Colasoft®
Maximize Network Value

nChronos

Network Forensic Analysis Application

スタートアップガイド

(nChronos 5.0)

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

要約

このスタートアップガイドは、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

このスタートアップガイドは、nChronos 初心者のために作成されています。

専門用語

このスタートアップ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

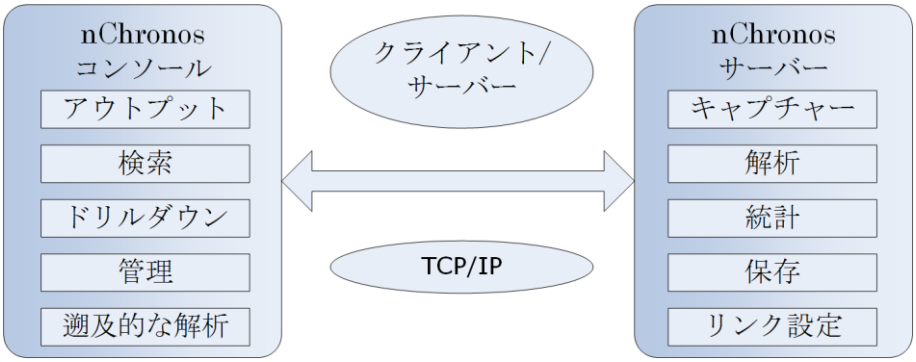
nChronos は nChronos サーバーと nChronos コンソールから構成されています。 nChronos サーバーは、nChronos の中核で、目標ネットワークパケットのキャプチャー、解析、および保存に役立ちます。 nChronos コンソールは、データのプレゼンテーションプラットフォームで、nChronos サーバーに接続して、プレゼンテーションのための統計情報やその他の解析データを取得することができます。データを表示するには、ユーザーはまず nChronos サーバーを設定して、nChronos サーバーをコンソールに接続する必要があります。

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。

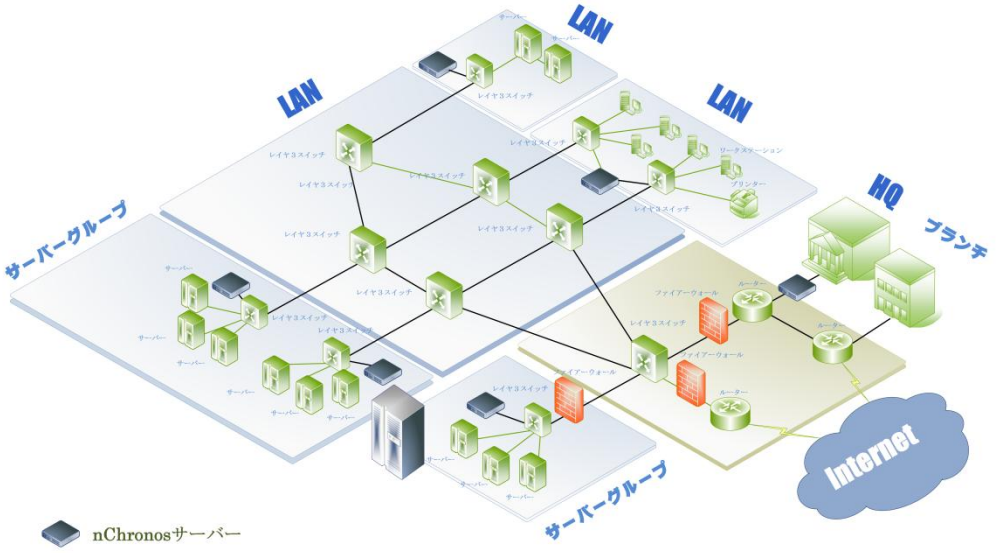
nChronos コンソールは C/S（クライアント/サーバー）技術を利用して、nChronos サーバーと通信します。 nChronos コンソールはリアルタイムにネットワークリンクを監視する、解析ビューに統計情報を表示する、統計情報をエクスポートする、パケットをダウンロードする、ネットワークオブジェクトをドリルダウンする、および他の通信操作を実行する場合、リクエストコマンドをサーバーに送信します。そしてサーバーは、そのコマンドにレスポンスして、対応のデータを返します。さらに、nChronos コンソールと nChronos サーバーは、指定されたポート番号を通じ、TCP/IP プロトコルを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

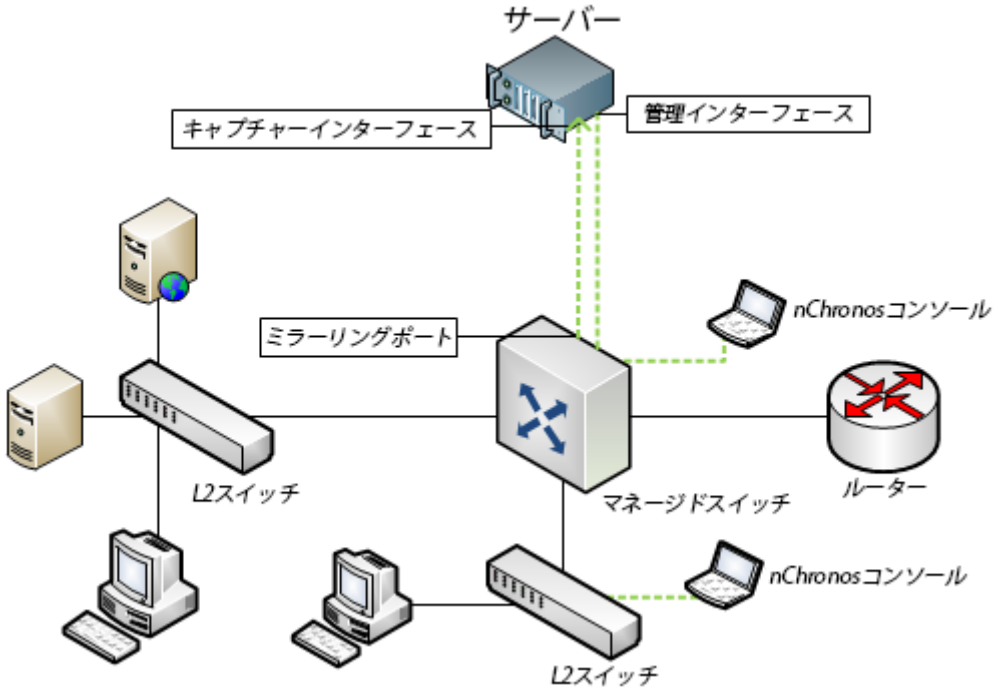
異なるネットワークと複数ネットワークリンクを持つネットワークでは、nChronos はローカルネットワークのネットワークデータをキャプチャーまたは保存するほかに、分散的デプロイメントとリモート監視をもサポートしています。重要なネットワークリンクの場合、複数の nChronos サーバーを配備することができ、ユーザーはデータ解析とネットワーク管理のため、いつでもどこでもリモート nChronos サーバーに接続することができます。さらに、nChronos コンソールを使用して、重要なネットワークリンクのトラフィックをリアルタイムに監視することができ、一旦異常が発生したら報告することもできます。nChronos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

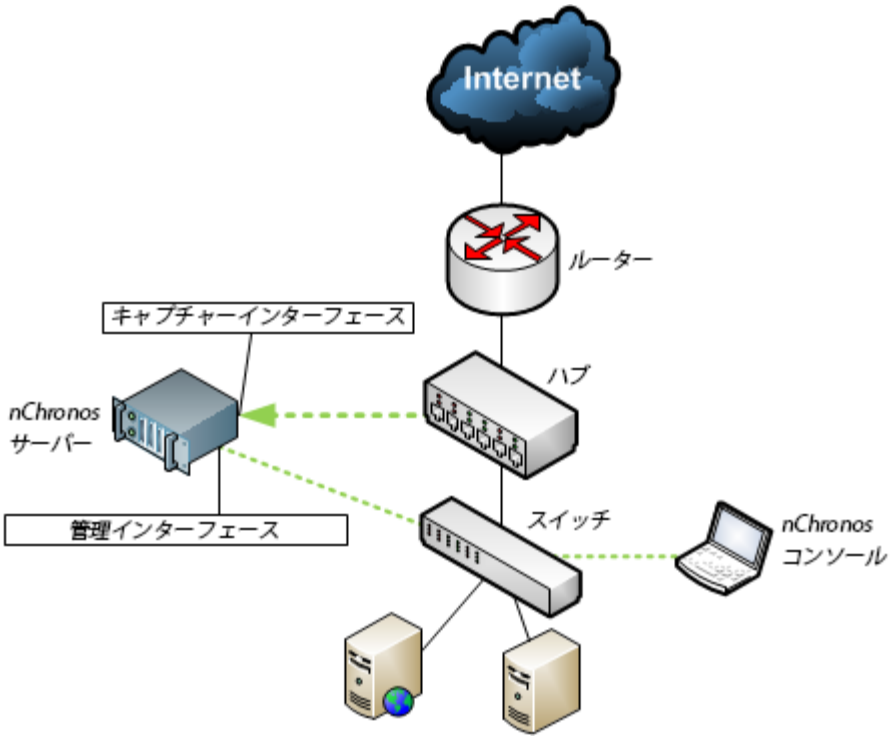
マネージドスイッチ

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。



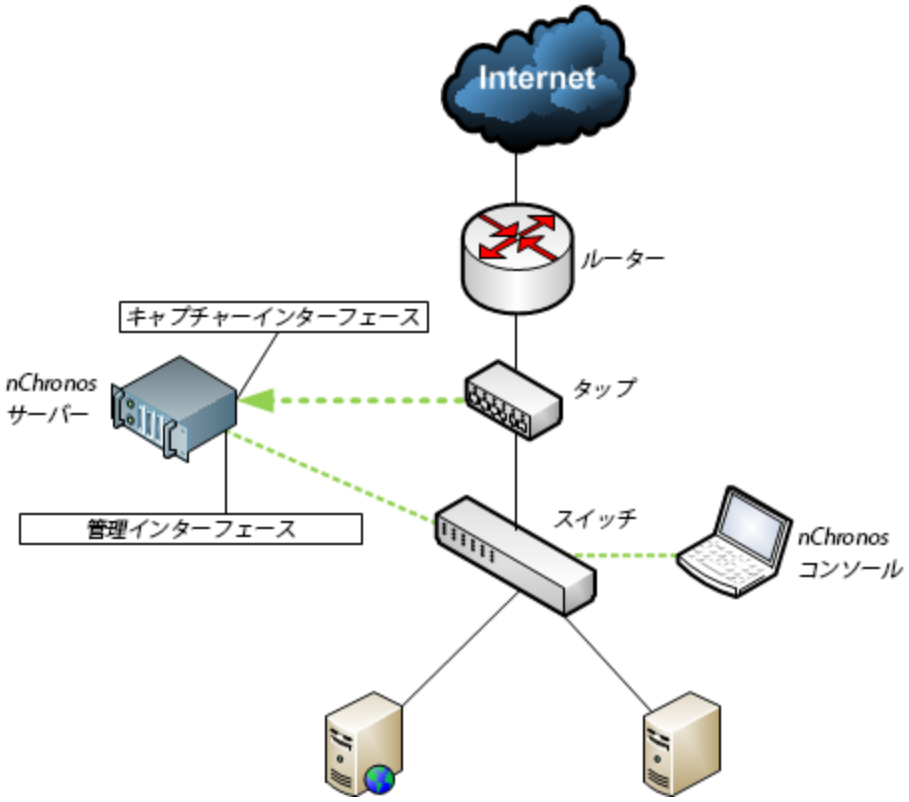
ハブ

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ーするほかに、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ーするために、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。



インストールとアクティベーション

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

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。

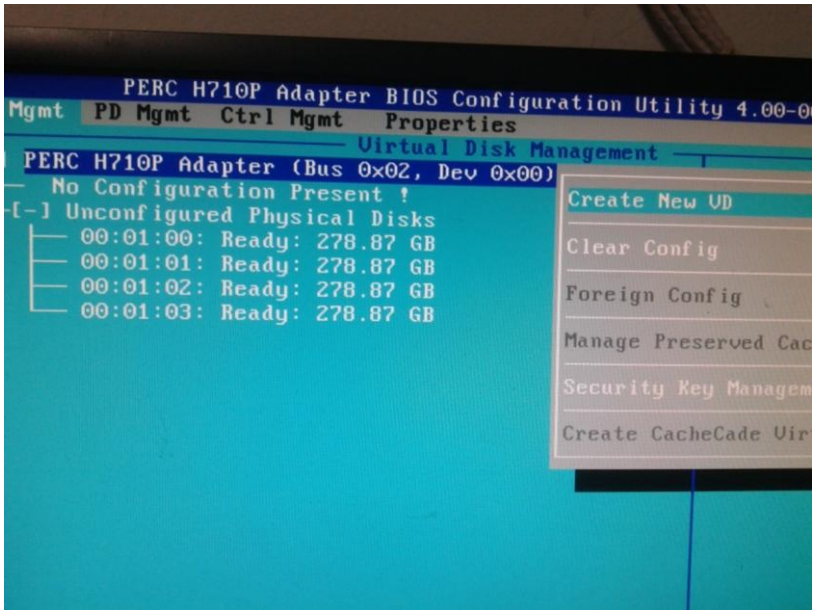
1. ColaOS 6.6 インストールディスク(CentOS 6.6)
2. nChronos サーバーインストールパッケージ: csras.xxxx.rpm、他の関連ソフトウェアインストールパッケージ: lrzrz.xxx.rpm、xfsprogos.xxxx.rpm、及び自動インストールスクリプト: csrass_install_1.2.sh
3. OS をインストールするには、二つの RAID パーティションが必要で、データパーション sdb を/data にアップロードする必要があります。

OS RAID パーティション

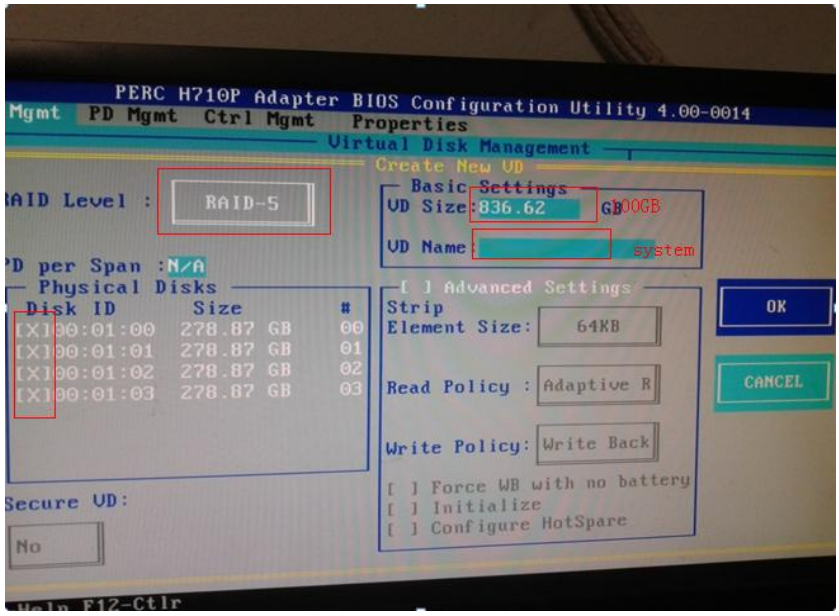
サーバーを起動する際、RAID カードのモデルにより、対応するショートカットキーをクリックすることで、RAID カード設定インターフェースに入ります。

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。

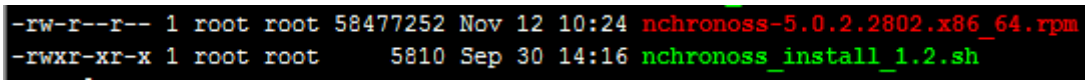
OS をインストール

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ます。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、旧いサーバーの場合、OS を再インストールする可能性があります。

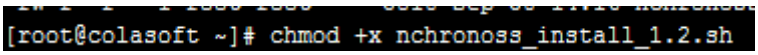
OS のインストールが完了した後、デフォルトで、ユーザー名は「root」で、パスワードは「!ColasoftL23」となります。デフォルトでイーサネットポートは eth0 で、IP アドレスは 192.168.5.160 となります。ユーザーはサーバーにログインし、「ethtool –p eth0 9」を入力することで、eth0 の位置を特定することができます。eth0 のランプは 9 秒点滅します。ランプの点滅する時間は必要に応じて設定できます。

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。



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。



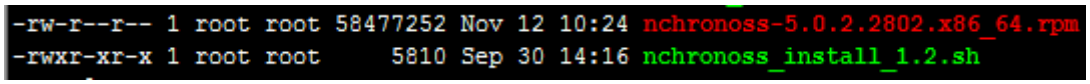
3. 「./nchronoss_install_1.2.sh」を入力して、スクリプトを実行しいます。

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。

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。



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。

「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

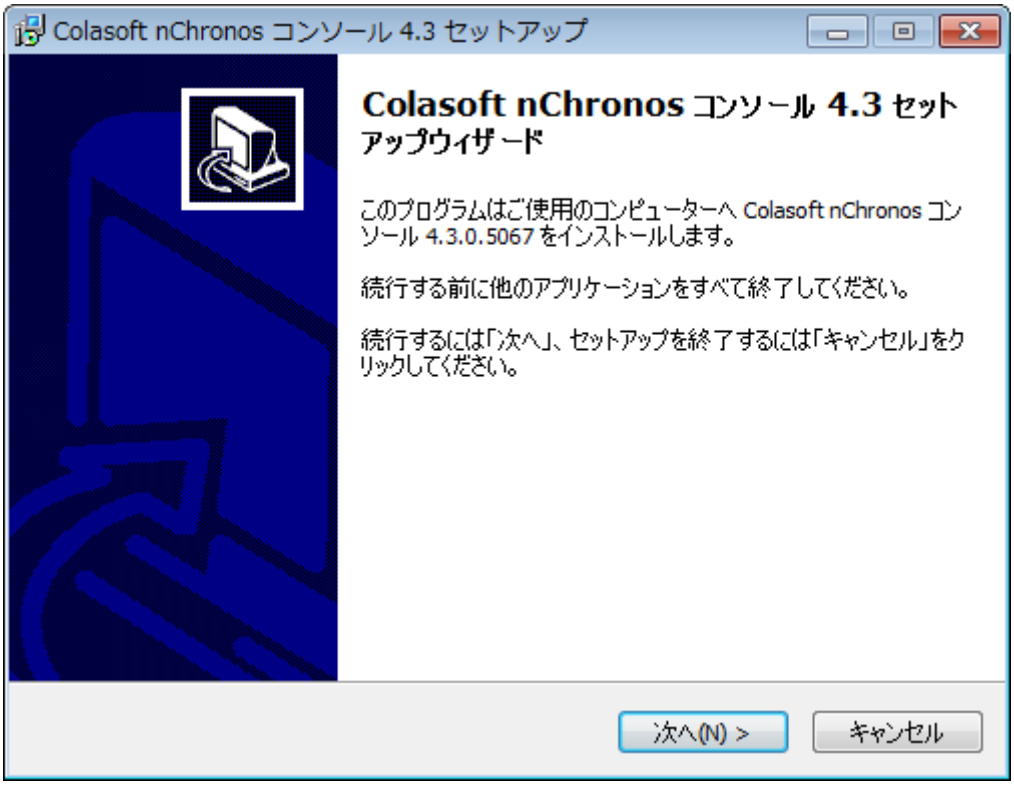
nChronos コンソールをインストール

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：

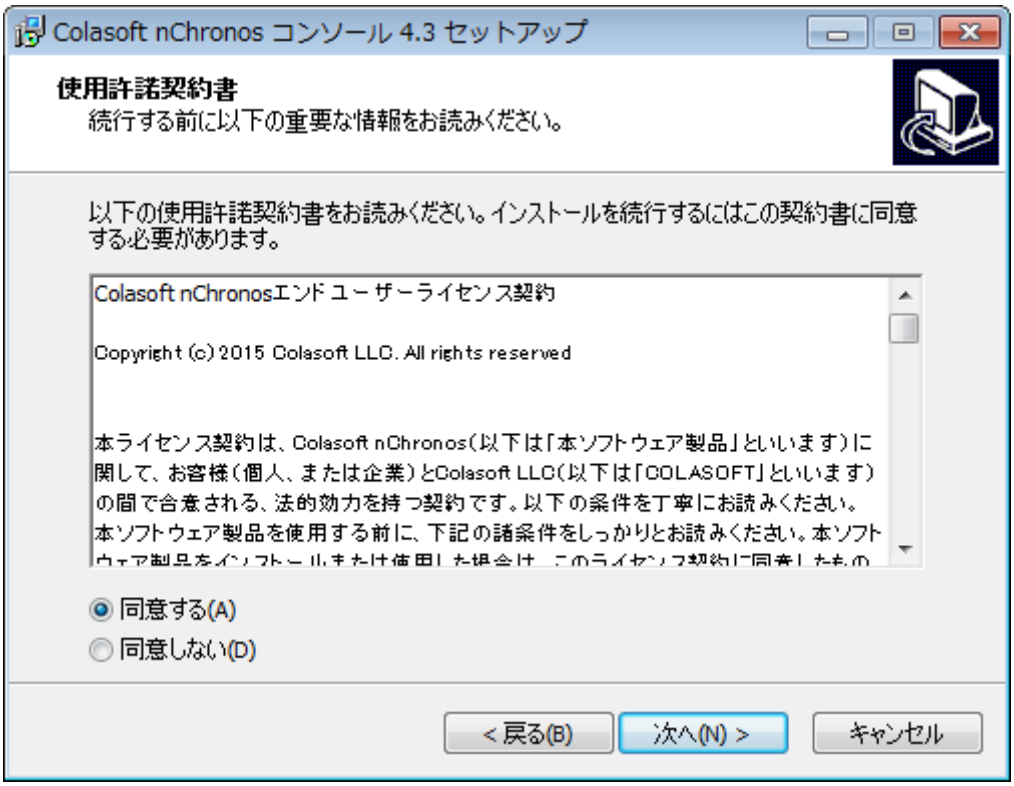
- お使いのマシンが最小システム要件を満たしていることを確認してください。
- お使いのマシンで実行中のすべてのアプリケーションを終了してください。
- 古いバージョン、または試用版の nChronos コンソールをアンインストールしてください。

コンソールをインストールするには、

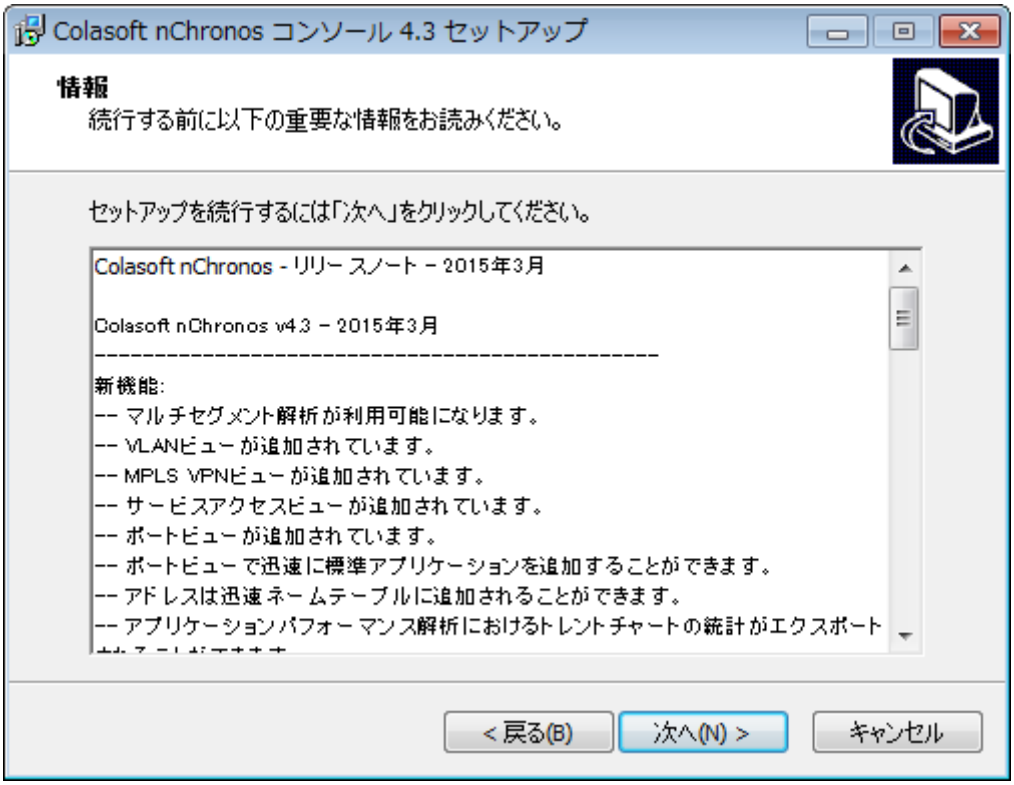
1. nChronos コンソールのインストールファイルをダブルクリックして、セットアップウィザードが下図のように、表示されます。



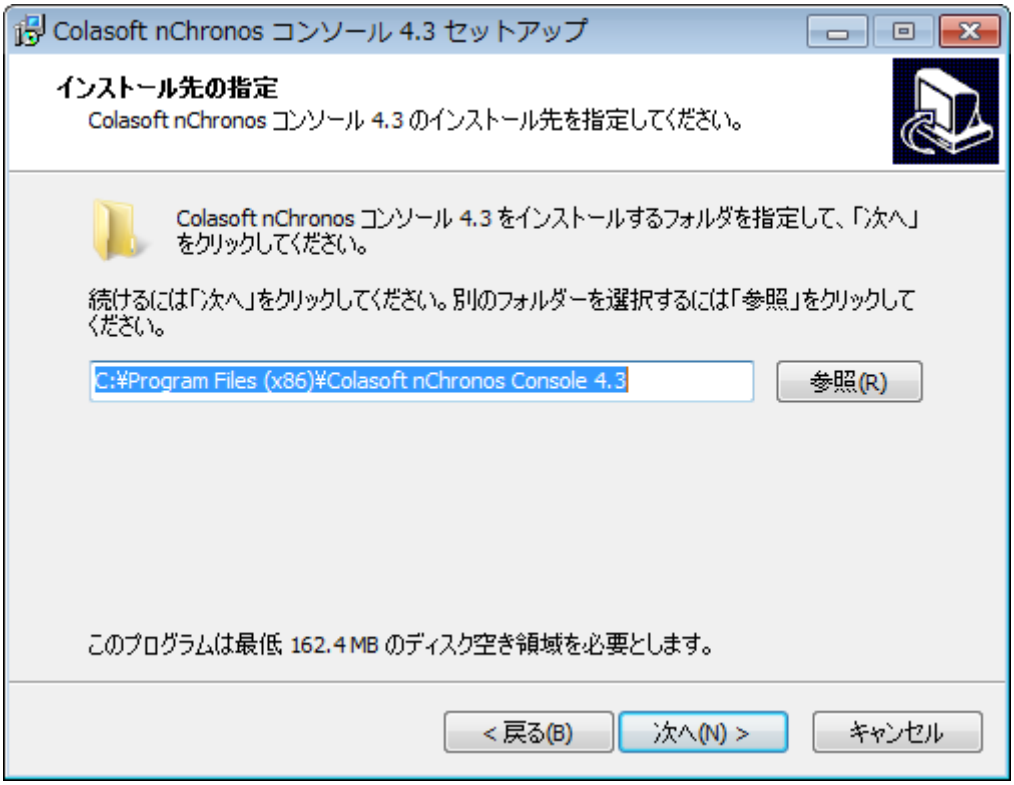
2. 「次へ」をクリックすることによって、下図のように使用許諾契約書ページが表示されます。使用許諾契約書を確認して、同意する場合、「同意する」にチェックを入れてください。



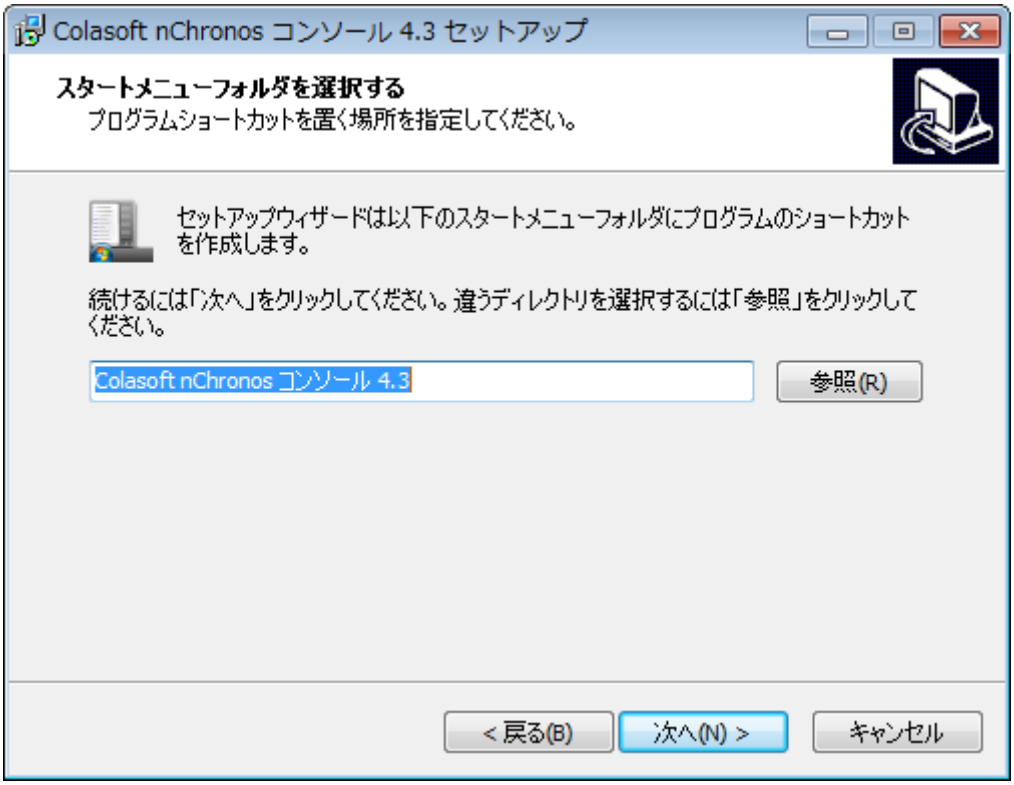
3. 「次へ」をクリックすることによって、下図のようにリリースノートが書いている nChronos 情報ページが表示されます。製品のアップデートを確認します。



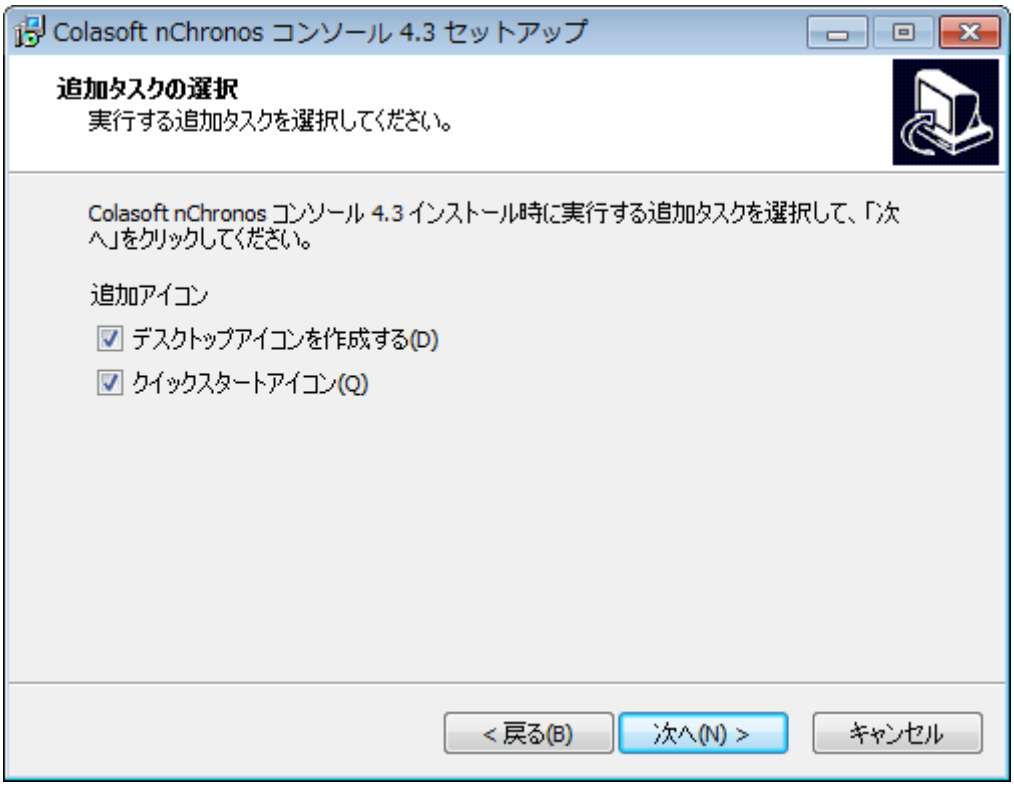
4. 「次へ」をクリックすることによって、インストール先を指定するページが表示されます。デフォルトでは、インストールディレクトリは C:\Program Files\Colasoft nChronos Console 5.0 となっています。ほかのディレクトリを指定するには、下図のように、インストールルートを入力するか、「参照」をクリックして、インストールフォルダを指定することができます。



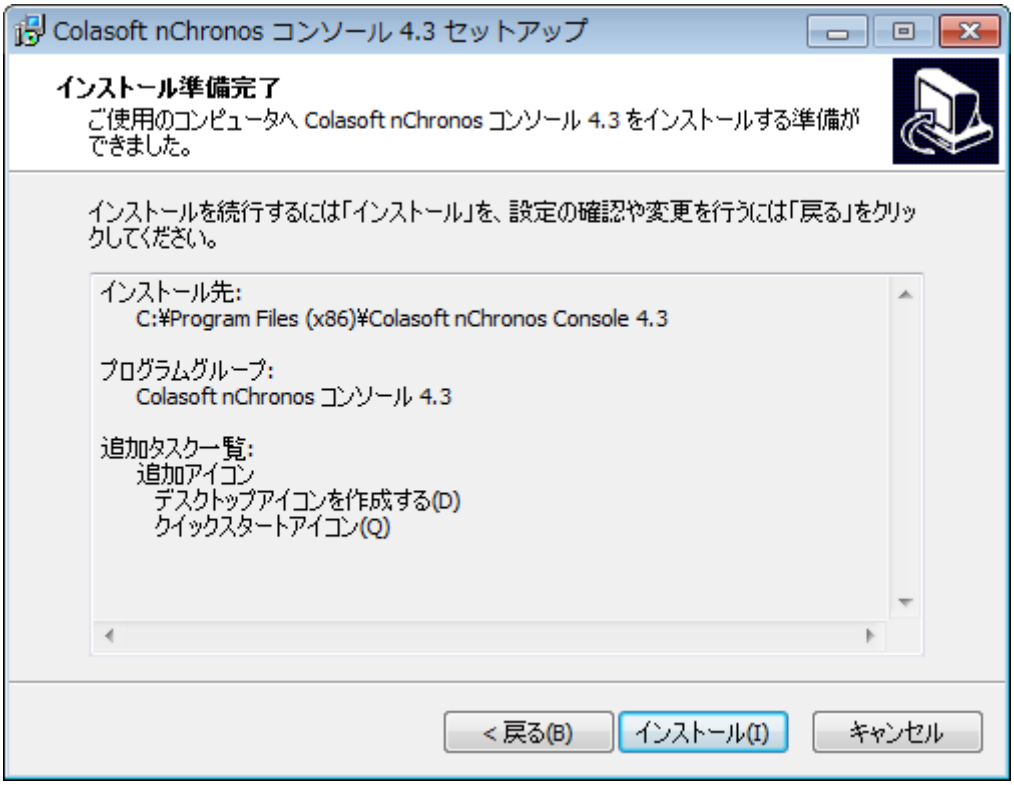
5. 「次へ」をクリックすることによって、下図のようにスタートメニューフォルダが表示されます。スタートメニューフォルダ名を指定します。



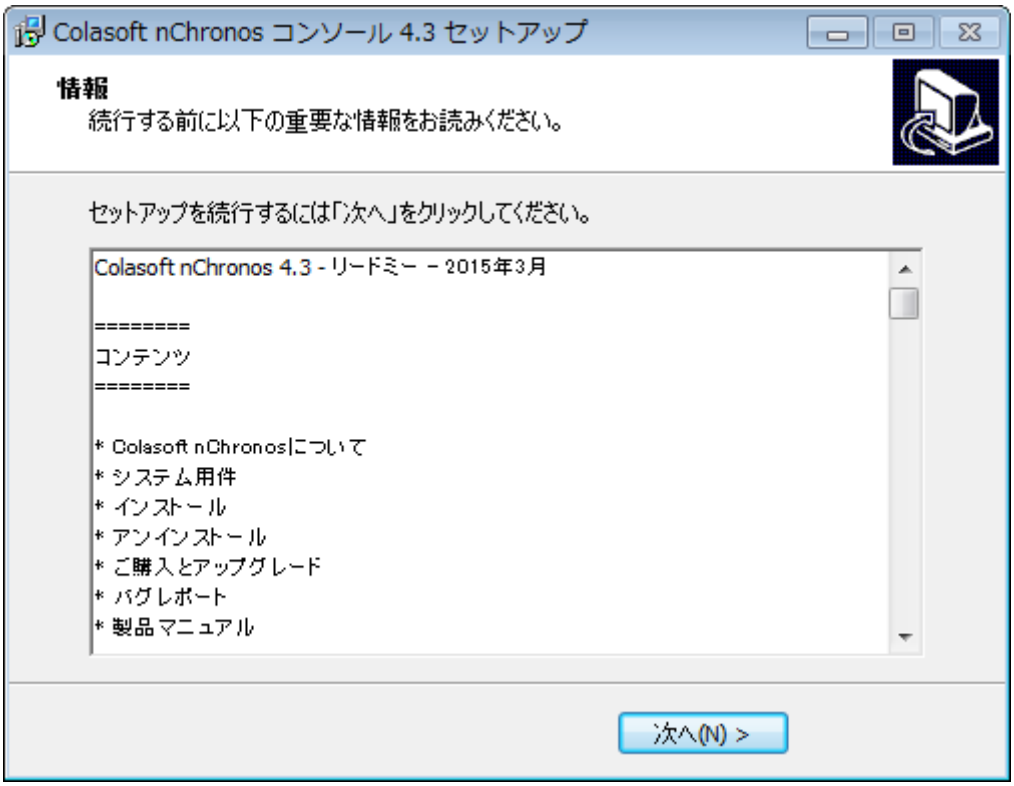
6. 「次へ」をクリックすることによって、追加タスクを選択するページが表示されます。下図のように、デスクトップアイコンとクイックスタートアイコンを作成するかどうかを指定します。



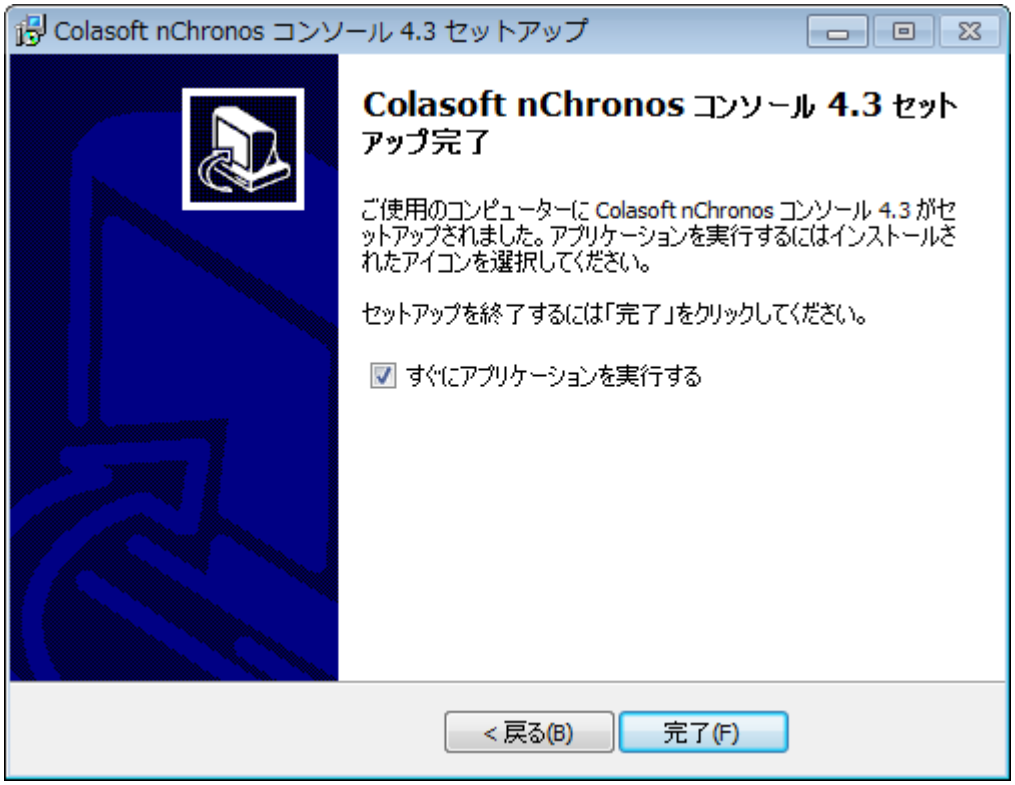
7. 「次へ」をクリックすることによって、インストール準備完了ページが表示されます。下図のように、インストール情報を確認して、すべての情報が正しい場合、「インストール」をクリックして、nChronos コンソールをインストールします。



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

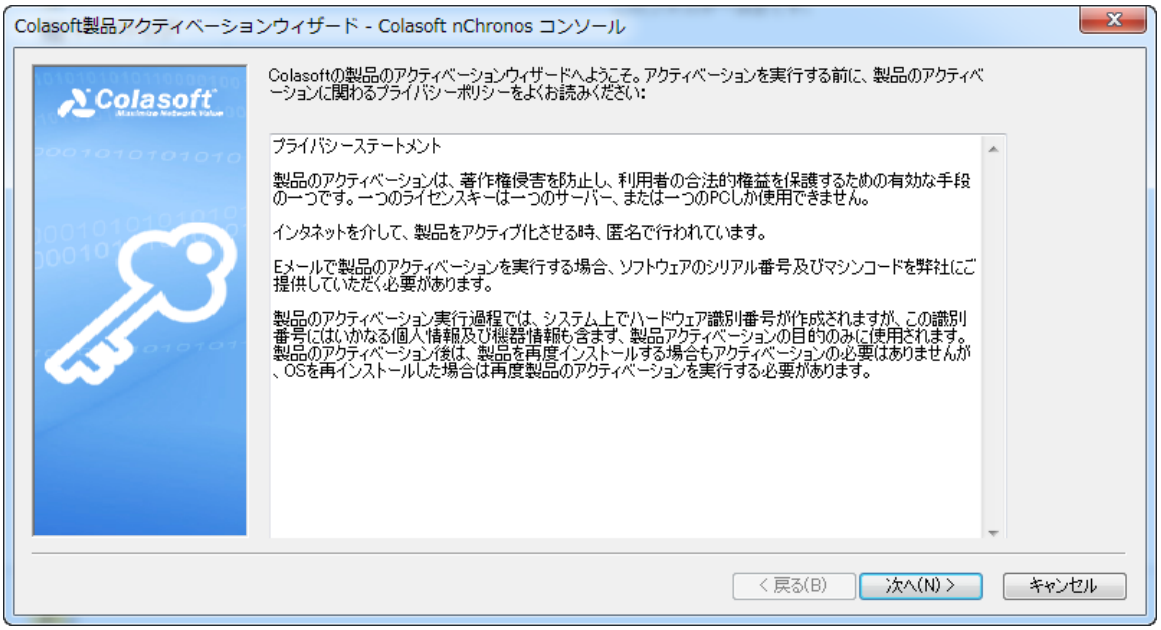


9. インストール完了ページがポップアップされます。「完了」をクリックして、インストールを終了します。



nChronos コンソールをアクティブ化

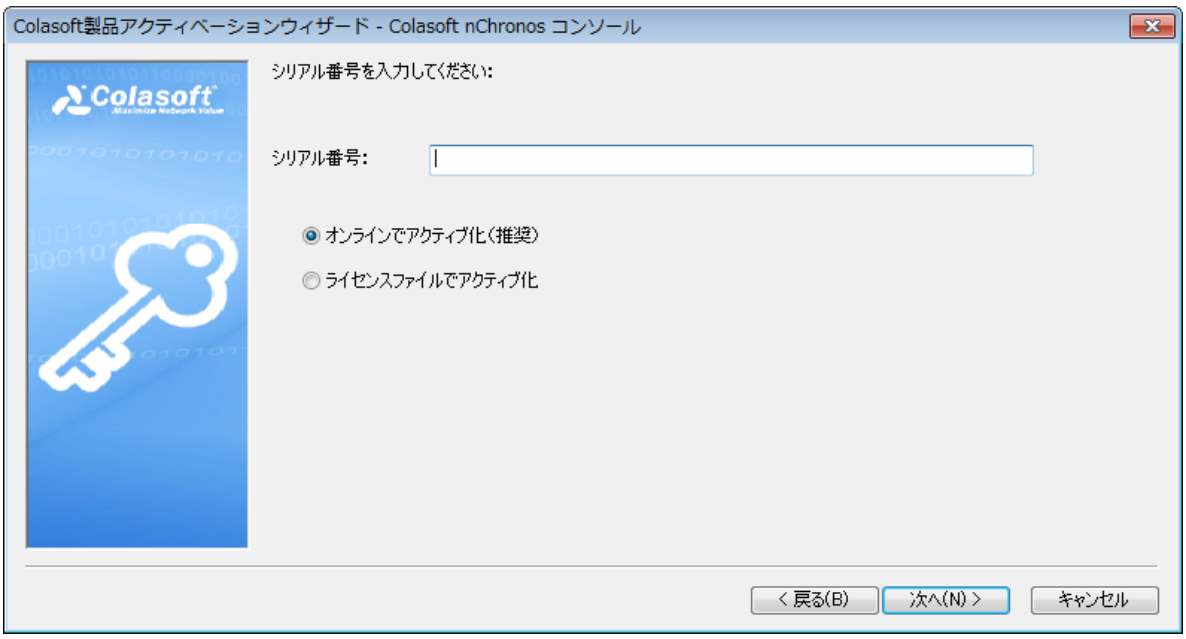
インストール後、アクティベーションウィザードが表示され、ステップごとにアクティベーションをガイドします。



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。

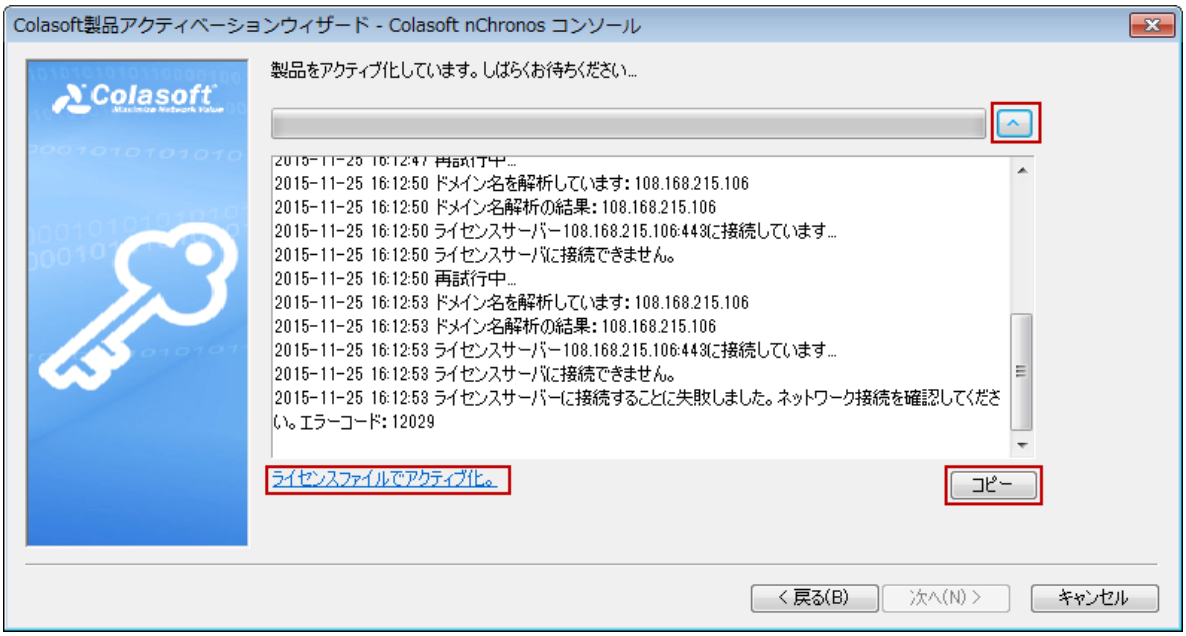
オンラインでアクティブ化

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、

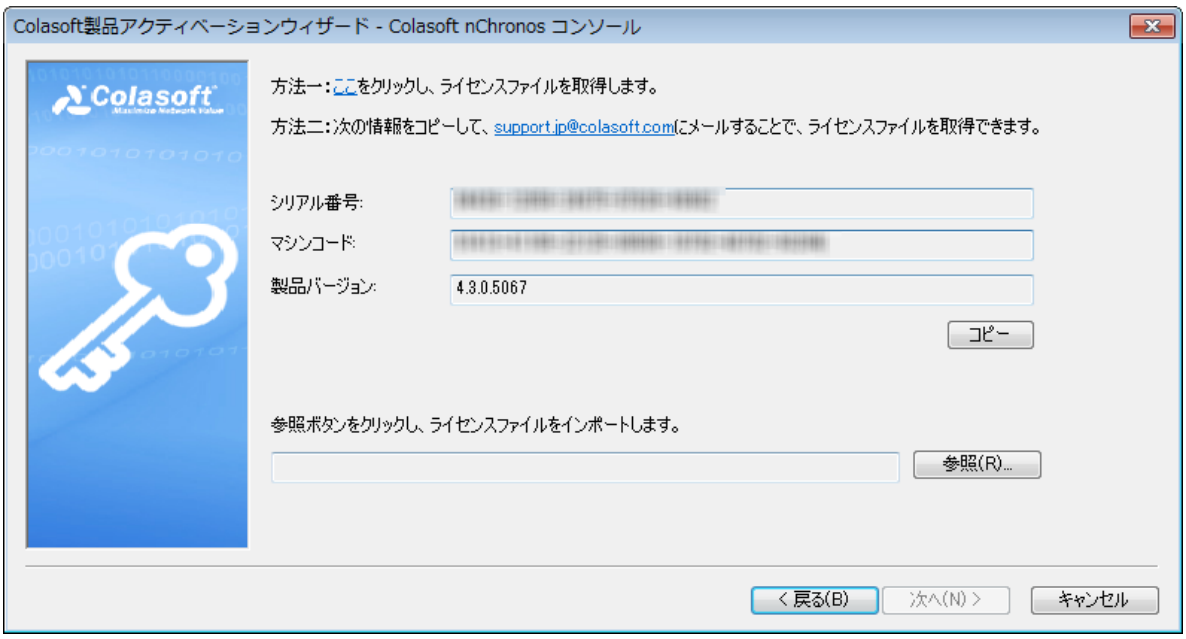
1. アクティベーション詳細を表示する、右側のアクティベーションプログレスバーの横にある二重矢印ボタンをクリックし、「コピー」をクリックします。



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。

4. 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。

5. 「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。
6. 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。

7. 「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。

コピーされた情報を support.jp@colasoft.com に送信します。

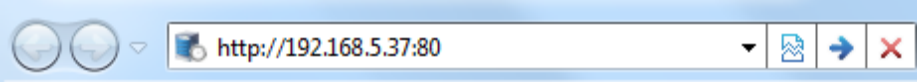
nChronos サーバー設定

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、まず 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

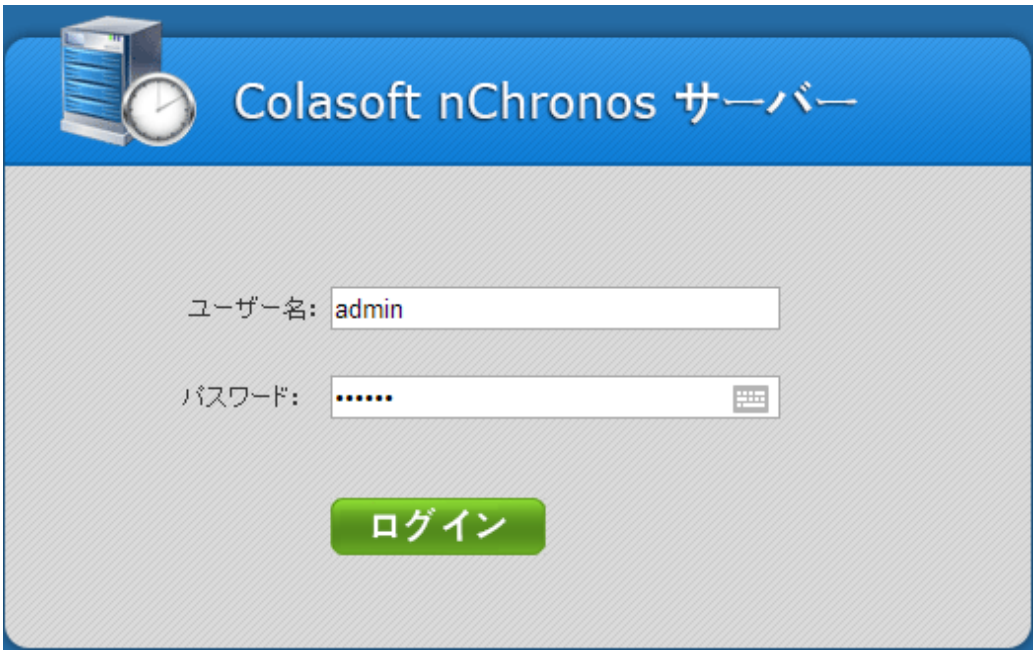
サーバー側とコンソール側の両方を介して、ブラウザから nChronos サーバーにログインすることができます。以下のステップに従い、ブラウザからサーバーにログインします。

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。

ストレージの設定

データを保存するために、ストレージスペースを設定する必要があります。

ストレージスペースを割当てるには、

1. ブラウザからサーバーにログインします。

2. 左のナビゲーションバーにおける「ストレージ」をクリックすることで、ストレージを設定します。

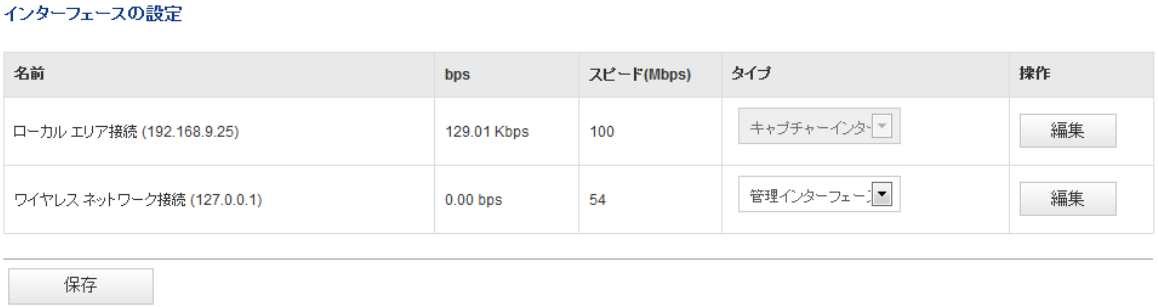
3. 配置スペースを設定します。
4. 必要に応じて、ストレージエリアを修正したり、新しいストレージエリアを追加したりします。
5. エクスポートデータがストレージスペースで占めている容量を設定します。
6. 「OK」をクリックして、設定を保存します。

インターフェースの設定

nChronos の独特なアーキテクチャーのために、nChronos サーバーをインストールしたお使いのマシンは、少なくとも 2 つのネットワークインターフェース/ポートを持つ必要があります。一つはキャプチャーインターフェースとして、もう一つは管理インターフェースとして使われます。キャプチャーインターフェースは、トラフィックをキャプチャーし、キャプチャーされたトラフィックを nChronos サーバーに配信します。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。

キャプチャーインターフェースと管理インターフェースを指定するには、

1. ブラウザからサーバーにログインします。
2. 左のナビゲーションバーにおける「インターフェース」をクリックすることで、インターフェースページに入ります。インターフェースページには、全ての利用可能なアダプタが表示されます。



3. 「タイプ」カラムにおいて、アダプタのために適切なインターフェースタイプを選択します。
4. 「保存」をクリックして、設定を保存します。

キャプチャーインターフェースと管理インターフェースを指定した後、管理インターフェースの設定を変更する必要がある場合、以下のステップに従います。

1. 「管理インターフェース」の後にある「編集」ボタンをクリックすることで、下図のように、管理インターフェース設定ページに入ります。

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

仮想キャプチャーインターフェースを設定する必要がある場合、「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、仮想インターフェースページに遷移します。ここで仮想キャプチャーインターフェースを設定することができます。

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. ブラウザからサーバーにログインします。
2. 左のナビゲーションバーにおける「ネットワークリンク」をクリックして、ネットワークリンクページに入ります。

3. 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。

4. 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。

5. 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。
6. 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。

7. 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。
8. 「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。
9. 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。
10. インバウンド帯域幅、アウト帯域幅、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。

11. 「保存」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。

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. ブラウザからサーバーにログインします。
2. 左のナビゲーションバーにおける「ユーザーアカウント」をクリックして、ユーザ

ーアカウントページに入ります。

3. 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。

4. 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。
5. 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。

6. 「保存」をクリックして、アカウントの追加を終了します。

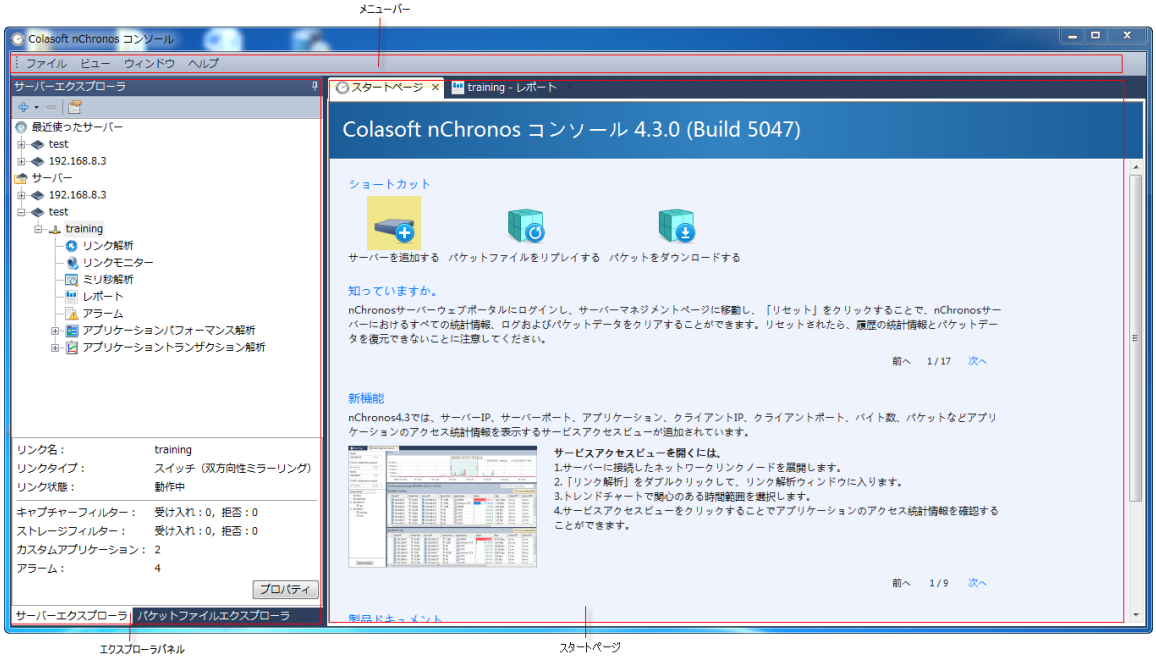
nChronos サーバーの追加と接続

nChronos の独特なアーキテクチャーのために、nChronos サーバーにおけるトラフィックとデータを表示するには、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。

コンソールユーザーインターフェース

インストールした後、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

メニューバーにはファイル、ビュー、およびヘルプという三つのメニューが含まれています。

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。

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から選択されたサーバーを削除します。
- :選択された項目のプロパティを表示します。

サーバーが接続されると、ネットワークリンクは、サーバーの下に表示されます。

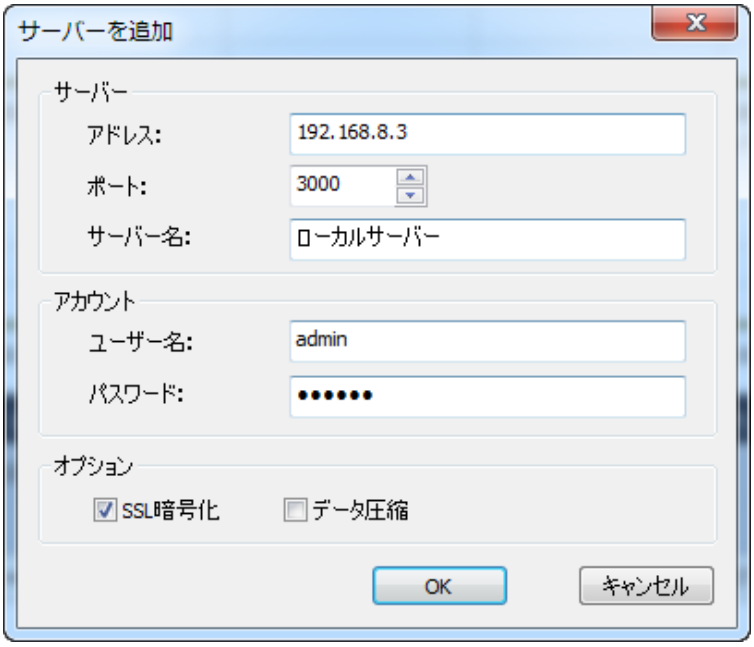
スタートページ

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。

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  ボタンをクリックし、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

次のいずれに従い、nChronos 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。

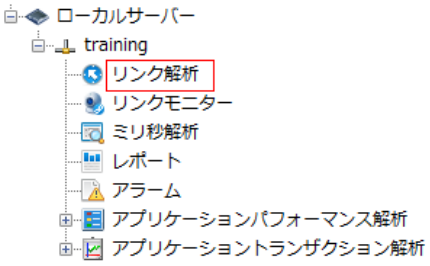
ネットワークリンクの解析

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

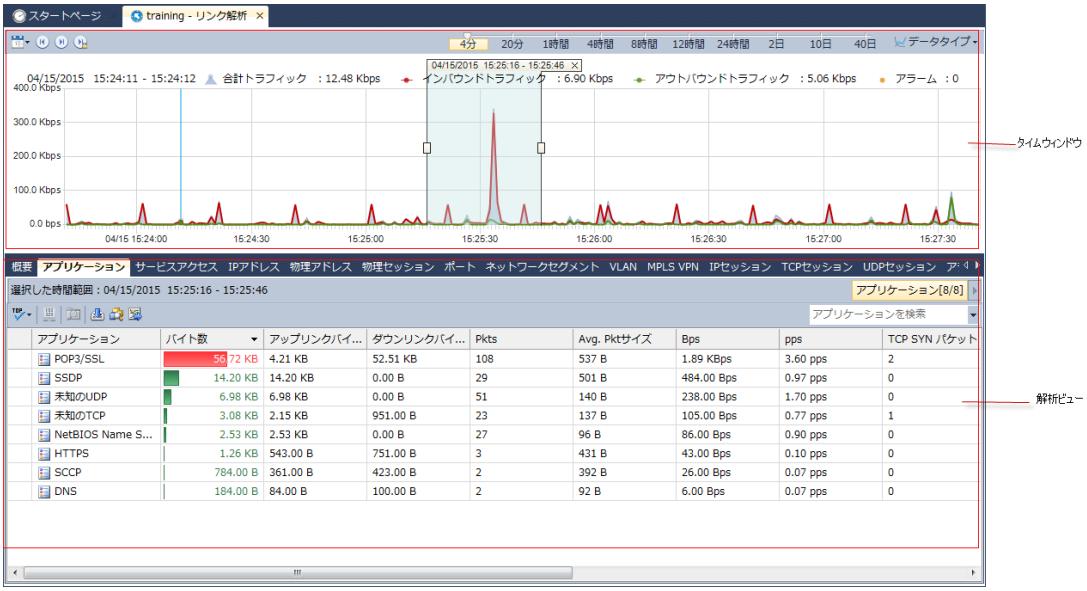
ネットワークリンクを遡及的に解析するには、

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。



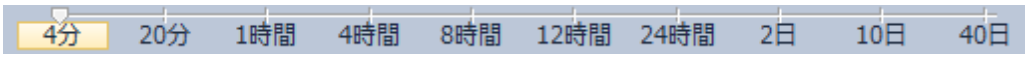
リンク解析ウィンドウはタイムウィンドウパネルと解析ビューパネルからなっています。

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

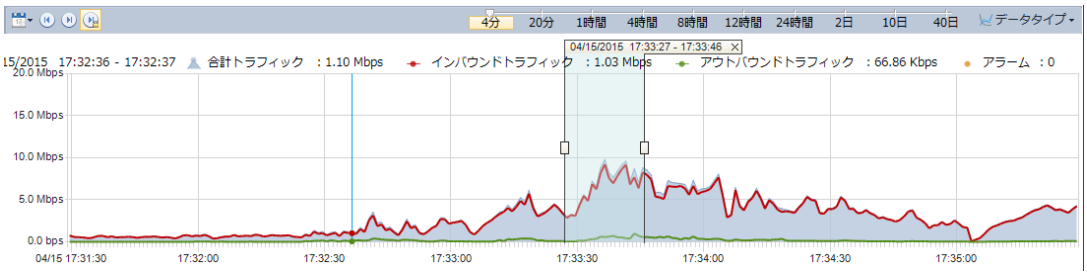
設けられたものです。



: 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。

: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

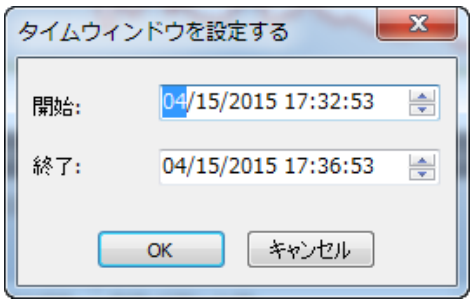
タイムウィンドウをドラッグして、履歴のネットワークデータを表示することができます。タイムウィンドウにおけるチャートの横軸にマウスを移動し、マウスが✋になると、ドラッグすればよいです。

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。そこの開始時間は、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、スピンボタン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。

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。

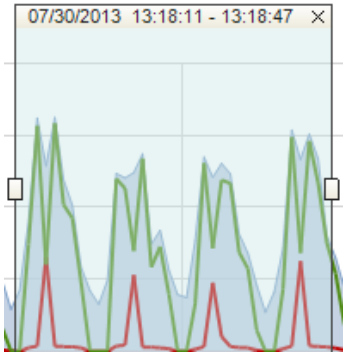
 : このボタンをクリックすると、現在のタイムウィンドウの開始時間は、このネットワークリンクの監視された時間となっています。

 :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。

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。

 :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 ファイルにエクスポートし、保存します。

 : 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新しい解析を行います。

 :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、ネットワークセグメントの統計情報を表示します。

 :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違います。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的解析します。
- **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、トレンドチャートで選択された時間範囲のトラフィック、パケット、パケットサイズ分布、TCP パケット、および利用率の全体的な概要統計を提供します。

アプリケーションビュー

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れることができます。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。

サービスアクセスビュー

サービスアクセスビューには、サーバー/クライアント IP、サービスポート番号、アプリケーション、トラフィック、および TCP パケットを含め、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。

物理アドレスビュー

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。

物理セッションビュー

物理セッションビューには、通信ノード、ノードバイト数、およびパケットに基づく、ネットワークのトラフィックが表示されます。

ポートビュー

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 つのタブがあり、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。

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。

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。

VLAN ビュー

VLAN ビューには、VLAN ID、トラフィック、TCP パケットに基づく VLAN 統計情報が表示されます。

MPLS VPN ビュー

MPLS VPN ビューには、MPLS VPN タグ、トラフィック、および TCP パケットに基づく MPLS VPN 統計情報が表示されます。

IP アドレスビュー

IP アドレスビューは、IP アドレスに基づくトラフィックの統計情報と解析を提供します。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 アドレス」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。

IP セッションビュー

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。

TCP セッションビュー

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トのラフィックが表示されます。

UDP セッションビュー

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。

アラームビュー

アラームビューには、「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」、および「特徴アラーム」を含め、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。全てのリンクアラームログは、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、およびトリガー条件などによって表示されます。

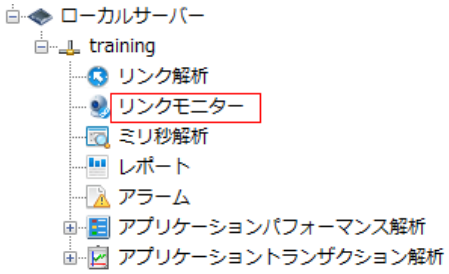
リンクモニター

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遡及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、トレントチャートパネル、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タ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。

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。

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。

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。

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。

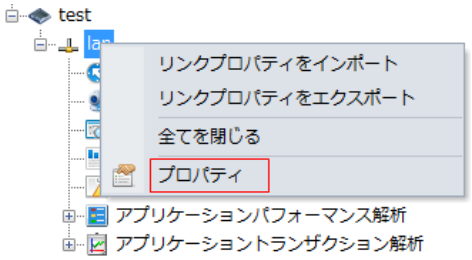
マトリックスパネル

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。

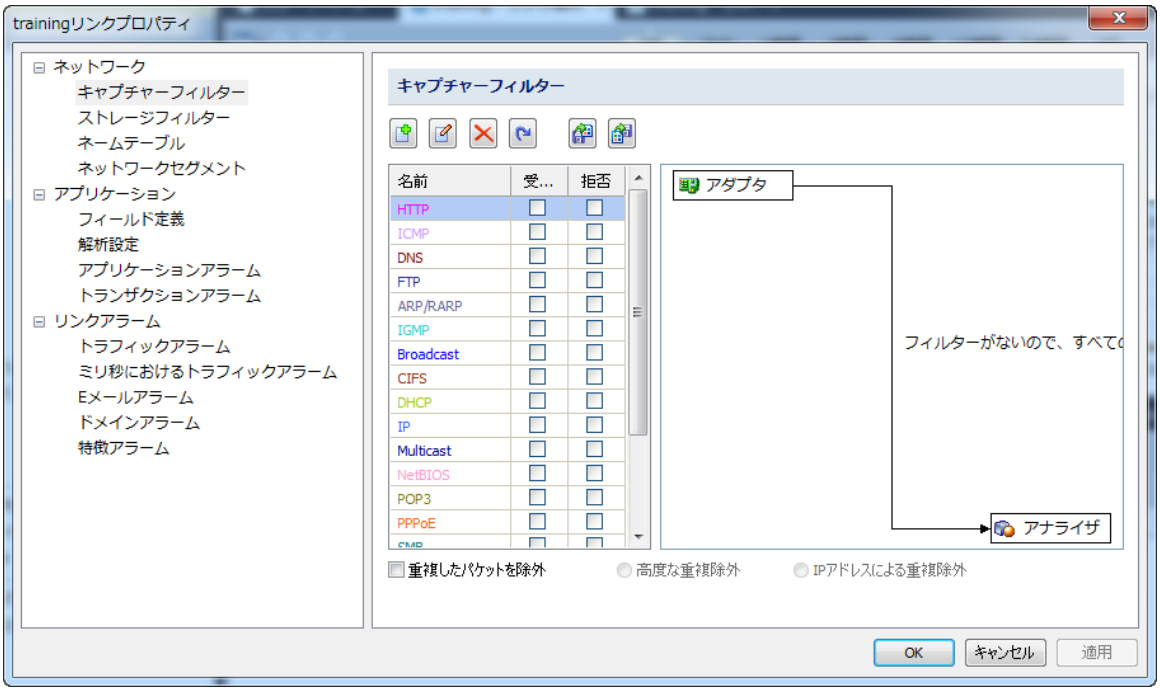
デフォルトでは、マトリックスパネルは、IP アドレス間の通信マトリックスグラフを表示します。マトリックスパネルで右クリックし、「MAC マトリックスグラフ」を選択することで、MAC アドレス間の通信マトリックスグラフを表示することができます。

ネットワークリンクの設定

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、ネットワークリンクを設定する必要があります。ネットワークリンクを設定するには、ネットワークリンクを右クリックし、「プロパティ」をクリックします。



その後、リンクプロパティダイアログボックスがポップアップされます。



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、ネームテーブル、ネットワークセグメント、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、および特徴アラームなどが含まれています。

フィルターを設定する方法、アプリケーションを定義する方法、アラームを設定する方法などの詳しい情報については、『ユーザーガイド』をご参照ください。

注意 リンクプロパティ設定が行われているコンソールとは関係なく、リンクプロパティは、ネットワークリンクに特有のものです。