

- **ストレージエリア**: ストレージエリアの名前を表示します。ユーザーが新しいストレージエリアを追加する際に設定されています。
- **統計データスペース**: 統計データがストレージスペースの中で占めている容量を表示します。
- **パケットスペース**: パケットがストレージスペースの中で占めている容量を表示します。
- **トランザクションログスペース**: トランザクションログがストレージスペースの中

で占めている容量を表示します。

- **アラームログスペース**：アラームログがストレージスペースの中で占めている容量を表示します。

新規ストレージエリアをクリックして、下図のように新規ストレージエリアダイアログボックスが表示されます。

New Storage Area ×

Name:

Statistics space: GB

Packets space: GB

Transaction logs space: GB

Alarm logs space: GB

OK
Cancel

「エクスポートデータ」オプションはエクスポートされたリンク統計データ、アプリケーション監視データ、及びトランザクション処理データがストレージスペースで占めている容量を設定することができます。

インターフェース

このページでは、nChronos サーバー上の全てのネットワークインターフェースが表示されます。キャプチャーインターフェースは、通常スイッチ、またはタップのミラーポートに接続され、トラフィックのキャプチャーに利用されます。管理インターフェースは、nChronos サーバーとコンソールとの通信に利用されます。インターフェースページは下図のように表示されます。

インターフェースの設定

名前	bps	スピード(Mbps)	タイプ	操作
ローカル エリア接続 (192.168.9.25)	129.01 Kbps	100	キャプチャーインタ...	編集
ワイヤレス ネットワーク接続 (127.0.0.1)	0.00 bps	54	管理インターフェー...	編集

保存

- **名前:** ネットワークインターフェース/ポートの名前と IP アドレスを表示します。
- **状態:** ネットワークインターフェース/ポートの接続状態を表示します。
- **スピード:** ネットワークインターフェース/ポートの接続スピードを表示します。
- **タイプ:** キャプチャーインターフェースか、または管理インターフェースかを指定します。
- **操作:** 管理インターフェースにのみ使用できます。

インターフェースタイプの定義

ネットワークインターフェース/ポートのインターフェースタイプを定義するには、単に「タイプ」カラムにおけるドロップダウンリストから適切なタイプを選択すればよいです。

ヒント 複数のキャプチャーインターフェースを定義することができます。

多注意 ネットワークインターフェース/ポートがキャプチャーインターフェースに定義され、そしてネットワークリンクに割当てられた以上、そのインターフェースタイプは変更することができません。変更したい場合は、まずネットワークリンクを削除する必要があります。

キャプチャーインターフェースの設定

キャプチャーインターフェースを設定するには、「キャプチャーインターフェース」の後にある「編集」ボタンをクリックして、下図のように仮想インターフェースページに遷移します。

インターフェースの設定 / 仮想インターフェース

ローカル エリア接続 (192.168.9.25)

タイプ:

VLAN ID	名前	操作
1	section1	<input type="button" value="編集"/> <input type="button" value="削除"/>
2	section2	<input type="button" value="編集"/> <input type="button" value="削除"/>
3	section3	<input type="button" value="編集"/> <input type="button" value="削除"/>

仮想インターフェースを追加するには、

1. 追加したい仮想インターフェースのタイプを選択します。VLAN と MPLS VPN のいずれかを選択することができます。
2. 「仮想インターフェースを追加する」ボタンをクリックすることによって、追加ダイアログボックスがポップアップされます。

×

仮想インターフェース

VLAN ID:

名前:

3. ID やラベル、および仮想インターフェースの名前を入力し、「保存」をクリックすることで、設定を保存します。

管理インターフェースの設定

以下のステップに従い、管理インターフェースを設定します。

1. 「操作」における「編集」をクリックして、下図のように、設定ページに遷移します。

インターフェースの設定 / 管理インターフェースを設定する

ワイヤレス ネットワーク接続 (0.0.0.0)

IPアドレス:

サブネットマスク:

ゲートウェイ:

DNSサーバー:

2. IP アドレス、サブネットマスク、ゲートウェイ、DNS サーバーアドレスを入力して、「保存」をクリックします。

ネットワークリンク

下図のように、ネットワークリンクページでは、ネットワークの基本的な情報が表示されます。ここで、ネットワークリンク状態を変更し、ネットワークリンクを追加、または削除することができます。

ネットワークリンク

番号	名前	タイプ	キャプチャーインターフェース数	bps	状態	操作
1	training	スイッチ(双方向性ミラーリンク)	1	2.03 Kbps	停止	<input type="button" value="編集"/> <input type="button" value="削除"/> <input type="button" value="開始"/>

次のリストは、このページの各カラムについて説明しています。

- **番号:** ネットワークリンクの番号で、1 から始まります。
- **名前:** ネットワークリンクの名前で、ネットワークリンクを追加する時に定義され、コンソール側のサイドバーにおける「サーバー」の下に表示されます。
- **タイプ:** ネットワークリンクのタイプで、トラフィックをキャプチャーする方法を表示します。
- **キャプチャーインターフェース数:** このネットワークリンクのキャプチャーインターフェース数を表示します。
- **状態:** ネットワークリンクの状態で、ネットワークリンクが動作しているか否かを表示します。「動作中」はネットワークリンクのトラフィックをキャプチャーし、解析していることを意味します。「停止」は nChronos サーバーがトラフィックのキャプチャーを停止したということを意味します。
- **操作:** ネットワークリンクについての操作で、以下のリストは、各操作について説明しています。
 - **編集:** ネットワークリンクの設定を変更します。ネットワークリンクを追加する時の設定と同じです。
 - **削除:** ネットワークリンクを削除します。この操作はリンク状態が「停止」である場合にしか、利用できません。
 - **停止:** ネットワークリンクにおける監視を停止します。
 - **開始:** ネットワークリンクのトラフィックのキャプチャーと解析を開始します。

ネットワークリンクの追加

以下のステップに従い、ネットワークリンクを追加します。

1. ネットワークリンクページにおける「新規リンク」をクリックして、次の図が表示されます。

ネットワークリンク / 新規ネットワークリンク

リンク名: リンク名には V : ? * < > | のような文字を含むことができません

リンクタイプ: ▼

ミリ秒統計を有効にする

スイッチタイムスタンプを使用する

ARISTA
 VSS Monitoring
 Gigamon

インバウンド/アウトトラフィックをキャプチャする

ネットワークアダプタ	IPアドレス	bps	スピード(Mbps)
<input checked="" type="checkbox"/> ローカル エリア接続	192.168.9.25	0.00 bps	100

内部ネットワークセグメント

192.168.9.25

説明:

内部IPアドレスを識別するためにネットワークセグメントを一行に一つ入力します。複数の場合、改行コードで区切ってください。

例えば:

IPアドレス/サブネットマスク: 192.168.0.0/24、192.168.0.0/255.255.255.0、または
2001:3ef0::/80
IPアドレス範囲: 192.168.0.0-192.168.1.255、または2001:3ef0::0001-2001:3ef0::0005
単一IPアドレス: 192.168.0.100、または2001:3ef0::0001

帯域幅の設定

インバウンド帯域幅: Mbps (範囲: 1-1,000,000 Mbps)

アウトバウンド帯域幅: Mbps (範囲: 1-1,000,000 Mbps)

総帯域幅: Mbps

(総帯域幅は、インバウンド帯域幅とアウトバウンド帯域幅の大きい方より大きく、両方の合計数より小さい必要があります。)

2. リンク名を入力し、リンクタイプを選択します。以下のリストはリンクタイプについて説明しています。

- **スイッチ (双方向性ミラーリング)** : nChronos はインバウンドとアウトバウンドを含む、トラフィックをミラーリングしているスイッチからのトラフィックをキャプチャーします。
- **スイッチ (単方向性ミラーリング)** : nChronos は、インバウンドとアウトバウンドのいずれのトラフィックをミラーリングしているスイッチからのトラフィックをキャプチャーします。
- **標準タップ**: インバウンドとアウトバウンドのいずれのトラフィックしかミラーリングしていないネットワークタップです。
- **アグリゲーションタップ**: インバウンドとアウトバウンドを含む、双方向のトラフィックをミラーリングしているネットワークタップです。

3. リンクのストレージエリアを選択します。複数リンクが同じストレージエリアを選択することができます。

4. キャプチャーインターフェースとネットワークセグメントを設定します。

スイッチ（双方向のトラフィックをミラーリングしている）、またはアグリゲーションタップを選択した場合、以下ステップに従います。

- 1) スイッチまたはタップのミラーポートに接続されているキャプチャーインターフェースを選択します。
- 2) パケットの転送方向を識別するネットワークセグメントを設定して、正確なインバウンドとアウトバウンドのトラフィックの統計情報を取得します。内部アドレスとして認められる IP アドレスとセグメントを入力する必要があります。

スイッチ（単方向トラフィックをミラーリングしている）、または標準タップを選択した場合、以下のステップに従います。

- 1) スイッチ、またはタップのアウトバウンドミラーポートに接続されているキャプチャーインターフェースを選択して、アウトバウンドトラフィックをキャプチャーします。
 - 2) スイッチ、またはタップのインバウンドミラーポートに接続されているキャプチャーインターフェースを選択して、インバウンドトラフィックをキャプチャーします。
5. スイッチのタイムスタンプを使用するかどうかを設定します。現時点では、ARISTA、VSS Monitoring、および GIGamon という 3 種類のスイッチだけがサポートされています。
 6. 「CSV フォーマットでデータをエクスポート」機能を有効にするかどうかを設定します。リンク統計データ、アプリケーション監視データ、及びトランザクション処理データをエクスポートすることができます。
 7. ミリ秒統計を有効にするかどうかを設定します。ミリ秒統計はバーストトラフィックに関心を持っている場合のために設けられています。ミリ秒統計が有効にしないと、ミリ秒におけるトラフィックアラームが設定できません。
 8. インバウンド帯域幅、アウトバウンド帯域幅、および総帯域幅を入力して、帯域幅を設定します。
正確な帯域幅の利用率を取得するために、実際の帯域幅を入力する必要があります。
 9. 「OK」をクリックして、設定を保存します。

ネットワークリンクを動作させる

コンソール側で、リアルタイム、かつダイナミックな秒までのネットワークデータを表示したり、ネットワークトラフィックの解析の統計情報を取得したりするために、またはサーバーからパケットをダウンロードするために、ネットワークリンクを動作させて、監視する必要があります。

ネットワークリンクを動作させるには、ネットワークリンクページの「開始」ボタンをクリックすればよいです。

ネットワークリンクを停止

ネットワークリンクを停止したい場合、ネットワークリンクページの「停止」ボタンをクリックすることによって、nChronos はトラフィックのキャプチャーを停止します。

ライブラリー

ライブラリーページは下図のように、アップロードされた全てのライブラリーファイルを表示します。

事前定義のライブラリー

名前	タイプ	バージョン	インポート時間	合計数	操作
SystemApplication	アプリケーションライブラリー	2.0.3	04/23/2015 17:02:50	166	<input type="button" value="編集"/> <input type="button" value="削除"/>

以下のリストは、このページにおける全てのカラムについて説明しています。

- **名前:** ファイルの名前ではなく、ライブラリーの名前を表示します。
- **タイプ:** ライブラリーのタイプを表示します。
- **バージョン:** ライブラリーのバージョンを表示します。
- **インポート時間:** ライブラリーファイルがアップロードされている時間を表示します。
- **合計数:** ライブラリーがアプリケーションライブラリーである場合、アプリケーションの数を、ライブラリーが特徴アラームである場合、特徴アラームの数を表示します。
- **操作:** 以下のリストは、各操作について説明しています。
 - **編集:** このボタンをクリックすることによって、ライブラリーの詳細情報が表示されます。表示されている情報における興味のある項目を有効/無効にすることができます。

ライブラリーページでは、アプリケーションライブラリーファイルと特徴ライブラリーファイルを含むライブラリーファイルをインポートすることができます。

- アプリケーションライブラリーは多くのアプリケーションが含まれています。コンソール側でそのアプリケーションを表示、または使用することができます。たとえば、トラフィックアラームを作成する際の、アプリケーションビューにおけるアプリケーションリストと、パケットのダウンロードにおけるアプリケーションルールを作成する際のアプリケーションリストがあります。
- 特徴ライブラリーには、多くの特徴アラームが含まれています。アラーム条件と一致したトラフィックフローをキャプチャーした場合、アラームがトリガーされます。そして、リンクモニターウィンドウとリンク解析ウィンドウのアラームビューにアラームログが表示されます。

自分でライブラリーファイルを作成し、それらをインポートすることができます。デフォルトとして、nChronos はアプリケーションライブラリーファイルをインポートします。また、他のライブラリーファイルをインポートすることもできます。ライブラリーページにおける「ファイルをインポートする」をクリックし、そのファイルをダブルクリックすればよいです。

解析センター

解析センター

nChronosサーバー名:	<input type="text" value="R&D"/>
センターアドレス:	<input type="text" value="192.168.9.25"/>
センターポート:	<input type="text" value="22100"/>
ユーザー名:	<input type="text" value="csadmin"/>
パスワード:	<input type="password" value="●●●●●●●●●●"/>
SSL:	<input type="checkbox"/>

🌀 解析センターに接続しています。しばらくお待ちください...

キャンセル

このページで、解析センターへの接続設定を行います。

- **nChronos サーバー名:** nChronos サーバーの名前を入力します。
- **センターアドレス:** 解析センターの IP アドレスを入力します。
- **センターポート:** 解析センターに接続するポート番号を入力します。デフォルトでは、22100 となっています。
- **ユーザー名:** 解析センターに接続するユーザー名を入力します。ユーザー名は解析センターで設定される必要があります。
- **パスワード:** 解析センターに接続するユーザー名のパスワードを入力します。ユーザー名とパスワードは、解析センターで設定される必要があります。
- **SSL:** このオプションにチェックを入れると、データ送信時に SSL 暗号化を適用します。

SMTP 設定

このページでは、アラームやスケジュールされたレポートを送信する SMTPE メールサーバーに関する接続パラメータを設定します。

SMTP設定

ユーザー情報

名前:

Eメールアドレス:

サーバー情報

Eメールサーバー:

SSL暗号化: ポート:

ログオン情報

ユーザー名:

パスワード:

テスト

保存

- **名前:**送信者の名前を入力します。
- **Eメールアドレス:** 送信者のEメールアドレスを入力します。
- **Eメールサーバー:**Eメールサーバーのアドレスを入力します。
- **SSL暗号化:**Eメールサーバーの暗号化接続タイプを選択します。
- **ポート番号:** 暗号化接続に使われたポート番号を表示します。
- **ユーザー名:** Eメールサーバーにログオンする送信者のユーザー名を入力します。
- **パスワード:**送信アドレスのパスワードを入力します。

設定した後、「テスト」をクリックすることで、設定が正しいかどうかをチェックすることができます。

アラーム通知

下図のように、このページで、アラームがトリガーされるときのアラーム通知パラメータを設定できます。

アラーム通知

Eメール通知

Eメール件名:

受信者アドレス:

通知間隔: 分

テスト

SYSLOG通知

SYSLOGアドレス:

毎秒送信

送信間隔を指定: 分

保存

Eメール通知

アラームがトリガーされたとき、Eメールで通知するには、以下のステップに従います。

1. このページにおける「Eメール通知」にチェックを入れます。
2. 件名と受信者のアドレスを入力します。複数の受信者アドレスを入力することができます。
3. 通知間隔を設定します。
4. 「保存」をクリックして、設定を保存します。

ヒント 「テスト」をクリックして、設定が正しいかどうかを確認することができます。受信者アドレスがテストメールを受信した場合、設定が正しいことを確認できます。

SYSLOG 通知

アラームがトリガーされたとき、syslog サーバーで通知するには、以下のステップに従います。

1. このページにおける「SYSLOG 通知」にチェックを入れます。
2. syslog サーバーのアドレスとポート番号を入力増す。
3. 通知間隔を設定します。Syslog に毎秒送信、または指定された間隔に送信することができます。
4. 「保存」をクリックして、設定を保存します。

レポート通知

このページでは、レポートオプションとレポート受信者アドレスを設定します。

レポート通知

レポートオプション

会社名:

作成者:

会社ロゴ: 

プレビュー

変更

プレフィックス:

生成時間を表示する

受信者アドレス

アドレス

テスト

保存

レポートオプション

レポートオプションを設定したら、設定されたオプション全てがレポートに表示されます。

- **会社名:** これはレポートの左上に表示されます。
- **作成者:** レポート作成者の名前を入力します。
- **会社ロゴ:** 会社のロゴで、レポートの右上に表示されます。
- **プレフィックス:** 接頭辞のように、全てのレポートの前に追加されます。
- **生成時間を表示する:** レポーターが生成された時間を表示します。

設定後、「プレビュー」をクリックして、確認することができます。

受信者アドレス

受信者のアドレスを入力します。受信者アドレスが複数の場合、改行コードによって、区切ってください。

ユーザーアカウント

このページは、全てのユーザーアカウントを表示します。そして、下図のように、このページでユーザーを追加、削除、および追い出すことができます。

ユーザーアカウント

番号	ユーザー名	タイプ	状態	作成時間	ログイン時間	備考	操作
1	admin	管理者	オンライン(ブラウザ)	04/23/2015 17:02:39	04/24/2015 10:56:57	デフォルトの管理者	<input type="button" value="編集"/> <input type="button" value="削除"/> <input type="button" value="追い出す"/>
2	test	管理者	オフライン	04/24/2015 11:24:05			<input type="button" value="編集"/> <input type="button" value="削除"/> <input type="button" value="追い出す"/>

新規アカウント

- **番号:** 1 から始まるアカウントの一連番号です。一つのユーザーアカウントが削除されると、その番号は次のユーザーアカウントに使用されます。ですから、一番下におけるユーザーアカウントの番号から、この nChronos サーバーのために、追加されたユーザーアカウントの数がわかります。
- **ユーザー名:** ユーザーアカウントが追加された際に、定義されたユーザー名を表示します。
- **タイプ:** アカウントのタイプで、管理者、ユーザー、および監査員という三つのタイプがあります。後ろにある「編集」ボタンをクリックして、アカウントのタイプを変更することができます。
- **状態:** アカウントの状態を表示します。以下のリストは状態について、詳しく説明しています。
 - **オンライン:** 「オンライン (コンソール) 」は、コンソールからサーバーにログインし、まだログアウトしていないことを意味しています。「オンライン (ブラウザ) 」はブラウザからサーバーにログインし、まだログアウトしていないことを示しています。「オンライン (コンソール、ブラウザ) 」は、コンソールとブラウザの両方からサーバーにログインし、まだログアウトし

ていないことを表しています。ログインの詳細情報について、監査ログをご参照ください。

- **オフライン:** アカウントは現在、サーバーにログインしていません。
- **無効:** アカウントは管理者によって無効にされており、コンソールからもブラウザからもサーバーにログインすることができません。
- **作成時間:** アカウントが追加された時間を表示します。
- **ログイン時間:** コンソール、またはブラウザからサーバーにログインした時間を表示します。
- **備考:** アカウントについての備考情報を表示します。
- **操作:** 以下のリストは、各操作について説明しています。
 - **編集:** アカウントの設定を変更します。新しいアカウントが追加された時の設定と同じです。
 - **削除:** アカウントを削除します。アカウントの状態をオフラインにしないと、削除出来ません。
 - **追い出す:** アカウントをコンソールとの接続から追い出します。このボタンは、アカウント状態がオンライン（コンソール）である場合にのみ、使用可能です。

アカウントの追加

以下のステップに従い、アカウントを追加します。

1. ユーザーアカウントページにおける「新規アカウント」をクリックすることで、以下の図が表示されます。

ユーザーアカウント / 新規アカウント

ユーザー名:	<input type="text" value="admin2"/>	<small>アカウントIDは数字、アルファベット、および以下の文字だけを含めることができます: '、'、@、'、'。20文字を超えることができません。</small>
パスワード:	<input type="password" value="....."/>	<small>パスワードの長さは6-20文字です。</small>
パスワードを再入力:	<input type="password" value="....."/>	
備考 (オプション):	<input type="text"/>	<small>40文字を超えることができません。</small>
タイプ:	<input type="text" value="ユーザー"/>	
<input type="checkbox"/> アカウントを無効にする。		

2. ユーザー名、アカウントのパスワード、および備考情報を入力します。
3. アカウントのタイプを選択します。
 - **管理者:** 管理者は管理者権限を持っていて、コンソールとブラウザの両方からサーバーにログインすることができます。そして、サーバーとリンクを設定することもできます。
 - **ユーザー:** ユーザーはコンソールからサーバーにログインすることができますが、リンクを設定できません。

- **監査員:** 監査員はブラウザからサーバーにログインすることができますが、監査ログだけが見られます。

4. 「保存」をクリックして、アカウントの追加を終了します。

デジタル証明書

下図のように、このページはデジタル証明書を更新するために設けられています。

デジタル証明書

発行者	サブジェクト	有効時間(開始)	有効時間(終了)	バージョン
CN= Colasoft-CA	C= US S= OK L= Tulsa O= Colasoft LLC CN= nChronos.colasoft.com	01/28/2013 02:28:50	01/28/2018 02:38:50	V3

更新

デフォルトでは、ここに Colasoft が提供しているデジタル証明書ファイルがあります。この証明書を更新することができます。

証明書を更新するには、デジタル証明書ページにおける「更新」をクリックして、証明書ファイルと対応するキーファイルをアップロードします。

デジタル証明書を更新する ×

デジタル証明書ファイル:

キーファイル:

セキュリティーポリシー

下図のように、このページはセキュリティーポリシーを設定するために提供されています。

セキュリティーポリシー

ロックアウトポリシー

IPロックアウト閾値: (回)

IPアドレスのサーバーにログインする失敗回数の閾値を設定します。失敗回数が閾値に達すると、そのIPアドレスはロックアウトされます。

管理者がロックアウトを解除したり、アカウントのロックアウト時間が切れたりする前に、ロックアウトされたアカウントは使用できません。

1から999までの整数を入力することができます。

IPロックアウト時間: (分)

このパラメータは、IPに対するロックアウトが自動的に解除されるまで、ロックアウト状態を保つ時間を設定するためのものです。IPロックアウト閾値が指定されている場合にのみこのパラメータは意味があります。

0から9,999までの整数を入力することができます。

IPロックアウト時間を0に設定した場合、サーバーが再起動するまで、IPはロックアウトされます。

リセットIPロックアウトカウンタ: (分)

このパラメータはログインに失敗した時から、失敗ログインカウンタが0にリセットされるまでの時間を設定するためのものです。IPロックアウト閾値が指定されている場合にのみこのパラメータは意味があります。

1から9,999までの整数を入力することができます。

このリセット時間はIPロックアウト時間以下に設定する必要があります。

ok

解除

以下のステップに従い、セキュリティーポリシーを設定します。

1. 「ロックアウトポリシー」にチェックを入れます。
2. 「IP ロックアウト閾値」ボックスに回数を入力します。

ある IP アドレスのサーバーにログインする失敗回数が閾値に達すると、その IP アドレスはロックアウトされます。管理者がロックアウトを解除したり、アカウントのロックアウト時間が切れたりする前に、ロックアウトされたアカウントは使用できません。1 から 999 までの整数を入力することができます。

3. 「IP ロックアウト時間」に時間を入力します。

これは、IP に対するロックアウトが自動的に解除されるまで、ロックアウト状態を保つ時間です。0 から 9,999 までの整数を入力することができます。IP ロックアウト時間を 0 に設定した場合、サーバーが再起動するまで、IP はロックアウトされます。

4. 「リセット IP ロックアウトカウンタ」に時間を入力します。

これはログインに失敗した時から、失敗ログインカウンタが 0 にリセットされるまでの時間です。1 から 9,999 までの整数を入力することができます。

5. 「保存」をクリックして、設定を保存します。

ロックポリシーが有効になっている場合、サーバーにログインする失敗回数が IP ロックアウト閾値に達すると、IP はロックされます。ロックポリシーが無効になっている場合、ロックされた IP は自動的に解除されます。

ロックされた IP アドレスを表示する

ある IP がロックされた場合、管理者はロック情報を見ることができます。

ロック情報を表示するには、セキュリティーポリシーページにおける「解除」をクリックすることによって、下図のように解除ページがポップアップされます。

IP	アクセス元	アカウント	最新アクセス時間	操作
192.168.8.3	ブラウザ	lanxinxing, lanxinxing, lanxinxing	04/16/2015 10:22:14	

- **IP:** ユーザーがログインしようとする IP アドレスを表示します。
- **アクセス元:** ユーザーがコンソールからサーバーにアクセスしようとするのか、またはブラウザからサーバーにアクセスしようとするのかを表示します。
- **アカウント:** ユーザーがサーバーにアクセスしようとする時のアカウントを表示します。
- **最新アクセス時間:** 最新のアクセス時間を表示します。
- **操作:** IP アドレスのロックを解除します。

ロックされた IP アドレスのほかに、解除ページには、サーバーのログインに失敗しましたが、失敗回数が IP ロックアウト閾値に達していない、IP アドレスも表示されます。

IP アドレスのロックを解除

ロックされた IP を解除するには、解除ページにおける をクリックします。

監査ログ

下図のように、ユーザーがコンソールまたはブラウザからサーバーにログインまたはログアウトすることや、他のイベントを含め、全てのイベントログをこのページに表示します。

監査ログ

タイプ: 時間: -

番号	タイプ	時間	ユーザー	イベント
17		04/24/2015 11:24:05	admin	追加したユーザーアカウント: test
16		04/24/2015 11:09:55	admin	解析センターにログインする
15		04/24/2015 10:56:57	admin	ブラウザ(192.168.9.25)からサーバーにログインする
14		04/24/2015 10:56:17	admin	ブラウザ(192.168.9.25)からサーバーにログインする
13		04/24/2015 08:56:33	N/A	サーバーの起動に成功しました。
12		04/23/2015 18:00:42	N/A	サービスを停止
11		04/23/2015 17:29:52	admin	タイムアウトしました。ブラウザからログアウトします。
10		04/23/2015 17:14:17	admin	ネットワークリンク training を追加する
9		04/23/2015 17:10:43	N/A	サーバーの起動に成功しました。
8		04/23/2015 17:10:40	N/A	サービスを停止
7		04/23/2015 17:10:38	admin	ストレージ設定を修正し、サーバーをリセットする
6		04/23/2015 17:10:26	admin	ブラウザ(192.168.9.25)からサーバーにログインする
5		04/23/2015 17:09:54	admin	ブラウザ(192.168.9.25)からサーバーにログインする
4		04/23/2015 17:09:15	N/A	サーバーの起動に成功しました。
3		04/23/2015 17:09:11	N/A	サービスを停止

合計 2 ページ (17 アイテム) / 1 ページ目

、、、、および  ボタンでページめくりすることによって、イベントログを見ることができます。

以下のリストはこのページのコラムについて説明しています。

- **番号**: イベントの番号で、1 から始まります。
- **タイプ**: イベントのタイプを表示します。
 - : 警告
 - : 情報
 - : エラー
- **時間**: イベントが発生した時間を表示します。
- **ユーザー**: イベントが発生させたユーザーと、イベントが発生した時、ユーザーが使用している IP アドレスを表示します。
- **イベント**: イベントの詳細を表示します。

ログをダウンロード

更なる使用や参照のために、ログをダウンロードすることができます。以下ステップに従い、ログをダウンロードします。

1. ログリストの上にある「ダウンロード」ボタンをクリックします。
2. 「保存」をクリックして、ログを.txt ファイルに保存します。

ログをフィルターする

タイプまたは時間によってログを表示することができます。

タイプによって、ログを表示するには、以下のステップに従います。

1. タイプドロップダウンリストから適切なタイプを選択します。
2. 「フィルター」をクリックします。

時間によって、ログを表示するには、以下のステップに従います。

3. 「時間」における一つ目のボックスをクリックして、時間を指定します。
4. 「時間」における二つ目のボックスをクリックして、時間を指定します。
5. 「フィルター」をクリックします。

同時にタイプと時間の両方によって、ログを表示することもできます。

時間同期

下図のように、このページは日付と時刻を同期させるために提供されています。

時間同期

手動で設定

タイムゾーン: (UTC+08:00) 北京、重慶、香港、ウルムチ ▼

時間: 04/15/2015 17:25:42

インターネット時刻サーバー

サーバー: ▼

時間同期の設定を変更すると、システムはリセットされます。インターネット時刻サーバーと同期させると、クロックは10分ごとにインターネット時刻サーバーと同期します。

保存

正確な解析と統計情報を取得するために、基準時間を設定することが必要です。クロックを同期させるには、2つの方法があります。

手動で同期させる

以下のステップに従い、手動で時間を設定します。

1. 「手動で設定」を選択します。
2. タイムゾーンを選択し、適切な時間を入力して、「OK」をクリックします。

NTP 同期

以下のステップに従い、インターネット時刻サーバーと同期します。

1. 「インターネット時刻サーバー」を選択します。
2. インターネット時刻サーバーを一つ選択して、「OK」をクリックします。

注意 時間同期の設定を変更すると、データはリセットされ、サービスは再起動されます。NTP 同期では、クロックがインターネット時刻サーバーと 10 分ごとに同期するように、設定されています。

サーバー情報

このページでは、nChronos サーバーについての基本的な情報を表示します。

サーバー情報

製品情報	
名前:	Colasoft nChronos サーバー
バージョン:	4.3.0.5047
エディション:	Standard

ライセンス情報	
アクティベーション状態:	アクティブ化した
シリアル番号:	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
ライセンスユーザー:	XXXXXXXXXX
ストレージ容量:	16384GB
最大解析スループット:	2000Mbps
最大ネットワークインターフェース数:	8
最大ネットワークリンク数:	4
サーバーへの同時接続数:	2
最大ユーザーアカウント数:	100
最大監視アプリケーション数:	5
最大解析トランザクション数:	15

製品情報

「製品情報」部分では、ソフトウェア製品についての情報が表示されます。

- **名前:** ソフトウェアの名前を表示します。
- **バージョン:** ソフトウェアのバージョンを表示します。
- **エディション:** ソフトウェアのエディションを表示します。

ライセンス情報

「ライセンス情報」部分では、ストレージ容量、最大解析スループット、最大ネットワークインターフェース数、最大ネットワークリンク数、サーバーへの同時接続数、最大ユーザーアカウント数を含め、ソフトウェア製品についてのライセンス情報が表示されます。シリア

ル番号の後の「再アクティブ化」ボタンをクリックして、製品を再アクティブ化することができます。

サーバー管理

このページは、サーバーを管理するページで、実行されている情報が表示されます。

サーバー管理

状態情報	
開始時間:	04/15/2015 14:06:16
実行時間:	02:38:23
CPU 利用率:	8%
メモリ情報 (4.00 GB):	 使用メモリ2.62GB (67.69%) 利用可能なメモリ1.25GB (32.31%)
ストレージディスク (100.00 GB):	 使用領域1.48GB (1.48%) 空き領域98.52GB (98.52%)

- **開始時間:** サービスが開始する時間を表示します。
- **実行時間:** サービスが実行している時間を表示します。
- **CPU 使用率:** サーバーの CPU 使用率を表示します。
- **メモリ情報:** 総メモリ、使用メモリ、および使用可能なメモリ情報を表示します。
- **ストレージディスク:** 配置スペースについての使用情報を表示します。

ボタン

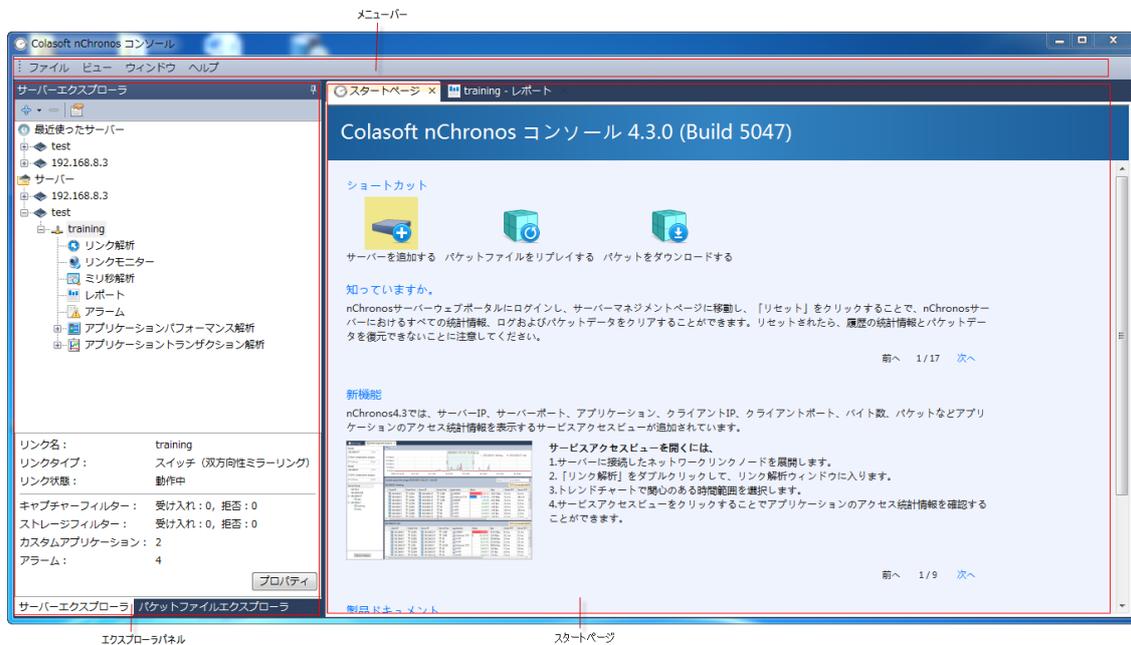
以下のリストは、このページにおける各ボタンについて説明しています。

- **更新:** 現在のページを更新します。
- **設定をエクスポート:** ウェブ側におけるサーバー設定とコンソール側におけるネットワークリンク設定を含め、全ての設定を*.dat ファイルにエクスポートします。更なる使用のために、設定が完了した後、サーバー設定をエクスポートし、バックアップすることがお勧めです。
- **設定をインポート:** この前に保存された設定ファイルをインポートし、現在の設定と取り換えます。設定ファイルのインポートに成功すると、サービスは再起動されます。
- **リセット:** 設定を除いて、全てのデータを空にします。つまりキャプチャーされたパケット、統計情報、およびログは全て削除されます。サーバーがリセットされた後、サービスは再起動されます。
- **再起動:** nChronos サーバーがインストールされているマシンを再起動します。再起動されると、nChronos サーバーと nChronos コンソールの接続は切断され、nChronos サーバーの実行時間もまた 0 から始まります。再起動後、手動で nChronos コンソールから nChronos サーバーに接続する必要があります。
- **シャットダウン:** nChronos サーバーがインストールされているマシンを消します。したがって、nChronos サーバーと nChronos コンソールの接続も切断されます。

コンソールユーザーインターフェース

nChronos コンソールを起動するには、スタート>すべてのプログラム> Colasoft nChronos Console 5.0 > Colasoft nChronos Console 5.0 をクリックします。

その後、プログラムが表示されます。



コンソールユーザーインターフェースは、メニューバー、サーバーエクスプローラ、およびスタートページという三つの部分からなっています。

メニューバー

メニューバーには三つのメニューが含まれています。

ファイルメニュー

- **パケットをダウンロードする**: パケットをダウンロードするダイアログボックスを開き、nChronos サーバーからパケットをダウンロードします。
- **オプション**: システムオプションに入ります。システムオプションでヒントと並び替えを設定することができます。
- **終了**: コンソールを終了します。

ビューメニュー

- **スタートページ**: スタートページを表示、または非表示にします。
- **エクスプローラ**: サーバーエクスプローラを表示、または非表示にします。
- **閉じる**: 現在アクティブなウィンドウを閉じます。
- **すべてを閉じる**: スタートページを除き、開いているすべてのウィンドウを閉じます。
- **統計データを表示**:
 - **数字で**: 数字で統計データを表示します。
 - **自動フォーマットで**: 自動フォーマットで統計データを表示します。
- **MAC アドレスを表示する**:

- **アドレスとして:** 16 進数で MAC アドレスを表示します。例えば、*AA:BB:CC:33:44:55* です。
- **別名として:** 別名で MAC アドレスを表示します。例えば、*localhost* です。
- **アドレスと別名で:** 16 進数と別名で MAC アドレスを表示します。例えば *AA:BB:CC:33:44:55[localhost]* です。
- **IP アドレスを表示する:**
 - **アドレスとして:** 10 進数で IP アドレスを表示します。例えば、*192.168.1.1* です。
 - **別名として:** 別名で IP アドレスを表示します。例えば、*localhost* です。
 - **アドレスと別名で:** 10 進数と別名で IP アドレスを表示します。例えば、*192.168.1.1[localhost]* です。
- **アダプタメーカーを表示する:** ネットワークアダプタを表示、または非表示します。例えば、*Intel-AA:BB:CC* です。
- **ダウンロードとエキスパート解析を管理する:** このボタンをクリックして、履歴のダウンロードとエキスパート解析が表示されます。ここで、ダウンロードとエキスパート解析を管理します。

ヘルプメニュー

- **コンテンツ:** .chm 形式のヘルプファイルを起動して、コンテンツページを表示します。
- **検索:** .chm 形式のヘルプファイルを起動して、検索ページを表示します。
- **インデックス:** .chm 形式のヘルプファイルを起動して、インデックスページを検索します。
- **Colasoft ホームページ:** Colasoft のホームページに移動します。
- **フォーラム:** 技術フォーラムに移動します。
- **nChronos について:** 製品情報とライセンスファイルを表示します。

サーバーエクスプローラ

エクスプローラパネルはプログラムの左側にあり、nChronos サーバーを管理するものです。サーバーエクスプローラでは、追加された全てのサーバーとサーバーグループを表示します。そして、何かサーバー、またはネットワークリンクが選択された場合、選択されたサーバー、またはネットワークリンクの基本的情報がサーバーエクスプローラの下に表示されます。

nChronos サーバーを追加した後、サーバーエクスプローラは、下図のように表示されます。



以下のリストは、サーバーエクスプローラにおける各アイコンボタンについて説明しています。



サーバー、またはサーバーグループをコンソールに追加します。



サーバーエクスプローラで選択されたサーバーを削除します。サーバーが切断されないと、削除することができません。



選択された項目のプロパティを表示します。

ヒント

-  アイコンはサーバーグループを表します。
-  アイコンは nChronos サーバーを表します。
-  アイコンはネットワークリンクを表します。

サーバーエクスプローラを表示、または非表示する

サーバーエクスプローラを非表示にするには、サーバーエクスプローラの右上隅にある  をクリックすることで、サーバーエクスプローラはプログラムの左側に細かいバーに縮小されます。

サーバーエクスプローラを表示したい場合、細かいバーにおける「サーバーエクスプローラ」をクリックし、そしてサーバーエクスプローラの右上隅にある  ボタンをクリックすればよいです。

スタートページ

スタートページは nChronos コンソールを起動する時に表示されるメインインターフェイスで、ヒント、特徴、および新規ユーザーのためのプログラムについてのほかの情報を提供します。

スタートページは主に五つの部分からなっています。

- **ショートカット**:この部分で、デフォルトでは三つのショートカットを提供しますが、ショートカットを新規追加することもできます。この部分におけるショートカットアイコンをクリックして、サーバーを追加したり、パケットファイルを再生したり、パケットをダウンロードしたりすることができます。ショートカットを新規追加するには、エクスプローラパネルで追加したい項目を右クリックし、「ショートカットを作成」をクリックすればよいです。
- **知っていますか**: この部分では、プログラムを使用する時のいくつかのヒントを提供します。
- **新機能**:この部分では、プログラムのいくつかの機能を提供し、これらの機能を体験するのをステップごとにガイドします。
- **ドキュメント**:この部分では、プログラムについてのいくつかのドキュメントを提供します。Colasoft のウェブサイトからそれらのドキュメントを取得することができます。
- **お問い合わせ**:この部分では、いくつかの連絡情報を提供します。プログラムについて何か問題があったら、遠慮なくお問い合わせください。

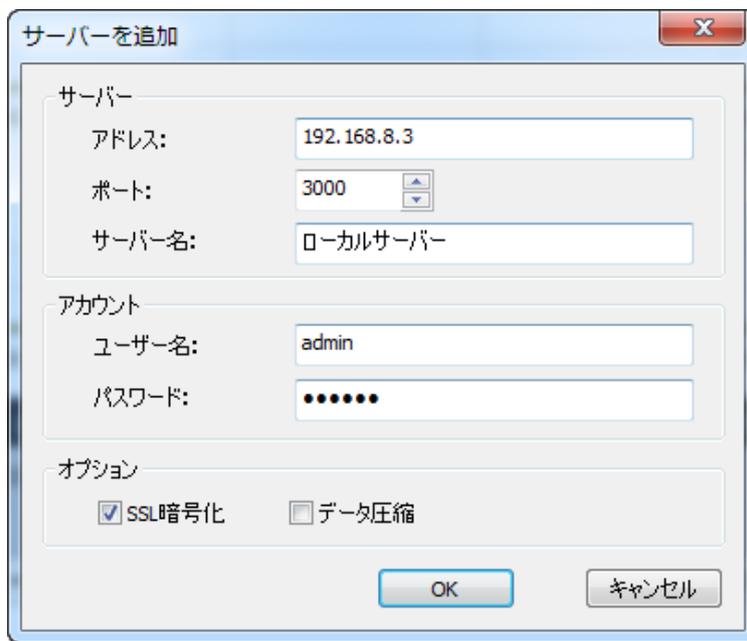
nChronos サーバーの追加と接続

nChronos は全てのキャプチャーされたパケット、統計情報、および他の解析データを nChronos サーバーに保存します。したがって、それらのデータを取得して、nChronos コンソールに表示するには、コンソールに nChronos サーバーを追加と接続する必要があります。

nChronos サーバーの追加

以下のステップに従い、nChronos サーバーを追加します。

1. サーバーエクスプローラにおける  をクリックし、そして「サーバーを追加」をクリックすることで、サーバーを追加するダイアログボックスが表示されます。



2. このダイアログボックスを完了します。各ラベルの詳細について、次のリストをご参照ください。
 - **アドレス**: nChronos サーバーにおける管理インターフェースの IP アドレスを入力します。
 - **ポート**: サーバーに接続するポート番号を入力します。デフォルトでは 3000 となっています。
 - **名前**: 「Marketing Dept」のようなサーバーを識別する名前を入力します。何も入力しないと、その名前は IP アドレスで表示されます。
 - **ユーザー名**: サーバーにログインするアカウントのユーザー名を入力します。
 - **パスワード**: アカウントのパスワードを入力します。
 - **SSL 暗号化**: サーバーからコンソールにデータを転送する際に SSL 暗号化を適用するかどうかを選択します。
 - **データ圧縮**: サーバーからコンソールに転送するデータを圧縮します。
3. 「サーバーを追加」ダイアログボックスを完了した後、「OK」をクリックすることによって、追加されたサーバーはサーバーエクスプローラに表示されます。

nChronos サーバーに接続

一般的に言えば、サーバーが追加された後、コンソールは自動的にサーバーに接続します。コンソールがサーバーに接続していない場合、次のいずれに従い、サーバーに接続します。

- 接続したいサーバーの名前をダブルクリックします。
- 接続したいサーバーの名前をクリックし、その前にある  をクリックします。
- 接続したいサーバーの名前をクリックし、サーバーエクスプローラの下にある「接続」をクリックします。
- 接続したいサーバーの名前を右クリック、「接続」をクリックします。

ネットワークリンクの設定

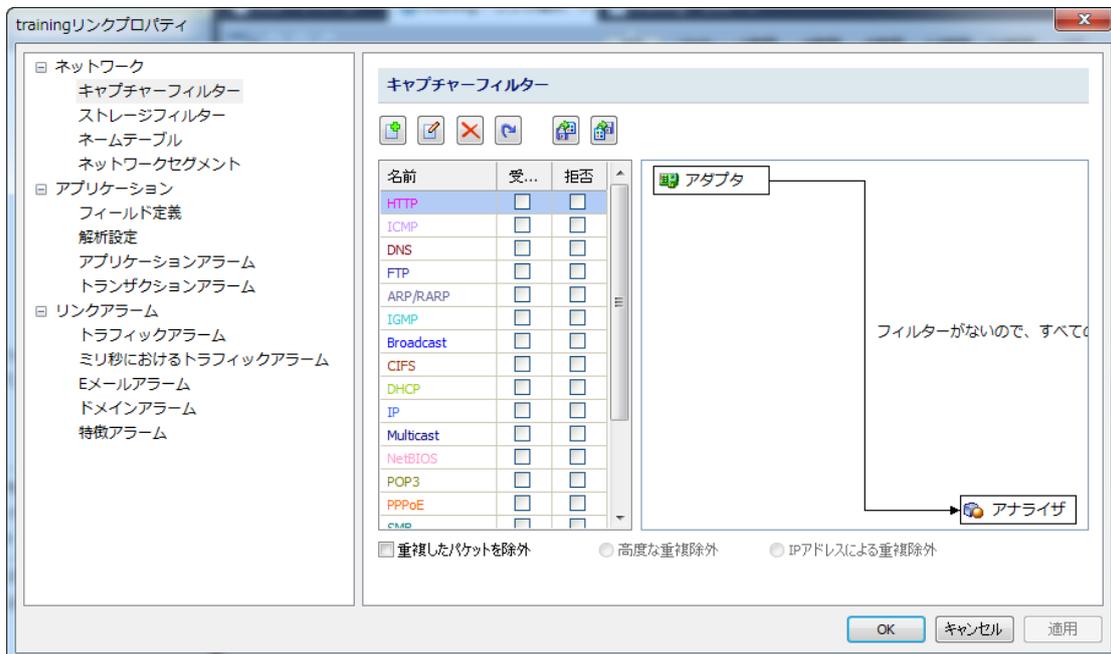
ネットワークリンクは、ネットワークトラフィックをキャプチャーしたり、インバウンドネットワークセグメントを定義することで内部 IP アドレスを定義したり、ネットワークの帯域幅を設定したりするために作成されたのです。したがって、有用なパケットをキャプチャーし、効果的な解析と統計情報を取得するには、監視、または解析する前にネットワークリンクを設定する必要があります。

nChronos サーバーに接続した後、ネットワークリンクは自動的に属しているサーバーの下に表示されます。

ネットワークリンクを設定するには、以下のいずれかに従います。

- ネットワークリンクを右クリックし、「プロパティ」をクリックすることで、リンクプロパティダイアログボックスが表示されます。
- ネットワークリンクをクリックし、サーバーエクスプローラの上にある  をクリックすることによって、リンクプロパティダイアログボックスが表示されます。
- ネットワークリンクをクリックし、サーバーエクスプローラの一番下にある「プロパティ」ボタンをクリックすることで、リンクプロパティダイアログボックスが表示されます。

リンクプロパティダイアログボックスは下図のように表示されます。



リンクプロパティダイアログボックスには、キャプチャーフィルター、ストレージフィルター、名前テーブル、ネットワークセグメント、参考値、フィールド定義、解析設定、アプリケーションアラーム、トランザクションアラーム、トラフィックアラーム、ミリ秒におけるトラフィックアラーム、Eメールアラーム、ドメインアラーム、特徴アラーム、アプリケーションパフォーマンス解析、アプリケーショントランザクション解析などさまざまな設定が含まれています。

キャプチャーフィルター

キャプチャーフィルターは、要件を満たしていないパケットをフィルターするために用いられています。下図のように、この部分には、左側のパネルと右側のパネルが含まれています。



左側パネルには、デフォルトフィルターとカスタムフィルターを含め、全てのフィルターが表示されています。各フィルターは「受け入れ」と「拒否」という2つのオプションがあります。「受け入れ」はフィルターに一致しているパケットだけが保存、解析されるということを意味します。それに対して、「拒否」はフィルターに一致していないパケットだけが保存、解析されることを表します。

右側のパネルは、「受け入れ」されているものと「拒否」されているものを含む、フィルターリストで選択された全てのフィルター項目を表示するフィルターフローチャートです。

ボタン

ここにはキャプチャーフィルターを設定するボタンが六つあります。

- : 新しいフィルターを作成します。
- : 選択されたフィルターを修正します。
- : 選択されたフィルターを削除します。
- : この前に保存されたフィルターファイルをインポートし、現在のフィルターファイルと取り換えます。フィルターファイルがインポートされると、現在のリストにおける全てのフィルターは削除されます。
- : 現在のフィルターリストにおける全てのフィルター設定をディスクにエクスポート、保存します。

: フィルターをデフォルトにリセットします。

フィルターを追加する

フィルターを追加するには、単に  をクリックし、「キャプチャーフィルター」ダイアログボックスを完了すればよいです。シンプルなフィルター、または高度なフィルターを追加することができます。

フィルターを適用する

フィルターを適用するには、単に「受け入れ」、または「拒否」にチェックを入れ、「OK」をクリックすればよいです。

重複したパケットを除外

キャプチャーフィルターを使用すると、重複したパケットを除外することができます。複数の重複したパケットが存在する場合、一つだけが解析され、残りは全部除外されます。設定が間違っているポートミラーリング (SPAN) 環境において、重複したパケットはたくさん存在します。もちろんこれは正常のネットワーク解析には悪い影響があります。重複したパケットを除外することは解析精度を向上させ、ストレージスペースを節約することができます。

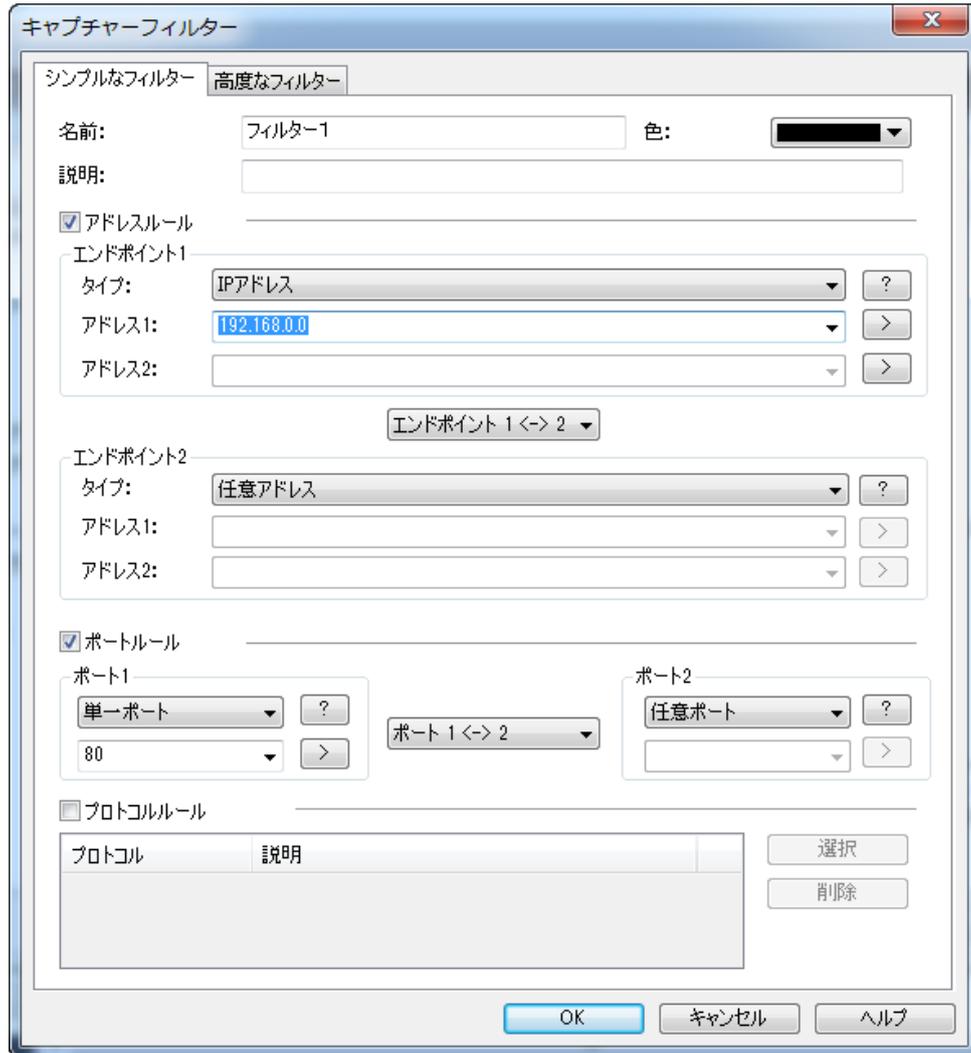
重複したパケットを除外するには、IP アドレスによる重複除外と高度な重複除外という 2 つの方法があります。

- **IP アドレスによる重複除外:** この方法は、送信元 IP アドレス、宛先 IP アドレス、および IP ID によって重複したパケットを特定します。2 つのパケットは送信元 IP アドレス、宛先 IP アドレス、および IP ID が同じである場合、一つだけ解析され、残りは除外されます。
- **高度な重複除外:** この方法は送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、宛先 MAC アドレス、IP ID、およびチェックサムによって重複したパケットを特定します。2 つのパケットは送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、宛先 MAC アドレス、IP ID、およびチェックサムが同じである場合、一つだけ解析され、残りは除外されます。

 **注意** 重複したパケットを有効にするのがストレージのパフォーマンスに大きな影響を与えるので、非常に必要な場合だけ、その機能を有効にすることをお勧めします。

シンプルなフィルター

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



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

正確にパケットを取得するために、IP アドレスルール、MAC アドレスルール、およびポートルールにおいて、パケットの転送方向を指定することができます。

アドレスルールを定義する

以下のステップに従い、アドレスルールを定義します。

1. 「アドレスルール」にチェックを入れます。
2. エンドポイント 1 において、アドレスタイプを選択し、その下のテキストボックスにアドレスを入力します。
3. 方向ドロップダウンリストボックスをクリックし、アドレス間のパケット転送方向を選択します。
4. エンドポイント 2 において、アドレスタイプを選択し、その下のテキストボックスにアドレスを入力します。
5. キャプチャーフィルターダイアログボックスにおける「OK」をクリックします。

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

ポートルールを定義する

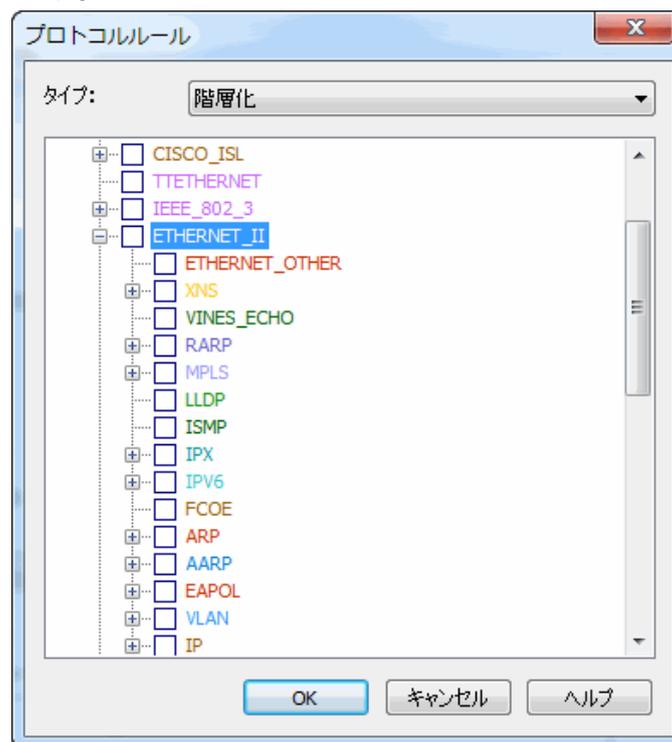
以下のステップに従い、ポートルールを定義します。

1. 「ポートルール」にチェックを入れます。
2. ポート 1 において、ポートタイプを選択し、その下にあるテキストボックスにポート番号を入力します。
3. 方向ドロップダウンリストボックスをクリックし、ポート間のパケット転送方向を選択します。
4. ポート 2 において、ポートタイプを選択し、その下にあるテキストボックスにポート番号を入力します。
5. キャプチャーフィルターダイアログボックスにおける「OK」をクリックします。

プロトコルルールを定義する

以下のステップに従い、プロトコルルールを定義します。

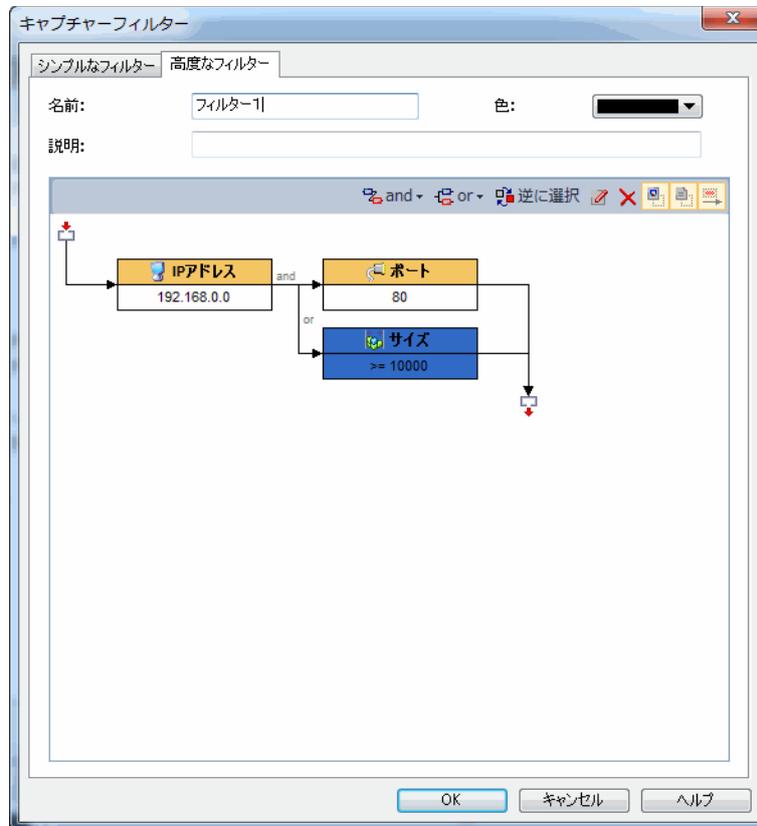
1. 「プロトコルルール」にチェックを入れます。
2. 「選択」をクリックすることで、下図のようにプロトコルルールダイアログボックスが表示されます。



3. 適切なプロトコルを選択し、「OK」をクリックします。
 4. キャプチャーフィルターダイアログボックスにおける「OK」をクリックします。
- 選択されたプロトコルは、プロトコルルール部分にリストされます。「削除」ボタンを使用して、リストからプロトコル項目を削除することができます。

高度なフィルター

高度なフィルターは下図のように表示されます。



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

ツールバー

ツールバーには、以下の項目が含まれています。

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

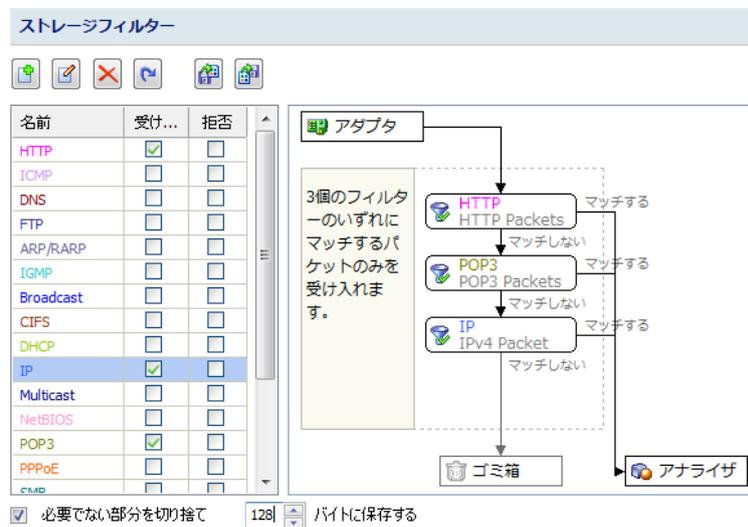
高度なフィルターにはアドレス、ポート、プロトコルという三種類のルールがあります。その三種類のルールはシンプルなフィルターと同じです。

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

ストレージフィルター

ストレージフィルターは、フィルターと一致するパケットを保存するために設けられています。例えば、HTTP パケットだけを保存したい場合、HTTP ストレージフィルターを有効にすればよいです。

ストレージフィルタータブは、下図のように、キャプチャーフィルタータブとは非常に類似しています。

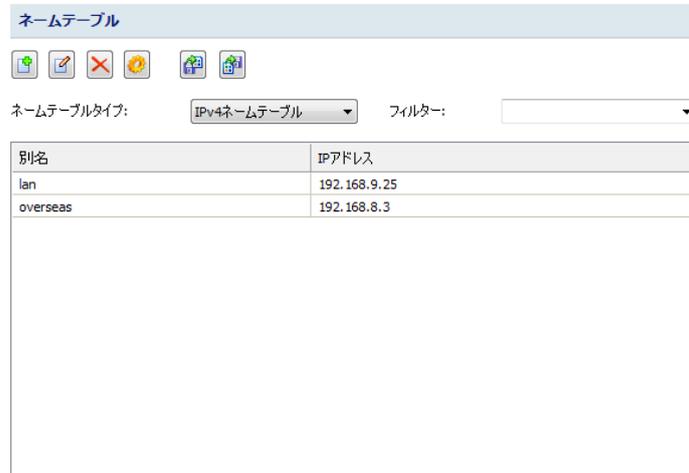


類似しているインターフェースのほかに、ストレージフィルターの設定も、キャプチャーフィルターと全く同じです。ストレージフィルターを作成する具体的な方法について、「キャプチャーフィルター」をご参照ください。

フィルターに加えて、ストレージフィルターは、必要でない部分を切り捨てて、指定されたサイズでパケットを保存する機能を提供します。ストレージフィルタータブ一番したにある「必要でない部分を切り捨て」にチェックをいれ、保存するパケットサイズを指定します。

ネームテーブル

下図のように、ネームテーブルで全ての MAC アドレスと IP アドレスの別名を管理します。

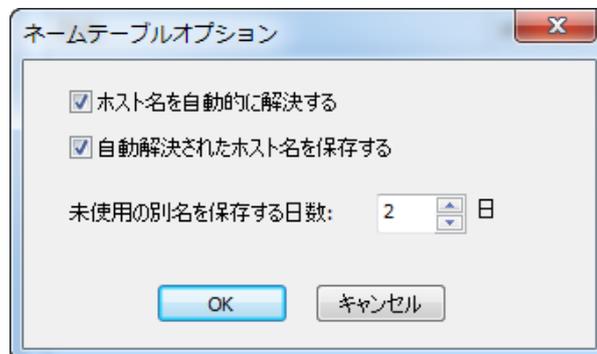


ボタン

このタブにおけるボタンは以下のように説明します。

- : アドレスの別名を追加します。
- : 選択された項目を修正します。
- : 選択された項目を削除します。
- : ネームテーブルオプションを設定します。
- : ネームテーブルファイルをインポートして、現在の別名リストと取り換えます。
- : 現在の別名リストを .csta ファイルに保存します。

 をクリックすることによって、ネームテーブルオプションダイアログボックスが表示されます。

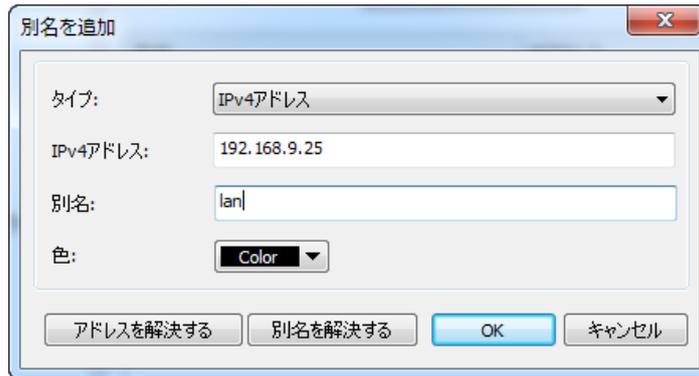


- **ホスト名を自動解決する**: デフォルトでは有効になっていて、自動的にホストの別名を解決します。
- **自動解決されたホスト名を保存する**: デフォルトでは有効になっていて、自動解決されたホスト名を保存します。
- **未使用の別名を保存する日数**: 未使用の別名を保存する日数を指定します。

アドレスの別名を追加する

以下のステップに従い、アドレスの別名を追加します。

1. ネームテーブルタイプドロップダウンリストから別名タイプを選択します。例えば、IPv4 アドレスの別名を追加したい場合、IPv4 ネームテーブルを選択する必要があります。
2.  をクリックすることによって、下図のように別名追加ダイアログボックスが表示されます。



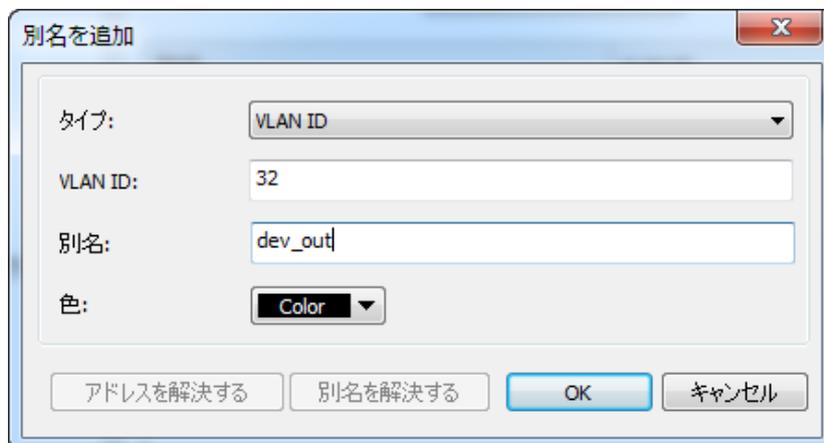
3. アドレスとアドレスの別名を入力します。
4. このダイアログボックスにおける「OK」をクリックして、ネームテーブルタブにおける「OK」をクリックします。

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

VLAN ID の別名を追加する

以下のステップに従い、VLAN ID の別名を追加します。

1. ネームテーブルタイプドロップダウンリストから VLAN ID を選択します。
2.  をクリックすることによって、下図のように別名追加ダイアログボックスが表示されます。



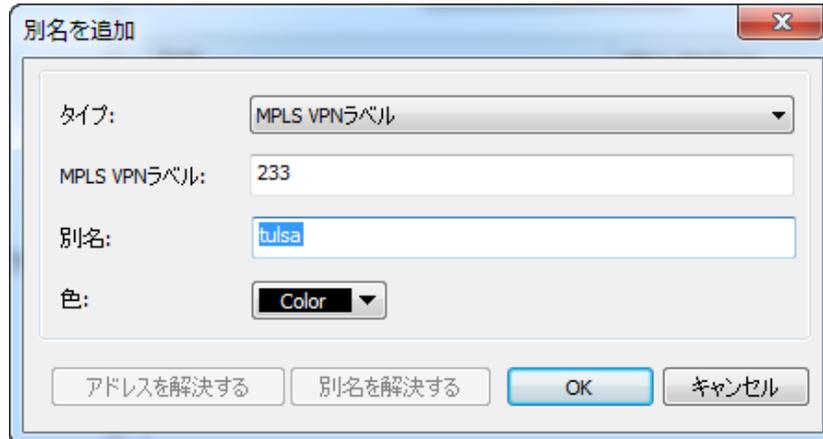
3. VLAN ID と VLAN ID の別名を入力します。
4. このダイアログボックスにおける「OK」をクリックして、ネームテーブルタブにお

ける「OK」をクリックします。

MPLS VPN ラベルの別名を追加する

以下のステップに従い、MPLS VPN ラベルの別名を追加します。

1. ネームテーブルタイプドロップダウンリストから MPLS VPN ラベルを選択します。
2.  をクリックすることによって、下図のように別名追加ダイアログボックスが表示されます。



3. MPLS VPN ラベルと MPLS VPN ラベルの別名を入力します。
4. このダイアログボックスにおける「OK」をクリックして、ネームテーブルタブにおける「OK」をクリックします。

ネットワークセグメント

このタブには、下図のように全てのネットワークセグメントとセグメントのルールを表示します。

ネットワークセグメント

名前	ジオロケーション	ルール
Dev.1		192.168.9.1-192.168.9.60
Dev.2		192.168.9.61-192.168.9.120
Test		192.168.9.121-192.168.9.255
Support		192.168.6.0/24
Sales		192.168.0.0/24#192.168.20.0/24#192.168.8.0/24

ボタン

以下のリストはこのタブにおけるボタンについて、説明しています。



: ネットワークセグメントを追加します。



: 選択されたネットワークセグメントを修正します。



: 選択されたネットワークセグメントを削除します。



: ネットワークセグメント設定ファイルをインポートします。

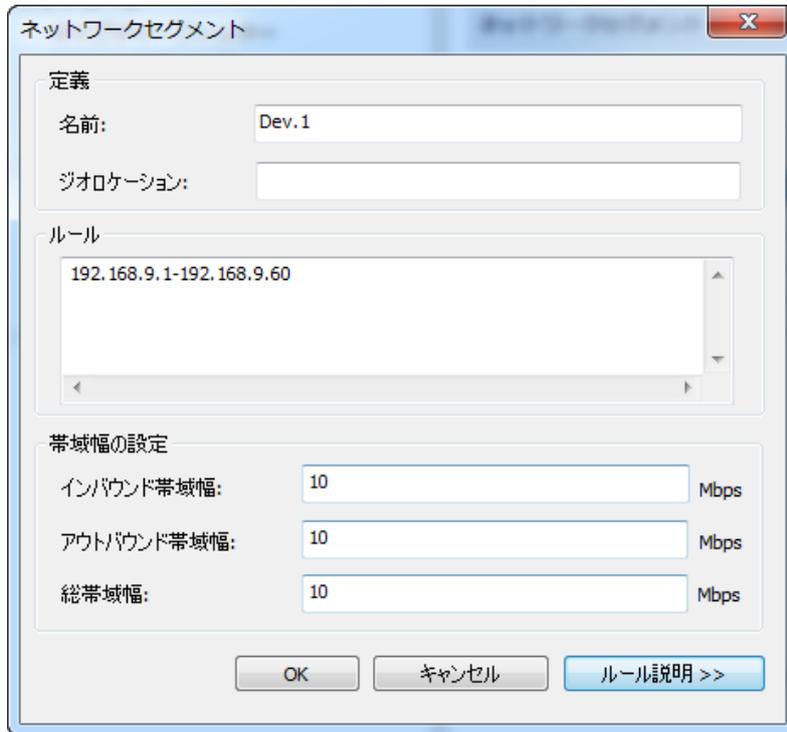


: 現在ネットワークセグメント設定をローカルディスクにエクスポートします。

ネットワークセグメントを追加する

以下のステップに従い、ネットワークセグメントを追加します。

1.  をクリックして、新規セグメント設定ダイアログボックスを開きます。



2. 新規セグメント設定ダイアログボックスにおいて、セグメントの名前を入力し、ジオロケーションを指定し、セグメントルールを入力します。
 - **名前:** ネットワークセグメントの名前で、セグメントが利用可能な場合、ネットワークセグメントビューに表示されます。
 - **ジオロケーション:** ネットワークセグメントの地理的位置で、セグメントに属している IP アドレスが利用可能な場合、IP アドレスビューと IP セッションにおけるジオロケーションカラムに表示されます。
 - **ルール:** IP アドレス、IP アドレス範囲、またはネットワークセグメントとしての IP アドレスサブネットを定義することができます。異なるネットワークセグメントのルールは同じ、または交差できないことに注意してください。

- 帯域幅の設定:** このオプションはネットワークセグメントの帯域幅を設定し、帯域幅の利用率の計算に役立ちます。インバウンド帯域幅とアウトバウンド帯域幅はそれぞれ、ネットワークセグメントが属しているネットワークリンクのインバウンド帯域幅とアウトバウンド帯域幅を超えることができません。総帯域幅は、インバウンド帯域幅とアウトバウンド帯域幅の大きい方より大きく、両方の合計数より小さく入力する必要があります。
3. 新規セグメント設定ダイアログボックスにおける「OK」をクリックし、ネットワークセグメントにおける「OK」をクリックします。

参考値

参考値タブでユーザーは概要統計ビューにおける各参考アイテムの参考値範囲を定義することができます。参考値タブは下図のように表示されています。

References			
Reference Item	Reference Range		
Unicast Bytes/Total IP Byt...	>=90.00%		
Broadcast Bytes/Total IP ...	<5.00%		
Multicast Bytes/Total IP B...	<5.00%		
Abnormal Address Bytes...	<1.00%		
Unicast Bytes/Total Non-...	>=90.00%		
Broadcast Bytes/Total N...	<5.00%		
Multicast Bytes/Total No...	<5.00%		
Abnormal Address Bytes...	<1.00%		
Broadcast Packets/Total ...	<10.00%		
Multicast Packets/Total P...	<10.00%		
ARP Packets/Total Packets	<3.00%		
ICMP Packets/Total Pack...	<3.00%		
<--64B Packets/Total Pac...	<15.00%		

ボタン

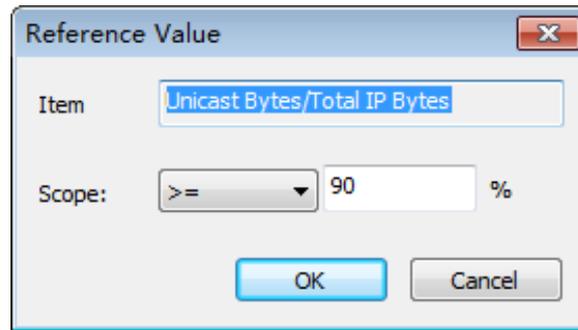
以下のリストは、このタブにおけるアイコンについて説明しています。

- : 選択された参考値を修正します。
- : このタブにおける全ての設定をデフォルトにリセットします。
- : 保存された参考値設定ファイルを現在のタブにインポートします。
- : このタブにおける全ての設定をローカルディスクに保存します。さらに保存された設定ファイルを他のリンクにインポートすることもできます。

参考値を修正

修正ボタンをクリックして、下図のように参考値を修正するダイアログボックスが表示され

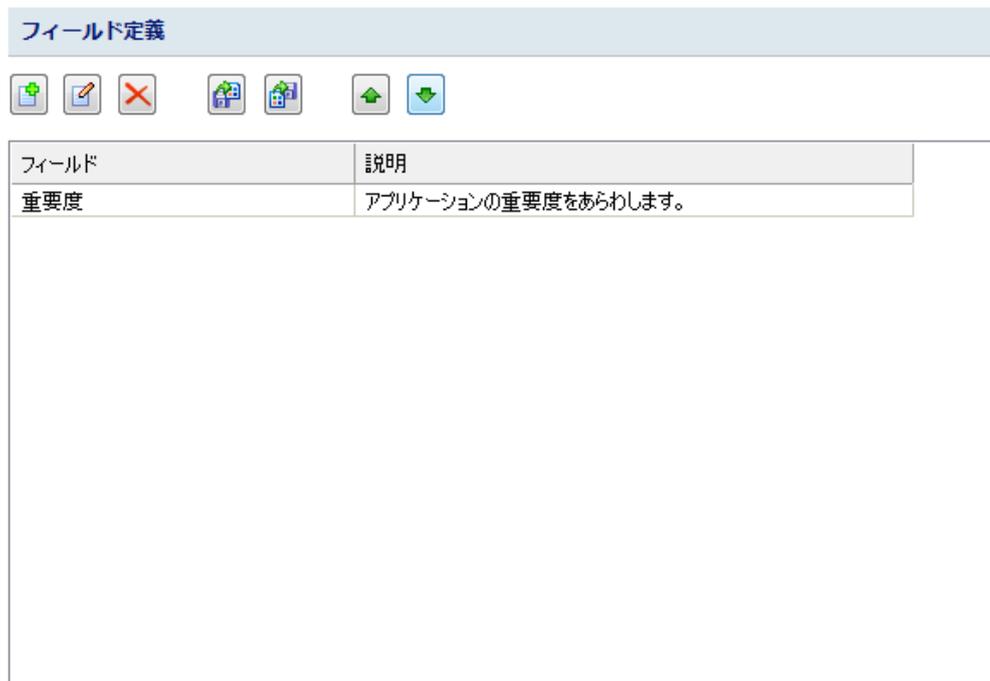
ます。



このダイアログボックスで、実際の状況によって、参考値範囲を修正することができます。

フィールド定義

下図のように、このタブはでカスタムアプリケーションのためのフィールドを定義します。



注意 フィールドの定義に成功した場合、カスタムアプリケーションを追加している時にそれが表示されます。フィールドに値を入力する必要があります。

ボタン

以下のリストは、このタブにおけるアイコンについて説明しています。

- : 新しいフィールドを追加します。
- : 選択されたフィールドを修正します。
- : 選択されたフィールドを削除します。
- : 保存された設定ファイルを現在のタブにインポートします。設定ファイルのインポ

ートに成功した場合、現在のリストにおける全てのフィールドが削除されます。



: このタブにおける全ての設定を*.csta ファイルに保存します。



: 選択されたフィールドを上に移動します。

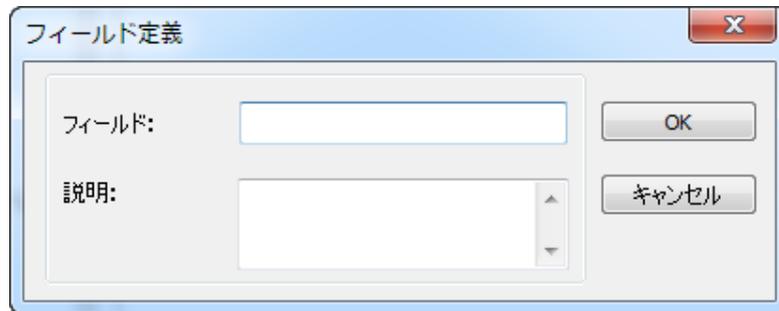


: 選択されたフィールドを下に移動します。

フィールドを追加する

以下のステップに従い、フィールドを追加します。

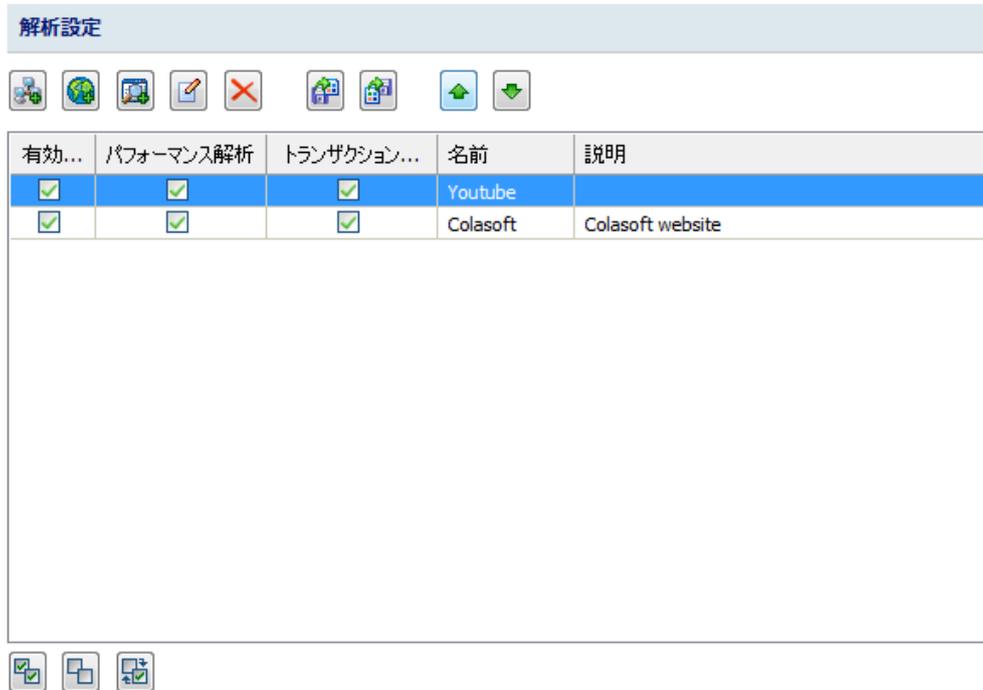
1.  をクリックすることによって、下図のようにフィールド定義ダイアログボックスが表示されます。



2. フィールド名、または必要な場合に説明を入力します。
3. 「OK」をクリックします。

解析設定

下図のように、このタブで、標準アプリケーション、Web アプリケーション、および特徴アプリケーションをカスタマイズし、パフォーマンス解析とトランザクション解析を有効にすることができます。



ボタン

以下のリストはこのタブにおけるアイコンについて説明しています。

- :新しい標準アプリケーションを追加します。
- :新しい Web アプリケーションを追加します。
- :新しい特徴アプリケーションを追加します。
- :選択されたアプリケーションを修正します。
- : 選択されたアプリケーションを削除します。
- : 保存されたカスタムアプリケーションの設定ファイルをインポートします。
- :現在のカスタムアプリケーションの設定をエクスポートします。
- :選択されたアプリケーションを上に移動します。上のアプリケーションは下のものに優先します。
- :選択されたアプリケーションを下に移動します。

カラム

以下のリストはこのタブにおけるカラムについて説明しています。

- **有効にする**: アプリケーションを有効にするかどうかを選択します。
- **名前**: アプリケーションの名前を表示します。
- **アプリケーションタイプ**:アプリケーションのタイプを表示します。
- **パフォーマンス解析**:モニターとパフォーマンス解析を有効にするかどうかを選択します。三つのカスタムアプリケーションのうち、どれもこの機能を持っています。「有効にする」にチェックを入れないと、このカラムを有効にできないことに注意

してください。

- **トランザクション解析**:アプリケーションのトランザクションを解析するかどうかを選択します。Web アプリケーションしかこの機能を持っていません。「有効にする」にチェックを入れないと、このカラムを有効にできないことに注意してください。

カラムにはテキストを表示するスペースが十分でないと、カラム間のラインにマウスを移動し、ドラッグすることで、スペースを拡大することができます。

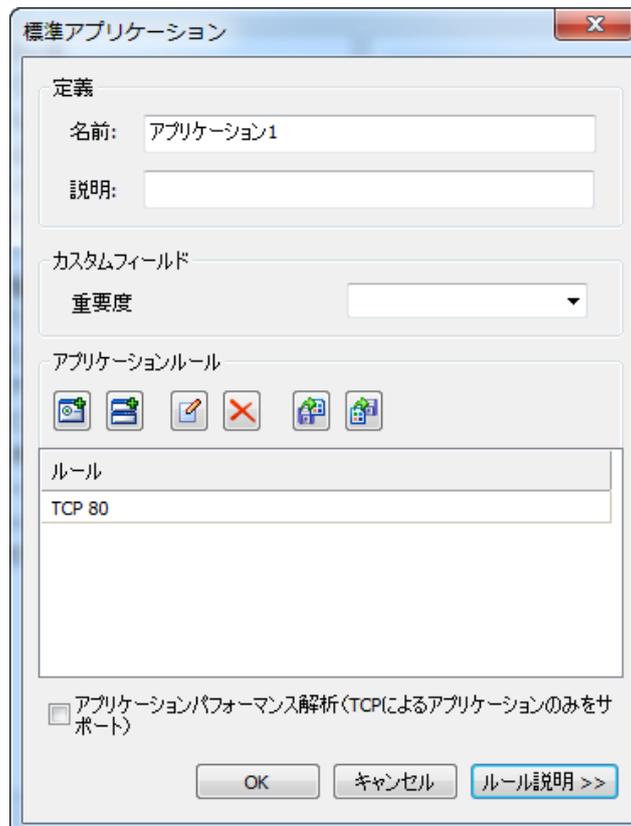
カスタムアプリケーションを有効にするには、「有効にする」カラムにチェックを入れる必要があります。

注意 コンフリクトが発生した場合、カスタムアプリケーションは、システムアプリケーションに優先します。

標準アプリケーションの追加

以下のステップに従い、標準アプリケーションを追加します。

1. 解析設定タブにおける  をクリックすることで、下図のように標準アプリケーションダイアログボックスが表示されます。



2. 標準アプリケーションダイアログボックスにおいて、アプリケーションの名前と説明を入力して、必要な場合、「フィールドを設定」ボタンをクリックして、フィールドを設定します。
3. レスポンス時間を設定します。レスポンス時間は、良い、普通、悪い、非常に悪いという四つのレベルに分けています。アプリケーションにおけるある TCP トランザクションのレスポンス時間が「非常に悪い」場合、一回のレスポンスタイムアウトと

されます。

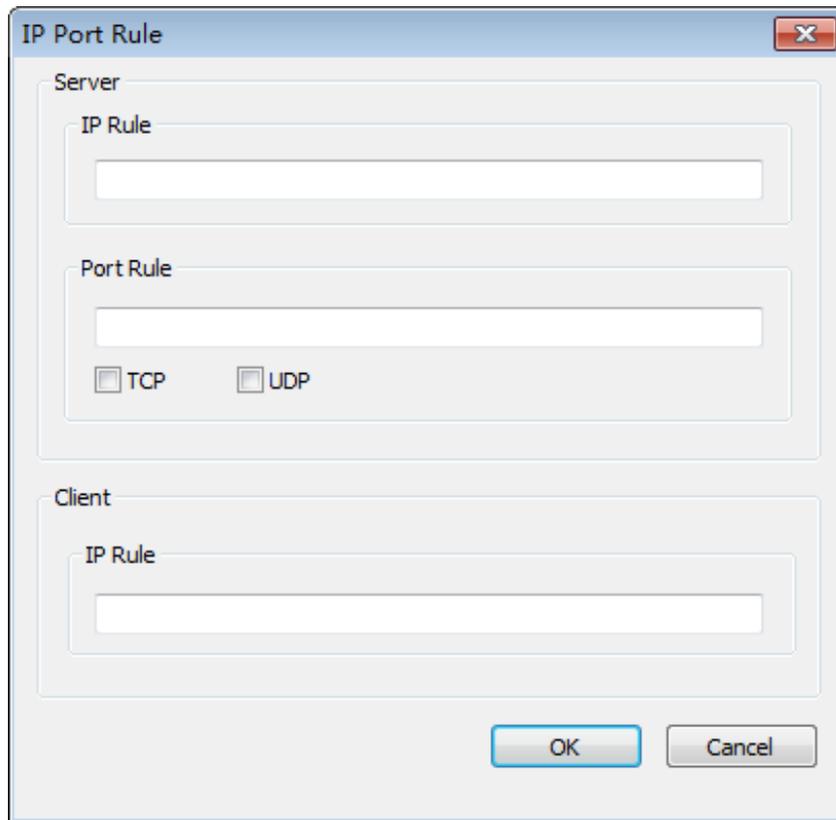
4.  をクリックすることで、IP ポートルールダイアログボックスが開かれます。このダイアログボックスで標準アプリケーションのルールを設定します。
5. 解析設定タブにおける「OK」をクリックして、標準アプリケーションの追加を完了します。

ヒント

- 標準アプリケーションダイアログボックスの下側にルールについて説明があります。その説明を参照にルールを入力してください。
- アプリケーションのために、特定のフィールドを追加したい場合、まずリンクプロパティダイアログボックスにおけるフィールド定義でフィールドを定義し、フィールドの値を入力する必要があります。
- 標準アプリケーションダイアログボックスにおける「アプリケーションパフォーマンス解析」オプションは、アプリケーションのパフォーマンス解析を有効にするかどうかにより使われます。解析設定タブにおける「パフォーマンス解析」カラムと同じ機能を持っています。

IP ポートルール

IP ポートルールダイアログボックスは下図のように表示されます。



このダイアログボックスで以下の四つのタイプのルールを設定することができます。

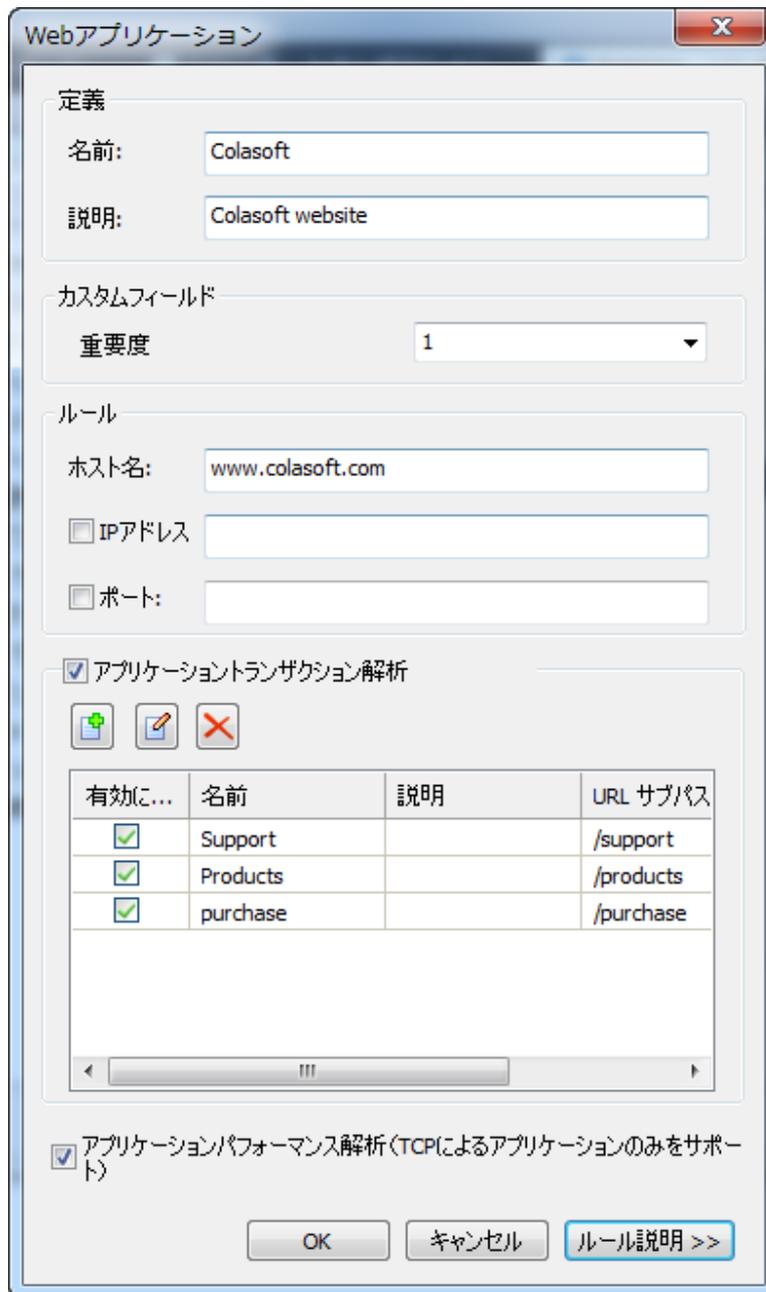
- サーバーポート
単一ポート(80)、「,」で区切られた複数ポート(80,90)、または「-」ポート範囲(80-90)をサポートします。

- サーバーIPアドレス、またはクライアント IP アドレス
単一 IP アドレス、複数 IP アドレス、及び IP アドレス範囲をサポートします。
- サーバーIPアドレス+ポート
- サーバーIPアドレス+ポート+クライアント IP アドレス

Web アプリケーションの追加

以下のステップに従い、Web アプリケーションを追加します。

1. 解析設定タブにおける  をクリックすることで、下図のように Web アプリケーションダイアログボックスが表示されます。



Webアプリケーション

定義

名前: Colasoft

説明: Colasoft website

カスタムフィールド

重要度: 1

ルール

ホスト名: www.colasoft.com

IPアドレス

ポート:

アプリケーショントランザクション解析

有効に...	名前	説明	URL サブパス
<input checked="" type="checkbox"/>	Support		/support
<input checked="" type="checkbox"/>	Products		/products
<input checked="" type="checkbox"/>	purchase		/purchase

アプリケーションパフォーマンス解析 (TCPによるアプリケーションのみをサポート)

OK キャンセル [ルール説明 >>](#)

2. Web アプリケーションダイアログボックスにおいて、アプリケーションの名前と説明を入力し、必要な場合「フィールドを設定」ボタンをクリックして、フィールドを設定します。

- **名前:** アプリケーションの名前を入力します。
 - **説明:** アプリケーションについての説明を入力します。
 - **フィールド設定:** リンクプロパティダイアログボックスにおけるフィールド定義で事前にフィールドを定義した場合にのみ、この部分は利用可能になります。
3. レスポンス時間を設定します。レスポンス時間は、良い、普通、悪い、非常に悪いという四つのレベルに分けています。アプリケーションにおけるある TCP トランザクションのレスポンス時間が「非常に悪い」場合、一回のレスポンスタイムアウトとされます。
 4. 「www.colasoft.com」のように、ホスト名を入力します。Web アプリケーションは、今のところ HTTP プロトコルしか識別できません。
 5. 必要な場合、アプリケーショントランザクション解析を有効し、 をクリックすることで、アプリケーショントランザクションを追加します。トランザクションを追加する詳しい情報について、この節における「アプリケーショントランザクションを追加する」をご参照ください。
以下のリスト、このダイアログボックスにおけるほかの三つのボタンについて、説明しています。



: アプリケーショントランザクションを追加します。



: 選択されたトランザクションを修正します。



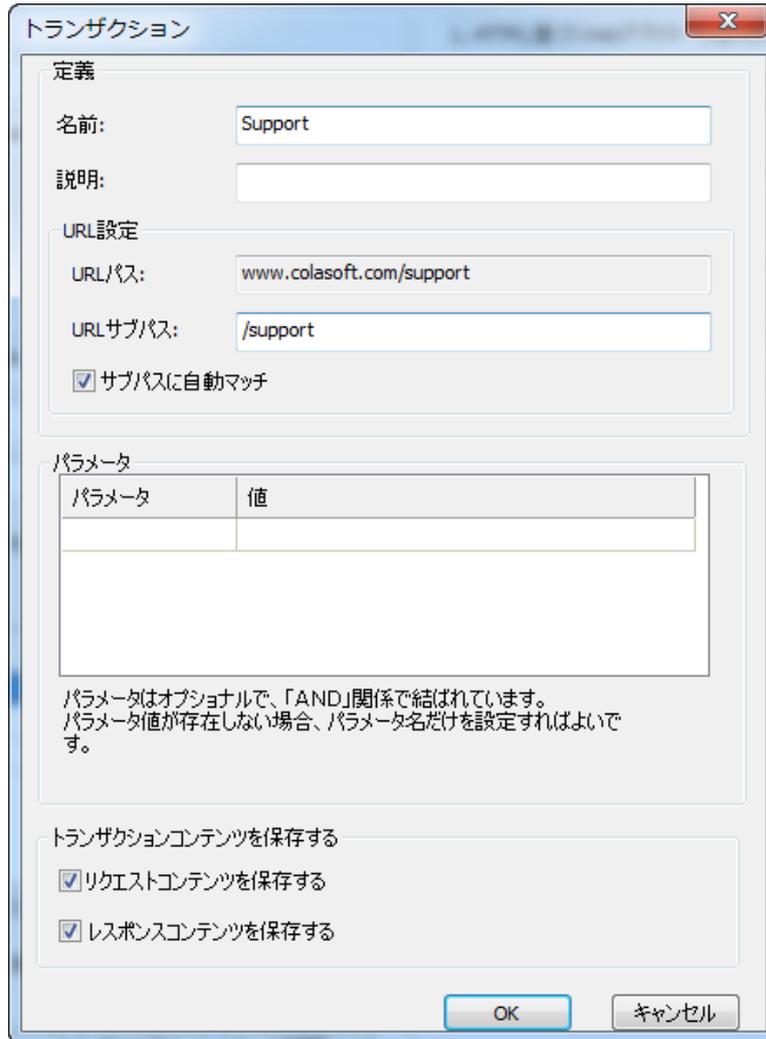
: 選択されたトランザクションを削除します。あるトランザクションが削除されると、そのトランザクションにおける全てのトランザクションプロセスも削除されます。

6. Web アプリケーションダイアログボックスにおける「OK」をクリックし、解析設定タブにおける「OK」をクリックして、Web アプリケーションの追加を完了します。

アプリケーショントランザクションを追加する

以下のステップに従い、アプリケーショントランザクションを追加します。

1. Web アプリケーションダイアログボックスにおける「アプリケーショントランザクション解析」を有効にし、 をクリックすることで、下図のようにトランザクションダイアログボックスが表示されます。



トランザクション

定義

名前: Support

説明:

URL設定

URLパス: www.colasoft.com/support

URLサブパス: /support

サブパスに自動マッチ

パラメータ

パラメータ	値

パラメータはオプションで、「AND」関係で結ばれています。
 パラメータ値が存在しない場合、パラメータ名だけを設定すればよいです。

トランザクションコンテンツを保存する

リクエストコンテンツを保存する

レスポンスコンテンツを保存する

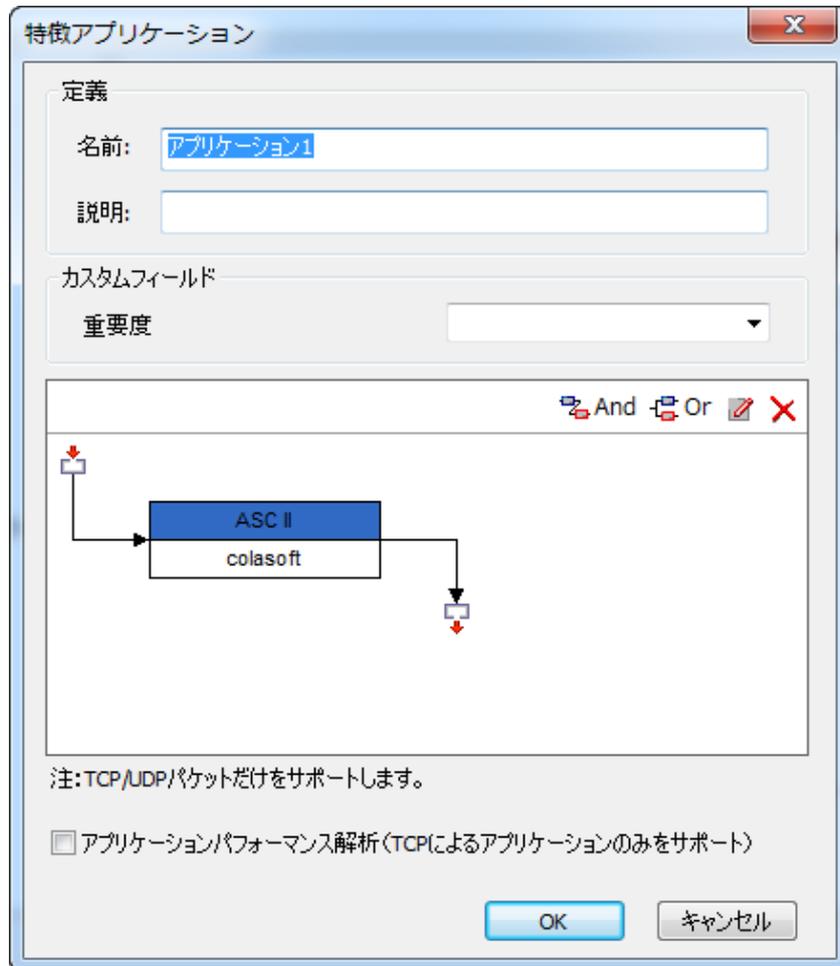
OK キャンセル

2. トランザクションダイアログボックスにおいて、トランザクションの名前と説明を入力します。
3. URL サブパスとパラメータを入力します。以下のリストは各オプションについて説明しています。
 - **URL パス**: トランザクションの URL パスで、ホスト名と URL サブパスから構成されています。URL サブパスを入力すると、自動的に生成されます。
 - **URL サブパス**: URL のサブパスを入力します。
 - **サブパスに自動マッチ**: このオプションを有効にすると、サブパスにあいまい一致が適用されます。このオプションにチェックを入れないと、URL サブパスが定義されているものと同じである場合にのみ、トランザクションは識別されます。
 - **パラメータ**: URL のパラメータで、パラメータ 1=値 1 のように、パラメータ名=パラメータ値という形でパラメータを入力します。1 行に一つで、複数のパラメータを入力することができます。
4. 必要な場合、「リクエストコンテンツを保存する」と「レスポンスコンテンツを保存する」にチェックを入れて、トランザクションのリクエストとレスポンスコンテンツを保存します。
5. 最後に「OK」をクリックして、Web アプリケーションの追加を完了します。

特徴アプリケーションの追加

以下のステップに従い、特徴アプリケーションを追加します。

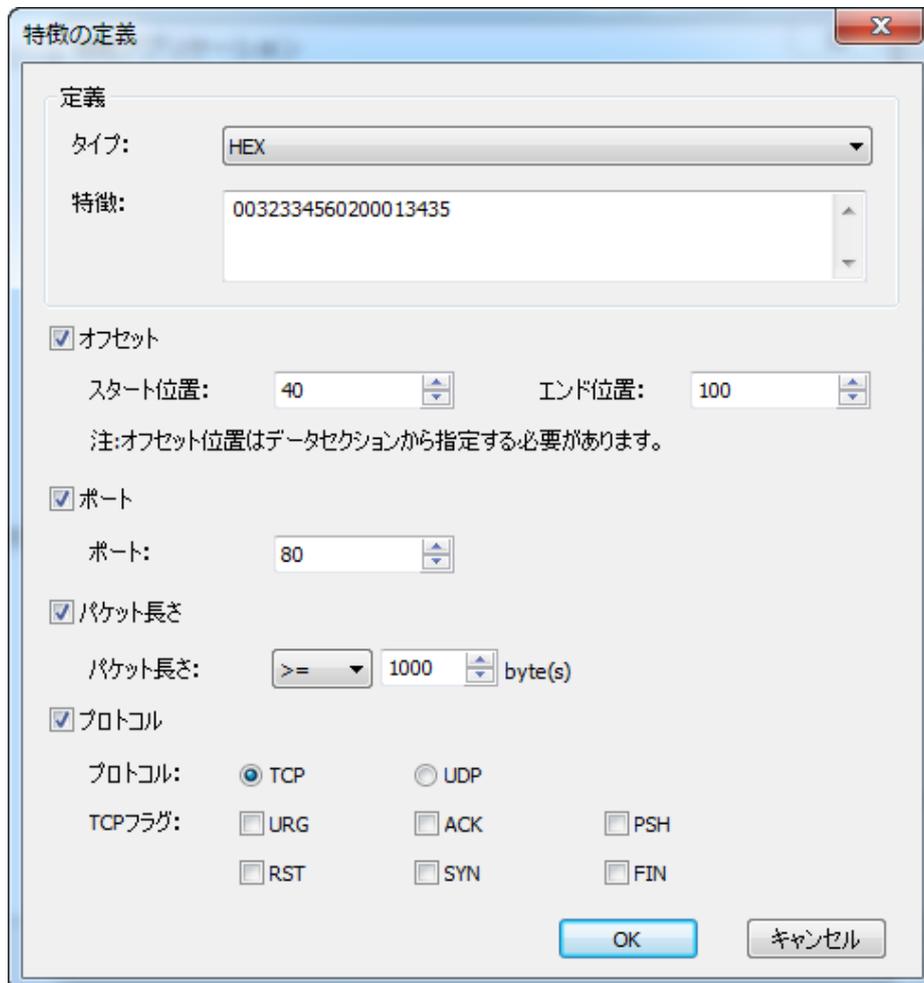
1. 解析設定タブにおける  をクリックして、下図のように特徴アプリケーションダイアログボックスを開きます。



2. 特徴アプリケーションダイアログボックスにおいて、アプリケーションの名前と説明を入力し、必要な場合「フィールドを設定」ボタンをクリックして、フィールドを設定します。
 - **名前:** アプリケーションの名前を入力します。
 - **説明:** トランザクションについての説明を入力します。
 - **フィールドを設定:** リンクプロパティダイアログボックスにおけるフィールド定義でフィールドが定義されている場合にのみ、この部分は利用可能となります。
3. レスpons時間を設定します。レスポンス時間は、良い、普通、悪い、非常に悪いという四つのレベルに分けています。アプリケーションにおけるある TCP トランザクションのレスポンス時間が「非常に悪い」場合、一回のレスポンスタイムアウトとされます。
4.  ボタンをクリックすることで、特徴の定義ダイアログボックスが表示されます。このダイアログボックスで特徴を定義します。

5. 特徴アプリケーションダイアログボックスにおける「OK」をクリックし、解析設定における「OK」をクリックして、特徴アプリケーションの追加を完了します。

特徴の定義のダイアログボックスは下図のように表示されます。



特徴の定義

定義

タイプ:

特徴:

オフセット

スタート位置: エンド位置:

注: オフセット位置はデータセクションから指定する必要があります。

ポート

ポート:

パケット長さ

パケット長さ: byte(s)

プロトコル

プロトコル: TCP UDP

TCPフラグ: URG ACK PSH

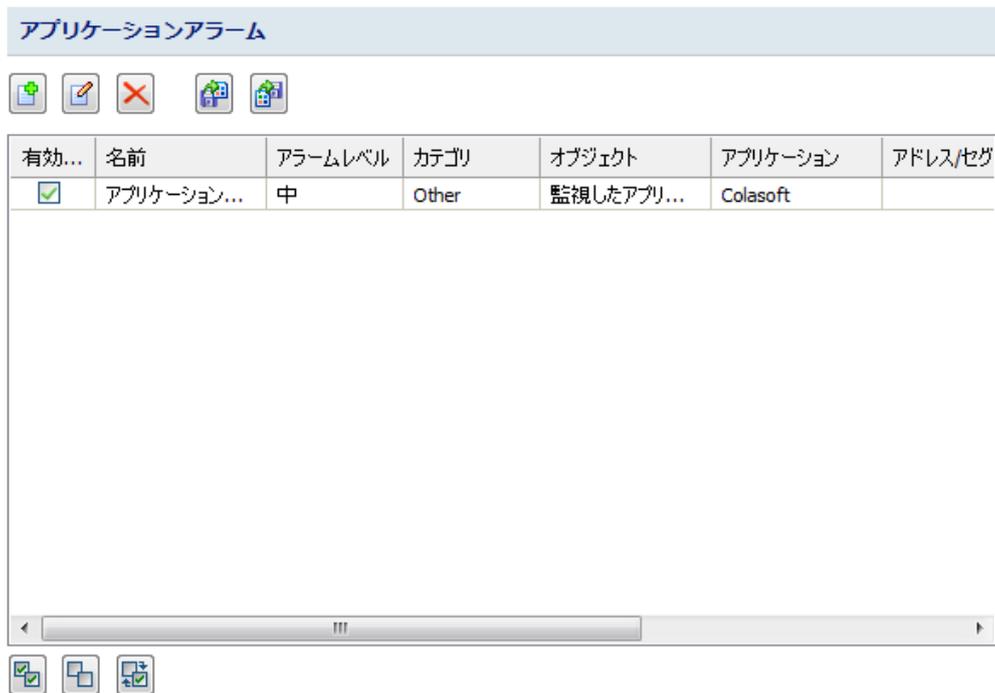
RST SYN FIN

以下のリストは、このダイアログボックスにおける各オプションについて説明しています。

- **タイプ:** パケット特徴のデータタイプを選択します。ASCII と HEX から選択することができます。
- **特徴:** パケットに含まれる特徴を入力します。パケットに設定された特徴が含まれている場合、このパケットは特徴パケットとされています。
- **プロトコル:** データフローのプロトコルを設定します。今は TCP と UDP という二つのプロトコルしかサポートしていません。

アプリケーションアラーム

「アプリケーションパフォーマンス解析」にチェックを入れたアプリケーションに対して、アプリケーションアラームを定義することができます。



注意 アプリケーションアラームを定義する前にカスタムアプリケーションを設定する必要があります。そうでなければ、アプリケーションアラームは利用できません。

このタブには、名前、アラームレベル、カテゴリ、オブジェクト、作成時間、およびア説明などによって定義された全てのアプリケーションアラームが表示されています。

ヒント カラムにはテキストを表示するスペースが十分でないと、カラム間のラインにマウスを移動し、ドラッグすることで、スペースを拡大することができます。

アラームを有効にするには、「有効にする」にチェックを入れる必要があります。

ボタン

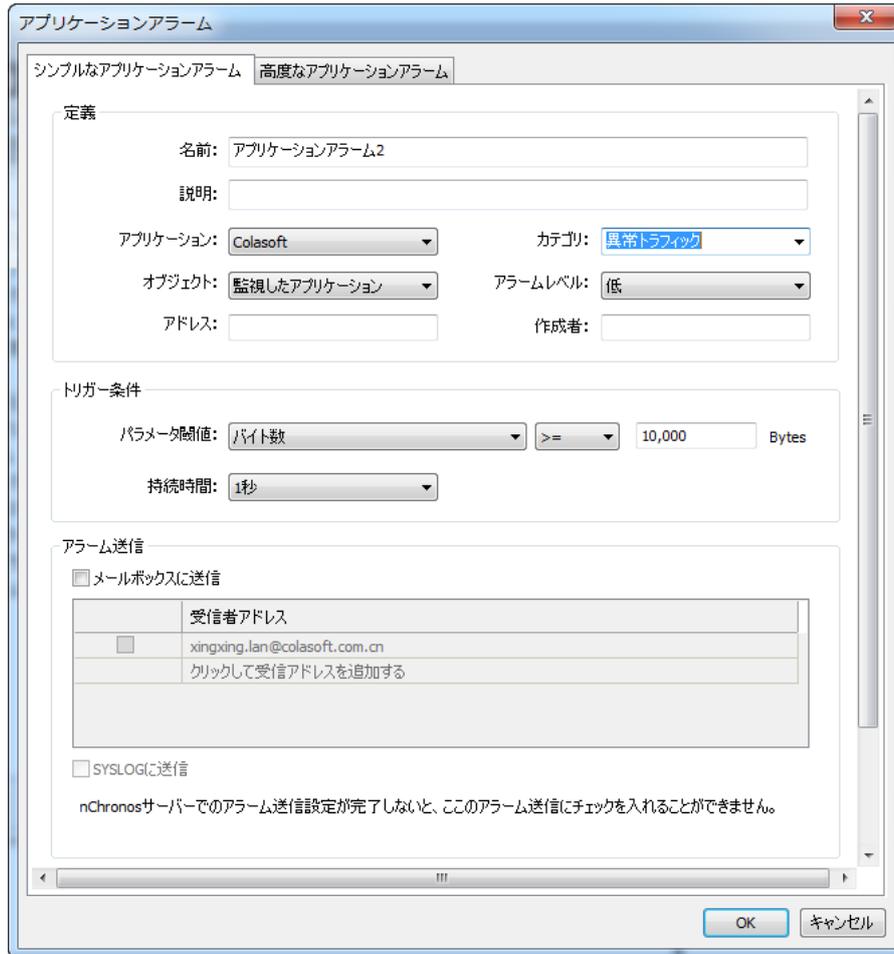
以下のリストはこのタブにおける各ボタンについて説明しています。

- : 新しいアプリケーションアラームを追加します。
- : 選択されたアラームを修正します。
- : 選択されたアラームを削除します。
- : バックアップアプリケーションアラーム設定ファイルをインポートします。
- : 現在のアプリケーションアラームの設定をエクスポートします。

アプリケーションアラームを作成

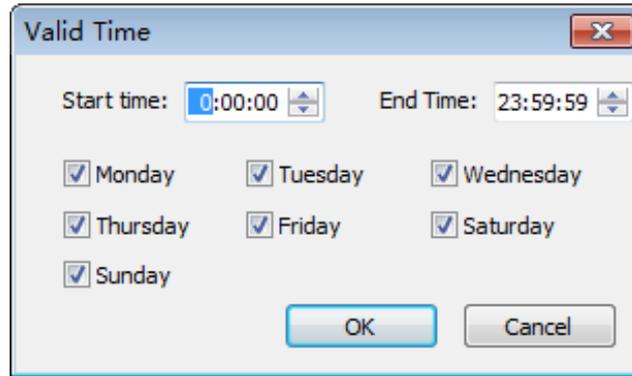
以下のステップに従い、アプリケーションアラームを作成します。

1. アプリケーションアラームタブにおける  をクリックして、アプリケーションアラームダイアログボックスが開かれます。

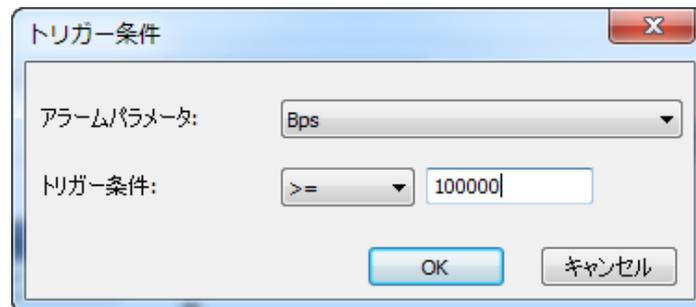


2. アプリケーションアラームダイアログボックスにおける「基本情報」部分の設定を完了します。以下のリストは、この部分の設定について、説明しています。
 - **名前:** 新しいアラームの名前を入力します。
 - **作成者:** このアラームを作成するユーザーを入力します。
 - **説明:** アラームの説明を入力します。
 - **アラームレベル:** 「低」「中」「高」から新しいアラームのレベルを選択します。
 - **カテゴリ:** 新しいアラームのカテゴリを入力するか、小さな三角形をクリックし、ドロップダウンリストからカテゴリを選択します。入力されたカテゴリは、次の使用のために記憶され、またはほかのアラームタイプに使用されることもできます。
 - **タイプ:** 作成しているアラームのタイプを指定します。
 - **アプリケーション:** 作成しているアラームのアプリケーションを選択します。

3. トリガー条件を設定します。「持続時間」パラメータは、トリガー値の統計時間を表します。「トリガー時間範囲を設定」をクリックして、「有効時間」ダイアログボックスが表示され、アラームの有効時間を設定することができます。有効時間を設定したら、アラームは設定された時間範囲以内でのみトリガーされます。「有効時間」ダイアログボックスは下図のように表示されます。



4. 「And」 ボタンまたは「Or」 ボタンをクリックして、トリガー条件を追加します。



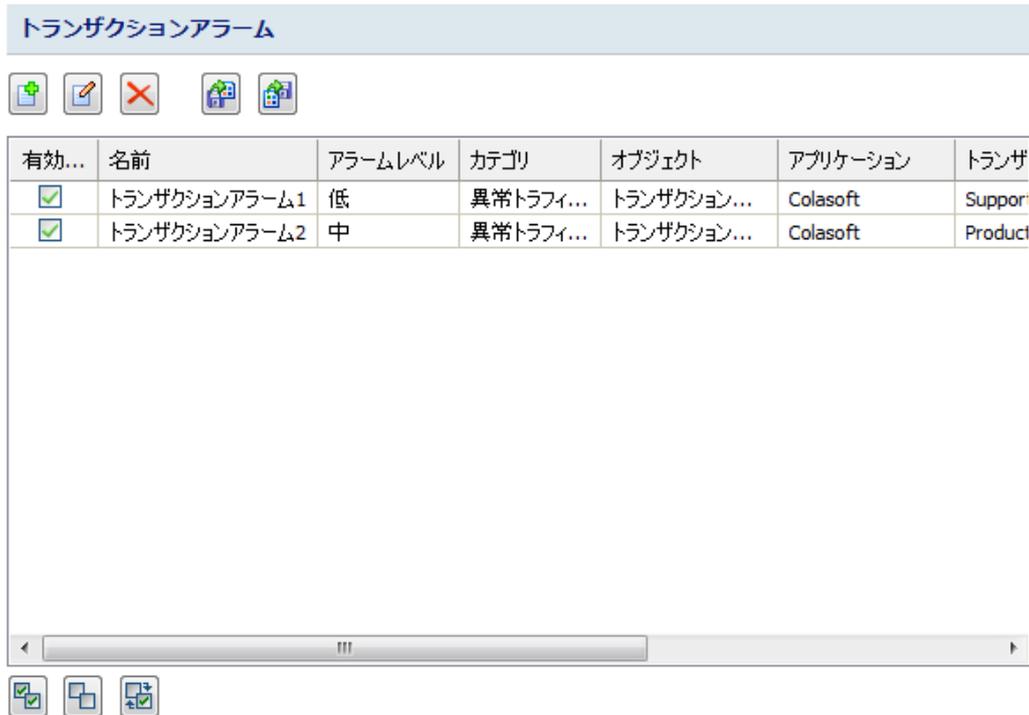
5. アラーム送信についてのパラメータを設定します。
- **Eメール**: アラームがトリガーされた時、Eメールでアラームログを送信します。既存の受信者を選択するか、新しい受信者を入力します。
 - **SYSLOG**: アラームがトリガーされた時、SYSLOG にアラームログを送信します。

nChronos サーバーにおけるアラーム通知の設定が完了しないと、このダイアログボックスにおける「アラーム送信」にチェックを入れることができません。

6. アプリケーションアラームダイアログボックスにおける「OK」をクリックし、アプリケーションアラームタブにおける「OK」をクリックします。

トランザクションアラーム

このタブは、トランザクション解析を有効にしているアプリケーションにおいて、トランザクションアラームを定義するために設けられています。このタブは、下図のように表示されます。



注意 トランザクションアラームを定義する前に、まず Web アプリケーションを設定し、その Web アプリケーションのトランザクション解析を有効にする必要があります。

このタブには、名前、アラームレベル、カテゴリ、タイプ、説明、作成時間などによって定義された全てのトランザクションアラームが表示されます。

ヒント カラムにはテキストを表示するスペースが十分でないと、カラム間のラインにマウスを移動し、ドラッグすることで、スペースを拡大することができます。

アラームを有効にするには、「有効にする」にチェックを入れる必要があります。

ボタン

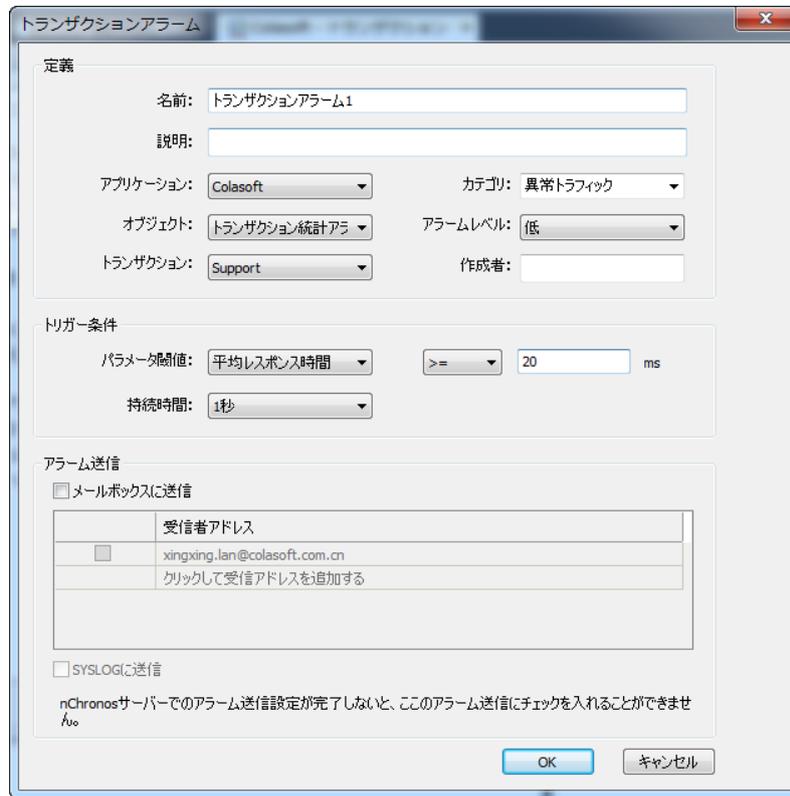
以下のリストは、このタブにおける各アイコンボタンについて説明しています。

- : 新しいトランザクションアラームを追加します。
- : 選択されたアラームを修正します。
- : 選択されたアラームを削除します。
- : バックアップされたトランザクションアラーム設定ファイルをインポートします。
- : 現在のトランザクションアラームの設定をエクスポートします。

トランザクションアラームを追加する

以下のステップに従い、トランザクションアラームを追加します。

1.  をクリックして、下図のようにトランザクションアラームダイアログボックスを開きます。



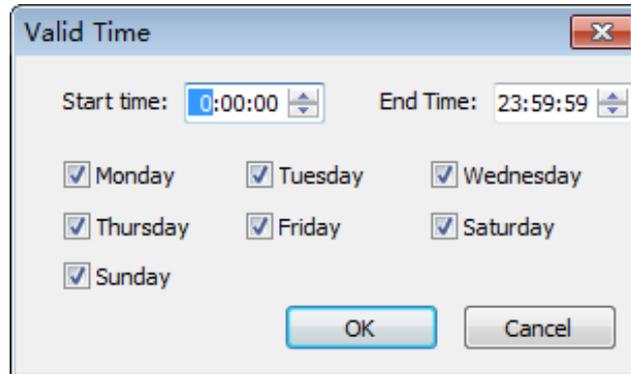
The dialog box is titled "トランザクションアラーム" (Transaction Alarm). It contains the following sections:

- 定義 (Definition):**
 - 名前 (Name): トランザクションアラーム1
 - 説明 (Description):
 - アプリケーション (Application): Colasoft
 - カテゴリ (Category): 異常トラフィック
 - オブジェクト (Object): トランザクション統計アラ
 - アラームレベル (Alarm Level): 低
 - トランザクション (Transaction): Support
 - 作成者 (Creator):
- トリガー条件 (Trigger Condition):**
 - パラメータ閾値 (Parameter Threshold): 平均レスポンス時間
 - 比較演算子 (Operator): >=
 - 値 (Value): 20
 - 単位 (Unit): ms
 - 持続時間 (Duration): 1秒
- アラーム送信 (Alarm Delivery):**
 - メールボックスに送信
 - 受信者アドレス (Recipient Address):
 - xingxing.lan@colasoft.com.cn
 - クリックして受信アドレスを追加する
 - SYSLOGに送信

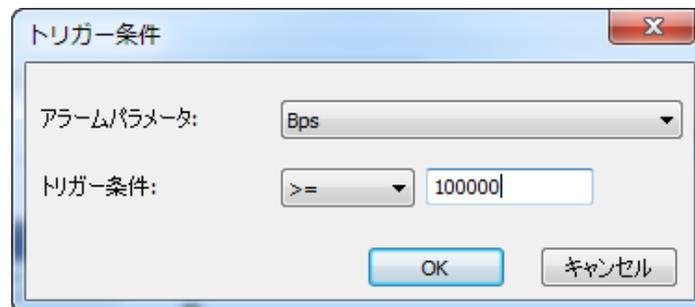
At the bottom, there is a note: "nChronosサーバーでのアラーム送信設定が完了しないと、このアラーム送信にチェックを入れることができません。" (If the alarm delivery setting on the nChronos server is not completed, you cannot check this alarm delivery.)

2. トランザクションアラームダイアログボックスにおいて、「基本情報」部分の設定を完了します。以下のリスト、「基本情報」部分の設定について説明しています。
 - **名前:** 新しいアラームの名前を入力します。
 - **作成者:** このアラームを作成するユーザーを入力します。
 - **説明:** アラームについての説明を入力します。
 - **アラームレベル:** 「低」「中」「高」から新しいアラームのレベルを選択します。
 - **カテゴリ:** 新しいアラームのカテゴリを入力するか、小さな三角形をクリックし、ドロップダウンリストからカテゴリを選択します。入力されたカテゴリは、次の使用のために記憶され、またはほかのアラームタイプに使用されることもできます。
 - **タイプ:** トランザクション統計アラームとトランザクションログアラームからアラームのタイプを指定します。
 - **アプリケーション:** アプリケーションを一つ選択します。ここに提供されるアプリケーションは、解析設定でトランザクション解析を有効している Web アプリケーションです。
 - **トランザクション:** 具体的なトランザクションを選択します。
3. トリガー条件を設定します。「持続時間」パラメータは、トリガー値の統計時間を表します。「トリガー時間範囲を設定」をクリックして、「有効時間」ダイアログボッ

クスが表示され、アラームの有効時間を設定することができます。有効時間を設定したら、アラームは設定された時間範囲以内でのみトリガーされます。「有効時間」ダイアログボックスは下図のように表示されます。



4. 「And」 ボタンまたは「Or」 ボタンをクリックして、トリガー条件を追加します。



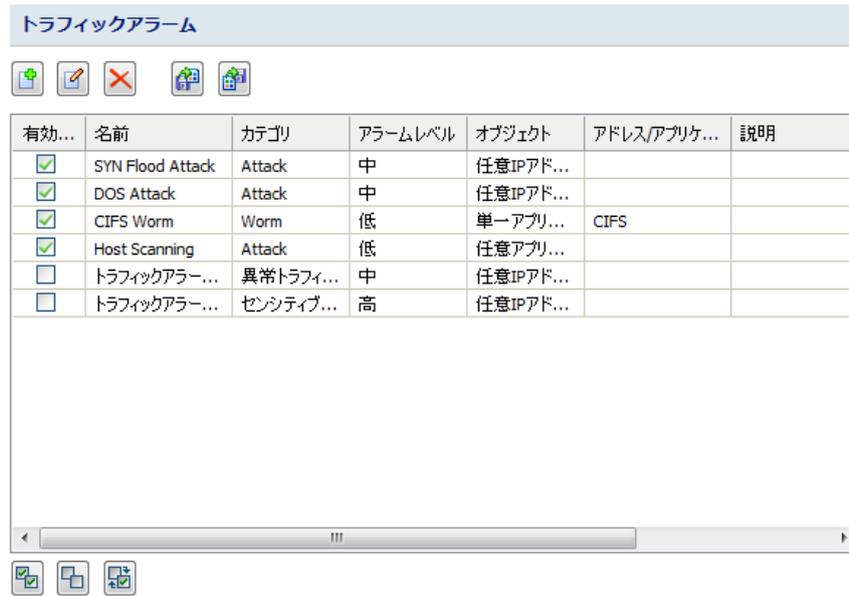
5. アラーム送信についてのパラメータを設定します。
 - **Eメール**: アラームがトリガーされた時、Eメールでアラームログを送信します。既存の受信者を選択するか、新しい受信者を入力します。
 - **SYSLOG**: アラームがトリガーされた時、SYSLOG にアラームログを送信します。

nChronos サーバーにおけるアラーム通知の設定が完了しないと、このダイアログボックスにおける「アラーム送信」にチェックを入れることができません。

6. トランザクションアラームダイアログボックスにおける「OK」をクリックし、トランザクションアラームタブにおける「OK」をクリックします。

トラフィックアラーム

このタブは、パケット、バイト数、および平均パケットサイズを含む、ネットワークトラフィックのアラームを設定するために設けられています。アラーム条件と一致したトラフィックをキャプチャーした時、トラフィックアラームがトリガーされます。このタブは下図のように表示されます。



ヒント カラムにはテキストを表示するスペースが十分でないと、カラム間のラインにマウスを移動し、ドラッグすることで、スペースを拡大することができます。

アラームを有効にするには、「有効にする」にチェックを入れる必要があります。

ボタン

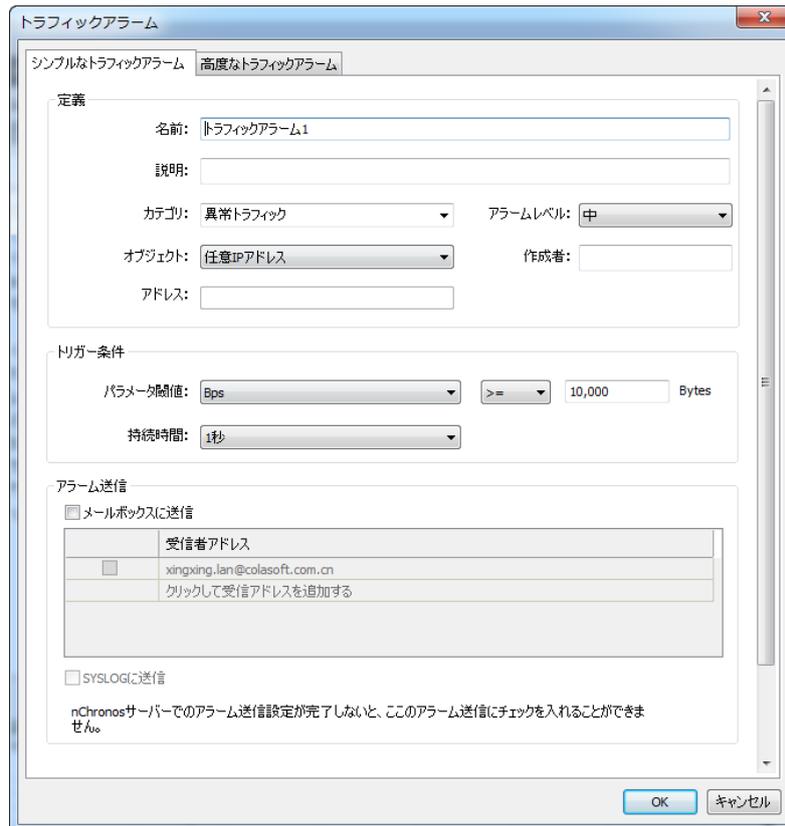
以下のリストは、このタブにおける各アイコンボタンについて説明しています。

- : 新しいトラフィックアラームを追加します。
- : 選択されたアラームを修正します。
- : 選択されたアラームを削除します。
- : 保存されたトラフィックアラームの設定ファイルをインポートします。
- : 現在のトラフィックアラームの設定をエクスポートします。

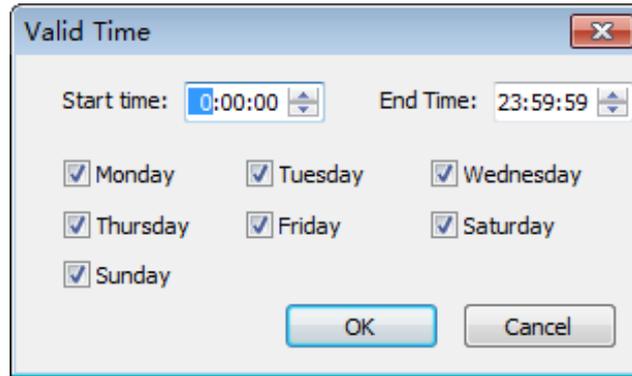
トラフィックアラームを作成

以下のステップに従い、トラフィックアラームを作成します。

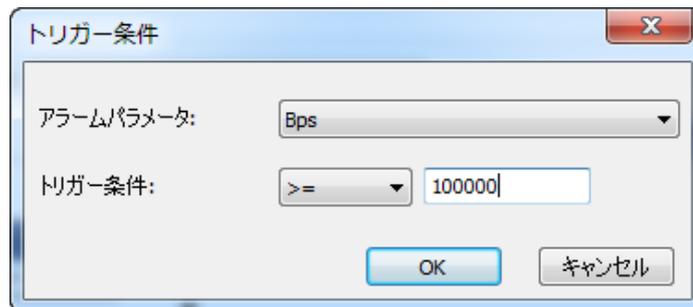
1. トラフィックアラームタブにおける  をクリックして、下図のようにトラフィックアラームダイアログボックスが開かれます。



2. トラフィックアラームダイアログボックスにおいて、「基本情報」部分の設定を完了します。以下のリストは、「基本情報」部分の設定について説明しています。
 - **名前:**新しいアラームの名前を入力します。
 - **作成者:**このアラームを作成するユーザーを入力します。
 - **説明:**アラームについての説明を入力します。
 - **カテゴリ:**新しいアラームのカテゴリを入力するか、小さな三角形をクリックし、ドロップダウンリストからカテゴリを選択します。入力されたカテゴリは、次の使用のために記憶され、またはほかのアラームタイプに使用されることもできます。
 - **タイプ:**作成しているアラームのタイプを指定します。
 - **アラームレベル:**「低」「中」「高」から新しいアラームのレベルを選択します。
3. トリガー条件を設定します。「持続時間」パラメータは、トリガー値の統計時間を表します。「トリガー時間範囲を設定」をクリックして、「有効時間」ダイアログボックスが表示され、アラームの有効時間を設定することができます。有効時間を設定したら、アラームは設定された時間範囲以内でのみトリガーされます。「有効時間」ダイアログボックスは下図のように表示されます。



4. 「And」 ボタンまたは「Or」 ボタンをクリックして、トリガー条件を追加します。



5. アラーム送信についてのパラメータを設定します。
- **Eメール:** アラームがトリガーされた時、Eメールでアラームログを送信します。
 - **SYSLOG:** アラームがトリガーされた時、SYSLOG にアラームログを送信します。

nChronos サーバーにおけるアラーム通知の設定が完了しないと、このダイアログボックスにおける「アラーム送信」にチェックを入れることができません。

6. トラフィックアラームダイアログボックスにおける「OK」をクリックし、トラフィックアラームタブにおける「OK」をクリックします。

ミリ秒におけるトラフィックアラーム

このタブはミリ秒におけるトラフィックアラームを定義するために設けられています。トラフィックアラームは、秒におけるトラフィックを統計しているのに対して、ミリ秒におけるトラフィックアラームは、ミリ秒におけるトラフィックを統計しています。

ミリ秒におけるトラフィックアラーム







有効...	名前	アラームレベル	カテゴリ	作成時間	作成者
<input type="checkbox"/>	ミリ秒におけるトラフィックアラーム1	低	異常トラフィック	2015/04/14 16:29:11	
<input type="checkbox"/>	ミリ秒におけるトラフィックアラーム2	中	センシティブ情報	2015/04/14 16:29:11	
<input type="checkbox"/>	ミリ秒におけるトラフィックアラーム3	高	異常トラフィック	2015/04/14 16:29:11	





このタブには、名前、アラームレベル、カテゴリ、説明、および作成時間などによって定義された全てのミリ秒におけるトラフィックアラームが表示されています。

ヒント カラムにはテキストを表示するスペースが十分でないと、カラム間のラインにマウスを移動し、ドラッグすることで、スペースを拡大することができます。

アラームを有効にするには、「有効にする」にチェックを入れる必要があります。

ボタン

以下のリストは、このタブにおける各アイコンボタンについて説明しています。

- : 新しいミリ秒におけるトラフィックアラームを追加します。
- : 選択されたアラームを修正します。
- : 選択されたアラームを削除します。
- : バックアップされたアラーム設定ファイルをインポートします。
- : 現在のアラーム設定をエクスポートします。

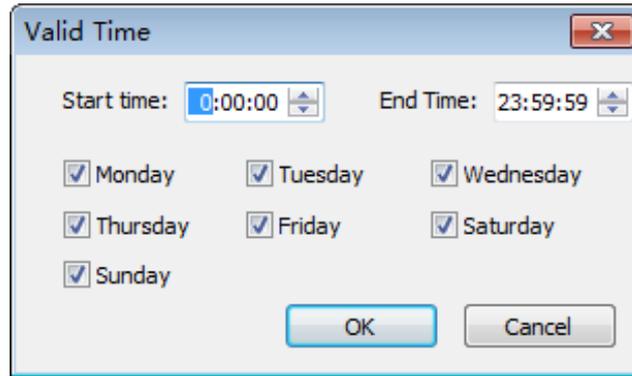
ミリ秒におけるトラフィックアラームを追加する

以下のステップに従い、トランザクションアラームを追加します。

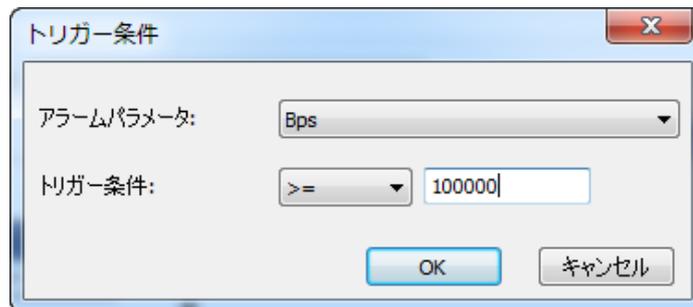
1.  をクリックして、下図のようにミリ秒におけるトラフィックアラームダイアログボックスを開きます。

2. ミリ秒におけるトラフィックアラームダイアログボックスにおいて、「基本情報」部分を完了します。以下のリスト、「基本情報」部分の設定について説明しています。
 - **名前:** 新しいアラームの名前を入力します。
 - **作成者:** このアラームを作成するユーザーを入力します。
 - **説明:** アラームについての説明を入力します。
 - **カテゴリ:** 新しいアラームのカテゴリを入力するか、小さな三角形をクリックし、ドロップダウンリストからカテゴリを選択します。入力されたカテゴリは、次の使用のために記憶され、またはほかのアラームタイプに使用されることもできます。
 - **タイプ:** 作成しているアラームのタイプを指定します。
 - **アラームレベル:** 「低」「中」「高」から新しいアラームのレベルを選択します。

3. トリガー条件を設定します。「持続時間」パラメータは、トリガー値の統計時間を表します。「トリガー時間範囲を設定」をクリックして、「有効時間」ダイアログボックスが表示され、アラームの有効時間を設定することができます。有効時間を設定したら、アラームは設定された時間範囲以内でのみトリガーされます。「有効時間」ダイアログボックスは下図のように表示されます。



4. 「And」 ボタンまたは「Or」 ボタンをクリックして、トリガー条件を追加します。



5. アラーム送信についてのパラメータを設定します。
- **Eメール**: アラームがトリガーされた時、Eメールでアラームログを送信します。既存の受信者を選択するか、新しい受信者を入力します。
 - **SYSLOG**: アラームがトリガーされた時、SYSLOG にアラームログを送信します。

nChronos サーバーにおけるアラーム通知の設定が完了しないと、このダイアログボックスにおける「アラーム送信」にチェックを入れることができません。

6. ミリ秒におけるトラフィックアラームダイアログボックスにおける「OK」をクリックし、ミリ秒におけるトラフィックアラームタブにおける「OK」をクリックします。

注意 nChronos サーバーでネットワークリンクを追加する時、ミリ秒におけるトラフィック統計を有効にしないと、ここでミリ秒におけるトラフィックアラームを設定することができません。

E メールアラーム

このタブは下図のように表示されます。



ユーザーはネットワーク上のEメールを対象に、Eメールアラームを作成することができます。Eメールに定義されているキーワードが含まれている場合、Eメールアラームがトリガーされます。

ボタン

以下のリストはこのタブにおける各アイコンボタンについて説明しています。

- : 新しいEメールアラームを追加します。
- : 選択されたアラームを修正します。
- : 選択されたアラームを削除します。
- : 保存されたEメールアラームの設定ファイルをインポートします。
- : 現在のEメールアラームの設定をエクスポートします。

カラム

以下のリストは、このタブにおけるカラムについて説明しています。

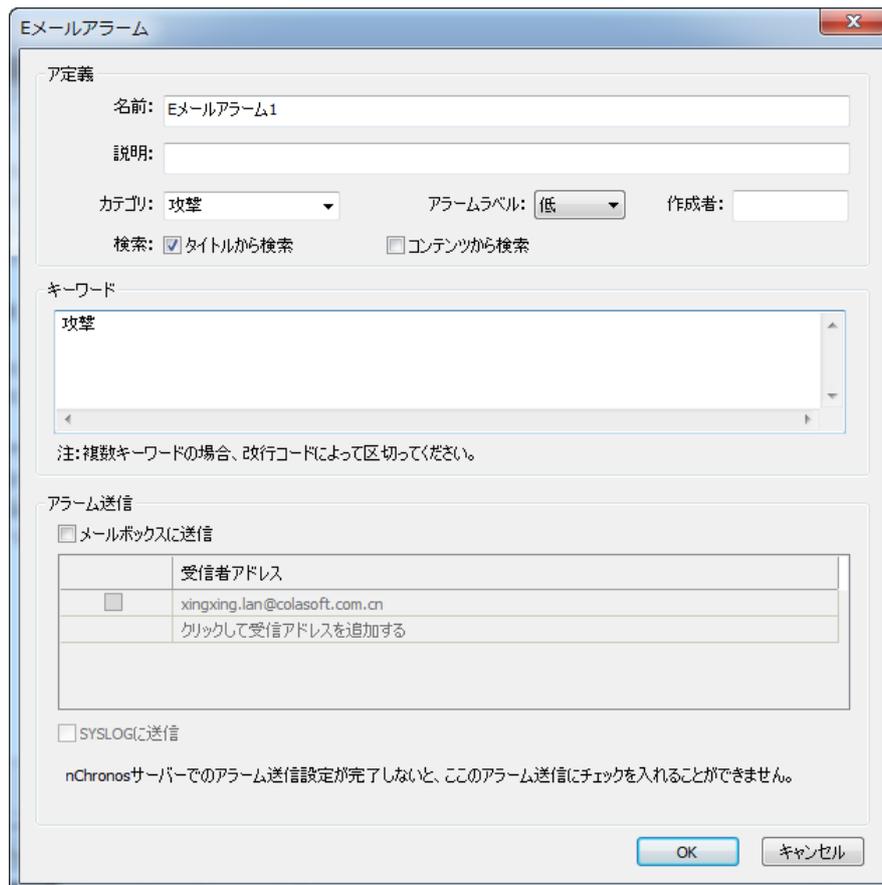
- **有効にする**: 定義されたEメールアラームを有効にするかどうかを選択します。
- **名前**: アラームの名前を表示します。
- **カテゴリ**: アラームのカテゴリを表示します。
- **オブジェクト**: アラームのオブジェクトを表示します。
- **アラームレベル**: アラームのレベルを表示します。
- **作成時間**: Eメールアラームの作成時間を表示します。
- **説明**: アラームについての説明を表示します。

ヒント カラムにはテキストを表示するスペースが十分でないと、カラム間のラインにマウスを移動し、ドラッグすることで、スペースを拡大することができます。

E メールアラームを作成する

以下のステップに従い、E メールアラームを作成します。

1. E メールアラームタブにおける  をクリックして、E メールアラームダイアログボックスを開きます。



ダイアログボックス「Eメールアラーム」のスクリーンショット。以下の設定が確認できます。

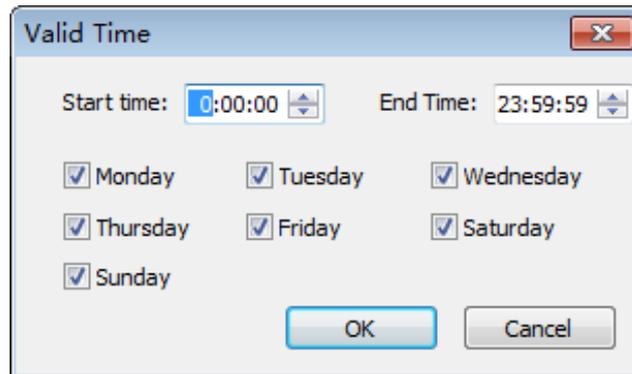
- ア定義**
 - 名前: Eメールアラーム1
 - 説明: (空)
 - カテゴリ: 攻撃
 - アラームレベル: 低
 - 作成者: (空)
 - 検索: タイトルから検索 コンテンツから検索
- キーワード**
 - 攻撃
 - 注: 複数キーワードの場合、改行コードによって区切ってください。
- アラーム送信**
 - メールボックスに送信

	受信者アドレス
<input type="checkbox"/>	xingxing.lan@colasoft.com.cn
	クリックして受信アドレスを追加する
 - SYSLOGに送信

ボタンの状態: OK (有効), キャンセル (有効)

2. E メールアラームダイアログボックスにおいて、「基本情報」部分の設定を完了します。以下のリスト、「基本情報」部分の設定について説明しています。
 - **名前:** 新しいアラームの名前を入力します。
 - **作成者:** このアラームを作成するユーザーを入力します。
 - **説明:** 新しいアラームについての説明を入力します。
 - **カテゴリ:** 新しいアラームのカテゴリを入力するか、小さな三角形をクリックし、ドロップダウンリストからカテゴリを選択します。入力されたカテゴリは、次の使用のために記憶され、またはほかのアラームタイプに使用されることもできます。
 - **アラームレベル:** 「低」「中」「高」から新しいアラームのレベルを選択します。
3. 「トリガー時間範囲を設定」をクリックして、「有効時間」ダイアログボックスが表示され、アラームの有効時間を設定することができます。有効時間を設定したら、アラームは設定された時間範囲以内でのみトリガーされます。

「有効時間」ダイアログボックスは下図のように表示されます。

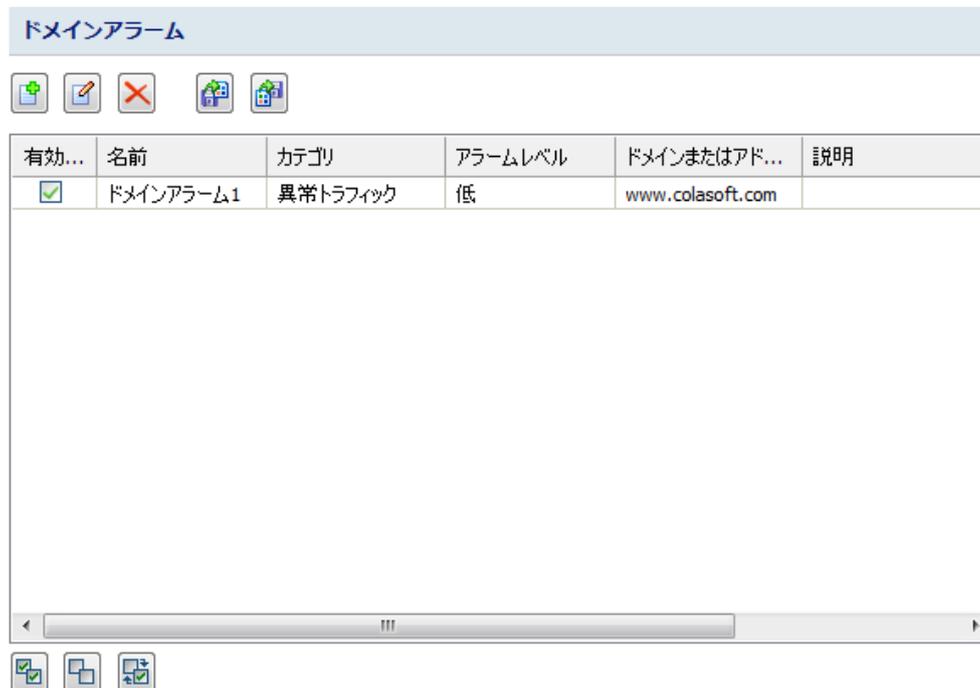


4. Eメールアラームをとリーガーするキーワードを入力します。一つのEメールアラームには、改行コードによって、複数のキーワードを入力することができます。
5. タイトルから検索するかコンテンツから検索するかを選択します。
 - **タイトルから検索する:** このオプションにチェックを入れると、タイトルだけからアラームをトリガーするキーワードを検索します。
 - **コンテンツから検索する:** このオプションにチェックを入れると、コンテンツだけからアラームをトリガーするキーワードを検索します。
6. アラーム送信についてのパラメータを設定します。
 - **Eメール:** アラームがトリガーされた時、Eメールでアラームログを送信します。既存の受信者を選択するか、新しい受信者を入力します。
 - **SYSLOG:** アラームがトリガーされた時、SYSLOG にアラームログを送信します。

nChronos サーバーにおけるアラーム通知の設定が完了しないと、このダイアログボックスにおける「アラーム送信」にチェックを入れることができません。
7. Eメールアラームダイアログボックスにおける「OK」をクリックし、Eメールアラームタブにおける「OK」をクリックします。

ドメインアラーム

このタブは下図のように表示されます。



ネットワークを介して訪問されたドメイン名を対象に、ドメインアラームを作成することができます。定義されたドメインが訪問される時、ドメインアラームはトリガーされます。

ボタン

以下のリストは、このタブにおける各アイコンボタンについて説明しています。

- : 新しいドメインアラームを追加します。
- : 選択されたアラームを修正します。
- : 選択されたアラームを削除します。
- : 保存されたドメインアラームの設定ファイルをインポートします。
- : 現在のドメインアラームの設定をエクスポートします。

カラム

以下のリストはこのタブにおけるカラムについて説明しています。

- **有効にする**: 定義されたドメインアラームを有効にするかどうかを選択します。
- **名前**: アラームの名前を表示します。
- **カテゴリ**: アラームのカテゴリを表示します。
- **オブジェクト**: アラームのオブジェクトを表示します。
- **アラームレベル**: アラームのレベルを表示します。
- **作成時間**: Eメールアラームの作成時間を表示します。
- **説明**: アラームについての説明を表示します。

ヒント カラムにはテキストを表示するスペースが十分でないと、カラム間のラインにマウスを移動し、ドラッグすることで、スペースを拡大することができます。

ドメインアラームを作成する

以下のステップに従い、ドメインアラームを作成します。

1. ドメインアラームタブにおける  をクリックして、ドメインアラームダイアログボックスを開きます。



ドメインアラーム

定義

名前:

説明:

カテゴリ: アラームレベル: 作成者:

ドメイン名またはIPアドレス

注: 1. ドメインは**入力をサポートしています(**は0または複数の文字を表しています)。
2. IPアドレスは、DNS名前解決で変換されたIPアドレスを指します。
3. 一行には一つのドメインまたはIPアドレスしか入力できません。複数の場合、改行コードによって区切ってください。

アラーム送信

メールボックスに送信

	受信者アドレス
<input type="checkbox"/>	xingxing.lan@colasoft.com.cn
	クリックして受信アドレスを追加する

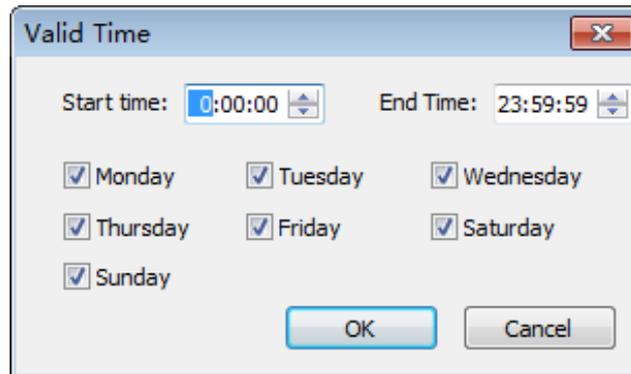
SYSLOGに送信

nChronosサーバーでのアラーム送信設定が完了しないと、このアラーム送信にチェックを入れることができません。

OK キャンセル

2. ドメインアラームダイアログボックスにおいて、「定義」部分の設定を完了します。以下のリスト、「定義」部分の設定について説明しています。
 - ・ **名前:** 新しいアラームの名前を入力します。
 - ・ **作成者:** このアラームを作成するユーザーを入力します。
 - ・ **説明:** 新しいアラームについての説明を入力します。
 - ・ **カテゴリ:** 新しいアラームのカテゴリを入力するか、小さな三角形をクリックし、ドロップダウンリストからカテゴリを選択します。入力されたカテゴリは、次の使用のために記憶され、またはほかのアラームタイプに使用されることもできます。
 - ・ **アラームレベル:** 「低」「中」「高」から新しいアラームのレベルを選択します。
3. 「トリガー時間範囲を設定」をクリックして、「有効時間」ダイアログボックスが表示され、アラームの有効時間を設定することができます。有効時間を設定したら、アラームは設定された時間範囲以内でのみトリガーされます。

「有効時間」ダイアログボックスは下図のように表示されます。



4. ドメイン、またはアドレスを入力します。ドメイン名とアドレスは、ドメインアラームのトリガー条件です。一つのドメインアラームには、改行コードによって、複数のドメインとアドレスを入力することができます。
5. アラーム送信についてのパラメータを設定します。

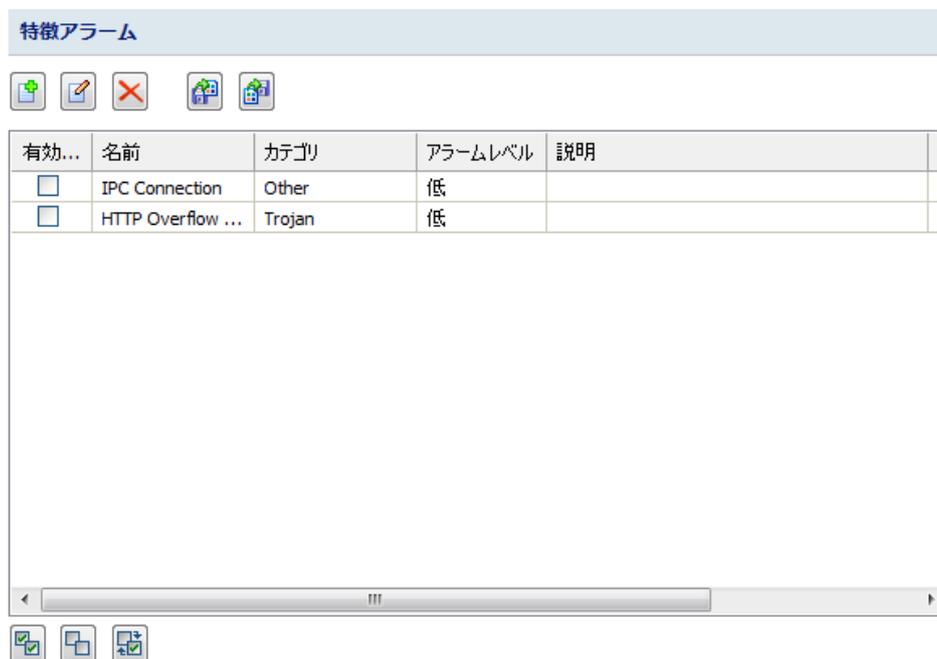
- **Eメール:** アラームがトリガーされた時、Eメールでアラームログを送信します。
- **SYSLOG:** アラームがトリガーされた時、SYSLOG にアラームログを送信します。

nChronos サーバーにおけるアラーム通知の設定が完了しないと、このダイアログボックスにおける「アラーム送信」にチェックを入れることができません。

6. ドメインアラームダイアログボックスにおける「OK」をクリックし、ドメインアラームタブにおける「OK」をクリックします。

特徴アラーム

このタブは以下のように表示されます。



ネットワークにおけるデータフローのために特徴アラームを設定することができます。定義されたデータフローがキャプチャーされると、特徴アラームはトリガーされます。

ボタン

以下のリストは、このタブにおける各アイコンボタンについて説明しています。



: 新しい特徴アラームを追加します。



: 選択されたアラームを修正します。



: 選択されたアラームを削除します。



: 保存された特徴アラームの設定ファイルをインポートします。



: 現在の特徴アラームの設定をエクスポートします。

カラム

以下のリストはこのタブにおけるカラムについて説明しています。

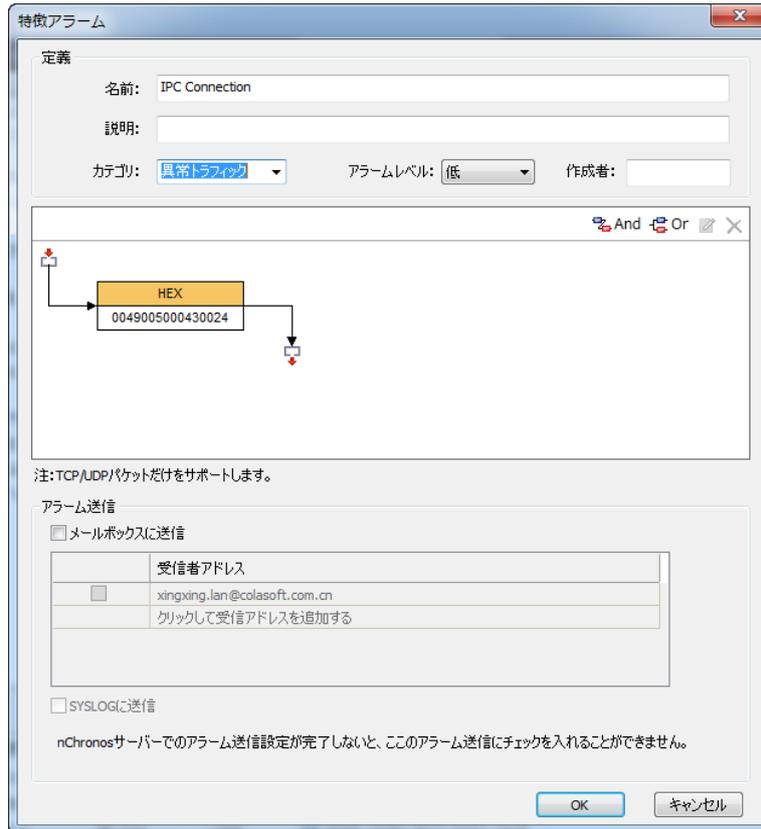
- **有効にする**: 定義された特徴アラームを有効にするかどうかを選択します。
- **名前**: アラームの名前を表示します。
- **カテゴリ**: アラームのカテゴリを表示します。
- **オブジェクト**: アラームのオブジェクトを表示します。
- **アラームレベル**: アラームのレベルを表示します。
- **作成時間**: Eメールアラームの作成時間を表示します。
- **説明**: アラームについての説明を表示します。

ヒント カラムにはテキストを表示するスペースが十分でないと、カラム間のラインにマウスを移動し、ドラッグすることで、スペースを拡大することができます。

特徴アラームを作成する

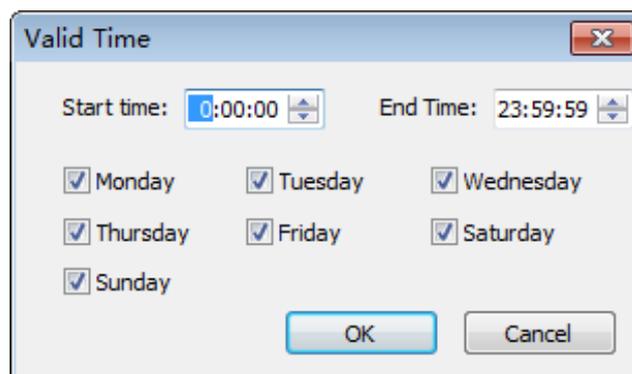
以下のステップに従い、特徴アラームを作成します。

1. 特徴アラームタブにおける  をクリックして、特徴アラームダイアログボックスを開きます。



2. 特徴アラームダイアログボックスにおいて、「基本情報」部分の設定を完了します。以下のリスト、「基本情報」部分の設定について説明しています。
 - **名前:** 新しいアラームの名前を入力します。
 - **作成者:** このアラームを作成するユーザーを入力します。
 - **説明:** 新しいアラームについての説明を入力します。
 - **カテゴリ:** 新しいアラームのカテゴリを入力するか、小さな三角形をクリックし、ドロップダウンリストからカテゴリを選択します。入力されたカテゴリは、次の使用のために記憶され、またはほかのアラームタイプに使用されることもできます。
 - **アラームレベル:** 「低」「中」「高」から新しいアラームのレベルを選択します。

3. 「トリガー時間範囲を設定」をクリックして、「有効時間」ダイアログボックスが表示され、アラームの有効時間を設定することができます。有効時間を設定したら、アラームは設定された時間範囲以内でのみトリガーされます。「有効時間」ダイアログボックスは下図のように表示されます。



4.  ボタンをクリックすることで、下図のように特徴の定義ダイアログボックスが表示されます。このダイアログボックスでアラームをトリガーする特徴を定義します。

以下のリストは、このダイアログボックスにおける各オプションについて説明しています。

- **タイプ:** パケット特徴のデータタイプを選択します。ASCII と HEX から選択することができます。
 - **特徴:** パケットに含まれる特徴を入力します。パケットに設定された特徴が含まれている場合、このパケットは特徴パケットとされています。
 - **プロトコル:** データフローのプロトコルを設定します。今は TCP と UDP という二つのプロトコルしかサポートしていません。
5. アラーム送信についてのパラメータを設定します。
- **Eメール:** アラームがトリガーされた時、Eメールでアラームログを送信します。既存の受信者を選択するか、新しい受信者を入力します。
 - **SYSLOG:** アラームがトリガーされた時、SYSLOG にアラームログを送信します。
- nChronos サーバーにおけるアラーム通知の設定が完了しないと、このダイアログボックスにおける「アラーム送信」にチェックを入れることができません。
6. 特徴アラームダイアログボックスにおける「OK」をクリックし、特徴アラームタブにおける「OK」をクリックします。

リンク解析

リンク解析タブでは、リンク解析における統計ビューを表示または非表示に設定することができます。そして、統計ビューの表示する順序を変更することもできます。リンク解析タブは下図のように表示されます。

Link Retrospective Analysis








Enable	Name	Object
<input checked="" type="checkbox"/>	Summary	default
<input checked="" type="checkbox"/>	MAC Address	default
<input checked="" type="checkbox"/>	MAC Conversation	default
<input checked="" type="checkbox"/>	Network Segment	default
<input checked="" type="checkbox"/>	Application	default
<input checked="" type="checkbox"/>	IP Address	default
<input checked="" type="checkbox"/>	IP Conversation	default
<input checked="" type="checkbox"/>	TCP Conversation	default
<input checked="" type="checkbox"/>	UDP Conversation	default
<input checked="" type="checkbox"/>	Statistics Between Segments	default
<input checked="" type="checkbox"/>	Service Access	default
<input checked="" type="checkbox"/>	Port	default
<input checked="" type="checkbox"/>	Link Alarm	default





ボタン

以下のリストは、このタブにおけるアイコンについて説明しています。

- : 選択された統計ビューを削除します。システムデフォルトのビューは削除できません。カスタムビューだけ削除できます。
- : 選択された統計ビューの名前とフィルター条件を修正します。システムデフォルトのビューは修正できません。カスタムビューだけ修正できます。
- : 保存された設定ファイルを現在のタブにインポートします。
- : このタブにおける統計ビューの設定ファイルをローカルにエクスポートします。エクスポートされた設定ファイルは他のネットワークリンクにインポートすることもできます。
- : 選択された統計ビューの位置を前に移動します。
- : 選択された統計ビューの位置を後に移動します。

ミリ秒解析

ミリ秒解析タブでは、ミリ秒解析における統計ビューを表示または非表示に設定することができます。そして、統計ビューの表示する順序を変更することもできます。ミリ秒解析タブは下図のように表示されます。

Millisecond Analysis









Enable	Name	Object
<input checked="" type="checkbox"/>	Summary	default
<input checked="" type="checkbox"/>	Millisecond Traffic Alarms	default





ボタン

以下のリストは、このタブにおけるアイコンについて説明しています。

- : 選択された統計ビューを削除します。システムデフォルトのビューは削除できません。カスタムビューだけ削除できます。
- : 選択された統計ビューの名前とフィルター条件を修正します。システムデフォルトのビューは修正できません。カスタムビューだけ修正できます。
- : 保存された設定ファイルを現在のタブにインポートします。
- : このタブにおける統計ビューの設定ファイルをローカルにエクスポートします。エクスポートされた設定ファイルは他のネットワークリンクにインポートすることもできます。
- : 選択された統計ビューの位置を前に移動します。
- : 選択された統計ビューの位置を後に移動します。

注意 nChronos サーバーでネットワークリンクを追加する時、ミリ秒におけるトラフィック統計を有効にしないと、このタブを利用することができません。

アラーム

アラームタブでは、アラームウィンドウにおける統計ビューを表示または非表示に設定することができます。そして、統計ビューの表示順序を変更することもできます。アラームタブは下図のように表示されます。

Alarms









Enable	Name	Object
<input checked="" type="checkbox"/>	All Alarms	default
<input checked="" type="checkbox"/>	Link Alarm	default
<input checked="" type="checkbox"/>	Application Alarms	default
<input checked="" type="checkbox"/>	Transaction Alarms	default





ボタン

以下のリストは、このタブにおけるアイコンについて説明しています。

- : 選択された統計ビューを削除します。システムデフォルトのビューは削除できません。カスタムビューだけ削除できます。
- : 選択された統計ビューの名前とフィルター条件を修正します。システムデフォルトのビューは修正できません。カスタムビューだけ修正できます。
- : 保存された設定ファイルを現在のタブにインポートします。
- : このタブにおける統計ビューの設定ファイルをローカルにエクスポートします。エクスポートされた設定ファイルは他のネットワークリンクにインポートすることもできます。
- : 選択された統計ビューの位置を前に移動します。
- : 選択された統計ビューの位置を後に移動します。

アプリケーションパフォーマンス解析

アプリケーションパフォーマンス解析タブでは、アプリケーションパフォーマンス解析における統計ビューを表示または非表示に設定することができます。そして、統計ビューの表示順序を変更することもできます。アラームタブは下図のように表示されます。

Application Performance Analysis









Enable	Name	Object
<input checked="" type="checkbox"/>	Client	default
<input checked="" type="checkbox"/>	Server	default
<input checked="" type="checkbox"/>	Network Segment	default
<input checked="" type="checkbox"/>	IP Conversation	default
<input checked="" type="checkbox"/>	TCP Conversation	default
<input checked="" type="checkbox"/>	Application Alarms	default
<input checked="" type="checkbox"/>	Packet Size Distribution	default





ボタン

以下のリストは、このタブにおけるアイコンについて説明しています。

- : 選択された統計ビューを削除します。システムデフォルトのビューは削除できません。カスタムビューだけ削除できます。
- : 選択された統計ビューの名前とフィルター条件を修正します。システムデフォルトのビューは修正できません。カスタムビューだけ修正できます。
- : 保存された設定ファイルを現在のタブにインポートします。
- : このタブにおける統計ビューの設定ファイルをローカルにエクスポートします。エクスポートされた設定ファイルは他のネットワークリンクにインポートすることもできます。
- : 選択された統計ビューの位置を前に移動します。
- : 選択された統計ビューの位置を後に移動します。

アプリケーショントランザクション解析

アプリケーショントランザクション解析タブでは、アプリケーショントランザクション解析における統計ビューを表示または非表示に設定することができます。そして、統計ビューの表示順序を変更することもできます。アラームタブは下図のように表示されます。

Application Transaction Analysis









Enable	Name	Object
<input checked="" type="checkbox"/>	Transaction	default
<input checked="" type="checkbox"/>	Client	default
<input checked="" type="checkbox"/>	Server	default
<input checked="" type="checkbox"/>	Network Segment	default
<input checked="" type="checkbox"/>	Transaction Log	default
<input checked="" type="checkbox"/>	Transaction Alarms	default





ボタン

以下のリストは、このタブにおけるアイコンについて説明しています。

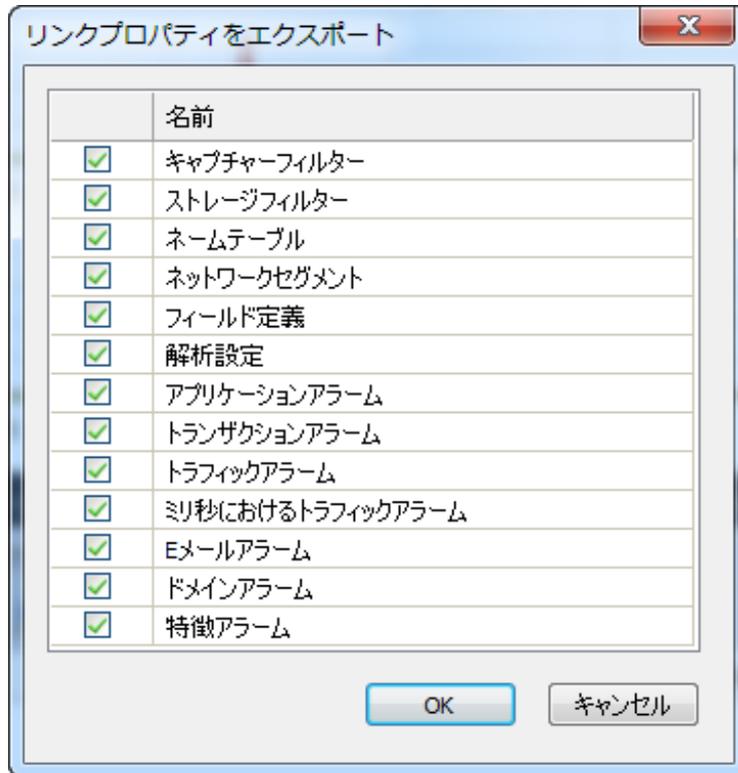
- : 選択された統計ビューを削除します。システムデフォルトのビューは削除できません。カスタムビューだけ削除できます。
- : 選択された統計ビューの名前とフィルター条件を修正します。システムデフォルトのビューは修正できません。カスタムビューだけ修正できます。
- : 保存された設定ファイルを現在のタブにインポートします。
- : このタブにおける統計ビューの設定ファイルをローカルにエクスポートします。エクスポートされた設定ファイルは他のネットワークリンクにインポートすることもできます。
- : 選択された統計ビューの位置を前に移動します。
- : 選択された統計ビューの位置を後に移動します。

ネットワークリンクプロパティをエクスポート

ネットワークリンクプロパティの全ての項目は、他のネットワークリンクで更なる使用のために、エクスポートすることができます。

以下のステップに従い、ネットワークリンクプロパティをエクスポートします。

1. ネットワークリンクを右クリックし、「リンクプロパティをエクスポート」をクリックして、リンクプロパティをエクスポートするダイアログボックスを開きます。

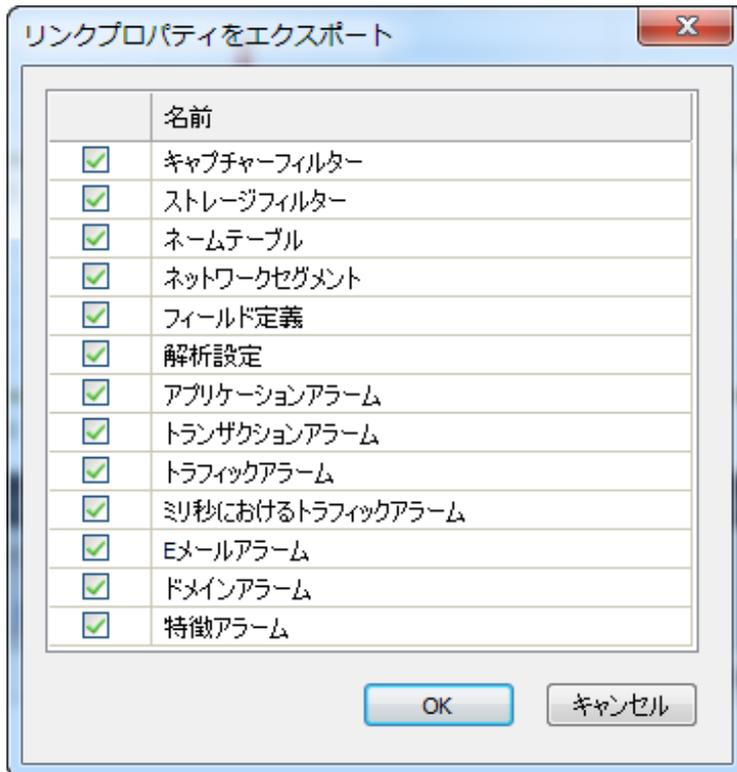


2. リンクプロパティをエクスポートするダイアログボックスにおいて、エクスポートしたい項目を選択します。
3.  ボタンをクリックして、保存ダイアログボックスを開きます。保存ダイアログボックスで、保存先を選択し、ファイル名を入力して、「保存」をクリックします。

ネットワークリンクプロパティをインポート

以下のステップに従い、ネットワークリンクプロパティをインポートします。

1. リンクを右クリックし、「リンクプロパティをインポート」をクリックします。
2.  ボタンをクリックして、ファイルを開くダイアログボックスを開きます。「ファイルを開く」ダイアログボックスで、インポートしたいファイルを選択します。
3. リンクプロパティをインポートするダイアログボックスで、インポートしたい項目を選択します。



4. OK をクリックして、ネットワークリンクプロパティのインポートを完了します。

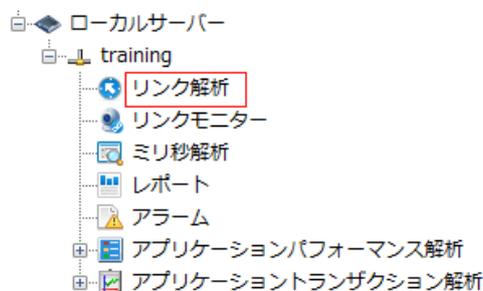
リンク解析

遡及的な解析を利用して、履歴のネットワーク状態を表示することができます。この章ではネットワークリンクに対する遡及的な解析の方法、リンク解析ウィンドウにおける各要素、およびエキスパートアナライザの使用方法について説明しています。

ネットワークリンクを遡及的に解析

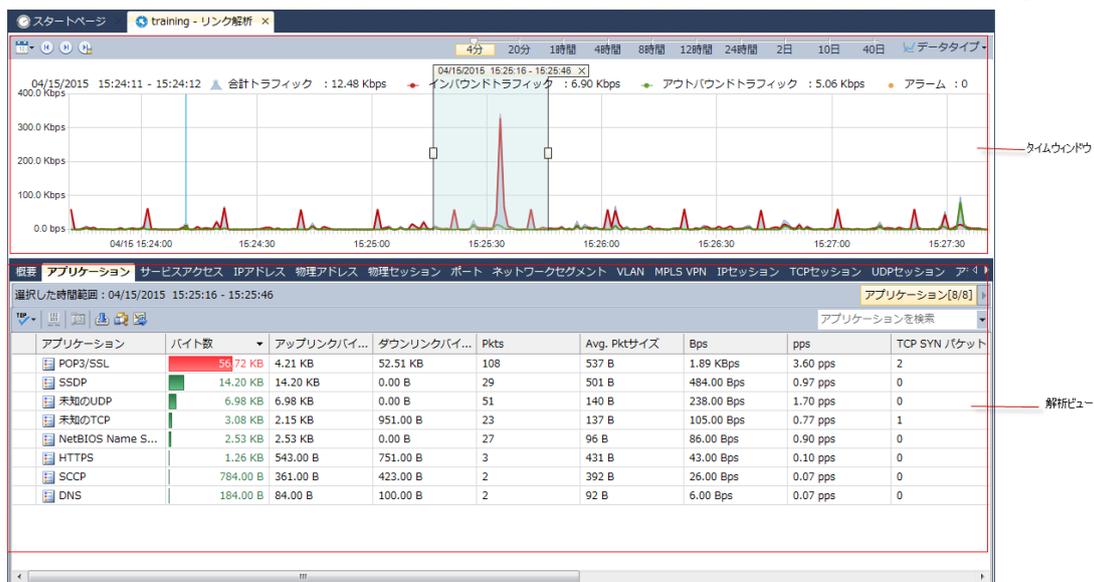
ネットワークリンクを遡及的に解析するには、

1. サーバーに接続すると、サーバーのために作成されたネットワークリンクはサーバーエクスプローラにおけるサーバーの下に表示されます。
2. ネットワークリンクの下にある「リンク解析」をダブルクリックして、リンク解析ウィンドウを開きます。



リンク解析ウィンドウ

下図のように、リンク解析ウィンドウは、遡及的な解析の主なワークベンチです。



リンク解析ウィンドウはタイムウィンドウパネルと解析ビューパネルからなっています。

パネルの幅を変更するには、パネル間のラインにマウスポインタを移動し、マウスポインタが両方向の矢印になると、ドラッグすることで、パネルの幅を変更することができます。

タイムウィンドウ

以下のリストはタイムウィンドウにおける各アイコンボタンについて説明しています。

:これらのアイコンボタンはタイムウィンドウの時間範囲を設定するために設けられたものです。

4分 20分 1時間 4時間 8時間 12時間 24時間 2日 10日 40日 :このアイコンをクリックして、タイムウィンドウタイプを選択します。タイムウィンドウで右クリックし、「タイムウィンドウタイプ」にマウスを移動し、適切なタイムウィンドウタイプをクリックすることで、タイムウィンドウタイプを選択することもできます。

データタイプ :このアイコンをクリックして、表示したいデータタイプを選択します。タイムウィンドウを右クリックし、「データタイプ」にマウスを移動し、適切なデータタイプをクリックすることで、データタイプを選択することもできます。

タイムウィンドウを利用することで、トラフィック、アラーム、パケット、パケットサイズ分布、TCP パケット、および利用率を含め、各データタイプのグラフィカルなビューを取得することができます。タイムウィンドウは下図のように表示されます。



ドラッグ可能なタイムウィンドウ

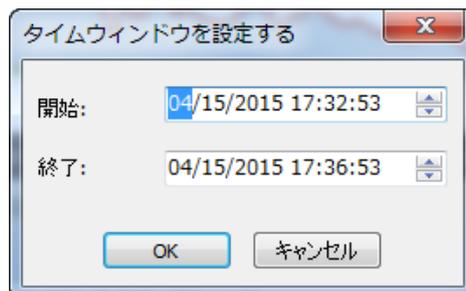
タイムウィンドウをドラッグして、履歴のネットワークデータを表示することができます。タイムウィンドウにおけるチャートの横軸にマウスを移動し、マウスがになると、ドラッグすればよいです。

タイムウィンドウを設定する

タイムウィンドウを設定するか、または選択したい時間範囲を設定することができます。

以下のステップに従い、タイムウィンドウを設定します。

1. をクリックし、「タイムウィンドウを設定する」をクリックして、下図のようにタイムウィンドウを設定するダイアログボックスが表示されます。



2. 「開始」と「終了」に開始時間と終了時間をそれぞれ設定します。その開始時間は、現在のネットワークリンクが監視された時間より前にはできないこと

に注意してください。

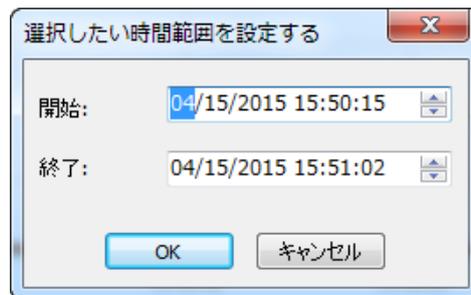
開始時間と終了時間を設定するには、テキストボックスにおける時間をクリックして、適切な時間を入力するか、スピンドットをクリックすることができます。

3. 「OK」をクリックします。

注意 設定された開始時間と終了時間の時間範囲が 4 分、20 分、1 時間、4 時間、8 時間、12 時間、24 時間、2 日、10 日、および 40 日でない場合、タイムウィンドウは、設定された開始時間を基準に、自動的に設定された時間範囲より大きい且つ一番近いタイムウィンドウに変更します。例えば、設定された時間範囲は 3 分の場合、タイムウィンドウは 4 分ウィンドウに変更します。設定された時間範囲は 5 分の場合、タイムウィンドウは 20 分ウィンドウに変更します。

以下のステップに従い、時間範囲を設定します。

1.  をクリックし、「時間範囲を設定する」をクリックすることで、選択したい時間範囲を設定するダイアログボックスが表示されます。



2. 「開始」と「終了」に開始時間と終了時間をそれぞれ設定します。その開始時間は、現在のネットワークリンクの監視された時間より前にすることはできないことに注意してください。

開始時間と終了時間を設定するには、テキストボックスにおける時間をクリックして、適切な時間を入力するか、スピンドットをクリックすることができます。

3. 「OK」をクリックします。

時間範囲を設定した後、設定された時間範囲は自動的に、タイムウィンドウに選択されます。

タイムウィンドウの位置決め

タイムウィンドウを設定するほかに、以下のボタンを利用して、タイムウィンドウの位置決めができます。

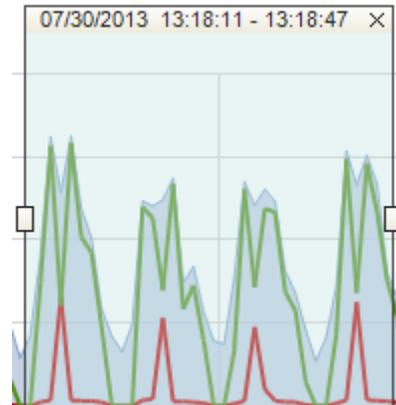
: このボタンをクリックすると、現在のタイムウィンドウの開始時間は、このネットワークリンクの監視された時間となっています。

: このボタンをクリックすると、現在のタイムウィンドウの終了時間はサーバーの現在時刻となっています。

時間範囲を選択する

タイムウィンドウの下における解析ビューは、タイムウィンドウに選択された時間範囲のデータを表示します。

時間範囲を選択するには、タイムウィンドウでマウスをドラッグすればよいです。そして選択された時間範囲は、下図のように、2つのハンドルとタイムバーに囲まれます。



マウスをハンドルに移動して、ドラッグすることで、時間範囲の幅を変更することができます。

タイムバーは囲まれた時間範囲の持続時間を示しています。マウスをタイムバーに移動し、マウスが☞になると、マウスをドラッグすることで、同じ持続時間で、囲まれた時間範囲を移動することができます。また、☒ボタンをクリックすることで、囲まれた時間範囲を閉じることができます。

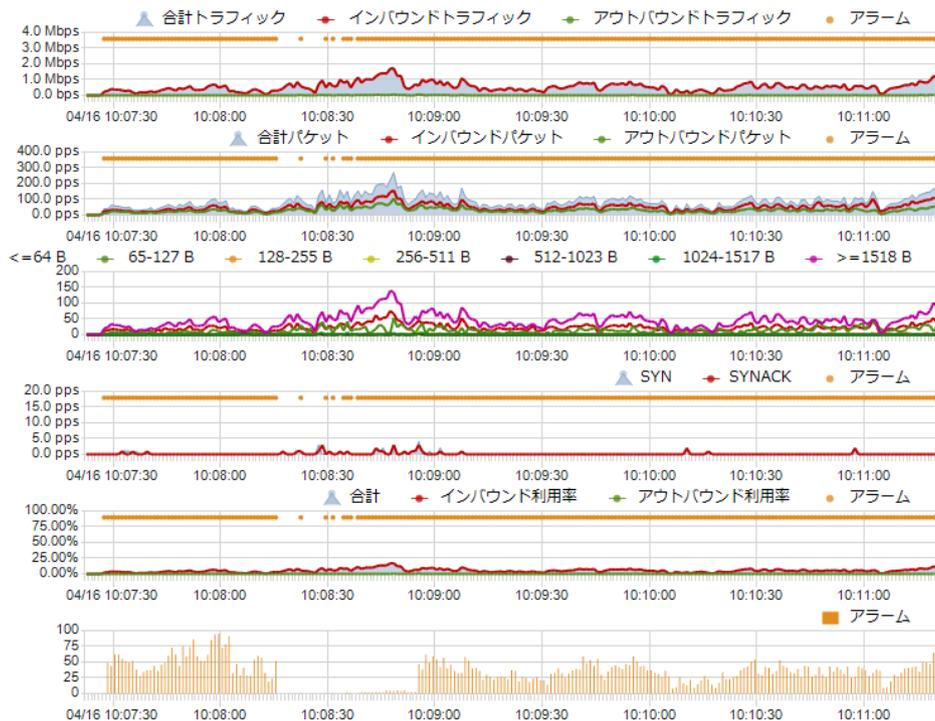
タイムウィンドウの目盛り

タイムウィンドウは、線によっていくつかの部分に区切られています。タイムウィンドウにおける最小目盛りと各部分の目盛り数は、タイムウィンドウタイプによって異なります。以下の表はタイムウィンドウタイプ、最小目盛り、および各部分の目盛り数を示しています。

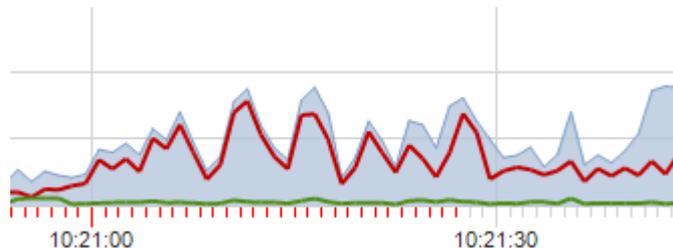
タイムウィンドウタイプ	最小目盛り	各部分の目盛り数
4分ウィンドウ	1秒	30
20分ウィンドウ	5秒	48
1時間ウィンドウ	15秒	40
4時間ウィンドウ	1分	30
8時間ウィンドウ	2分	30
12時間ウィンドウ	3分	40
24時間ウィンドウ	6分	40
2日ウィンドウ	12分	40
10日ウィンドウ	1時間	30
40日ウィンドウ	4時間	24

リンク解析のトレントチャート

タイムウィンドウには、リンクモニターウィンドウと同じく、下図のようにさまざまなトレントチャートがあります。



横軸にある赤色の目盛りは、その間でキャプチャーされたパケットはクリアされたことを表しています。例えば、下図では 10:21:27 前のパケットはクリアされています。



解析ビュー

解析ビューには、タイプごとの統計情報を表示するいくつかのビューがあります。タイムウィンドウを利用することで、解析ビューに表示する統計データボリュームを削減し、ネットワーク問題の解析とドリルダウンに集中させることができます。タイムウィンドウにおけるトレントチャートで時間範囲が選択されていないと、概要ビューを除いて、他のビューには記録が何も表示されないことに注意してください。トレントチャートにおける時間範囲を変更すると、各解析ビューの統計情報は自動的に更新されます。

ツールバーとポップアップメニュー

ツールバーにおけるボタン

各解析ビューの上部には、ツールバーがあります。各解析ビューにおけるツールバーは違うかもしれませんが、ツールバーにおけるボタンが同じであれば、ボタンの機能も同じになります。

以下のリストは、ツールバーにおける各ボタンについて説明しています。



: 現在選択されていた時間範囲のパケットをダウンロードします。パケットのダウン

ロードについての詳細情報については、この章における「パケットのダウンロード」をご参照ください。

: エキスパートアナライザを起動して、選択された時間範囲のパケットを解析します。

: 現在の統計情報を.csvファイルに保存します。統計情報のエクスポートについての詳しいことは、この節における「統計情報をエクスポート」をご参照ください。

: このビューで表示する統計情報のトップ数を選択します。

: 新しい解析ウィンドウを開き、選択されたオブジェクトに対する専用の解析を行います。サービスアクセスビュー、IPアドレスビュー、ネットワークセグメントビュー、物理アドレスビュー、アラームビューという五つのビューの場合にのみ、利用可能となります。

: 解析ビューの左におけるネットワークセグメントパネルを開き、IPアドレスのセグメント情報を表示します。IPアドレスビューの場合にのみ、利用可能となります。

: マルチセグメント解析ウィンドウを開き、マルチセグメント解析を実行します。

: レポートを生成します。統計ビューのデータを一時的なレポートで表示します。選択した時間範囲内にはデータがある場合にのみ、利用可能となります。

: チャートを生成します。統計ビューのデータをチャートで表示します。システムは棒グラフと円グラフという二つのタイプを提供します。

: 現在ビューのために高度なフィルターを作成します。

ポップアップメニュー

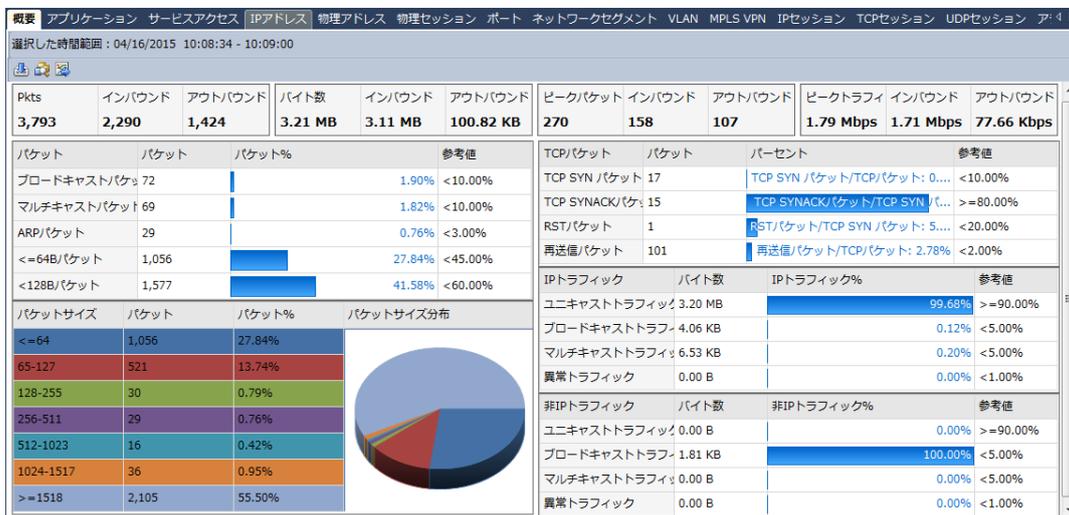
解析ビューを右クリックすると、ポップアップメニューが開かれます。ポップアップメニューにおけるコマンド項目は解析ビューによって異なります。以下のリストは、各解析ビューにおける全てのコマンド項目について説明しています。

- **高度なフィルター**: 現在ビューのために、高度なフィルターを作成します。
- **新しいウィンドウで解析する**: 新しいウィンドウを開き、解析ビューで選択されたネットワークオブジェクトを専用の解析します。
- **ドリルダウン**: 選択されたオブジェクトに対して、ドリルダウンを行います。
- **ドリルダウンを閉じる**: 統計ビューで開いているドリルダウンウィンドウを閉じます。
- **コピー**: 選択された行とヘッダー行をクリップボードにコピーします。
- **カラムをコピー**: 選択されたカラムをクリップボードにコピーします。
- **カラムを表示する**: 解析ビューで表示するカラムを選択します。デフォルトをクリックすると、デフォルトカラムしか表示されません。ヘッダーカラムを右クリックすることで、表示したいカラムを選択することもできます。
- **ネームテーブルに追加**: 物理アドレス、IPアドレス、VLAN IDおよびMPLS VPNラベルをネームテーブルに追加します。
- **統計情報をエクスポートする**: 現在選択された時間範囲の統計情報を.csvファイルにエクスポートします。
- **パケットをダウンロードする**: 現在選択された時間範囲のパケットをダウンロードします。

- **パケットを解析**：エキスパートアナライザを起動して、選択した時間範囲内のパケットを解析します。
- **レポートを生成**：現在統計ビューのデータを一時的なレポートで表示します。
- **すべてを表示する**：現在統計ビューにおけるすべての記録を表示します。
- **マルチセグメント解析**：マルチセグメント解析ウィンドウを開き、マルチセグメント解析を実行します。
- **ダウンロードとエキスパート解析を管理**：ダウンロード中またはダウンロード済みのタスクを表示します。これらのタスクに対して、削除したり、解析したりすることができます。

概要ビュー

概要ビューは、下図のように、現在のタイムウィンドウと選択された時間範囲の統計情報を提供します。



タイムウィンドウにおける時間範囲が選択されていないと、このビューにはデータが何も表示されません。

アプリケーションビュー

アプリケーションビューは下図のように表示されます。

アプリケーション	バイト数	アップリンクバイ...	ダウンリンクバイ...	Pkts	Avg. Pktサイズ	Bps	pps	TCP SYN /パケット
HTTP	15.71 MB	447.47 KB	15.27 MB	17,768	927 B	73.46 KBps	81.13 pps	32
未知のUDP	74.74 KB	72.38 KB	2.36 KB	759	100 B	349.00 Bps	3.47 pps	0
NetBIOS Name S...	47.93 KB	47.93 KB	0.00 B	509	96 B	224.00 Bps	2.32 pps	0
SSDP	18.55 KB	18.55 KB	0.00 B	108	175 B	86.00 Bps	0.49 pps	0
POP3/SSL	10.33 KB	3.04 KB	7.29 KB	58	182 B	48.00 Bps	0.26 pps	2
HTTPS	6.34 KB	3.40 KB	2.94 KB	32	203 B	29.00 Bps	0.15 pps	0
DNS	6.19 KB	2.14 KB	4.05 KB	48	132 B	28.00 Bps	0.22 pps	0
未知のTCP	3.98 KB	2.11 KB	1.88 KB	46	88 B	18.00 Bps	0.21 pps	0
NetBIOS Datagra...	1.48 KB	1.48 KB	0.00 B	6	252 B	6.00 Bps	0.03 pps	0
mDNS	358.00 B	358.00 B	0.00 B	1	358 B	1.00 Bps	0.00 pps	0

アプリケーションビューは、システムアプリケーションとカスタムアプリケーションを含むネットワークアプリケーションの統計情報を提供します。システムアプリケーションは、サーバー側でサーバーを設定する際に、ライブラリーにアップロードされます。一方、カスタムアプリケーションは、コンソール側でネットワークリンクを設定する際にカスタマイズさ

ることができます。カスタムアプリケーションは、システムアプリケーションより優先されています。

アプリケーション統計情報を表示する

アプリケーションビューには、アプリケーション名、バイト数、パケット、および平均パケットサイズに基づく、ネットワークのトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、アプリケーションビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

アプリケーションビューにおけるアプリケーションがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

アプリケーションをドリルダウンする

アプリケーションをドリルダウンして、より詳しい情報を取得することができます。あるアプリケーションをドリルダウンするには、このアプリケーションを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。続いて、表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のようにアプリケーションビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。

アプリケーション[6/6] ▶ ネットワークセグメント[1/1] ▶ 内部IP[1/1] ▶ IPセッション[11/11] ▶ TCPセッション[2/2]

ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

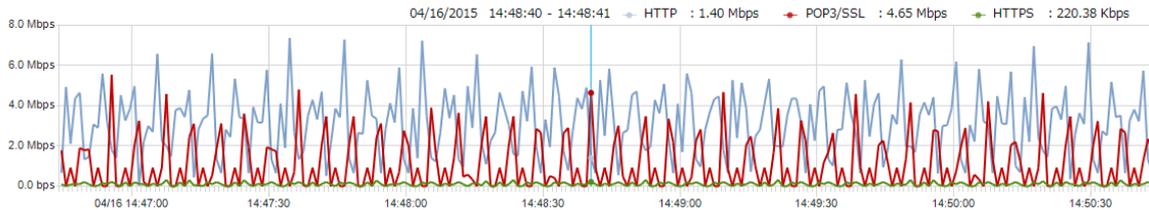
新しいウィンドウでアプリケーションを解析する

あるアプリケーションを右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、このアプリケーションを専用のに解析することができます。

選択されたアプリケーションを専用のに解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは選択されたアプリケーションのトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは全体ネットワークのトラフィックチャートを表示します。

新しいウィンドウにおけるタイムウィンドウは、選択された各アプリケーションのトラフィックチャートを提供します。例えば、元のリンク解析ウィンドウにおけるアプリケーション

ビューで三つのアプリケーションが選択された場合、新しいウィンドウにおけるタイムウィンドウは、色が異なる三つのチャートを提供します。チャート上にマウスを移動すると、下図のように、その時点の統計情報がチャートの右上に表示されます。



サービスアクセスビュー

サービスアクセスビューは下図のように表示されます。

サーバーIP	サーバーポート	TCP/UDP	クライアントIP	アプリケーション	バイト数	Bps	アップリンクバイト数	ダウンリンクバイト数
108.168.215.106	80	TCP	192.168.9.25	HTTP	15.09 MB	71.89 KBps	395.05 KB	14.71 MB
182.140.130.51	80	TCP	192.168.9.25	HTTP	274.23 KB	3.56 KBps	15.57 KB	258.66 KB
61.188.191.84	80	TCP	192.168.9.25	HTTP	201.80 KB	2.76 KBps	10.60 KB	191.20 KB
182.140.147.104	80	TCP	192.168.9.25	HTTP	100.71 KB	2.65 KBps	10.16 KB	90.55 KB
175.154.189.30	80	TCP	192.168.9.25	HTTP	24.15 KB	374.76 Bps	2.07 KB	22.08 KB
218.30.103.237	80	TCP	192.168.9.25	HTTP	12.57 KB	79.43 Bps	9.45 KB	3.12 KB
192.168.9.255	137	UDP	192.168.9.12	NetBIOS Name Service	12.02 KB	135.30 Bps	12.02 KB	0.00 B
192.168.9.255	137	UDP	192.168.9.76	NetBIOS Name Service	11.72 KB	244.90 Bps	11.72 KB	0.00 B
239.255.255.250	1,900	UDP	192.168.9.76	SSDP	11.01 KB	126.70 Bps	11.01 KB	0.00 B
FF02::1:3	5,355	UDP	FE80::ACDC:AA8:CF0:6AFF	未知のUDP	10.76 KB	224.82 Bps	10.76 KB	0.00 B
220.181.76.71	80	TCP	192.168.9.25	HTTP	10.36 KB	964.55 Bps	767.00 B	9.61 KB

サービスアクセス統計情報を表示する

サービスアクセスビューには、監視されたネットワークリンクにおけるアプリケーションの接続統計情報が表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

サービスアクセスビューにおける項目がたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。ここのトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。このビューにおける全ての統計項目を表示したい場合、 をクリックし、「全てを表示」をクリックすればよいです。

サービスアクセス項目をドリルダウンする

サービスアクセス項目をドリルダウンして、詳しい情報を取得することができます。あるサービスアクセス項目をドリルダウンするには、この項目を右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。続いて、表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のようにサービスアクセスビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。

サーバーIP	サーバーポート	TCP/UDP	クライアントIP	クライアントポート	サーバーポート	バイト数	Pkts	クライアントRTT	保持
192.168.0.196	8,118	TCP	192.168.9.25	54,435	8,118	160.77 KB	199	0.1 ms	00:0
239.255.255.250	1,900	UDP	192.168.9.20	54,438	8,118	14.45 KB	142	0.0 ms	00:0
192.168.0.183	8,000	TCP	192.168.9.25	54,439	8,118	11.35 KB	49	0.0 ms	00:0
114.112.67.55	80	TCP	192.168.9.25	54,433	8,118	9.34 KB	20	0.0 ms	00:0
222.218.45.207	80	TCP	192.168.9.25	54,434	8,118	8.79 KB	37	0.1 ms	00:0
FF02::1:2	547	UDP	FE80::DCFD:88BD:CAAD:42...	54,451	8,118	5.07 KB	12	0.1 ms	00:0
221.228.204.31	80	TCP	192.168.9.25	54,440	8,118	3.78 KB	19	0.0 ms	00:0
FF02::1:2	547	UDP	FE80::1CDE:3437:2AB2:90A3...	54,432	8,118	3.22 KB	11	0.0 ms	00:0
192.168.20.1	53	UDP	192.168.9.25	54,453	8,118	1.96 KB	10	0.0 ms	00:0
FF02::1:2	547	UDP	FE80::E816:E6AB:9E95:7AB6...	54,449	8,118	1.96 KB	10	0.1 ms	00:0
192.168.9.255	137	UDP	192.168.9.51	54,445	8,118	1.96 KB	10	0.1 ms	00:0

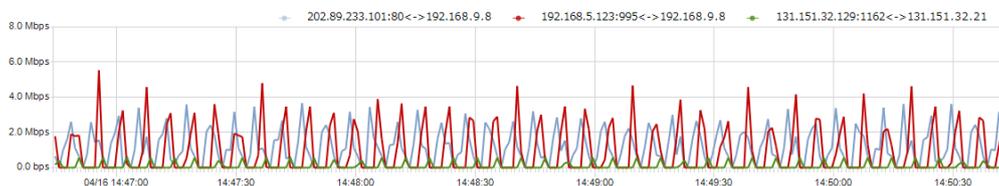
ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

新しいウィンドウでサービスアクセスを解析する

選択されたサービスアクセス項目を右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、このサービスアクセス項目を専用の解析することができます。

選択されたサービスアクセス項目を専用の解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは選択されたサービスアクセス項目のトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは、全体ネットワークのトラフィックチャートを表示します。

新しいウィンドウにおけるタイムウィンドウは、選択された各サービスアクセス項目のトラフィックチャートを提供します。例えば、元のリンク解析ウィンドウにおけるサービスアクセスビューで三つのサービスアクセス項目が選択された場合、新しいウィンドウにおけるタイムウィンドウは、色が異なる三つのチャートを提供します。チャート上にマウスを移動すると、下図のように、その時点の統計情報がチャートの右上に表示されます。



タイムウィンドウで任意の時間範囲を選択して、選択された時間範囲の詳細な統計情報を下の解析ビューに表示することができます。

サービスアクセスビューで検索

サービスアクセスビューに統計情報がたくさんある場合、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックス

サービスアクセスを検索 に適切なキーワードを入力することで、キーワードが含まれている項目のみがサービスアクセスビューに表示されます。

物理アドレスビュー

物理アドレスビューは、下図のように、MAC アドレスによるトラフィックの統計情報と解析を提供します。

アドレス	バイト数	Pkts	Tx Bytes	Tx Pkts	Rx Bytes	Rx Pkts	Bps	pps	ブロードキャスト/パケット	マルチキャスト
08:00:27:04:29:42:88	15.75 MB	18,120	472.67 KB	7,322	15.29 MB	10,798	73.66 KBps	82.74 pps	57	83
00:0E:4E:00:00:00	15.74 MB	17,988	15.29 MB	10,806	460.45 KB	7,182	73.61 KBps	82.14 pps	0	0
00:00:00:00:00:00	70.23 KB	837	0.00 B	0	70.23 KB	837	328.00 Bps	3.82 pps	527	0
28:02:44:39:A5:4D	59.95 KB	630	59.95 KB	630	0.00 B	0	280.00 Bps	2.88 pps	126	458
33:33:00:01:00:02	24.34 KB	148	0.00 B	0	24.34 KB	148	113.00 Bps	0.68 pps	0	148
00:00:0E:00:00:0C	22.36 KB	326	0.00 B	0	22.36 KB	326	104.00 Bps	1.49 pps	0	326
33:33:00:01:00:03	21.95 KB	248	0.00 B	0	21.95 KB	248	102.00 Bps	1.13 pps	0	248
74:04:25:84:3A:CC	18.21 KB	219	18.21 KB	219	0.00 B	0	85.00 Bps	1.00 pps	126	82
00:00:0E:7F:FF:FA	13.88 KB	82	0.00 B	0	13.88 KB	82	64.00 Bps	0.37 pps	0	82
FC:AA:34:33:33:83	12.95 KB	154	12.95 KB	154	0.00 B	0	60.00 Bps	0.70 pps	65	89
FC:AA:34:33:3D:05	12.88 KB	200	12.88 KB	200	0.00 B	0	60.00 Bps	0.91 pps	12	0

物理アドレス統計情報を表示する

物理アドレスビューには、MAC アドレス、バイト数、パケットに基づく、ネットワークのトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、物理アドレスビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

物理アドレスビューにおける MAC アドレスがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

MAC アドレスをドリルダウンする

MAC アドレスをドリルダウンして、より詳しい情報を取得することができます。ある MAC アドレスをドリルダウンするには、この MAC アドレスを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。続いて、表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のように物理アドレスビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。



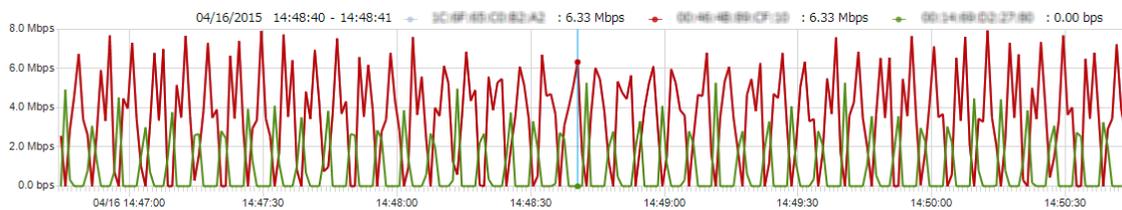
ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

新しいウィンドウで MAC アドレスを解析する

ある MAC アドレスを右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、この MAC アドレスを専用的に解析することができます。

選択された MAC アドレスを専用的に解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは、選択された MAC アドレスのトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは、全体ネットワークのトラフィックチャートを表示します。

新しいウィンドウは、選択された各 MAC アドレスのトラフィックチャートを提供します。例えば、元のリンク解析ウィンドウにおける物理アドレスビューで三つの MAC アドレスが選択された場合、新しいウィンドウにおけるタイムウィンドウは、色が異なる三つのチャートを提供します。チャート上にマウスを移動すると、下図のように、その時点の統計情報がチャートの右上に表示されます。



物理セッションビュー

物理セッションビューは、下図のように、物理セッションによるトラフィックの統計情報と解析を提供します。

ノード1	ノード2	バイト数	Pkts	Bps	pps	ノード1 Tx Bytes	ノード1 Tx Pkts	ノード2 Tx Bytes	ノード2 Tx Pkts
00:70:F4:29:41:80	00:40:40:09:CF:35	15.74 MB	17,980	73.60 KBps	82.10 pps	460.45 KB	7,182	15.29 MB	10,798
FF:FF:FF:FF:FF:FF	28:02:44:59:A5:4D	14.83 KB	172	69.00 Bps	0.79 pps	0.00 B	0	14.83 KB	172
FF:FF:FF:FF:FF:FF	FC:AA:34:35:5D:05	12.88 KB	200	60.00 Bps	0.91 pps	0.00 B	0	12.88 KB	200
FF:FF:FF:FF:FF:FF	74:04:35:84:3A:CC	12.71 KB	137	59.00 Bps	0.63 pps	0.00 B	0	12.71 KB	137
28:02:44:59:A5:4D	01:00:5E:7F:FF:FA	11.01 KB	64	51.00 Bps	0.29 pps	11.01 KB	64	0.00 B	0
33:33:00:01:00:03	28:02:44:59:A5:4D	10.76 KB	118	50.00 Bps	0.54 pps	0.00 B	0	10.76 KB	118
28:02:44:59:A5:4D	01:00:5E:00:00:FC	8.45 KB	118	39.00 Bps	0.54 pps	8.45 KB	118	0.00 B	0
33:33:00:00:00:36	28:02:44:59:A5:4D	6.14 KB	66	28.00 Bps	0.30 pps	0.00 B	0	6.14 KB	66
FF:FF:FF:FF:FF:FF	FC:AA:34:33:53:83	6.09 KB	65	28.00 Bps	0.30 pps	0.00 B	0	6.09 KB	65
FF:FF:FF:FF:FF:FF	88:70:F4:29:41:80	5.34 KB	57	24.00 Bps	0.26 pps	0.00 B	0	5.34 KB	57
74:04:35:84:3A:CC	01:00:5E:00:00:FC	5.25 KB	78	24.00 Bps	0.36 pps	5.25 KB	78	0.00 B	0

物理セッション統計情報を表示する

物理セッションビューには、通信ノード、ノードバイト数、パケットに基づく、ネットワークのトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、物理セッションビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

物理セッションビューにおける物理セッションがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

ポートビュー

下図のように、ポートビューには、TCP サービスポートと UDP サービスポートという 2 つのタブが含まれています。

アドレス	ポート	アプリケーション	バイト数	アップリンクバ...	ダウンリンクバ...	Pkts	アップリンクバケ...	ダウンリンクバケ...	Rx TCP SYN Pkts
108.168.215.106	80	HTTP	15.09 MB	395.05 KB	14.71 MB	16,724	6,561	10,163	0
182.140.130.51	80	HTTP	274.23 KB	15.57 KB	258.66 KB	395	185	210	6
61.188.191.84	80	HTTP	201.80 KB	10.60 KB	191.20 KB	296	140	156	7
182.140.147.104	80	HTTP	100.71 KB	10.16 KB	90.55 KB	174	84	90	7
175.154.189.30	80	HTTP	24.15 KB	2.07 KB	22.08 KB	47	23	24	2
218.30.103.237	80	HTTP	12.57 KB	9.45 KB	3.12 KB	53	30	23	3
220.181.76.71	80	HTTP	10.36 KB	767.00 B	9.61 KB	17	6	11	1
74.53.97.226	995	POP3/SSL	6.27 KB	1.66 KB	4.61 KB	33	17	16	1
65.54.184.48	443	HTTPS	5.02 KB	2.49 KB	2.53 KB	15	9	6	0
192.168.0.197	995	POP3/SSL	4.06 KB	1.38 KB	2.68 KB	25	12	13	1
192.168.0.183	8,000	未知のTCP	2.32 KB	1.20 KB	1.12 KB	27	15	12	0

ポート統計情報を表示する

ポートビューには、IP アドレス+ポート番号に基づく、ポートアクセス統計情報が表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、ポートビューで表示したいカラムを選択することができます。

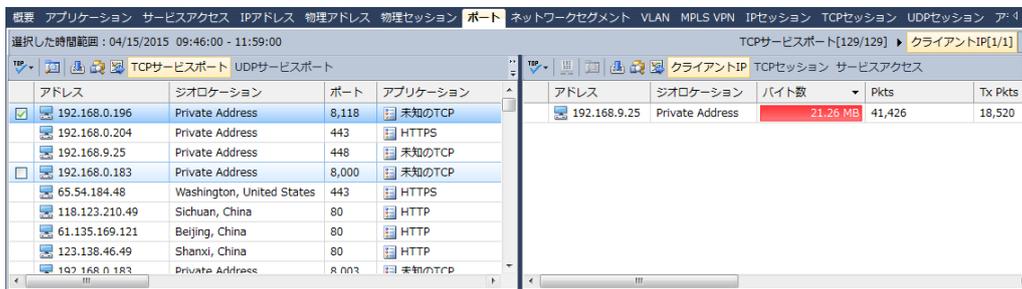
さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

ポートビューにおける項目がたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。このビューにおける全ての統計項目を表示したい場合、 をクリックし、「全てを表示」をクリックすればよいです。

サービスポートをドリルダウンする

サービスポートをドリルダウンして、より詳しい情報を取得することができます。あるサービスポートをドリルダウンするには、このポートを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。続いて、表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のようにポートビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます



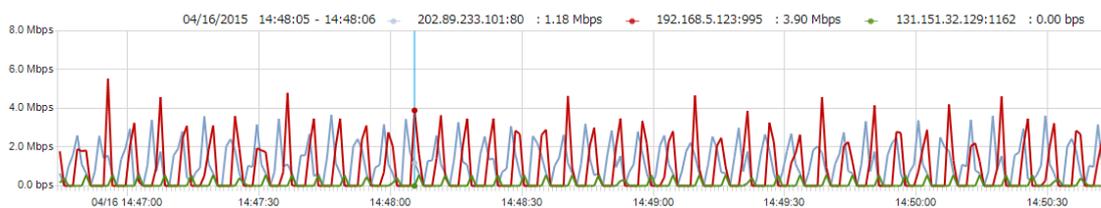
ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

新しいウィンドウでポートを解析する

あるポートを右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、このポートを専用のに解析することができます。

選択されたポートを専用のに解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは選択されたポートのトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは全体ネットワークのトラフィックチャートを表示します。

新しいウィンドウにおけるタイムウィンドウは、選択された各ポートのトラフィックチャートを提供します。例えば、元のリンク解析ウィンドウにおけるポートビューで三つのポートが選択された場合、新しいウィンドウにおけるタイムウィンドウは、色が異なる三つのチャートを提供します。チャート上にマウスを移動すると、下図のように、その時点の統計情報がチャートの右上に表示されます。



デフォルトでは、表示されたのはトラフィックチャートですが、「データタイプ」をクリックして、パケットチャートを表示することもできます。

タイムウィンドウで任意の時間範囲を選択して、選択された時間範囲の詳細な統計情報を下の解析ビューに表示することができます。

ポートビューで検索する

ポートビューに統計情報がたくさんある場合、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックス **TCPサービスポートを検索** に適

切なキーワードを入力することで、キーワードが含まれている項目のみがポートビューに表示されます。

ネットワークセグメントビュー

ネットワークセグメントビューは、下図のように表示されます。

名前	バイト数	Pkts	内部バイト数	内部パケット	Tx Bytes	Rx Bytes	Tx Pkts	Rx Pkts	Bytes Tx/Rx	Pkts Tx/Rx	Bps	bps	Tx I
Dev.1	15.79 MB	18,592	0.00 B	0	514.59 KB	15.29 MB	7,794	10,798	0.03	0.72	73.85 KBps	605.00 Kbps	19.1
Dev.2	37.02 KB	391	0.00 B	0	37.02 KB	0.00 B	391	0	37907.00	391.00	173.00 Bps	1.38 Kbps	1.3
Sales	12.57 KB	100	0.00 B	0	7.85 KB	4.72 KB	47	53	1.66	0.89	58.00 Bps	470.00 bps	293
Support	1.42 KB	9	0.00 B	0	543.00 B	915.00 B	3	6	0.59	0.50	6.00 Bps	53.00 bps	19.1
Test	49.76 KB	516	576.00 B	6	358.00 B	48.85 KB	1	509	0.01	0.00	232.00 Bps	1.86 Kbps	13.1

ネットワークセグメントビューには、ネットワークリンクを設定する際に定義されたネットワークセグメントによって、トラフィックの統計情報と解析が提供されます。

セグメント統計情報を表示する

ネットワークセグメントビューには、セグメント、バイト数、パケット、内部バイト数、および内部パケットに基づく、セグメントのトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、ネットワークセグメントビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

ネットワークセグメントビューにおける統計項目がたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

セグメントをドリルダウンする

セグメントをドリルダウンして、より詳しい情報を取得することができます。あるセグメントをドリルダウンするには、このセグメントを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。続いて、表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のようにネットワークセグメントビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。

ネットワークセグメント[4/4] ▶ アプリケーション[6/6] ▶ IPセッション[3/3] ▶ TCPセッション[23/23]

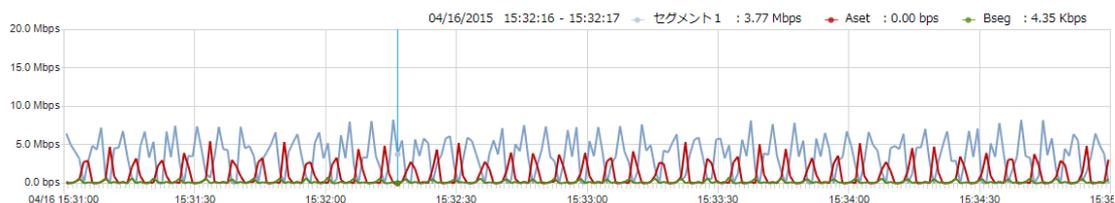
ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

新しいウィンドウでセグメントを解析する

あるセグメントを右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、このセグメントを専用的に解析することができます。

選択されたセグメントを専用的に解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは選択されたセグメントのトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは全体のネットワークのトラフィックチャートを表示します。

新しいウィンドウにおけるタイムウィンドウは、選択された各セグメントのトラフィックチャートを提供します。例えば、元のリンク解析ウィンドウにおけるネットワークセグメントビューで三つのセグメントが選択された場合、新しいウィンドウにおけるタイムウィンドウは、色が異なる三つのチャートを提供します。チャート上にマウスを移動すると、下図のように、その時点の統計情報がチャートの右上に表示されます。



セグメント間統計ビュー

セグメント間統計ビューはネットワークリンクで設定されたセグメント情報によって、セグメント間の通信情報を表示します。セグメント間統計ビューは下図のように表示されます。

Endpoint 1	Endpoint 2	Protocol	Application	Total ...	Bps	Bytes Sent by Endpoint 1	Bytes Sent by Endpoint 2	Total Packets
Unknown Segment	Unknown Segment	TCP	Unknown TCP Application	96.38 MB	22.22 KBps	95.42 MB	961.03 KB	19502
Unknown Segment	Unknown Segment	TCP	Standard Application2	67.56 MB	15.58 KBps	66.48 MB	1.08 MB	26369
Unknown Segment	Unknown Segment	UDP	Unknown UDP Application	4.75 MB	1.09 KBps	4.84 KB	4.74 MB	47449
Unknown Segment	Unknown Segment	UDP	DNS	739.34 KB	170.51 Bps	385.59 KB	353.75 KB	9532
Unknown Segment	Unknown Segment	UDP	DHCP	494.96 KB	114.15 Bps	0.00 B	494.96 KB	3222
Unknown Segment	Unknown Segment	IGMP	Unknown Application	17.14 KB	3.95 Bps	0.00 B	17.14 KB	274
Unknown Segment	Unknown Segment	UNKNOWN	Unknown Application	13.53 KB	3.12 Bps	0.00 B	13.53 KB	145
Unknown Segment	Unknown Segment	ICMPv6	Unknown Application	11.74 KB	2.71 Bps	0.00 B	11.74 KB	137
Unknown Segment	Unknown Segment	ICMP	ICMP	936.00 B	0.21 Bps	936.00 B	0.00 B	6

セグメント間通信情報を表示する

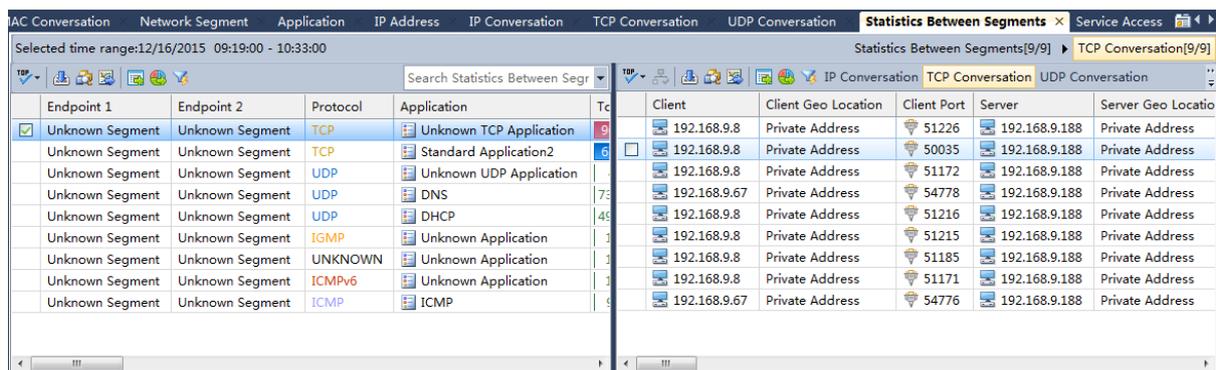
セグメント間統計ビューには、バイト数、パケット、および3ウェイハンドシェイク時間などに基づく、ネットワークのトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、セグメント間統計ビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

セグメント間統計ビューにおける統計項目がたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。ここのトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

セグメント間通信をドリルダウンする

セグメント間通信をドリルダウンして、より詳しい情報を取得することができます。あるセグメント間の通信をドリルダウンするには、この通信を右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。続いて、表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。



Endpoint 1	Endpoint 2	Protocol	Application	Tcp	Client	Client Geo Location	Client Port	Server	Server Geo Location
Unknown Segment	Unknown Segment	TCP	Unknown TCP Application	9	192.168.9.8	Private Address	51226	192.168.9.188	Private Address
Unknown Segment	Unknown Segment	TCP	Standard Application2	6	192.168.9.8	Private Address	50035	192.168.9.188	Private Address
Unknown Segment	Unknown Segment	UDP	Unknown UDP Application	1	192.168.9.8	Private Address	51172	192.168.9.188	Private Address
Unknown Segment	Unknown Segment	UDP	DNS	175	192.168.9.67	Private Address	54778	192.168.9.188	Private Address
Unknown Segment	Unknown Segment	UDP	DHCP	145	192.168.9.8	Private Address	51216	192.168.9.188	Private Address
Unknown Segment	Unknown Segment	IGMP	Unknown Application	1	192.168.9.8	Private Address	51215	192.168.9.188	Private Address
Unknown Segment	Unknown Segment	UNKNOWN	Unknown Application	1	192.168.9.8	Private Address	51185	192.168.9.188	Private Address
Unknown Segment	Unknown Segment	ICMPv6	Unknown Application	1	192.168.9.8	Private Address	51171	192.168.9.188	Private Address
Unknown Segment	Unknown Segment	ICMP	ICMP	6	192.168.9.67	Private Address	54776	192.168.9.188	Private Address

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、セグメント間統計ビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。

ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外したり、右クリックして、ポップアップされたメニューで「ドリルダウンを閉じる」をクリックしたりすることができます。

セグメント間統計ビューで検索する

セグメント間統計ビューに統計情報がたくさんある場合、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックスに適切なキーワードを入力することで、キーワードが含まれている項目のみがポートビューに表示されます。

VLAN ビュー

VLAN ビューには、下図のように、監視されたネットワークリンクの VLAN トラフィック統計情報を表示します。

VLAN ID	バイト数	Pkts	TCP SYN パケット	TCP SYNACK パケット	RST パケット	Bps	bps	pps
1127	14.29 MB	220,343	5,168	4,389	1,520	64.18 KBps	525.73 Kbps	966.42 pps
2133	4.32 MB	66,614	342	342	0	19.40 KBps	158.94 Kbps	292.17 pps
2132	4.26 MB	65,930	323	342	0	19.20 KBps	157.31 Kbps	289.17 pps
1128	3.04 MB	46,949	817	95	437	13.67 KBps	112.02 Kbps	205.92 pps
32	2.55 MB	5,282	0	0	0	11.46 KBps	93.90 Kbps	23.17 pps
2128	753.25 KB	11,343	342	0	266	3.30 KBps	27.06 Kbps	49.75 pps

VLAN 統計情報を表示する

VLAN ビューには、VLAN ID に基づく VLAN 統計情報が表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、VLAN ビューで表示したいカラムを選択することができます。

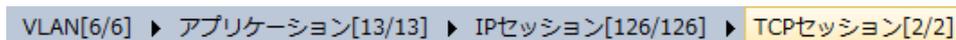
さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

VLAN ビューにおける項目がたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。このビューにおける全ての統計項目を表示したい場合、 をクリックし、「全てを表示」をクリックすればよいです。

VLAN をドリルダウンする

VLAN をドリルダウンして、より詳しい情報を取得することができます。ある VLAN をドリルダウンするには、この VLAN を右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。また、続いて表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のように VLAN ビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。



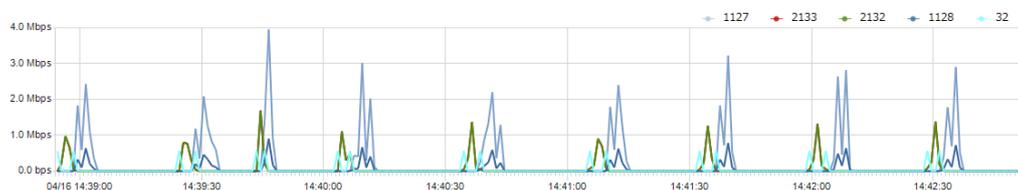
ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

新しいウィンドウで VLAN を解析する

ある VLAN を右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、この VLAN を専用的に解析することができます。

選択された VLAN を専用の解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは選択された VLAN のトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは全体ネットワークのトラフィックチャートを表示します。

新しいウィンドウにおけるタイムウィンドウは、選択された各 VLAN のトラフィックチャートを提供します。例えば、元のリンク解析ウィンドウにおける VLAN ビューで二つの VLAN が選択された場合、新しいウィンドウにおけるタイムウィンドウは、色が異なる二つのチャートを提供します。チャート上にマウスを移動すると、下図のように、その時点の統計情報がチャートの右上に表示されます。



デフォルトでは、表示されたのはトラフィックチャートですが、「データタイプ」をクリックして、パケットチャートを表示することもできます。

タイムウィンドウで任意の時間範囲を選択して、選択された時間範囲の詳細な統計情報を下の解析ビューに表示することができます

VLAN ビューで検索する

VLAN ビューに統計情報がたくさんある場合、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックス **VLANを検索** に適切なキーワードを入力することで、キーワードが含まれている項目のみが VLAN ビューに表示されます。

MPLS VPN ビュー

下図のように MPLS VPN ビューには、監視されたネットワークリンクの MPLS VPN トラフィックの統計情報が表示されます。

MPLS VPNラベル	バイト数	Pkts	TCP SYN /パケット	TCP SYNACK/パケット	RST/パケット	Bps	bps	pps
327	5.20 MB	66,352	0	0	780	34.83 KBps	285.37 Kbps	433.67 pps
283	5.02 MB	41,418	0	26	26	33.59 KBps	275.16 Kbps	270.71 pps
1006	2.06 MB	17,498	0	0	0	13.76 KBps	112.77 Kbps	114.37 pps
277	1.16 MB	9,932	0	0	0	7.77 KBps	63.67 Kbps	64.92 pps
509	913.12 KB	7,644	0	0	104	5.97 KBps	48.89 Kbps	49.96 pps
274	627.86 KB	5,460	0	0	0	4.10 KBps	33.62 Kbps	35.69 pps
257	531.78 KB	4,368	0	0	0	3.48 KBps	28.47 Kbps	28.55 pps
585	415.59 KB	4,082	0	0	0	2.72 KBps	22.25 Kbps	26.68 pps
297	214.35 KB	1,846	0	0	0	1.40 KBps	11.48 Kbps	12.07 pps
677	102.58 KB	884	0	0	0	686.00 Bps	5.49 Kbps	5.78 pps
3632	95.52 KB	910	0	0	52	639.00 Bps	5.11 Kbps	5.95 pps

MPLS VPN 統計情報を表示する

MPLS VPN ビューには、MPLS VPN タグに基づく MPLS VPN 統計情報が表示されます。コラムヘッダーを右クリックし、適切なコラムをクリックすることで、MPLS VPN ビューで表示したいコラムを選択することができます。

さらに、コラムヘッダーにおけるコラム名をクリックすることで、そのコラムによって統計情報を並べ替えることができます。

MPLS VPN ビューにおける項目がたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数コラムの値によって、並べ替える項目数であることに注意してください。このビューにおける全ての統計項目を表示したい場合、 をクリックし、「全てを表示」をクリックすればよいです。

MPLS VPN をドリルダウンする

MPLS VPN をドリルダウンして、より詳しい情報を取得することができます。ある MPLS VPN をドリルダウンするには、この MPLS VPN を右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。また、続いて表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のように MPLS VPN ビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。

MPLS VPN[13/13] ▶ アプリケーション[1/1] ▶ 外部IP[102/102] ▶ IPセッション[6/6]

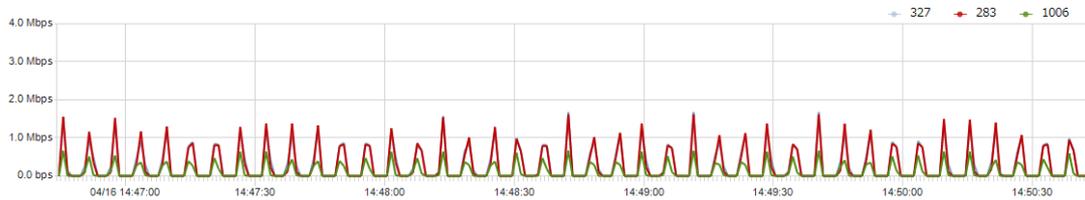
ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

新しいウィンドウで MPLS VPN を解析する

ある MPLS VPN を右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、この MPLS VPN を専用的に解析することができます。

選択された MPLS VPN を専用的に解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは選択された MPLS VPN のトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは全体ネットワークのトラフィックチャートを表示します。

新しいウィンドウにおけるタイムウィンドウは、選択された各 MPLS VPN のトラフィックチャートを提供します。例えば、元のリンク解析ウィンドウにおける MPLS VPN ビューで二つの MPLS VPN が選択された場合、新しいウィンドウにおけるタイムウィンドウは、色が異なる二つのチャートを提供します。チャート上にマウスを移動すると、下図のように、その時点の統計情報がチャートの右上に表示されます。



デフォルトでは、表示されたのはトラフィックチャートですが、「データタイプ」をクリックして、パケットチャートを表示することもできます。

タイムウィンドウで任意の時間範囲を選択して、選択された時間範囲の詳細な統計情報を下の解析ビューに表示することができます

MPLS VPN ビューで検索する

MPLS VPN に統計情報がたくさんある場合、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックス **MPLS VPNを検索** に適切なキーワードを入力することで、キーワードが含まれている項目のみがポートビューに表示されます。

IP アドレスビュー

下図のように IP アドレスビューには、IP アドレスに基づくトラフィックの統計情報と解析が表示されます。

アドレス	バイト数	Pkts	Tx Pkts	Rx Pkts	Bps	pps	bps	Pkts Tx/Rx	Avg. Pktサイズ	Tx TCP SYN Pkts
192.168.9.25	15.75 MB	18,075	7,277	10,798	73.64 KBps	82.53 pps	603.26 Kbps	0.67	913 B	34
192.168.9.255	49.41 KB	515	0	515	231.00 Bps	2.35 pps	1.85 Kbps	0.00	98 B	0
FF02::1:2	24.34 KB	148	0	148	113.00 Bps	0.68 pps	910.00 bps	0.00	168 B	0
224.0.0.252	22.36 KB	326	0	326	104.00 Bps	1.49 pps	836.00 bps	0.00	70 B	0
FF02::1:3	21.95 KB	248	0	248	102.00 Bps	1.13 pps	821.00 bps	0.00	90 B	0
239.255.255...	13.88 KB	82	0	82	64.00 Bps	0.37 pps	519.00 bps	0.00	173 B	0
FF02::16	6.60 KB	71	0	71	30.00 Bps	0.32 pps	246.00 bps	0.00	95 B	0
FF02::C	4.67 KB	26	0	26	21.00 Bps	0.12 pps	174.00 bps	0.00	184 B	0
224.0.0.22	4.63 KB	74	0	74	21.00 Bps	0.34 pps	173.00 bps	0.00	64 B	0
255.255.255...	1.45 KB	12	0	12	6.00 Bps	0.05 pps	54.00 bps	0.00	123 B	0
224.0.0.251	358.00 B	1	0	1	1.00 Bps	0.00 pps	13.00 bps	0.00	358 B	0

IP アドレス統計情報を表示する

デフォルトでは、このビューには、内部 IP アドレスの統計情報を表示します。「外部 IP」をクリックすることで、外部ネットワークの統計情報を表示することができます。

IP アドレスビューには、IP アドレス、バイト数、パケット、および平均パケットサイズに基づくネットワークのトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、IP アドレスビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

IP アドレスビューにおける IP アドレスがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

そのほかに、 をクリックすることで、ネットワークセグメントパネルを開き、セグメントに基づく統計情報を表示することができます。利用可能な全てのクラス C セグメントは、自動的にネットワークセグメントパネルに表示されます。あるセグメントをクリックすることで、そのセグメントについての統計情報のみを表示することができます。

IP アドレスをドリルダウンする

IP アドレスをドリルダウンして、より詳しい情報を取得することができます。ある IP アドレスをドリルダウンするには、この IP アドレスを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。また、続いて表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のように IP アドレスビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。

内部IP[11/11] ▶ アプリケーション[4/4] ▶ IPセッション[17/17] ▶ TCPセッション[1/1]

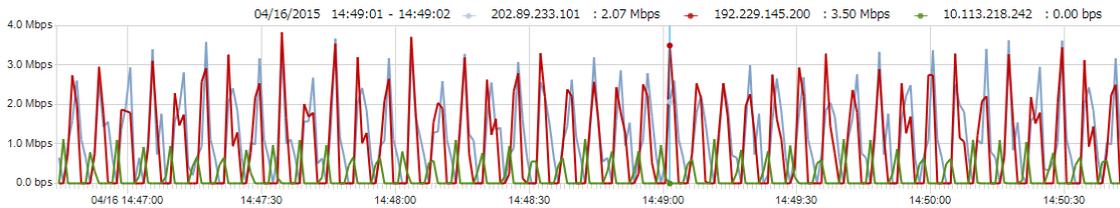
ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

新しいウィンドウで IP アドレスを解析する

ある IP アドレスを右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、この IP アドレスを専用のに解析することができます。

選択された IP アドレスを専用のに解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは選択された IP アドレスのトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは全体ネットワークのトラフィックチャートを表示します。

新しいウィンドウにおけるタイムウィンドウは、選択された各 IP アドレスのトラフィックチャートを提供します。例えば、元のリンク解析ウィンドウにおける IP アドレスビューで三つの IP アドレスが選択された場合、新しいウィンドウにおけるタイムウィンドウは、色が異なる三つのチャートを提供します。チャート上にマウスを移動すると、下図のように、その時点の統計情報がチャートの右上に表示されます。



IPセッションビュー

下図のように、IPセッションビューには、IPセッションに基づくトラフィックの統計情報と解析が表示されます。

ノード1	ノード2	バイト数	Bps	ノード1 Tx Bytes	ノード2 Tx Bytes	Pkts	pps	ノード1 Tx Pkts	ノード2 Tx Pkts
192.168.9.25	192.168.215.106	15.09 MB	70.58 KBps	395.05 KB	14.71 MB	16,724	76.37 pps	6,561	10,163
192.168.9.25	192.140.130.56	274.23 KB	1.25 KBps	15.57 KB	258.66 KB	395	1.80 pps	185	210
192.168.9.25	192.168.215.84	201.80 KB	943.00 Bps	10.60 KB	191.20 KB	296	1.35 pps	140	156
192.168.9.25	192.140.147.104	100.71 KB	470.00 Bps	10.16 KB	90.55 KB	174	0.79 pps	84	90
192.168.9.25	175.154.188.30	24.15 KB	112.00 Bps	2.07 KB	22.08 KB	47	0.21 pps	23	24
192.168.9.25	192.168.9.25	12.57 KB	58.00 Bps	3.12 KB	9.45 KB	53	0.24 pps	23	30
192.168.9.25	192.168.9.12	12.02 KB	56.00 Bps	0.00 B	12.02 KB	126	0.58 pps	0	126
192.168.9.25	192.168.9.76	11.96 KB	55.00 Bps	0.00 B	11.96 KB	126	0.58 pps	0	126
192.168.9.25	192.168.9.76	11.01 KB	51.00 Bps	0.00 B	11.01 KB	64	0.29 pps	0	64
192.168.9.25	192.168.9.76	10.76 KB	50.00 Bps	0.00 B	10.76 KB	118	0.54 pps	0	118
192.168.9.25	192.168.9.25	10.36 KB	48.00 Bps	9.61 KB	767.00 B	17	0.08 pps	11	6
192.168.9.25	192.168.9.76	8.45 KB	39.00 Bps	0.00 B	8.45 KB	118	0.54 pps	0	118

IPセッション統計情報を表示する

IPセッションビューには、通信ノード、ノードの地理的位置、バイト数、パケットに基づくネットワークトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、IPセッションビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

IPセッションビューにおけるIPセッションがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

IPセッションをドリルダウンする

IPセッションをドリルダウンして、より詳しい情報を取得することができます。あるIPセッションをドリルダウンするには、このIPセッションを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のようにIPセッションビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。



ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

TCP セッションビュー

下図のように、TCP セッションビューには、TCP セッションに基づくトラフィックの統計情報と解析が表示されます。

クライアントIP	クライアントポート	サーバーIP	サーバーポート	アプリケーション	バイト数	Bps	Pkts	クライアント/パケ...	サーバー/パケ...
192.168.9.25	49,983	108.168.215.106	80	HTTP	3.17 MB	13.41 KBps	3,491	1,357	2,134
192.168.9.25	49,989	108.168.215.106	80	HTTP	2.99 MB	12.65 KBps	3,307	1,294	2,013
192.168.9.25	49,988	108.168.215.106	80	HTTP	2.94 MB	15.60 KBps	3,213	1,232	1,981
192.168.9.25	49,991	108.168.215.106	80	HTTP	2.72 MB	11.57 KBps	3,034	1,202	1,832
192.168.9.25	49,990	108.168.215.106	80	HTTP	2.48 MB	10.50 KBps	2,795	1,127	1,668
192.168.9.25	50,010	182.140.130.51	80	HTTP	104.38 KB	2.05 KBps	125	50	75
192.168.9.25	50,033	61.188.191.84	80	HTTP	53.46 KB	1.62 KBps	79	39	40
192.168.9.25	50,037	182.140.130.51	80	HTTP	47.98 KB	1.30 KBps	72	35	37
192.168.9.25	50,014	182.140.147.104	80	HTTP	46.15 KB	1.32 KBps	67	32	35
192.168.9.25	50,013	182.140.147.104	80	HTTP	46.09 KB	1.21 KBps	64	29	35
192.168.9.25	50,036	61.188.191.84	80	HTTP	45.36 KB	928.92 Bps	66	32	34

TCP セッション統計情報を表示する

TCP セッションビューには、通信ノード、ノードの地理的位置、ポート番号、アプリケーション、RTT、バイト数、パケット、および平均パケットサイズに基づくネットワークのトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、TCP セッションビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

TCP セッションビューにおける TCP セッションがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。ここのトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

UDP セッションビュー

下図のように、UDP セッションビューには、UDP セッションに基づくトラフィックの統計情報と解析が表示されます。

クライアントIP	クライアントポート	サーバーIP	サーバーポート	アプリケーション	バイト数	Pkts	pps	クライアント/パケ...	サーバー/パケ...
192.168.9.12	137	192.168.9.255	137	NetBIOS Name Service	12.02 KB	126	1.38 pps	126	0
192.168.9.76	137	192.168.9.255	137	NetBIOS Name Service	10.59 KB	113	2.69 pps	113	0
192.168.9.40	137	192.168.9.255	137	NetBIOS Name Service	5.53 KB	59	0.83 pps	59	0
192.168.9.25	137	192.168.9.255	137	NetBIOS Name Service	5.34 KB	57	1.12 pps	57	0
192.168.9.56	137	192.168.9.255	137	NetBIOS Name Service	2.25 KB	24	0.18 pps	24	0
192.168.9.76	51,359	239.255.255.250	1,900	SSDP	2.24 KB	13	1.18 pps	13	0
192.168.9.76	60,879	239.255.255.250	1,900	SSDP	2.24 KB	13	1.00 pps	13	0
192.168.9.18	137	192.168.9.255	137	NetBIOS Name Service	2.16 KB	23	0.25 pps	23	0
192.168.9.76	51,663	239.255.255.250	1,900	SSDP	1.89 KB	11	2.20 pps	11	0
192.168.9.39	137	192.168.9.255	137	NetBIOS Name Service	1.41 KB	15	0.07 pps	15	0
192.168.9.42	49,787	255.255.255.255	1,211	未知のUDP	1.38 KB	11	0.05 pps	11	0

UDP セッション統計情報を表示する

UDP セッションビューには、通信ノード、ノードの地理的位置、ポート番号、アプリケーション、バイト数、パケット、および平均パケットサイズに基づく、ネットワークのトラフィックが表示されます。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、UDP セッションビューで表示したいカラムを選択することができます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

UDPセッションビューにおけるユーシーピーセッションがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。ここのトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

アラームビュー

下図のように、アラームビューには、全てのアラームログが表示されます。

統計時間	トリガー時間	カテゴリ	アラーム名	アラームレベル	概要
04/16/2015 10:09:46	04/16/2015 10:09:45	異常トラフィック	トラフィックアラーム1	▲ 中	108.168.215.106, Bps : 45918 >= 10000
04/16/2015 10:09:47	04/16/2015 10:09:46	異常トラフィック	トラフィックアラーム1	▲ 中	108.168.215.106, Bps : 38960 >= 10000
04/16/2015 10:09:55	04/16/2015 10:09:54	異常トラフィック	トラフィックアラーム1	▲ 中	108.168.215.106, Bps : 114906 >= 10000
04/16/2015 10:09:41	04/16/2015 10:09:40	異常トラフィック	トラフィックアラーム1	▲ 中	108.168.215.106, Bps : 108958 >= 10000
04/16/2015 10:09:45	04/16/2015 10:09:44	異常トラフィック	トラフィックアラーム1	▲ 中	108.168.215.106, Bps : 105840 >= 10000
04/16/2015 10:09:43	04/16/2015 10:09:42	異常トラフィック	トラフィックアラーム1	▲ 中	108.168.215.106, Bps : 103000 >= 10000
04/16/2015 10:09:53	04/16/2015 10:09:52	異常トラフィック	トラフィックアラーム1	▲ 中	108.168.215.106, Bps : 101118 >= 10000
04/16/2015 10:09:55	04/16/2015 10:09:54	センシティブ情報	トラフィックアラーム2	▲ 高	192.168.9.25, Bps : 114906 >= 100000
04/16/2015 10:09:41	04/16/2015 10:09:40	センシティブ情報	トラフィックアラーム2	▲ 高	192.168.9.25, Bps : 108958 >= 100000
04/16/2015 10:09:45	04/16/2015 10:09:44	センシティブ情報	トラフィックアラーム2	▲ 高	192.168.9.25, Bps : 105840 >= 100000
04/16/2015 10:09:43	04/16/2015 10:09:42	センシティブ情報	トラフィックアラーム2	▲ 高	192.168.9.25, Bps : 103000 >= 100000
04/16/2015 10:09:53	04/16/2015 10:09:52	センシティブ情報	トラフィックアラーム2	▲ 高	192.168.9.25, Bps : 101118 >= 100000

アラームログを表示する

アラームビューには、アラームタイプに基づく、リンクアラームログが表示されます。ツールバーにおける「全てのアラーム」タブをクリックすることで全てのリンクアラームログを、「トラフィックアラーム」をクリックすることでトラフィックアラームログを、「Eメールアラーム」をクリックすることでEメールアラームログを、「ドメインアラーム」をクリックすることでドメインアラームログを、「特徴アラーム」をクリックすることで特徴アラームログを表示することができます。

全てのアラームログは、トリガー時間、カテゴリ、オブジェクト、アラーム名、およびアラームレベルによって、表示されます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

アラームビューにおけるアラームログがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。ここのトップ数はトリガー時間カラムによって、並べ替える項目数であることに注意してください。

新しいウィンドウでアラームログを解析する

あるアラームログを右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックすることで、このアラームログを専用的に解析することができます。

選択されたアラームログを専用的解析する新しいウィンドウは、元のリンク解析ウィンドウと同じく、上のタイムウィンドウと下の解析ビューから構成されています。ただし、新しいウィンドウにおけるタイムウィンドウは選択されたアラームログにおけるアドレス、またはは

アプリケーションのトラフィックチャートのみを表示するのに対して、元のリンク解析ウィンドウにおけるタイムウィンドウは全体ネットワークのトラフィックチャートを表示します。

トラフィックアラームログの解析は、Eメールアラームログ、ドメインアラームログ、および特徴アラームログの解析とは異なっています。

新しいウィンドウでトラフィックアラームログを解析するのは、実際のところ、新しいウィンドウでIPアドレス、MACアドレス、アプリケーションのようなトリガースソースを解析することです。トリガースソースによって、トレントチャートと解析ビューも異なります。以下のリストは、その詳しいことについて説明しています。

- IPアドレスがトリガースソースである場合、新しいウィンドウでトラフィックアラームを解析することは、IPアドレスビューにおけるノードの解析となっています。
- MACアドレスがトリガースソースである場合、新しいウィンドウでトラフィックアラームを解析することは、MACアドレスビューにおけるノードの解析となっています。
- アプリケーションがトリガースソースである場合、新しいウィンドウでトラフィックアラームを解析することは、アプリケーションビューにおけるアプリケーションの解析となっています。

新しいウィンドウでEメールアラームログ、ドメインアラームログ、および特徴アラームログを解析するのは、実際のところ、新しいウィンドウで送信元IPアドレス、または宛先IPアドレスを解析することです。

新しいウィンドウでEメールアラームログ、ドメインアラームログ、および特徴アラームログを解析するには、そのログを右クリックし、ポップアップされたメニューにおける「新しいウィンドウで解析する」をクリックし、適切なIPアドレスをクリックして、新しいウィンドウを開きます。したがって、一度に一つのIPアドレスを解析することができます。

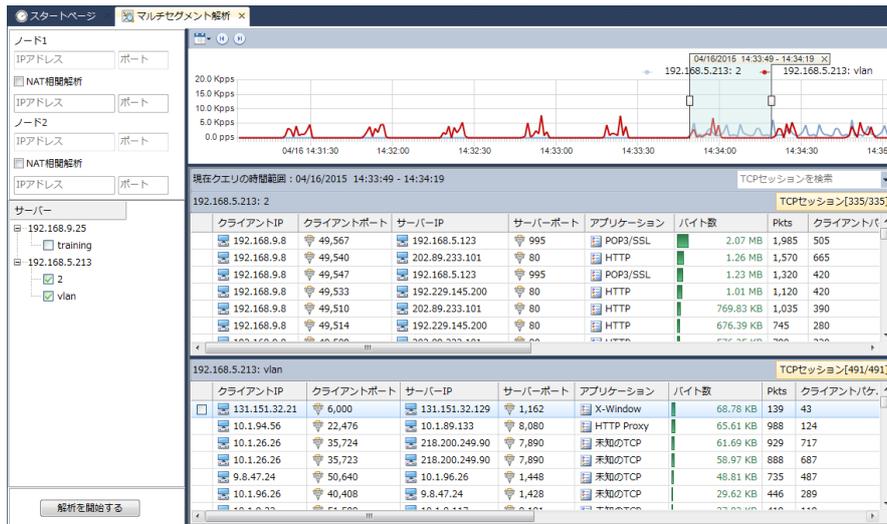
マルチセグメント解析

マルチセグメント解析は、複数セグメントにおけるセッションの相関解析で、パケットロス、ネットワーク遅延、再送信および他の関連情報を提供します。

マルチセグメント解析は、複数セグメントにおけるセッションの概要解析と詳細解析を提供します。

概要解析

TCPセッションビュー、またはIPセッションビューにおいて、関心のセッションを右クリックし、「マルチセグメント解析」をクリックするか、あるいはツールバーにおける  ボタンをクリックします。マルチセグメント解析ウィンドウは下図のように表示されます。



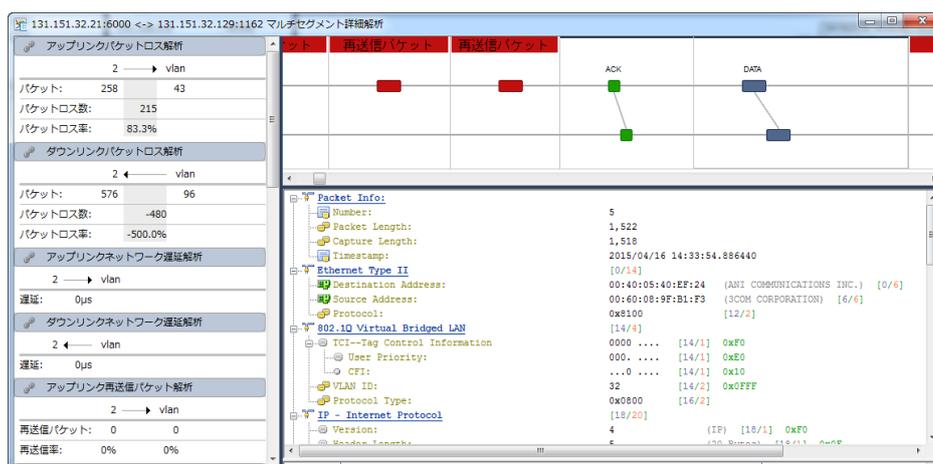
「NAT 相関解析」は NAT 解析を設定するものです。それを有効にして、IP アドレスとポート番号を入力します。

マルチセグメント解析は、最大で三つのネットワークリンクの同時解析をサポートしています。サーバーが接続されていない場合、ダブルクリックし、サーバーに接続して、適切なネットワークリンクを選択します。

マルチセグメント解析のセッションを選択する際に、他のネットワークリンクが同じセッションを持っている場合、このセッションは自動的に選択され、ハイライト表示されます。

詳細解析

マルチセグメントウィンドウにおいて、関心のあるセッションをクリックし、「解析を開始する」をクリックします。マルチセグメント詳細解析ウィンドウは、下図のように表示されます。



マルチセグメント詳細解析ウィンドウは、パラメータの統計情報を表示する左のパネル、タイムシーケンス図、パケットデコーディングパネルから構成されています。

左のパネルは、アップリンクとダウンリンクのパケットロス、アップリンクとダウンリンクのネットワーク遅延、アップリンクとダウンリンクの再送信、アップリンクとダウンリンクの TCP フラグなどの統計情報を提供します。

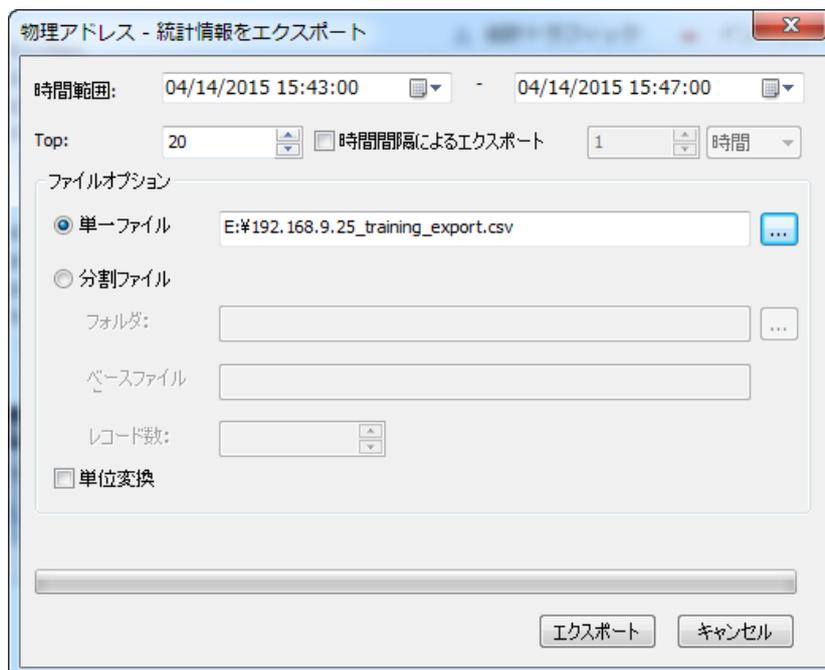
タイムシーケンス図は、セッション時間を横軸にして、ネットワークリンク間でのパケット転送を表示します。

タイムシーケンス図におけるパケットをクリックすると、パケットデコーディングパネルには、そのパケットの詳細なデコーディング情報が表示されます。

統計情報をエクスポート

以下のステップに従い、統計情報をエクスポートします。

1. ツールバーにおけるをクリックして、下図のように統計情報をエクスポートするダイアログボックスが表示されます。



2. ダイアログボックスを完了して、「エクスポート」をクリックします。

注意 概要ビューにおける統計情報をエクスポートするダイアログボックスは、他の解析ビューにおける統計情報をエクスポートするダイアログボックスとは異なっています。

統計情報をエクスポートするダイアログボックス

以下のリストは、統計情報をエクスポートするダイアログボックスにおける各項目について説明しています。

- **時間範囲**: このオプションはエクスポートする統計情報の時間範囲を指定するために設けられています。テキストボックスにおける数字をクリックするか、小さな三角形をクリックして、時間を指定することができます。デフォルトでは、タイムウィンドウで選択された時間範囲がある場合、ここの時間範囲はその選択された範囲と同じになっています。タイムウィンドウで選択された時間範囲がない場合、ここの時間範囲はタイムウィンドウの範囲と同じになっています。
- **トップ数**: このオプションは、エクスポートされる統計情報のトップ項目数を指定するために設けられています。トリガー時間によって並べ替えるアラームビューを除いて、他の全ての解析ビューにおける統計項目は、バイト数カラムの値によって並

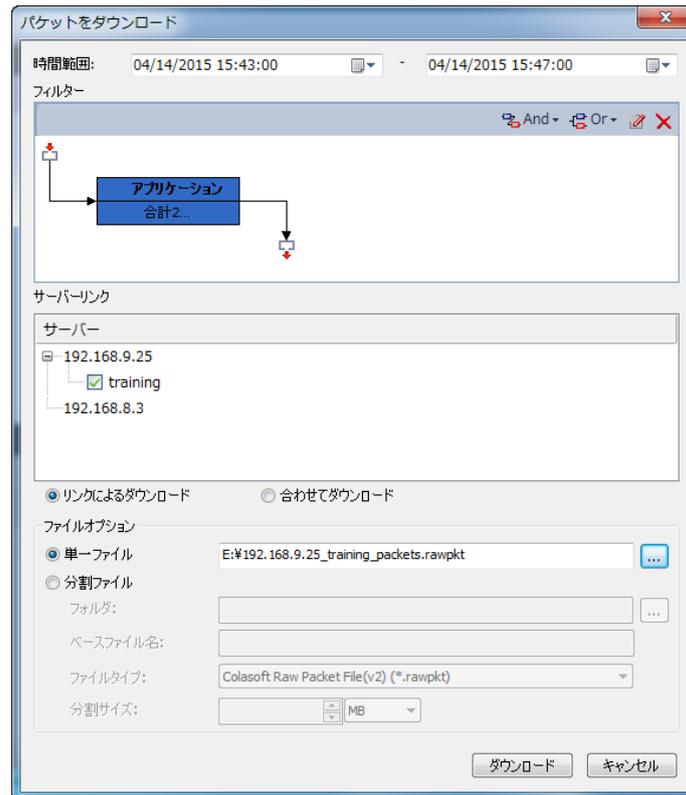
べ替えています。このオプションは、概要ビューでは、利用できません。

- **時間間隔によるエクスポート:**このオプションは、指定された時間間隔に応じて、選択された時間範囲の統計情報をエクスポートすることを示しています。例えば、時間範囲を8時間に、時間間隔を1時間にする場合、1時間の統計情報に一つ、8時間の統計情報を八つの部分にエクスポートします。
- **単一ファイル:**このオプションが選択されると、選択された時間範囲の統計情報が一つのファイルにエクスポートされます。をクリックして、ファイルパスとファイル名を指定することができます。
- **分割ファイル:**このオプションが選択されると、選択された時間範囲の統計情報が分割ファイルにエクスポートされます。そして、以下のオプションについて、設定する必要があります。
 - **フォルダ:**このオプションは分割ファイルを保存するフォルダを指定するために設けられています。
 - **ベースファイル名:**このオプションは、ファイル名における接頭語部分を指定するために設けられています。
 - **レコード数:**このオプションは一つのファイルに含まれているレコード数を指定するために設けられています。一つのファイルに含まれているレコード数が設定された数に達すると、他のレコードを保存するために新しいファイルが生成されます。
- **単位変換:**このオプションにチェックを入れると、統計情報の単位変換が自動的に行われます。例えば、統計情報が1024 bytesの場合、このオプションにチェックを入れると、統計情報が1 KBになります。
- **進行状況:**このオプションは、エクスポートの進行状況とエクスポートされたレコードの合計数を表示するために設けられています。

パケットのダウンロード

以下のステップに従い、パケットをダウンロードします。

1. ツールバーにおけるをクリックすることで、パケットをダウンロードするダイアログボックスは下図のように表示されます。



2. ダイアログボックスを完了して、「ダウンロード」をクリックします。

パケットをダウンロードするダイアログボックス

以下のリストは、パケットをダウンロードするダイアログボックスにおける各項目について説明しています。

- 時間範囲:** このオプションはダウンロードするパケットの時間範囲を指定するために設けられています。テキストボックスにおける数字をクリックするか、小さな三角形をクリックして、時間を指定することができます。デフォルトでは、タイムウィンドウで選択された時間範囲がある場合、ここの時間範囲はその選択された範囲と同じになっています。タイムウィンドウで選択された時間範囲がない場合、ここの時間範囲はタイムウィンドウの範囲と同じになっています。
- フィルター:** このオプションは必要ではないパケットをフィルターするために設けられています。論理的な And 関係と OR 関係でアプリケーション、セッション、アドレス、ポート、およびネットワークセグメントなどによってフィルターを設定することができます。
- リンクによるダウンロード:** このオプションが有効にされた場合、パケットはネットワークリンクに応じて別々にダウンロードされます。
- 合わせてダウンロード:** このオプションが有効にされた場合、複数ネットワークリンクのパケットは一緒にダウンロードされます。
- 単一ファイル:** このオプションが選択されると、選択された時間範囲のパケットを一つのファイルにダウンロードされます。  をクリックして、ファイルパスとファイル名を指定することができます。
- 分割ファイル:** このオプションが選択されると、選択された時間範囲のパケットが分割ファイルにダウンロードされます。そして、以下のオプションについて、設定す

る必要があります。

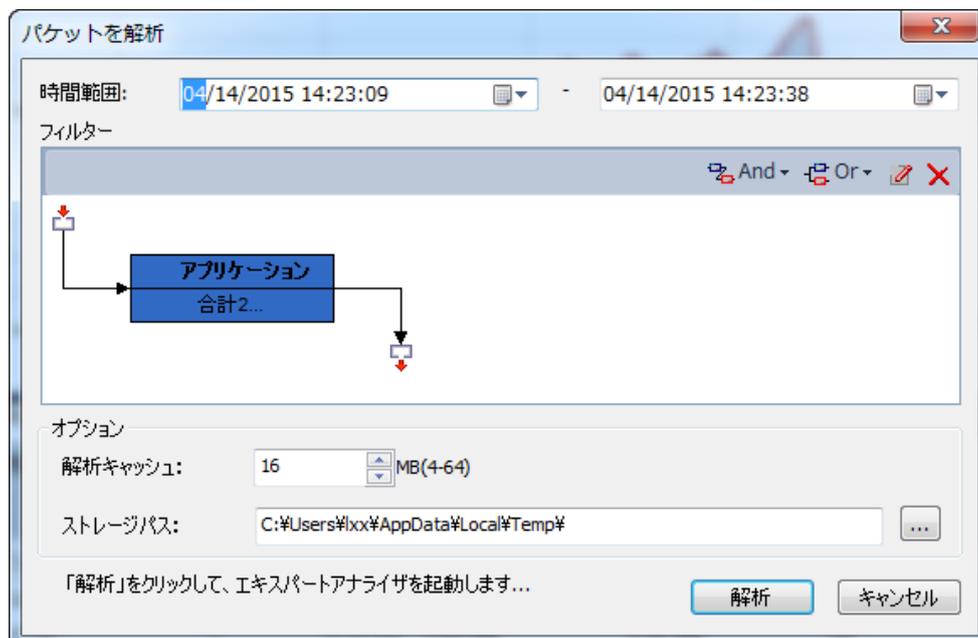
- **フォルダ:** このオプションは分割ファイルを保存するフォルダを指定するために設けられています。
- **ベースファイル名:** このオプションは、ファイル名における接頭語部分を指定するために設けられています。
- **ファイルタイプ:** このオプションはパケットを保存するパケットファイルのフォーマットを指定するために設けられています。パケットを.rawpkt フォーマットと.cap フォーマットに保存することができます。
- **分割サイズ:** このオプションはダウンロードされたパケットのファイルサイズを指定するために設けられています。ダウンロードされたパケットは分割サイズに応じて自動的に分割ファイルに分割されます。

エキスパートアナライザで解析

エキスパートアナライザは、エキスパート解析と診断を提供し、ダウンロードされたパケットをデコードします。

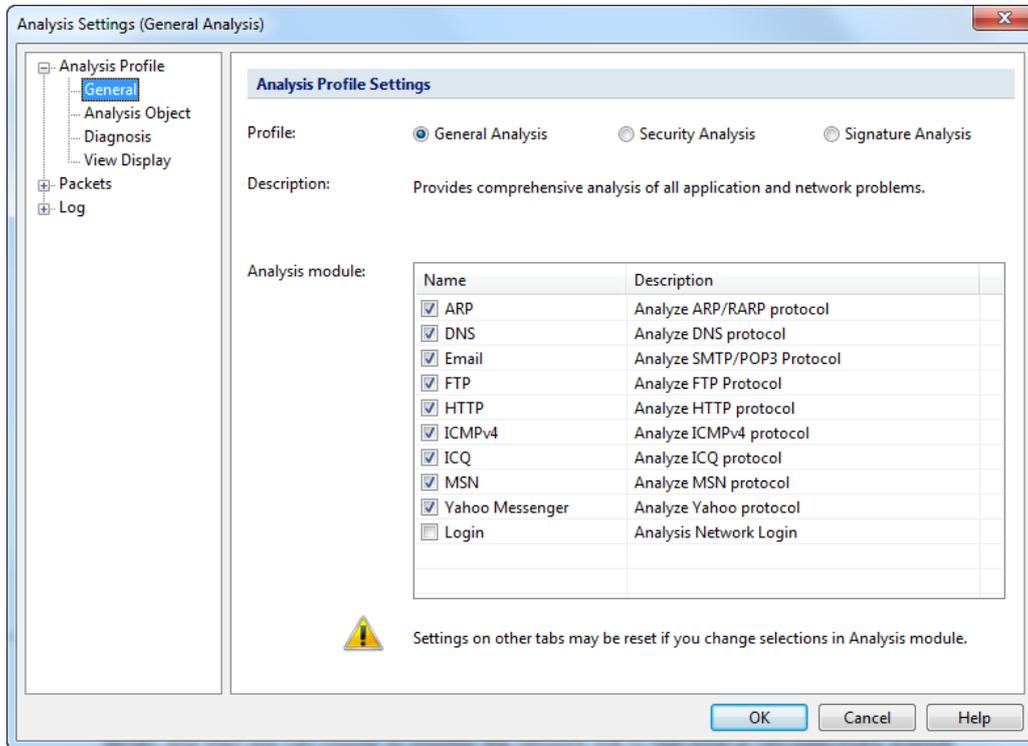
以下のステップに従い、エキスパートアナライザでパケットを解析します。

1. 解析ビューにおけるツールバーでをクリックすることで、「パケットを解析」するダイアログボックスが下図のように表示されます。



- **時間範囲:** このオプションは解析されるパケットの時間範囲を指定するために設けられています。テキストボックスにおける数字をクリックするか、小さな三角形をクリックして、時間を指定することができます。デフォルトでは、タイムウィンドウで選択された時間範囲がある場合、ここの時間範囲はその選択された範囲と同じになっています。タイムウィンドウで選択された時間範囲がない場合、ここの時間範囲はタイムウィンドウの範囲と同じになっています。

- ・ **フィルター**:このオプションは、特定の packets をフィルターするために設けられています。「And」と「Or」をクリックして、フィルター条件を定義することができます。
- 解析される時間範囲を指定し、フィルターを設定し、「解析」をクリックすることで、エキスパートアナライザ Colasoft Capsa が起動されます。



- 解析プロファイルを選択、設定し、「スタート」をクリックすることで、エキスパートアナライザで packets を解析します。

ヒント 解析ビューで右クリックし、「packets を解析」をクリックして、packets を解析するダイアログボックスを開くこともできます。

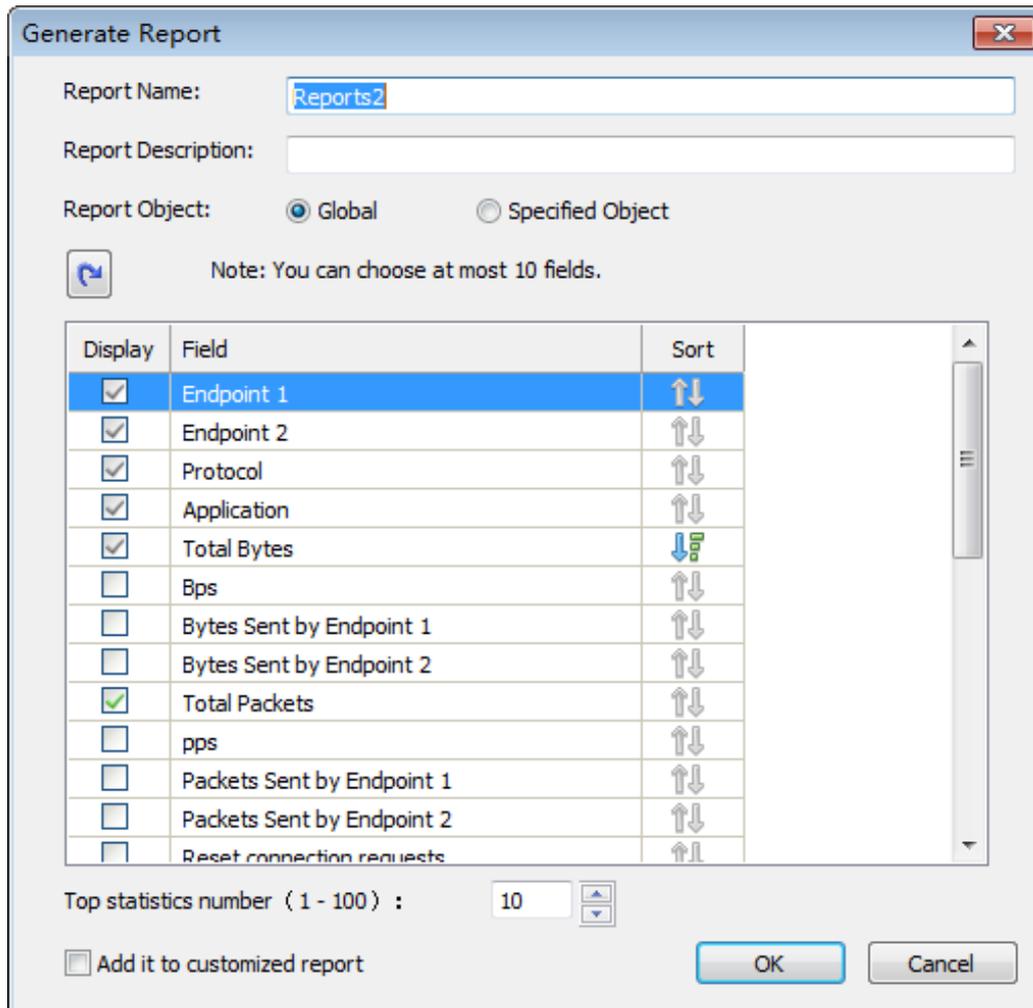
エキスパートアナライザの詳しい情報について、エキスパートアナライザを起動した後、「F1」キーを押すことで、エキスパートアナライザのヘルプドキュメントを取得することができます。

一時的なレポートを生成

一時的なレポートとは、統計ビューで直接生成されたレポートのことです。

以下のステップに従い、一時的なレポートを生成します。

- 統計ビューで ボタンをクリックして、レポートを生成するダイアログボックスが表示されます。



2. レポートの名前、説明、オブジェクト、統計フィールドなどを設定して、OK をクリックすることで、レポートウィンドウに遷移し、生成された一時的なレポートが表示されます。

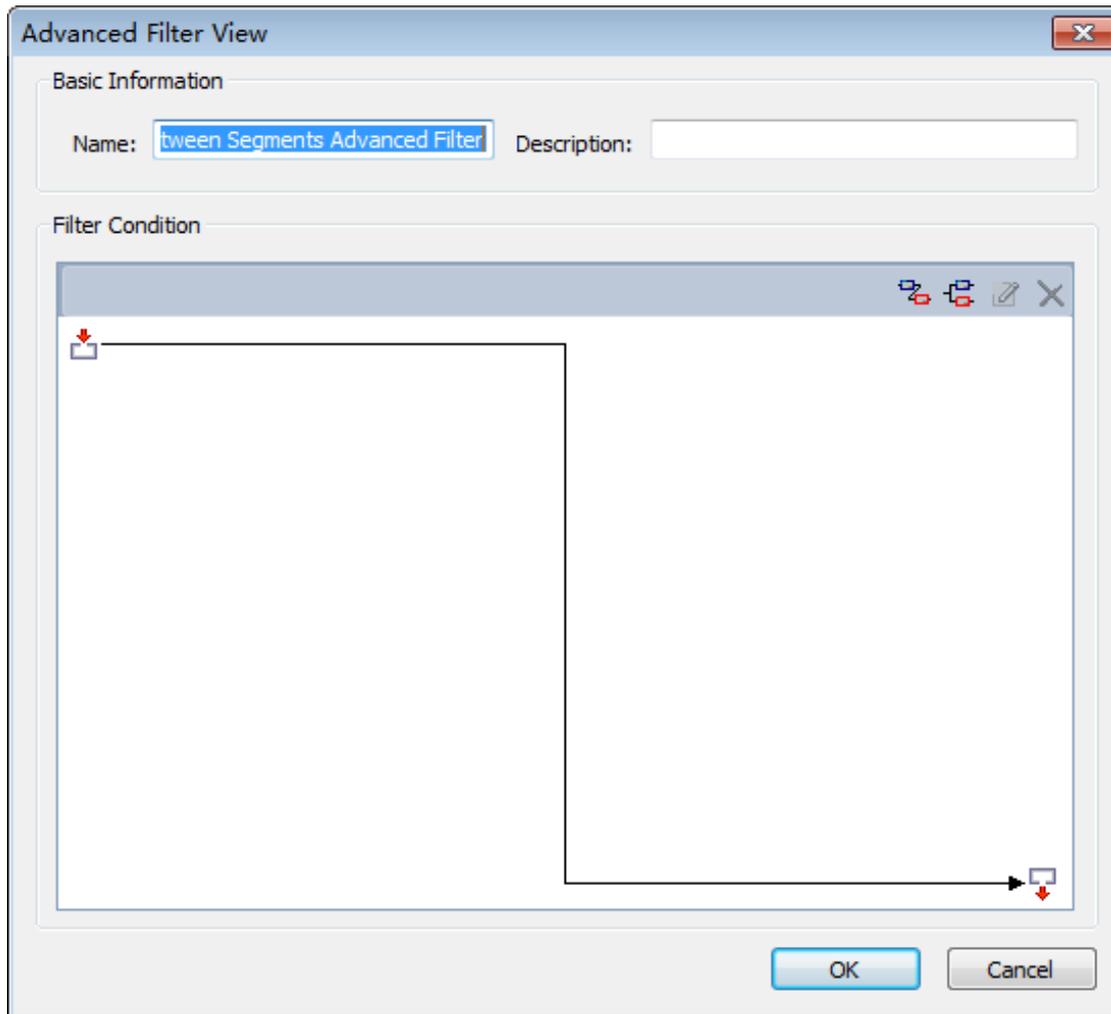
注意 レポートウィンドウを閉じると、生成された一時的なレポートも削除されます。一時的なレポートを生成するとき、「ユーザー定義のレポートに追加」にチェックを入れると、その一時的なレポートをユーザー定義のレポートに追加し、保存することができます。

統計ビューにおける高度なフィルター

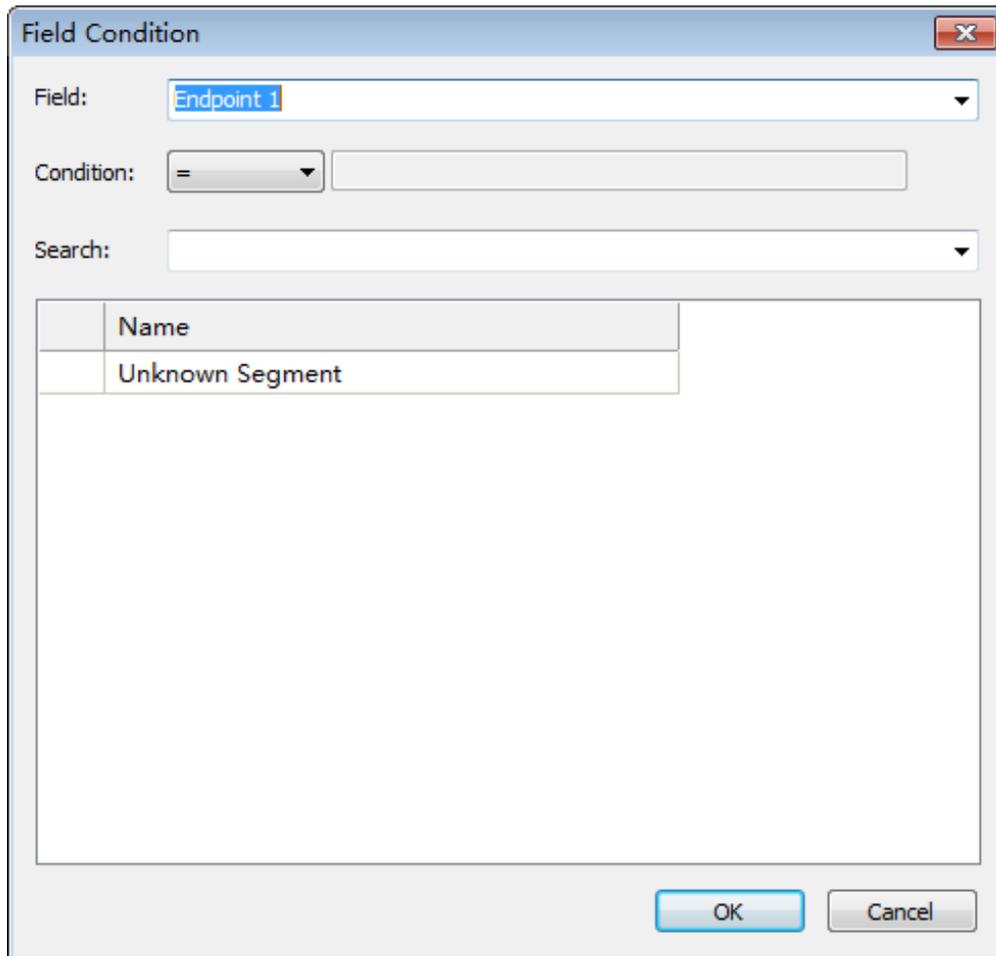
概要ビューを除いて、リンク解析の各統計ビューには高度なフィルターを提供します。高度なフィルターでは現在統計ビューにおける統計フィールドに対して、フィルター条件を設定することで、フィルター条件と一致した項目だけが表示されます。

以下のステップに従い、高度なフィルターを設定します。

1. 統計ビューにおける  ボタンをクリックし、または統計ビューで右クリックし、ポップアップされたメニューで「高度なフィルター」をクリックすることで、下図のように高度なフィルターダイアログボックスが表示されます。



2. 高度なフィルターでは、フィルター条件を設定することで、一つまたは複数の統計フィールドをフィルタリングすることができます。複数統計フィールドは「And」関係または「Or」関係で結ばれています。And ボタンまたは Or ボタンをクリックして、下図のようにフィールド条件を設定するダイアログボックスが表示されます。



The image shows a 'Field Condition' dialog box. It has a title bar with a close button (X). The dialog contains the following fields:

- Field:** A dropdown menu with 'Endpoint 1' selected.
- Condition:** A dropdown menu with '=' selected, followed by an empty text input field.
- Search:** A dropdown menu.

Below these fields is a table with the following content:

Name
Unknown Segment

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

3. フィールド条件を設定して、OK をクリックすることで高度なフィルターの設定を完了します。高度なフィルターの設定が終わったら、フィルター条件と一致した項目だけが統計ビューに表示されます。

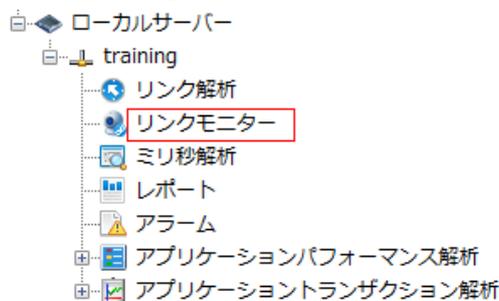
リンクモニター

nChronos サーバーに接続したら、サーバーエクスプローラにおけるサーバーの下にネットワークリンクが表示されます。そしてネットワークリンクをリアルタイムに監視するか、ネットワークリンクを適時的に解析するかを選択することができます。この章では、ネットワークリンクを監視する方法とリンクモニターウィンドウにおける要素について説明しています。

リアルタイムにネットワークリンクを監視

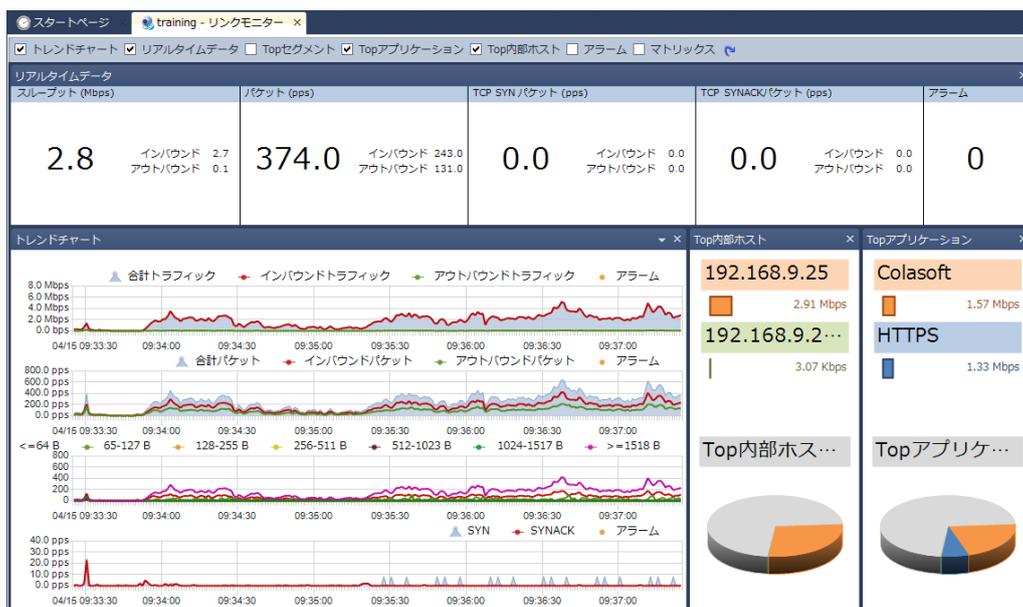
ネットワークリンクをリアルタイムに監視するには、

1. サーバーに接続して、サーバーエクスプローラにおけるサーバーの下に作成されたネットワークリンクが表示されます。
2. ネットワークリンクの下にある「リンクモニター」ノードをダブルクリックして、モニターウィンドウを開きます。



リンクモニターウィンドウ

監視されたネットワークリンクがある場合、リンクモニターウィンドウには、下図のようにそのネットワークリンクのリアルタイム状況が表示されます。



リンクモニターウィンドウは、トップバーといくつかのパネルからなっています。パネルには、リアルタイムデータパネル、トレンドチャートパネル、トップセグメントパネル、トップ

内部ホストパネル、トップアプリケーションパネル、アラームパネル、マトリックスパネルがあります。

トップバーは、7つのパネルを表示、または非表示するチェックボックスとデフォルトレイアウトボタンからなっています。パネルの前にあるチェックボックスにチェックを入れると、そのパネルを表示することができます。  をクリックして、リンクモニターウィンドウのデフォルトレイアウトを表示することができます。

パネルを閉じるには、各パネルの右上にある閉じるボタンをクリックするか、リンクモニターウィンドウのトップバーにおけるパネル名の前にあるチェックを外すことができます。

パネル間にマウスポインタを移動して、ポインターが両方向の矢印になると、マウスをドラッグすることで、パネルのサイズを変更することができます。

リアルタイムデータパネル

リアルタイムデータパネルには、スループット、パケット、帯域幅利用率、TCP SYN パケット、TCP SYNACK パケット、アラーム数を含む、ネットワークリンクのリアルタイムデータが表示されます。

リアルタイムデータパネルで右クリックして、リフレッシュ間隔を設定することができます。

さらに、リアルタイムデータパネルで右クリックして、表示、または非表示するリアルタイムデータのタイプを選択することができます。

トレンドチャートパネル

時間スケールでマークされた横軸と値スケールでマークされた縦軸を持っているリンクモニターウィンドウにおけるトレンドチャートは、ネットワークリンクのリアルタイム状況を表示します。トレンドチャートは自動的に右から左へ更新され、最新のデータを表示します。トレンドチャートを利用することで、ネットワーク状況を直接に確認することができます。

デフォルトでは、全てのトレンドチャートは、4分を横軸にして、4分ウィンドウで表示されます。そして、トレンドチャートは1秒ごとに更新されます。当然、他のタイムウィンドウタイプで表示することもできます。

他のタイムウィンドウでトレンドチャートを表示するには、トレンドチャートを右クリックし、適切なタイムウィンドウタイプを選択します。以下の表は、トレンドチャートにおけるタイムウィンドウタイプ、タイムスパン、リフレッシュ間隔をリストしています。

タイムウィンドウタイプ	タイムスパン	リフレッシュ間隔
4分ウィンドウ	4分	1秒
20分ウィンドウ	20分	5秒
1時間ウィンドウ	1時間	15秒
4時間ウィンドウ	4時間	1分
8時間ウィンドウ	8時間	2分
12時間ウィンドウ	12時間	3分

24 時間ウィンドウ	24 時間	6 分
2 日ウィンドウ	2 日	12 分
10 日ウィンドウ	10 日	1 時間
40 日ウィンドウ	40 日	4 時間

トップセグメントパネル

トップセグメントパネルには、ネットワークセグメントのトラフィックに応じて並べ替えるトップネットワークセグメントが表示されます。そのトラフィックは、セグメントの下に棒グラフとリアルタイムグラフの形式で表示されます。セグメントは、ネットワークリンクを設定する際に、定義されています。

トップセグメントリストの下にカラ円グラフがあります。一つの色は対応するトップセグメントを表しています。2つ以上のセグメントが一つの色を共有する場合、その色は、対応するセグメントの合計を表しています。

トップセグメントパネルで右クリックし、適切なリフレッシュ間隔を選択することで、トップセグメントパネルのリフレッシュ間隔を設定することができます。

また、トップセグメントのトップ数を設定することもできます。

トップ内部ホストパネル

トップ内部ホストパネルには、内部ホストのトラフィックに応じて並べ替えるトップ内部ホストが表示されます。そのトラフィックは、ホストの下に棒グラフとリアルタイムグラフの形式で表示されます。ビューメニューで設定されているように、ホストは名前、または IP アドレスとして表示されます。

トップ内部ホストリストの下にカラ円グラフがあります。一つの色は対応するトップ内部ホストを表しています。2つ以上のホストが一つの色を共有する場合、その色は、対応するホストの合計を表しています。

トップ内部ホストパネルで右クリックし、適切なリフレッシュ間隔を選択することで、トップ内部ホストパネルのリフレッシュ間隔を設定することができます。

トップアプリケーションパネル

トップアプリケーションパネルには、アプリケーションのトラフィックに応じて並べ替えるトップアプリケーションが表示されます。そのトラフィックは、アプリケーションの下に棒グラフとリアルタイムグラフの形式で表示されます。

このアプリケーションには、システムアプリケーションとカスタムアプリケーションが含まれていますが、カスタムアプリケーションは、システムアプリケーションより優先されています。システムアプリケーションは、サーバーを設定する際に、ライブラリーにアップロードされます。一方、カスタムアプリケーションは、ネットワークリンクを設定する際にカスタマイズされることができます。

トップアプリケーションリストの下にカラ円グラフがあります。一つの色は対応するトップアプリケーションを表しています。2 つ以上のアプリケーションが一つの色を共有する場合、その色は、対応するアプリケーションの合計を表しています。

トップアプリケーションパネルで右クリックし、適切なリフレッシュ間隔を選択することで、トップアプリケーションパネルのリフレッシュ間隔を設定することができます。また、トップアプリケーションのトップ数を設定することもできます。

アラームパネル

アラームパネルには、トリガー時間、アラームカテゴリ、アラームオブジェクト、アラーム名、アラームレベル、およびトリガー条件によって、1 秒内でトリガーされた全てのアラームが表示されます。

全てのアラームはネットワークリンクを設定する際に、定義されています。さらに、特徴アラームはサーバーを設定する際に、ライブラリーにアップロードされるすることができます。

マトリックスパネル

マトリックスパネルでは、マトリックスグラフでネットワーク通信を表示します。

マウスをあるノードの上に移動すると、そのノードの送信パケットとバイト数、および受信パケットとバイト数が表示されます。ピアノード間の直線もハイライト表示されます。

デフォルトでは、マトリックスパネルは、IP アドレス間の通信マトリックスグラフを表示します。マトリックスパネルで右クリックし、「MAC マトリックスグラフ」を選択することで、MAC アドレス間の通信マトリックスグラフを表示することができます。

さらにマトリックスパネルで右クリックし、適切なリフレッシュ間隔を選択することで、マトリックスパネルのリフレッシュ間隔を設定することができます。

ミリ秒解析

ミリ秒解析は、1 ミリ秒精度のトラフィック解析を提供します。

サーバーを設定する際に、ネットワークリンクのミリ秒統計を有効にしないと、ミリ秒解析ウィンドウは利用できません。例えば、下図のネットワーク「training」は、ミリ秒統計を有効しています。

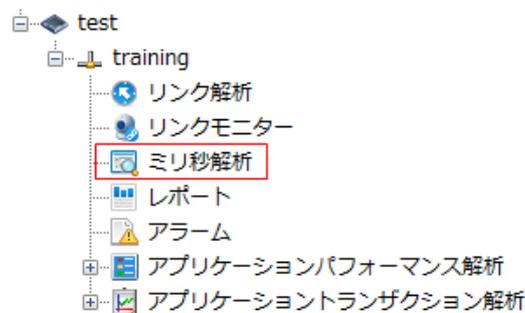
ネットワークリンク/ネットワークリンクを編集する

リンク名:

リンクタイプ:

ミリ秒統計を有効にする

そして、ネットワークリンク「training」には、ミリ秒解析が提供されています。

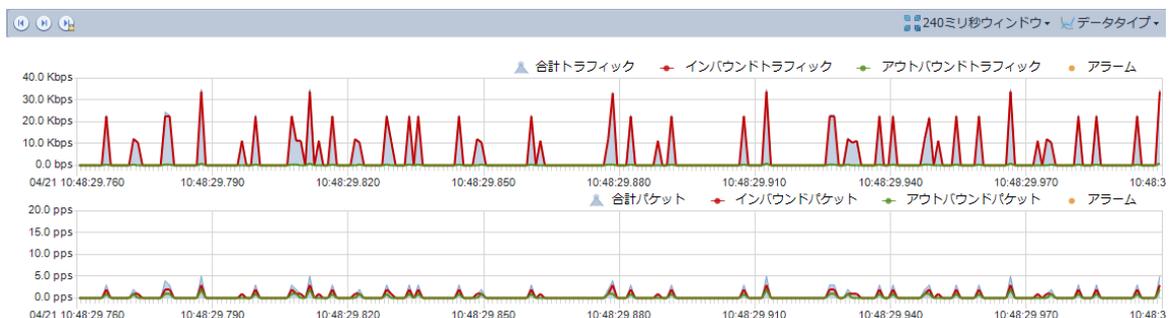


ミリ秒解析ウィンドウは、タイムウィンドウと2つの解析ビューから構成されています。

タイムウィンドウ

ミリ秒解析のタイムウィンドウは、240 ミリ秒ウィンドウで、横軸における最小目盛りは1 ミリ秒です。

タイムウィンドウには、トラフィックとパケットという2つのタイプのチャートがあります。



ミリ秒解析のタイムウィンドウは、リンク解析のタイムウィンドウとは類似していて、マウスを移動したり、ドラッグしたりして、履歴トラフィックを表示することができます。

概要ビュー

タイムウィンドウで時間範囲が選択された場合、概要ビューには、その時間範囲の概要統計が表示されます。その統計はパケット情報とバイト数情報からなっています。

概要 ミリ秒におけるトラフィックアラーム					
選択した時間範囲 : 04/21/2015 10:48:29.803 - 10:48:29.855					
Pkts	インバウンド	アウトバウンド	バイト数	インバウンド	アウトバウンド
34	23	11	32.38 KB	31.76 KB	638.00 B

ボタンをクリックして、選択された時間範囲を含んでいるその1秒のパケットをダウンロードすることができます。

ボタンをクリックして、選択された時間範囲を含んでいるその1秒のパケットをエキスパートアナライザで解析することができます。

ボタンをクリックして、選択された時間範囲を含んでいるその1秒の統計情報をエクスポートすることができます。

ミリ秒におけるトラフィックアラームビュー

ミリ秒におけるトラフィックアラームビューには、選択された時間範囲内でトリガーされた全てのミリ秒トラフィックアラームが表示されます。

概要 ミリ秒におけるトラフィックアラーム						
選択した時間範囲 : 04/14/2015 16:29:58.772 - 16:29:58.860						
統計時間	ミリ秒トリガー時間	カテゴリ	オブジェクト	アラーム名	アラームレベル	トリガー条件
04/14/2015 16:29:58	2015/04/14 16:29:57.808	異常トラフィック	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 低	1ミリ秒におけるバイト数: 3094 >= 10
04/14/2015 16:29:58	2015/04/14 16:29:57.808	センシティブ情報	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 中	1ミリ秒におけるバイト数: 3094 >= 1000
04/14/2015 16:29:58	2015/04/14 16:29:57.820	異常トラフィック	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 低	1ミリ秒におけるバイト数: 3176 >= 10
04/14/2015 16:29:58	2015/04/14 16:29:57.820	センシティブ情報	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 中	1ミリ秒におけるバイト数: 3176 >= 1000
04/14/2015 16:29:58	2015/04/14 16:29:57.821	異常トラフィック	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 低	1ミリ秒におけるバイト数: 1588 >= 10
04/14/2015 16:29:58	2015/04/14 16:29:57.821	センシティブ情報	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 中	1ミリ秒におけるバイト数: 1588 >= 1000
04/14/2015 16:29:58	2015/04/14 16:29:57.831	異常トラフィック	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 低	1ミリ秒におけるバイト数: 3094 >= 10
04/14/2015 16:29:58	2015/04/14 16:29:57.831	センシティブ情報	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 中	1ミリ秒におけるバイト数: 3094 >= 1000
04/14/2015 16:29:58	2015/04/14 16:29:57.832	異常トラフィック	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 低	1ミリ秒におけるバイト数: 1576 >= 10
04/14/2015 16:29:58	2015/04/14 16:29:57.832	センシティブ情報	ミリ秒におけるトラフィックアラーム	ミリ秒における...	▲ 中	1ミリ秒におけるバイト数: 1576 >= 1000

全てのアラームログは、ミリ秒トラフィック統計時間、トリガー時間、アラームカテゴリ、アラーム名、アラームレベル、トリガーソース、およびトリガー条件によって、表示されています。さらに、カラムヘッダーにおけるカラム名をクリックして、そのカラムによってアラームログを並べ替えることができます。

このビューにおけるアラームログがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。ここのトップ数はトリガー時間によって、並べ替える項目数であることに注意してください。このビューにおける全ての統計項目を表示したい場合、 をクリックし、「全てを表示」をクリックすればよいです。

レポート

nChronos はデフォルトでシステムレポートを提供していますが、ユーザーは自分でレポートを定義することもできます。デフォルトレポートとユーザー定義のレポートの両方が E メールで送信することができます。さらにレポートをスケジュールすることもできます。

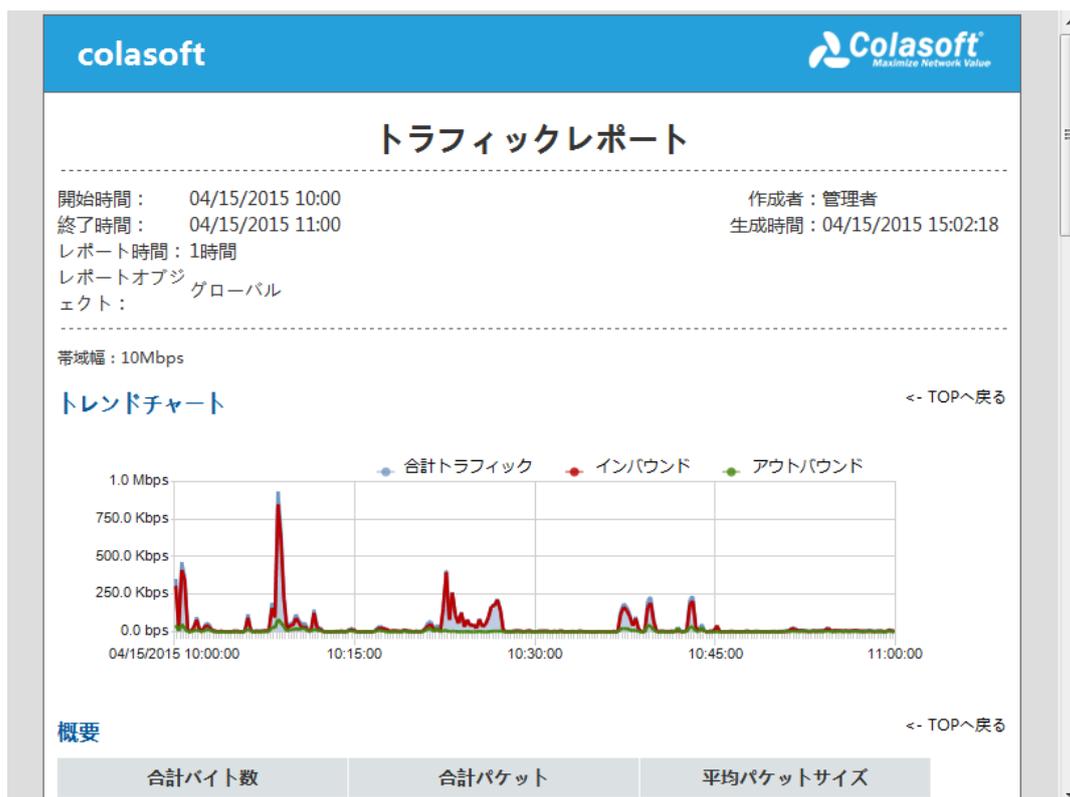
レポートビューのタイプによって、レポートには、インスタントレポートとスケジュールされたレポートがあります。

インスタントレポートは nChronos コンソールにおけるレポートウィンドウで直接表示され、システムレポートとユーザー定義のレポートのいずれかである可能性があります。

スケジュールされたレポートは、ユーザーによってスケジュールされたレポートで、E メール受信トレイでしか利用できません。

インスタントレポート

インスタントレポートは下図のように表示されます。



ユーザーがコンソールでレポートを見たい場合、左パネルにおけるレポート名をクリックすればよいです。レポートの統計時間は、デフォルトで過去1時間となっていますが、ユーザーはレポート時間ドロップダウンリストをクリックして、関心のある時間範囲を選択するか、デフォルト時間をクリックして、変更することができます。履歴データと比較して、レポート統計を生成したい場合、まず「レポート時間」をクリックし、レポート時間ダイアログボックスを開きます。そして、レポート時間ダイアログボックスにおける「比較時間」にチェックを入れて、比較時間を設定すればよいです。

ヒント 統計情報を比較する場合、0.00%は、変化がないことを表し、∞%は比較された時間範囲内でデータがないことを表しています。

インスタントレポートは、印刷、保存、およびEメールで送信されることができます。

印刷



をクリックして、インスタントレポートを印刷します。

ヒント IPトラフィック、MACアドレス、またはセグメントレポートモジュールを含むインスタントレポートを印刷する場合、ランドスケープ印刷がお勧めです。

保存

nChronos コンソールでインスタントレポートを表示することができますが、自動的に保存することができません。 をクリックして、インスタントレポートを保存することができます。

Eメール

インスタントレポートは、Eメール受信者に送信することができます。

インスタントレポートをEメールで送信するには、

1.  をクリックして、レポートを送信するダイアログボックスを開きます。



2. 受信者を指定します。
受信者アドレスがリストにない場合、空リストをクリックして、新しい受信者アドレスを入力することができます。
3. 「今すぐ送信」をクリックして、インスタントレポートを送信します。
「スケジュール」をクリックして、インスタントレポートに基づいて、レポートをスケジュールすることができます。

注意 レポートを送信する前に、サーバー管理ウェブでSMTPが正しく設定されていることを確認してください。

システムレポート

nChronos は、デフォルトで 12 種類のシステムレポートを提供します。これらのシステムレポートは編集、または削除されることができませんが、複製されることができます。システムレポートを複製して、複製されたレポートに対していくつかの変更を行うことで、効率的にユーザー定義のレポートを取得することができます。

システムレポートは以下のものから構成されています。

レポート名	レポートモジュール	サポートされているレポートスコープ
グローバルレポート	トレンドチャート、概要、パケットサイズ分布、トップアプリケーション、トップホスト、トップセグメント、アラーム	グローバル、IP アドレス、MAC アドレス、アプリケーション、セグメント
トラフィックレポート	トレンドチャート、概要、パケットサイズ分布、インバウンド&アウトバウンド、ピーク値	グローバル、IP アドレス、MAC アドレス、アプリケーション、セグメント
IP トラフィックレポート	IP トラフィック	グローバル、IP アドレス
IP アプリケーションレポート	IP アプリケーション分布	グローバル、IP アドレス、セグメント
MAC トラフィックレポート	MAC トラフィック	グローバル、MAC アドレス
アラームレポート	アラーム	グローバル
アプリケーションパフォーマンスレポート	アプリケーションパフォーマンス	グローバル、アプリケーション
アプリケーショントランザクションレポート	アプリケーショントランザクション	グローバル、アプリケーション
トップアプリケーションレポート	トップアプリケーション	グローバル
トップホスト	トップホスト	グローバル

レポート		
トップ内部ホ ストレポート	トップ内部ホスト	グローバル
トップセグメ ントレポート	トップセグメント	グローバル

ユーザー定義のレポート

ユーザーは、2つの方法でレポートを作成することができます。

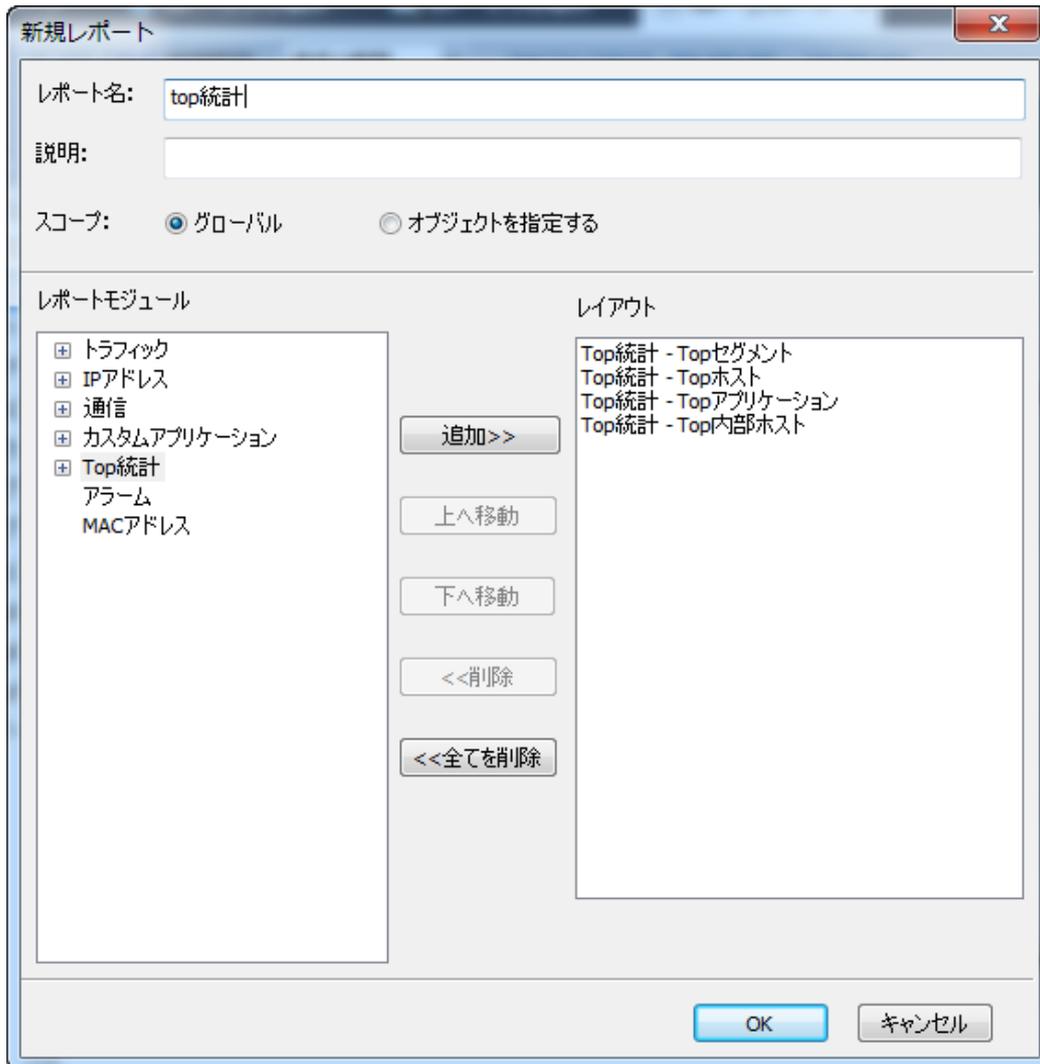
- レポートの作成: 全く新しいレポートを作成します。
- レポートの複製: 既存のレポートを複製し、複製されたレポートに対していくつかの変更を行うことで、迅速に新しいレポートを追加することができます。

レポートの作成

ビルトインレポートモジュールに基づいて、レポートを作成することができます。

レポートを作成するには、

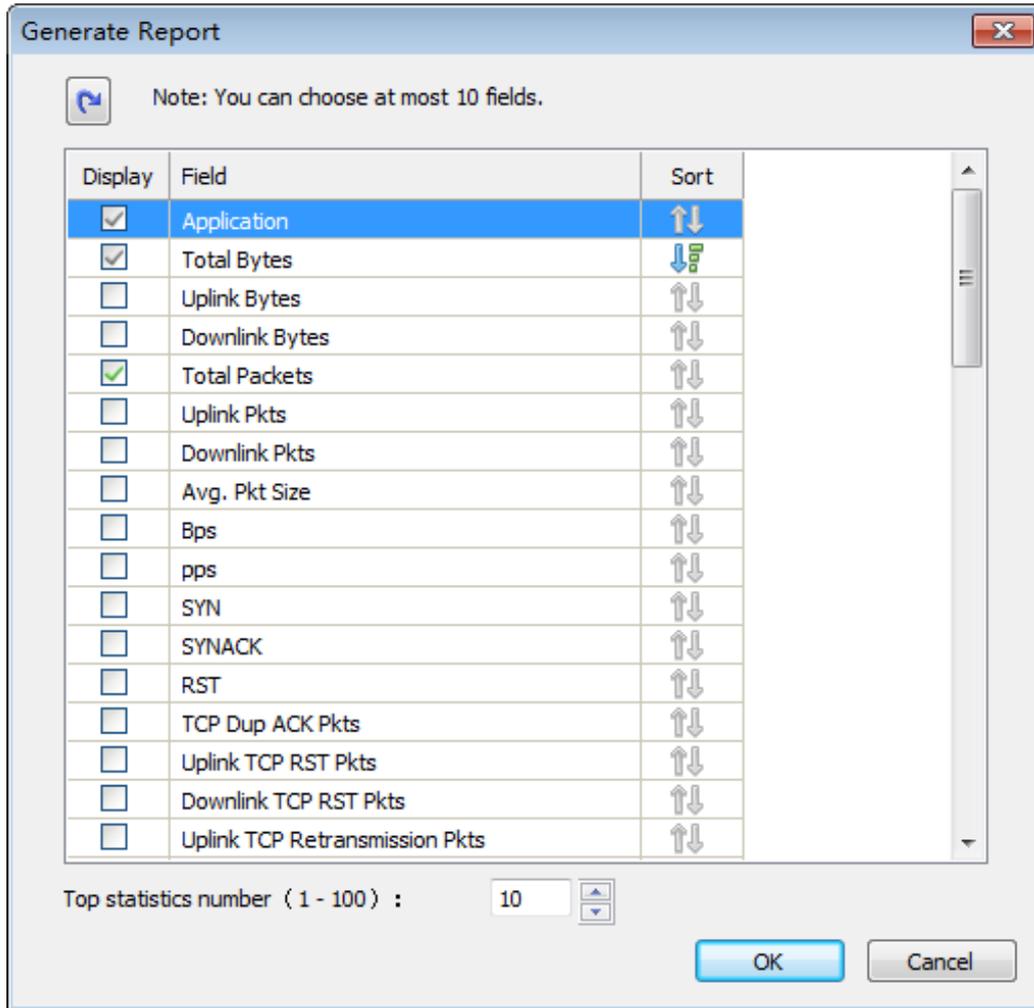
1. レポートウィンドウで「ユーザー定義のレポート」を見つけ出し、をクリックすることで、「新規レポート」ダイアログボックスを開きます。



2. レポート名と説明を入力します。レポート名は存在しているレポートと同じにすることはできません。ユニークなものである必要があります。
3. レポートスコープを選択します。
 - すべてのネットワークオブジェクトのためにレポートを作成したい場合、「グローバル」をクリックします。そうすると、レポート統計情報は、全てのネットワークオブジェクトに基づくものとなります。
 - 指定されるネットワークオブジェクトのためにレポートを作成したい場合、「オブジェクトを指定する」をクリックすることで、レポートスコープダイアログボックスを開きます。

オブジェクトを IP アドレス、MAC アドレス、ネットワークセグメント、ユーザー定義のアプリケーションにすることができます。オブジェクトを指定すると、レポート統計情報が指定されたオブジェクトに基づいたことを表します。

4. 関心のあるレポートモジュールをクリックし、「追加」をクリックすることで、関心のあるレポートモジュールを新しいレポートに追加することができます。レポートスコープによって、提供されるレポートモジュールも異なります。グローバルスコープは、全てのレポートモジュールと一緒に提供されています。レポートモジュールの詳細については、「レポートモジュール」をご参照ください。
5. 追加されたモジュールを選択し、「編集」ボタンをクリックすることで、モジュールを編集するダイアログボックスが表示されます。モジュールを編集するダイアログボックスでモジュールに含まれるフィールドを設定することができます。



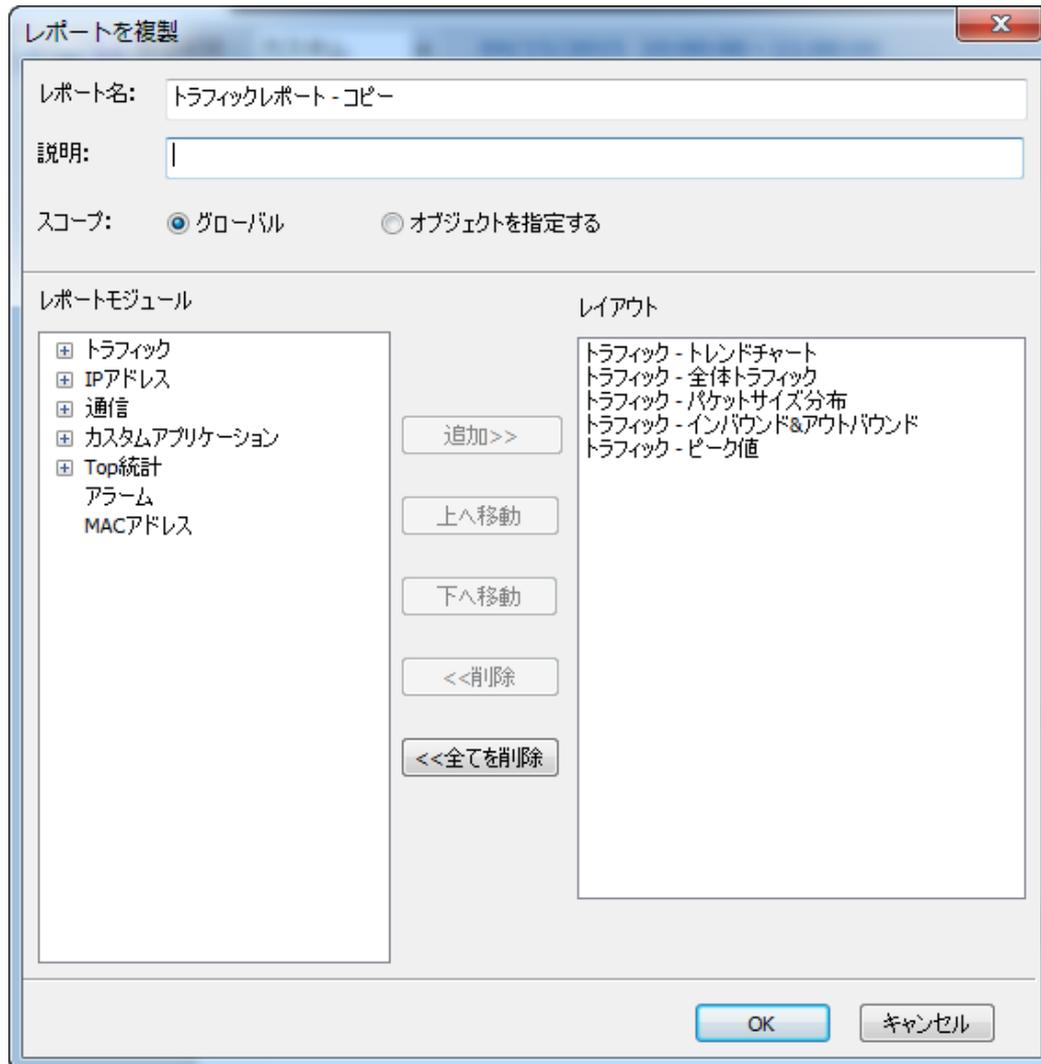
6. 「OK」をクリックして、レポートの作成を完了します。作成されたレポートは、ユーザー定義のレポートノードに表示されます。

レポートの複製

ユーザーは、既存のシステムレポート、またはユーザー定義のレポートを複製することで、迅速に新しいレポートを作成することができます。

レポートを複製するには、

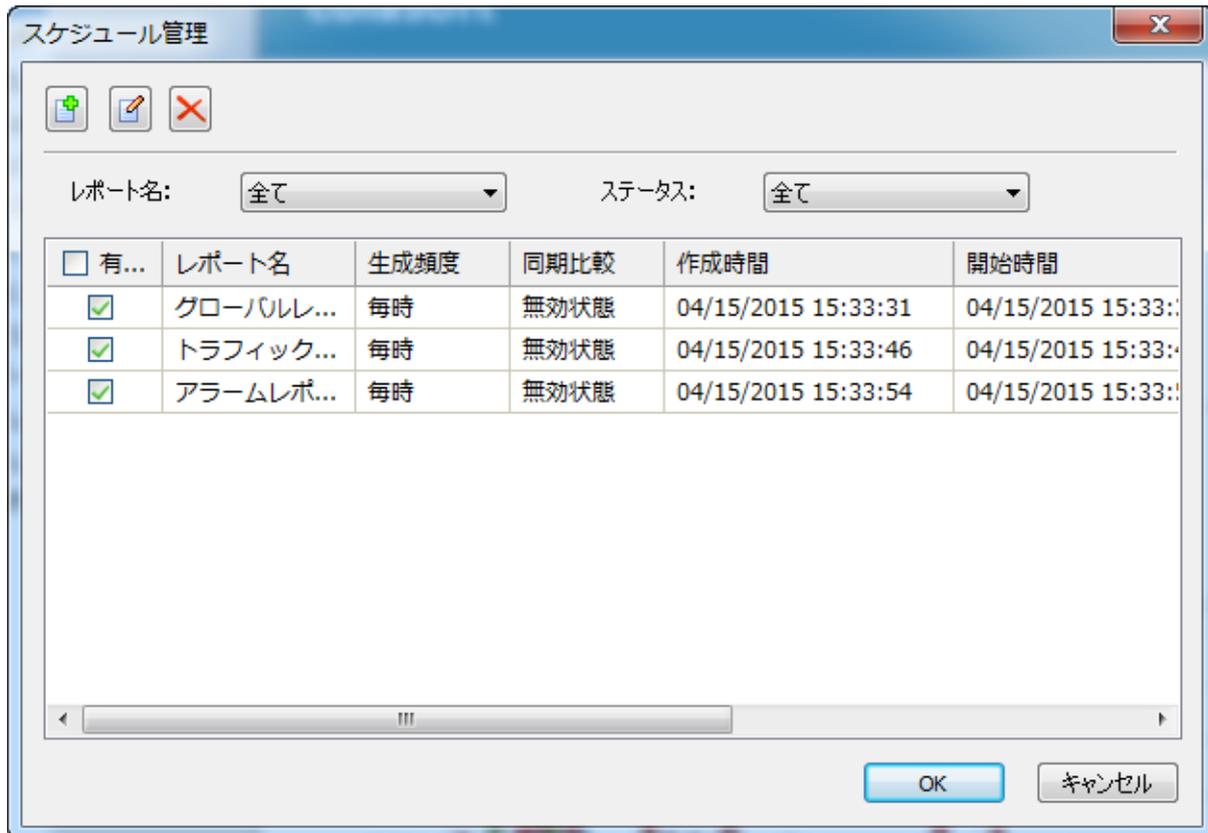
1. レポートウィンドウで、複製したいレポートを見つけ出し、をクリックすることで、レポートを複製するダイアログボックスを開きます。



2. レポート名と説明を入力します。レポート名はもとのレポートと同じにすることはできません。
3. 必要に応じて、レポートスコープを変更します。
4. 必要に応じて、レポートモジュールを変更します。
レポートスコープによって、提供されるレポートモジュールも違います。グローバルスコープは、全てのレポートモジュールと一緒に提供されています。レポートモジュールの詳細については、「レポートモジュール」をご参照ください。
5. 「OK」をクリックして、レポートの複製を完了します。複製された新しいレポートは、ユーザー定義のレポートノードに表示されます。

スケジュールの管理

レポートを作成するほかに、ユーザーはレポートをスケジュールし、自動的に生成されたレポートを指定されたEメールアドレスに送信することができます。これらのスケジュールを管理するには、レポートウィンドウで、 をクリックすることで、「スケジュール管理」ダイアログボックスを開きます。



- **レポート名:** スケジュールが基づいているレポートの名前を表示します。
- **生成頻度:** レポートが自動的に生成される頻度を表示します。
- **同期比較:** スケジュールされたレポートが履歴の統計情報と比較する機能を有効にするかどうかを表示します。
- **作成時間:** スケジュールの作成時間を表示します。
- **開始時間:** スケジュールを開始する時間を表示します。
- **終了時間:** スケジュールを終了する時間を表示します。終了時間が指定されていない場合、「永久有効」と表示されます。つまり、このスケジュールはネットワークリンクが削除されるまで、ずっと有効であることを意味しています。
- **生成されたレポート数:** これまで生成されたレポートの数を表示します。
- **ステータス:** スケジュールのステータスを表示します。
 - **準備:** 準備ができていますが、スケジュールはまだ実行されていません。
 - **実行中:** スケジュールは実行されているところです。
 - **終了:** スケジュールは終了しました。このスケジュールのために、レポートは生成されません。

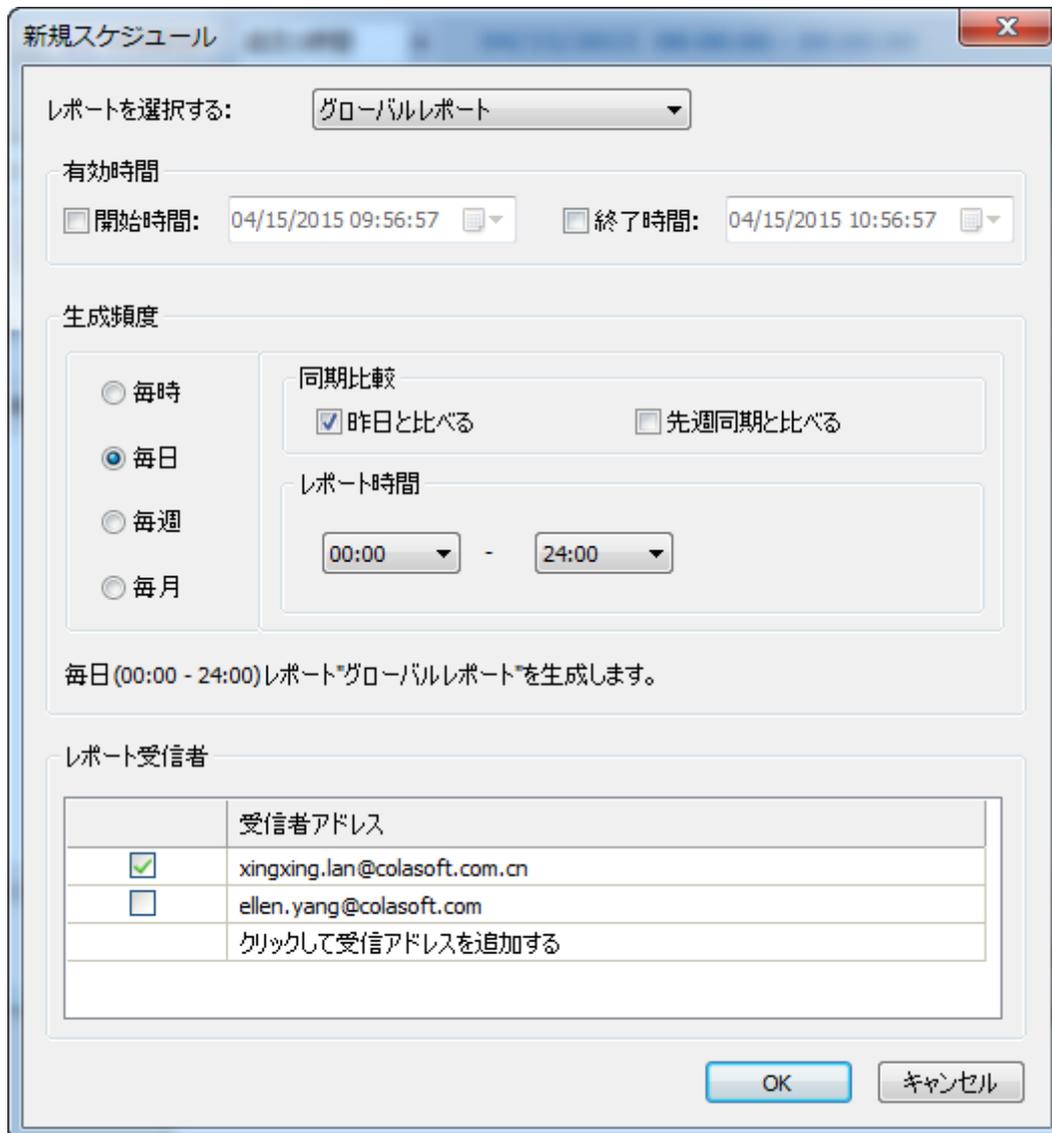
レポート名とスケジュールのステータスによって、「スケジュール管理」ダイアログボックスで、関心のあるレポートスケジュールを検索することができます。

レポートをスケジュール

ユーザーは既存のレポートに基づいて、レポートをスケジュールすることができます。

レポートをスケジュールするには、

1. レポートウィンドウで、 をクリックすることで、「スケジュール管理」ダイアログボックスを開きます。
2. 「スケジュール管理」ダイアログボックスで、 をクリックすることで、「新規スケジュール」ダイアログボックスを開きます。



新規スケジュール

レポートを選択する:

有効時間

開始時間: 終了時間:

生成頻度

毎時
 毎日
 毎週
 毎月

同期比較

昨日と比べる
 先週同期と比べる

レポート時間

-

毎日(00:00 - 24:00)レポート"グローバルレポート"を生成します。

レポート受信者

	受信者アドレス
<input checked="" type="checkbox"/>	xingxing.lan@colasoft.com.cn
<input type="checkbox"/>	ellen.yang@colasoft.com
	クリックして受信アドレスを追加する

OK キャンセル

3. スケジュールが基づいているレポート名を選択します。
4. 必要に応じて、スケジュールの有効時間を指定します。
 - 開始時間も終了時間も現在時刻より前にすることはできません。
 - 開始時間が指定されていない場合、開始時間はスケジュールの作成時間となります。
 - 終了時間が指定されていない場合、終了時間は、リンクが削除される時の時間と同じです。
5. レポートの生成頻度を指定し、履歴の統計情報と比較するかどうかを選択します。
6. スケジュールされたレポートを受信する受信アドレスを指定します。リストにおける受信者アドレスを有効にするか、または受信する E メールアドレスを入力することができます。

ヒント 既存レポートを右クリックし、「新規スケジュール」をクリックすることで、効率的にレポートをスケジュールすることもできます。

レポートモジュール

レポートは、一つまたは複数のレポートモジュールから構成されています。以下は各レポートモジュールについて説明しています。

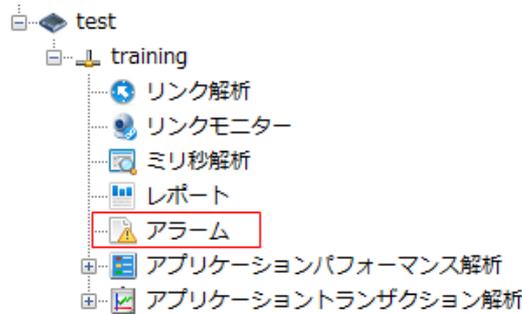
カテゴリ	モジュール
リンク解析	概要統計(トレンドチャート、概要、パケット、パケットサイズ分布、TCP パケット、IP トラフィック、非 IP トラフィック、ピーク値)、物理アドレス、内部アドレス、外部アドレス、アプリケーション、IP アドレネットワークスアプリケーション分布、ネットワークセグメント、物理セッション、IP セッション、TCP セッション、UDP セッション、TCP サービスポート、UDP サービスポート、サービスアクセス、セグメント間統計、VLAN 統計、MPLS VPN 統計、及びアラーム統計
アプリケーションパフォーマンス解析	クライアント、サーバー、ネットワークセグメント、IP セッション、TCP セッション、及びアラーム統計
アプリケーショントランザクション解析	クライアント、サーバー、ネットワークセグメント、トランザクション統計、及びアラーム統計

アラーム

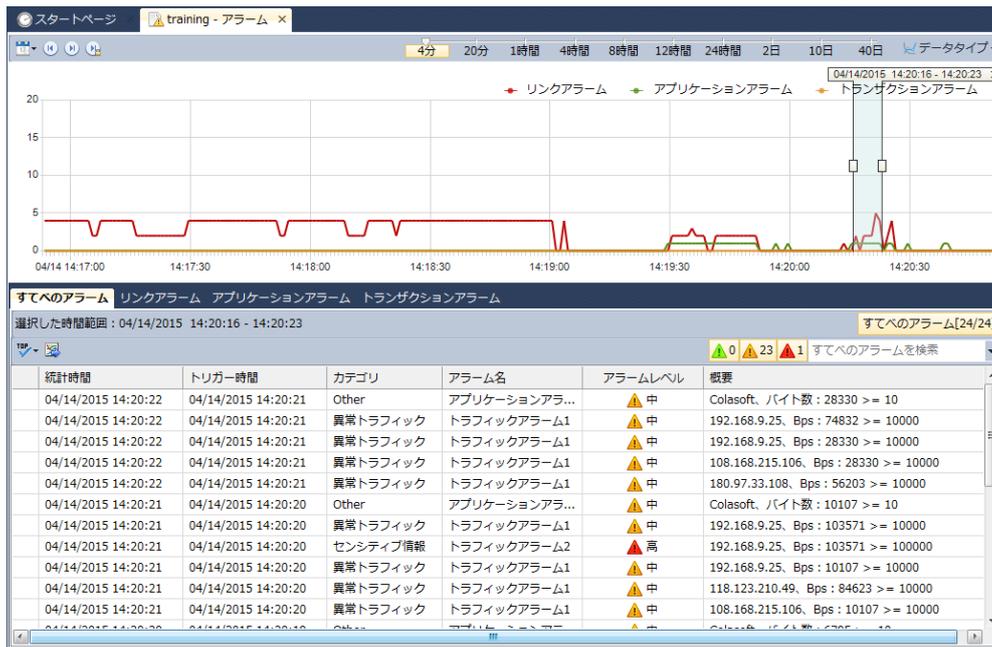
ネットワークリンクを設定する際に、必要に応じて、アラームを定義することができます。アラームがトリガーされると、定義されたアラームのためにアラームログが生成されます。

アラームログを表示するには、

1. ネットワークリンクの下にあるアラームノードをダブルクリックします。



2. そして、アラームウィンドウが開かれます。開かれたアラームウィンドウには、リンクアラームログとアプリケーションアラームログを含め、全てのアラームログが表示されます。



アラームウィンドウは、上のアラームトレンドチャートと下のいくつかのアラームビューから構成されています。アラームトレンドチャートには、トリガーされた全てのアラームが表示されます。アラームビューは、アラームタイプによって並べ替えます。

全てのアラームビュー、トラフィックアラームビュー、Eメールアラームビュー、ドメインアラームビュー、および特徴アラームビューは、リンク解析ウィンドウにおけるアラームビューと同じです。そして、アプリケーションアラームビュー、クライアントアラームビュー、サーバーアラームビュー、セグメントアラームビュー、およびTCPセッションアラームビューは、アプリケーションパフォーマンス解析ウィンドウにおけるアラームビューと同じです。

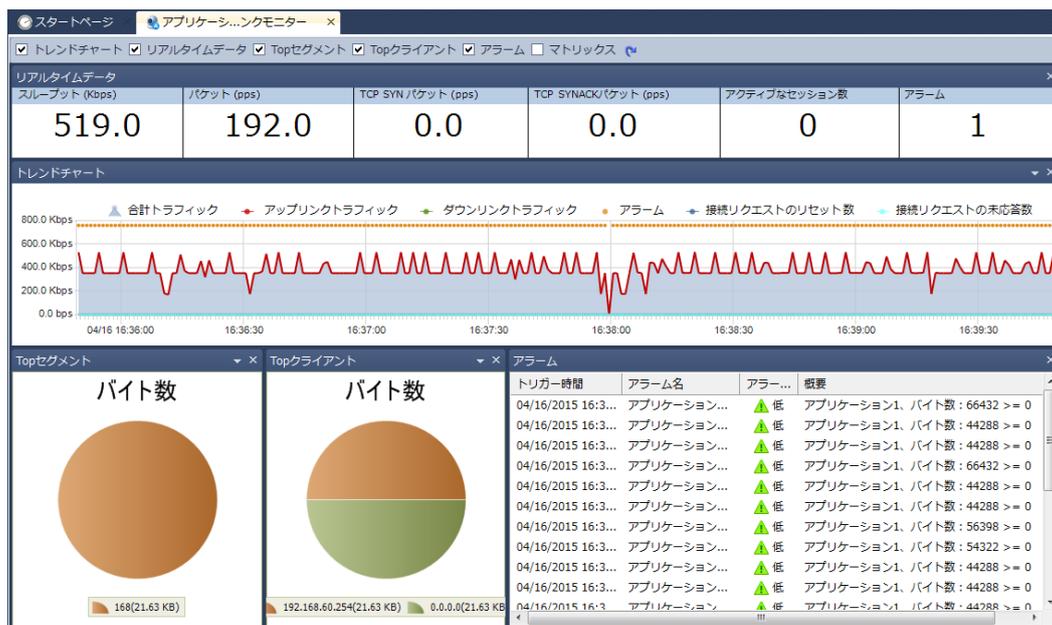
アプリケーションモニター

ネットワークリンクを監視するほか、nChronosは、独立で単一アプリケーションを監視することもできます。このアプリケーションは、任意カスタムアプリケーションであることができます。この章では、アプリケーションを監視する方法、およびアプリケーション監視ウィンドウにおける各要素について説明しています。

アプリケーションを監視

アプリケーションを監視するには、

1. リンクプロパティダイアログボックスにおける解析設定タブで、「有効にする」と「パフォーマンス解析」にチェックを入れます。
2. アプリケーションが監視されると、サーバーエクスプローラにおけるネットワークリンクの下に表示されます。
3. ネットワークリンクの下にあるアプリケーションを右クリックし、「モニター」をクリックすることで、アプリケーションのリアルタイムステータスを表示するアプリケーション監視ウィンドウが開かれます。



アプリケーション監視ウィンドウは、ネットワークリンクのリンク監視ウィンドウとは、非常に類似していて、六つのパネルからなっています。

- トrendチャート
- リアルタイムデータ
- トップセグメント
- トップクライアント
- アラーム
- マトリックス

アプリケーション監視のパネルは、リンク監視のパネルと、非常に類似していて、ただ前者はアプリケーション監視に、後者は全体ネットワークリンク監視に利用されています。

トレンドチャートパネル

トレンドチャートパネルにおいて、いくつかのトレンドチャートがあります。例えば、レスポンス時間、TCP 再送信、TCP セッション、トランザクション、トラフィック、およびパケットがあります。

トレンドチャートで右クリックすることで、表示したいチャートを選択したり、タイムウィンドウを設定したりすることができます。

リアルタイムデータパネル

リアルタイムデータパネルには、スループット、パケット、TCP SYN パケット、TCP SYNACK パケット、TCP RST パケット、作成したセッション数、アクティブなセッション数、閉じたセッション数、アラーム数を含め、アプリケーションリアルタイムデータが表示されます。

リアルタイムデータパネルで右クリックして、リフレッシュ間隔を設定することができます。

トップセグメントパネル

トップセグメントパネルは、円グラフでアプリケーションのトップネットワークセグメントを表示します。円グラフの下に、セグメントとリアルタイムデータが表示されます。セグメントは、ネットワークリンクを設定する際に、既に定義されています。

トップセグメントパネルで右クリックして、このパネルのリフレッシュ間隔を設定することができます。

さらに、トップセグメントパネルで右クリックして、「データタイプ」を選択することで、他のデータタイプによって、トップセグメントを表示することができます。

トップクライアントパネル

トップクライアントパネルは、円グラフでアプリケーションのトップクライアントを表示します。円グラフの下にクライアントとリアルタイムデータが表示されます。

トップクライアントパネルで右クリックして、このパネルのリフレッシュ間隔を設定することができます。

さらに、トップクライアントパネルで右クリックして、「データタイプ」を選択することで、他のデータタイプによって、トップクライアントを表示することができます。

アラームパネル

アラームパネルには、トリガー時間、アラームカテゴリ、アラームオブジェクト、アラーム名、アラームレベル、およびトリガー条件によって、1秒内でトリガーされた全てのアプリケーションアラームが表示されます。

マトリックスパネル

マトリックスパネルでは、マトリックスグラフでアプリケーション通信を表示します。

マウスをあるノードの上に移動すると、そのノードの送信パケットとバイト数、および受信パケットとバイト数が表示されます。ピアノード間の直線もハイライト表示されます。

さらにマトリックスパネルで右クリックし、適切なリフレッシュ間隔を選択することで、マトリックスパネルのリフレッシュ間隔を設定することができます。

そのほかに、マトリックスパネルで表示するトップ数を選択することもできます。

アプリケーション解析

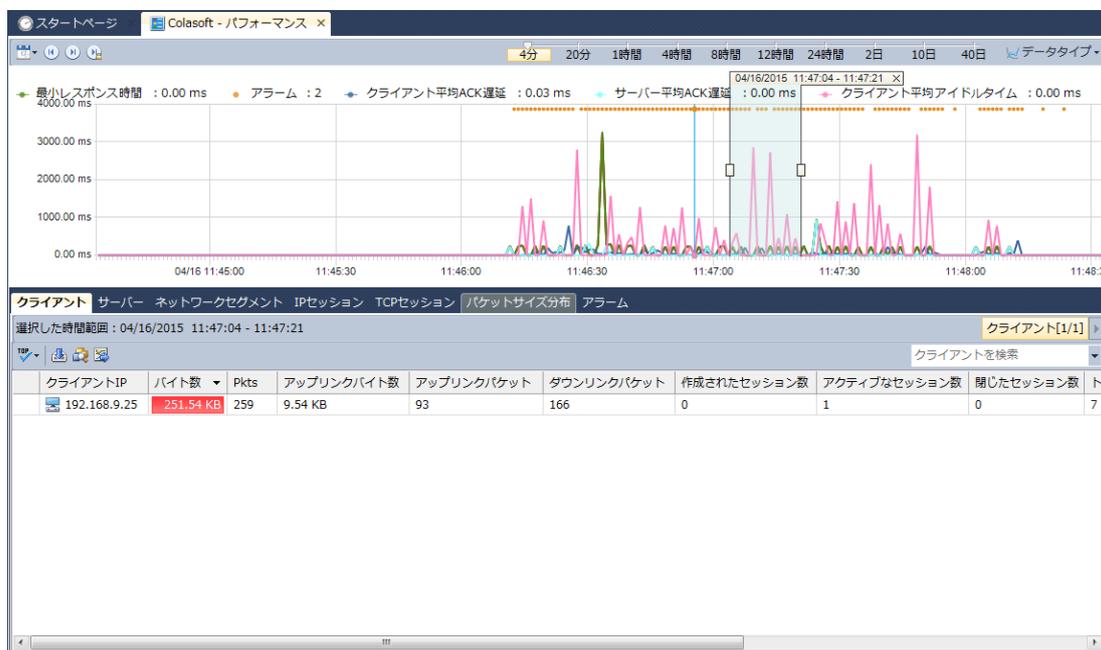
ネットワークリンクを監視するほか、nChronosは、独立で指定されたアプリケーションを解析することもできます。アプリケーション解析ウィンドウには、その指定されたアプリケーションのクライアント、サーバー、セグメント、セッション、およびアラームが表示されます。さらに、あるアプリケーションを適時的に解析し、そのアプリケーションの履歴データを表示することができます。

アプリケーションパフォーマンスを解析

独立でアプリケーションのパフォーマンスを解析するには、

1. リンクプロパティダイアログボックスにおける解析設定タブで、「有効にする」と「パフォーマンス解析」にチェックを入れます。
2. アプリケーションが監視されると、サーバーエクスプローラにおけるネットワークリンクの下に表示されます。
3. ネットワークリンクの下にあるアプリケーションをダブルクリックすることで、そのアプリケーションのトラフィックデータを表示するパフォーマンス解析ウィンドウが表示されます。

パフォーマンス解析ウィンドウは、リンク解析ウィンドウとは、非常に類似していて、タイムウィンドウと六つの解析ビューから構成されています。



アプリケーションパフォーマンス解析におけるトレンドチャート

タイムウィンドウにおけるトレンドチャートのデータには、以下のような12のタイプがあります。

- **レスポンス時間:** このタイプが選択されると、アプリケーションのレスポンス時間トレンドチャートが表示されます。「平均レスポンス時間」は、全体のTCPトランザ

クッション処理時間を TCP トランザクション数で割ったものです。「最大レスポンス時間」は、全ての TCP トランザクション処理時間の中で、最大な一つです。「最小レスポンス時間」は、全ての TCP トランザクション処理時間の中で、最小の一つです。

- **TCP セッション:**このタイプが選択されると、アプリケーションの TCP セッションのトレンドチャートが表示されます。「作成したセッション数」は、3 ウェイハンドシェイクを完了した TCP セッションを表します。「閉じたセッション数」は、接続をリリースした TCP セッションを表します。「アクティブなセッション」は、3 ウェイハンドシェイクを完了しましたが、接続をリリースしなかった TCP セッションを表します。
- **トランザクション:**このタイプが選択されると、アプリケーションの TCP トランザクショントレンドチャートが表示されます。「リクエスト数」はトランザクションのリクエスト数を表します。「レスポンス数」は、トランザクションのレスポンス数を表します。「リクエスト数」と「レスポンス数」は異なる色で表示されます。一つの TCP セッションには、複数の TCP トランザクションが含まれる可能性があります。
- **トラフィック:**このタイプが選択されると、アプリケーションのトラフィックトレンドチャートが表示されます。トラフィックトレンドチャートには、「合計トラフィック」、「アップリンクトラフィック」、および「ダウンリンクトラフィック」が表示されます。
- **パケット:**パケットトレンドチャートには、「合計パケット」、「アップリンクパケット」、および「ダウンパケット」が表示されます。
- **TCP パケット:** TCP パケットトレンドチャートには、「TCP SYN パケット」と「TCP SYNACK パケット」が表示されます。
- **TCP ロスセグメントパケット:** TCP ロスセグメントパケットは、失われた TCP セグメントパケットを表します。TCP ロスセグメントパケットトレンドチャートには、「TCP ロスセグメントパケット」、「アップリンク TCP ロスセグメントパケット」、および「ダウンリンク TCP ロスセグメントパケット」が表示されます。
- **セグメント損失率:**セグメント損失率トレンドチャートには、「セグメント損失率」、「アップリンクセグメント損失率」、および「ダウンリンクセグメント損失率」が表示されます。
- **再送信パケット:**再送信パケットトレンドチャートには、「再送信パケット」、「アップリンク TCP 再送信パケット」、「ダウンリンク TCP 再送信パケット」、「アップリンク TCP 重複 ACK パケット」、および「ダウンリンク TCP 重複 ACK パケット」が表示されます。
- **再送信率:**再送信率トレンドチャートには、「再送信率」、「アップリンク再送信率」、および「ダウンリンク再送信率」が表示されます。
- **TCP ゼロウィンドウ数:** TCP ゼロウィンドウ数トレンドチャートには、「サーバー TCP ゼロウィンドウ数」と「クライアント TCP ゼロウィンドウ数」が表示されます。
- **転送効率:**転送効率トレンドチャートには、「転送効率」、「アップリンク転送効率」、および「ダウンリンク転送効率」が表示されます。

パフォーマンス解析ビュー

指定されたアプリケーションのパフォーマンスを解析する際に、nChronos は、このアプリケーションの統計情報と解析データを表示する独立したウィンドウを提供します。この独立したウィンドウは、リンク解析ウィンドウとは、非常に類似していて、いくつかデータタイプのトレンドチャートが含まれているタイムウィンドウといくつかの解析ビューから構成されています。

アプリケーションパフォーマンス解析におけるパフォーマンス解析ウィンドウには、クライアントビュー、サーバービュー、ネットワークセグメントビュー、IP セッションビュー、TCP セッションビュー、パケットサイズ分布ビュー、およびアラームビューという 7 つのパフォーマンス解析ビューがあります。

クライアントビュー

アプリケーション解析におけるクライアントビューは、アプリケーションクライアントの IP アドレスに基づいて、トラフィックの統計情報と解析データを提供します。

クライアント統計情報を表示する

クライアントビューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

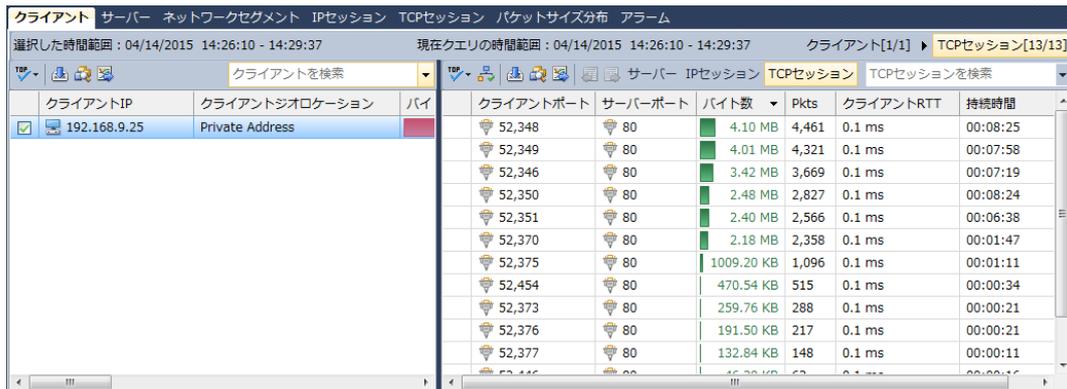
クライアントビューにおけるクライアントがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

その上、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックスに適切なキーワードを入力することで、キーワードが含まれている項目のみがクライアントビューに表示されます。

クライアントをドリルダウンする

クライアントビューにおける任意オブジェクトをドリルダウンして、より詳しい情報を取得することができます。あるオブジェクトをドリルダウンするには、このオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のようにクライアントビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。



クライアントIP	クライアントジオロケーション	バイ	クライアントポート	サーバーポート	バイト数	Pkts	クライアントRTT	持続時間
<input checked="" type="checkbox"/>	192.168.9.25	Private Address	52,348	80	4.10 MB	4,461	0.1 ms	00:08:25
			52,349	80	4.01 MB	4,321	0.1 ms	00:07:58
			52,346	80	3.42 MB	3,669	0.1 ms	00:07:19
			52,350	80	2.48 MB	2,827	0.1 ms	00:08:24
			52,351	80	2.40 MB	2,566	0.1 ms	00:06:38
			52,370	80	2.18 MB	2,358	0.1 ms	00:01:47
			52,375	80	1009.20 KB	1,096	0.1 ms	00:01:11
			52,454	80	470.54 KB	515	0.1 ms	00:00:34
			52,373	80	259.76 KB	288	0.1 ms	00:00:21
			52,376	80	191.50 KB	217	0.1 ms	00:00:21
			52,377	80	132.84 KB	148	0.1 ms	00:00:11

ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

サーバービュー

アプリケーション解析におけるサーバービューは、アプリケーションサーバーの IP アドレスに基づいて、トラフィックの統計情報と解析データを提供します。

サーバー統計情報を表示する

サーバービューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

サーバービューにおけるサーバー数がたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

その上、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックスに適切なキーワードを入力することで、キーワードが含まれている項目のみがサーバービューに表示されます。

サーバーをドリルダウンする

サーバービューにおける任意オブジェクトをドリルダウンして、より詳しい情報を取得することができます。あるオブジェクトをドリルダウンするには、このオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。また、続いて表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のようにサーバービューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。

クライアントポート	サーバーポート	バイト数	Pkts	クライアントRTT	持続時間
54,651	80	468.55 KB	518	0.1 ms	00:00:30
54,635	80	264.69 KB	295	0.1 ms	00:00:33
54,662	80	254.27 KB	271	0.1 ms	00:00:21
54,660	80	224.36 KB	245	0.1 ms	00:00:21
54,634	80	188.05 KB	224	0.1 ms	00:00:19
54,647	80	150.65 KB	173	0.1 ms	00:00:15
54,664	80	150.23 KB	171	0.1 ms	00:00:18
54,657	80	134.05 KB	160	0.1 ms	00:00:22
54,665	80	79.12 KB	99	0.1 ms	00:00:19
54,645	80	39.35 KB	55	0.1 ms	00:00:08
54,677	80	37.62 KB	50	0.1 ms	00:00:09

ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

ネットワークセグメントビュー

アプリケーション解析におけるネットワークセグメントビューは、アプリケーションのネットワークセグメントに基づいて、トラフィックの統計情報と解析データを提供します。ネットワークセグメントは、ネットワークリンクを設定する際に、既に定義されています。

セグメント統計情報を表示する

ネットワークセグメントビューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

ネットワークセグメントビューにおけるセグメントがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

その上、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックスに適切なキーワードを入力することで、キーワードが含まれている項目のみがネットワークセグメントビューに表示されます。

セグメントをドリルダウンする

ネットワークセグメントビューにおける任意オブジェクトをドリルダウンして、より詳しい情報を取得することができます。あるオブジェクトをドリルダウンするには、このオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。また、続いて表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ドリルダウンウィンドウはいつも右から出てきます。元のビューや他のドリルダウンウィンドウに戻りたい場合、下図のようにネットワークセグメントビューの右上にあるウィンドウの名前をクリックすることで、戻ることができます。

クライアント		サーバー		ネットワークセグメント		IPセッション		TCPセッション		パケットサイズ分布		アラーム	
名前		バイト数	Pkts	トランザクション数	アップリンクバイ...	ダウンリンクバ	クライアントポート	サーバーポート	バイト数	Pkts	クライアントRTT	持続時間	
<input checked="" type="checkbox"/>	Dev.1	1.94 MB	2,259	30	74.44 KB	1.87 MB	54,651	80	468.55 KB	518	0.1 ms	00:00:30	
							54,635	80	264.69 KB	295	0.1 ms	00:00:33	
							54,662	80	254.27 KB	271	0.1 ms	00:00:21	
							54,660	80	224.36 KB	245	0.1 ms	00:00:21	
							54,634	80	188.05 KB	224	0.1 ms	00:00:19	
							54,647	80	150.65 KB	173	0.1 ms	00:00:15	
							54,664	80	150.23 KB	171	0.1 ms	00:00:18	
							54,657	80	134.05 KB	160	0.1 ms	00:00:22	
							54,665	80	79.12 KB	99	0.1 ms	00:00:19	
							54,645	80	39.35 KB	55	0.1 ms	00:00:08	
							54,677	80	37.62 KB	50	0.1 ms	00:00:09	

ドリルダウンウィンドウを閉じるには、ドリルダウンオブジェクトの前にあるチェックを外せばよいのです。

IP セッションビュー

アプリケーション解析における IP セッションビューは、アプリケーションの IP セッションに基づいて、トラフィックの統計情報と解析データを提供します。

IP セッションビューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

IP セッションビューにおけるセッションがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

その上、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックスに適切なキーワードを入力することで、キーワードが含まれている項目のみが IP セッションビューに表示されます。

TCP セッションビュー

アプリケーション解析における TCP セッションビューは、アプリケーションの TCP セッションに基づいて、トラフィックの統計情報と解析データを提供します。

TCP セッションビューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

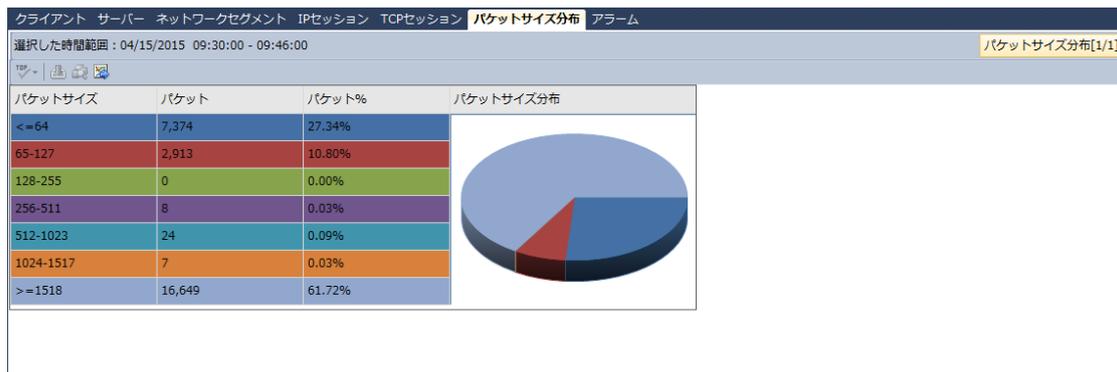
さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

TCP セッションビューにおける TCP セッションがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。このトップ数はバイト数カラムの値によって、並べ替える項目数であることに注意してください。

その上、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックスに適切なキーワードを入力することで、キーワードが含まれている項目のみが TCP セッションビューに表示されます。

パケットサイズ分布ビュー

パケットサイズ分布ビューは、パケットサイズの分布を統計していて、下図のように表示されます。



アラームビュー

アプリケーション解析におけるアラームビューは、全てのアプリケーションアラームログを提供します。これら全てのアプリケーションアラームは、リンクプロパティを設定する際に、定義されています。

アラームビューは、アラームタイプによって、アラームログを表示します。

- 「アプリケーションアラーム」タブには、トリガーされた全てのアプリケーションアラームログが表示されます。それらのアプリケーションアラームは、監視されたアプリケーションをアラームオブジェクトとして、定義されています。
- 「クライアントアラーム」タブには、トリガーされた全てのクライアントアラームログが表示されます。それらのクライアントアラームは、クライアントをアラームオブジェクトとして、定義されています。
- 「サーバーアラーム」タブには、トリガーされた全てのサーバーアラームログが表示されます。それらのサーバーアラームは、単一サーバー、または複数サーバーをアラームオブジェクトとして、定義されています。
- 「セグメントアラーム」タブには、トリガーされた全てのセグメントアラームログが表示されます。それらのセグメントアラームは、ネットワークセグメントをアラームオブジェクトとして、定義されています。
- 「TCPセッションアラーム」タブには、トリガーされた全てのTCPセッションアラームログが表示されます。それらのTCPセッションアラームは、TCPセッションをアラームオブジェクトとして、定義されています。

全てのアラームログは、トリガー時間、カテゴリ、オブジェクト、アラーム名、アラームレベル、およびトリガー条件によって、表示されます。さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

アラームビューにおけるアラームログがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。ここのトップ数はトリガー時間カラムによって、並べ替える項目数であることに注意してください。

その上、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックスに適切なキーワードを入力することで、キーワードが含まれている項目のみがアラームビューに表示されます。

トランザクション解析

アプリケーションのトランザクションを解析するには、

1. リンクプロパティダイアログボックスにおける解析設定タブで、「有効にする」と「トランザクション解析」にチェックを入れます。
2. そうすると、アプリケーションがサーバーエクスプローラにおけるネットワークリンクの下に表示されます。
3. ネットワークリンクの下にあるアプリケーションをダブルクリックすることで、アプリケーションのトランザクションデータを表示するトランザクション解析ウィンドウが表示されます。

トランザクション解析ウィンドウは、リンク解析ウィンドウとは非常に類似していて、下図のように、タイムウィンドウと六つの解析ビューから構成されています。



トランザクション解析ウィンドウには、クライアントビュー、サーバービュー、ネットワークセグメントビュー、トランザクションビュー、トランザクションログビュー、およびアラームビューという六つの解析ビューがあります。

クライアントビュー

トランザクション解析におけるクライアントビューは、アプリケーションクライアントのIPアドレスに基づいて、解析されたアプリケーションのトランザクションのために、トラフィックの統計情報と解析データを提供します。

クライアントビューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

クライアントビューにおける任意オブジェクトをドリルダウンして、より詳しい情報を取得することができます。あるオブジェクトをドリルダウンするには、このオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。

サーバービュー

トランザクション解析におけるサーバービューは、アプリケーションサーバーの IP アドレスに基づいて、解析されたアプリケーションのトランザクションのために、トラフィックの統計情報と解析データを提供します。

サーバービューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

サーバービューにおける任意オブジェクトをドリルダウンして、より詳しい情報を取得することができます。あるオブジェクトをドリルダウンするには、このオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。また、続いて表示されたドリルダウンウィンドウにおいて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

ネットワークセグメントビュー

トランザクション解析におけるネットワークセグメントビューは、アプリケーションのネットワークセグメントに基づいて、解析されたアプリケーションのトランザクションのために、トラフィックの統計情報と解析データを提供します。ネットワークセグメントは、ネットワークリンクを設定する際に、既に定義されています。

ネットワークセグメントビューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

ネットワークセグメントビューにおける任意オブジェクトをドリルダウンして、より詳しい情報を取得することができます。あるオブジェクトをドリルダウンするには、このオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、適切なドリルダウンオブジェクトを選択します。そして、ドリルダウンウィンドウがこのビューの右の部分に表示されます。また、続いて表示されたドリルダウンウィンドウにお

いて、あるオブジェクトを右クリックし、ポップアップされたメニューにおける「ドリルダウン」をクリックして、もっと詳しい情報を取得することができます。

トランザクションビュー

トランザクションビューは、下図のようにアプリケーションのトランザクション統計情報を提供します。



トランザクション	成功回数	失敗回数	成功率	トランザクション数	リクエスト数	レスポンス数	バイト数	リクエストバイト数	レスポンスバイト数	Pkts	リクエストパケット数
purchase	11	0	100.00%	11	11	11	344.78 KB	6.80 KB	337.98 KB	253	11
Support	9	1	90.00%	10	10	9	317.13 KB	5.93 KB	311.21 KB	235	10
Products	9	0	100.00%	9	9	9	292.41 KB	5.35 KB	287.06 KB	211	9

注意 全てのトランザクションは、ネットワークリンクプロパティにおける「解析設定」で設定する必要があります。そうしないと、このビューには統計情報が、何も表示しません。

トランザクションビューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

トランザクションビューにおける任意オブジェクトをドリルダウンして、より詳しい情報を取得することができます。あるオブジェクトをドリルダウンするには、このオブジェクトをダブルクリックすることで、ドリルダウンウィンドウがこのビューの右の部分に表示されます。

トランザクションログビュー

トランザクションログビューは、下図のように全てのトランザクションログを提供します。一つのトランザクションは、ログを一つ持っています。

トランザクション	サーバーポート	サーバージオロケーション	クライアントポート	クライアントジオロケーション	リクエスト時刻	リクエストバイト数	レスポンスバイト
Products	80	Texas, United States	49,610	Private Address	04/16/2015 09:35:18.534177	606.00 B	34.10 KB
Support	80	Texas, United States	49,610	Private Address	04/16/2015 09:35:16.864697	606.00 B	34.58 KB
Support	80	Texas, United States	49,609	Private Address	04/16/2015 09:35:10.670272	606.00 B	34.58 KB
purchase	80	Texas, United States	49,610	Private Address	04/16/2015 09:35:14.731157	638.00 B	30.73 KB
Products	80	Texas, United States	49,610	Private Address	04/16/2015 09:35:12.361082	639.00 B	34.10 KB
Products	80	Texas, United States	49,608	Private Address	04/16/2015 09:35:08.745854	607.00 B	14.26 KB
purchase	80	Texas, United States	49,607	Private Address	04/16/2015 09:35:04.660791	638.00 B	30.73 KB
Support	80	Texas, United States	49,608	Private Address	04/16/2015 09:35:06.506383	638.00 B	34.58 KB
Support	80	Texas, United States	49,606	Private Address	04/16/2015 09:34:59.000160	597.00 B	34.58 KB
purchase	80	Texas, United States	49,606	Private Address	04/16/2015 09:34:57.000000	638.00 B	30.73 KB
purchase	80	Texas, United States	49,605	Private Address	04/16/2015 09:34:52.270859	639.00 B	30.73 KB

トランザクションログビューで統計情報を表示している時、いくつかのデフォルトカラムがあります。カラムヘッダーを右クリックし、適切なカラムをクリックすることで、このビューで表示したい他のカラムを選択することもできます。

さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによって統計情報を並べ替えることができます。

トランザクションログビューにおいて、一つまたは複数トランザクションログを選択、右クリックし、ポップアップされたメニューにおける「トランザクションを解析する」をクリックすることで、トランザクションの詳細情報を表示するトランザクションコンテンツ解析ウィンドウが開かれます。

クライアント		サーバー	
IPアドレス	192.168.9.25	IPアドレス	108.168.215.106
ポート	49610	ポート	80
リクエスト時刻	04/16/2015 09:35:14.731157	レスポンス時刻	04/16/2015 09:35:15.000000
リクエストコンテンツ長さ	638.00 B	レスポンスコンテンツ長さ	30.73 KB
リクエストコンテンツ	GET /purchase/purchase_and_payment_options.php HTTP/1.1..Host: www.colasoft.com..Connection: keep-alive..Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8..User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36 SE 2.X MetaSr 1.0..Referer: http://www.colasoft.com/support/..Accept-Encoding: gzip,deflate,sdch..Accept-Language: zh-CN,zh;q=0.8..Cookie: InternalAccess=capsa2007; __utma=253999386.64157362.1428633200.1429061131.142906480.5.10; __utmc=253999386; __utmz=253999386.1428633200.1.1.utmcsr=(direct) utmccn=(direct) utmcmd=(none)....	レスポンスコンテンツ	HTTP/1.1 200 OK..Date: Thu, 16 Apr 2015 01:35:13 GMT..Server: Apache/2.2.26 (Unix) mod_ssl/2.2.26 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.17..X-Powered-By: PHP/5.2.17..Keep-Alive: timeout=5, max=99..Connection: Keep-Alive..Transfer-Encoding: chunked..Content-Type: text/html...550f.<DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">.<html xmlns="http://www.w3.org/1999/xhtml">.<head>.<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />.<title>Colasoft Store</title>.<meta name="keywords" content="Purchase Colasoft Capsa, Purchase Colasoft EtherLook, Purchase Colasoft MAC Scanner Pro" />.<meta

トランザクションコンテンツ解析ウィンドウには、クライアントとサーバーの IP アドレスとポート番号、リクエストとレスポンス時刻、リクエストコンテンツとレスポンスコンテンツの長さ、リクエストコンテンツとレスポンスコンテンツの詳細情報が表示されます。

複数トランザクションログを解析する場合、 または  をクリックして、便利に関連するトランザクションコンテンツを表示することができます。

アラームビュー

トランザクション解析におけるアラームビューは、全てのトランザクションアラームログを提供します。これら全てのトランザクションアラームは、ネットワークリンクを設定する際に、定義されています。

アラームログを表示する

アラームビューは、アラームタイプによって、アラームログを表示します。

- 「全てのトランザクションアラーム」タブには、トリガーされた全てのトランザクションアラームログが表示されます。
- 「トランザクションログアラーム」タブには、トリガーされた全てのトランザクションログアラームのログが表示されます。これらのトランザクションログアラームは、トランザクションログをアラームオブジェクトとして、定義されています。
- 「トランザクション統計アラーム」タブには、トリガーされた全てのトランザクション統計アラームログが表示されます。これらのトランザクション統計アラームは、トランザクション統計をアラームオブジェクトとしています。

全てのアラームログは、統計時間、トリガー時間、カテゴリ、アラーム名、アラームレベル、トリガー条件などによって、表示されます。さらに、カラムヘッダーにおけるカラム名をクリックすることで、そのカラムによってアラームログを並べ替えることができます。

アラームビューにおけるアラームログがたくさんある場合、 をクリックすることで、このビューで表示するトップ数を選択することができます。ここのトップ数はトリガー時間カラムによって、並べ替える項目数であることに注意してください。このビューにおける全ての統計項目を表示したい場合、 をクリックし、「全てを表示」をクリックすればよいです。

アラームビューで検索する

アラームビューにアラームログがたくさんある場合、表示フィルターを利用して、関心のあるデータを表示することができます。右上にある検索ボックス

全てのトランザクションアラーム  に適切なキーワードを入力することで、キーワードが含まれている項目のみがアラームビューに表示されます。