

nchronos Network Forensic Analysis Application

スタートアップガイド

(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 <u>support.jp@colasoft.com</u>

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
デプロイメント
インストールとアクティベーション7
nChronos コンソールをインストール10
nChronos コンソールをアクティブ化15
オンラインでアクティブ化16
ライセンスファイルでアクティブ化
nChronos サーバー設定19
ブラウザからサーバーにログイン
ストレージの設定
インターフェースの設定
ネットワークリンクの追加
ネットワークリンクを動作させる
アカウントの追加
nChronos サーバーの追加と接続25
コンソールユーザーインターフェース
nChronos サーバーの追加
nChronos サーバーに接続
ネットワークリンクの解析
ネットワークリンクを遡及的に解析
リンク解析ウィンドウ
タイムウィンドウ
解析ビュー30
リンクモニター
リアルタイムにネットワークリンクを監視
リンクモニターウィンドウ
ネットワークリンクの設定



はじめに

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。

はじめに



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。
I P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。

ジ注意 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)
- 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	ンス	トールと	\mathcal{T}	クテ	イベー	・ショ	ン
---	----	------	---------------	----	-----	-----	---

The first Haapter (Bus 0x02, Dev 0x0	Management
- no configuration Present ! [-] Unconfigured Physical Disks	Create New VD
00:01:00: Ready: 278.87 GB 00:01:01: Ready: 278.87 GB 00:01:02: Ready: 278.87 GB 00:01:02: Ready: 278.87 GB 00:01:03: Ready: 278.87 GB	
	Foreign Config
	Manage Preserved Cac
	Create CacheCade Uir

 「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。

Mgmt PD Mgmt Ctrl Mgr	nt Pr Uirt	IOS Configuration Utility 4.00-0 roperties tual Disk Management	014
AID Level : RAID-5		UD Size:836.62 GB00CB	
'D per Span :NZA		VD Name system	
Physical Disks — Disk ID Size [X] 0:01:00 278.87 GB	# 00 01	L 1 Advanced Settings Strip Element Size: 64KB	OK
[X]00:01:02 278.87 GB [X]00:01:03 278.87 GB	02 03	Read Policy : Adaptive R	CANCEL
		Write Policy: Write Back	
Secure UD:		[] Force WB with no battery [] Initialize [] Configure HotSpare	

- 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。

インストールとアクティベーション



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。

0S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。

```
-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。

「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。



インストールとアクティベーション



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。

号 Colasoft nChronos コンソール 4.3 セットアップ	- • •
使用許諾契約書 続行する前に以下の重要な情報をお読みください。	
以下の使用許諾契約書をお読みください。インストールを続行するにはこの契約 する必要があります。 	書(こ同意
Colasoft nChronosエンドユー ザーライセンス契約	*
Copyright (c) 2015 Colasoft LLC. All rights reserved	
本ライセンス契約は、Colasoft nChronos(以下は「本ソフトウェア製品」といいます 関して、お客様(個人、または企業)とColasoft LLO(以下は「COLASOFT」といい。 の間で合意される、法的効力を持つ契約です。以下の条件を丁寧にお読みくださ 本ソフトウェア製品を使用する前に、下記の諸条件をしっかりとお読みください。本 ウェア製品をオンフトールまたけ使用した場合け、このライセンフ契約に同会した	ま)に ます) い。 :∨フト -
◎ 同意する(A)	
○ 同意しない(D)	
< 戻る(B) 次へ(N) >	キャンセル

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。



🖞 Colasoft nChronos コンソール 4.3 セットアップ 📃 📼 💌
情報 続行する前に以下の重要な情報をお読みください。
セットアップを続行するには「次へ」をクリックしてください。
Colasoft nChronos - リリースノート - 2015年3月
Colasoft nChronos v4.3 - 2015年3月
 新機能: マルチセグメント解析が利用可能になります。 マルチセグメント解析が利用可能になります。 VLANビューが追加されています。 サービスアクセスビューが追加されています。 ボートビューが追加されています。 ボートビューで迅速に標準アプリケーションを追加することができます。 アドレスは迅速ネームテーブルに追加されることができます。 アブリケーションパフォーマンス解析におけるトレントチャートの統計がエクスポート
< 戻る(B) 次へ(N) > キャンセル

「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。

骨 Colasoft nChronos コンソール 4.3 セットアップ	
インストール先の指定 Colasoft nChronos コンソール 4.3 のインストール先を指定してください。	
Colasoft nChronos コンソール 4.3 をインストールするフォルダを打 をクリックしてください。	指定して、「次へ」
続けるには「次へ」をクリックしてください。別のフォルダーを選択するには「参 ください。	細いをクリックして
C:¥Program Files (x86)¥Colasoft nChronos Console 4.3	参照(R)
このプログラムは最低 162.4 MB のディスク空き領域を必要とします。	
< 戻る(B) 次へ(N) >	キャンセル

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。



弱 Colasoft nChronos コンソール 4.3 セットアップ	
スタートメニューフォルダを選択する プログラムショートカットを置く場所を指定してください。	
2001 セットアップウィザードは以下のスタートメニューフォルダにプログラムの を作成します。)ショートカット
続けるには「次へ」をクリックしてください。違うディレクトリを選択するには「参照 ください。	しをクリックして
Colasoft nChronos コンソール 4.3	参照(R)
< 戻る(B) 次へ(N) >	キャンセル

「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。

弱 Colasoft nChronos コンソール 4.3 セットアップ	- • •
追加タスクの選択 実行する追加タスクを選択してください。	
Colasoft nChronos コンソール 4.3 インストール時に実行する追加タスクを遠 へ」をクリックしてください。	翻訳して、「次
追加アイコン ☑ デスクトップアイコンを作成する(D) ☑ クイックスタートアイコン(Q)	
< 戻る(B) 次へ(N) >	キャンセル

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。



弱 Colasoft nChronos コンソール 4.3 セットアップ	- • 💌
インストール準備完了 ご使用のコンピュータへ Colasoft nChronos コンソール 4.3 をインストールする準 できました。	
インストールを続行するには「インストール」を、設定の確認や変更を行うには「夏 クしてください。	見る」をクリッ
インストール先: C:¥Program Files (x86)¥Colasoft nChronos Console 4.3	*
プログラムグループ: Colasoft nChronos コンソール 4.3	
追加タスクー覧: 追加アイコン デスクトップアイコンを作成する(D) クイックスタートアイコン(Q)	
<	
< 戻る(B) インストール(I)	キャンセル

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。

骨 Colasoft nChronos コンソール 4.3 セットアップ	
情報 続行する前に以下の重要な情報をお読みください。	
セットアップを続行するには「次へ」をクリックしてください。	
Colasoft nChronos 4.3 - リードミー - 2015年3月	<u>^</u>
コンテンツ	
======	
* Colasoft nChronosについて * システム用件 * インストール * アンインストール * ご購入とアップグレード * バグレポート * 製品マニュアル	~
次へ(N) >	

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。



インストールとアクティベーション



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。

Colasoft製品アクティベーショ	ンウィザード - Colasoft nChronos コンソール	x
	Colasoftの製品のアクティベーションウィザードへようこそ。 アクティベーションを実行する前に、製品のアクティベ ーションに関わるプライバシーボリシーをよくお読みください:	
	プライバシーステートメント 製品のアクティベーションは、著作権侵害を防ち止し、利用者の合法的特益な保護するための有効な手段 の一つです。一つのライゼンスキーは一つのサーバー、または一つのPOLか使用できません。 インタネットを介して、製品をアクティブ化させる時、匿名で行われています。 Eメールで製品のアクティベーションを実行する場合、ソフトウェアのシリアル番号及びマシンコードを弊社にご 提供していただく必要があります。 製品のアクティベーション実行過程では、システム上でハードウェア識別番号が作成されますが、この識別」 番号には、かねる個人情報及び提器情報に含まず、製品アクティベーションの目的のみに使用されます。 製品のアクティベーションが後は、製品を再度インストールする場合もアクティベーションの必要はありませんが 、OSを再インストールした場合は再度製品のアクティベーションを実行する必要があります。	
	< 戻る(B) 次へ(N) > キャン	1世ル

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。

Colasoft製品アクティベーショ	ンウィザード - Colasoft nChronos コンソール	— ×-
Colasoft	シリアル番号を入力してください:	
0001010101010	シリアル番号:	
	 ● オンラインでアクティブ化(推奨) ● ライセンスファイルでアクティブ化 	
	< 戻る(B) 次へ(N) >	キャンセル

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。

Colasoft製品アクティベーショ	ョンウィザード - Colasoft nChronos コンソール	×
Colasoft製品アクティペーショ	a ンウィザード - Colasoft nChronos コンソール 製品をアクティブ化しています。しばらくお待ちください… 2015-11-25 16:12:50 ドメイン名を解析しています:108.168.215.106 2015-11-25 16:12:50 ドメイン名解析の結果:108.168.215.106 2015-11-25 16:12:50 ライセンスサーバー108.168.215.106 2015-11-25 16:12:50 ライセンスサーバー108.168.215.106 2015-11-25 16:12:50 再話行中… 2015-11-25 16:12:53 ドメイン名解析の結果:108.168.215.106 2015-11-25 16:12:53 ドメイン名解析の結果:108.168.215.106 2015-11-25 16:12:53 ドメイン名解析の結果:108.168.215.106 2015-11-25 16:12:53 ドメイン名解析の結果:108.168.215.106 2015-11-25 16:12:53 デイン名中バー108.168.215.106 2015-11-25 16:12:53 ライセンスサーバー108.168.215.106 2015-11-25 16:12:53 ライセンスサーバー108.168.215.106	×
	2015-11-25 16:12:53 ライセンスサーバーに接続することに失敗しました。ネッドワーク接続を確認してくたさい。エラーコード:12029	
	<u>ライセンスファイルでアクティブ化。</u>	
	く 戻る(B) /ズへ(N) > キャノセノ	۶.

- 「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 <u>support. jp@colasoft.com</u>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。

Colasoft製品アクティベーションウィザード - Colasoft nChronos コンソール				
	方法一: <u>ここ</u> をクリックし、 方法二:次の情報をコピ	ライセンスファイルを取得します。 ーして、 <u>support.jp@colasoft.com(</u> こメールすることで、ライセンスファイルを取得できます。		
3	シリアル番号: マシンコード: 製品パージョン:			
	参照ボタンをクリックし、ラ	イセンスファイルをインボートします。 参照(R)… く 戻る(B) 次へ(N) > キャンセノ		

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。

Serial Number	03930-12345-12345-12345-12345	
Machine Code	12345-12345-12345-12345-12345-12345-12345	
	1935zMTOz9DMzMTKydDZzMzMy9DPzMzNztDMzMXJzNDOzcjIzdDOzzzZyWP0/f3GMzjiteS4gppz1cK hRlafpKhgd+c/gwxhN/xU0Hb5nQOIc7/iGuVne/TxcbTCnO1/1H2ZOIRmMWD3MpRha/41gNV0e7yId5	L9vLBAfHMVNJU/102MYON ctr6BEsbmH+Oascor8vHz
	90	:x/h
	30	Jrdb
	on	IVTM
	Wp	JEDR
isanca Fila		3806
icense rile		JUSE DWAT
	-7	71W1
	III/ 710	1350
		109
		112 D
	uta/rJOSiPjJ6pWx1rurVVTx5eGOPf60/wHerNPrEmifwdot5kGI8rnY4fLGP7XZVSWfjoX4i4LshNH goGJ8dEBc8KYzvvVKLIhiAKy0hyJmr6creID4cvVhJM5w5KlhkWS1U44bbUY0Uipc+V7T7g0KZoJv5m	d1ZtIP89xz3HkWrER0YSB vkpE1w/bP4+sSAvgbfprL

Copy to Clipboard Save as Bin

Contact service@colasoft.com if you have any questions.

- 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。
- 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。

「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<u>support.jp@colasoft.com</u>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 オルトでは 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。

Colasoft nChronos サーバー						
ユーザー名:	admin]				
パスワード:	•••••]				
	ログイン					

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。



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。

いレージ設定								
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	使用室
	C:	79GB	7GB	0 GB	}	0GB	0 GB	0.00%
	D:	100GB	87GB	0 GB	1	0GB	0 GB	0.00%
•	E:	285GB	254GB	100 GB	3	0GB	0 GB	0.00%
システム予約領域 SMFデータ	116GB	未割当て3	348GB	使用領域	ф0GB	残	りのスペース0GB	
統計情報	30 %			パケッ	ŀ: 7 0) %		
ログデータ								
アラームログ	: 100 MB			トランザクションログ	5: 10	МВ		

3. 配置スペースを設定します。

ОК

- 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。
- 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。

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ー▼	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

- 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。

「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。

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:	192.168.5.160
サブネットマスク:	225.225.225.0
ゲートウェイ:	192.168.5.1
DNSサーバー:	8.8.8.8
保存	キャンセル

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。
- 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。



クレて、次の図が表示

・ イツトワ されます	- / / / / / / -	シにわり	◇「朳焼リンク」・	とクリックして、伏の図。
ネットワークリンク/第	っ f規ネットワークリンク			
リンク名:	training	リンク名には	\/:?" <> のような文字を含むことができ。	ません
リンクタイプ:	スイッチ(双方向性ミラーリング)	•		
🔽 ミリ秒統計を有効にす	3			
🔲 スイッチタイムスタン:	プを使用する			
c	ARISTA	O VSS Monitoring	C Gigamon	
インアウトバウンドトラフィ	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)
🔽 ローカル エリア指	 衰続	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PFドレスを読別するためにネット 行コードで区切ってください。 例えれば: IPFドレス/サブネットマスク:192.10 2001:3ef0:260 IPFドレス範囲:192.168.0.0192.1 単ーIPFドレス:192.168.0.100、ま	ワークセダメントを一行に一つ入力します。 雑数の場合、 お 38.0.0/24、192.168.0.0/255.255.255.0、または 168.1.255、または2001:3ef0::0001-2001:3ef0::0005 たは22001:3ef0::0001
帯域幅の設定				
インバウンド帯域幅:	10	Mbps〈範囲	:1-1,000,000 Mbps)	
アウトバウンド帯域幅:	10	Mbps〈範囲	:1-1,000,000 Mbps)	
総帯域幅: (総帯域幅は、インバウンド	10	Mbps きい方より大きく、両方の	の合計数より小さい必要があります。〉	
OK	キャンセル			

- 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。

- 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。

- 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。
- 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。
- 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。
- 「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。
- 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。

ユーザーアカウント / 新規アカウント

ユーザー名:	admin2	アカウントには数字、アルファペット、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。
パスワード:		パスワードの長さは6-20文字です。
バスワードを再入力:		
備考(オブショナル):		40文字を超えることができません。
タイプ:	2~#~	T
	■ アカウントを無効にする。	
保存	キャンセル	

- 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>すぺてのプログラム > 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。

Oclasoft nChronos コンソール		×
ファイル ビュー ウィンドウ ヘルプ		
ナーバーエクスプローラ ₽	· ○スタートページ × 🛄 training - レポート	
◆ + 😁 ⑦ 最近使ったサーバー ☆ ◆ test	Colasoft nChronos コンソール 4.3.0 (Build 5047)	
	ショートカット ショートカット レーバーを追加する パケットファイルをリプレイする パケットをダウンロードする 知っていますか、 nChronosサーバーウェブポータルにログインし、サーバーマネジメントページに移動し、「リセット」をクリックすることで、nChronosサーバーにおけるすべての統計時報、ログおよびパケットデータをクリアすることができます。リセットされたら、 履歴の統計情報とパケットデー タを復元できないことに注意してください。 約へ 1/17 次へ	E
Uング名: training Uングタイプ: スイッチ (双方向性ミラーリング) Uング状態: 動作中 キャプチャーフィルター: 受け入れ:0,拒否:0 ストレージフィルター: 受け入れ:0,拒否:0 カフィなーブリート	新編記 nChronod.3では、サーバーP. サーバーボート、アプリケーション、クライアントIP. クライアントボート、バイト数、パケットなどアプリ ケーションのアクセス検討情報を表示するサービスアクセスとユーやWELMEれています。 サービスアクセスとユーを描くには、 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	_
ガスション・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	<u> </u>	
	7.5 - 1.00 - 21	

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。

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。

サーバーを追加	×
サーバー	
アドレス:	192.168.8.3
ポート:	3000
サーバー名:	ローカルサーバー
アカウント	
ユーザー名:	admin
パスワード:	•••••
オプション	
ISSL暗号化	□ データ圧縮
	OK キャンセル

- 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H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。
- 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。

🤇 スタートページ 💦 🔇 t	raining - リンク解析 ×	<							
t• ® Ø ₽			4	分 20分 :	1時間 4時間 8時間	12時間 24時間	2日 10日 4	Ю日 ビデータタイプ・	
04/15/2015 15:24:11 - 00.0 Kbps	15:24:12 🗼 合計トラ	5フィック :12.48 K	bps 🔶 インパウ:	015 15:25:16 - 15:2 ンドトラフィック	25:46 × 7 : 6.90 Kbps 🔶 🏸	ウトバウンドトラフ	イック :5.06 Kbps	• アラーム :0	
00.0 Kbps					1				
00.0 Kbps					-				
0.0 bps	15:24:3	30 15:2	A	5:25:30	15:26:00	15:26:30	15:27:00	15:27:30	
腰 アプリケーション サ- 駅した時間範囲:04/15/201	-ビスアクセス IPアド 5 15:25:16 - 15:25:4	レス 物理アドレス 4 6	物理セッション ポー	トネットワーク	ウセグメント VLAN MPL	LS VPN IPセッショ	ン TCPセッション	UDPセッション ア:4) アプリケーション[8/8] ▶	
⊱ 🚊 🖾 🖾 📖							アプリケー	-ションを検索 🗸	
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	
POP3/SSL	56 <mark>.72 KB</mark>	4.21 KB	52.51 KB	108	537 B	1.89 KBps	3.60 pps	2	
5SDP	14.20 KB	14.20 KB	0.00 B	29	501 B	484.00 Bps	0.97 pps	0	
iii 未知のUDP	6.98 KB	6.98 KB	0.00 B	51	140 B	238.00 Bps	1.70 pps	0	解析ビ
EI 未知のTCP	3.08 KB	2.15 KB	951.00 B	23	137 B	105.00 Bps	0.77 pps	1	
E NetBIOS Name S	2.53 KB	2.53 KB	0.00 B	27	96 B	86.00 Bps	0.90 pps	0	
E HTTPS	1.26 KB	543.00 B	751.00 B	3	431 B	43.00 Bps	0.10 pps	0	
SCCP	784.00 B	361.00 B	423.00 B	2	392 B	26.00 Bps	0.07 pps	0	
E DNS	184.00 B	84.00 B	100.00 B	2	92 B	6.00 Bps	0.07 pps	0	

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。

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。 メデータタイプ・: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¹⁰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。

タイムウィ	ンドウを設定する	x					
開始:	04/15/2015 17:32:53						
終了:	04/15/2015 17:36:53	-					
ОК キャンセル							

「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。



ジ注意 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テ 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、 マウスがいたなると、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、メ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。

第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。

詳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。

I 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。



ネットワークリンクの解析

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。



ネットワークリンクの解析

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



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。
- 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。

◎ トレンドチャート ◎ リアルタイムデータ □ Topセグメント ◎ Topアプリケーション ◎ Top内部ホスト □ アラーム □ マトリックス 🍋									
リアルタイムデータ									×
スループット (Mbps)		パケット (pps)		TCP SYN パケット (p	ps)	TCP SYNACKパケッ	ト (pps)		アラーム
2.8	インバウンド 2.7 アウトバウンド 0.1	374.0	インパウンド 243.0 アウトバウンド 131.0	0.0	インバウンド 0.0 アウトバウンド 0.0	0.0	インバウ アウトバウ	ンド 0.0 ンド 0.0	0
トレンドチャート					~ ×	Top内部ホスト		Topアプリク	rーション ×
8.0 Mbps 6.0 Mbps 4.0 Mbps 2.0 Mbps		 インパウンドトラ: 	フィック + アウト.		· · · · · · · · · · · · · · · · · · ·	192.168.9	9.25 2.91 Mbps	Colas	oft 1.57 Mbps
04/15 09:33:30	09:34:00 09:34	4:30 09:35:00	09:35:30 09:36	5:00 09:36:30	09:37:00	192.168.	9.2	нпр	5
800.0 pps 600.0 pps 400.0 pps 200.0 pps 0.0 pps						I	3.07 Kbps		1.33 Mbps
04/15 09:33:30 <=64 B 800 600 400 200 0	09:34:00 09:3- 127 B + 128-255	4:30 09:35:00 B - 256-511 B	09:35:30 09:36 ← 512-1023 B	6:00 09:36:30	09:37:00 + >=1518 B	Top内部オ	⊼ス…	Торӯ	プリケ…
04/15 09:33:30 40.0 pps 30.0 pps 20.0 pps 10.0 pps 0.0 pps 0.4/15 09:33:30	09:34:00 09:34	4:30 09:35:00	09:35:30 09:36	3:00 09:36:30 SYN ← SYNACH AA A AA A 5:00 09:36:30	09:37:00 ・ アラーム AAAAAAAA 09:37:00				

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。 で 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。



リンクモニター

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。