Colasoft

Colasoft nChronos

ユーザーガイド

ウェブサイト: https://www.colasoft-japan.com
メールボックス: support@colasoft-japan.com

目次

目次

1 はじめに

概要

このドキュメントでは、nChronos の一般的な構成操作と日常メンテナンスの操作を紹介します。

対象読者

このドキュメントは、主に次のエンジニアに適用されます:

- データ構成エンジニア
- ネットワークエンジニア

専門用語

このドキュメントで使用されている用語は、以下の表にリストされています。

表 1.1 専門用語リスト

専門用語	説明
分析対象	分析対象とはネットワーク内の各ノード要素，たとえば、ネットワークプロトコル,物理アドレス,IP アドレスなどを指します。
分析サーバー	分析サーバーはネットワークリンクに対してトラフィック収集、統計分析、データのリアルタイムストレージを行います。同時に、通信口を提供して、それぞれ分析コンソールと分析センターとデータのインタラクティブを行って、全体の遡及分析システムの核心です。
分析コンソール	分析コンソールは、ヒューマンマシンインタフェースを提供してから、分析サーバに接続し、各種の通信データをリアルタイムで出力します。ユーザーは、分析コンソールを通じて、異なる幹線ネットワークの分析サーバに接続して、幹線ネットワークのネットワーク通信状況を見るおよび分析することができます。

専門用語	説明
分析センター	分析センターは統一的で集中的な監視分析プラットフォームを提供して、各ネットワークリンクに配置された分析サーバー内のデータを定期的に収集と統計することによって、集中的なデータ展示を提供します。同時に、分析サーバについての集中管理、監視、分析レポートと警報などの機能があります。
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。
タイムウィンドウ	タイムウィンドウでは、4 分、40 分、4 時間、16 時間、240 時間、240 日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。
タイムピッカー	分析サーバーは数時間、数日、数週間、さらには数か月のデータを保存するため、特定の時間範囲のデータを表示する場合は、時間セレクターで時間範囲を選択して、その時間範囲のデータを表示できます。
データストレージ	分析サーバーは RAID アレイを採用しており、統計データやデータパケットストレージなどの大容量データストレージ機能を備えています。 データストレージを介して、分析コンソールのデータクエリと取得にリアルタイムで応答し、履歴データの遡及的分析を実行できます。
データマイニング	ユーザーのニーズに応じて、期間やネットワークオブジェクトごとにデータを取得することで、ユーザーが必要とするデータをすばやく取得できます。
特徴アプリケーション	データストリームの固有値シグネチャに基づいてカスタマイズされたアプリケーション。
統計データ	統計は、分析サーバーによってキャプチャおよび分析されたネットワーク操作情報です。 統計データは、分析コンソールによるデータクエリと分析のために分析サーバーに保存されます。 分析サーバーのストレージスペースがいっぱいに

専門用語	説明
	なると、統計データは循環的に保存されます。つまり、最も古いデータが削除され、最新の統計データが保持されます。
Web アプリケーション	URL 分析アプリケーションの場合、現在のバージョンは HTTP ベースのアプリケーションの分析のみをサポートしており、Web アプリケーションには複数のトランザクションを含めることができます。

声明

Colasoft nChronos は、ユーザーネットワーク内のデータパケットをキャプチャして分析することにより、ネットワークパフォーマンスの分析と監視を実現するシステムです。ユーザーが nChronos を使用してネットワーク通信データパケットをキャプチャおよび分析する場合、ユーザーは現地の国または地域の法律および規制に準拠する必要があります。

nChronos は、キャプチャとクリッピングのフィルタリングとストレージのクリッピングフィルタリングを提供します。これにより、機密性の高いネットワーク情報のキャプチャとストレージを回避できます

2 nChronos について

Colasoft nChronos は、Colasoft が立ち上げた新しいネットワーク遡及分析製品であり、エンタープライズネットワーク管理の新しいソリューションを提供します。

製品構成

nChronos は nChronos サーバー(以下「サーバー」という) 、nChronos コンソール（以下「コンソール」という）および分散ネットワーク分析センター（以下「分析センター」という）から構成されています。

サーバー

サーバーは独立したハードウェアデバイスであり、主に、サーバーが配置されているネットワークセグメントのトラフィック収集、分析、統計、およびストレージを担当します。 サーバーは、各ネットワークオブジェクトに対して詳細なデータ統計を実行して、システム全体のコア部分である潜在的なネットワークの問題を診断および警告します。

サーバーは、コンソールからさまざまなコマンド要求を受信し、その結果をリアルタイムでコンソールに返す役割を果たします。

コンソール

コンソールは新しいインターフェースとレイアウトを採用し、データ分析と表示のためにサーバーに接続するための人間とコンピューターの相互作用インターフェースを提供します。 サーバーへの接続に成功すると、コンソールはサーバーによって分析されたさまざまなデータをトレンドグラフとデータビューの形式で表示します。 ネットワーク管理者は、コンソールを介してさまざまなブランチネットワークに配置されたサーバーに接続し、サーバーから送信および返されるデータを表示することで、ブランチネットワークのネットワーク通信ステータスを理解および習得できます。

分析センター

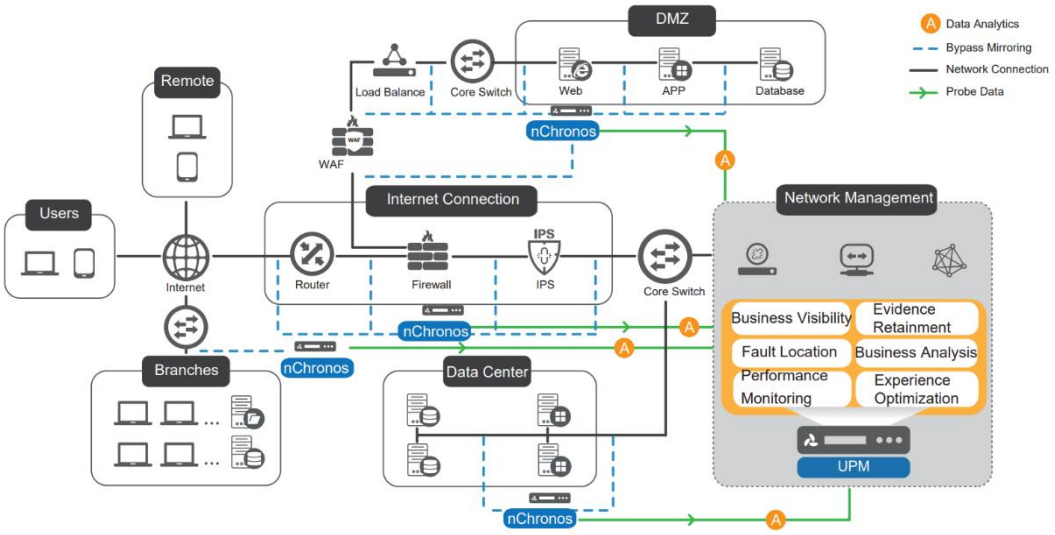
分散分析センターは、統合された集中型の監視および分析プラットフォー

ムを提供します。サーバーとの定期的なデータ対話を通じて、各ブランチネットワークに配置されたサーバーの通信データが収集およびソートされ、サーバー/ネットワークリンクの単位で表示されます。主に各サーバー下の各ネットワークリンクのトラフィック統計結果を提供し、自動アラーム機能を提供し、長期トレンド統計や自動レポートなどの機能を提供します。

1.1 製品の展開

製品の一般的な展開を次の図に示します。

図 2.1 製品展開の概略図



サーバー

製品全体の中核として、サーバーはネットワーク通信データのリアルタイムの収集と分析に使用されます。 サーバーは、ネットワーク遡及分析システムの展開の焦点です。展開が正しくない場合、必要なデータが収集されず、製品の通常の使用に影響します。 重要なリンクの通信データを収集および分析するために、監視および分析が必要なネットワークリンクにサーバーを展開することをお勧めします。

コンソール

コンソールとサーバーは B/S アーキテクチャを採用し、ブラウザでサーバ

ーを統一的に管理でき、接続されたサーバーに対するネットワークトラフィック分析をサポートする。

分析センター

分析センターとサーバーは B/S（ブラウザ/サーバー）アーキテクチャを採用し、定期的なハートビートを介してデータを交換し、グローバルなネットワーク通信の監視を実現します。 分析センターのネットワーク通信全体をグローバルに監視し、ローカルネットワークであれ、別の場所にあるブランチネットワークであれ、包括的なネットワーク通信監視を実現できます。

1.2 リスニングインターフェイス

Colasoft nChronos で使用される合法的リスニングインターフェイスを次の表に示します:

表 0.1 合法的リスニングインターフェイス

インターフェイス	説明
22	SSH リモートアクセスインターフェイスリモートアクセスインターフェイスを介して nChronos サーバーにログインします。 ユーザーは、デフォルトで有効になっているサーバーWeb 構成ページから SSH リモートアクセスインターフェイスを有効または無効にできます。
3000	遡及コンソールは、遡及サーバーのインタフェースに接続します。コンソールとサーバー間のデータ転送に使用します。
3001	遡及コンソールは、遡及サーバーのインタフェースに接続します。コンソールとサーバ間のデータ SSL 暗号化転送用。
443	nChronos サーバーの Web アクセスインターフェイスをバックトラックします。このインターフェイスは常に有効にする必要があります。
8080	nChronos サーバーAPI 送信インターフェース。デフォルトでは無効になっています。 API のニーズに使用する場合は、nChronos サーバーのファイアウォールでこのインターフェイスを開きます。
8081	Web コンソールはインタフェースにアクセスします。

2 インストールとアンインストール

この項では、サーバーとコンソールのインストール手順について説明します。

2.1 サーバー

サーバーは、工場出荷前にソフトウェアのインストールとハードウェアの構成を完了しており、ユーザーはケーブルを介して実際のネットワーク環境にサーバーを展開するだけで済みます。

2.1.1 ハードウェアパネル

サーバーにはさまざまなモデルがあります。サーバーのモデルが異なれば、ハードウェアパネルとネットワークインターフェイスもわずかに異なります。ハードウェアパネルの詳細図については、サーバーの背面パネルにあるマップを参照してください。

2.1.2 ケーブル接続

電源コード

電源モジュールはサーバーに電源を供給するために使用され、サーバーは 2 つの電源モジュールを提供します。

電源コードの接続手順は次のとおりです:

1.パッケージを開封し、AC 電源コードを取り出します。

2.AC 電源コードを電源コネクタに接続します。

3.AC 電源コードプラグをコンセントに挿入します。

管理ポートの構成

管理ポートは、サーバーのパラメーターを構成するために使用されます。サーバーが工場出荷時に、サーバーの「管理ポート」ページの eh0 に対応する eh0 の IP のみが構成されます。 eh0 の IP アドレスはデフォルトで 192.168.5.160 です。

管理ポートを構成するには、次の 2 つの方法があります:

- 設定方法 1:

1. サーバーの電源がオンになっていて、外部モニターが接続されています。
2. サーバーを起動してログインします。デフォルトのユーザー名は root です。
3. 任意のテキストエディタ（nano や vi など）を使用して、ディレクトリ/etc / sysconfig/network-scripts にある構成ファイル ifcfg-eth0 を開きます。
4. 実際のネットワーク環境に応じて、以下のフィールドを変更または追加します。「＃」の後に説明が続きます。説明は、構成ファイルに追加する必要はありません。
   ONBOOT =” yes” ＃yes は、起動後にネットワークインターフェイスが自動的に有効になることを意味します。

IPADDR = 192.168.5.177＃インターフェースの IP アドレス。実際の状況に応じて入力します。
NETMASK = 255.255.255.0＃サブネットマスク、実際の状況に応じて入力します。
GATAWAY = 192.168.5.1＃ゲートウェイアドレス、実際の状況に応じて入力します。

DNS1 = 8.8.8.8 #DNS サーバーアドレス、実際の状況に応じて入力します。デフォルトにすることができます。

5. コマンド: 「servicenetworkrestart」を実行してネットワークサービスを再起動し、新しい構成を有効にします。
6. eh0 の IP アドレスを設定すると、モニターを切断できます。 PC を使用してブラウザに eh0 の IP アドレスを入力し、サーバーの Web 構成インターフェイスにログインして、サーバーを構成します。

設定方法 2:

1.「eh0」を PC に接続し、PC の IP アドレスを 192.168.5.10 に変更します。

2. PC のブラウザに「192.168.5.160」と入力して、サーバーの Web ログインインターフェイスに入ります。

3.ログイン名: admin を入力し、[ログイン]をクリックしてサーバーの Web 構成インターフェイスに入ります。

4.左側のナビゲーションで[インターフェイス管理]をクリックして、[インターフェイス管理]ページに入ります。 [編集]をクリックして[インターフェイスの編集]ページに入り、eh0 の IP アドレスを設定します。

5. eh0 の IP アドレス設定が完了したら、サーバーと PC 間のネットワークケーブルを抜きます。ユーザーは、ブラウザーに eh0 の IP アドレスを入力してサーバーを構成することにより、サーバーWeb 構成インターフェイスにログインできます。

収集ポートの構成

収集ポートは通信データの収集に使用され、具体的な配置方法に基づい

て、スイッチのミラーポートまたはシャントを対応する収集ポートに接続すればよい。

2.1.3 サーバーポート管理

コンソールとサーバー間のデータの正常な送信を保証し、サーバーをリモートで管理するために、サーバーはいくつかのポートを開いています。各パラメーターの具体的な説明は次のとおりです:

表 3.1 ポートリスト

ポート番号	機能
443	ブラウザのアクセスポート。これを介して、ブラウザはサーバーの Web 設定ページに入ることができます。
8081	コンソールアクセスポート。 コンソールは、データ送信のためにこのポートを介してサーバーに接続します。

2.1.4 スイッチポートミラーリングの構成

サーバーは通常、4 つ以上のネットワーク取得インターフェイスを提供します。さまざまなネットワーク環境とユーザーのニーズに応じて、スプリッターまたはポートミラーリングを使用してネットワーク通信データを収集できます。 データ収集にポートミラーリングを使用する場合は、最初にスイッチでポートミラーリングを実行し、監視対象のネットワークリンクトラフィックをサーバーのデータ収集ポートにミラーリングする必要があります。

同じメーカーのスイッチの場合、ポートミラーリングの構成手順は異なります。特定の構成操作については、スイッチに付属のドキュメントを参照してください。 当社の公式ウェブサイトでは、一般的なスイッチのポートミラーリングの構成方法を提供しています:

http：//www.colasoft.com.cn/support/port_mirroring.php にアクセスしてください。

例として、CiscoCatalyst4000 シリーズスイッチでのポートミラーリングの

設定を取り上げます。

スイッチのアップリンクポートが f5/48 の場合、このポートはルーターへの接続に使用されます。 したがって、ネットワーク全体のデータ通信をキャプチャするには、ポートをミラーリングされたポート（つまり、監視対象ポート）として使用し、ポートのデータを指定された監視ポートにコピーする必要があります。ここでは、f5 を使用します。例として/1、つまりミラーポート（監視ポート）として f5/1。 次に、サーバーの任意の収集ポートをポート f5/1 に接続します。

上記の要件に基づいて、ポートミラーリングの構成は次のようになります:

ミラーリングされたポートを構成します:

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

ミラーポートを構成します:

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

構成が完了すると、構成を表示できます:

Switch# show monitor session 1

説明:

ネットワーク展開でスプリッターを使用する場合、スプリッターの構成については、スプリッターに付属のドキュメントを参照してください。

2.2 コンソール

リファレンス Colasoft nChronos 製品インストールガイド

次の表に、コンソールのお勧め構成を示します。

表 3.2 お勧めコンソール構成

ンジケーター項目	最小構成
ブラウザ	Google　Chrome50 以降をお勧める Firefox46 以降
画面の解像度	お勧め：1920×1200 最小：1280×800

3 nChronos サーバ構成

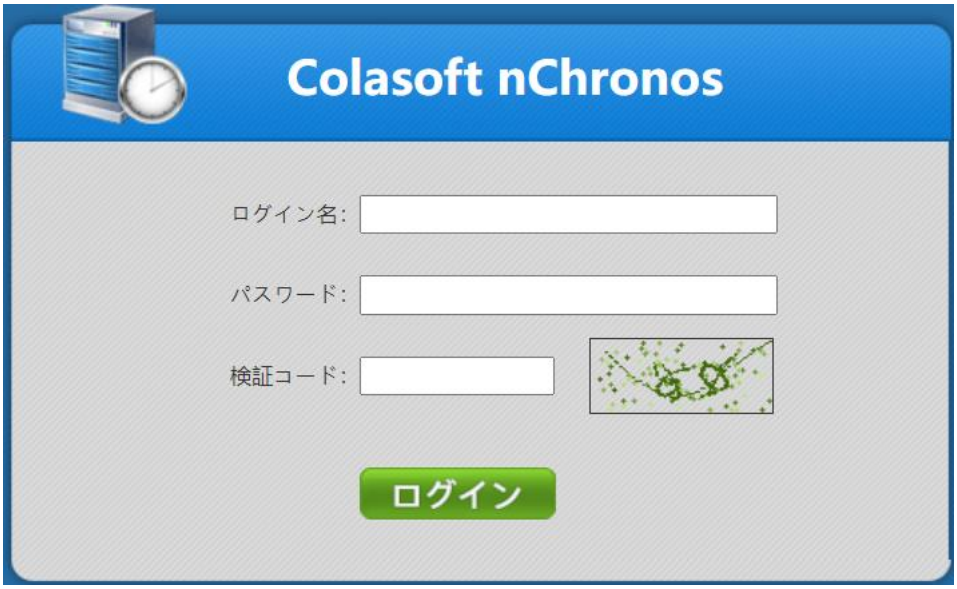
このセクションでは、nChronos で一般的に使用される構成操作について説明します。

3.1 サーバ構成インタフェースへ

サーバーの構成操作はすべて、サーバーの Web 構成インターフェースで実行されます。サーバーの Web 構成インターフェースに入る手順は次のとおりです:

1. PC のブラウザを開き、アドレスバーに設定されている管理設定ポート 1 の IP アドレスを入力し、Enter キーを押すと、下図のように「ユーザーログイン」インターフェースが表示されます:

図 4.1 ユーザーログインインターフェイス



2. ユーザー名、パスワード、認証コードを入力し、「ログイン」をクリックすると、サーバーの Web 構成インタフェースに入ります

3.2 サーバー管理

以下に示すように、サーバー管理には、SSH リモートアクセスの有効化/無

効化、システム監視ログ送信の有効化/無効化、切り捨てられたパケット分析の有効化/無効化、更新、構成のエクスポート、構成のインポート、システムのリセット、システムの再起動、サーバーの再起動、およびサーバーのシャットダウンが含まれます:

図 4.2 サーバー管理インターフェース

3.2.1 SSH リモートアクセスを有効/無効にする

ユーザーは、バックトラッキングサーバーのリモートアクセス機能を有効/無効にできます。 リモートアクセスが有効になっている場合、システムのデフォルトのリモートアクセスポートは 22 であり、変更できません。

3.2.2 システム監視ログ送信の有効化/無効化

ユーザーは、バックトラッキングサーバーのシステム監視ログの送信を有効/無効にできます。 有効にすると、「4.12.2 アラーム送信」で syslog パラメータを設定した後にのみログ情報を正しく送信できます。

3.2.3 切り捨てられたパケット分析の有効化/無効化

ユーザーは、切り捨てパケット分析機能をオン/オフにできます。オープン状態では、コンソールは統計的にパケットをトランケートする時間が大きい場合、トランケート前のパケットで行います。オフの状態では、コンソ

ールはデータをトランケートする時間を統計し、トランケート後のパケットで統計します。

3.2.4 システムアラームのオン/オフ

ユーザーは、バックトラッキングサーバーのシステムアラートをオン/オフにできます。 オープン状態では、アクセス許可アラーム、パスワードエラー番号超過アラーム、センター接続アラーム、異常システム再起動アラーム、キャプチャカードパフォーマンスアラーム、分析パフォーマンスアラーム、トラフィックなしアラームをサポートします。 同時に、アラームメール送信と SYSLOG 送信ステータスの設定をサポートします。 以下に示すように、[設定の送信]をクリックします。

図 4.3 送信構成インターフェース

3.2.5 リフレッシュ

[リフレッシュ]ボタンをクリックして、サーバーの実行時間、開始時間、CPU 使用率、合計メモリ、使用可能なメモリ、メモリ使用量、ディスク構成容量、残りのディスク容量、ディスク容量占有率などのサーバーの実行情報を表示します。

3.2.6 構成のエクスポート

サーバーのすべての構成情報をエクスポートします。エクスポートされた構成ファイルは「*.dat」形式です。 サーバーの構成が完了したら、[構成のエクスポート]ボタンをクリックして、サーバーの構成情報をバックアップできます。

3.2.7 インポート構成

サーバーの構成情報をインポートします。サーバーを再インストールした後、[構成のインポート]ボタンをクリックして、以前にバックアップした構成情報をサーバーに再インポートできます。

説明:

構成をインポートすると、サーバーのすべてのデータがクリアされ、サーバーが再起動します。注意して使用してください。

3.2.8 システムのリセット

システムをリセットすると、構成データに加えて、統計、アラートログ、パケットなどのデータがクリアされます。

3.2.9 システムの再起動

履歴データを削除せずに、Colasoft nChronos を再起動します

3.2.10 サーバーの再起動

サーバーを再起動すると、コンソールとサーバー間の接続が一時的に切断されます。サーバーの再起動後、コンソールでサーバーを再接続する必要があります。

3.2.11 サーバーのシャットダウン

サーバーをシャットダウンすると、コンソールがサーバーから切断され、サーバーが再起動されるまでコンソールはサーバーに接続できなくなります。

3.3 ストレージスペース管理

ストレージスペース管理は、主にディスクスペースと分析スペースの設定に使用されます。

説明:

- サーバーのディスクスペースは拡張をサポートします。ディスクスペースの構成容量が小から大に増加する場合、構成されたストレージパーティションと既存のデータは影響を受けません。ディスクスペースの構成容量が大から小に増加する場合、すべてサーバー内のデータは消去されます。注意して続行してください。
- ディスク容量の構成容量を減らす場合は、まずストレージ領域の構成容量を解放する必要があります。

ディスク容量の設定

ユーザーは必要に応じてディスク容量を設定できます。構成中、各デバイスの最小構成容量は 100GB です。デバイスの構成容量が 100GB 未満の場合、構成は失敗します。 構成されたエクスポートデータ容量とストレージデータ容量の合計は、構成可能な容量を超えることはできません。

分析スペースの設定

分析スペースは、サーバーのストレージ領域とエクスポートされたデータが占める容量を設定するために使用されます。 バケットに保存されるデータには、統計、パケット、トランザクションログ、およびアラートログが

含まれます。 その中で、統計データは、さまざまなタイムバケットのストレージ比率をさらに構成できます。

リンクを追加するときは、リンクが属するストレージ領域を指定する必要があります。ストレージ領域には複数のリンクを含めることができます。サーバーのデータは記憶域に基づいて循環しますので、リンクが属する記憶域を指定する場合は、同じ記憶域に同じトラフィックサイズのリンクを割り当てることをお勧めします。

エクスポートデータは、エクスポートされたリンク統計、アプリケーション監視データ、およびトランザクション処理データが占めるストレージスペースを設定するために使用されます。

3.4 インターフェース管理

インターフェイスタイプには、設定インターフェイスと取得インターフェイスが含まれます。

3.4.1 インターフェースの構成

サーバーとコンソールを接続するために構成インターフェースを使用します。ユーザーは、必要に応じて、管理インターフェースの IP アドレス、IP マスク、ゲートウェイアドレス、および DNS サーバーアドレスを設定できます。 コンソールにサーバーを追加する場合、サーバーを正常に追加できるように、入力 IP アドレスは管理インターフェイスの IP アドレスと同じである必要があります。

システムのデフォルトの管理ポートは eh0 です。

3.4.2 キャプチャインターフェイス

キャプチャインターフェイスは、ネットワーク内のパケットをキャプチャするために使用されます。 インターフェイスがコレクションインターフェイスとして設定され、ネットワークリンクに割り当てられている場合、インターフェイスのタイプは変更できません。 インターフェイスのタイプは、ネットワークリンクが削除された場合にのみ変更できます。

仮想インターフェイスの設定

ユーザーは必要に応じて収集ポートに仮想インターフェイスを追加でき、追加された仮想インターフェイスは収集ポートにバインドされます。 仮想インターフェイスには、VLAN、ISL VLAN、MPLS VPN、VXLAN、ネットワークセグメント、Netflow、GRE、および物理アドレスの 8 種類があります。 収集ポートに追加される仮想インターフェイスのタイプは同じである必要があります。

仮想インターフェイスを追加する手順は次のとおりです:

1. 仮想インターフェイスのタイプを選択します。VLAN、ISL VLAN、MPLS VPN、VXLAN、ネットワークセグメント、Netflow、GRE、および物理アドレスのいずれかを選択できます。
2. [仮想インターフェイスの追加]ボタンをクリックすると、[追加]ダイアログボックスが表示され、対応する情報を入力します。 VLAN、ISL VLAN、MPLS VPN、VXLAN、GRE、物理アドレス仮想インターフェイスを設定する場合、このインターフェイスでネットワークセグメント情報を設定できます。 NETFLOW 仮想インターフェースを設定する場合、サーバーに Netflow データを送信するルーターIP、フローバージョン、および Netflow エクスポートポートを設定できます。
3. [OK]ボタンをクリックすると、仮想インターフェイスが仮想インターフェイスリストに正常に追加されたことがわかります。

説明

仮想インターフェイスのタイプを変更する場合は、最初に追加された仮想インターフェイスを削除する必要があります。

伝送媒体の選択

システムは、すべての取得インターフェースの伝送媒体が ETHERNET を使用するようにデフォルト設定されており、ユーザーは実際の状況に応じて PPP に切り替えることができます。

IP レベルの特定

ユーザーはシステムの IP レベルを設定してインターフェースデータを識別でき、システムはデフォルトで最初のレベルになります。 ユーザーはそれ

を変更することができ、最大認識レベルは第 4 レベルに設定することができます。 実際のデータパケットの IP レベルが設定レベルよりも低い場合、実際のデータパケットの最も内側の IP によって識別されます。

3.4.3 管理インターフェースの IP アドレスの設定

管理インターフェースは、サーバーとコンソールを接続するために使用されます。ユーザーは、必要に応じて、管理インターフェースの IP アドレス、IP マスク、ゲートウェイアドレス、および DNS サーバーアドレスを設定できます。 コンソールにサーバーを追加する場合、サーバーを正常に追加できるように、入力 IP アドレスは管理インターフェイスの IP アドレスと同じである必要があります。

システムのデフォルトの管理ポートは eh0 です。

3.5 ネットワークリンク管理

ネットワークリンク管理には、リンクの追加、リンクの変更、リンクの削除、リンクステータスの変更、およびリンク構成のインポート/エクスポートが含まれます。

3.5.1 リンクの追加

ネットワークリンクがサーバーに追加された場合にのみ、コンソールでネットワークリンクのリアルタイム監視と遡及的分析を実行できます。 nChronos でサポートされているリンクには、リアルタイムリンクと再生リンクが含まれます。 リアルタイムリンクと再生リンクを追加する手順は次のとおりです

1. 次の図に示すように、[新しいリンク]をクリックして[新しいリンク]ページに入ります

図 4.4 新しいリンクページ

2. ネットワークリンク名を設定し、ネットワークリンクタイプを選択します。 リンクタイプには、標準タップ、スイッチ単方向トラフィックミラーリング、集約タップ、スイッチ双方向トラフィックミラーリング、Netflow 双方向トラフィック、エージェント、および集約分析が含まれます。
3. リンクのストレージ領域を選択します。複数のリンクで同じストレージ領域を選択できます。 Netflow 双方向トラフィックタイプのリンクは、Netflow タイプのストレージパーティションのみを選択できます。 集約分析リンクによって選択されるストレージ領域は、他のリンクのストレージ領域から独立している必要があります。
4. 着信ネットワークトラフィックと発信ネットワークトラフィックをキャプチャするための収集ポートを設定します。
5. リンクタイプがアグリゲーションスプリッタ、スイッチ双方向トラフィックミラーリング、データパケット再生、エージェントの場合、インバウンドとアウトバウンドのネットワークセグメントの情報を設定する必要があります。
6. リンクタイプが Netflow 双方向トラフィックタイプの場合、インバウンドおよびアウトバウンドネットワークキャプチャインターフェイスは、物理インターフェイスまたは Netfow 仮想インターフェイスのいずれかになり

ます。 インターフェイスタイプは互いに独立しており、同時に選択することはできません。

7. Netflow リンクデバイスキャプチャインターフェイスが物理インターフェイスの場合、ユーザーはリンクのデバイス情報を設定する必要があります
8. スイッチのタイムスタンプ分析を有効にするかどうかを設定します。現在、現在、ARISTA、VSS Monitoring、Gigamon、HUAWEI スイッチをサポートしています。。
9. データを CSV 形式で自動的にエクスポートするかどうかを設定します。エクスポートされるデータには、リンク統計、アプリケーション監視データ、トランザクション処理データが含まれます。 [設定]をクリックして、エクスポートする統計とコンテンツを設定することもできます。
   統計のデフォルトのエクスポートディレクトリは cd/data/ colasoft-csrass-export です。
10. ミリ秒レベルのトラフィック統計を有効にするかどうかを設定します
11. リンク上で統計的に識別する必要がある IP レベルを設定します
12. 仮想ネットワーク統計を設定するときに ID の複数のレイヤーがある場合、統計のレベルが必要です。
13. 着信ネットワーク帯域幅、発信ネットワーク帯域幅、および合計帯域幅を設定します。
14. 一般ユーザーに対してこのリンクの操作権限を設定します。 ここで、リンクの操作権限を設定できるのは、「リンク認証」の一般ユーザーのみです。
15. [OK]をクリックして、ネットワークリンクの追加を終了します。

再生リンクを追加する手順は次のとおりです:

1. [新しいリンク]をクリックして[リンク構成]ページに入ります。インターフェイスは、リアルタイムリンクとまったく同じです。
2. ネットワークリンク名を設定し、ネットワークリンクタイプを「パケット再生」として選択します。 パケットタイプを選択すると、設定インターフェイスは次のようになります。

図 4.5 再生リンクページ

3. 「新しいストレージエリア」を選択して、データパケットを再生するためのストレージスペースを設定します。 各再生リンクのストレージ領域は個別に構成する必要があり、複数のリンクが同じストレージ領域を共有することはできません。
4. バックトラッキングサーバーまたはローカルアップロードを含む、再生データパケットのソースを設定します。 再生用に選択されたデータパケットのサイズは 1G を超えることはできません。
5. ネットワークセグメントの情報を出し入れします
6. スイッチのタイムスタンプ分析を有効にするかどうかを設定します。現在、ARISTA、VSS Monitoring、Gigamon、HUAWEI スイッチをサポートしています。

7. データを CSV 形式で自動的にエクスポートするかどうかを設定します。エクスポートされるデータには、リンク統計、アプリケーション監視データ、トランザクション処理データが含まれます。 [設定]をクリックして、エクスポートする統計とコンテンツを設定することもできます。

   統計のデフォルトのエクスポートディレクトリは cd/data/ colasoft-csrass-export です。

8. ミリ秒レベルのトラフィック統計を有効にするかどうかを設定します。
9. このリンクで統計的に識別する必要がある IP レベルを設定します。
10. 仮想ネットワーク統計を設定するときに ID のレイヤーが複数ある場合は、カウントするレベルが必要です。
11. 着信ネットワーク帯域幅、発信ネットワーク帯域幅、および合計帯域幅を設定します。
12. 一般ユーザーのリンクの操作権限を設定します。 ここで、リンクの操作権限を設定できるのは、「リンク認証」の一般ユーザーのみです。
13. [OK]をクリックして、ネットワークリンクの追加を完了します。

3.5.2 リンクの編集

[編集]ボタンは、追加されたネットワークリンクを変更するために使用されます。これには、ネットワークリンクの名前、トラフィックキャプチャ方法、トラフィック収集ポート、インバウンドおよびアウトバウンドネットワークセグメントのアドレス、インバウンドおよびアウトバウンドネットワーク帯域幅の変更が含まれます。

3.5.3 リンクの削除

「削除」ボタンは、追加されたネットワークリンクを削除するために使用されます。

3.5.4 リンクステータスの変更

ネットワークリンクのステータスには、「実行中」と「停止」が含まれます。ネットワークリンクのステータスが「実行中」の場合、リンクを介して送信されたデータがバックトラッキング分析システムによってキャプチャされていることを意味します。ステータスが「停止しました」とは、リンクデータの取得が停止したことを意味します。

ユーザーは、サーバーの Web 構成インターフェースを介してリンクステータスを変更できます。 左側のナビゲーションツリーの「リンク設定」をクリックして「リンク情報設定」ページに入り、ネットワークリンクの「操

作」欄の「実行」または「停止」ボタンをクリックしてリンク状態を変更します。

3.6 エージェント構成

トラフィック転送エージェントはサードパーティのサーバーにインストールされ、サーバーを通過するトラフィックをバックトラッキングサーバーによって指定されたキャプチャカードに転送する役割を果たします。 エージェントは、Alibaba Cloud、Qingyun などの標準クラウドをサポートします。

エージェント設定は、主に転送トラフィックのパケットトリミングとパケットフィルタリングを設定することです。

- パケットトリミング：データパケットを転送するときのパケットトリミングの長さを設定するために使用されます。 パケットトリミング設定が有効になっている場合、パケット転送時にトリミング長のみが転送されます。トリミング長は 64 バイト～65535 バイトの範囲で設定できます。
- パケットフィルタリング：データパケットのフィルタリングルールを設定するために使用され、フィルタリングルールを満たすデータパケットのみが転送されます。 パケットフィルター条件は、IP アドレスとポートに対するフィルター処理をサポートし、複数のフィルター条件や関係の組み合わせもサポートします。

エージェントがバックトラッキングサーバーとの接続を確立するとき、バックトラッキングサーバーにアクティブに接続するのはエージェントです。 したがって、エージェントの構成ファイルでバックトラッキングサーバーの IP アドレスとポートを構成する必要があります。具体的な説明は次のとおりです:

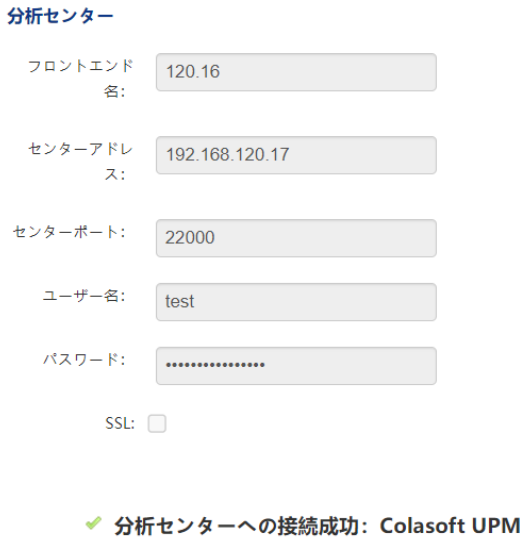
- エージェント名：エージェントリストに表示されるエージェントの名前を設定するために使用されます。
- エージェントトラフィック転送ネットワークカード：エージェントのトラフィックが転送されるネットワークカードを設定するために使用されます。

- サーバーの IP アドレス：エージェントが接続するサーバーの IP アドレスを設定するために使用されます。
- サーバーポート：エージェントとバックトラッキングサーバー間の通信用のポートを設定するために使用されます。デフォルトは 5111 です。
- サーバートラフィック受信ネットワークカードのバックトラック：エージェントによって転送されたトラフィックを受信するネットワークカードを設定するために使用されます。

3.7 分析センター

分析センターページを使用して、フロントエンド名、分析センターの IP アドレス、ポート、ユーザー名、パスワード、暗号化転送の有無を設定します。次の図に示すように、分析センター設定ページ。

図 4.6 分析センター接続ページ



分析センター設定ページでは、各設定項目の詳細を次の表に示します。

表 4.1 分析センターの構成

アイテムの設定	具体的な説明
フロントエンド名	フロントエンド、つまり現在の nChronos サーバの名前を設定するために使用されます。
センタアドレス	分析センターの IP アドレスを設定するために使用されます。
中央ポート	分析センターを設定するためのポートです。デフォルトは 22000 です。

アイテムの設定	具体的な説明
ユーザー名	分析センターに接続するためのユーザー名を設定します。このユーザー名はまず分析センターで作成する必要があります。
パスワード	3.7 分析センターユーザーを接続するためのパスワードを設定します。このパスワードは入力したユーザー名と一致する必要があり、現在の 3.7 分析センターで作成する必要があります。
SSL	SSL 暗号化伝送を使用するかどうかを設定するために使用され、システムのデフォルトでは SSL 暗号化は有効になっていません。SSL 暗号化が有効な場合、中央ポートはデフォルトで 22100 になります。

3.8 事前定義ライブラリ

事前定義ライブラリでは、次の図に示すように、システムアプリケーションライブラリを管理するために使用されます。システムはデフォルトでシステムアプリケーションライブラリファイルを持っています:

図 4.7 事前定義ライブラリ

「ライブラリファイル更新」ボタンをクリックして、ファイル選択ダイアログボックスをポップアップし、ユーザーは新しいライブラリファイルを選択して以前のライブラリファイルを上書きすることができます。

次の表に示すように、事前定義されたライブラリ構成インタフェースのパ

ラメータの説明。

表 4.2 事前定義ライブラリ表

アイテムの設定	具体的な説明
ライブラリ名	ライブラリファイルの名前を表示します。
種類	ライブラリファイルのタイプを表示します。現在はアプリケーションとフィーチャーの 2 種類が含まれています。
ライブラリバージョン	ライブラリファイルのバージョン情報を表示します。
インポート時間	ライブラリファイルのインポート時間を表示します。
合計数	ライブラリファイルで定義されている適用数を表示します。
操作	ライブラリファイルの編集操作に使用します。 「編集」ボタンをクリックすると、ライブラリファイル内の詳細を表示でき、ライブラリファイル内のアプリケーションを有効化および無効化できます。システムアプリケーションライブラリを表示すると、システム定義アプリケーションの番号、名前、説明を表示できます。ライブラリファイルを無効に設定した場合、ライブラリファイルで定義されているアプリケーションまたはフィーチャはシステムに認識されません。

3.9 サードパーティの拡張

サードパーティ拡張は、次の図に示すように、SDL トランザクションのカスタムトランザクションフィールド拡張に使用されます。

図 4.8 サードパーティ拡張

「インポート」ボタンをクリックすると、ファイル選択ダイアログがポップアップ表示され、ユーザーはサードパーティ製拡張 Lua スクリプトを選択できます。

次の表に示すように、サードパーティ拡張構成インタフェースのパラメータの説明を示します。

表 4.3 第三者による拡張構成

アイテムの設定	具体的な説明
ファイル名	スクリプト・ファイルの名前を表示します。
種類	スクリプトファイルのタイプを表示します。現在は Lua スクリプトのみがサポートされています。
作成日	スクリプト・ファイルのインポート日を表示します。
有効化時間	スクリプト・ファイルの有効化時間を表示します。
ステータス	スクリプト・ファイルの有効化ステータスを表示します。
ドキュメント名	スクリプト・ファイルで返されたドキュメント名が表示されます。
フィールド情報	スクリプトファイル内のカスタムフィールド情報を表示します。

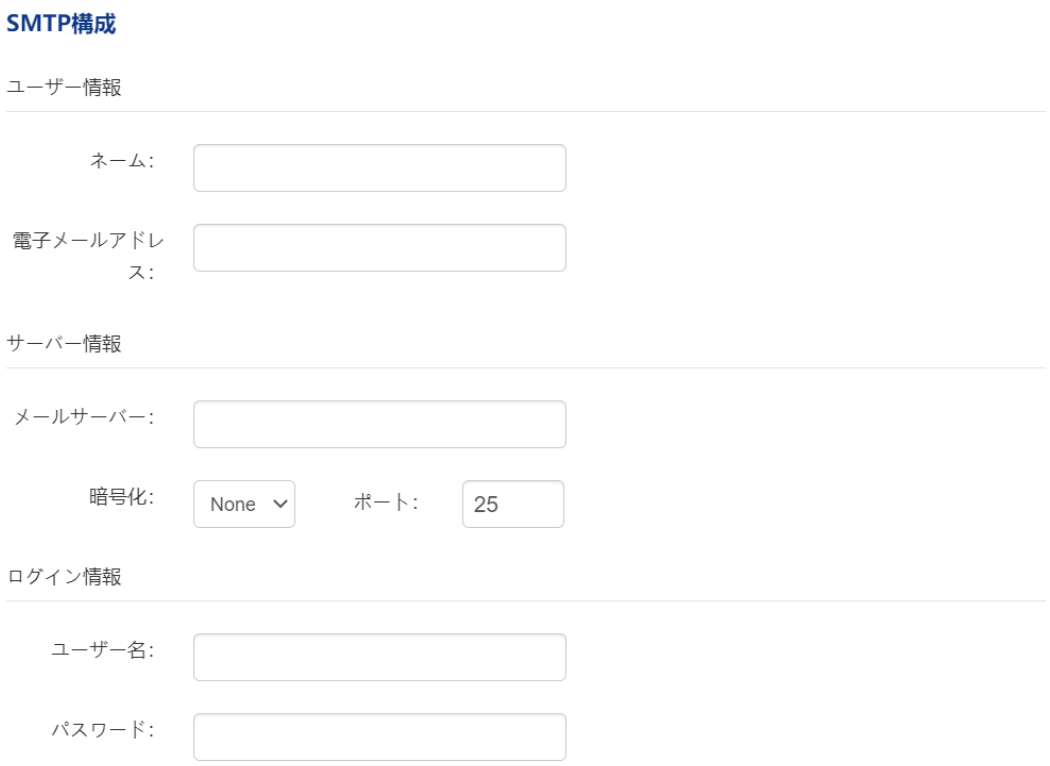
3.10 メッセージ通知の構成

メッセージ通知の設定には、SMTP 設定、アラーム送信、レポート送信が含まれます。ユーザーが正しく設定すると、システムは自動的にトリガーされたアラームと定期的に生成されたレポートを指定された受信者のメールボックスに送信します。

3.10.1 SMTP 構成

SMTP サーバーは、SMTP プロトコルに準拠し、送信メールを送信または転送するために使用される送信メールサーバーです。 SMTP サーバーが正しく設定されている場合にのみ、システムは指定された受信者のメールボックスにアラートとレポートを送信できます。 次の図に、SMTP 構成ページを示します。

図 4.9 SMTP 構成



各設定項目の具体的な説明は以下のとおりです

表 4.4SMTP 構成

設定項目	具体的な説明
名前	送信者の名前を設定するために使用されます。
電子メールアドレス	送信者のメールアドレスを設定するために使用されます。
メールサーバー	メールサーバーアドレスを設定するために使用されます。

設定項目	具体的な説明
暗号化	暗号化方式の設定に使用します。システムでサポートされている暗号化方式には、TLS と SSL があります。
ポート	メールサーバーのポートを設定するために使用されます。暗号化が選択されていない場合、デフォルトのポートは 25 です。暗号化方法が SSL または TLS として選択されている場合、デフォルトのポートは 465 です。
ユーザー名	送信者の名前を設定するために使用されます。
パスワード	送信者のメールパスワードを設定するために使用します。

設定が完了したら、「テスト」ボタンをクリックして、SMTP サーバーの設定が正しいかどうかをテストできます。

3.10.2 アラーム送信

アラート送信]ページは、電子メールの受信者、SYSLOG サーバー、およびアラートを送信する間隔を設定するために使用されます。 アラート送信設定ページを以下に示します。

図 3.1 アラートの送信

メール送信

メール送信は、アラートメールの件名と受信者アドレスを設定するために使用されます。各設定項目の具体的な説明は次のとおりです:

表 4.5 電子メールの送信

設定項目	具体的な説明
メールの件名	アラートメールの件名を設定するために使用されます。
受信者アドレス	アラートメールの受信者アドレスを設定するために使用されます。複数の受信者アドレスは、キャリッジリターンとラインフィードで区切られます。 SMTP サーバー情報を設定しないと、受信者アドレスを設定できません。
時間間隔	アラーム情報の送信頻度を設定するために使用します。

設定項目	具体的な説明
	システムは、時間間隔内のすべてのアラーム情報を一度に電子メールの受信者に送信します。システムのデフォルトは 1 分です。

SYSLOG パラメーター

システムはアラートの SYSLOG 送信をサポートします。SYSLOG アドレスが正しく設定されると、システムは指定されたサーバーにアラートを送信します。

各パラメータ設定項目の詳細は以下のとおりです:

表 4.6 SYSLOG パラメーター

設定項目	具体的な説明
SYSLOG アドレス	SYSLOG サーバーのアドレスとポートを設定するために使用されます。各行は 1 つの SYSLOG サーバーとポート情報を構成します。複数の SYSLOG サーバーがある場合、それらはキャリッジリターンとラインフィードで区切られます。
コード	システムは UTF-8 および GBK エンコーディングをサポートしています。
毎秒インスタントプッシュ	SYSLOG の送信頻度を設定するために使用されます。1 秒あたりのインスタントプッシュは、システムが 1 秒ごとに SYSLOG を SYSLOG サーバーに即座に送信することを意味します。 説明 この構成は、アラート SYSLOG に対してのみ有効です。
時限プッシュ間隔	SYSLOG の送信頻度を設定するために使用されます。システムは、間隔内のすべての SYSLOG を一度に SYSLOG サーバーに送信します。デフォルトは 1 分です。

設定項目	具体的な説明
	説明： この設定は、アラーム SYSLOG に対してのみ有効であり、システムによって監視される SYSLOG システムは、1 分ごとに送信されるように固定されています。

3.10.3 レポート送信

レポート配信設定は、レポートテンプレートとレポートの受信者を設定するために使用されます。 次の図に、レポート送信設定ページを示します。

図 4.13 レポート送信

レポートテンプレート

レポートテンプレートの設定項目には、集計単位、集計表、会社ロゴなどがあります。設定が完了したら、「プレビュー」ボタンをクリックしてレポートをプレビューしてください。各設定項目の具体的な説明は次のとお

りです。

設定項目	具体的な説明
集計ユニット	レポートに表示されるユニット名を設定するために使用されます。
テーブル作成者	レポートに表示されるレポートプロデューサー情報を設定するために使用されます。
会社のロゴ	レポートに表示される会社のロゴを設定するために使用されます。
レポートヘッダーの背景設定	レポートヘッダーの背景色を設定するために使用されます。
タイトルプレフィックス	レポートのタイトルプレフィックスを設定するために使用されます。
レポートの生成時間を表示する	レポートにレポート生成時間を表示するかどうかを設定するために使用されます。
レポート形式	ユーザーは、レポートの送信形式を HTML または PDF に設定します。

表 4.7 レポートテンプレート

レポート受信者

レポート送信ユーザーはレポートの受信者アドレスを設定し、複数の受信者アドレスはキャリッジリターンとラインフィードで区切られます。
SMTP サーバー情報を設定しないと、受信者アドレスを設定できません。

3.11 ユーザー管理

ユーザー管理ページでは、ユーザーを追加、編集、削除、およびキックアウトできます。

ユーザーは、さまざまな権限に応じて、管理者、通常のユーザー、監査人に分けられます。対応する権限は次のとおりです:

- 管理者: システムのすべての権限を持っています。

- 通常のユーザー：管理者は、ユーザーを作成するときに権限を構成します。設定可能な権限には、「リンクモニター」、「リンク分析」、「アラームログクエリ」、「レポートビュー」、「データパッケージのダウンロード」が含まれます。
- 監査人：Web ページにログインして監査ログを表示することしかできず、他の権限はありません。

3.11.1 ユーザーの追加

次の図に示すように、管理者は[ユーザーの追加]をクリックして[新しいユーザー]ページに入ることができます：

図 4.12 ユーザーの追加

ユーザー認証方法

ユーザーを追加するとき、管理者はユーザーの認証方法を選択できます。現在、サーバーは、ローカル認証、LDAP 認証、Radius 認証、UPM 認証などの複数のユーザー認証方法をサポートしています。 UPM 認証は、ユーザーがローカルで作成される場合はオプションではなく、UPM センターによってのみ発行できます。

- ローカル認証：ユーザー名とパスワードはローカルで設定されます。ユーザーがログインすると、サーバーはユーザー名とパスワードに基づいて認証を実行します。

- LDAP 認証：LDAP 認証を選択した場合、ユーザー名は LDAP サーバーのユーザー名と同じである必要があります。同じでない場合、ユーザーはログインできません。 ユーザーがログインすると、システムは認証構成の LDAP 認証情報に基づく認証のために LDAP サーバーに接続します。

説明：

「認証構成」が適切に構成され、LDAP 認証が有効になっている場合にのみ、ユーザーは正常にログインできます。

- Radius 認証：Radius 認証を選択する場合、ユーザー名はドメインサーバーの名前と同じである必要があります。同じでない場合、ユーザーはログインできません。 ユーザーがログインすると、システムは「認証構成」の Radius 認証情報に従って認証を行うために Radius サーバーに接続します。

説明：

「認証構成」が適切に構成され、Radius 認証が有効になっている場合にのみ、ユーザーは正常にログインできます。

ユーザー権利

ユーザーの操作権限に応じて、システムはユーザーを管理者、一般ユーザー、監査人の 3 つのタイプに分類します。 新しいユーザーを作成するときに、これらのタイプのいずれかを選択できます。

- 管理者：権限を修正しました。権限を個別に構成する必要はありません。 システム全体を管理し、コンソールとサーバーのすべての操作および管理権限を持ちます。
- 監査人：権限を修正しました。権限を個別に構成する必要はありません。 Web ページにログインして監査ログを表示することのみが可能であり、他の権限はありません。
- 通常のユーザー：次の図に示すように、実際の状況に応じて権限を個別に構成する必要があります：

図 4.12 通常のユーザーの追加

一般ユーザーのアクセス許可を構成する場合、リンクまたはサーバーによる承認を選択できます。

✓ リンクで承認

リンクごとに異なる権限を個別に構成します。 リンクごとに 1 つずつ権限を設定する必要があります。

✓ サーバーによる承認

サーバー上の各リンクに同じ権限を構成します（後でリンクを追加する ことを含む）。

一般ユーザーの構成可能な権限には、「リンクモニター」、「リンク分 析」、「アラームログクエリ」、「レポートビュー」、および「データ パッケージのダウンロード」が含まれます。 対応する権限を持つユー ザーのみが、対応する機能を操作できます。 各権限設定モジュールの 機能は次のように分かれています。

✓ リンクモニタリング

コンソールは、各リンクのリアルタイム監視機能と、対応するリンクの下にあるアプリケーションのリアルタイム監視機能をサポートしています。

✓ リンク分析

コンソール：各リンクの遡及解析機能。

✓ アラームログクエリ
コンソールには、リンク/アプリケーションのリアルタイム監視用のアラームログ、リンク/アプリケーション/トランザクション分析用のアラーム統計ビュー、アラームログ用の統合ビューページなどの機能があります。

✓ データパッケージのダウンロード

コンソール：各統計ビューの「パケットダウンロード」機能。データパッケージのダウンロード長の設定は、データパッケージのダウンロード機能と連動しています。ユーザーがデータパッケージのダウンロード機能を持っている限り、データパッケージの長さをダウンロードできるように設定する必要があります。 リンクに保存されているデータの長さがダウンロードデータパケットの長さよりも長い場合は、ダウンロードデータパケットの長さが優先され、データパケットのダウンロードが実行されます。 保存されたデータパケットの長さがダウンロードされたデータパケットの長さよりも短い場合、ダウンロードは保存されたデータパケットの長さで実行されます。

3.11.2 ユーザーの編集

「編集」ボタンは、ユーザー名、ログインパスワード、備考、ユーザータイプ、権限など、追加されたユーザーの情報を変更するために使用されます。

ユーザーのステータスには、「オンライン」、「無効」、「オフライン」が含まれ、対応する具体的な意味は次のとおりです:

- オンライン：ユーザーがコンソールまたはブラウザーを介してサーバーに接続したことを示します。
- 無効：ユーザーが無効になっていて、コンソールでサーバーに接続できず、Web 経由でサーバーにログインできないことを示します。 非アクティブ化をキャンセルするには、[アカウントの非アクティブ化]の横にあるチェックボックスをオフにします。
- オフライン：ユーザーがコンソールとブラウザーを介してサーバーに接続していないことを示します。

3.11.3 ユーザーの削除

管理者は、自分以外のすべてのユーザーを削除できます。

3.11.4 ユーザーの追い出し

キックボタンは、ユーザーコンソールをサーバーから強制的に切断するために使用されます。 管理者タイプのユーザーは、すべてのオンラインユーザーを追い出すことができます。

ユーザーがすでにログインしているアカウントを使用して繰り返しログインすると、最初にログインしたユーザーが回線から切断され、ユーザーのコンソールとサーバー間の接続が切断されます。

3.12 認証構成

認証構成ページは、Radius および LDAP サーバー情報を設定するために使用されます。 Radius および LDAP 認証を使用するユーザーは、Radius および LDAP サーバー情報が正しく構成されている場合にのみ正しくログインできます。 以下に示すように、有効にできる Radius/LDAP 認証は 1 つだけです。

図 4.14 サードパーティの構成

構成が完了したら、[テスト]ボタンをクリックして、現在構成されているサーバー情報が正しいかどうかをテストできます。

3.13 セキュリティ設定

セキュリティ設定ページは、サーバーのセキュリティを確保し、不正アクセスを防止するために、ロックポリシーやクライアントアクセス制御ポリシーなど、システムのセキュリティポリシーを設定するために使用されます。

3.13.1 ロックポリシー

システムが提供するロックアウトポリシーには、IP ロックアウトしきい値、IP ロックアウト時間、およびリセットロックアウトカウントが含まれます。

IP ロックアウトしきい値

ユーザーロックアウトのしきい値のパラメーターの詳細な説明は次のとおりです:

- このパラメータは、IP アドレスのログイン試行の失敗回数を設定するために使用されます。 IP アドレスのログイン失敗回数が設定値に達すると、システムは IP アドレスをロックし、管理者が手動でロックを解除するか、IP ロック時間が経過するまで、サーバーはこの IP アドレスを介してサーバーにログインできません。
- このパラメーターの値の範囲は 1~999 の整数で、単位は時間です。

IP ロック時間

「IP ロック時間」パラメータの詳細な説明は次のとおりです:

- このパラメータは、IP アドレスがロックされてからの分数を設定するために使用されます。 このパラメーターは、IP ロックしきい値が設定されている場合にのみ意味があります。
- このパラメータの値は、リセットロックカウントで設定された値以上である必要があります。
- このパラメーターの値の範囲は、0 から 9999 までの整数（分単位）です。
- 0 に設定すると、サーバーが再起動されるまで IP アドレスがロックされることを意味します。

ロックカウントのリセット

「リセットロックカウント」パラメータの詳細な説明は次のとおりです。

- このパラメーターは、特定のログイン試行が失敗した後、失敗したログイン試行カウンターを 0 にリセットする時間間隔を設定するために使用されます。 このパラメーターは、IP ロックしきい値が設定されている場合にのみ意味があります。
- このパラメータの値は、IP ロック時間で設定された値以下である必要があります。
- このパラメーターの値の範囲は、1~9999 の整数（分単位）です。

IP を手動でロック解除する

ユーザーIP がロックされている場合、システムが自動的にロック解除される前に、管理者は[ロック解除]ボタンをクリックして、ポップアップロックされた IP リストの特定の IP アドレスを手動でロック解除できます。

3.13.2 パスワードポリシー

パスワード長設定

ユーザーパスワードの長さを設定するために使用されます。範囲は 8～20 文字です。

パスワード有効期間の設定

パスワードの有効期間を設定するために使用されます。有効期限が切れたら、システムを使用し続けるためにパスワードを変更する必要があります。0 は制限されていないことを示します。

履歴パスワードを記憶する数

システムが記憶している履歴パスワードの数を設定するために使用されます。パスワードを変更すると、最近使用したパスワードと重複することはできません。範囲 1～5 の整数を設定できます。

初回ログインパスワードの変更

ユーザーの初回ログイン時にパスワードを変更する必要があるかどうかを設定します。

3.13.3 タイムアウトポリシー

セッションのタイムアウト時間を設定するために使用されます。非監視ページの下で、ユーザーがタイムアウト時間に何の操作もしていない場合、システムは自動的にログインを終了します。システムを正常に使用するには、ユーザーが再ログインする必要があります。

パラメータは、0～9999 の範囲の整数をとります。

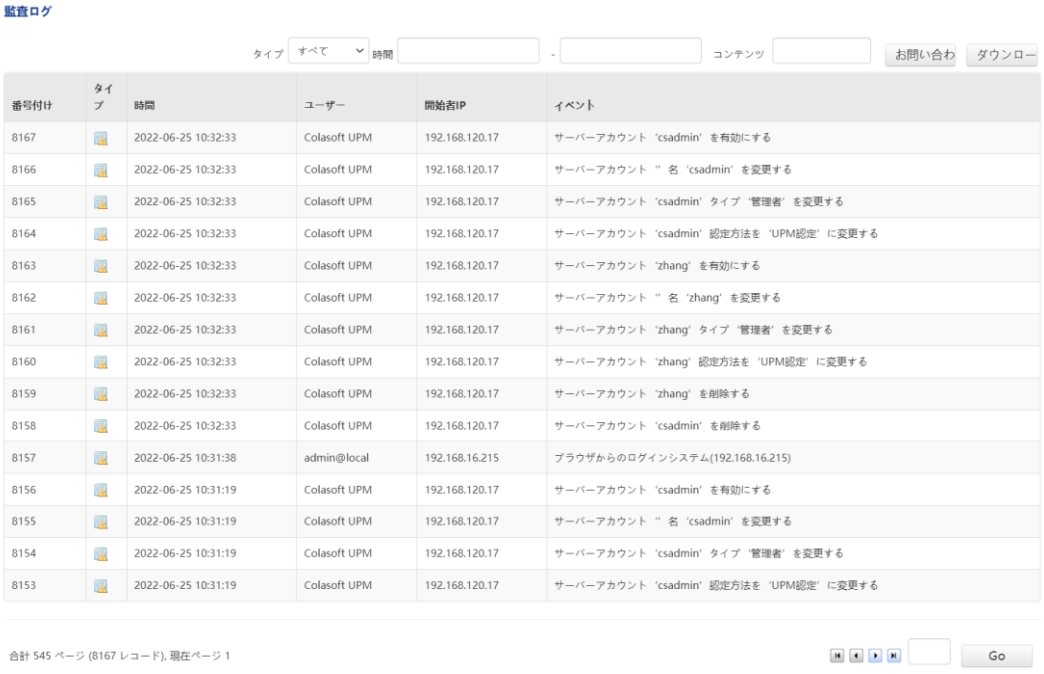
3.13.4 クライアントアクセス制御ポリシー

アクセス制御機能を有効にした後、ユーザーがコンソールと WEB を介してサーバーにログインすると、制御リスト内の IP のみがサーバーに正常にログインできます。

3.14 監査ログ

監査ログには、番号、タイプ、時間、ユーザー、イベント情報を含むバックトラック分析システムに対するユーザーの操作が記録されています。監査ログページを下図に示します。

図 4.15 監査ログ



説明:

監査ログを表示できるのは、管理者権限または監査人権限を持つユーザーのみです。

ログフィルタリング

ユーザーは、ログのタイプと時間範囲に基づいてログをフィルタリングできます。

- ログタイプによるフィルタリング
  ログ・タイプには情報、警告、エラーの 3 種類があり、ユーザーは必要なログ・タイプを選択でき、「フィルタ」ボタンをクリックすると、監査ログ・リストにはユーザーが選択したタイプのログのみが表示されます。
- 時間範囲による濾過
  ユーザーが監査ログを表示する必要がある開始時間と終了時間を選択し、「フィルタ」ボタンをクリックすると、監査ログリストにはその時間範囲内のログのみが表示されます。

ログ検索

システムはログコンテンツの検索をサポートしています。

ログのダウンロード

ユーザーは、フィルタリングされたログ情報をローカルにダウンロードして表示することもできます。「ダウンロード」ボタンをクリックしてファイル名とダウンロードパスを設定したら、「ダウンロード」をクリックして、ログ情報を指定したパスにダウンロードすることができます。ダウンロードファイルのフォーマットは「*.txt」です。

3.15 時刻同期

システム時刻を変更する必要がある場合は、手動変更と NTP（Network Time Protocol）同期の 2 つの方法を使用できます。

手動で変更する

説明:

システム時刻を手動で変更すると、すべての分析データがクリアされ、システムが再起動します。注意して行ってください。

システム時刻を手動で変更するには、タイムゾーンと日付を選択し、時刻を手動で入力する必要があります。変更が完了したら、[OK]をクリックし

ます。

NTP 同期

説明:

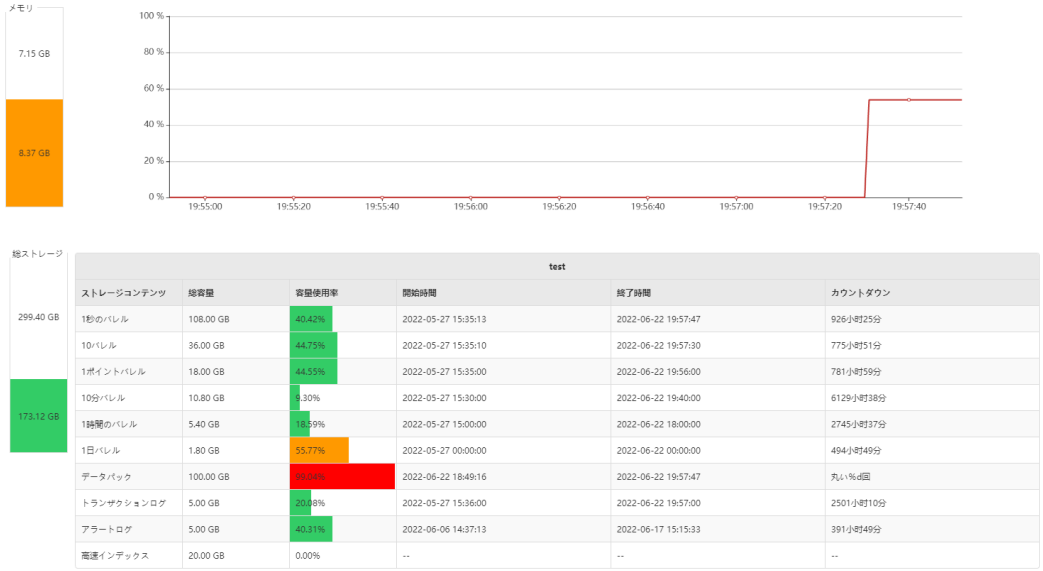
NTP 同期では、最初の同期中にすべてのデータがクリアされ、システムが再起動されます。注意して操作してください。 NTP サーバーを設定すると、分析サーバーの時刻が 1 分ごとに NTP サーバーと自動的に同期されます。

システム時刻をタイムサーバーと自動的に同期する場合は、対応するタイムサーバーを選択する必要があります。 サーバーは、インターネットタイムサーバーまたはユーザー自身のタイムサーバーにすることができます。サーバーは、インターネットに接続できる場合にのみインターネットタイムサーバーを使用できます。

3.16 サーバーステータスビュー

サーバーステータスは、リアルタイムの CPU、メモリ、およびハードディスクの使用量を提供します。 以下に示すよう、にディスクステータスでは、ユーザーはパーティションごとに各タイムバケットのストレージ容量の使用状況を表示できます:

図 4.16 サーバーのステータス



[ステータス設定]ボタンをクリックすると、CPU、メモリ、ハードディスク

を用途別に色分けできます。 次の図に、デフォルトのシステム構成を示します:

図 4.17 ステータス設定

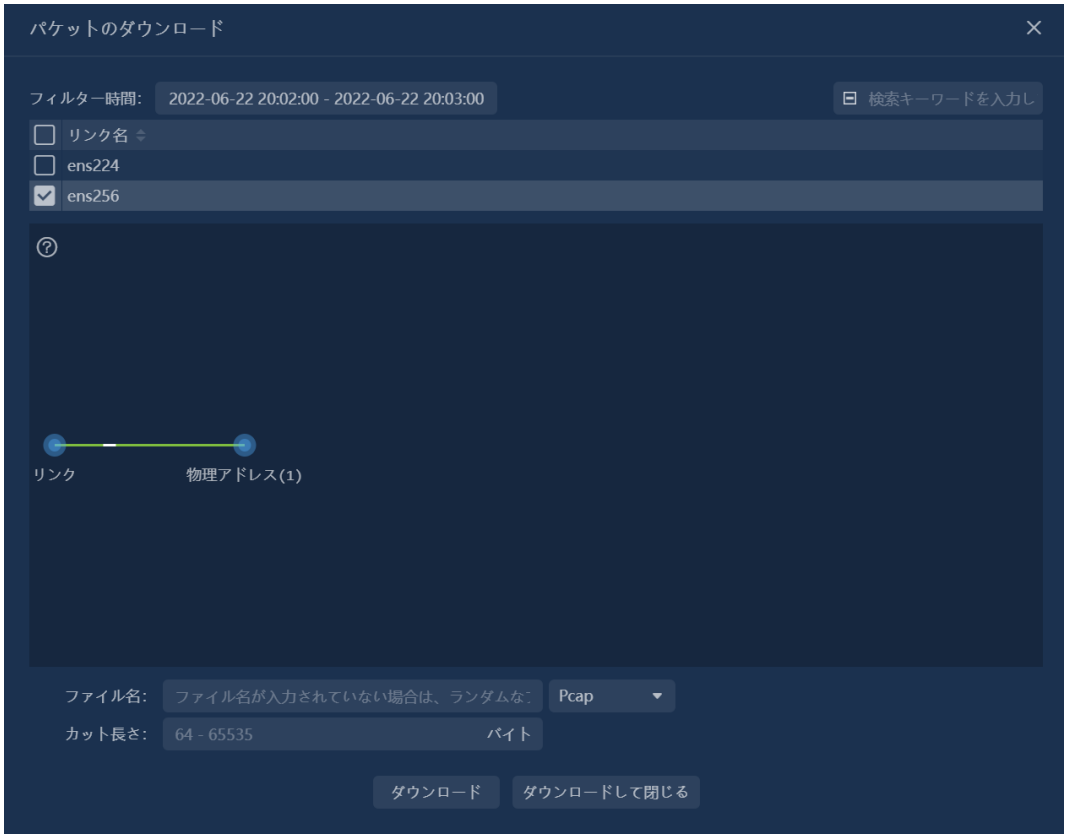
3.17 データのダウンロード

nChronos のすべての統計データとデータパケットはサーバーに保存され、ユーザーは必要なデータパケットをダウンロードして、ダウンロードしたデータパケットに対してより詳細な分析を実行できます。

3.17.1 データパッケージのダウンロード

[データパッケージのダウンロード]ボタンをクリックすると、次の図に示すように、[データパッケージのダウンロード]ダイアログボックスが表示されます。

図 4.18 データパッケージのダウンロード



ユーザーは、データパッケージのダウンロード時間範囲、フィルター条件、ファイルの保存方法、ファイルタイプ、およびその他の情報を必要に応じて設定し、[ダウンロード]ボタンをクリックしてデータパッケージをダウンロードできます。

説明:

クロスリージョン、トラフィックが多く、ネットワーク帯域幅が制限されているネットワーク環境では、ダウンロード時間が長すぎたり、応答がなかったりしないように、データパケットをダウンロードするときに長い期間を選択しないようにしてください。

3.17.2 ダウンロード統計

統計ビューテーブルの右上にある「データのエクスポート」ボタンをクリックすると、統計ビューのデータをエクスポートしてファイルとしてブラウザのデフォルトダウンロードディレクトリに保存できます。

3.18 コマンドライン構成

nChronos サーバーは、コマンドライン構成方法を提供します。コマンドラインを介して、コンソール通信ポート、ブラウザーアクセスポート、アカウント名のリセット、およびその他の情報を設定できます。

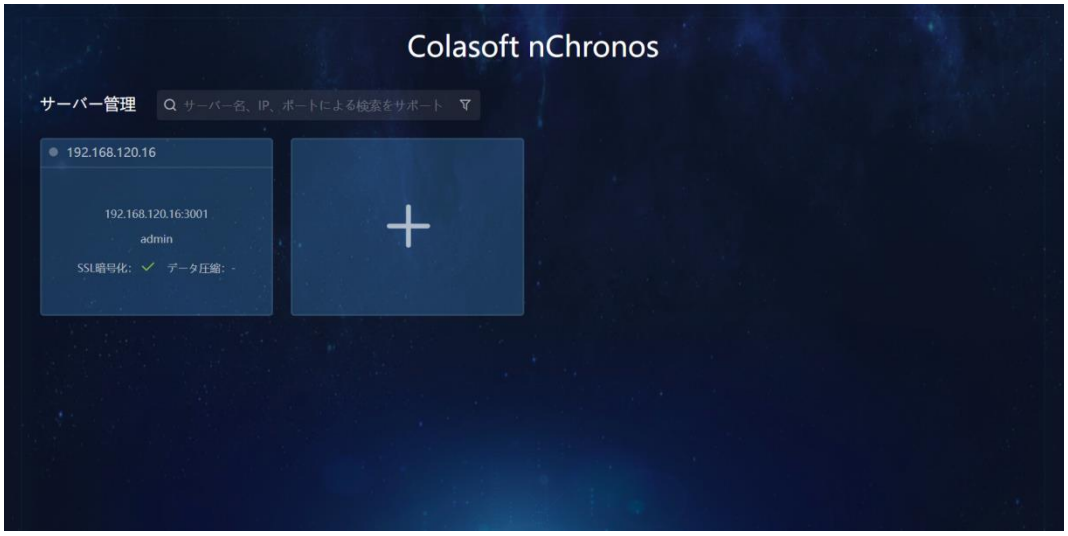
1. ユーザーは、リモートログインツールを使用して、root ユーザーとして nChronos サーバーにログインします。
2. コマンド「cd/usr / local / bin / csrass / tools」を入力して、nChronos のインストールディレクトリに入ります。
3. コマンド「./assist -h」を入力して、サポートされているコマンドをコマンドラインに表示します。

4 コンソール構成

4.1 ログインコンソール

コンソールを配備したサーバーの IP アドレスをブラウザに入力します。たとえば、次のようにします。https://192.168.120.12:8081/、ノックバック、サーバー管理インタフェースが現れ、下図のように。

図 5.1 サーバ管理ページ



4. 追加ボタンをクリックして、次の図に示すように、追加サーバーの弾枠をポップアップします。

図 5.2 ログインインターフェイス

5. ボックスにサーバーのアドレス、ポート、アカウント、パスワード情報を入力したら、「保存して接続」ボタンをクリックして、サーバーの追加を完了し、追加したサーバーのコンソール画面に直接ジャンプします。

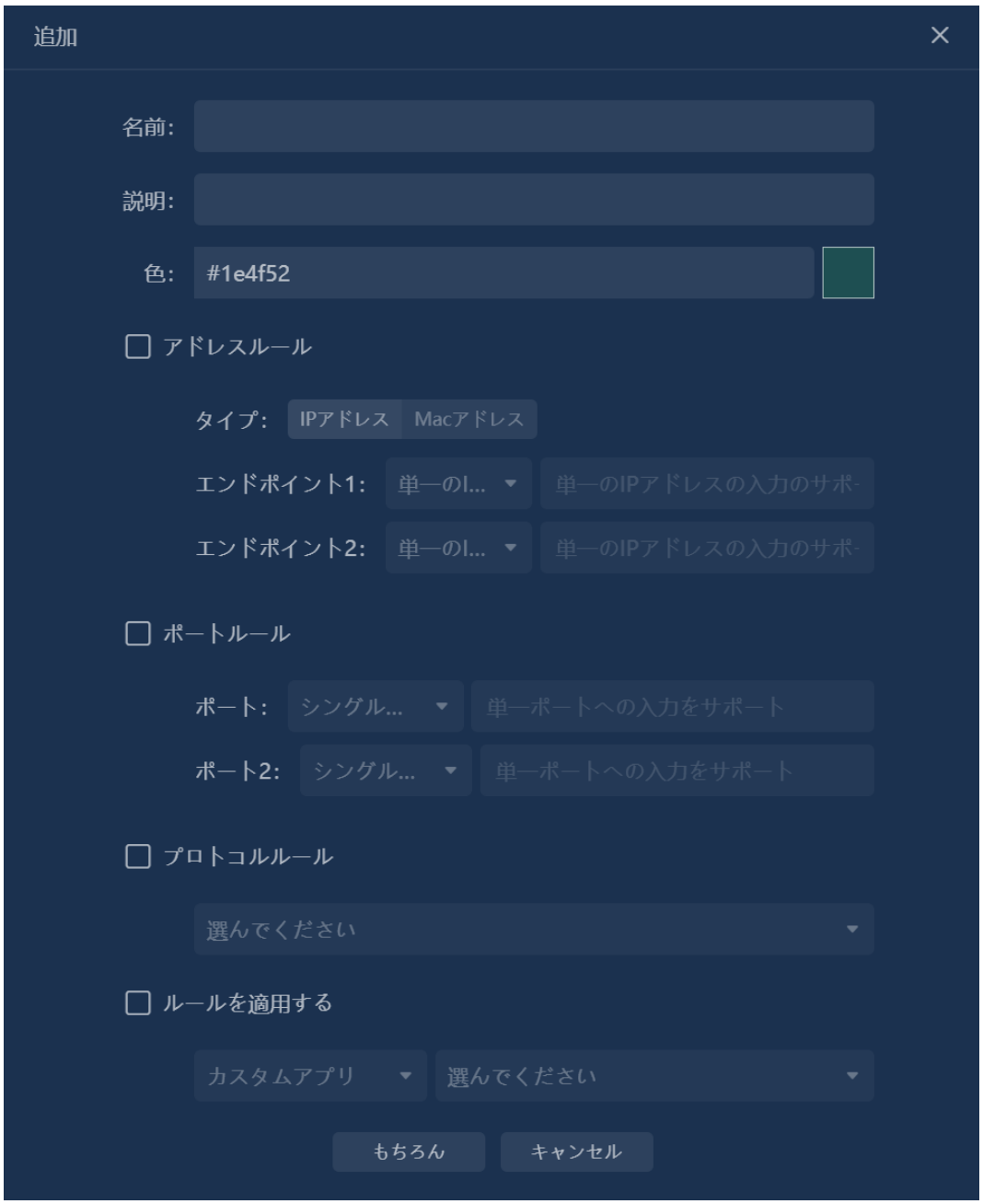
4.2 キャプチャフィルター

キャプチャフィルターを構成することにより、ユーザーが必要とする特定のデータのみをキャプチャし、重要なデータを分離し、不要なデータをフィルターで除外し、データの干渉を減らし、システムの分析パフォーマン

スを向上させることができます。

次の図に示すように、["+"]ボタンをクリックして、[キャプチャフィルターの追加]ダイアログボックスをポップアップします。

図 5.3 キャプチャフィルターの追加



4.2.1 フィルタールール

キャプチャフィルタで設定できるルールには、アドレスルール、ポートルール、プロトコルルール、アプリケーションルールなどがあります。複数のルールが有効になっている場合は、ルール間に AND の関係があります。

アドレスルール

アドレスルールのフィルタリングを有効にする場合、フィルタ条件として IP アドレスまたは MAC アドレスを選択できます。

- IP アドレスを選択する場合、単一の IP アドレス、IP アドレス範囲、IP マスクの入力、および任意の IP アドレスの選択をサポートします。
- MAC アドレスを選択する場合、単一の物理アドレスの入力と任意の物理アドレスの選択をサポートします。

ポートルール

ポートルールフィルタリングを有効にすると、ユーザーはフィルター条件として単一のポート、ポートの範囲、および複数のポートを選択できます。

プロトコルルール

プロトコルルールフィルタリングが有効になっている場合、ユーザーは 1 つ以上のプロトコルをフィルター条件として選択できます。

ルールの適用

アプリケーションルールのフィルタリングを有効にすると、ユーザーは 1 つ以上のアプリケーションをフィルター基準として選択できます。 アプリケーションを選択すると、[アプリケーションタイプ]ドロップダウンリストからアプリケーションをフィルタリングできます。

4.2.2 パケット重複排除設定

重複するパケットは、キャプチャフィルター設定でフィルターで除外することもできます。 ポートミラーリングが誤って構成されているネットワーク環境では、多数の重複パケットが表示され、通常のネットワーク分析に干渉します。 重複したパケットは、分析の精度を向上させ、ディスク容量を節約できます。

システムは、データパケットを重複排除する 2 つの方法、つまり IP アドレスによる重複排除と高度な重複排除を提供します。

- IP アドレス重複排除ルール：送信元 IP アドレス、宛先 IP アドレス、IPID に基づいて判断し、2 つのデータパケットの情報がまったく同じである場合は、重複データパケットと判断します。
- 高度な重複排除ルール：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、IPID、チェックサムに基づいて判断し、2 つのデータパケットの情報がまったく同じである場合、重複データパケットと判断します。

データパケット重複排除設定では、オンサイトのネットワーク状況に応じて、重複データパケットを判断する時間間隔を設定できます。

に注意:

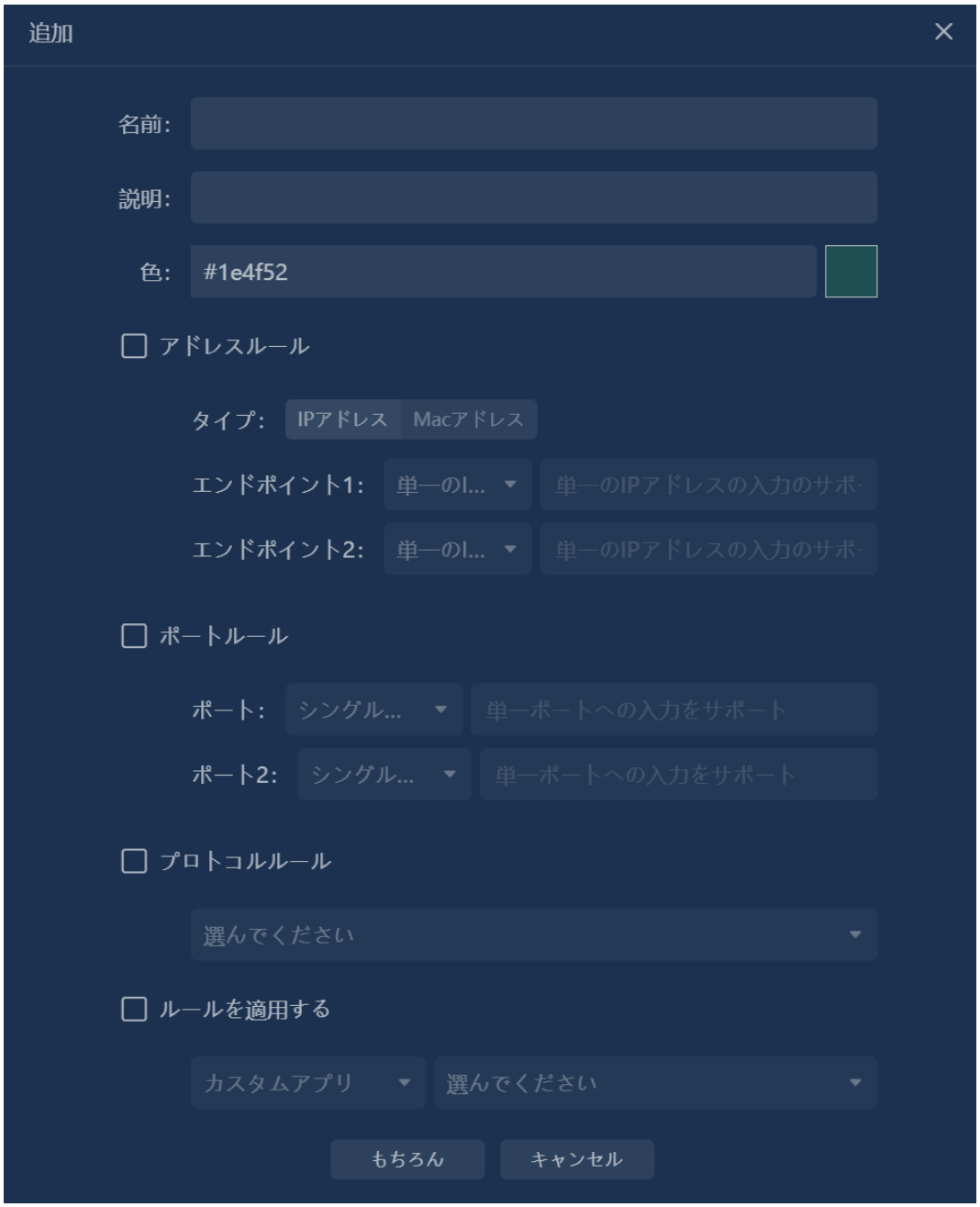
パケット重複排除機能を有効にすると、システムのストレージパフォーマンスに深刻な影響を及ぼします。この機能は、必要な場合にのみ有効にしてください。

4.3 ストレージフィルター

ストレージフィルターを構成することにより、ユーザーが必要とする特定のデータのみを保存できるため、ストレージスペースを節約できます。

次の図に示すように、[+]ボタンをクリックして、[ストレージフィルターの追加]ダイアログボックスをポップアップします。

図 5.4 ストレージフィルター



ストレージフィルターで設定できるルールには、アドレスルール、ポートルール、プロトコルルール、アプリケーションルールなどがあります。複数のルールが有効になっている場合、ルールは AND の関係にあります。

ストレージフィルターでは、各ルールの設定方法はキャプチャーフィルタ

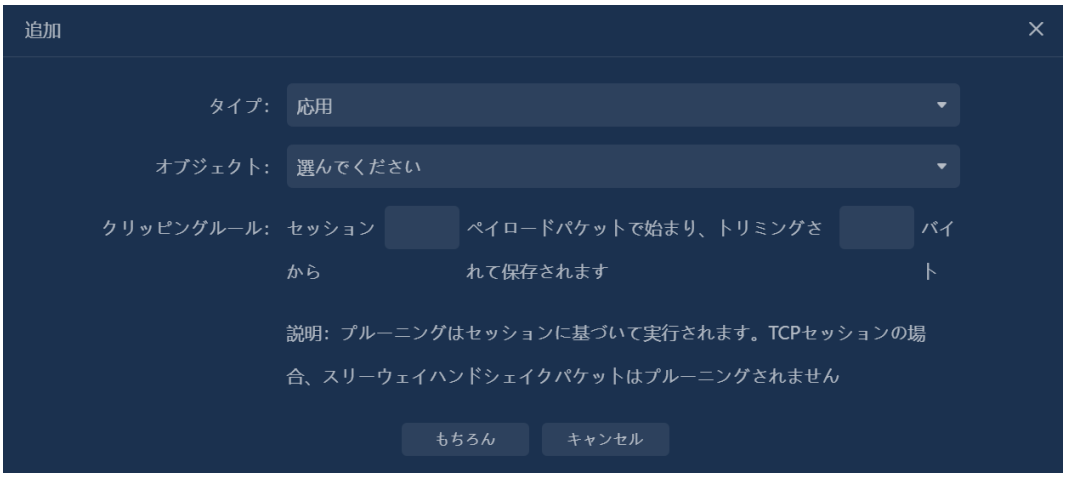
ーの設定方法と同じです。

4.4 パケットクリッピング

パケットトリミング構成では、データパケットをトリミングして保存し、ストレージのパフォーマンスを向上させ、ストレージスペースを節約できます。

次の図に示すように、[ ]ボタンをクリックして、[データパケットクリッピングの追加]ダイアログボックスをポップアップします。

図 5.5 パケットクリッピング



システムでサポートされるオブジェクトタイプには、アプリケーション、プロトコル、VLAN、MPLS VPN、VXLAN、および ISLVLAN が含まれます。

デフォルトでは、システムは HTTPS、POP3_SSL、および SMTP_SSL プロトコルのパケットトリミング構成を提供します。

グローバルストレージクリッピング構成

システムはグローバルストレージトリミング構成を提供します。この構成が有効になっている場合、すべてのデータパケットは、保存時に設定されたトリミング長に従って保存されます。 パケットプルーニングポリシーで

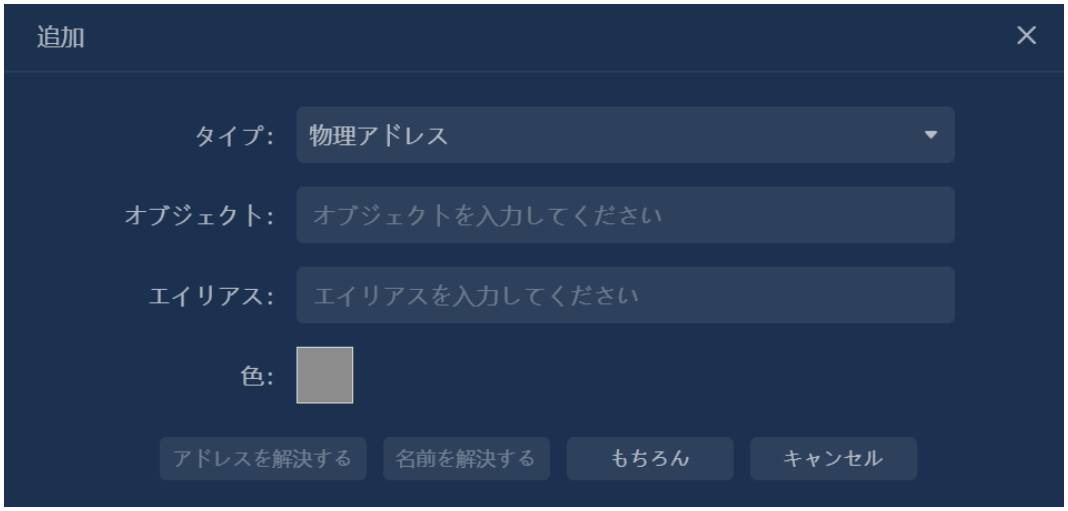
個別に構成されたオブジェクトは、グローバルストレージプルーニング構成の対象ではありません。

4.5 名前リスト

名前テーブルの構成では、さまざまなオブジェクトのエイリアスをカスタマイズできます。これは、ユーザーがネットワークをより便利に識別および管理するのに役立ちます。

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

図 5.6 名前テーブルの追加



名前テーブルでサポートされるオブジェクトタイプには、IPv4 アドレス、IPv6 アドレス、物理アドレス、VLAN ID、MPLS VPN ラベル、ISL VLAN ID、DSCP タグ、および VXLANID が含まれます。

- アドレスの解析：このボタンをクリックして、IPv4 アドレスのエイリアスを解決し、解決結果を[エイリアス]テキストボックスに表示します。 このボタンは、「タイプ」が「IPv4 アドレス」の場合にのみ使用できます。
- 名前の解析：このボタンをクリックして、エイリアスに対応する IPv4 アドレスを解決し、解決結果を[IP アドレス]テキストボックスに表示し

ます。 このボタンは、「タイプ」が「IPv4 アドレス」の場合にのみ使用できます。

ホスト名を自動的に解析する

システムは、自動ホスト名解決を有効にするかどうか、自動解決されたホスト名を保存するかどうか、および未使用の名前を保存する時間の設定をサポートします。

4.6 サブリンク

サブリンクを構成することにより、ユーザーは、ネットワーク環境内の仮想ネットワーク統計、ネットワークセグメントデータ、および物理アドレスデータをより便利に管理および監視できます。

次の図に示すように、[ "]ボタンをクリックして、[サブリンクの追加]ダイアログボックスをポップアップします。

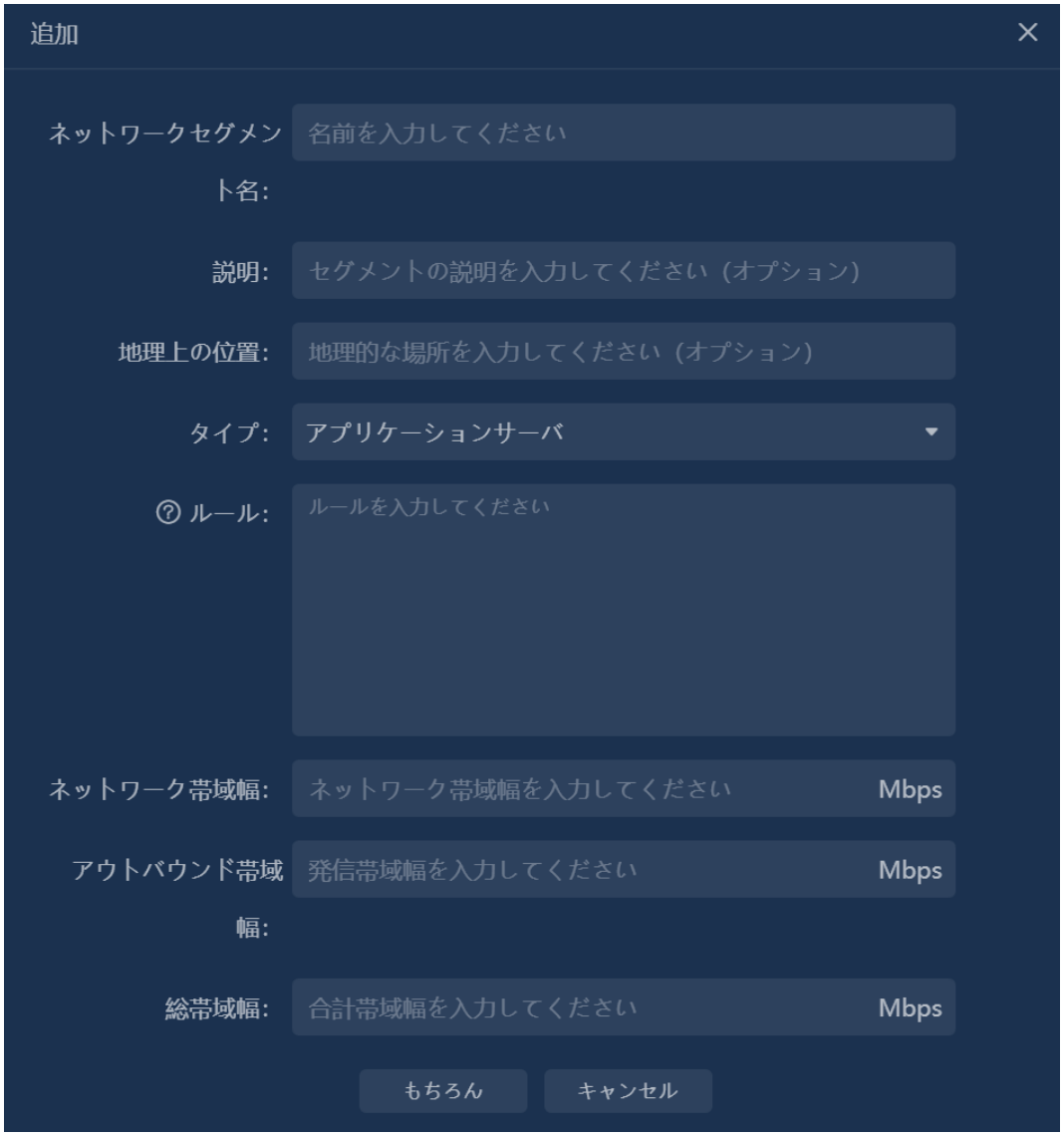
図 5.7 サブリンクの追加

サポートされているサブリンクのタイプには、VLAN ID、ISL VLAN ID、VXLAN ID、MPLS VPN ID、MAC アドレス、インターフェイス ID、およびネットワークセグメントが含まれます。 インターフェイス ID タイプのサブリンクは、Netflow リンクと Sflow リンクでのみ作成できます。

4.7 ネットワークセグメントの構成

次の図に示すように、[+"]ボタンをクリックして、[ネットワークセグメントの追加]ダイアログボックスをポップアップします。

図 5.8 ネットワークセグメントの追加



ネットワークセグメントルールを構成する場合、複数のネットワークセグメントルールはキャリッジリターンで区切られ、複数のネットワークセグメントは「または」の関係にあります。 IP ネットワークセグメントは、次

の 3 つの形式をサポートしています:

- 192.168.1.1、FE80 :: AAAA：C202 などの個別の IP アドレス。
- 192.168.1.1-192.168.1.100、FE80 :: AAAA：C202-FE80 :: AAAA：C2FE などの IP アドレス範囲。
- 192.168.1.0/24、FE80 :: AAAA：C202/100 などの IP アドレス/マスク。

4.8 アプリケーション構成

4.8.1 アプリケーション

このシステムは、標準アプリケーション、Web アプリケーション、機能値アプリケーション、暗号化アプリケーション、およびプロトコルアプリケーションの定義をサポートしています。

標準アプリケーション

標準アプリケーションとは、定義されたルールとして IP とポートを使用するアプリケーションを指します。 [標準アプリケーションの追加]ダイアログボックスを以下に示します。

図 5.9 標準アプリケーションの追加

Web アプリケーション

コンソール構成

Web アプリケーションとは、ホスト名を定義されたルールとして使用するアプリケーションを指します。現在、分析できるのは HTTP プロトコルに基づく Web アプリケーションのみです。 [Web アプリケーションの追加] ダイアログボックスを以下に示します。

図 5.10 Web アプリケーションの追加

コンソール構成

固有値アプリケーション

固有値アプリケーションとは、データパケット内の機能値を照合することによるアプリケーションの識別を指します。 次の図に、[固有値の追加]ダイアログボックスを示します。

図 5.11 固有値アプリケーションの追加

暗号化アプリケーション

アプリケーション構成を暗号化するときは、RSA キーをアップロードする必要があります。 次の図に、[暗号化アプリケーションの追加]ダイアログボックスを示します。

図 5.12 暗号化アプリケーションの追加

プロトコルアプリケーション

プロトコルアプリケーションとは、アプリケーション層のプロトコルをアプリケーションとして定義することです。 次の図に、[プロトコルアプリケーションの追加]ダイアログボックスを示します。

図 5.13 プロトコルアプリケーションの追加

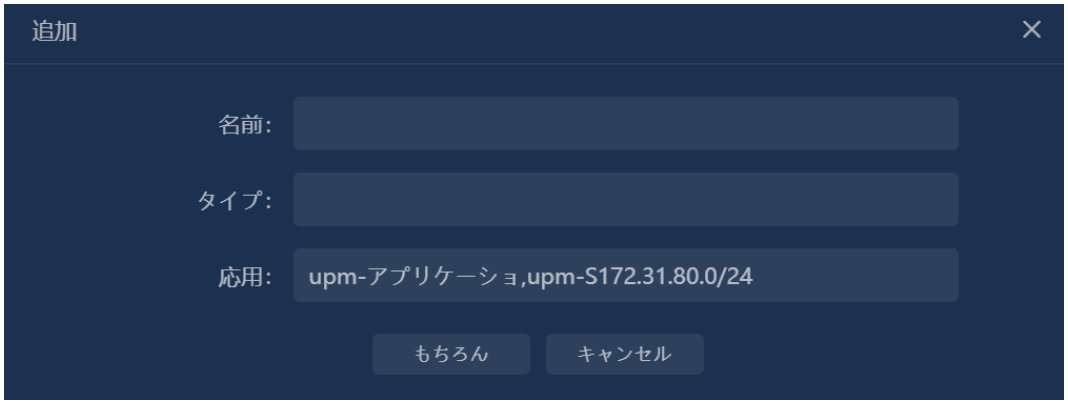
4.8.2 アプリケーションのグループ化

ユーザーは、実際の状況に応じて複数のアプリケーションをアプリケーシ

ョングループに分割し、複数のアプリケーションに対して組み合わせた分析を実行できます。

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

図 5.14 アプリケーショングループの追加



4.9 アラーム設定

4.9.1 フローアラーム

トラフィックアラートの原理は、パケット数、バイト数、平均パケット長などの統計指標を設定することです。トリガー時間内の平均トラフィックがトリガー条件に達すると、対応するトラフィックアラートがトリガーされます。 このアラートをメールボックスと SYSLOG サーバーに自動的に送信するように設定することもできます。

次の図に、トラフィックアラート設定のポップアップを示します。

図 5.15 アラームの追加

アラーム設定ポップアップボックスの各設定フィールドの説明を次の表に示します。

表 5.1 アラートフィールドの説明

パラメータ名	具体的な説明
名前	定義されたアラームの名前を設定するために使用されます。アラームの名前は一意である必要があり、他のアラームで定義された名前と同じにすることはできません。
アラートレベル	アラームレベルの設定に使用され、システムは「低」、「中」、「高」の 3 つのアラームレベルを提供します。
分類	アラームの分類を設定するために使用され、ユーザーは必要に応じてアラームを選択または追加できます。
サブリンク	オプション設定。サブリンクを選択すると、サブリンクのアラームが追加されます。サブリンクを選択しない場合は、リンクのアラームが追加されます。
タイプ	アラームの種類を設定するために使用されます。リンク

コンソール構成

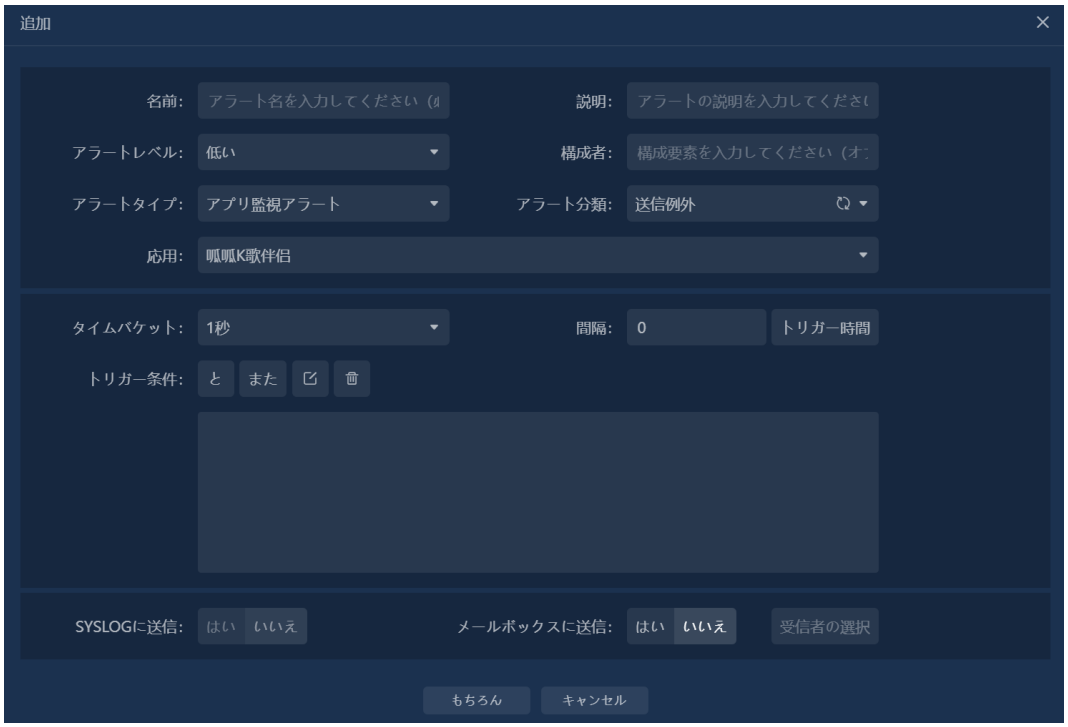
パラメータ名	具体的な説明
	とサブリンクは、さまざまなアラームの種類に対応しています。
構成者	オプションで、このアラートの設定に使用するコンフィギュレーターを構成します。
説明	オプションの設定は、定義されたアラームを解釈するために使用されます。
トリガーディメンション	アラームタイプがネットワークセグメント間の IP セッションアラーム、物理セッションアラーム、および統計アラームを選択する場合、トリガーディメンションの設定をサポートします。
トリガー条件	アラームパラメータのタイプとアラームトリガー条件を設定するために使用され、システムは複数のアラームパラメータ間の「and」、「or」の関係をサポートします。
タイムバケット	アラーム設定用のタイムバケット。システムは「1 秒」、「10 秒」、「1 分」、「5 分」、「10 分」、「1 時間」、「1 日」を提供します。 タイムバケット内の平均トラフィックがトリガー条件に達すると、トラフィックアラームがトリガーされます。
持続回数	アラームの持続時間を設定するために使用されます。アラーム条件が満たされた回数が設定されたしきい値以上になると、アラームがトリガーされます。 抑制しきい値を設定することにより、誤警報を効果的に減らすことができます。
トリガー時間	アラームのトリガー時間範囲を設定するために使用されます。アラームは、指定された時間範囲内でのみトリガーされます。
アラートの送信	アラームがトリガーされた後に送信するかどうかを設定するために使用されます。システムには、「SendtoEmail」と「SendtoSYSLOG」の 2 つの送信方法があります。 ユーザーがメールボックスに送信することを選択すると、アラートに別の受信者を指定したり、受信者を一時的に追加したりできます。

4.9.2 アラートの適用

アプリケーションアラートは、監視対象アプリケーションにのみ設定できます。アプリケーションアラートには、アプリケーション監視アラート、サーバーアラート、クライアントアラート、ネットワークセグメントアラート、IP セッションアラート、TCP セッションアラート、UDP セッションアラート、サービスアクセスアラート、および TCP サービスポートアラートが含まれます。これらの 10 種類の UDP サービスポートアラート。

アラーム設定を適用する弾枠を下図に示します。

図 5.16 応用警報の追加



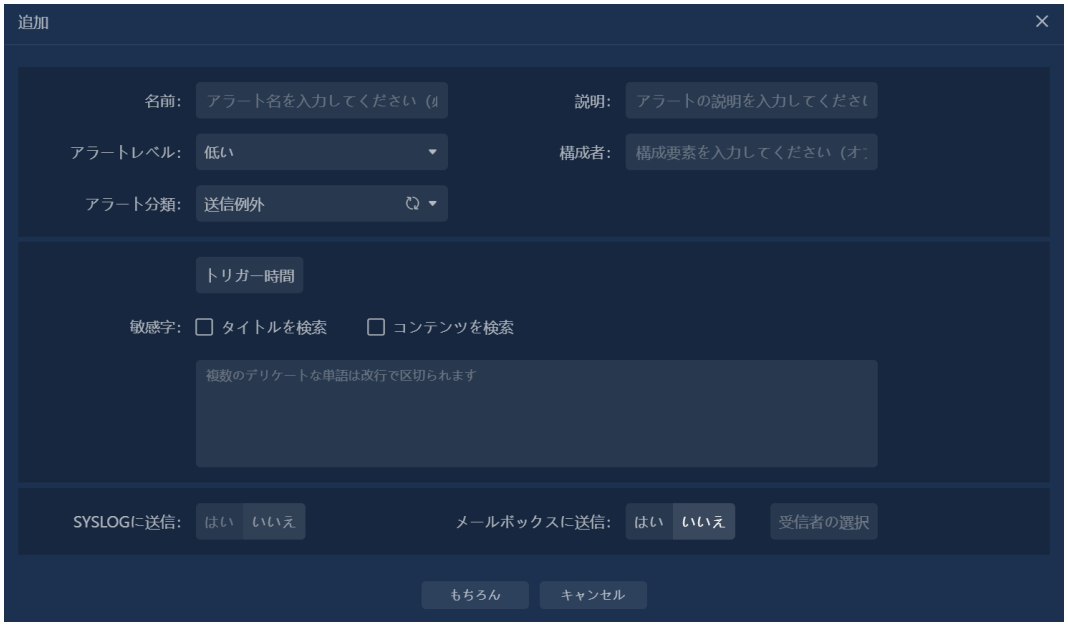
4.9.3 メール機密ワードアラート

メールセンシティブワードアラートの原則は、メールのタイトルとコンテンツを検索することです。設定されたセンシティブワードに一致するコンテンツが見つかると、メールセンシティブワードアラートがトリガーされます。 このアラートをメールボックスと SYSLOG サーバーに自動的に送

信するように設定することもできます。

メールセンシティブワードアラームの設定ボックスを下図に示します。

図 5.17 メール機密ワードアラートの追加



4.9.4 不審なドメイン名のアラート

疑わしいドメイン名アラートは、ドメイン名と IP アドレスのアラートの設定をサポートします。原則は、キャプチャされたデータパケットを検索することです。検索されたドメイン名がアラートで設定されたドメイン名と一致する場合、または DNS によって解決された IP アドレスはアラートで設定された IP アドレスと同じです。それらが一貫している場合、疑わしいドメイン名アラートがトリガーされます。 このアラートをメールボックスと SYSLOG サーバーに自動的に送信するように設定することもできます。

不審なドメイン名のアラート設定ボックスを下図に示します。

図 5.18 不審なドメイン名アラートの追加

4.9.5 ベースライン警報

ベースラインアラームの原理は、キャプチャされた実際のデータをベースラインデータと比較することです。たとえば、偏差率がアラーム設定の条件に達すると、ベースラインアラームがトリガーされます。

説明:

ベースラインデータは、履歴データに基づいて特定のルールに従ってシステムによって自動的に計算されます。

ベースライン警報配置弾枠を下図に示します。

図 5.19 ベースラインアラームの追加

4.9.6 突発警報

突然のアラートは、異常にバーストしてトレンドを維持するためのアラートです。 特定の期間に、キャプチャされた実際のデータが前の N サイクルのデータと比較されると同時に、ベースラインデータおよびインジケータしきい値データとの比較がサポートされ、アラームの精度が向上します。

突発警報配置弾枠を下図に示す。

図 5.20 突発警報の追加

コンソール構成

5 リンクトラフィックモニタリング

メニューから[リンク分析]>[リンクトラフィック分析]を選択して、リンクリストページに入ります。 リンクリストで監視するリンクを選択します。

次の図に示すように、リンクトラフィック分析ページで、[監視モード]タブをクリックして、リンクトラフィック監視状態に切り替えます。

図 6.1 リンクトラフィックの監視

6 リンクトラフィック分析

メニューから[リンク分析>リンクトラフィック分析]を選択して、リンクリストページに入ります。 リンクリストで監視するリンクを選択します。

次の図に示すように、リンクトラフィック分析ページで、[分析モード]タブをクリックして、リンクトラフィック分析状態に切り替えます。

図 7.1 リンクトラフィック分析

6.1 比較分析

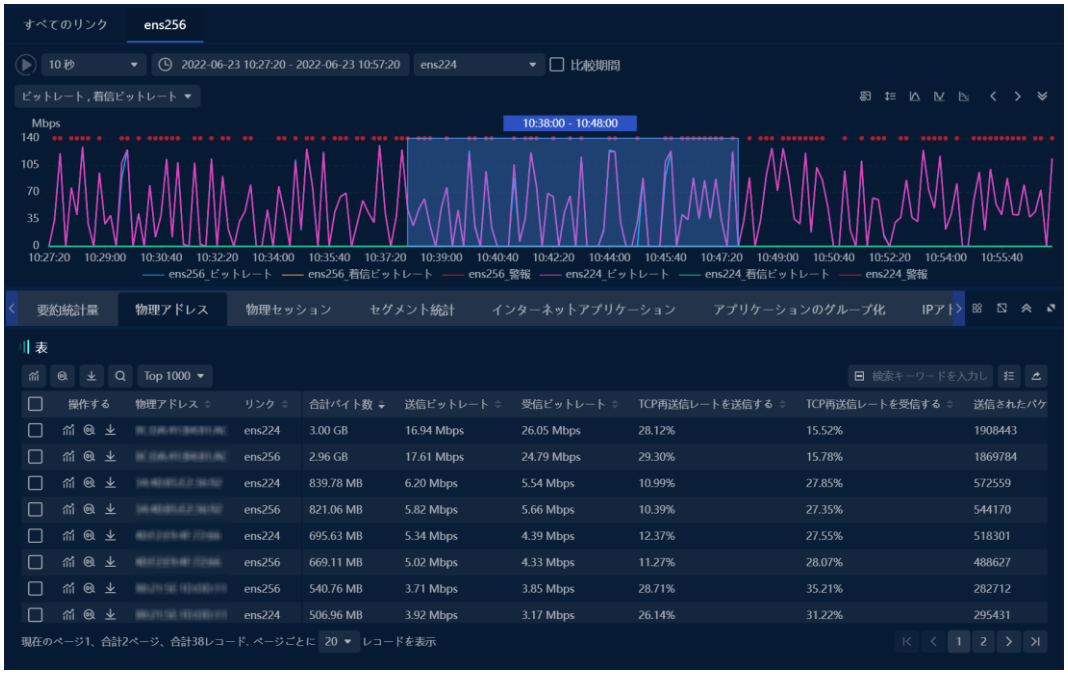
リンク分析は、さまざまなリンクとの比較およびさまざまな期間との比較をサポートします。

6.1.1 異なるリンクの比較

[比較リンク]ドロップダウンリストで、比較および分析するリンクを選択すると、複数の選択がサポートされます。

選択が完了すると、次の図に示すように、比較リンクのデータがトレンドグラフと統計ビューの表に表示されます。

図 7.2 さまざまなリンクの比較



6.1.2 異なる期間の比較

「比較期間」チェックボックスをチェックし、比較期間（システムは、前年比、先週の前年比、前月の前年比、およびカスタムを提供します）を選択し、「OK」ボタンをクリックします。さまざまな期間のリンクのデータ比較を表示するには、以下に示します。

図 7.3 さまざまな期間の比較

6.2 傾向分析

傾向分析ページは、傾向グラフと統計ビューで構成されています。データマイニングは統計ビューでサポートされています。

6.2.1 Web アプリケーション

ネットワークアプリケーションビューでは、次の図に示すように、システムに付属するアプリケーションとユーザー定義のアプリケーションで統計と表示が実行されます。

図 7.4 Web アプリケーションビュー

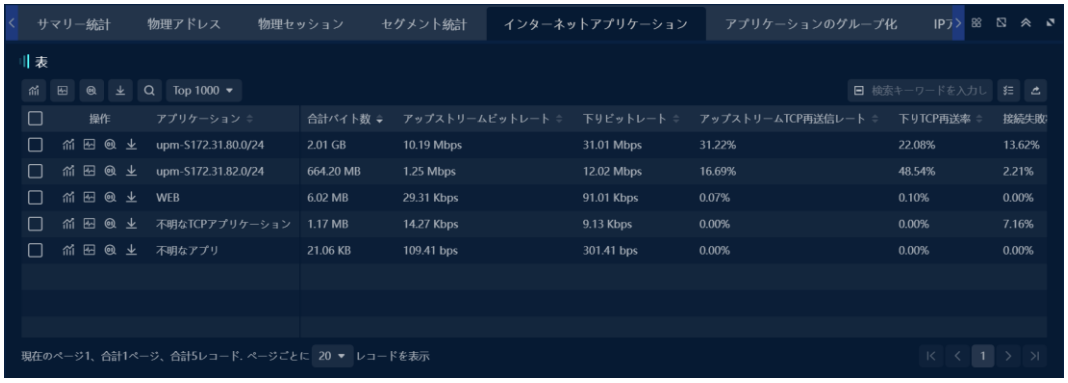


図 5.20 突発警報ネットワークアプリケーションの追加ビューでは、1 つ以上のアプリケーションについてトレンド分析を行うことができます。トレンド分析が必要なネットワークアプリケーションを選択し、ボタンをクリック  して、ネットワークアプリケーションのトレンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、アプリケーションに関連するクライアント、サーバ、ネットワークセグメント、IP セッション、TCP セッション、UDP セッション、パケットサイズ分布、TCP サービスポート、UDP サービスポート、およびサービスアクセス情報を迅速にマイニングすることができます。

図 7.5 応用傾向分析 应用趋势分析

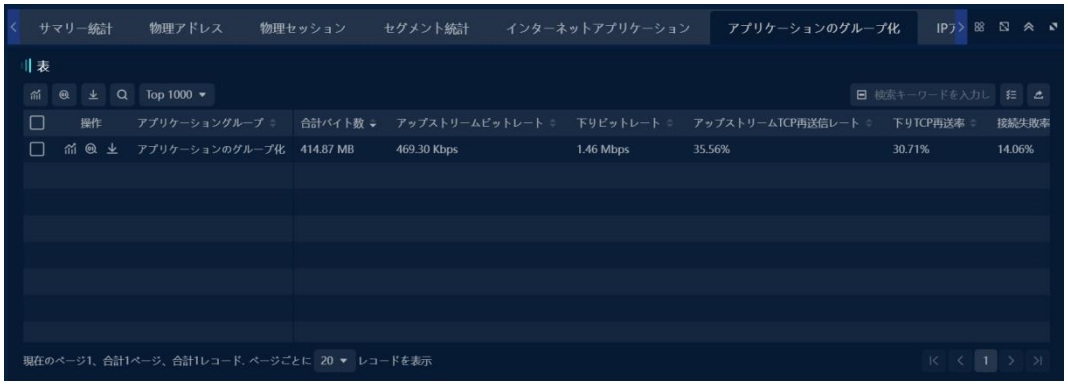
Web アプリケーションビューでは、データマイニングを 1 つ以上のアプリケーションで実行できます。 データマイニングが必要なネットワークアプリケーションを選択して右クリックし、ポップアップコンテキストメニューで[マイニング]を選択して、ネットワークアプリケーションのマイニングインターフェイスに入ります。

データマイニングを通じて、ネットワークセグメントの統計、イントラネットアドレス、エクストラネットアドレス、IP セッション、TCP セッション、UDP セッション、パケットサイズの分散、TCP サービスポート、UDP サービスポート、およびアプリケーションに関連するサービスアクセスをすばやくマイニングできます。

6.2.2 アプリケーションのグループ化

アプリケーショングループ化ビューでは、ネットワークリンクに設定されているアプリケーショングループ化情報に従って、次の図に示すように、データがカウントされ、アプリケーショングループの単位で表示されます。

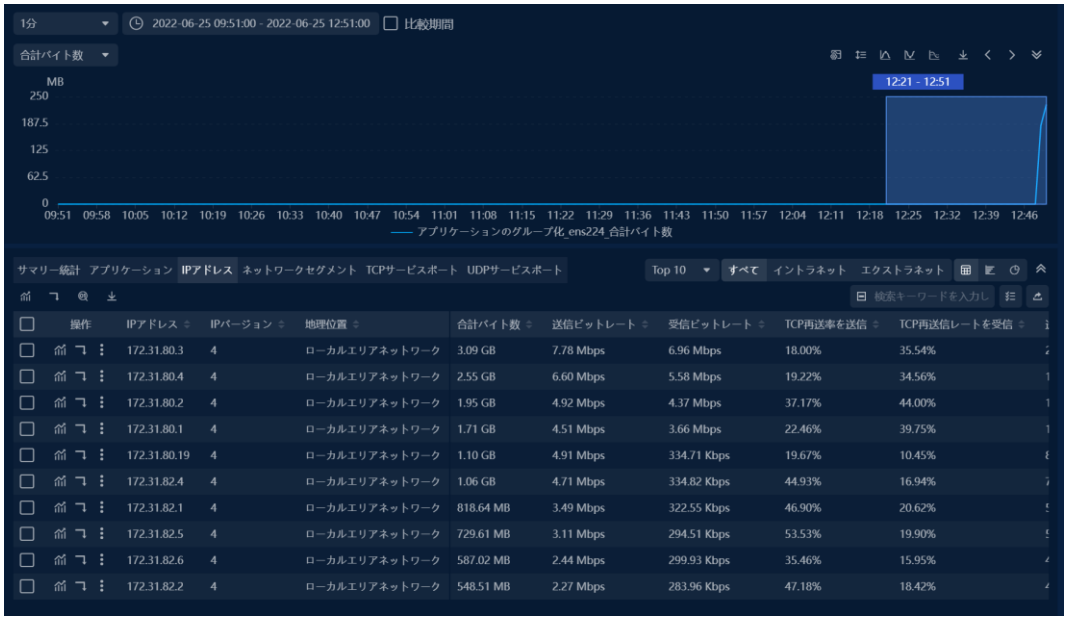
図 7.6 アプリケーションのグループ化ビュー



適用グルーピングビューでは、1 つ以上の適用グルーピングについてトレンド分析を行うことができます。トレンド分析を行う必要があるアプリケーショングループを選択し、ボタンをクリック  して、アプリケーショングループのトレンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、アプリケーションパケットに関連するネットワークアプリケーション、IP アドレス、ネットワークセグメント、TCP サービスポート、UDP サービスポート情報を迅速にマイニングすることができます。

図 7.7 パケットトレンド解析の適用



アプリケーショングループ化ビューでは、1 つ以上のアプリケーショングループでデータマイニングを実行できます。 データマイニングが必要なアプリケーショングループを選択して右クリックし、ポップアップコンテキストメニューで[マイニング]を選択して、アプリケーショングループのマイニングインターフェイスに入ります。

データマイニングを通じて、ネットワークアプリケーション、イントラネットアドレス、エクストラネットアドレス、ネットワークセグメントのグループ化、ネットワークセグメントの統計、TCP サービスポート、およびアプリケーショングループに関連する UDP サービスポートの情報をすばやくマイニングできます。

6.2.3 サービスアクセス

次の図に示すように、サービスアクセスビューは、監視対象リンク内のさまざまなネットワークアプリケーションのアクセスステータスを表示するために使用されます:

図 7.8 サービスアクセスビュー

サービスアクセスビューでは、1 つまたは複数のサービスアクセスレコード についてトレンド分析を行うことができます。トレンド分析が必要なサービ スアクセス履歴を選択し、ボタンをクリック  して、サービスアクセスのトレ ンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、サービスアクセスに関連する TCP または UDP セッション情報を迅速にマイニングします。

図 7.9 サービスアクセス動向分析

サービスアクセスビューでは、1 つ以上のサービスアクセスレコードに対してデータマイニングを実行できます。 マイニングする必要のあるサービスアクセスレコードを選択して右クリックし、ポップアップコンテキストメニューで[マイニング]を選択して、サービスアクセスのマイニングインターフェイスに入ります。

データマイニングを通じて、サービスアクセスに関連する TCP または UDP セッション情報をすばやくマイニングできます。

6.2.4 物理アドレス

次の図に示すように、物理アドレスビューでは、選択した期間の物理アドレス情報の統計と表示が実行されます:

図 7.10 物理アドレスビュー

物理アドレスビューでは、1 つ以上の物理アドレスをトレンド解析できます。トレンド分析を行う必要がある物理アドレスを選択し、ボタンをク

 リックして、物理アドレスのトレンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、物理アドレスに関連する物理セッション、IP アドレス、IP セッション、ネットワークアプリケーション、およびネットワークセグメント情報を迅速にマイニングすることができます。

図 7.11 物理アドレストレンド解析

物理アドレスビューでは、データマイニングは 1 つ以上の物理アドレスで実行できます。 データマイニングの物理アドレスを選択して右クリックし、ポップアップコンテキストメニューで[マイニング]を選択して、物理アドレスのマイニングインターフェイスに入ります。

データマイニングを通じて、物理セッション、外部ネットワークアドレス、内部ネットワークアドレス、IP セッション、ネットワークアプリケーション、および物理アドレスに関連するネットワークセグメントの統計をすばやくマイニングできます。

6.2.5 物理セッション

次の図に示すように、物理セッションビューでは、選択した期間の物理セッション情報の統計と表示が実行されます。

図 7.12 物理セッションビュー

6.2.6 サービスポート

次の図に示すように、サービスポートビューでは、選択した期間のサービスポート情報の統計と表示が実行されます。

図 7.13 サービスポートの図

サービスポートビューでは、1 つ以上のサービスポートのトレンド分析を行うことができます。トレンド分析が必要なサービスポートを選択し、ボタンをクリックして、サービスポートのトレンド分析インタフェースに入ります。

トレンド分析により、オブジェクトのサービスポートに関連するクライアント、TCP セッション、UDP セッション、およびサービスアクセス情報を迅速にマイニングできます。

図 7.14 サービスポートトレンド解析

サービスポートビューでは、1 つ以上のサービスポートでデータマイニングを実行できます。 データマイニング用のサービスポートを選択して右クリックし、ポップアップコンテキストメニューで[マイニング]を選択して、サービスポートのマイニングインターフェイスに入ります。

データマイニングを通じて、クライアント、サーバー、TCP サービスポート、UDP サービスポート、サービスアクセス、TCP セッション、およびオブジェクトのサービスポートに関連する UDP セッション情報をすばやくマイニングできます。

6.2.7 ポート統計

ポート統計ビューは次の図の通りです:

図 7.15 ポート統計ビュー

ポート統計ビューでは、1 つ以上のポートについてトレンド分析を行うことができます。トレンド分析が必要なポートを選択し、ボタンをクリックして、ポートのトレンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、ポートに関連するクライアント、サーバ、サービスアクセス、サービスポート、TCP セッション、UDP セッション情報を迅速にマイニングできます。

図 7.16 ポート統計トレンド分析

ポート統計ビューでは、1 つ以上のポートでデータマイニングを実行できます。 データマイニング用のポートを選択して右クリックし、ポップアップコンテキストメニューで[マイニング]を選択して、ポートマイニングイン

ターフェイスに入ります。

データマイニングを通じて、ポートに関連するクライアント IP、TCP セッション/ UDP セッション、およびサービスアクセス情報をすばやくマイニングできます。

6.2.8 ネットワークセグメント統計

ネットワークセグメント統計ビューでは、次の図に示すように、ネットワークリンクに設定されているネットワークセグメント情報に従って、データがネットワークセグメントごとに収集および表示されます。

ネットワークセグメント統計ビュー

ネットワークセグメント統計ビューでは、1 つまたは複数のネットワークセグメントのトレンド分析を行うことができます。トレンド分析を行う必要があるネットワークセグメントを選択し、ボタンをクリックして、ネットワークセグメントのトレンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、ネットワークセグメントに関連するネットワークアプリケーション、IP アドレス、IP セッション、DSCP 統計を迅速にマイニングすることができます。

図 7.18 セグメント傾向解析

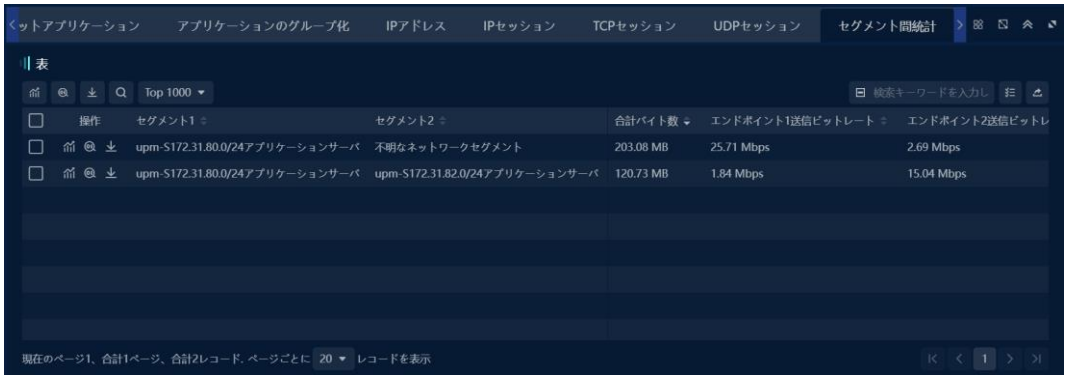
ネットワークセグメント統計ビューでは、1 つ以上のネットワークセグメントでデータマイニングを実行できます。 データマイニングを実行する必要のあるネットワークセグメントを選択して右クリックし、ポップアップコンテキストメニューで[マイニング]を選択して、ネットワークセグメントマイニングインターフェイスに入ります。

データマイニングを通じて、ネットワークアプリケーション、セグメント内アドレス、セグメント外アドレス、すべてのアドレス、IP セッション、TCP セッション、UDP セッション、サービスアクセス、およびネットワークセグメントに関連する DSCP 統計をすばやくマイニングできます。

6.2.9 ネットワークセグメント間の統計

ネットワークセグメント間の統計ビューでは、次の図に示すように、ネットワークセグメント間の通信情報は、ネットワークリンクに設定されたネットワークセグメント情報に従って計算されます。

図 7.19 ネットワークセグメント間の統計ビュー



ネットワークセグメント間統計ビューでは、1 つまたは複数のネットワークセグメント間のデータをトレンド分析できます。トレンド分析を行う必要があるネットワークセグメントを選択し、ボタンをクリックして、ネットワークセグメント間のトレンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、ネットワークセグメント間の IP セッション、TCP セッション、UDP セッション情報を迅速にマイニングすることができます。

図 7.20 セグメント間トレンド分析

ネットワークセグメント間の統計ビューでは、1 つ以上のネットワークセ

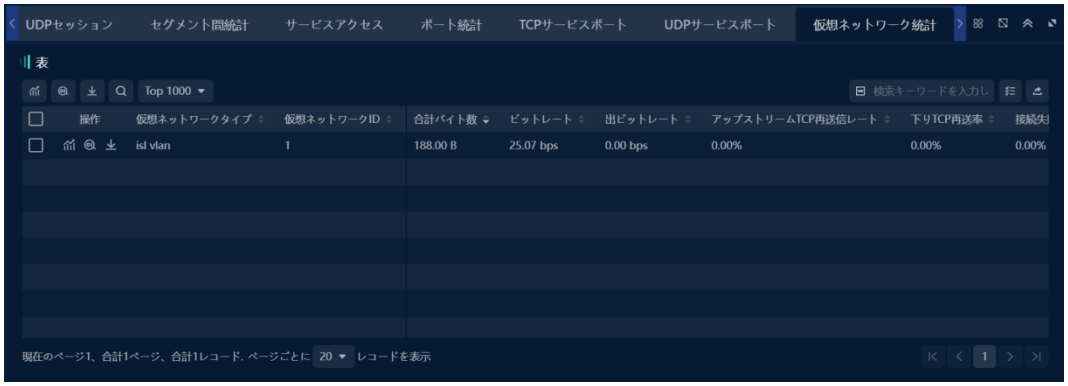
グメント間でデータをマイニングできます。 データマイニングを実行する必要のあるネットワークセグメントを選択して右クリックし、ポップアップコンテキストメニューで[マイニング]を選択して、ネットワークセグメント間のマイニングインターフェイスに入ります。

データマイニングを通じて、IP セッション、TCP セッション、UDP セッション、およびネットワークセグメント間のサービスアクセス情報をすばやくマイニングできます。

6.2.10 仮想ネットワーク統計

次の図に示すように、仮想ネットワーク統計ビューには、VLAN 統計、MPLS VPN 統計、VXLAN 統計、および仮想ネットワークのタイプに応じたすべての仮想ネットワーク統計が含まれます。

図 7.21 仮想ネットワーク統計ビュー



統計ビューでは、1 つ以上の VLAN/MPLS VPN/VXLAN に対してトレンド分析を行うことができます。トレンド分析が必要な VLAN/MPLS VPN/VXLAN を選択し、ボタンをクリックして VLAN/MPLS VPN/VXLAN のトレンド分析インタフェースに入ります。

トレンド分析により、下図に示すように、VLAN/MPLS VPN/VXLAN に関連するネットワークアプリケーション、IP アドレス、通信アドレス、IP セッション、サービスアクセス、DSCP 統計を迅速にマイニングすることがで

きます。

図 7.22 仮想ネットワークトレンド解析

統計ビューでは、データマイニングは 1 つ以上の VLAN / MPLS VPN/VXLAN で実行できます。 データマイニングを実行する必要のある VLAN/MPLS VPN / VXLAN を選択して右クリックし、ポップアップコンテキストメニューから[マイニング]を選択して、VLAN / MPLS VPN/VXLAN マイニングインターフェイスに入ります。

データマイニングを通じて、ネットワークアプリケーション、外部ネットワークアドレス、内部ネットワークアドレス、すべてのアドレス、通信アドレス、IP セッション、サービスアクセス、および VLAN / MPLS VPN/VXLAN に関連する DSCP 統計をすばやくマイニングできます。

6.2.11 DSCP 統計

DSCP 統計ビューは、下図に示すように、監視されているリンク内の DSCP のトラフィック情報を表示するために使用される。

図 7.23 DSCP 統計図

DSCP 統計ビューでは、1 つまたは複数の DSCP レコードに対してトレンド分析を行うことができます。データマイニングが必要な DSCP レコードを選択し、ボタンをクリックして、DSCP のトレンド分析インタフェースに入ります。

トレンド分析により、下図に示すように、DSCP レコードに関連するアプリケーション、IP アドレス、IP セッション、TCP セッション情報を迅速にマイニングすることができます。

図 7.24 DSCP トレンド解析

6.2.12 IP アドレス

次の図に示すように、IP アドレスビューでは、選択した期間の IP アドレス

がカウントされ、て表示:

図 7.25 IP アドレスビュー

IP アドレスビューでは、1 つまたは複数の IP アドレスをトレンド分析することができます。トレンド分析が必要な IP アドレスを選択し、ボタンをクリックして、IP アドレスのトレンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、IP アドレスに関連するネットワークアプリケーション、IP セッション、TCP セッション、UDP セッション、物理アドレス、TCP サービスポート、UDP サービスポート、およびサービスアクセス情報を迅速にマイニングすることができます。

図 7.26 IP アドレストレンド解析

6.2.13 IP セッション

次の図に示すように、IP セッションビューでは、選択した期間の IP セッション情報の統計と表示が実行されます。

図 7.27 IP セッションビュー

IP セッションビューでは、1 つまたは複数の IP セッションのトレンド分析を行うことができます。トレンド分析が必要な IP セッションを選択し、ボタンをクリックして、IP セッションのトレンド分析インタフェースに入ります。

トレンド分析により、次の図に示すように、IP セッションに関連する TCP セッションと UDP セッション情報を迅速にマイニングすることができます。

図 7.28 IP アドレストレンド解析

6.2.14 TCP セッション

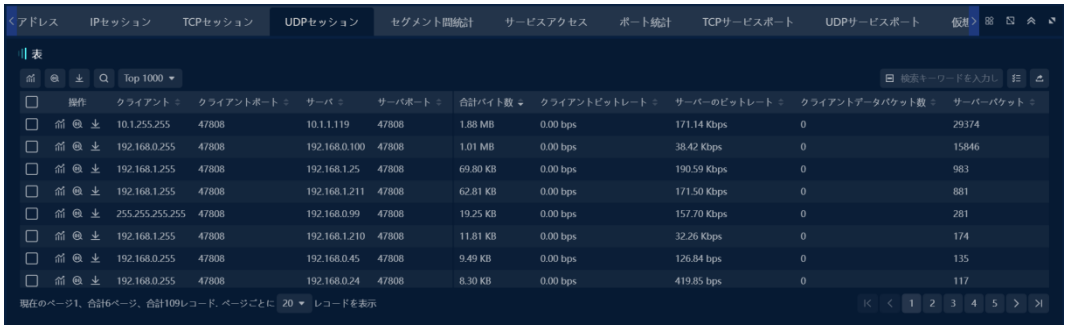
次の図に示すように、TCP セッションビューでは、選択した期間の TCP セッション情報の統計と表示が実行されます:

図 7.29 TCP セッションビュー

6.2.15 UDP セッション

次の図に示すように、UDP セッションビューでは、選択した期間の UDP セッション情報の統計と表示が実行されます:

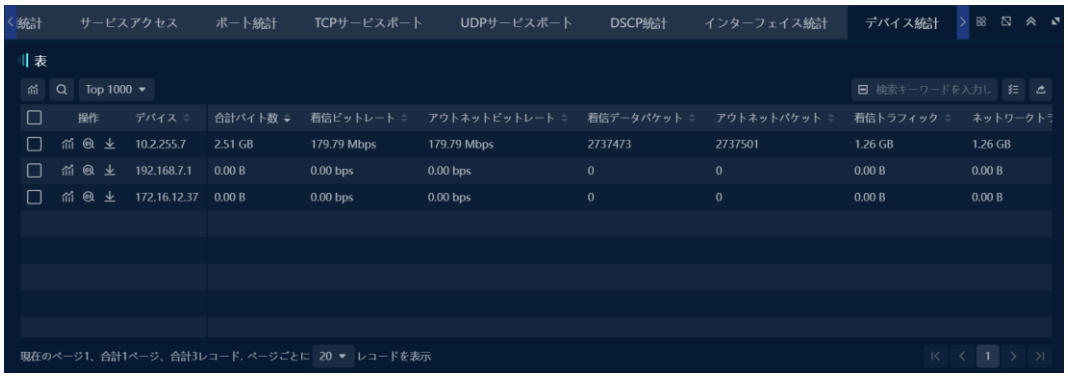
図 7.30 UDP セッションビュー



6.2.16 デバイス統計

NETFLOW リンクと SFLOW リンクは、次の図に示すように、選択した期間のデバイス情報がカウントおよび表示されるデバイス統計ビューの表示をサポートします:

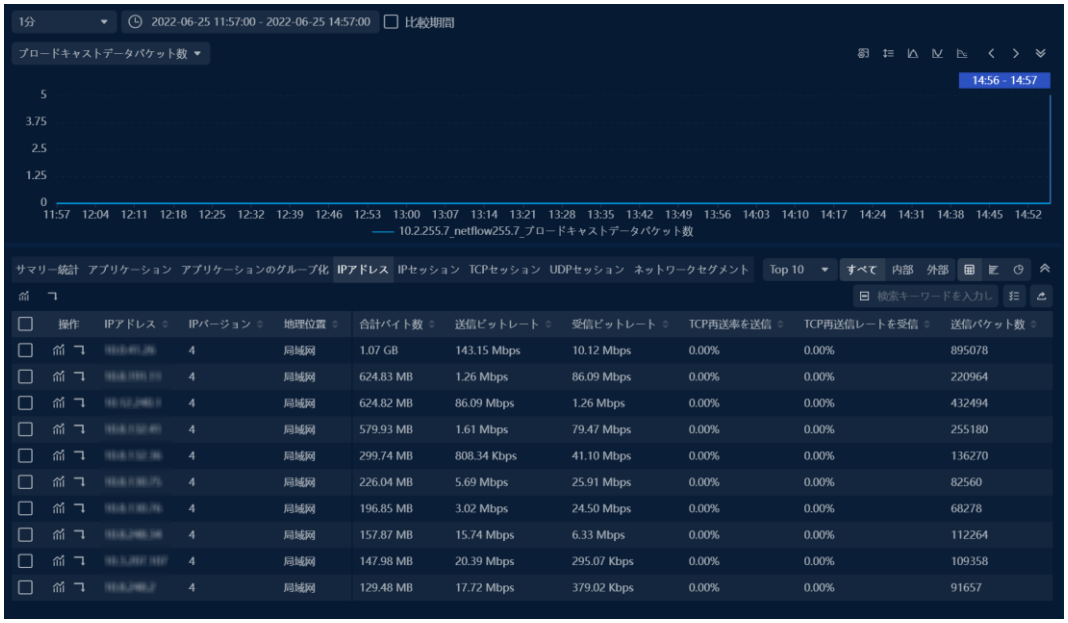
図 7.31 デバイス統計ビュー



行 デバイスビューでは、1 つまたは複数のデバイスに対してトレンド分析を うことができます。トレンド分析を行う必要があるデバイスを選択し、ボタ ンをクリックして、デバイスのトレンド分析インタフェースに入ります。

ク トレンド分析により、下図に示すように、デバイスに関連するネットワーアプリケーション、TCP セッション、UDP セッション、ネットワークセグメント、アプリケーションパケット、IP アドレス、IP セッション情報を迅速にマイニングすることができます。

図 7.32 設備動向分析



6.2.17 インターフェース統計

NETFLOW リンクと SFLOW リンクは、次の図に示すように、統計を収集し、選択した期間のインターフェイス情報を表示するインターフェイス統計ビューをサポートします:

図 7.33 インターフェース統計ビュー

インタフェース・ビューでは、1 つ以上のインタフェースについてトレンド分析を行うことができます。トレンド分析が必要なインタフェースを選択し、 ボタンをクリックして、インタフェースのトレンド分析インタフ

ェース　に入ります。

トレンド分析マイニングにより、次の図に示すように、インタフェースに関　連するネットワークアプリケーション、IP アドレス、通信アドレス、サービ　スアクセス、DSCP 統計、ネットワークセグメント、TCP セッション、UDP　　セッション、IP セッション情報を迅速にマイニングすることができます。

図 7.34 インタフェーストレンド解析

6.3 オブジェクト分析

Colasoft nChronos はアプリケーション、IP アドレス、IP セッションのオブジェクト分析をサポートし、異なるオブジェクトに対して異なる分析テンプレートを提供している。

6.3.1 应用对象分析

アプリケーション統計ビューで操作カラムのボタンをクリックし、次の図に示すようにアプリケーションオブジェクト解析インタフェースに進

みます。

図 7.35 応用対象分析

6.3.2 IP 地址対象分析

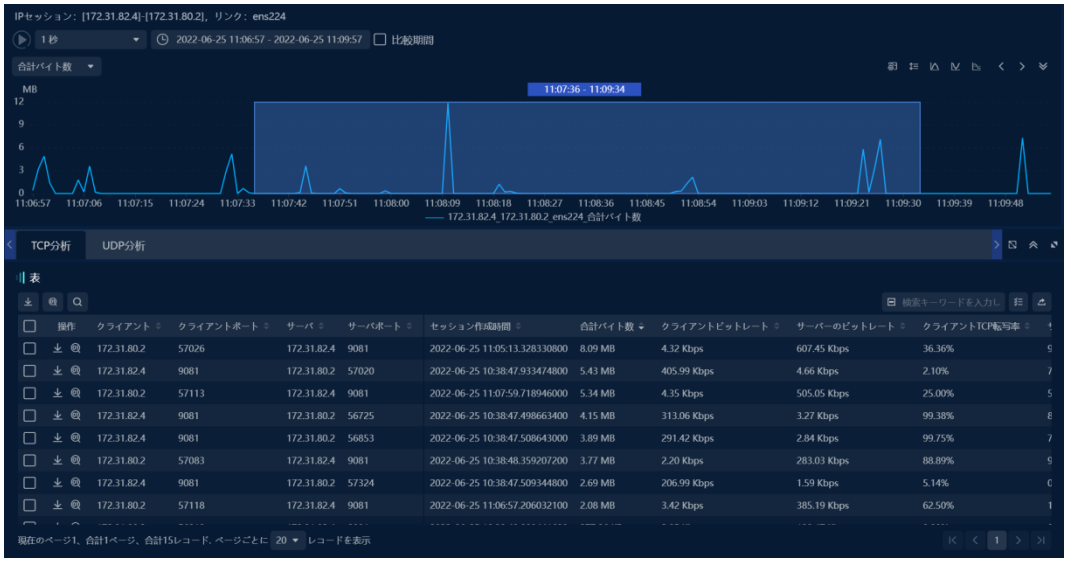
IP アドレス統計ビューで操作列のボタンをクリックして、次の図に示すように IP アドレスオブジェクト解析インタフェースに入ります。

図 7.36 IP アドレスオブジェクト解析

6.3.3 IP 会话对象分析

IP セッション統計ビューで操作列のボタンをクリックして、次の図に示すように IP セッションオブジェクト分析インタフェースに入ります。

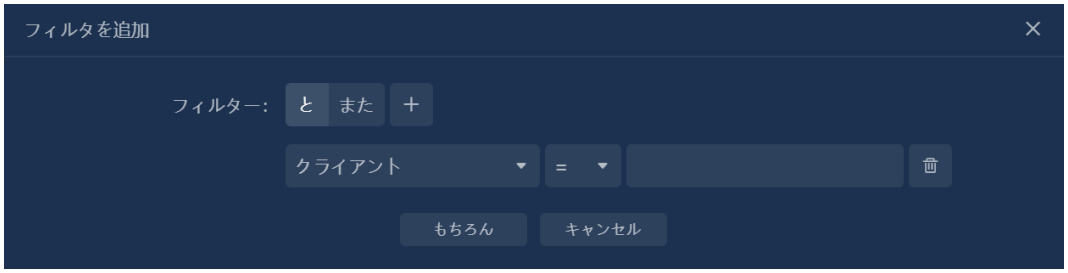
図 7.37 IP セッションオブジェクト解析



6.4 完全な検索と並べ替え

リンクトラフィック分析統計テーブルは、完全な検索機能をサポートしています。統計テーブルの上にある検索ボタンをクリックすると、次の図に示すようなダイアログボックスが表示されます。

図 7.38 フィルター条件の追加



ポップアップボックスに 1 つ以上のフィルター条件を追加できます。フィルター条件は AND または OR の関係であり、システムはフィルター条件に従って完全な検索を実行します。

統計テーブルのインジケーター名をクリックして、選択した列に従って統計テーブル内のすべてのデータを並べ替えます。

6.5 インジケーターの配置

統計テーブルに表示されるインジケーターについては、次の図に示すように、テーブルの右上隅にある[表示列の選択]ドロップダウンリストからインジケーターをすばやく見つけることができます。

図 7.39 インジケーターの配置

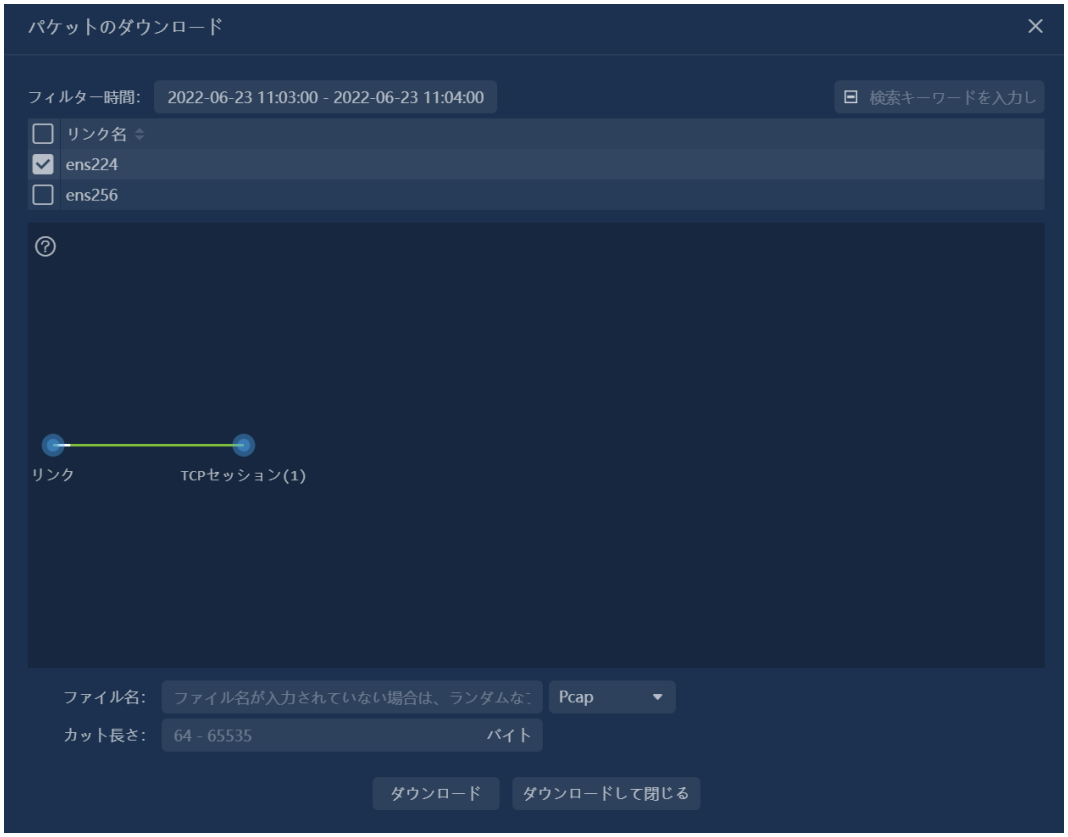
6.6 エントリの総数を照会

リンク統計テーブルは、エントリの総数のクエリをサポートしています。統計テーブルのエントリの総数をクエリするには、テーブルの上にある[トップ]オプションのドロップダウンリストから[すべて]を選択します。

6.7 データパッケージのダウンロード

オブジェクトを選択した後、「データパッケージのダウンロード」ボタンをクリックすると、次の図に示すように、データパッケージのダウンロードダイアログボックスがポップアップ表示されます。

図 7.40 パケットのダウンロード

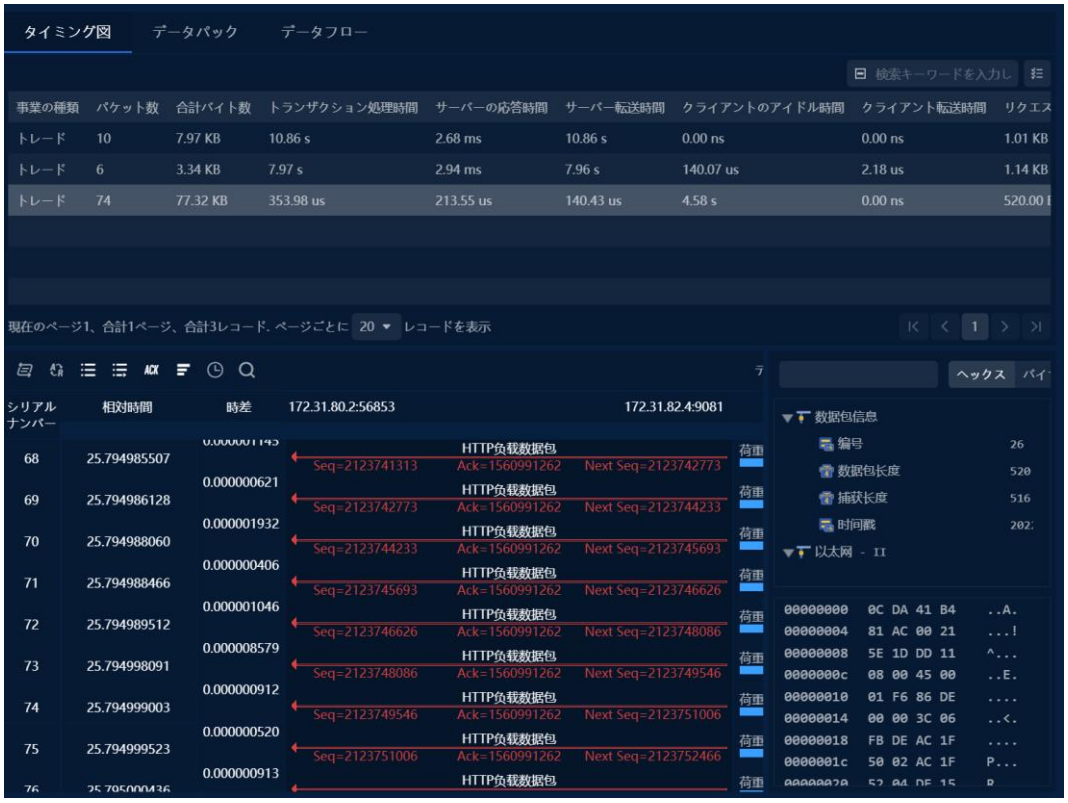


ポップアップボックスで、時間範囲の選択、フィルター条件の設定、ファイル名、ファイルタイプ、およびデータパケットのトリミングの長さを選択できます。

6.8 パケットデコード

オブジェクトを選択したら、次の図に示すように、[パケットデコード]ボタンをクリックしてパケットデコードページに入ります。

図 7.41 パケットのデコード



データパケットデコードページには、シーケンス図、データパケット、データフローの 3 つのタブがあります。

7 サブリンクの監視と分析

サブリンクの監視と分析ユーザー定義のサブリンクで監視と分析を実行します。

ネットワークセグメントアプリケーション

ネットワークアプリケーションビューでは、統計と表示は、システムに付属するアプリケーションとユーザー定義のアプリケーションで実行されます。

IP アドレス

IP アドレスビューでは、選択した期間の IP アドレスがカウントされ、イントラネットアドレス、エクストラネットアドレス、すべてのアドレス、および通信アドレスに従って表示されます。

IP セッション

IP セッションビューでは、選択した期間の IP セッション情報の統計と表示が実行されます。

DSCP 統計

DSCP 統計ビューは、監視対象リンクの DSCP トラフィック情報を表示するために使用されます。

8 アラートログ

nChronos はリンクアラートの集中クエリ機能を提供しています。アラート・　ログ・ビューでは、次の図に示すように、ネットワーク上のすべてのアラー　ト・ログを表示できます。

図 9.1 アラートログ

説明:

リンクでミリ秒トラフィック分析が有効になっている場合にのみ、リンクアラートにミリ秒トラフィックアラートタブが表示されます。

9 データマイニングと検索

nChronos は、高速で使いやすいデータマイニング機能を提供します。これにより、ユーザーはさまざまな視点やレベルから必要なデータをすばやくマイニングできます。

9.1 時間範囲によるマイニング

nChronos は、時間ベースのデータマイニングおよびフィルタリングテクノロジを提供し、タイムゾーンの選択、時間ウィンドウの選択、およびカスタム時間によって時間範囲を設定し、この時間範囲内の統計データをすばやくフィルタリングします。

タイムゾーンの選択

トレンドパネルでマウスをドラッグすると、タイムゾーンを選択できます。 トレンドグラフの任意の時点にマウスを移動し、左ボタンを押したまま左または右にドラッグして目的の位置に移動し、マウスの左ボタンを放します。灰色の網掛け部分が選択された時間領域であり、選択された時間はエリア内のすべての統計ビューデータに表示されます。

時間を調整する必要がある場合は、影付きの部分のタイムバーにマウスを移動し、選択した時間範囲をドラッグし、セレクターを移動して、選択した開始時刻と終了時刻をリアルタイムで表示および表示します。 同時に、シャドウ部分の 2 つの境界線も任意に調整できます。シャドウ部分の境界線にマウスを移動したとき、ポインタにマウスが移動したときに、境界線をドラッグしてより理想的な時間を設定できます。

時間枠の選択

トレンドパネルでは、1 秒、10 秒、1 分、5 分、10 分、1 時間、1 日など、さまざまなタイムスケールを使用できます。 タイムスケールが大きいほど、より多くの履歴データを表示できます。

カスタム時間

データマイニングと検索

ユーザーは時間をカスタマイズすることで、特定の期間のデータを表示できます。トレンドパネルの時間選択コントロールをクリックし、次の図に示すように、スプリングボックスで時間範囲選択を行います。

図 10.1 ウィンドウの時間範囲の設定

9.2 Web オブジェクトからのマイニング

nChronos は、ネットワークオブジェクトに基づくデータマイニングテクノロジーを提供します。ネットワークオブジェクトには、ネットワークアプリケーション、物理アドレス、ネットワークセグメント統計、ネットワーク間セグメント統計、アプリケーショングループ化、IP セッション、サービスアクセス、TCP サービスポート、UDP サービスポート、サービスが含まれます。ポート、VLAN 統計、VXLAN 統計、MPLS VPN 統計、DSCP 統計、および IP アドレス。 ユーザーは、ネットワークオブジェクトを介して階層データマイニングを実行できるため、ユーザーは特定の重要なデータをすばやくマイニングし、実際のネットワークの問題を解決できます。

9.3 データ検索

nChronos は、データ検索機能を提供します。データ検索は、キーワードのあいまい一致検索です。複数のキーワードを同時に検索でき、メモリ機能を備えています。検索速度が速く、データをすばやくフィルタリングして

検索できます。 。 データマイニングを行う場合、検索機能を合理的に使用することで、ユーザーは表示する必要のあるデータをすばやく見つけることができます。

10 パケット再生分析

WEB 設定ページにリンクを追加した後、リンクを実行してデータパケットを再生します。 リアルタイムリンクと同様に、再生リンクは、ネットワークリンクの遡及的分析のリアルタイム監視と遡及的分析を実行できます。

11 共通情報クエリ

このセクションでは、サーバー情報、ネットワークリンク構成、ユーザー情報、インターフェイス構成、ポート設定、アラーム通知パラメーター、監査ログのクエリなど、一般的な情報のクエリ操作について説明します。

11.1 サーバー情報の照会

サーバ情報には、製品名、サーババージョン、サーバモデル、ライセンス情報が含まれます。その中の許可情報には、アクティブ化状態、サーバシリアル番号、ソフトウェア期限、サービス期限、許可ユーザー、最大ストレージスペース、最大分析トラフィック、最大ネットワークインタフェース数、最大ネットワークリンク数、最大コンソール接続数、最大トランザクション分析数、製御局多段分析、コンソール非アクティブ化、VoIP 監視も含まれています。

サーバー情報を照会する手順は次のとおりです:

1. 管理者アカウントとしてサーバーの Web 構成ページにログインします。
2. 左側のナビゲーションツリーで[サーバー情報]を選択して、[サーバー情報]ページに入ります。
3. 次の図に示すように、サーバーの関連情報を照会します:

図 12.1 サーバー情報

共通情報クエリ

基本情報	
サーバーネーム:	Colasoft nChronos（試験機）
サーバーバージョン:	V7.0 (build 6.3.0.20026_git27c5f4c7_C7_avx2)
サーバーモデル:	[redacted]

認証情報	
アクティブ状態:	アクティベーション
サーバーシリアル番号:	[redacted] 再アクティブ化
ソフトウェア期間:	制限
サービス期間:	[redacted]
許可ユーザー:	[redacted]
最大ストレージ容量:	64000GB
最大分析トラフィック:	6000Mbps
ネットワークインターフェイスの最大数:	12
ネットワークリンクの最大数:	12
コンソール接続の最大数:	8
貿易分析の最大数:	3
マルチセグメント分析をコンソール:	無効
無料のアクティベーションをコンソール:	有効
VoIPモニタリング:	無効

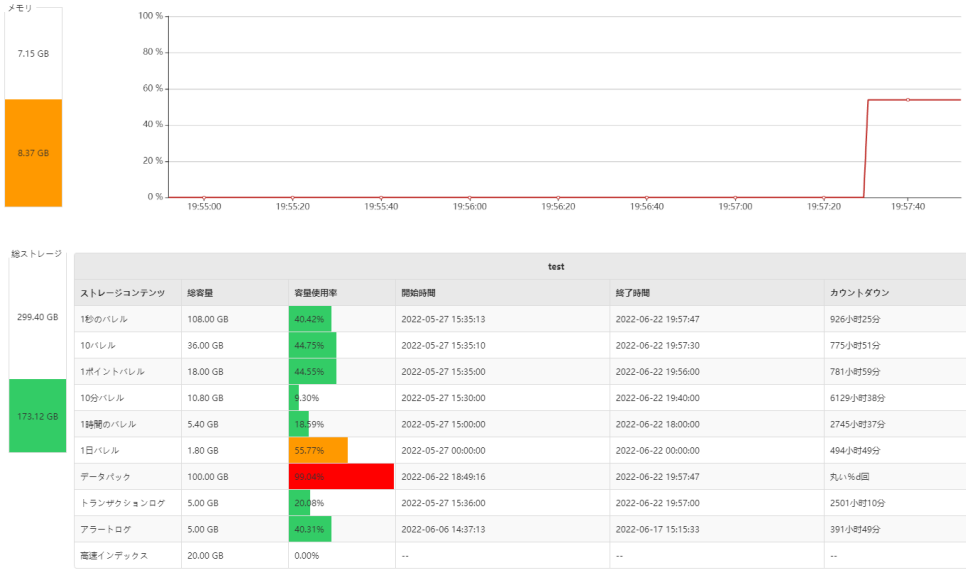
11.2 サーバーの実行ステータスのクエリ

サーバーの実行ステータスには、開始時間、実行時間、CPU 使用率、メモリ、使用可能なメモリ、メモリ使用量、ディスク容量の構成、ディスクの残り容量、およびディスク容量の占有率が含まれます。

サーバーの実行ステータスを照会する手順は次のとおりです:

1. 管理者アカウントとしてサーバーの Web 構成ページにログインします。
2. 左側のナビゲーションツリーで[サーバーステータス]を選択して、[サーバーステータス]ページに入ります。
3. 次の図に示すように、サーバーの関連する実行ステータス情報を照会します:

図 12.2 サーバーの実行ステータス



11.3 ユーザー情報の照会

ユーザー情報には、ユーザー名、ユーザータイプ、ユーザーステータス、作成時間、備考、および現在のユーザーが実行できる操作が含まれます。

ユーザー情報を照会する手順は次のとおりです:

1. 管理者アカウントとしてサーバーの Web 構成ページにログインします。
2. 左側のナビゲーションツリーで[ユーザー管理]を選択して、[ユーザー管理]ページに入ります。
3. 次の図に示すように、ユーザーの関連情報を照会します。

図 12.3 ユーザー情報

11.4 構成インターフェース情報の照会

インタフェース情報には、インタフェース名、インタフェースステータス、接続速度、インタフェースタイプが含まれます。「インタフェースを構成」タイプのインタフェースであれば、構成インタフェースの名前、IP アドレスとマスク、ゲートウェイアドレス、DNS サーバアドレスを問い合わせることができます。

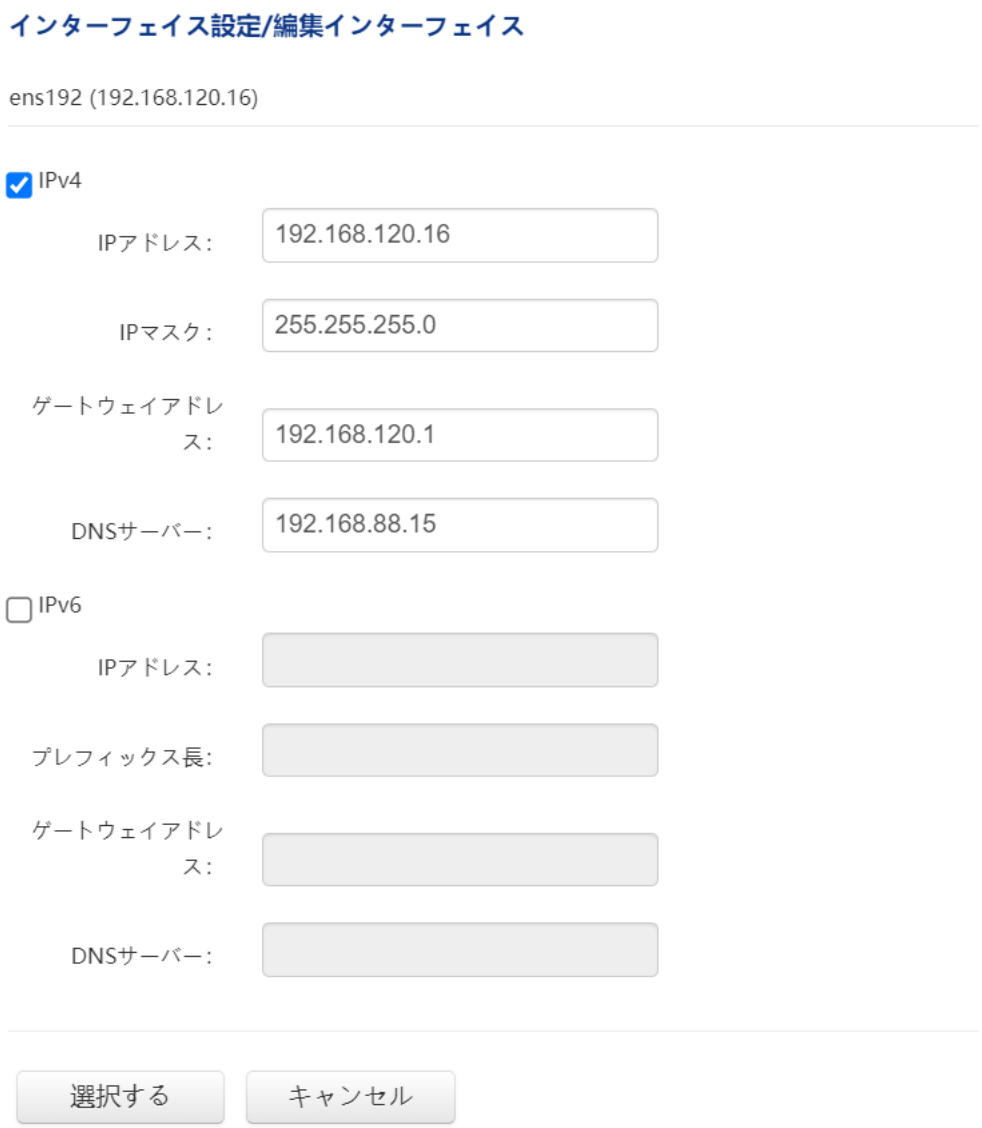
構成インターフェース情報を照会する手順は次のとおりです:

1. 管理者アカウントとしてサーバーの Web 構成ページにログインします。
2. 左側のナビゲーションツリーで、[インターフェイス構成]を選択して、[インターフェイス構成]ページに入ります。
3. 次の図に示すように、インターフェイスの関連情報を照会します:

図 12.4 インターフェース設定

4. インターフェースタイプが「構成インターフェース」の場合、次の図に示すように、「編集」ボタンを使用して管理ポートの IP アドレスを設定できます:

図 12.5 インターフェース設定の構成



11.5 ストレージ構成情報の照会

ストレージ構成情報には、遡及分析システムの合計ストレージスペース、および統計データ、データパケット、アラームログ、およびトランザクションログが占めるストレージスペースの割合が含まれます。

ストレージ設定情報を照会するための操作手順は次のとおりです:

1. 管理者アカウントとしてサーバーの Web 構成ページにログインします。

2. 左側のナビゲーションツリーで[ストレージ構成]を選択して、[ストレージ構成]ページに入ります。
3. 次の図に示すように、ストレージ構成関連の情報を照会します:

図 12.6 ストレージ設定

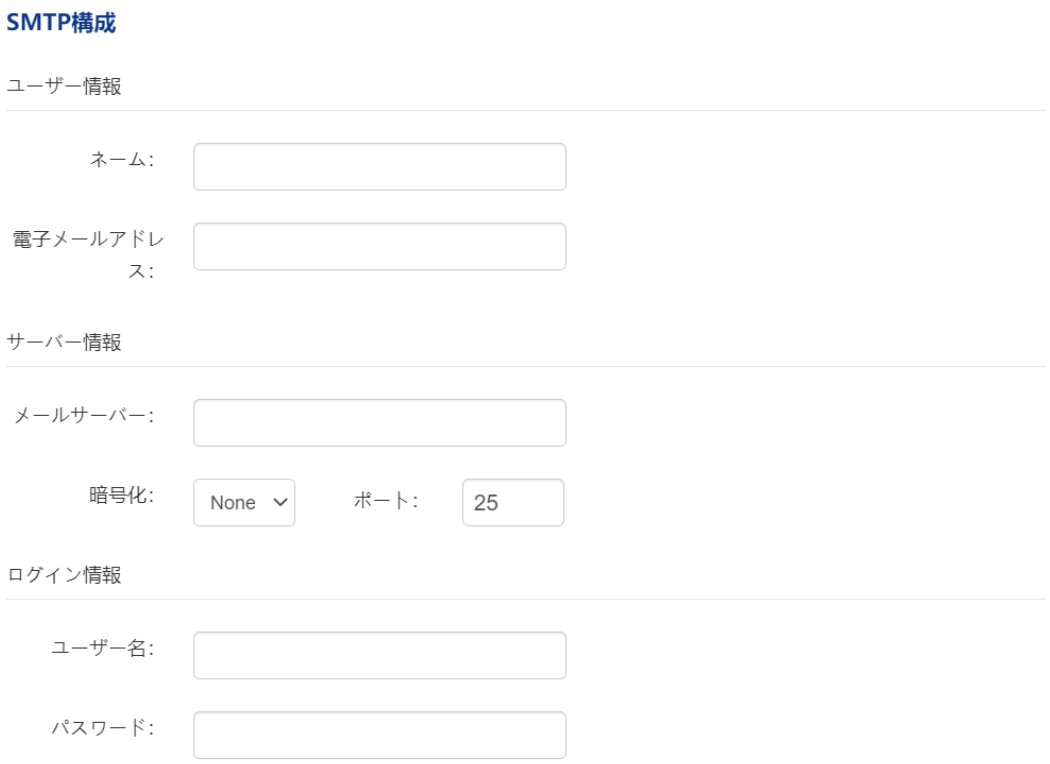
11.6 SMTP 構成情報の照会

SMTP サーバーは、SMTP プロトコルに準拠し、送信メールを送信または転送するために使用される送信メールサーバーです。 SMTP サーバーが正しく設定されている場合にのみ、システムは指定された受信者のメールボックスにアラートとレポートを送信できます。

SMTP 設定を照会する手順は次のとおりです。

1. 管理者アカウントとしてサーバーの Web 構成ページにログインします。
2. 左側のナビゲーションツリーで[SMTP 構成]を選択して、[SMTP 構成]ページに入ります。
3. 次の図に示すように、SMTP サーバーパラメータの設定をクエリします:

図 12.7 SMTP 構成



11.7 アラーム送信構成情報の照会

アラーム送信設定には、アラーム受信者設定と SYSLOG パラメータ設定が含まれます。システムでアラームが発生すると、システムは自動的に指定されたメールボックスに電子メールでアラーム情報を送信し、ログで SYSLOG サーバーに送信します。

アラーム送信設定を照会する手順は次のとおりです:

1. 管理者アカウントとしてサーバーの Web 構成ページにログインします。
2. 左側のナビゲーションツリーで、[アラーム送信]を選択して[アラーム送信]ページに入ります。
3. 次の図に示すように、アラーム送信パラメータの設定を照会します:

図 12.8 アラート送信の構成

11.8 構成情報を送信するクエリレポート

レポート送信設定には、レポートテンプレート設定とレポート受信者アドレス設定が含まれます。

レポート送信設定を照会する手順は次のとおりです:

1. 管理者アカウントとしてサーバーの Web 構成ページにログインします。
2. 左側のナビゲーションツリーで、[レポート送信]を選択して[レポート送信]ページに入ります。
3. 次の図に示すように、レポート送信パラメーターの設定を照会します:

図 12.9 レポート送信構成

11.9 監査ログ情報のクエリ

監査ログ情報には、ログタイプ、ログ時間、ユーザー、およびイベントが含まれます。 監査ログを介して、nChronos でユーザーが実行した操作を照会できます。

監査ログ情報を照会する手順は次のとおりです:

1. 管理者または監査人アカウントとしてサーバーの Web 構成ページにログインします。
2. 左側のナビゲーションツリーで[監査ログ]を選択して、[監査ログ]ページに入ります。
3. 次の図に示すように、ログの種類ごとにログをフィルタリングしてダウンロードするか、時間範囲を選択できます:

図 12.10 監査ログ