WebSAM Network Management
Web コンソール
リファレンスマニュアル

著作権

商標

はじめに

このたびは、WebSAM のネットワーク運用管理製品をお買い求めいただき、誠にありがとうございます。WebSAM のネットワーク運用管理製品では、WebSAM Integrated Management Server (以下、IMS と示す) コンポーネントを活用することで、複数製品の情報、操作を 1 つの Web コンソールでシームレスに統合し、運用することができます。

本書では、IMS コンポーネント (バージョン 4.0) を利用した Web コンソールの機能、および、操作の詳細について説明しています。Web コンソールを用いて、効率的にネットワーク運用を行うために、本書を活用してください。

本書の構成

本書の構成は、以下の通りです。表の対象者を参考にして読み進めてください。

表　本書の構成

管理者 

Web コンソールのすべての利用者

タイトル	内容	対象者
「第 1 章　Web コンソールの概要と基本操作（1 ページ）」	Web コンソールの機能概要と基本的な操作方法について説明します。	User
「第 2 章　運用前の環境設定（33 ページ）」	Web コンソールを利用する前に必要となる環境設定の方法について説明します。	Admin
「第 3 章　運用時の各種設定（72 ページ）」	Web コンソールを利用した運用時に、必要に応じて行う環境設定の方法について説明します。	Admin
「第 4 章　運用操作（112 ページ）」	Web コンソールによる運用操作の方法について説明します。	User
「第 5 章　システムメンテナンス（178 ページ）」	Web コンソールの利用環境に対するメンテナンス方法について説明します。	Admin
付録	Web コンソールを利用した運用における補足情報について説明します。	Admin
用語集 (「A - Z（245 ページ）」,「あ - わ（248 ページ）」)	Web コンソールの各種機能および本書で使用している用語、略語について説明します。	User

本書の表記規則

本書では、注意すべき事項や補足事項について、以下の表記を用います。

表　注意補足事項の表記

表記	説明
⚠ **注意** ————	機能設定、操作を行う上で守らなければならない事柄や特に注意すべき点を示します。
ヒント ————	知っておくと役に立つ便利な情報を示します。

本書では、以下の表記規則に従って記述しています。

表　表記規則

表記	説明	例
[**item**]	メニュー、項目名、ボタンなどの画面要素を示します。	[**ダッシュボード**]メニュー、[**OK**]ボタン
<*userinput*>	ユーザー環境により変化する項目、および入力値を示します。	<*%インストールパス%*>、<*filepath*>
`configuration file`	設定ファイルの記述内容を示します。	以下の値を設定します。 `port = 27120`
`command line`	コマンドライン操作を示します。	以下のコマンドを実行します。 `> Setup.exe`

本書では、以下の略称を用いて記述しています。

表　略称表現

正式表記	略称表現
WebSAM Integrated Management Server	Integrated Management Server、IMS
WebSAM NetvisorPro V	NetvisorPro
WebSAM Network Flow Analyzer	NFA
WebSAM NetvisorPro V Event Adapter	Event Adapter
WebSAM SystemManager G	SystemManager G

Web コンソールを利用する際に IMS コンポーネントをインストールする必要があります。IMS コンポーネントのインストールパスのデフォルト値は以下となります。

デフォルトのインストールパス(Windows 環境):

C:\Program Files\NEC\IMS

デフォルトのインストールパス(Linux 環境):

/opt/nec/ims

本書では、上記のインストールパスを<*%インストールパス%*>と記述します。インストールパスを変更している場合は、適宜読み替えてください。

IMS コンポーネントのインストールの際に、IMS コンポーネントが管理するデータの格納先をインストールパスとは異なるディレクトリに設定することができます。本書では、この場合のデータの格納先を<*%データパス%*>と記述します。インストールパスとデータパスを

分離していない場合は、*<%データパス%>*と*<%インストールパス%>*は、同じディレクトリを指します。

本書では、OS の種別によらず、ディレクトリ記号として"\"を使用している箇所があります。Linux 環境の場合は、"/"と読み替えてください。

目次

第 1 章
Web コンソールの概要と基本操作

Web コンソールの機能概要と基本的な操作方法について説明します。

目次

1.1　Web コンソールの概要

Web コンソールの利用目的や機能概要について説明します。

1.1.1　Web コンソールの利用目的

Web コンソールでは、任意の端末から Web ブラウザーを用いて、リモートから運用する仕組みを提供します。また、ネットワークの監視、分析、制御を担う個々の製品での運用をシームレスに統合し、ネットワーク運用のライフサイクル管理業務を効率化するための仕組みを提供します。

Web コンソールは、以下のような運用を行いたい場合に活用することができます。

- 任意の端末からネットワーク状況を確認したい場合

  Web コンソールは、Web ブラウザーを利用しているため、クライアントソフトウェアのインストールは必要ありません。そのため、緊急時に、任意の端末の Web ブラウザーを利用してネットワーク状況の確認を行うことができます。

  例えば、NetvisorPro を利用している場合、Web による通信が許可された環境であれば、リモートから Web コンソールにアクセスし、各ノードの状態や障害の影響範囲の確認を行うことができます。

- 複数の WebSAM のネットワーク運用管理製品を統合して運用したい場合

  Web コンソールは、複数製品の管理情報を一箇所に統合して見ることができます。ネットワークの全体状況を把握する際に、各製品が提供する個々の画面を確認する必要はなくなり、効率的に管理業務を行うことができます。

  例えば、複数配置した NetvisorPro の管理情報の統合や、NetvisorPro と NFA の情報の統合を行うことができます。

ヒント

Web コンソールは、イベントの発生状況の確認や、各ノードの性能情報の確認、分析など、定常的に行う運用に対して、活用することができます。しかしながら、各製品が提供するすべての機能操作を行えるわけではありません。必要に応じて、各製品が提供する管理コンソールと使い分けて運用してください。

1.1.2　Web コンソールの機能概要

Web コンソールで提供する機能の概要について説明します。

ダッシュボード

- 現在のネットワーク性能やイベントの発生状況を即座に把握することができます。
- 表示する内容は観点毎に複数定義することができ、プルダウンメニューで切り替えることによって、様々な観点での状況把握が行えます。

- グラフや一覧を表示する構成要素である[**ウィジェット**]をドラッグ&ドロップの直観的な操作で自由に配置していくことで、運用にあったダッシュボード定義を簡単に作成することができます。

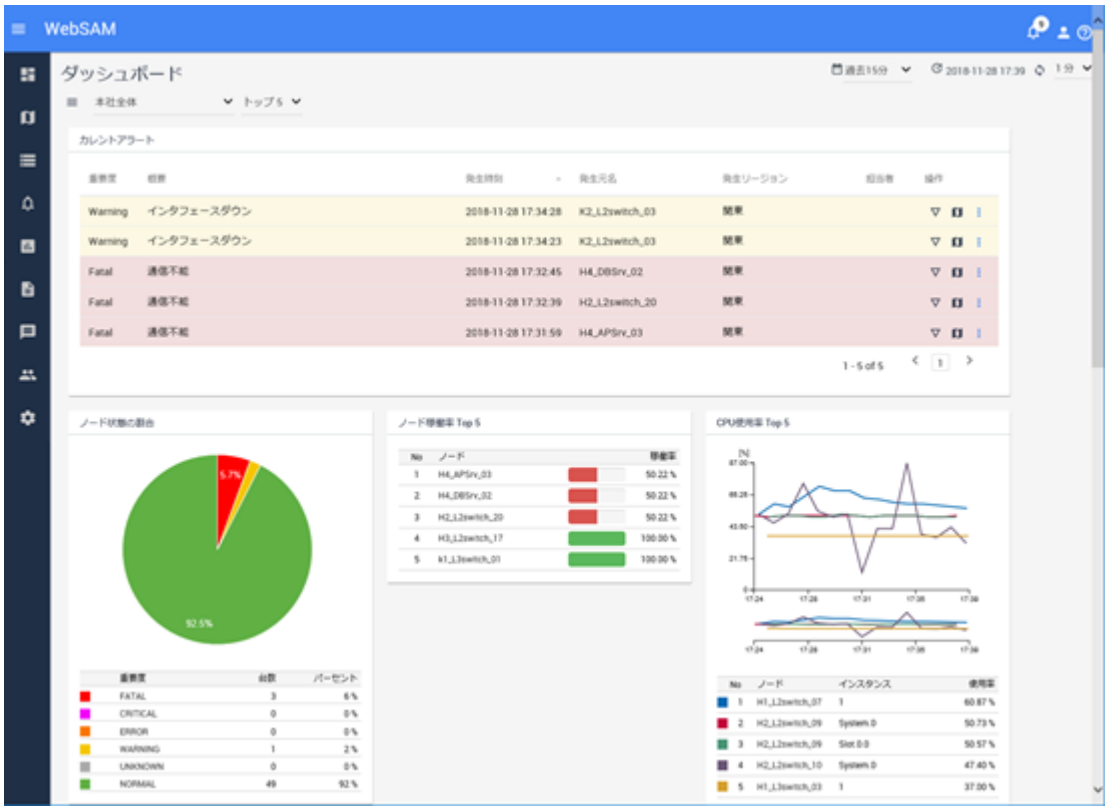

図 1-1　ダッシュボード表示

ノード管理・分析

- NetvisorPro の管理対象ノードや NFA のエクスポーターなどを 「ノード」 として管理し、複数製品で同一とみなせるノードの情報は、1 つに統合して管理します。
- すべての管理対象ノードの中から、特定の条件に合致するノードを見つけ出し、プロパティ情報の確認、比較を行うことができます。
- ノード毎のダッシュボード(ノード詳細画面)により、指定したノードのプロパティ情報や負荷状況を詳細に確認、分析することができます。また、ネットワークインターフェイス毎のダッシュボード(ネットワークインターフェイス詳細画面)により、指定したネットワークインターフェイスのプロパティ情報や通信状況を詳細に確認することができます。

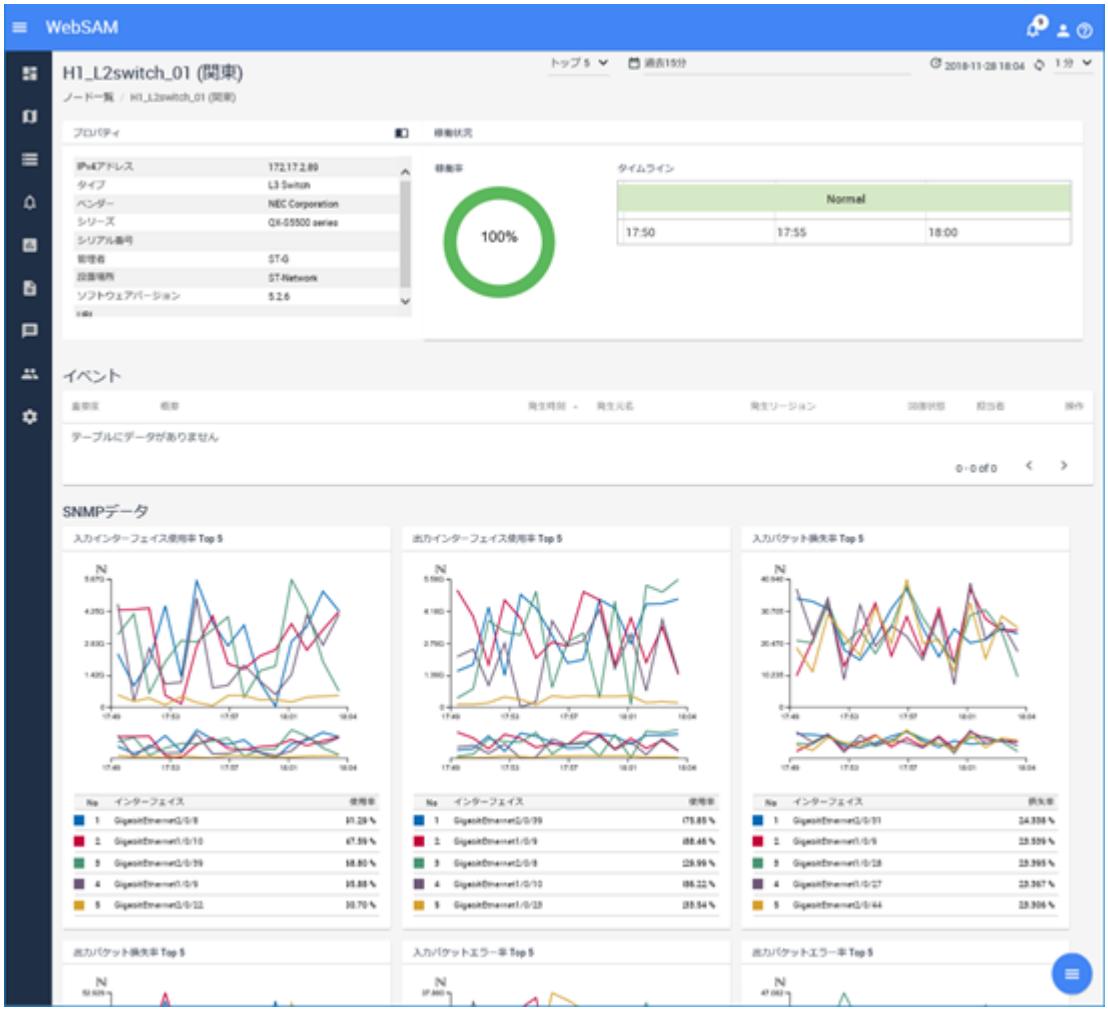

図 1-2　ノード詳細表示

トポロジーマップ(NetvisorPro 利用時)

- ノード間の物理的な接続関係や、建物、フロア毎での配置状況などをトポロジーマップとして表示し、障害時の影響範囲の確認作業などを支援します。トポロジーマップでは、背景画像の挿入などネットワーク構成の把握を容易にする様々な編集機能を提供しています。
- ノードのプロパティや性能情報をマップを見ながら確認する仕組み(サイドパネル)を提供しています。マップ上で関連し合うノードを 1 つ 1 つ確認していくような調査の際に、活用することができます。
- トポロジーマップを[**分析モード**]で表示することで、過去の時間帯の各ノードのイベント重要度がどのような状況だったかを確認することができます(タイムライン機能)。例えば、昨夜発生し、現時点で回復状態のイベントに対し、マップ上で昨夜の時間帯にさかのぼり、発生イベントの影響範囲をマップ上で可視化することで、当時の状況を把握することに役立てられます。

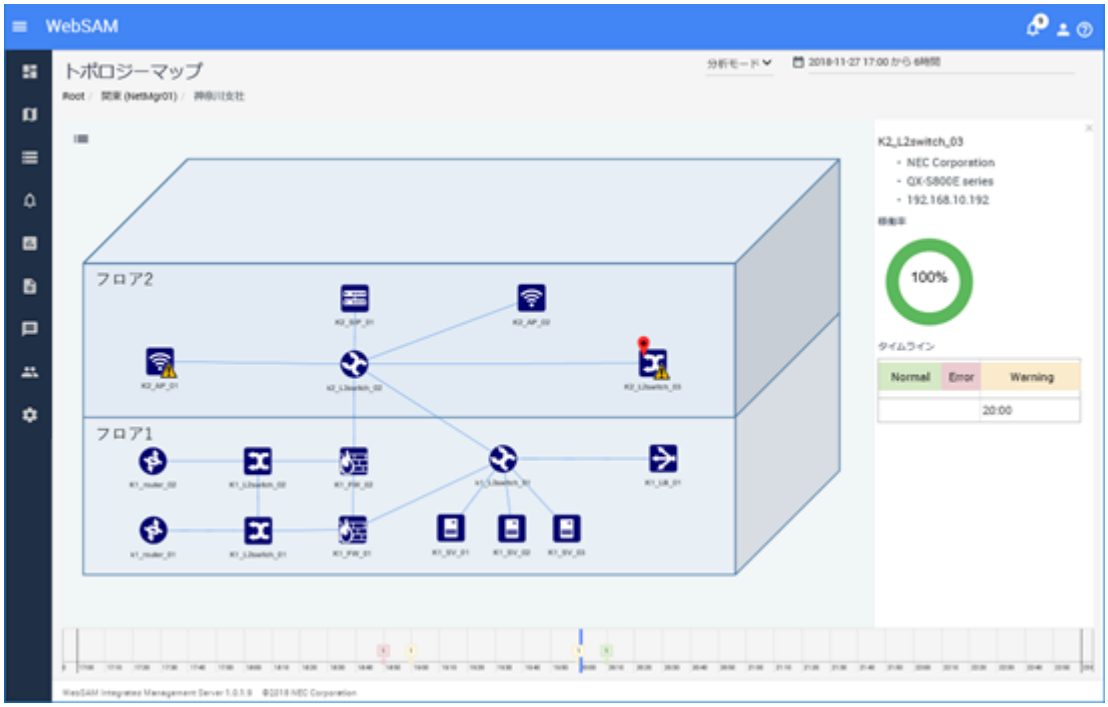

図 1-3　トポロジーマップ表示

イベント監視

- NetvisorPro で検知したアラートや NFA で検出した通信量のしきい値超過のイベントを「イベント」として統合的に管理します。また、イベントから当該ノードの詳細情報を確認したり、トポロジーマップにジャンプしたり、イベントを中心とした調査操作もスムーズに行うことができます。
- 発生イベントは一覧で概要を確認することができ、また、指定した条件で表示内容を絞り込むことで、必要な情報のみを確認することができます。ダッシュボード画面に[**カレントアラート**]ウィジェットを配置することで、現在発生中の障害イベントの状況を即座に把握することも可能です。
- 発生イベントの内容に対する条件定義を行うことで、イベント発生を契機としたメール送信やコマンド実行などのアクションを実行することができます。関係者への一斉通知や、自動リカバリ制御などに活用することができます。

図 1-4　イベント一覧表示

データ分析

- NetvisorPro を用いて装置の MIB から収集したデータや NFA が受信した通信フローのデータに対し、アノマリー分析、トレンドライン分析の 2 つの分析機能を提供します。
- アノマリー分析は、一定のしきい値による監視とは異なり、データの普段とは異なる不穏な挙動を検出すること(アノマリー検知)ができるため、ネットワークシステムの異常に関する予兆検知として活用することができます。
- トレンドライン分析は、これまでに蓄積してきたデータの増減傾向の分析結果から、数ケ月後のデータ状況を予想することができるため、リソースのキャパシティ管理の指標として活用することができます。

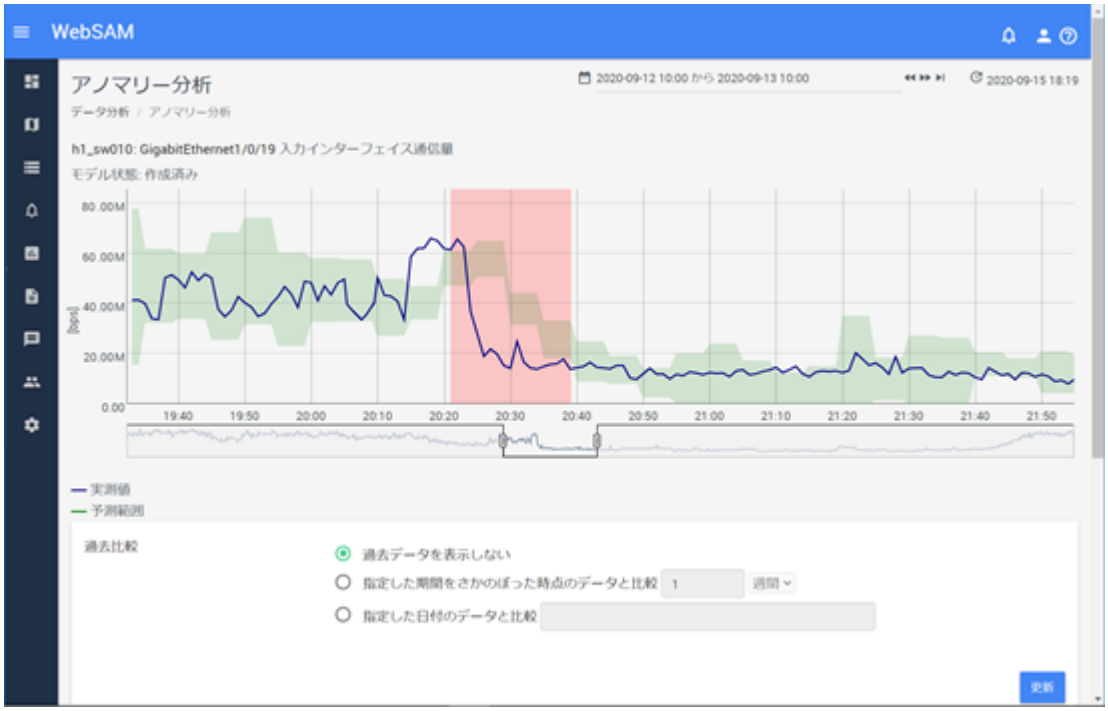

図 1-5　アノマリー分析

1.1.3　システム構成

Web コンソールを利用するためのシステム構成について説明します。

Web コンソールを利用するためには、IMS コンポーネントをセットアップし、IMS コンポーネントと WebSAM のネットワーク運用管理製品とを接続する必要があります。この接続のためには、IMS コンポーネント上に製品別の連携アプリケーションを追加インストールした上で、製品ごとの設定を行う必要があります。

IMS コンポーネントと複数の製品を接続する場合は、同一ノードを管理対象に含んでいる製品をリージョンというグループでグルーピングします。

例えば、ノード 1~45 を管理する NetvisorPro と、ノード 40~50 をエクスポーターとして管理する NFA とが存在する環境の場合は、管理するノードが、ノード 40~45 の範囲で重複しているので、この 2 つの製品を同じリージョングループとします。2 つの製品で管理するノード 40~45 の情報は、Web コンソール側で統合され、見ることができます。

複数のリージョングループで構成するシステム構成例を「図 1-6 システム構成図（8 ページ）」に示します。

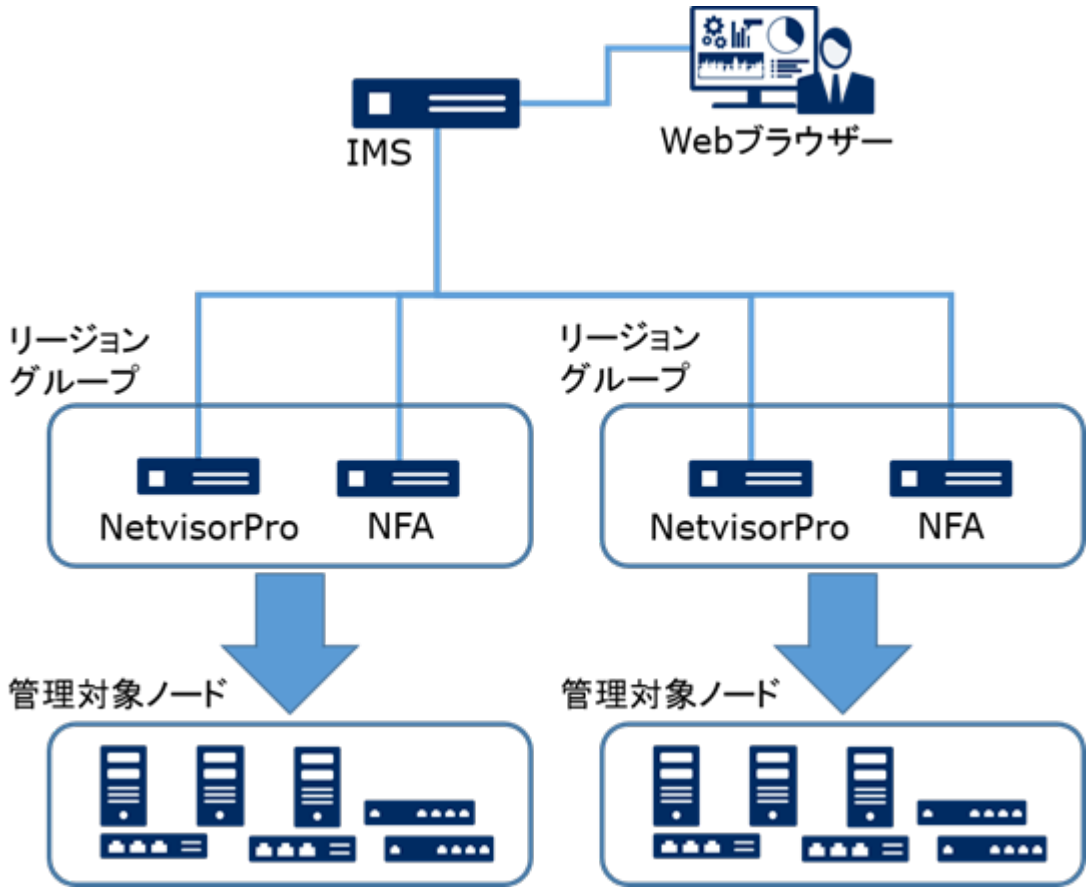

図 1-6　システム構成図

ヒント

- IMS コンポーネントと NetvisorPro などの WebSAM のネットワーク運用管理製品とは、同じサーバーにインストールして、システムを構築することができます。
- IMS コンポーネントと複数製品を同一サーバーにインストールする構成をとった場合は、Web コンソールの操作に対する応答が遅いなどの問題が発生する可能性があります。十分に検証した上で、運用を開始してください。また、可能な限り、利用する製品を複数サーバーに分散してインストールする構成を推奨します。

1.2　Web コンソールの基本操作

Web コンソールに接続する方法、および、Web コンソールの基本的な操作方法について説明します。

1.2.1　Web コンソールを使用するための準備を行う

Web コンソールを使用するための準備作業について説明します。

Web コンソールを使用する前に、Web ブラウザー側の設定作業を行います。これらの作業は最初に 1 回だけ行います。

1.2.1.1　Web ブラウザーのセキュリティ設定を確認する

Web コンソールを使用するために必要な、Web ブラウザーのセキュリティ設定について説明します。

Web コンソールにアクセスするためには、Web ブラウザーで、JavaScript と Cookie が有効になっている必要があります。

サポートしている Web ブラウザーは、初期設定で JavaScript と Cookie は有効になっており、特別な設定なく使用することができます。設定を変更している場合は、Web コンソールを使用するのに適切な設定かどうか確認してください。

また、Windows Server で[**セキュリティ強化の構成**]を「有効」にしている場合は「Windows Server での設定（9 ページ）」の設定が必須となります。

Google Chrome の設定確認

Google Chrome の設定画面で確認を行います。[**詳細設定**]以下にある、[**プライバシーとセキュリティ**]セクションで確認を行うことができます。詳細な設定手順については、Google Chrome のヘルプを参照してください。

- [**プライバシーとセキュリティ**]セクション

  JavaScript の実行が許可されていること、Cookie を保存する設定になっていることを確認します。

Windows Server での設定

[**セキュリティ強化の構成**]を「有効」にしている場合は、インターネット オプションダイアログの設定で、「信頼済みサイト」に「about:blank」を追加してください。

1.2.1.2　Web ブラウザーに SSL サーバー証明書をインポートする

HTTPS を用いて、Web コンソールにアクセスする場合は、SSL サーバー証明書を Web ブラウザーにインポートします。

使用する SSL サーバー証明書に自己署名形式を選択した場合、証明書を Web ブラウザーにインポートすることで、Web コンソールに安全にアクセスすることができます。

ヒント

認証局に証明書を発行してもらう場合でも、認証局によっては、Web ブラウザーに認証局のルート証明書をインポートするよう、指示がある場合があります。その場合は、認証局からの指示に従ってください。

- Microsoft Edge および Google Chrome の場合は、以下の手順を実施します。

  1. 「A.1　ims-ssl-keytool（205 ページ）」の `exportcert` コマンドで出力した証明書 (.cer ファイル) を Web ブラウザーが動作する端末に配置します。

2. 証明書ファイルをダブルクリックします。
3. 表示された証明書ダイアログで、[**証明書のインストール**]ボタンをクリックします。

   [**証明書のインポートウィザード**]が表示されます。[**次へ**]ボタンをクリックします。
4. [**証明書をすべて次のストアに配置する**]を選択し、[**参照**]ボタンをクリックします。
5. 証明書ストアの選択ダイアログで、「信頼されたルート証明書機関」を選択し、[**OK**]ボタンをクリックします。
6. [**次へ**]ボタンをクリックします。
7. [**完了**]ボタンをクリックします。
8. 自己署名のため、セキュリティ警告が表示されますが、[**はい**]ボタンをクリックします。

正しくインポートされましたというダイアログが表示されれば、証明書のインポートは完了です。

1.2.2　Web コンソールにアクセスする

Web ブラウザーから Web コンソールにアクセスする手順について説明します。

Web コンソールにアクセスするために、以下の手順を実行します。

1. Web ブラウザーで、Web コンソールの URL を指定します。
   - HTTP 通信の場合の URL

     http://<IMS サーバーのドメイン名(FQDN)>/
   - HTTPS 通信の場合の URL

     https://<IMS サーバーのドメイン名(FQDN)>/

     <IMS サーバーのドメイン名(FQDN)>は、SSL サーバー証明書の作成時に入力した名前と一致している必要があります。一致していない場合、不正な証明書として警告が表示されます。

   ヒント
   - Web コンソールにアクセスするためには、URL に指定した<IMS サーバーのドメイン名(FQDN)>に対して、名前解決が可能な環境である必要があります。
   - Web コンソールにアクセスする通信のポート番号を変更している場合は、上記の URL に、変更後のポート番号を加えて指定してください。

     例： http://webconsole.co.jp:8080/

   Web コンソールに正しくアクセスできると、ログイン画面が表示されます。
2. ユーザー名、パスワードを入力し、Web コンソールにログインします。

Web コンソールへのログインが成功すると、ユーザーごとに設定したダッシュボード画面を表示します。

⚠ 注意

- Web コンソールへのログイン、および、操作に関する注意事項を以下に示します。
  - 初回のログイン時に、必ず、パスワードを変更してください。

    パスワードは、画面右上の[ ]をクリックして表示する [**プロファイル編集**] メニューから、プロファイル編集画面を表示して、変更します。
  - 30 分の間に、5 回以上のログイン失敗を検知すると、ユーザー情報がロックされた状態となり、当該ユーザーでのログインが、30 分の間できなくなります。

    ロックされた状態をすぐに解除したい場合は、アカウント管理者の役割を持つグループのユーザーによる操作で、ロックを解除することができます。
  - 設定情報の操作(追加、変更、削除)を、複数の Web コンソールから同時に行うことは可能ですが、同一画面に対し実施した場合は、データの整合性を保つために、後から実施した操作を失敗にする場合があります。
  - 各画面の入力欄の指定において、Unicode のサロゲートペア文字は、2 文字として扱われます。そのため、各入力欄に実際に入力できる文字数は少なくなります。
  - 画面表示において、連続した半角スペースは 1 つにまとめられて表示されます。そのため、以下のような点に注意してください。
    * 各種設定で指定する名前に連続した半角スペースを含めた場合、画面上に表示される名前が指定した名前と異なって見えてしまいます。
    * イベントの内容に連続した半角スペースが含まれていた場合、画面上に表示されている内容と各製品が提供する管理コンソールでの表示が異なって見えてしまいます。
    * 半角スペースが 1 つにまとめられて表示された文字列をコピーして検索条件のキーワードとして利用しても、適切に絞り込みができません。
- 接続する製品の Web コンソールへのシングルサインオンを有効にしている場合の注意事項を以下に示します。
  - IMS コンポーネントと接続する製品とで、同一名のユーザーを登録しておく必要があります。同一名のユーザーに対してのみ、シングルサインオンが有効に動作します。
  - IMS コンポーネントが停止している状態では、接続製品の Web コンソールにアクセスできない場合があります。この場合は、接続製品のログイン画面に直接アクセスする URL を指定して、Web コンソールにアクセスしてください。

1.2.3　Web コンソールの画面構成

Web コンソールの画面構成について説明します。

Web コンソールは、「図 1-7 Web コンソールの画面構成（12 ページ）」で示す 4 つの領域で構成されています。

図 1-7　Web コンソールの画面構成

ヘッダー領域

ログインしているユーザー名や新着イベントの状況などを表示します。

- [ ]アイコン

  メニュー領域の幅を最大化、または、最小化します。

- [**新着通知**]アイコン

  Web コンソールへのログイン後に発生した、イベントやメッセージの新着状況を表示します。

  表示する数字は、新着イベント、メッセージの件数を示しています。

  ヒント

  メッセージとは、Web コンソールの処理に対するエラーなどの通知のことを指します。

- [ ]アイコン

  クリックすると以下を表示します。

  - ユーザー名

    ログインしているユーザー名(表示名)を表示します。

  - [**プロファイル編集**] メニュー

    プロファイル編集画面を表示します。プロファイル編集画面では、ログインのための[**パスワード**]など、自身のユーザー情報の内容を変更することができます。

ヒント

初回のログイン時に、必ず、パスワードの変更を行ってください。

- [**ログアウト**] メニュー

  Web コンソールからログアウトします。

- [ **ヘルプ**]アイコン

  Web コンソールのヘルプを表示します。

メニュー領域

Web コンソールで操作可能な機能のメニューを表示します。

⚠ 注意

ログインしているユーザーの役割やシステムを構成する製品によって、表示するメニューの内容は変化します。

- [ **ダッシュボード**] メニュー

  ダッシュボード画面を表示します。現在の状況を確認することができます。

- [ **トポロジーマップ**] メニュー(NetvisorPro 利用時)

  トポロジーマップ画面を表示します。ネットワークの構成を確認することができます。

- [ **ノード一覧**] メニュー

  ノード一覧画面を表示します。すべての管理対象ノードの情報を確認することができます。

- [ **イベント**] メニュー

  イベント画面を表示します。発生したイベントの情報を確認することができます。

- [ **データ分析**] メニュー

  データ分析画面を表示します。分析対象の一覧や分析結果を確認することができます。

- [ **Syslog**] メニュー(NetvisorPro SyslogDiagnosis 機能利用時)

  Syslog 画面を表示します。蓄積している Syslog を検索、確認することができます。

- [ **イベントアクション設定**] メニュー

  クリックするとイベントアクション(通報処理)に関する以下のサブメニューを表示します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、メニューの表示や選択を行うことができます。

- [**イベントアクション**] メニュー

  イベントアクション画面を表示します。イベント発生を契機にした通報処理の設定を行うことができます。

- [**メールサーバー**] メニュー

  メールサーバー画面を表示します。メールでの通報を行う際のメールサーバーの設定を行います。

- [**アクションログ**] メニュー

  アクションログ画面を表示します。イベントアクションの実行ログを確認することができます。

- [**アカウント管理**] メニュー

クリックすると Web コンソールのアカウントに関する以下のサブメニューを表示します。

ヒント

アカウント管理者の役割を持つグループのユーザーのみ、メニューの表示や選択を行うことができます。

- [**ユーザー**] メニュー

  ユーザー画面を表示します。ユーザーの情報を管理します。

- [**グループ**] メニュー

  グループ画面を表示します。ユーザーの役割を定義するグループを管理します。

- [**システム設定**] メニュー

クリックするとシステム設定に関する以下のサブメニューを表示します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、メニューの表示や選択を行うことができます。

- [**ノードマッピング**] メニュー

  ノードマッピング画面を表示します。複数製品で管理するノードが物理的に同一かどうかを判別し、管理します。

- [**構成情報同期**] メニュー

構成情報同期画面を表示します。IMS コンポーネントと接続する製品との間で、構成情報の同期処理を行います。

- [**スケジュール**] メニュー

  スケジュール画面を表示します。運用を制御するスケジュールを設定することができます。

コンテンツ領域

選択したメニューに合わせた操作画面を表示します。

フッター領域

IMS コンポーネントのバージョン、および、コピーライトの情報を表示します。

1.2.4　自身のユーザー情報を更新する

Web コンソールにログインしたユーザーが、自身のログインパスワードを含むユーザー情報を更新する場合の手順について説明します。

ヒント

[**ユーザー名**]、および、[**グループ**]については、変更することができません。

1. プロファイル編集画面を表示します。

   画面右上の[]アイコンをクリックして表示する [**プロファイル編集**] メニューを選択します。

2. プロファイル編集画面で、必要に応じて、自身の表示情報を変更します。

   - [**表示名**]

     Web コンソール上の表示用ユーザー名を任意の文字で指定します。最大文字数は 128 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     省略した場合は、[**ユーザー名**]で指定した名前を表示名としても使用します。

   - [**初期表示ダッシュボード**]

     ユーザーがログインした時に、最初に表示するダッシュボード定義を、一覧のチェックボックスをオンにして選択します。

ヒント

事前にダッシュボード定義の追加を行っていない場合は、接続する製品が提供するビルトインダッシュボードの中から選択します。

変更内容を入力後、[**保存**]ボタンをクリックします。

指定した内容で情報が更新されたことを示すメッセージが表示されます。

3. 必要に応じて、パスワードを変更します。

   - [**パスワード(旧)**]

     現在のパスワードを指定します。

   - [**パスワード**]

     新しいパスワードを指定します。パスワードは、以下の文字を組み合わせて、8~64 文字の文字数で指定します。

     - 半角英大文字
     - 半角英小文字
     - 半角数字
     - 半角スペース と 以下の記号

       ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

     パスワードには、上記の 4 種類の文字のうち、3 種類以上の文字を含んでいる必要があります。また、過去 10 回分のパスワードとは異なっている必要があります。

   - [**パスワード(確認用)**]

     入力確認のため、[**パスワード**]で指定したものと同じパスワードを指定します。

   変更前、変更後のそれぞれのパスワードを入力後、[**パスワード更新**]ボタンをクリックします。

   指定した内容でパスワードが更新されたことを示すメッセージが表示されます。

4. Web API を利用する場合は、Web API アクセスキーを発行します。

   [**発行**]ボタンをクリックすると、Web API アクセスキーが発行されます。

   [**表示**]ボタンをクリックすると、発行された以下の 2 つの Web API アクセスキーが表示されます。

   - Access Key ID
   - Secret Access Key

   [**削除**]ボタンをクリックすると、発行された Web API ライセンスキーが削除されます。

1.2.5　新着イベントを確認する

Web コンソールでは、ダッシュボード画面および、イベント画面以外の画面を表示している場合であっても新規に発生したイベントの有無を把握することができます。

新規に発生したイベントの把握と、そのイベント内容を確認する手順について説明します。

1. 新着通知の有無を確認します。

   画面右上の[**新着通知**]アイコンの状態を確認します。

   表示している件数のイベント、または、メッセージが新規に発生していることを示します。

   ヒント

   メッセージとは、Web コンソールの処理に対するエラーなどの通知のことを指します。

2. [**新着通知**]アイコンをクリックします。

   通知一覧が表示されます。

3. 新着イベントの有無を確認します。

   イベントが発生していた場合は、通知一覧に、新着イベントの発生を示す通知が表示されます。また、合わせて、新着イベントに対する通知時刻と重要度の情報が表示されます。通知された重要度の情報から、イベントに対する緊急性を把握することができます。

   ヒント

   イベントに対しては、1 分間隔で発生有無をチェックし、通知します。そのため、新着イベントの通知時刻は、イベントの実際の発生時刻と比べて、最大で 1 分の遅れが生じます。

   同時に複数イベントの発生を検知した場合は、1 件にまとめた形式で新着イベントを通知します。このとき、通知される重要度は、まとめたイベントの中で最も高い重要度となります。

4. イベントの詳細な内容を確認します。

   イベントの詳細を確認する場合は、[**イベント**] メニューをクリックして、イベント画面に遷移します。新着イベントの通知時刻とイベント画面の表示情報を照らし合わせて、新着イベントの詳細な内容を確認します。

5. 内容確認済みのイベントを通知一覧から削除します。

   通知一覧の通知内容に対する[✕]アイコンをクリックすると、当該通知内容を通知一覧から削除することができます。通知一覧の[**通知をすべて削除する**]アイコンをクリックすると、通知一覧のすべての通知を削除することができます。

ヒント

通知一覧には、最大 10 件までの通知を行います。10 件を超える場合は、古い通知から削除していきます。

1.2.6　ウィジェットの種類

ダッシュボード画面、ノード詳細画面などの画面では、通信状況やノードの負荷状況、イベントの発生状況など、様々な情報をウィジェットと呼ぶ構成要素を用いて、グラフ表示、一覧表示しています。ここでは、Web コンソールで表示するウィジェットの種類について説明します。

ウィジェットは表示する内容から 4 つのタイプに分類することができます。

折れ線グラフ表示タイプ

対象項目の指定期間における値の時間的推移を折れ線グラフで表示します。また、一覧表示で、指定期間における各項目の順位を表示します。

例えば、[**入力インターフェイス使用率 Top5**]ウィジェットの表示の場合は、対象となるネットワークインターフェイスのうち、入力側の使用率(%)が高い 5 つのネットワークインターフェイスに対して、指定期間での使用率(%)の推移を折れ線グラフで表示します。一覧には、使用率の高い順に、5 つのネットワークインターフェイスに対する指定期間での平均使用率(%)の値を表示します。

折れ線グラフ表示タイプのウィジェットのイメージを「図 1-8 折れ線グラフ表示タイプのウィジェット（18 ページ）」に示します。

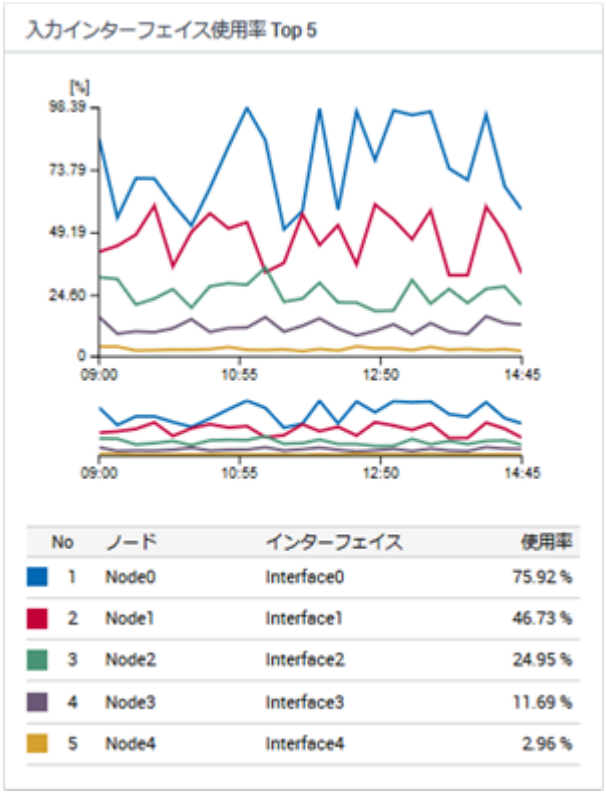

図 1-8　折れ線グラフ表示タイプのウィジェット

折れ線グラフ表示タイプのウィジェットでは、以下の表示操作を行うことができます。

- [**レンジセレクター**]によるグラフの拡大表示

折れ線グラフと一覧の間に配置する[**レンジセレクター**]を操作することで、折れ線グラフの時間幅を狭めることができ、グラフを拡大表示することができます。

- フィルタリング設定による表示項目の絞り込み

  一覧の各項目の左側に配置するグラフ色を示すマークをクリックすることで、グラフの表示項目を絞り込むことができます。

円グラフ表示タイプ

対象項目の指定期間における値の割合を円グラフで表示します。また、一覧表示で、指定期間における各項目の順位を表示します。

例えば、[**アプリケーション Top5**]ウィジェットの表示の場合は、指定したネットワークインターフェイスで収集したフロー情報のうち、指定期間での通信量が多い 5 つのアプリケーションの通信量と、その他のアプリケーションの割合を円グラフで表示します。一覧には、通信量の多い順に、5 つのアプリケーションに対する指定期間での通信量の値を表示します。

円グラフ表示タイプのウィジェットのイメージを「図 1-9 円グラフ表示タイプのウィジェット（19 ページ）」に示します。

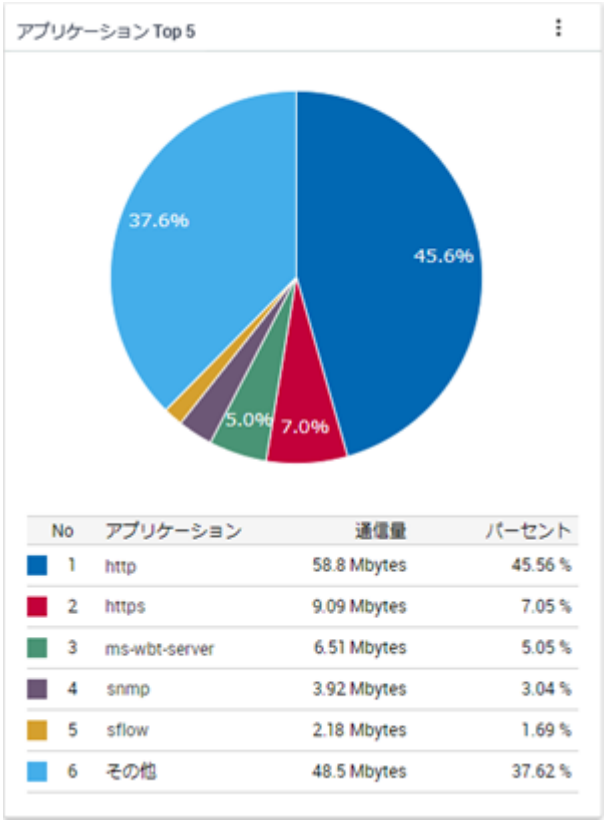

図 1-9　円グラフ表示タイプのウィジェット

円グラフ表示タイプのウィジェットでは、以下の表示操作を行うことができます。

- 折れ線グラフ表示への切り替え

ウィジェットの[⋮]アイコンをクリックし、操作することで、円グラフから折れ線グラフ、折れ線グラフから円グラフに表示を切り替えることができます。

- フィルタリング設定による表示項目の絞り込み

  一覧の各項目の左側に配置するグラフ色を示すマークをクリックすることで、特定の項目を除外した割合の円グラフを表示することができます。

ヒント

対象項目によっては、上記の表示操作が行えない場合があります。例えば、[**ノード状態の割合**]ウィジェットの表示においては、折れ線グラフ表示への切り替え操作を行うことができません。

一覧表示タイプ

イベント情報やノードの稼働状況などを一覧で表示します。

例えば、[**カレントアラート**]ウィジェットの表示の場合は、現時点で未解決の障害イベントの一覧を表示します。

一覧表示タイプのウィジェットのイメージを「図 1-10 一覧表示タイプのウィジェット（20 ページ）」に示します。

図 1-10　一覧表示タイプのウィジェット

その他の表示タイプ

個々の監視画面の特長に合わせて、特殊なタイプのウィジェットを表示する場合があります。

例えば、ノード詳細画面では、NetvisorPro で監視しているノードに対し、[**稼働状況**]ウィジェットを表示します。この[**稼働状況**]ウィジェットでは、当該ノードの稼働率を示すドーナツチャートや、時間推移に対する重要度状態の変化を示すチャートを表示します。

その他の表示タイプのウィジェットのイメージを「図 1-11 その他の表示タイプのウィジェット（21 ページ）」に示します。

図 1-11　その他の表示タイプのウィジェット

1.2.7　ウィジェットの表示内容

各ウィジェットに表示することができる情報の範囲や画面の各種パラメーターに対するウィジェットの挙動について説明します。

1 つのウィジェットで集計するデータの範囲

ダッシュボード画面で表示するウィジェットにおいては、基本的に、1 つのリージョングループの範囲でデータを集計し、ランキング形式(TopN)での表示を行います。複数のリージョングループにまたがって情報を集計したランキング形式(TopN)の表示を行うことはありません。

ヒント

障害イベントの発生状況に関連する以下の 3 つのウィジェットでは、例外として、複数のリージョングループにまたがって、すべてノードのデータを 1 つのウィジェットで表示することができます。

- [**カレントアラート**]ウィジェット
- [**ノード状態の割合**]ウィジェット
- [**ノード稼働率**]ウィジェット

ノード詳細画面では、選択したノードの範囲の情報のみを表示し、ネットワークインターフェイス詳細画面では、さらに情報を絞り込み、選択したネットワークインターフェイスの範囲のみの情報を表示します。

[期間]の指定

ウィジェットを表示する各画面では、データの表示範囲を[**期間**]で指定します。指定した期間の時間幅やどれだけ遠い過去を指定したかによって、表示するデータの粒度が変化します。

ヒント

以下のウィジェットにおいては、[**期間**]の指定値に関係せず、常に現在の状況を表示します。

- [**ノード状態の割合**]ウィジェット

[件数](ランキング)の指定

ウィジェットを表示する画面では、データの表示範囲を[**件数**]で指定します。指定した期間における値の降順、または、昇順に、指定した件数のデータをランキング形式(TopN)で表示します。Web コンソールでは、最大 Top20 までのデータ表示を行うことができます。

ヒント

以下のウィジェットにおいては、[**件数**]の指定値に関係せず、表示を行います。

- [**イベント**]ウィジェット
- [**カレントアラート**]ウィジェット
- [**ノード状態の割合**]ウィジェット

1.2.8　ウィジェットの基本操作

各ウィジェットでは、一覧表示する項目などのリンクをクリックすることで、クリックした項目に関する詳細な情報を確認するための画面に遷移することができます。また、各ウィジェットでは、表示内容を詳しく確認するためのいくつかの仕組みを提供しています。

ここでは、ウィジェットにおける基本操作について説明します。

1.2.8.1　ノードの詳細状況を確認する

ウィジェットで表示するノード名のリンクをから、当該ノードに対するノード詳細画面を簡単に表示することができます。

ウィジェットからノード詳細画面を表示した場合は、元の画面で指定していた[**期間**]の値をそのまま維持します。

ヒント

ウィジェットを含むすべての画面において、管理対象ノードを示すノード名のリンクをクリックした場合は、当該ノードに対するノード詳細画面を表示します。

ここでは、ダッシュボード画面に表示する[**ノード稼働率**]ウィジェットから、ノード詳細画面を表示する例を用いて、具体的な操作手順を説明します。

1. ダッシュボード画面を表示します。

   [**ダッシュボード**] メニューをクリックします。

2. ダッシュボード画面の[**期間**]を指定します。

   ここでは、プルダウンメニューから [**過去 24 時間**] を選択します。

3. [**ノード稼働率**]ウィジェットの内容を確認します。

   過去 24 時間の稼働率が低いノードを確認します。

4. 詳細を確認したいノードを選択します。

[**ノード稼働率**]ウィジェットで表示するノード名のリンクをクリックします。

この場合、当該ノードに対するノード詳細画面を、[**期間**]の[**過去 24 時間**]を維持したまま表示します。

5. ノード詳細画面のイベントから稼働率が低い原因を確認します。

稼働率は、重要度が[**Fatal**]を示すイベントの発生により、低くなります。

1.2.8.2　ネットワークインターフェイスの詳細状況を確認する

ウィジェットで表示するネットワークインターフェイス名のリンクから、当該ネットワークインターフェイスに対するネットワークインターフェイス詳細画面を簡単に表示することができます。

ウィジェットからネットワークインターフェイス詳細画面を表示した場合は、元の画面で指定していた[**期間**]の値をそのまま維持します。

ヒント

ウィジェットを含むすべての画面において、管理対象ノードのネットワークインターフェイス名のリンクをクリックした場合は、当該ネットワークインターフェイスに対するネットワークインターフェイス詳細画面を表示します。

ここでは、ダッシュボード画面に表示する[**入力インターフェイス使用率**]ウィジェットから、ネットワークインターフェイス詳細画面を表示する例を用いて、具体的な操作手順を説明します。

1. ダッシュボード画面を表示します。

[**ダッシュボード**] メニューをクリックします。

2. ダッシュボード画面の[**期間**]を指定します。

ここでは、プルダウンメニューから [**過去 24 時間**] を選択します。

3. [**入力インターフェイス使用率**]ウィジェットの内容を確認します。

過去 24 時間の入力側の使用率が高いネットワークインターフェイスを確認します。

4. 詳細を確認したいネットワークインターフェイスを選択します。

[**入力インターフェイス使用率**]ウィジェットで表示するネットワークインターフェイス名のリンクをクリックします。

この場合、当該ネットワークインターフェイスに対するネットワークインターフェイス詳細画面を、[**期間**]の[**過去 24 時間**]を維持したまま表示します。

5. ネットワークインターフェイス詳細画面の[**フローデータ**]から使用率が高い原因を確認します。

[**アプリケーション**]ウィジェットや[**カンバセーション**]ウィジェットの情報から、使用率を高めている原因を調べることができます。

より詳細な通信内容の分析を行う場合は、[**フロー分析**]ボタンをクリックして、NFA の Web コンソールに接続します。

1.2.8.3　フロー情報の詳細を確認する

ウィジェットに表示するフロー情報に対するエンドポイントの IP アドレスやアプリケーション名のリンクから、NFA のエクスポーター分析画面を簡単に表示することができます。

ウィジェットから NFA のエクスポーター分析画面を表示した場合は、元の画面で指定していた[**期間**]の値をそのまま維持します。また、クリックした項目内容などを[**フィルター条件**]に自動的に設定し、エクスポーター分析画面を表示します。

ここでは、ノード詳細画面に表示する[**アプリケーション**]ウィジェットから、NFA のエクスポーター分析画面を表示する例を用いて、具体的な操作手順を説明します。

1. ノード詳細画面を表示します。

   [**ノード一覧**] メニューをクリックします。表示されたノード一覧画面から詳細状況を確認したいノードのノード名のリンクをクリックします。

2. ノード詳細画面の[**期間**]を指定します。

   ここでは、プルダウンメニューから [**過去 24 時間**] を選択します。

3. [**アプリケーション**]ウィジェットの内容を確認します。

   過去 24 時間で通信量の多いアプリケーションの状況を確認します。

4. 詳細を確認したいアプリケーションを選択します。

   [**アプリケーション**]ウィジェットで表示するアプリケーション名のリンクをクリックします。

   この場合、[**対象エクスポーター**]に当該ノードを指定し、[**フィルター条件**]に当該アプリケーションを指定した状態で、NFA のエクスポーター分析画面を表示します。また、[**期間**]の指定値は、[**過去 24 時間**]を維持します。

5. エクスポーター分析画面の各ウィジェットから通信量が多い原因を確認します。

   [**カンバセーション**]ウィジェット等の情報から、通信量を高めている原因を調べることができます。

1.2.8.4　グラフの表示項目をフィルタリングする

折れ線グラフ表示タイプ、および、円グラフ表示タイプのウィジェットでは、 フィルタリングの機能を用いることで、現在の表示項目の一部を表示対象から除外すること ができます。

本操作は、一部の項目を一時的に非表示にし、注目したい項目のみを残してグラフを見やすくしたい場合に行います。

例えば、Top 20 の表示に対し、10 位から 20 位の項目を比較したい場合に、1 位から 9 位までの項目を非表示にしてグラフを見やすくします。以下に具体的な手順を示します。

ヒント

表示画面の[**更新間隔**]において、[**なし**]を指定した状態で本手順を実施することを推奨します。表示画面の更新処理を行うと、後述するフィルタリングの設定は元の状態に戻ります。

1. 対象ウィジェットにおいて、表示項目のフィルタリング設定を行います。

   ウィジェット内の一覧において、項目のグラフ色を示すマークをクリックすることで、当該データのグラフを非表示にすることができます。

2. グラフ表示から当該項目の表示が除外されたことを確認します。

除外対象の項目が複数ある場合は、上記手順を繰り返します。

除外した項目のグラフ色を示すマークを再度クリックすると、当該項目のグラフが表示対象に戻ります。

1.2.8.5　折れ線グラフの表示をズームインする

折れ線グラフ表示タイプのウィジェットにおいて、指定期間の全体を示す折れ線グラフの時間幅を狭めることで、グラフを拡大表示することができます。

表示画面の[**期間**]で指定した範囲から更に時間幅を狭めて、通信状況の詳細を確認したい場合に、以下の操作を行います。

ヒント

表示画面の[**更新間隔**]において、[**なし**]を指定した状態で本手順を実施することを推奨します。表示画面の更新処理を行うと後述する[**レンジセレクター**]の設定は元の状態に戻ります。

1. 下側の全体を表示する折れ線グラフ([**レンジセレクター**]と呼ぶ)で、表示する時間範囲を選択します。

   ドラッグ&ドロップで、表示範囲を指定します。

   上側の折れ線グラフの表示が、[**レンジセレクター**]で選択した範囲に切り替わります。

2. 表示範囲を、さらに細かく指定します。

   表示範囲を、さらに細かく調整する場合は、以下の操作を行います。

   - [**レンジセレクター**]で指定した範囲の左右の境界線をドラッグ&ドロップで移動することで、時間幅を調整します。
   - [**レンジセレクター**]で指定した表示範囲をドラッグ&ドロップし、表示範囲自体を移動させます。
   - [**レンジセレクター**]の指定エリア外をクリックして、範囲指定を解除し、新しく表示範囲をドラッグ&ドロップで指定します。

ヒント

範囲指定を解除せずに、単に範囲外のエリアをドラッグして、表示範囲を指定することもできます。

[**レンジセレクター**]の操作が反映されるのは、折れ線グラフの表示のみになります。一覧の表示内容は変化しません。

1.2.8.6　IP アドレス表示をホスト名表示に変換する

フロー情報におけるエンドポイントの IP アドレスを表示している場合、エンドポイントの IP アドレスをホスト名に変換して表示することができます。

エンドポイントを示す IP アドレスをホスト名に変換するためには、エンドポイントのホスト名と IP アドレスを管理する DNS(Domain Name System)に対し、フロー情報を受信する NFA が、ネットワークを介してホスト名を問い合わせできる環境である必要があります。

ヒント

- DNS に登録されていないエンドポイントについては、ホスト名の問い合わせが行えないため、本操作を行っても IP アドレスの表示のままになります。
- 本操作で変換されるホスト名は、本操作を実施した時点でのホスト名ではなく、NFA が、フロー情報を受信した時点に DNS から取得したホスト名です。そのため、過去の通信状況を分析する場合に、当時と現在のホスト名が異なっている場合は、当時のホスト名で表示します。

フロー情報に対するエンドポイントの IP アドレスをホスト名に変換する操作手順を以下に示します。

1. 対象ウィジェットの[⋮]アイコンをクリックします。

   [⋮]アイコンをクリックすると表示切り替えが可能な項目のチェックボックスが表示されます。

2. [**ホスト名で表示**]チェックボックスをオンにします。

   エンドポイントの IP アドレスがホスト名に変化します。

元の IP アドレスの表示に戻す場合は、同様の手順で[**ホスト名で表示**]チェックボックスをオフにします。

1.2.8.7　グラフの種類を変更する

円グラフ表示タイプのウィジェットにおいては、円グラフを折れ線グラフに、または、折れ線グラフを円グラフに変更することができます。

本操作により、1 つのウィジェットの情報から、指定期間に対する各項目の通信状況の割合と時間的推移の両方を確認することができます。以下に具体的な操作手順について示します。

⚠ 注意

[**ノード状態の割合**]ウィジェットは、円グラフ表示タイプのウィジェットですが、グラフの表示切替えを行うことはできません。

1. 対象ウィジェットの[⋮]アイコンをクリックします。

   [⋮]アイコンをクリックすると表示切り替えが可能な項目のチェックボックスが表示されます。

2. [**円グラフで表示**]チェックボックスをオフにします。

   ウィジェットの円グラフが折れ線グラフに変化します。ここで行ったグラフの表示変更は、別の画面に移動するか、F5 キーを押して画面全体を更新することにより、デフォルトのグラフに戻ります。

折れ線グラフをデフォルトのグラフとして定義しているウィジェットにおいては、同様の手順で[**円グラフで表示**]チェックボックスをオンにすることで、円グラフの表示に変更することができます。

1.2.9　特定ウィジェットによる固有操作

一部のウィジェットにおいては、ウィジェットの種類に応じた固有のリンクやアイコンを表示し、当該ウィジェットに特化した操作が行える仕組みを提供しています。

ここでは、特定のウィジェットだけが行える固有の操作について説明します。

1.2.9.1　イベントに関連した操作を行う

[**カレントアラート**]ウィジェット、および、[**イベント**]ウィジェットにおいては、発生したイベントに対し、固有の操作を行うことができます。

ここでは、イベントに対して行える操作の詳細について説明します。

イベントの詳細内容を確認する

[**カレントアラート**]ウィジェット、および、[**イベント**]ウィジェットにおいては、イベント詳細ダイアログを表示して、イベントの詳細内容を確認することができます。

[**カレントアラート**]ウィジェット、および、[**イベント**]ウィジェットで表示するイベント一覧では、障害発生状況の把握を第一の目的にしているため、発生したイベントの概要情報のみを表示しています。特定のイベントに対して詳細内容を確認したい場合は、イベント詳細ダイアログを表示します。

ここでは、[**カレントアラート**]ウィジェットでの操作例を用いて、具体的な操作手順を説明します。

1. ダッシュボード画面を表示します。

[**ダッシュボード**] メニューをクリックします。

2. [**カレントアラート**]ウィジェットの内容を確認します。

   [**カレントアラート**]ウィジェットは、現在発生中の障害イベントを表示します。

3. 確認が必要なイベントに対し、イベント詳細ダイアログを表示します。

   対象イベントの[**操作**]欄に配置する[**イベント詳細**]アイコンをクリックします。

4. イベント詳細ダイアログの内容を確認します。

   イベント詳細ダイアログでは、以下の情報を表示します。

   - [**概要**]

     イベントの概要情報を表示します。

   - [**重要度**]

     イベントの重要度を表示します。Web コンソールで表示するイベントの重要度の詳細については、「4.2.1.3　イベント重要度（137 ページ）」を参照してください。

   - [**回復状態**]

     イベントの回復状態を表示します。現在発生中のイベントに対しては、[**未回復**]の表示になります。

   - [**発生時刻**]

     イベントの発生時刻を表示します。

   - [**発生元名**]

     イベントの発生元となるノード名、および、ネットワークインターフェイス名を表示します。また、当該ノードの IP アドレスの情報と所属するリージョングループの情報も表示します。

     ⚠ 注意

     イベントの発生元として通知する IP アドレスの値は、イベントを検知した製品で管理する IP アドレスの値となります。そのため、環境によっては、Web コンソールのノード詳細画面などに表示している IMS コンポーネントで管理する IP アドレスの値とは異なる場合があります。

     [**トポロジーマップ**]アイコンをクリックすることで、イベントの発生元となるノードを配置しているマップを表示します。

     ヒント

     - [**トポロジーマップ**]アイコンは、NetvisorPro を利用している場合に表示されます。
     - [**カレントアラート**]ウィジェットから起動したイベント詳細ダイアログの場合は、現在の状況を表示する[**通常モード**]でトポロジーマップ画面を表示します。それ以外の

場合は、イベント発生当時の状況を表示することができる[**分析モード**]でトポロジーマップ画面を表示し、イベントの発生時刻を中心とした[**期間**]が設定されます。

- 当該ノードのアイコンを複数のマップに配置している場合は、表示するマップの選択画面が表示されます。

- [**担当者**]

  当該イベントの対応を担当するユーザー名(表示名)を表示します。誰も担当者として割り当てられていない場合は、空欄となります。

- [**詳細**]

  イベントの詳細情報を表示します。

- [**対処**]

  イベントの対処方法の情報を表示します。

- [**SNMP トラップ Enterprise**]、[**Generic Code**]、[**Specific Code**]

  SNMP トラップの情報を表示します。本項目は SNMP トラップのイベントでのみ表示されます。

- [**Syslog Facility**]、[**Severity**]

  Syslog の情報を表示します。本項目は Syslog のイベントでのみ表示されます。

- [**アプリケーション名**]

  イベントを検知したアプリケーション名(IMS コンポーネントと接続する製品名)を表示します。

ヒント

イベント情報の内容を印刷したい場合は、イベント詳細画面を表示し、Web ブラウザーの印刷機能を用いて印刷を行います。イベント詳細画面は、[**印刷用画面を開く**]アイコンをクリックすることで表示することができます。

イベントに対する操作を行う

[**カレントアラート**]ウィジェット、および、[**イベント**]ウィジェットにおいては、一覧に表示するイベントに対し、対応操作を行うことができます。

Web コンソールでは、通知されたイベントに対し、以下の操作を行うことができます。

- イベント対処の担当者に自分を割り当てる
- イベント対処の担当者の割り当てを解除する
- イベントの状態を回復させる
- イベントを削除する

ここでは、[**カレントアラート**]ウィジェットでの操作例を用いて、具体的な操作手順を説明します。

1. ダッシュボード画面を表示します。

   [**ダッシュボード**] メニューをクリックします。

2. [**カレントアラート**]ウィジェットの内容を確認します。

   [**カレントアラート**]ウィジェットは、現在発生中の障害イベントを表示します。

3. 必要に応じてイベントの詳細情報を確認します。

   [**イベント詳細**]アイコンをクリックするとイベント詳細ダイアログを表示することができ、イベントの詳細情報が確認できます。

4. イベントの対応操作を行います。

   詳細内容を把握したイベントの[ ]アイコンをクリックすると、以下のメニューが表示されます。

   - [**担当者に自分を割り当てる**] メニュー

     イベントに対し、自分を担当者として割り当てます。選択すると、当該イベントの[**担当者**]欄に自分のユーザー名が登録されます。すでに担当者が割り当てられているイベントに対しても操作することができます。

   - [**担当者を解除する**] メニュー

     イベントに対し割り当てられていた担当者を解除します。選択すると、当該イベントの[**担当者**]欄が空欄になります。自分以外の担当者の割り当ても解除することができます。

   - [**回復する**] メニュー

     イベントを回復状態にします。選択すると当該イベントの[**回復状態**]が[**未回復**]から[**回復済**]に変わり、[**カレントアラート**]ウィジェットから当該イベントの表示が消えます。

     ヒント

     イベントを検出した製品の仕様に依存して、イベントによっては、自動で回復状態を検出し、回復処理が行われます。

   - [**削除する**] メニュー

     イベントを削除します。選択すると当該イベントが削除され、イベントの一覧から消えます。

   上記メニューを選択すると、確認ダイアログが表示されます。内容の確認後、[**OK**]ボタンをクリックすることで、処理が実行されます。

5. 操作後の[**カレントアラート**]ウィジェットの内容を確認します。

   選択したメニューの操作が適切に行えていることをイベントの一覧から確認します。

発生イベントの影響をトポロジーマップで確認する

[**カレントアラート**]ウィジェット、および、[**イベント**]ウィジェットにおいては、表示するイベントから発生元となるノードが登録されているトポロジーマップ画面を簡単に表示することができます。

トポロジーマップ画面を表示することで、ノードの接続関係から直観的に、発生イベントの影響範囲を確認することができます。

ここでは、ダッシュボード画面に表示する[**カレントアラート**]ウィジェットから、トポロジーマップ画面を表示する例を用いて、具体的な操作手順を説明します。

1. ダッシュボード画面を表示します。

   [**ダッシュボード**] メニューをクリックします。

2. [**カレントアラート**]ウィジェットの内容を確認します。

   [**カレントアラート**]ウィジェットは、現在発生中の障害イベントを表示します。

3. 影響範囲の確認が必要なイベントに対しトポロジーマップ画面を表示します。

   対象イベントの[**操作**]欄に配置する[**トポロジーマップ**]アイコンをクリックします。

   対象イベントの発生元となるノードが、1 つのマップのみに登録されている場合は、当該ノードが登録されているトポロジーマップ画面を表示します。

   対象イベントの発生元となるノードが複数のマップに登録されている場合は、表示候補となるマップのリンク一覧を表示します。表示したいマップのリンクをクリックすると、トポロジーマップ画面が表示されます。

   ヒント

   - [**カレントアラート**]ウィジェットからは、トポロジーマップ画面を[**通常モード**]で表示します。
   - [**イベント**]ウィジェットからは、トポロジーマップ画面を[**分析モード**]で表示し、イベントの発生時刻を中心とした[**期間**]が設定されます。これにより、イベント発生当時のマップの状況を確認することができます。

4. トポロジーマップ画面の当該ノード周辺を確認します。

   イベントの発生元となるノードを中心に、隣接するノードやその先につながるノードの状況を確認し、ネットワーク全体の影響を確認します。

1.2.9.2　指定した状態のノードを一覧で確認する

[**ノード状態の割合**]ウィジェットから、指定した状態のノードを簡単に調べることができます。

[**ノード状態の割合**]ウィジェットでは、管理するノードが、現在どのような状態にあるのかを重要度に対するノード数や割合で表示します。各重要度状態のノードを具体的に調べたい場合は以下の操作を行います。

1. ダッシュボード画面の[**ノード状態の割合**]ウィジェットの内容を確認します。

   [**ノード状態の割合**]ウィジェットは、管理するノードの現在の重要度の状態を表示します。

2. 具体的なノード名を調べたい重要度のリンクをクリックします。

   [**ノード状態の割合**]ウィジェットの重要度のリンクをクリックすると、[**検索条件**]に重要度を指定した状態でノード一覧画面を表示します。

   表示されたノード一覧が、現在、指定した重要度の状態にある具体的なノードを示します。

第 2 章
運用前の環境設定

Web コンソールを利用する前に必要となる環境設定の方法について説明します。

目次

2.1　ユーザーを管理する

Web コンソールにログインするユーザーの管理について説明します。

2.1.1　グループとユーザー

ユーザー管理におけるグループとユーザーの関係と操作に関する権限について説明します。

Web コンソールを操作するユーザーは、必ず、グループに所属します。そのグループに付与している役割の範囲でユーザーは Web コンソールを操作することができます。役割の異なる複数のグループを作成し、各ユーザーを適切なグループに振り分けていくことで、ユーザーの操作範囲を管理していくことができます。

グループに割り当てることができる役割は以下の 3 つです。

- アドミニストレーター
- オペレーター
- オブザーバー

各役割と権限についての詳細を以下に示します。

アドミニストレーター

Web コンソールを用いて、すべての運用、管理を実施する役割を担い、すべての画面の参照、運用操作、定義操作が行える権限を持ちます。

また、別途、[**アカウント管理者**]の役割を割り当てることができます。[**アカウント管理者**]の役割を割り当てると、グループ、および、ユーザーの管理のための操作が行えるようになります。

オペレーター

Web コンソールを用いたネットワークの監視作業を実施する役割を担い、各画面の参照、運用操作が行える権限を持ちます。

ヒント

上記説明における「運用操作」とは、各画面から行える処理の実行のことを指します。例えば、イベントに対する確認、回復処理などが該当します。

オブザーバー

Web コンソールを用いてネットワークの状況を観察する役割を担い、各画面の参照のみの権限を持ちます。

2.1.2　グループの情報を管理する

ユーザーが所属するグループの情報を管理する画面、および、グループの管理操作について説明します。

ヒント

アカウント管理者の役割を持つグループのユーザーのみ、グループの管理操作が行えます。

2.1.2.1　グループ画面

グループ画面について説明します。

グループ画面では、グループ内容の確認、および、操作(追加、編集、削除)を行います。

グループ画面は、[**アカウント管理**] >[**グループ**] メニューをクリックして表示します。

ヒント

アカウント管理者の役割を持つグループのユーザーのみ、グループ画面を表示することができます。

図 2-1　グループ画面

- [**グループの追加**]ボタン

  グループを新規に追加します。[**グループの追加**]ボタンをクリックすると、グループ追加画面が表示されます。詳細は、「2.1.2.2　グループを追加する（36 ページ）」を参照してください。

グループ一覧

- [**グループ名**]

  グループの名前を表示します。

- [**説明**]

グループの説明を表示します。

- [**役割**]

  グループに割り当てた役割の内容を表示します。

- [**操作**]

  各アイコンをクリックすることで、グループに対する操作を行うことができます。

  - [**編集**]アイコン

    グループの登録内容を変更します。[**編集**]アイコンをクリックすると、グループ編集画面が表示されます。詳細は、「2.1.2.3　グループを更新する（37 ページ）」を参照してください。

  - [**削除**]アイコン

    グループの情報を削除します。詳細は、「2.1.2.4　グループを削除する（38 ページ）」を参照してください。

    ⚠ 注意

    初期状態から登録されているグループ「Administrators」は、削除できません。

2.1.2.2　グループを追加する

新規にグループを追加する手順について説明します。

ここでは、運用の実務を担当するメンバーを所属させるグループとして「実務担当グループ」という名前のグループを追加する例を用いて、具体的な操作手順を説明します。

1. グループ画面を表示します。

   [**アカウント管理**] >[**グループ**] メニューをクリックします。

2. [**グループの追加**]ボタンをクリックします。

   グループ追加画面が表示されます。

3. グループ追加画面で適切な値を指定します。

   - [**グループ名**]

     一意に識別できるグループの名前を指定します。最大文字数は 128 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     既存のグループ名と重複する名前を指定することはできません。

     本例では、「実務担当グループ」と指定します。

- [**説明**]

  グループ内容の説明を指定します。最大文字数は 512 文字です。

  本例では、「運用の実務を担当するメンバー用のグループ」と指定します。

- [**役割**]

  グループの役割を以下から選択します。

  - [**アドミニストレーター**]
  - [**オペレーター**]
  - [**オブザーバー**]

  各役割の詳細については、「2.1.1　グループとユーザー（34 ページ）」を参照してください。

  本例では、「[**オペレーター**]」を選択します。

  ヒント

  [**アドミニストレーター**]を選択した場合のみ、[**アカウント管理者**]の役割の有無を選択することができます。

4. グループの情報を保存します。

   設定内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、新規にグループが追加されます。

グループ画面の一覧で、グループ「実務担当グループ」が追加されていることを確認します。

2.1.2.3　グループを更新する

登録済みのグループの内容を更新する手順について説明します。

ここでは、グループ「実務担当グループ」の説明内容を変更する例を用いて、具体的な操作手順を説明します。

1. グループ画面を表示します。

   [**アカウント管理**] >[**グループ**] メニューをクリックします。

2. 更新対象のグループ「実務担当グループ」の[**編集**]アイコンをクリックします。

   グループ「実務担当グループ」に対するグループ編集画面が表示されます。

3. グループ編集画面で更新対象の項目の入力値を変更します。

   以下のすべての項目に対し、変更の操作が行えます。

   - [**グループ名**]

     一意に識別できるグループの名前を指定します。最大文字数は 128 文字です。

以下に示す文字は指定することができません。

- 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
- 先頭および末尾への半角スペース

既存のグループ名と重複する名前を指定することはできません。

本例では、変更しません。

- [**説明**]

  グループ内容の説明を指定します。最大文字数は 512 文字です。

  本例では、「ネットワークの運用管理における実務担当者用グループ」に内容を変更します。

- [**役割**]

  グループの役割を以下から選択します。

  - [**アドミニストレーター**]
  - [**オペレーター**]
  - [**オブザーバー**]

  各役割の詳細については、「2.1.1　グループとユーザー（34 ページ）」を参照してください。

  本例では、変更しません。

  ヒント

  [**アドミニストレーター**]を選択した場合のみ、[**アカウント管理者**]の役割の有無を選択することができます。

4. 変更内容を保存します。

   変更内容を確認し、[**登録**]ボタンをクリックします。

   指定した内容で、グループ内容が更新されます。

グループ画面の一覧で、グループ「実務担当グループ」の[**説明**]欄の内容が更新されていることを確認します。

2.1.2.4　グループを削除する

登録済みのグループを削除するための手順について説明します。

1. グループ画面を表示します。

   [**アカウント管理**] >[**グループ**] メニューをクリックします。

2. 削除対象のグループの[**削除**]アイコンをクリックします。

   削除処理に対する確認ダイアログが表示されます。

⚠ 注意

削除対象として指定したグループに、所属するユーザーが存在している場合は、グループの削除はできません。所属するユーザーをすべて別のグループに移してから削除を行ってください。

3. 確認ダイアログで内容を確認します。
4. 削除を実行します。

   確認ダイアログの[**OK**]ボタンをクリックします。

   グループ画面の一覧から、指定したグループの情報が削除されます。

2.1.3　ユーザー情報を管理する

ユーザー情報を管理する画面、および、ユーザー情報の操作手順について説明します。

ヒント

アカウント管理者の役割を持つグループのユーザーのみ、ユーザー情報の管理操作が行えます。

2.1.3.1　ユーザー画面

ユーザー画面について説明します。

ユーザー画面では、ユーザー内容の確認、および、操作(追加、編集、削除)を行います。

ユーザー画面は、[**アカウント管理**] >[**ユーザー**] メニューをクリックして表示します。

ヒント

アカウント管理者の役割を持つグループのユーザーのみ、ユーザー画面を表示することができます。

図 2-2　ユーザー画面

- [**ユーザーの追加**]ボタン

ユーザーを新規に追加します。[**ユーザーの追加**]ボタンをクリックすると、ユーザー追加画面が表示されます。詳細は、「2.1.3.2　ユーザーを追加する（41 ページ）」を参照してください。

ユーザー一覧

- [**ユーザー名**]

  登録しているユーザーを識別するための名前を表示します。

- [**表示名**]

  ログイン時に表示するユーザー表示名の設定値を表示します。

- [**グループ**]

  ユーザーが所属するグループを表示します。

- [**役割**]

  ユーザーが所属するグループの役割を表示します。

- [**操作**]

  各アイコンをクリックすることで、ユーザーに対する操作を行うことができます。

  - [**編集**]アイコン

    ユーザーの登録内容を変更します。[**編集**]アイコンをクリックすると、ユーザー編集画面が表示されます。詳細は、「2.1.3.3　ユーザーを更新する（42 ページ）」を参照してください。

  - [**削除**]アイコン

    ユーザー情報を削除します。詳細は、「2.1.3.4　ユーザーを削除する（44 ページ）」を参照してください。

    ⚠ 注意

    初期状態から登録されているユーザー「admin」は、削除できません。

ヒント

30 分の間に、5 回以上のログイン失敗を検知すると、ユーザー情報がロックされた状態となり、当該ユーザーでのログインが、30 分の間できなくなります。

ロック状態になったユーザーに対しては、ユーザー一覧の先頭に[ ]アイコンが表示されます。ユーザー情報のロックは、30 分後に自動で解除されますが、[ ]アイコンをクリックすると、すぐにロック状態を解除することができます。

2.1.3.2　ユーザーを追加する

新規にユーザーを追加する手順について説明します。

ここでは、事前に作成しているグループ「実務担当グループ」にユーザー「tyamada」を追加する例を用いて、具体的な操作手順を説明します。

1. ユーザー画面を表示します。

   [**アカウント管理**] >[**ユーザー**] メニューをクリックします。

2. [**ユーザーの追加**]ボタンをクリックします。

   ユーザー追加画面が表示されます。

3. ユーザー追加画面で適切な値を指定します。

   - [**ユーザー名**]

     一意に識別できるユーザーの名前を指定します。最大文字数は 255 文字です。指定可能な文字は、半角英数字、ハイフン(-)、アンダーバー(_)、ドット(.)、アットマーク(@)、アポストロフィ(')です。

     既存のユーザー名と重複する名前を指定することはできません。

     本例では、「tyamada」と指定します。

   - [**表示名**]

     画面上の表示用のユーザーの名前を任意の文字で指定します。最大文字数は 128 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     省略した場合は、[**ユーザー名**]で指定した名前を表示名として使用します。

     本例では、「山田太郎」と指定します。

   - [**パスワード**]

     登録するユーザーの初期パスワードを指定します。以下の文字を組み合わせて、8~64 文字の文字数で指定します。

     - 半角英大文字
     - 半角英小文字
     - 半角数字
     - 半角スペース と 以下の記号

       ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

パスワードには、上記の 4 種類の文字のうち、3 種類以上の文字を含んでいる必要があります。

- [**パスワード(確認用)**]

  [**パスワード**]で指定したものと同じパスワードを指定します。

- [**グループ**]

  事前に作成しているグループの中から、ユーザーを所属させるグループを選択します。

  本例では、「実務担当グループ」と選択します。

- [**初期表示ダッシュボード**]

  ログインした時に、最初に表示するダッシュボードの名前を選択します。

ヒント

事前にダッシュボードの定義追加を行っていない場合は、接続する製品が提供するビルトインダッシュボードの中から選択します。

4. ユーザー情報を保存します。

   設定内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、新規にユーザーが追加されます。

ユーザー画面で、グループ「実務担当グループ」に所属するユーザー「tyamada」が追加されていることを確認します。

2.1.3.3　ユーザーを更新する

登録済みのユーザーを更新する手順について説明します。

ここでは、ユーザー「tyamada」の所属するグループをグループ「Administrators」に変更する例を用いて、具体的な操作手順を説明します。

ヒント

[**ユーザー名**]については、変更することができません。

1. ユーザー画面を表示します。

   [**アカウント管理**] >[**ユーザー**] メニューをクリックします。

2. 更新対象のユーザー「tyamada」の[**編集**]アイコンをクリックします。

   ユーザー「tyamada」に対するユーザー編集画面が表示されます。

3. ユーザー編集画面で更新対象の項目の入力値を変更します。

   - [**表示名**]

画面上の表示用のユーザーの名前を任意の文字で指定します。最大文字数は 128 文字です。

以下に示す文字は指定することができません。

- 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
- 先頭および末尾への半角スペース

省略した場合は、[**ユーザー名**]で指定した名前を表示名として使用します。

- [**パスワード**]

  ユーザーの新しいパスワードを指定します。パスワードは、以下の文字を組み合わせて、8~64 文字の文字数で指定します。

  - 半角英大文字
  - 半角英小文字
  - 半角数字
  - 半角スペース と 以下の記号

    ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

  パスワードには、上記の 4 種類の文字のうち、3 種類以上の文字を含んでいる必要があります。また、過去 10 回分のパスワードとは異なっている必要があります。

- [**パスワード(確認用)**]

  [**パスワード**]で指定したものと同じパスワードを指定します。

- [**グループ**]

  事前に作成しているグループの中から、ユーザーを所属させるグループを選択します。

  本例では「Administrators」を選択し、所属グループを変更します。

- [**初期表示ダッシュボード**]

  ログインした時に、最初に表示するダッシュボードの名前を選択します。

  ヒント

  事前にダッシュボードの定義追加を行っていない場合は、接続する製品が提供するビルトインダッシュボードの中から選択します。

4. 変更内容を保存します。

   変更内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、ユーザー情報の内容が更新されます。

ユーザー画面で、ユーザー「tyamada」の所属グループが「Administrators」に変更されていることを確認します。

ヒント

Web API の認証処理で利用する Web API アクセスキーを発行していた場合は、[**Web API アクセスキー**]の[**削除**]ボタンをクリックすることで、発行済みの Web API アクセスキーを削除することができます。

2.1.3.4　ユーザーを削除する

登録済みのユーザーを削除するための手順について説明します。

1. ユーザー画面を表示します。

   [**アカウント管理**] >[**ユーザー**] メニューをクリックします。

2. 削除対象のユーザーの[**削除**]アイコンをクリックします。

   削除処理に対する確認ダイアログが表示されます。

3. 確認ダイアログで内容を確認します。

4. 削除を実行します。

   確認ダイアログの[**OK**]ボタンをクリックします。

   ユーザー画面の一覧から、指定したユーザーの情報が削除されます。

2.2　運用スケジュールを管理する

運用を制御するスケジュール機能について説明します。

事前に定義したスケジュールに合わせて各機能を制御するための仕組みとして、スケジュール機能を提供しています。定義したスケジュールに対する制御内容は、各機能で異なっています。

本バージョンにおいてスケジュール機能に対応している機能、および、その制御内容は、以下の通りです。

- アノマリー分析

  アノマリー分析では、過去に収集したデータから今後のデータの挙動を予測し、アノマリーを検知します。あらかじめ、普段とは異なる挙動になる可能性が高い期間をスケジュールとして定義しておくことで、アノマリーの分析対象から指定期間を除外することができます。

  例えば、1 週間ごとに周期性を示すデータの分析において、突発的なデータの変化が懸念される祝日や企業の特別な休日を事前にスケジュール機能で定義しておくことで、アノマリーの誤検知を防止することができます。

2.2.1　スケジュール画面

スケジュール画面について説明します。

スケジュール画面では、スケジュール定義の内容確認、および、操作(追加、編集、削除)を行います。

スケジュール画面は、[**システム設定**] >[**スケジュール**] メニューをクリックして表示します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、スケジュール画面を表示することができます。

図 2-3　スケジュール画面

- [**スケジュール定義の追加**]ボタン

  スケジュール定義を新規に追加します。[**スケジュール定義の追加**]ボタンをクリックすると、スケジュール定義の追加画面が表示されます。詳細は、「2.2.2　スケジュール定義を追加する（46 ページ）」を参照してください。

スケジュール定義一覧

- [**名前**]

  スケジュール定義の名前を表示します。

- [**説明**]

  スケジュール定義の説明を表示します。

- [**操作**]

  各アイコンをクリックすることで、スケジュール定義に対する操作を行うことができます。

  - [**編集**]アイコン

スケジュール定義の内容を変更します。[**編集**]アイコンをクリックすると、スケジュール定義の編集画面が表示されます。詳細は、「2.2.3　スケジュール定義を更新する（47 ページ）」を参照してください。

- [**削除**]アイコン

  スケジュール定義を削除します。詳細は、「2.2.4　スケジュール定義を削除する（49 ページ）」を参照してください。

- [**コピー**]アイコン

  既存のスケジュール定義の内容を利用して、新規のスケジュール定義を追加します。[**コピー**]アイコンをクリックすると、スケジュール定義の内容を含んだ形で、スケジュール定義の追加画面が表示されます。

  登録済みの内容から一部を変更し、新たなスケジュール定義を作成する場合に利用します。詳細は、「2.2.2　スケジュール定義を追加する（46 ページ）」を参照してください。

2.2.2　スケジュール定義を追加する

新規にスケジュール定義を追加する手順について説明します。

ここでは、2020 年における会社の特別休日として「6/12」、「11/2」のスケジュールを追加する例を用いて、具体的な操作手順を説明します。

1. スケジュール画面を表示します。

   [**システム設定**] >[**スケジュール**] メニューをクリックします。

2. [**スケジュール定義の追加**]ボタンをクリックします。

   スケジュール定義の追加画面が表示されます。

3. スケジュール定義の追加画面で適切な値を指定します。

   - [**名前**]

     一意に識別できるスケジュール定義の名前を指定します。最大文字数は 64 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     既存のスケジュール定義と重複する名前を指定することはできません。

     本例では、「2020 年特別休日」と指定します。

   - [**説明**]

     スケジュール定義の内容の説明を指定します。最大文字数は 1024 文字です。

本例では、「2020 年における特別休日 (6/12, 11/2)」と指定します。

- [**期間**]

  スケジュールによる制御対象の期間を指定します。[＋]アイコンをクリックし、以下の項目を指定します。

  - [**名前**]

    期間に対する名前を指定します。最大文字数は 64 文字です。

    以下に示す文字は指定することができません。

    * 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
    * 先頭および末尾への半角スペース

  - [**日付を指定**](デフォルト値)

    カレンダーから日付を選択し、指定します。

  - [**特定の期間を指定**]

    期間の起点と終点の日時を指定します。

  [**OK**]ボタンをクリックすると、指定した内容で期間が登録されます。

  登録した期間の内容を変更したい場合は、期間の[**編集**]アイコンをクリックします。また、登録した期間を削除する場合は、期間の[**削除**]アイコンをクリックします。

  ここでは、[**日付を指定**]を選択し、「特別休日」という名前で「2020-06-12」、「2020-11-02」の 2 つを登録します。

4. スケジュール定義を保存します。

   設定内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、新規にスケジュール定義が追加されます。

スケジュール画面で、スケジュール定義「2020 年特別休日」が追加されていることを確認します。

2.2.3　スケジュール定義を更新する

登録済みのスケジュール定義の内容を更新する手順について説明します。

ここでは、スケジュール定義「2020 年特別休日」に「12/11」を追加する例を用いて、具体的な操作手順を説明します。

1. スケジュール画面を表示します。

   [**システム設定**] >[**スケジュール**] メニューをクリックします。

2. 更新対象のスケジュール定義「2020 年特別休日」の[**編集**]アイコンをクリックします。

   スケジュール定義の更新画面が表示されます。

3. スケジュール定義の更新画面で適切な値を指定します。

   - [**名前**]

     一意に識別できるスケジュール定義の名前を指定します。最大文字数は 64 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     既存のスケジュール定義と重複する名前を指定することはできません。

   - [**説明**]

     スケジュール定義の内容の説明を指定します。最大文字数は 1024 文字です。

     本例では、「2020 年における特別休日 (6/12, 11/2, 12/11)」に変更します。

   - [**期間**]

     スケジュールによる制御対象の期間を指定します。[＋]アイコンをクリックし、以下の項目を指定します。

     - [**名前**]

       期間に対する名前を指定します。最大文字数は 64 文字です。

       以下に示す文字は指定することができません。

       * 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
       * 先頭および末尾への半角スペース

     - [**日付を指定**]

       カレンダーから日付を選択し、指定します。

     - [**特定の期間を指定**]

       期間の起点と終点の日時を指定します。

     [**OK**]ボタンをクリックすると、指定した内容で期間が登録されます。

     登録した期間の内容を変更したい場合は、期間の[**編集**]アイコンをクリックします。また、登録した期間を削除する場合は、期間の[**削除**]アイコンをクリックします。

     ここでは、[**日付を指定**]を選択し、「特別休日」という名前で「12/11」を追加登録します。

4. スケジュール定義を保存します。

   設定内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、スケジュール定義が更新されます。

スケジュール画面で、スケジュール定義「2020 年特別休日」の[**説明**]欄の内容が更新されていることを確認します。

2.2.4　スケジュール定義を削除する

登録済みのスケジュールの定義を削除するための手順について説明します。

⚠ 注意

スケジュール定義を削除する場合は、利用している機能の有無や影響を確認した上で実施してください。

1. スケジュール画面を表示します。

   [**システム設定**] >[**スケジュール**] メニューをクリックします。

2. 削除対象のスケジュール定義の[**削除**]アイコンをクリックします。

   削除処理に対する確認ダイアログが表示されます。

3. 確認ダイアログで内容を確認します。

4. 削除を実行します。

   確認ダイアログの[**OK**]ボタンをクリックします。

   スケジュール画面の一覧から、指定したスケジュール定義が削除されます。

2.3　イベント検知時のアクションを設定する

イベントの発生を契機に、任意のアクションを実行することができます。ここでは、アクションを実行するために事前に行っておく環境設定の内容、および、実行するアクションの定義内容について説明します。

イベントに対するアクション(イベントアクション)定義においては、以下の 2 つの要素を設定します。

- アクションを実行するイベント条件

  重要度や発生元名などのイベントに含まれる様々な情報に対し、アクションの実行を判断するための条件を設定します。

- 実行するアクション内容

  イベント内容をメールで通報したり、IMS コンポーネントをインストールしたサーバー上の任意のコマンドを実行させるなど、実行するアクションの内容を設定します。

2.3.1　イベントアクション定義のための事前の環境設定を行う

イベントアクション定義の設定作業に際し、事前に実施する環境設定の内容について説明します。

以下のイベントアクションを実行する場合は、事前の環境設定が必要となります。

- メール通報

  イベントアクション定義の設定作業よりも前に、利用するメールサーバーの情報を登録しておく必要があります。

- SystemManager G へのイベントメッセージ連携

  イベントアクション定義の設定作業よりも前に、連携対象となる SystemManager G の情報を設定ファイル (ims-conf.ini) に登録しておく必要があります。詳細は、「F.1　連携対象の SystemManager G 情報を登録する（235 ページ）」を参照してください。

ここでは、事前に行っておく必要があるメールサーバーの登録やその情報管理について説明します。

2.3.1.1　メールサーバー画面

メールサーバー画面について説明します。

メールサーバー画面では、利用するメールサーバーの内容確認、および、操作(追加、編集、削除)を行います。

メールサーバー画面は、[**イベントアクション設定**] >[**メールサーバー**] メニューをクリックして表示します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、メールサーバー画面を表示することができます。

図 2-4　メールサーバー画面

- [ **メールサーバーの追加**]ボタン

  メールサーバーを新規に追加します。[ **メールサーバーの追加**]ボタンをクリックすると、メールサーバー追加画面が表示されます。詳細は、「2.3.1.2　メールサーバーを追加する（51 ページ）」を参照してください。

メールサーバー一覧

- [**メールサーバー名**]

  メールサーバーの名前を表示します。

- [**ホスト名**]

  メールサーバーのドメイン名(FQDN)、もしくは、IP アドレスを表示します。

- [**ポート番号**]

  メール送信で利用するポート番号を表示します。

- [**SMTP 認証タイプ**]

  メールサーバーとの SMTP 認証の方式を表示します。

- [**操作**]

  各アイコンをクリックすることで、メールサーバーの登録情報に対する操作を行うことができます。

  - [ **編集**]アイコン

    メールサーバーの登録情報を変更します。[ **編集**]アイコンをクリックするとメールサーバー編集画面が表示されます。詳細は、「2.3.1.3　メールサーバーを更新する（53 ページ）」を参照してください。

  - [ **削除**]アイコン

    メールサーバーの登録情報を削除します。詳細は、「2.3.1.4　メールサーバーを削除する（54 ページ）」を参照してください。

2.3.1.2　メールサーバーを追加する

新規にメールサーバーを追加する手順について説明します。

1. メールサーバー画面を表示します。

   [ **イベントアクション設定**] >[**メールサーバー**] メニューをクリックします。

2. [ **メールサーバーの追加**]ボタンをクリックします。

   メールサーバー追加画面が表示されます。

3. メールサーバー追加画面で適切な値を指定します。

- [**メールサーバー名**]

  一意に識別できるメールサーバーの名前を指定します。最大文字数は 64 文字です。

  以下に示す文字は指定することができません。

  - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
  - 先頭および末尾への半角スペース

- [**ホスト名**]

  メールサーバーのドメイン名(FQDN)、もしくは、IP アドレスを指定します。最大文字数は 128 文字です。

- [**ポート番号**]

  メール送信で利用するポート番号を 1～65535 の範囲で指定します。

- [**送信元メールアドレス**]

  メール通報の際の送信元メールアドレスを指定します。最大文字数は 64 文字です。

- [**SMTP 認証タイプ**]

  プルダウンメニューから以下のいずれかを選択します。

  - [**認証なし**]

    SMTP 認証を使用せずにメールサーバーにアクセスします。

  - [**LOGIN**]

    LOGIN 認証を用いてメールサーバーにアクセスします。

  - [**PLAIN**]

    PLAIN 認証を用いてメールサーバーにアクセスします。

  [**LOGIN**]、または、[**PLAIN**]を選択した場合は、以下の認証情報の指定が必要になります。

  - [**ユーザー名**]

    メールサーバーへの認証に用いるユーザー名を指定します。最大文字数は 36 文字です。

    以下に示す文字は指定することができません。

    * 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
    * 先頭および末尾への半角スペース

  - [**パスワード**]

    メールサーバーへの認証に用いるユーザー名に対するパスワードを指定します。最大文字数は 64 文字です。

    以下に示す文字は指定することができません。

* 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
* 先頭および末尾への半角スペース

4. メールサーバーの情報を保存します。

   設定内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、新規にメールサーバーの情報が追加されます。

メールサーバー画面で、メールサーバーの情報が追加されていることを確認します。

2.3.1.3　メールサーバーを更新する

登録済みのメールサーバーの情報を更新する手順について説明します。

1. メールサーバー画面を表示します。

   [**イベントアクション設定**] >[**メールサーバー**] メニューをクリックします。

2. 更新対象のメールサーバーの[**編集**]アイコンをクリックします。

   当該メールサーバーに対するメールサーバー編集画面が表示されます。

3. メールサーバー編集画面で更新対象の項目の入力値を変更します。

   以下のすべての項目に対し、変更の操作が行えます。

   - [**メールサーバー名**]

     一意に識別できるメールサーバーの名前を指定します。最大文字数は 64 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**ホスト名**]

     メールサーバーのドメイン名(FQDN)、もしくは、IP アドレスを指定します。最大文字数は 128 文字です。

   - [**ポート番号**]

     メール送信で利用するポート番号を 1～65535 の範囲で指定します。

   - [**送信元メールアドレス**]

     メール通報の際の送信元メールアドレスを指定します。最大文字数は 64 文字です。

   - [**SMTP 認証タイプ**]

     プルダウンメニューから以下のいずれかを選択します。

     - [**認証なし**]

       SMTP 認証を使用せずにメールサーバーにアクセスします。

- [**LOGIN**]

  LOGIN 認証を用いてメールサーバーにアクセスします。

- [**PLAIN**]

  PLAIN 認証を用いてメールサーバーにアクセスします。

[**LOGIN**]、または、[**PLAIN**]を選択した場合は、以下の認証情報の指定が必要になります。

- [**ユーザー名**]

  メールサーバーへの認証に用いるユーザー名を指定します。最大文字数は 36 文字です。

  以下に示す文字は指定することができません。

  * 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
  * 先頭および末尾への半角スペース

- [**パスワード**]

  メールサーバーへの認証に用いるユーザー名に対するパスワードを指定します。最大文字数は 64 文字です。

  以下に示す文字は指定することができません。

  * 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
  * 先頭および末尾への半角スペース

4. 変更内容を保存します。

   変更内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、メールサーバーの情報が更新されます。

メールサーバー画面の一覧で、当該メールサーバーに対する変更内容が適切に反映されていることを確認します。

2.3.1.4　メールサーバーを削除する

登録済みのメールサーバーの情報を削除するための手順について説明します。

⚠ 注意

イベントアクション定義の中で利用しているメールサーバーの情報は削除することができません。

1. メールサーバー画面を表示します。

   [**イベントアクション設定**] >[**メールサーバー**] メニューをクリックします。

2. 削除対象のメールサーバーの[**削除**]アイコンをクリックします。

削除処理に対する確認ダイアログが表示されます。

3. 確認ダイアログで内容を確認します。
4. 削除を実行します。

   確認ダイアログの[**OK**]ボタンをクリックします。

   メールサーバー画面から、指定したメールサーバーの情報が削除されます。

2.3.2　イベントアクション定義を設定する

アクションを実行するイベントの条件やそのアクション内容を定義するイベントアクション定義について説明します。

1 つのイベントアクション定義において、アクションを実行するイベントの条件や実行するアクションの内容は、それぞれ複数の内容を指定することができます。例えば、アクションを実行するイベントの条件として、重要度と発生元名など 2 つ以上の条件を組み合わせて指定することができます。また、実行するアクションにおいては、メール通報と任意のコマンドの実行など、2 つ以上のアクションを実行させることができます。

イベントアクション定義は、複数登録しておくことができ、個々のイベントに対し、固有のアクションを定義していくことができます。複数のイベントアクション定義を登録した場合は、優先度の高いイベントアクション定義から順に、発生したイベントの内容と照らし合わせて、アクションの実行を判断していきます。

イベントアクション定義の管理については、イベントアクション画面で行います。

⚠ 注意

コマンド実行アクションには、以下のような性質のコマンドを登録することはできません。

- コマンド実行中に、ユーザーによる入力や応答を必要とするコマンド
- コマンド実行が終了せずに常駐するコマンド

2.3.2.1　イベントアクション画面

イベントアクション画面について説明します。

イベントアクション画面では、イベントアクション定義の内容確認、および、操作(追加、編集、削除)を行います。

イベントアクション画面は、[**イベントアクション設定**] >[**イベントアクション**] メニューをクリックして表示します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、イベントアクション画面を表示することができます。

図 2-5　イベントアクション画面

- [**イベントアクションの追加**]ボタン

  イベントアクション定義を新規に追加します。[**イベントアクションの追加**]ボタンをクリックすると、イベントアクション追加画面が表示されます。詳細は、「2.3.2.2　イベントアクション定義を追加する（57 ページ）」を参照してください。

イベントアクション定義一覧

- [**有効**]

  イベントアクション定義が有効かどうかを示します。有効な定義の先頭には、✓マークが表示されます。

- [**イベントアクション名**]

  イベントアクション定義に対する名前を表示します。

- [**説明**]

  イベントアクション定義についての説明を表示します。

- [**優先度変更**]

  イベントアクション定義の処理の適用に関する優先度を変更します。イベントアクション定義は、一覧の上から順番に処理が適用されます。

  - [**優先度を上げる**]アイコン

    当該イベントアクションの優先度を 1 つ上げます。

  - [**優先度を下げる**]アイコン

    当該イベントアクションの優先度を 1 つ下げます。

- [**操作**]

  各アイコンをクリックすることで、イベントアクション定義に対する操作を行うことができます。

  - [**編集**]アイコン

    イベントアクション定義の登録内容を変更します。[**編集**]アイコンをクリックするとイベントアクション編集画面が表示されます。詳細は、「2.3.2.3　イベントアクション定義を更新する（65 ページ）」を参照してください。

  - [**削除**]アイコン

    イベントアクション定義を削除します。詳細は、「2.3.2.4　イベントアクション定義を削除する（71 ページ）」を参照してください。

2.3.2.2　イベントアクション定義を追加する

新規にイベントアクション定義を追加する手順について説明します。

ここでは、以下のイベントアクションを実行する定義作成の例を用いて、具体的な操作手順を説明します。

- [**重要度**]が[**Warning**]以上のイベントに対し、作業担当者のメーリングリスト「nw_operator_ml@xx.zz.com」にメール通報を行う。
- 上記のイベントのうち、[**重要度**]が[**Critical**]以上のイベントがあった場合は、管理者のメーリングリスト「nw_admin_ml@xx.zz.com」にもメール通報を行う。

1. イベントアクション画面を表示します。

   [**イベントアクション設定**] >[**イベントアクション**] メニューをクリックします。

2. [**イベントアクションの追加**]ボタンをクリックします。

   イベントアクション追加画面が表示されます。

3. イベントアクション追加画面で適切な値を指定します。

   まずは、[**重要度**]が[**Warning**]以上のイベントに対し、作業担当者のメーリングリスト「nw_operator_ml@xx.zz.com」にメール通報を行うためのイベントアクション定義を作成します。

   a. イベントアクションの基本情報について指定します。

      - [**イベントアクション名**]

        一意に識別できるイベントアクションの名前を指定します。最大文字数は 64 文字です。

        以下に示す文字は指定することができません。

        - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~

- 先頭および末尾への半角スペース

- [**説明**]

  イベントアクション定義の内容の説明を指定します。最大文字数は 1024 文字です。

- [**このイベントアクションを有効にする**]チェックボックス

  - チェック：オン

    イベントアクション定義を有効にします。通常はオンにします。

  - チェック：オフ

    イベントアクション定義を無効にします。無効にした場合は、イベントアクションの処理を一切、実施しません。定義されたイベントアクションを一時的に停止させる場合に利用します。

- [**イベント条件の合致時に以降の照合処理を停止する**]チェックボックス

  - チェック：オン

    イベント条件に合致し、アクションを実行した後は、他のイベントアクション定義との照合を行わず、処理を停止します。

  - チェック：オフ

    イベント条件に合致し、アクションを実行した後も、他のイベントアクション定義との照合を行います。

本例では、以下のような設定値で、概要情報を指定します。

- [**イベントアクション名**]

  「メール通報(作業担当者向け)」

- [**説明**]

  「Warning 以上のイベントが発生した場合に、作業担当者へメール通報するための定義」

- [**このイベントアクションを有効にする**]チェックボックス： オン

- [**イベント条件の合致時に以降の照合処理を停止する**]チェックボックス： オン

b. アクションを実行するイベント条件を指定します。

- イベント条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから条件を追加することができます。

  追加した条件の先頭に表示する[−]アイコンをクリックすると追加した条件を取り消すことができます。

- イベント条件の指定

イベントデータに含まれる項目に対し、以下の 2 つの方法で、条件指定を行います。条件指定の方法は、選択した項目ごとに異なります。

- チェックボックスによる指定

  選択した項目に合わせて表示するチェックボックスを用いて、条件指定を行います。対象項目は以下の通りです。

  * 対象項目：

    [**重要度**]

- キーワードの指定

  選択した項目に対して、キーワードと照合方法を指定します。対象項目は以下の通りです。

  * 対象項目：

    [**概要**]、[**詳細**]、[**対処**]、[**発生元ノード**]、[**発生元インターフェイス**]、[**発生リージョン**]、[**IPv4 アドレス**]、[**IPv6 アドレス**]、[**アプリケーション名**]

  照合方法については、以下を指定することができます。

  * 照合方法：

    [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

    [**IPv4 アドレス**]、[**IPv6 アドレス**]に対しては、[**は次と等しい**](一致)、[**は次と異なる**](不一致)のみ指定することができます。

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

本例では、以下のような設定値で、イベント条件を指定します。

- [**重要度**]

  以下のチェックボックスをオン

  [**Fatal**]、[**Critical**]、[**Error**]、[**Warning**]

c. 実行するアクション内容を指定します。

アクションの種類として、以下の 3 つから選択します。

- [**メール通報**]

  イベント条件に合致したイベントの内容を指定した宛先にメール送信します。

  [**メール通報**]の[＋]アイコンをクリックし、以下の項目を指定します。

- [**アクション名**]

  アクションを識別する名前を指定します。最大文字数は 128 文字です。

  以下に示す文字は指定することができません。

  * 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~

  * 先頭および末尾への半角スペース

  [**アクション名**]は、アクションログにおける実行内容の識別情報として利用します。

- [**メールサーバー名**]

  事前に設定したメールサーバーをプルダウンメニューから選択します。

- [**To**]、[**Cc**]

  メール送信する宛先を指定します。複数の宛先を指定する場合は、コンマ(,)で区切って指定します。

  ヒント

  複数の宛先へメール通報したい場合は、メーリングリストの活用を推奨します。

- [**件名**]

  送信するメールの件名を指定します。最大文字数は 128 文字です。

- [**本文**]

  送信するメールの本文を指定します。

ヒント

メールの文字コードとしては、UTF-8 を利用しています。

- [**コマンド実行**]

IMS コンポーネントをインストールしたサーバー上のコマンドを実行します。

[**コマンド実行**]の[＋]アイコンをクリックし、以下の項目を指定します。

- [**アクション名**]

  アクションを識別する名前を指定します。最大文字数は 128 文字です。

  以下に示す文字は指定することができません。

  * 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~

  * 先頭および末尾への半角スペース

  [**アクション名**]は、アクションログにおける実行内容の識別情報として利用します。

- [**コマンド**]

イベント条件に合致した場合に実行するコマンドを絶対パスで指定します。

- [**コマンド引数**]

  コマンドのオプションや引数を指定します。

- [**作業ディレクトリ**]

  起動したコマンドで利用する作業ディレクトリを指定します。

⚠ 注意

コマンド実行アクションには、以下のような性質のコマンドを登録することはできません。

- コマンド実行中に、ユーザーによる入力や応答を必要とするコマンド
- コマンド実行が終了せずに常駐するコマンド

- [**SystemManager G メッセージ連携**]

  イベント条件に合致したイベントのメッセージを SystemManager G に転送します。[**SystemManager G メッセージ連携**]の[＋]アイコンをクリックすることで設定が行われます。

ヒント

- 設定ファイル (ims-conf.ini) に SystemManager G 情報を登録していない場合は、[＋]アイコンのクリック時にエラーメッセージが表示されます。
- 転送先として指定できる SystemManager G は 1 つだけです。

追加したアクション内容を削除する場合は、各設定に対する[**削除**]ボタンをクリックします。

[**メール通報**]の[**件名**]や[**本文**]、[**コマンド実行**]の[**コマンド引数**]の指定において、以下の置換文字列を利用することができます。アクションの実行時に適切な文字列に置換されます。

表 2-1　置換文字列

置換文字列	説明
{occurTime}	イベントの発生日時に置換します。
{severity}	イベントの重要度に置換します。
{sourceName}	イベントの発生元(ノード名およびインターフェイス名)に置換します。
{sourceIpv4Address}	イベントの発生元ノードの IPv4 アドレスに置換します。
{sourceIpv6Address}	イベントの発生元ノードの IPv6 アドレスに置換します。
{sourceRegion}	イベントの発生元ノードが属するリージョングループの名前に置換します。

置換文字列	説明
{summary}	イベントの概要情報に置換します。
{detail}	イベントの詳細情報に置換します。
{action}	イベントの対処情報に置換します。
{applicationName}	イベントを検知したアプリケーション名(IMS コンポーネントと接続する製品名)に置換します。
{eventDetailUrl}	イベントの詳細画面の URL に置換します。 **⚠ 注意** 事前に、以下の設定ファイルに対し、Web コンソールにアクセスするための URL を設定しておく必要があります。 • 設定ファイル <%***データパス***%>\conf\ims-conf.ini • 指定形式 `noms.core.url.external-base-url = <URL>` 設定ファイルの内容は、サービスの再起動により、動作に反映されます。
{node.location}	イベントの発生元ノードのプロパティ情報の[**設置場所**]に置換します。
{node.vendor}	イベントの発生元ノードのプロパティ情報の[**ベンダー**]に置換します。
{node.series}	イベントの発生元ノードのプロパティ情報の[**シリーズ**]に置換します。
{node.nodeType}	イベントの発生元ノードのプロパティ情報の[**ノードタイプ**]に置換します。
{node.serialNumber}	イベントの発生元ノードのプロパティ情報の[**シリアル番号**]に置換します。

また、実行するコマンド内の処理において、以下の環境変数を利用することができます。

表 2-2　環境変数

環境変数	説明
NEC_IMS_OCCUR_TIME	イベントの発生日時に置換します。
NEC_IMS_SEVERITY	イベントの重要度に置換します。
NEC_IMS_SOURCE_NAME	イベントの発生元(ノード名およびインターフェイス名)に置換します。
NEC_IMS_SOURCE_IPV4_ADDRESS	イベントの発生元ノードの IPv4 アドレスに置換します。
NEC_IMS_SOURCE_IPV6_ADDRESS	イベントの発生元ノードの IPv6 アドレスに置換します。
NEC_IMS_SOURCE_REGION	イベントの発生元ノードが属するリージョングループの名前に置換します。
NEC_IMS_SUMMARY	イベントの概要情報に置換します。

環境変数	説明
NEC_IMS_DETAIL	イベントの詳細情報に置換します。
NEC_IMS_ACTION	イベントの対処情報に置換します。
NEC_IMS_APPLICATION_NAME	イベントを検知したアプリケーション名(IMS コンポーネントと接続する製品名)に置換します。
NEC_IMS_NODE_LOCATION	イベントの発生元ノードのプロパティ情報の[**設置場所**]に置換します。
NEC_IMS_NODE_VENDOR	イベントの発生元ノードのプロパティ情報の[**ベンダー**]に置換します。
NEC_IMS_NODE_SERIES	イベントの発生元ノードのプロパティ情報の[**シリーズ**]に置換します。
NEC_IMS_NODE_NODE_TYPE	イベントの発生元ノードのプロパティ情報の[**ノードタイプ**]に置換します。
NEC_IMS_NODE_SERIAL_NUMBER	イベントの発生元ノードのプロパティ情報の[**シリアル番号**]に置換します。

本例では、以下のような設定値で、アクション内容を指定します。

- [**アクションの設定**]：[**メール通報**]
  - [**To**]： nw_operator_ml@xx.zz.com
  - [**件名**]：

```
重要度： {severity} のイベント発生
```

  - [**本文**]：

```
自動送信メールです。

{occurTime} に、以下のイベントが発生しました。
====================================
重要度： {severity}
発生元： {sourceName} ({sourceIpv4Address})
リージョン: {sourceRegion}
概要： {summary}
詳細： {detail}
対処： {action}
検出アプリケーション： {applicationName}
URL： {eventDetailUrl}
====================================
```

4. イベントアクション定義を保存します。

   設定内容を確認し、[**保存**]ボタンをクリックします。

   イベントアクション画面の一覧に、イベントアクション定義「メール通報(作業担当者向け)」が登録されます。

5. [**イベントアクションの追加**]ボタンをクリックします。

   イベントアクション追加画面が表示されます。

6. イベントアクション追加画面で、もう 1 つのイベントアクション定義の内容を指定します。

   [**重要度**] が [**Critical**] 以上のイベントに対し、管理者のメーリングリスト「nw_admin_ml@xx.zz.com」にメール通報を行うためのイベントアクション定義を作成します。

   - イベントアクションの基本情報の指定内容：
     - [**イベントアクション名**]

       「メール通報(管理者向け)」

     - [**説明**]

       「Critical 以上のイベントが発生した場合に、管理者へメール通報するための定義」

     - [**このイベントアクションを有効にする**]チェックボックス： オン
     - [**イベント条件の合致時に以降の照合処理を停止する**]チェックボックス： オフ
   - イベント条件の指定内容：
     - [**重要度**]

       以下のチェックボックスをオン

       [**Fatal**]、[**Critical**]
   - アクションの指定内容：
     - [**アクションの設定**]：[**メール通報**]
       * [**To**]： nw_admin_ml@xx.zz.com
       * [**件名**]：

         ```
         重要度： {severity} のイベント発生
         ```

       * [**本文**]：

         ```
         自動送信メールです。

         {occurTime} に、以下のイベントが発生しました。
         ====================================
         重要度： {severity}
         発生元： {sourceName} ({sourceIpv4Address})
         リージョン: {sourceRegion}
         概要： {summary}
         詳細： {detail}
         対処： {action}
         検出アプリケーション： {applicationName}
         URL： {eventDetailUrl}
         ====================================
         ```

7. イベントアクション定義を保存します。

設定内容を確認し、[**保存**]ボタンをクリックします。

イベントアクション画面の一覧に、イベントアクション定義「メール通報(管理者向け)」が登録されます。

8. イベントアクション画面で、イベントアクション定義の優先度を変更します。

   新たにイベントアクション定義を追加した場合は、[**優先度を上げる**]アイコン、または、[**優先度を下げる**]アイコンを用いて、既存のイベントアクション定義に影響を与えないように優先度を見直します。

   本例では、「メール通報(作業担当者向け)」の定義よりも、「メール通報(管理者向け)」の定義の優先度を高く設定します。

2.3.2.3　イベントアクション定義を更新する

登録済みのイベントアクション定義の内容を更新する手順について説明します。

ここでは、イベントアクション定義「メール通報(管理者向け)」のメール通報先に、IT システム部門長のメールアドレス「it_gm@xx.zz.com」を追加する例を用いて、具体的な操作手順を説明します。

1. イベントアクション画面を表示します。

   [**イベントアクション設定**] >[**イベントアクション**] メニューをクリックします。

2. 更新対象のイベントアクション定義「メール通報(管理者向け)」の[**編集**]アイコンをクリックします。

   イベントアクション定義「メール通報(管理者向け)」に対するイベントアクション編集画面が表示されます。

3. イベントアクション編集画面で更新対象の項目の入力値を変更します。

   以下のすべての項目に対し、変更の操作が行えます。

   - イベントアクションの基本情報
     - [**イベントアクション名**]

       一意に識別できるイベントアクションの名前を指定します。最大文字数は 64 文字です。

       以下に示す文字は指定することができません。

       * 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
       * 先頭および末尾への半角スペース

     - [**説明**]

       イベントアクション定義の内容の説明を指定します。最大文字数は 1024 文字です。

- [**このイベントアクションを有効にする**]チェックボックス
  * チェック：オン

    イベントアクション定義を有効にします。通常はオンにします。
  * チェック：オフ

    イベントアクション定義を無効にします。無効にした場合は、イベントアクションの処理を一切、実施しません。定義されたイベントアクションを一時的に停止させる場合に利用します。
- [**イベント条件の合致時に以降の照合処理を停止する**]チェックボックス
  * チェック：オン

    イベント条件に合致し、アクションを実行した後は、他のイベントアクション定義との照合を行わず、処理を停止します。
  * チェック：オフ

    イベント条件に合致し、アクションを実行した後も、他のイベントアクション定義との照合を行います。

• アクションを実行するイベント条件
- イベント条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから条件を追加することができます。

  追加した条件の先頭に表示する[ー]アイコンをクリックすると追加した条件を取り消すことができます。
- イベント条件の指定

  イベントデータに含まれる項目に対し、以下の 2 つの方法で、条件指定を行います。条件指定の方法は、選択した項目ごとに異なります。
  * チェックボックスによる指定

    選択した項目に合わせて表示するチェックボックスを用いて、条件指定を行います。対象項目は以下の通りです。
    + 対象項目：

      [**重要度**]
  * キーワードの指定

    選択した項目に対して、キーワードと照合方法を指定します。対象項目は以下の通りです。
    + 対象項目：

      [**概要**]、[**詳細**]、[**対処**]、[**発生元ノード**]、[**発生元インターフェイス**]、[**発生リージョン**]、[**IPv4 アドレス**]、[**IPv6 アドレス**]、[**アプリケーション名**]

照合方法については、以下を指定することができます。

+ 照合方法：

  [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

  [**IPv4 アドレス**]、[**IPv6 アドレス**]に対しては、[**は次と等しい**](一致)、[**は次と異なる**](不一致)のみ指定することができます。

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

- 実行するアクション内容

  アクションの種類として、以下の 3 つから選択します。

  - [**メール通報**]

    イベント条件に合致したイベントの内容を指定した宛先にメール送信します。

    [**メール通報**]の[＋]アイコンをクリックし、以下の項目を指定します。

    * [**アクション名**]

      アクションを識別する名前を指定します。最大文字数は 128 文字です。

      以下に示す文字は指定することができません。

      + 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
      + 先頭および末尾への半角スペース

      [**アクション名**]は、アクションログにおける実行内容の識別情報として利用します。

    * [**メールサーバー名**]

      事前に設定したメールサーバーをプルダウンメニューから選択します。

    * [**To**]、[**Cc**]

      メール送信する宛先を指定します。複数の宛先を指定する場合は、コンマ(,)で区切って指定します。

      ヒント

      複数の宛先へメール通報したい場合は、メーリングリストの活用を推奨します。

    * [**件名**]

      送信するメールの件名を指定します。最大文字数は 128 文字です。

    * [**本文**]

送信するメールの本文を指定します。

ヒント

メールの文字コードとしては、UTF-8 を利用しています。

- [**コマンド実行**]

IMS コンポーネントをインストールしたサーバー上のコマンドを実行します。[**コマンド実行**]の[＋]アイコンをクリックし、以下の項目を指定します。

* [**アクション名**]

アクションを識別する名前を指定します。最大文字数は 128 文字です。

以下に示す文字は指定することができません。

+ 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
+ 先頭および末尾への半角スペース

[**アクション名**]は、アクションログにおける実行内容の識別情報として利用します。

* [**コマンド**]

イベント条件に合致した場合に実行するコマンドを絶対パスで指定します。

* [**コマンド引数**]

コマンドのオプションや引数を指定します。

* [**作業ディレクトリ**]

起動したコマンドで利用する作業ディレクトリを指定します。

⚠ 注意

コマンド実行アクションには、以下のような性質のコマンドを登録することはできません。

- コマンド実行中に、ユーザーによる入力や応答を必要とするコマンド
- コマンド実行が終了せずに常駐するコマンド

- [**SystemManager G メッセージ連携**]

イベント条件に合致したイベントのメッセージを SystemManager G に転送します。[**SystemManager G メッセージ連携**]の[＋]アイコンをクリックすることで設定が行われます。

ヒント

- 設定ファイル (ims-conf.ini) に SystemManager G 情報を登録していない場合は、[＋]アイコンのクリック時にエラーメッセージが表示されます。

- 転送先として指定できる SystemManager G は 1 つだけです。

追加したアクション内容を削除する場合は、各設定に対する[**削除**]ボタンをクリックします。

[**メール通報**]の[**件名**]や[**本文**]、[**コマンド実行**]の[**コマンド引数**]の指定において、以下の置換文字列を利用することができます。アクションの実行時に適切な文字列に置換されます。

表 2-3　置換文字列

置換文字列	説明
{occurTime}	イベントの発生日時に置換します。
{severity}	イベントの重要度に置換します。
{sourceName}	イベントの発生元(ノード名およびインターフェイス名)に置換します。
{sourceIpv4Address}	イベントの発生元ノードの IPv4 アドレスに置換します。
{sourceIpv6Address}	イベントの発生元ノードの IPv6 アドレスに置換します。
{sourceRegion}	イベントの発生元ノードが属するリージョングループの名前に置換します。
{summary}	イベントの概要情報に置換します。
{detail}	イベントの詳細情報に置換します。
{action}	イベントの対処情報に置換します。
{applicationName}	イベントを検知したアプリケーション名(IMS コンポーネントと接続する製品名)に置換します。

{eventDetailUrl}	イベントの詳細画面の URL に置換します。
	⚠ 注意
	事前に、以下の設定ファイルに対し、Web コンソールにアクセスするための URL を設定しておく必要があります。
	• 設定ファイル
	`<%データパス%>\conf\ims-conf.ini`
	• 指定形式
	`noms.core.url.external-base-url = <URL>`
	設定ファイルの内容は、サービスの再起動により、動作に反映されます。

{node.location}	イベントの発生元ノードのプロパティ情報の[**設置場所**]に置換します。
{node.vendor}	イベントの発生元ノードのプロパティ情報の[**ベンダー**]に置換します。
{node.series}	イベントの発生元ノードのプロパティ情報の[**シリーズ**]に置換します。

置換文字列	説明
{node.nodeType}	イベントの発生元ノードのプロパティ情報の[**ノードタイプ**]に置換します。
{node.serialNumber}	イベントの発生元ノードのプロパティ情報の[**シリアル番号**]に置換します。

また、実行するコマンド内の処理において、以下の環境変数を利用することができます。

表 2-4　環境変数

環境変数	説明
NEC_IMS_OCCUR_TIME	イベントの発生日時に置換します。
NEC_IMS_SEVERITY	イベントの重要度に置換します。
NEC_IMS_SOURCE_NAME	イベントの発生元(ノード名およびインターフェイス名)に置換します。
NEC_IMS_SOURCE_IPV4_ADDRESS	イベントの発生元ノードの IPv4 アドレスに置換します。
NEC_IMS_SOURCE_IPV6_ADDRESS	イベントの発生元ノードの IPv6 アドレスに置換します。
NEC_IMS_SOURCE_REGION	イベントの発生元ノードが属するリージョングループの名前に置換します。
NEC_IMS_SUMMARY	イベントの概要情報に置換します。
NEC_IMS_DETAIL	イベントの詳細情報に置換します。
NEC_IMS_ACTION	イベントの対処情報に置換します。
NEC_IMS_APPLICATION_NAME	イベントを検知したアプリケーション名(IMS コンポーネントと接続する製品名)に置換します。
NEC_IMS_NODE_LOCATION	イベントの発生元ノードのプロパティ情報の[**設置場所**]に置換します。
NEC_IMS_NODE_VENDOR	イベントの発生元ノードのプロパティ情報の[**ベンダー**]に置換します。
NEC_IMS_NODE_SERIES	イベントの発生元ノードのプロパティ情報の[**シリーズ**]に置換します。
NEC_IMS_NODE_NODE_TYPE	イベントの発生元ノードのプロパティ情報の[**ノードタイプ**]に置換します。
NEC_IMS_NODE_SERIAL_NUMBER	イベントの発生元ノードのプロパティ情報の[**シリアル番号**]に置換します。

本例では、[**メール通報**]の指定内容において、[**Cc**]欄に IT システム部門長のメールアドレス「it_gm@xx.zz.com」を入力します。その他の項目については、変更しません。

4. 変更内容を保存します。

   変更内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、イベントアクション定義が更新されます。

イベントアクション定義の更新内容によっては、既存のイベントアクション定義の動作に影響を与えてしまう場合があります。必要に応じて、イベントアクション画面の一覧で、イベントアクション定義の優先度の見直しを行ってください。

2.3.2.4　イベントアクション定義を削除する

登録済みのイベントアクション定義を削除するための手順について説明します。

1. イベントアクション画面を表示します。

   [**イベントアクション設定**] >[**イベントアクション**] メニューをクリックします。

2. 削除対象のイベントアクション定義の[**削除**]アイコンをクリックします。

   削除処理に対する確認ダイアログが表示されます。

3. 確認ダイアログで内容を確認します。

4. 削除を実行します。

   確認ダイアログの[**OK**]ボタンをクリックします。

   イベントアクション画面の一覧から、指定したイベントアクション定義の情報が削除されます。

第 3 章
運用時の各種設定

Web コンソールを利用した運用時に、必要に応じて行う環境設定の方法について説明します。

目次

3.1　ダッシュボード定義を管理する

現在のネットワーク性能やイベントの発生状況を即座に把握するために利用するダッシュボードの定義について説明します。

ダッシュボードは、様々な観点でネットワークの状況を即座に把握するためのホーム画面として提供しています。Web コンソールにログインするとユーザー毎に設定したダッシュボードが最初に表示されます。事前に、作業毎に関連する情報をまとめたダッシュボードを複数定義しておくことで、作業毎にダッシュボードの表示を切り替えながら運用していくことが可能です。

個々の作業に対応したダッシュボード定義の作成や管理については、ダッシュボード一覧画面で行います。

3.1.1　ダッシュボード一覧画面

ダッシュボード一覧画面について説明します。

ダッシュボード一覧画面では、ダッシュボード定義の内容確認、および、操作(追加、編集、削除)を行います。

ダッシュボード一覧画面は、 [**ダッシュボード**] メニューをクリックして表示するダッシュボード画面の[**ダッシュボード一覧**]アイコンをクリックして表示します。

ヒント

アドミニストレーター、または、オペレーターの役割を持つグループに属するユーザーの場合に、ダッシュボード画面の[**ダッシュボード一覧**]アイコンが表示され、ダッシュボード一覧画面を表示することができます。

図 3-1　ダッシュボード一覧画面

- [**ダッシュボードの追加**]アイコン

ダッシュボード定義を新規に追加します。[**ダッシュボードの追加**]アイコンをクリックすると、ダッシュボード追加画面が表示されます。詳細は、「3.1.2　ダッシュボードの定義を追加する（75 ページ）」を参照してください。

ダッシュボード一覧

- [**ダッシュボード名**]

  ダッシュボードの名前を表示します。

  ヒント

  ✓マークは、ログイン時に、最初に表示するダッシュボードとして設定していることを示します。

- [**説明**]

  ダッシュボードの定義内容についての説明を表示します。

- [**操作**]

  各アイコンをクリックすることで、ダッシュボードの定義内容に対する操作を行うことができます。

  - [**編集**]アイコン

    ダッシュボードの定義内容を変更します。[**編集**]アイコンをクリックするとダッシュボード編集画面が表示されます。詳細は、「3.1.3　ダッシュボードの定義を更新する（78 ページ）」を参照してください。

    ⚠ 注意

    - ビルトインダッシュボードに対しては、編集することができません。
    - オペレーターの役割を持つグループに属しているユーザーの場合は、自分で作成したダッシュボード定義に対してのみ編集することができます。

  - [**削除**]アイコン

    ダッシュボードの定義を削除します。詳細は、「3.1.4　ダッシュボードの定義を削除する（81 ページ）」を参照してください。

    ⚠ 注意

    - ビルトインダッシュボードに対しては、削除することができません。
    - オペレーターの役割を持つグループに属しているユーザーの場合は、自分で作成したダッシュボード定義に対してのみ削除することができます。

  - [**コピー**]アイコン

既存のダッシュボードの定義内容を利用して、新規のダッシュボードを追加します。[**コピー**]アイコンをクリックすると、ダッシュボードの定義内容を含んだ形で、ダッシュボード追加画面が表示されます。

登録済みの定義内容から一部を変更し、新たなダッシュボード定義を作成する場合に利用します。詳細は、「3.1.2　ダッシュボードの定義を追加する（75 ページ）」を参照してください。

3.1.2　ダッシュボードの定義を追加する

新規にダッシュボードの定義を登録する手順について説明します。

1. ダッシュボード一覧画面を表示します。

   [**ダッシュボード**] メニューをクリックしてダッシュボード画面を表示します。次に、ダッシュボード画面の[**ダッシュボード一覧**]アイコンをクリックします。

2. [**ダッシュボードの追加**]アイコンをクリックします。

   ヒント

   既存のダッシュボードの定義内容を利用して、新規のダッシュボードを追加する場合は、[**ダッシュボードの追加**]アイコンではなく、元になるダッシュボード定義の[**コピー**]アイコンをクリックしてください。

   ダッシュボード追加画面が表示されます。

3. ダッシュボードの基本情報を指定します。

   ダッシュボード追加画面で、以下の項目を指定します。

   - [**ダッシュボード名**]

     一意に識別できるダッシュボードの名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**説明**]

     ダッシュボード内容の説明を指定します。最大文字数は 1024 文字です。

   - [**ウィジェット列数**]

     ダッシュボード上で、横に並べることができるウィジェットの最大数を指定します。1～8 列の範囲で指定でき、デフォルト値は「3 列」です。

ヒント

[**カレントアラート**]ウィジェットなど、一部のウィジェットにおいては、複数列分の幅をとります。

- [**表示のデフォルト設定**]

  ダッシュボードの表示直後に採用する表示設定のデフォルト値を指定します。

  - [**期間**]

    各ウィジェットで表示するデータの期間をプルダウンメニュー([**過去 15 分**]、[**過去 30 分**]、[**過去 1 時間**]、[**過去 6 時間**]、[**過去 24 時間**]、[**過去 48 時間**]、[**過去 72 時間**])から選択します。デフォルト値は、[**過去 1 時間**]です。

  - [**件数**]

    各ウィジェットで表示するランキングデータの件数をプルダウンメニュー([**トップ 5**]、[**トップ 10**]、[**トップ 20**])から選択します。デフォルト値は、[**トップ 5**]です。

  - [**更新間隔**]

    ダッシュボードで表示するデータの更新間隔をプルダウンメニュー([**1 分**]、[**5 分**]、[**15 分**]、[**なし**])から選択します。デフォルト値は、[**1 分**]です。

4. ウィジェットを追加します。

   以下の手順で、ウィジェットを 1 つずつ追加していきます。

ヒント

1 つのダッシュボードに配置できるウィジェットの最大数は 16 個です。

a. ダッシュボード追加画面の[**ウィジェット追加**]ボタンをクリックします。

   ウィジェット追加画面が表示されます。

b. ウィジェット追加画面で追加するウィジェットの種類を選択します。

   最初に、プルダウンメニューから製品名を選択します。製品名を選択すると当該製品が提供するウィジェットの種類が[**ウィジェット種別**]に表示されます。

   次に、表示されたウィジェットの中から追加するウィジェットを選択します。

   選択したウィジェットに合わせた設定項目が表示されます。

c. ウィジェットに対する設定を行います。

   - [**タイトル**]

     ウィジェットに対するタイトルを指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~

- 先頭および末尾への半角スペース

デフォルト値はウィジェットの種別名です。

- [**リージョン**]

対象となるリージョングループをプルダウンメニューから選択します。

以下の項目については、ウィジェット種別に応じて指定します。

- [**件数**]

ウィジェット固有にランキング表示の件数を設定したい場合に指定します。ウィジェット固有の件数は、プルダウンメニュー([**ダッシュボード画面に合わせる**]、[**トップ 5**]、[**トップ 10**]、[**トップ 20**])から選択します。デフォルト値は、[**ダッシュボード画面に合わせる**]です。

[**件数**]の指定値に関係せず表示を行うウィジェットでは、[**件数**]のプルダウンメニューは表示されません。

- [**グラフタイプ**]

円グラフ、および、線グラフの両方を表示できるウィジェットでは、ダッシュボード画面の表示時に、最初に表示するグラフタイプ([**円グラフ**]、[**線グラフ**])を選択します。デフォルト値は、[**線グラフ**]です。

- [**単位**]

NFA が提供する通信量を表示するウィジェットでは、通信量の表示単位を[**bps/bytes**]、[**pps/packets**]から選択します。デフォルト値は、[**bps/bytes**]です。

- 対象範囲(ノード、インターフェイス)の選択

データの分析範囲を指定できるウィジェットについては、対象とする範囲を指定します。

- [**分析対象**]の指定

ウィジェットで表示するデータの分析対象を[**すべてのノード**]、[**ノード**]、[**インターフェイス**]のいずれかから選択します。ウィジェットの種類によって、選択できる選択肢は異なります。

[**ノード**]、または、[**インターフェイス**]を選択した場合は、具体的なノードやネットワークインターフェイスの選択を行います。

ヒント

NFA 3.2 以降を利用している場合、一部のウィジェットでは分析対象のネットワークインターフェイスに対して、抽出するフローの方向を指定することができます。

d. ウィジェットを登録します。

設定内容を確認し、[**OK**]ボタンをクリックします。

ダッシュボード追加画面に設定したウィジェットが登録されます。

追加したいウィジェットの数に応じて、本手順を繰り返し実施します。

追加したウィジェットの内容を変更したい場合は、ウィジェットの[**編集**]アイコンをクリックして、ウィジェット編集画面を表示します。ウィジェット編集画面では、ウィジェット種別を選択した後に指定したすべての項目の内容変更が可能です。

5. ウィジェットの表示位置を調整します。
   - ウィジェットの表示位置を変更する場合

     表示位置を変えたいウィジェットにカーソルを重ねてドラッグし、移動先でドロップします。
   - 不要なウィジェットを削除する場合

     ウィジェットの[**削除**]アイコンをクリックします。
6. ダッシュボードの定義内容を保存します。

   設定内容を確認し、[**保存**]ボタンをクリックします。

   ダッシュボード一覧画面に設定したダッシュボードが追加されます。

3.1.3　ダッシュボードの定義を更新する

登録済みのダッシュボードの定義内容を更新する手順について説明します。

ヒント

オペレーターの役割を持つグループに属しているユーザーの場合は、自分で作成したダッシュボード定義に対してのみ更新することができます。

1. ダッシュボード一覧画面を表示します。

   [**ダッシュボード**] メニューをクリックしてダッシュボード画面を表示します。次に、ダッシュボード画面の[**ダッシュボード一覧**]アイコンをクリックします。
2. 更新対象のダッシュボードの[**編集**]アイコンをクリックします。

   当該ダッシュボードに対するダッシュボード編集画面が表示されます。
3. ダッシュボードの基本情報を更新します。

   ダッシュボード編集画面では、以下のすべての項目に対し、変更の操作が行えます。
   - [**ダッシュボード名**]

     一意に識別できるダッシュボードの名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。
     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

- [**説明**]

  ダッシュボード内容の説明を指定します。最大文字数は 1024 文字です。

- [**ウィジェット列数**]

  ダッシュボード上で、横に並べることができるウィジェットの最大数を指定します。1～8 列の範囲で指定できます。

  ヒント

  [**カレントアラート**]ウィジェットなど、一部のウィジェットにおいては、複数列分の幅をとります。

- [**表示のデフォルト設定**]

  ダッシュボードの表示設定のデフォルト値を指定します。

  - [**期間**]

    各ウィジェットで表示するデータの期間をプルダウンメニュー([**過去 15 分**]、[**過去 30 分**]、[**過去 1 時間**]、[**過去 6 時間**]、[**過去 24 時間**]、[**過去 48 時間**]、[**過去 72 時間**])から選択します。

  - [**件数**]

    各ウィジェットで表示するランキングデータの件数をプルダウンメニュー([**トップ 5**]、[**トップ 10**]、[**トップ 20**])から選択します。

  - [**更新間隔**]

    ダッシュボードで表示するデータの更新間隔をプルダウンメニュー([**1 分**]、[**5 分**]、[**15 分**]、[**なし**])から選択します。

4. ウィジェットを追加します。

   新規にウィジェットを追加する場合は、以下の手順を実施します。

   ヒント

   1 つのダッシュボードに配置できるウィジェットの最大数は 16 個です。

   a. ダッシュボード編集画面の[**ウィジェット追加**]ボタンをクリックします。

      ウィジェット追加画面が表示されます。

   b. ウィジェット追加画面で追加するウィジェットの種類を選択します。

      最初に、プルダウンメニューから製品名を選択します。製品名を選択すると当該製品が提供するウィジェットの種類が[**ウィジェット種別**]に表示されます。

      次に、表示されたウィジェットの中から追加するウィジェットを選択します。

      選択したウィジェットに合わせた設定項目が表示されます。

   c. ウィジェットに対する設定を行います。

- [**タイトル**]

  ウィジェットに対するタイトルを指定します。最大文字数は 32 文字です。

  以下に示す文字は指定することができません。

  - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
  - 先頭および末尾への半角スペース

  デフォルト値はウィジェットの種別名です。

- [**リージョン**]の指定

  対象となるリージョングループをプルダウンメニューから選択します。

以下の項目については、ウィジェット種別に応じて指定します。

- [**件数**]

  ウィジェット固有にランキング表示の件数を設定したい場合に指定します。ウィジェット固有の件数は、プルダウンメニュー([**ダッシュボード画面に合わせる**]、[**トップ 5**]、[**トップ 10**]、[**トップ 20**])から選択します。デフォルト値は、[**ダッシュボード画面に合わせる**]です。

  [**件数**]の指定値に関係せず表示を行うウィジェットでは、[**件数**]のプルダウンメニューは表示されません。

- [**グラフタイプ**]

  円グラフ、および、線グラフの両方を表示できるウィジェットでは、ダッシュボード画面の表示時に、最初に表示するグラフタイプ([**円グラフ**]、[**線グラフ**])を選択します。デフォルト値は、[**線グラフ**]です。

- [**単位**]

  NFA が提供する通信量を表示するウィジェットでは、通信量の表示単位をプルダウンメニュー([**bps**]、[**pps**])から選択します。デフォルト値は、[**bps**]です。

- 対象範囲(ノード、インターフェイス)の選択

  データの分析範囲を指定できるウィジェットについては、対象とする範囲を指定します。

  - [**分析対象**]の指定

    ウィジェットで表示するデータの分析対象を[**すべてのノード**]、[**ノード**]、[**インターフェイス**]のいずれかから選択します。ウィジェットの種類によって、選択できる選択肢は異なります。

    [**ノード**]、または、[**インターフェイス**]を選択した場合は、具体的なノードやネットワークインターフェイスの選択を行います。

ヒント

NFA 3.2 以降を利用している場合、一部のウィジェットでは分析対象のネットワークインターフェイスに対して、抽出するフローの方向を指定することができます。

d. ウィジェットを登録します。

設定内容を確認し、[**OK**]ボタンをクリックします。

ダッシュボード編集画面に設定したウィジェットが登録されます。

追加したいウィジェットの数に応じて、本手順を繰り返し実施します。

5. 登録済みのウィジェットの内容を更新します。

ウィジェットの内容を変更したい場合は、ウィジェットの[**編集**]アイコンをクリックして、ウィジェット編集画面を表示します。ウィジェット編集画面では、ウィジェット種別を選択した後に指定したすべての項目の内容変更が可能です。

6. 不要なウィジェットを削除します。

削除対象のウィジェットの[**削除**]アイコンをクリックします。

7. ウィジェットの表示位置を変更します。

表示位置を変えたいウィジェットにカーソルを重ねてドラッグし、移動先でドロップします。

8. 変更内容を保存します。

変更内容を確認し、[**保存**]ボタンをクリックします。

指定した内容で、ダッシュボードが更新されます。

3.1.4　ダッシュボードの定義を削除する

登録済みのダッシュボードの定義を削除するための手順について説明します。

ヒント

オペレーターの役割を持つグループに属しているユーザーの場合は、自分で作成したダッシュボード定義に対してのみ削除することができます。

1. ダッシュボード一覧画面を表示します。

[**ダッシュボード**] メニューをクリックしてダッシュボード画面を表示します。次に、ダッシュボード画面の[**ダッシュボード一覧**]アイコンをクリックします。

2. 削除対象のダッシュボードの[**削除**]アイコンをクリックします。

削除処理に対する確認ダイアログが表示されます。

3. 確認ダイアログで内容を確認します。

4. 削除を実行します。

確認ダイアログの[**OK**]ボタンをクリックします。

ダッシュボード一覧画面から、指定したダッシュボードの情報が削除されます。

⚠ 注意

ユーザー情報の設定において、ログイン時に、最初に表示する[**ダッシュボード**]として設定されているダッシュボードであっても削除することができます。この場合は、ユーザーのログイン時に、プロファイル編集画面から[**初期表示ダッシュボード**]の設定を再度行う必要があります。

3.2　トポロジーマップの表示内容を編集する

Web コンソールにおけるトポロジーマップの表示方法とその編集手順について説明します。

Web コンソールでは、NetvisorPro のマップビューに登録している以下の構成情報を取り込み、Web コンソール用のトポロジーマップのデータを作成します。

- ネットワーク構成(マップの階層構成)
- ノード情報
- ノード間の接続情報

Web コンソールでは、このデータを用いて、トポロジーマップ画面でネットワーク構成のマップを表示します。

ヒント

IMS コンポーネントと NetvisorPro の接続設定を行っている場合は、IMS コンポーネントが、自動的に上記の情報を取り込み、Web コンソール用のマップデータを作成します。

Web コンソールには NetvisorPro の上記の情報以外を取り込まないため、NetvisorPro の各マップビューに配置した図形や背景画像は、Web コンソールのトポロジーマップ画面には反映されません。トポロジーマップ画面で表示するマップにも、図形や背景画像を挿入したり、ノードを示すアイコンの位置を変更したりしたい場合は、別途、Web コンソール側でもマップの編集作業を行ってください。

マップの編集作業は、トポロジーマップ画面の[**表示モード**]を[**編集モード**]に切り替えて行います。

3.2.1　編集モードと編集ツール

トポロジーマップ画面の[**編集モード**]と[**編集ツール**]について説明します。

トポロジーマップ画面では、[**表示モード**]を[**編集モード**]に切り替えることで、マップの様々な編集作業を行うことができます。

トポロジーマップ画面は、[**トポロジーマップ**] メニューをクリックして表示します。[**編集モード**]への切り替えは、[**表示モード**]のプルダウンメニューから[**編集モード**]を選択します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、[**編集モード**]へ切り替えることができます。

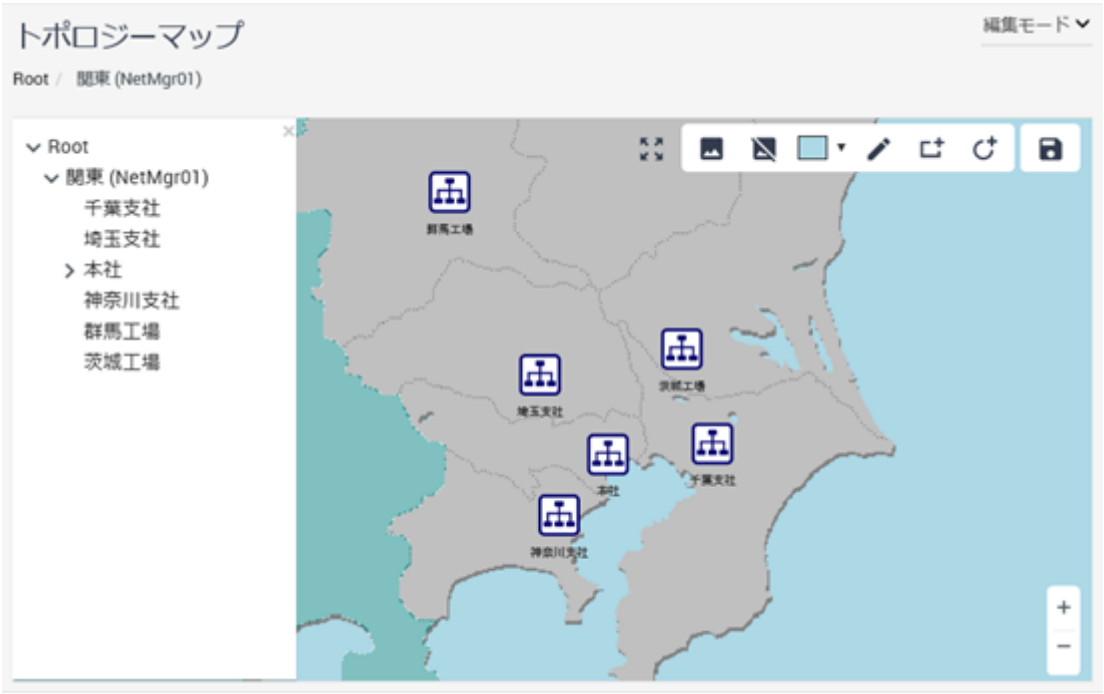

図 3-2　トポロジーマップ画面(編集モード)

[**表示モード**]を[**編集モード**]へ切り替えると[**編集ツール**]が表示されます。また、[**マップビュー**]のノードアイコン、および、マップアイコンの位置を変更することができるようになります。

ヒント

ノード間を結ぶ接続線は、NetvisorPro 上のノード間の接続情報を元に描画します。接続線を編集したい場合は、NetvisorPro のマップビューで接続線([**if 線**]、[**直線**])を編集してください。

編集ツール

[**編集ツール**]の各アイコンをクリックすることで、マップの背景に図形や画像、テキストの挿入などを行うことができます。[**編集ツール**]の詳細を以下に示します。

- [**背景変更**]アイコン

  マップの背景に画像を挿入することができます。背景画像として指定できるファイル形式は、「JPG」、「GIF」、「PNG」です。

- [**背景削除**]アイコン

  マップの背景への画像の挿入を解除することができます。

- [**背景色変更**]アイコン

マップの背景色の変更を行うことができます。

- [**線**]アイコン

  [**マップビュー**]に直線を描くことができます。描いた直線に対しては、太さや色を指定することができます。

- [**矩形**]アイコン

  [**マップビュー**]に矩形を描くことができます。描いた矩形に対しては、線の太さと色、塗りつぶし色を指定することができます。また、テキストを挿入することもできます。

- [**楕円**]アイコン

  [**マップビュー**]に楕円を描くことができます。描いた楕円に対しては、線の太さと色、塗りつぶし色を指定することができます。

- [**保存**]アイコン

  ノードアイコンの位置の変更、マップ背景の編集内容を保存します。

  ⚠ 注意

  保存していない状態で、表示対象のマップ変更や画面遷移を行うと編集内容が破棄されます。必ず、編集内容を保存してから、表示対象のマップ変更、画面遷移を行うようにしてください。

図形編集ツール

[**マップビュー**]に配置した図形を選択すると[**図形編集ツール**]が表示されます。[**図形編集ツール**]の各アイコンをクリックすることで、選択した図形に対する編集を行うことができます。

- [**色変更**]アイコン

  選択した図形の塗りつぶし色を指定することができます。[**色変更**]アイコンをクリックすると、色指定のための画面が表示されます。色を指定し、[**選択**]ボタンをクリックすることで、図形の塗りつぶし色が変化します。下部の[**スライダー**]を操作すると、色の透過性の指定を行うことができます。

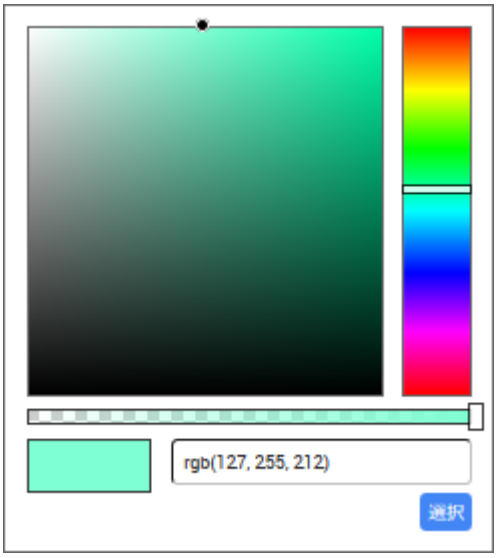

図 3-3　色の指定

- [**枠の色変更**]アイコン

  選択した図形の線の色を指定することができます。[**枠の色変更**]アイコンをクリックすると、色指定のための画面が表示されます。色を指定し、[**選択**]ボタンをクリックすることで、図形の枠の色が変化します。下部の[**スライダー**]を操作すると、色の透過性の指定を行うことができます。

- [**文字の色変更**]アイコン

  選択した図形に入力した、テキストの文字色を指定することができます。[**文字の色変更**]アイコンをクリックすると、色指定のための画面が表示されます。色を指定し、[**選択**]ボタンをクリックすることで、図形の文字色が変化します。

- [**線幅を編集**]アイコン

  選択した図形の線の太さを指定することができます。[**線幅を編集**]アイコンをクリックすると線の太さを指定するためのダイアログが表示され、[**スライダー**]を右に動かすと線が太くなります。

図 3-4　線幅の指定

- [**テキスト編集**]アイコン

選択した図形に対し、テキストを挿入することができます。[**テキスト編集**]アイコンをクリックするとテキスト入力ダイアログが表示され、テキストの入力に関する操作を行うことができます。

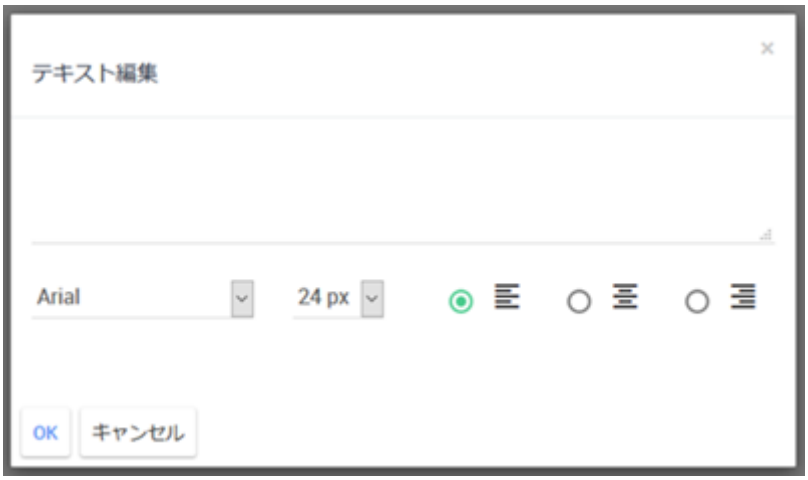

図 3-5　テキスト入力ダイアログ

- [**前へ移動**]アイコン

  選択した図形を最前面に移動することができます。

- [**後へ移動**]アイコン

  選択した図形を最背面に移動することができます。

- [**削除**]アイコン

  選択した図形を削除することができます。

3.2.2　マップ上のアイコン位置を変更する

マップ上のノード、および、マップを示すアイコンの位置を変更する手順について説明します。

1. トポロジーマップ画面を表示します。

   [**トポロジーマップ**] メニューをクリックします。

2. トポロジーマップ画面の[**表示モード**]を[**編集モード**]に切り替えます。

   [**表示モード**]のプルダウンメニューから[**編集モード**]を選択します。

3. 編集対象のマップを表示します。

   トポロジーマップ画面のツリービューから、編集対象の[**マップ**]アイコンを選択します。

   トポロジーマップ画面のマップビューに、選択した[**マップ**]アイコンに対するマップが表示されます。

4. ノードまたはマップのアイコン位置を変更します。

移動させたいアイコンをドラッグし、位置を決めてドロップします。

本手順を繰り返して、移動させたいすべてのノード、または、マップのアイコン位置を変更します。

5. マップの変更を保存します。

   変更内容を確認し、[**保存**]アイコンをクリックします。

   ⚠ 注意

   本手順を実施しない状態で、マップの移動や画面遷移を行うと変更内容がすべて破棄されます。

   マップの変更内容が保存されます。

ヒント

- マップの編集作業は、マップ単位に 1 つ 1 つ実施していきます。
- アイコン位置の変更とともに、背景の編集を行うことで、より分かりやすいマップを構成することができます。詳細は、「3.2.3　編集ツールでマップを分かりやすく編集する（87 ページ）」を参照してください。

3.2.3　編集ツールでマップを分かりやすく編集する

トポロジーマップを分かりやすく表現するための背景の編集手順について説明します。

ここでは、以下の編集を行う例を用いて、具体的な操作手順を説明します。

- フロアの構成を示す画像の挿入
- クラスタ構成の装置のグルーピングを表現する枠線(矩形)の挿入
- クラスタ構成を補足説明するテキストの挿入

1. トポロジーマップ画面を表示します。

   [**トポロジーマップ**] メニューをクリックします。

2. トポロジーマップ画面の[**表示モード**]を[**編集モード**]に切り替えます。

   [**表示モード**]のプルダウンメニューから[**編集モード**]を選択します。

3. 編集対象のマップを表示します。

   トポロジーマップ画面のツリービューから、編集対象の[**マップ**]アイコンを選択します。

   トポロジーマップ画面のマップビューに、選択した[**マップ**]アイコンに対するマップが表示されます。

4. マップの背景を編集します。

   [**編集ツール**]を活用してマップの背景の編集作業を行います。

   - 背景への画像挿入

a. [**編集ツール**]の[**背景変更**]アイコンをクリックします。

ファイルを開くダイアログが表示されます。

b. マップの背景に挿入する画像ファイルを選択します。

選択可能な画像ファイルの形式は、「JPG」、「GIF」、「PNG」です。

c. 選択した画像がマップの背景に挿入されたことを確認します。

ここでは、フロアの構成を示す画像ファイルを選択します。

- 背景への図形の挿入

a. [**編集ツール**]の図形挿入のためのアイコンをクリックします。

図形挿入のためのアイコンとは、[**線**]、[**矩形**]、[**楕円**]のアイコンのことを指します。

b. 図形を挿入します。

図形を挿入したい位置をクリックすると、図形が配置されます。

再度、図形を選択して、図形のポインターをドラッグして図形の大きさを調整し、ドロップで大きさを確定します。

挿入した図形は、ドラッグとドロップの操作により、位置を移動させることができます。

c. 挿入した図形の色を変更します。

図形を選択し、[**図形編集ツール**]の[**背景色変更**]アイコンをクリックし、塗りつぶし色を変更します。また、[**枠の色変更**]、および、[**線幅を編集**]アイコンをクリックすることで、枠の色、および、線の太さを変更することができます。

ここでは、[**矩形**]を用いて、クラスタ構成を組むノードアイコンを矩形で囲みます。また、[**背景色変更**]を用いて、塗りつぶし色を透過にします。

- 背景図形へのテキストの挿入

a. テキストを入力する図形(矩形、または、楕円)を選択します。

事前に図形を挿入しておく必要があります。

b. [**図形編集ツール**]の[**テキスト編集**]アイコンをクリックします。

c. 挿入したい文字を入力します。

ヒント

マップの背景にテキストだけを挿入したい場合は、テキストの挿入後、当該図形の線、および、塗りつぶし色を「透過」に設定します。

ここでは、クラスタ構成を組むノードアイコンを囲んだ矩形を選択し、テキストとして、「クラスタ構成」を挿入します。

5. マップの変更を保存します。

   変更内容を確認し、[**保存**]アイコンをクリックします。

   ⚠ 注意

   本手順を実施しない状態で、マップの移動や画面遷移を行うと変更内容がすべて破棄されます。

   マップの変更内容が保存されます。

ヒント

- マップの編集作業は、マップ単位に 1 つ 1 つ実施していきます。
- 背景の編集とともにアイコン位置の変更を行うことで、より分かりやすいマップを構成することができます。詳細は、「3.2.2　マップ上のアイコン位置を変更する（86 ページ）」を参照してください。

3.3　収集データを分析する

NetvisorPro、または、NFA で収集しているデータを分析する機能について説明します。

IMS コンポーネントでは、収集中の時系列データに対する以下の 2 つのデータ分析機能を提供しています。この 2 つのデータ分析機能により、ネットワークシステムの障害予兆の早期検知やキャパシティ管理業務をサポートします。

アノマリー分析

過去のデータ変動を元に分析対象データの分析モデルを作成し、作成した分析モデルを用いて、現在のデータが特異な挙動となっていないかを分析することで、アノマリー検知を行います。

一定のしきい値による監視とは異なり、データの普段とは異なる不穏な挙動を検出することができるため、ネットワークシステムの異常に関する予兆検知として活用することができます。

ヒント

- アノマリー分析では、データ変動において、一週間ごと(曜日ごと)、または、1 日ごと(24 時間ごと)におおよその周期性が見られるデータを分析対象とします。
- 分析処理に用いることができる過去の蓄積データが増加していくことで、アノマリー分析の精度が高まっていきます。アノマリー分析は、中長期的な運用の中で有効性を判断してください。

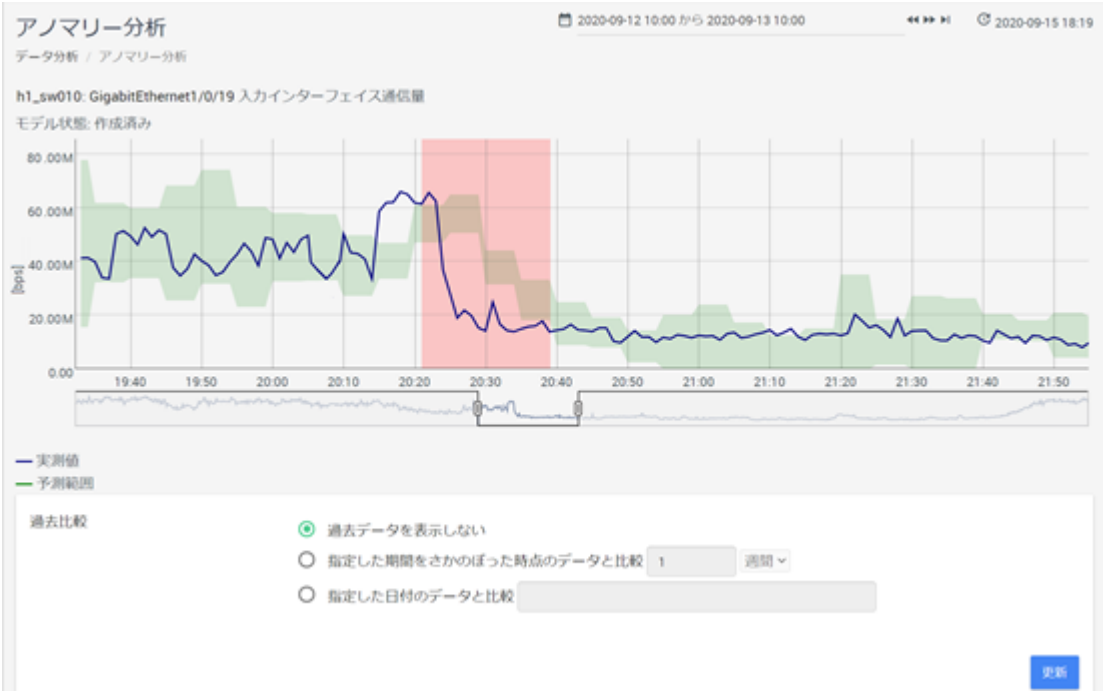

図 3-6　アノマリー分析

トレンドライン分析

現在までに収集したデータ変動状況から、データの増減に関する傾向を分析し、グラフ表示します。

数ケ月後の通信状況を予想するなど、リソースのキャパシティ管理を行う際の指標として活用することができます。

図 3-7　トレンドライン分析

データ分析機能を利用するための事前準備

データ分析機能を利用するためには、事前にどのデータを分析対象とするのかを指定する必要があります。分析対象の指定は、データ分析画面から実施します。詳細な操作方法については、「3.3.1.2　分析対象を追加する（95 ページ）」を参照してください。

アノマリー分析を実施する場合は、分析対象の指定に加え、分析ポリシーの作成、および、適用を行う必要があります。分析ポリシーでは、分析のためのパラメーター、および、アノマリー検知時の通知方法などを定義します。分析ポリシーの詳細については、「3.3.2　アノマリー検知のための分析ポリシーを定義する（99 ページ）」を参照してください。また、分析ポリシーの適用方法については、「3.3.3.1　分析ポリシーを適用する（108 ページ）」を参照してください。

ヒント

アノマリー分析において、分析対象データの周期性が崩れる期間を事前に把握している場合は、分析ポリシーにおけるスケジュールの設定を行うことで、指定期間のデータを分析処理の対象から除外することができます。

例えば、企業の特別休日やシステムのメンテナンス日など普段と異な挙動になることが明らかな期間を除外することで、不要なアノマリー検知の通知を防ぐことができます。

3.3.1　データ分析の対象を管理する

NetvisorPro、または、NFA で収集しているデータの中から、分析対象を指定することで、指定データに対する分析を行うことができます。ここでは、分析対象の指定に関する操作や管理について説明します。

3.3.1.1　データ分析画面

データ分析画面について説明します。

データ分析画面では、分析対象の内容確認、および、操作(追加、編集、削除)を行います。

データ分析画面は、[**データ分析**] メニューをクリックして表示します。

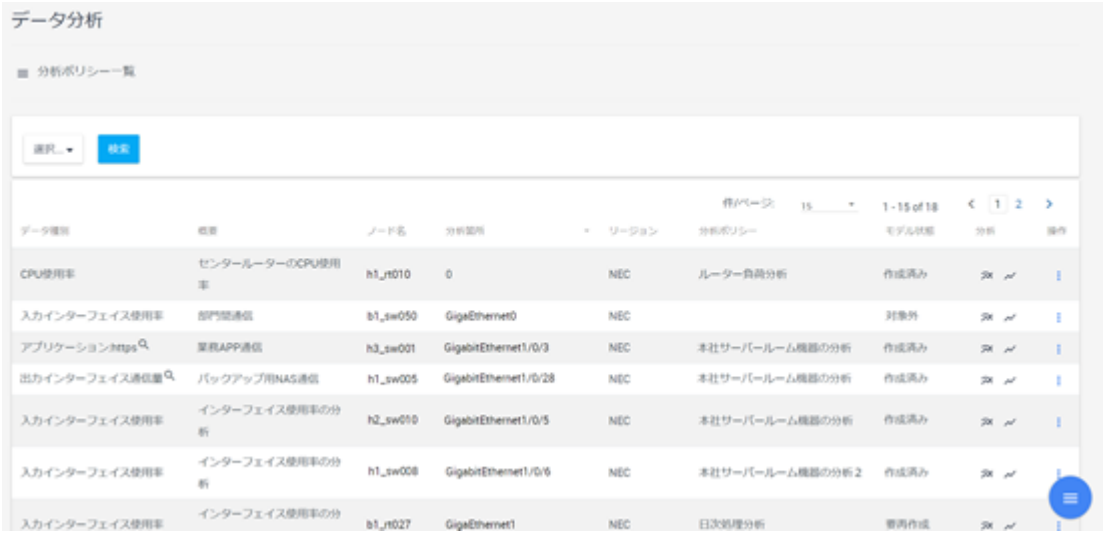

図 3-8　データ分析画面

- [**分析ポリシー一覧**]アイコン

  分析ポリシー一覧画面を表示します。分析ポリシー一覧画面では、分析ポリシーの内容確認、および、操作(追加、編集、削除)を行います。詳細は、「3.3.2.1　分析ポリシー一覧画面（99 ページ）」を参照してください。

- [**MENU**]ボタン

  画面の右下に配置する[**MENU**]ボタンにカーソルを重ねると以下の操作ボタンが表示されます。以下の操作ボタンをクリックすることで、分析対象の操作に関する各画面を表示することができます。

  - [**分析対象を追加**]ボタン

    分析対象を新規に追加します。[**分析対象を追加**]ボタンをクリックすると、分析対象追加画面が表示されます。詳細は、「3.3.1.2　分析対象を追加する（95 ページ）」を参照してください。

  - [**モデル再作成**]ボタン

    アノマリー分析のための分析モデルを再作成します。モデル再作成の対象は、現在一覧に表示されていて、状態が[**要再作成**]となっている分析対象となります。詳細は、「3.3.3.2　分析モデルを再作成する（109 ページ）」を参照してください。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、[**分析ポリシー一覧**]アイコン、および、[**MENU**]ボタンの表示や選択を行うことができます。

検索条件の指定

分析対象一覧で表示する各項目の内容に対し、条件を指定して表示する分析対象の情報を絞り込むことができます。

- 条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。

  追加した条件の先頭に表示する[ー]アイコンをクリックすると追加した条件を取り消すことができます。

- 条件指定

  分析対象一覧で表示する各項目に対し、以下の 2 つの方法で、検索条件を指定します。検索条件の指定方法は、選択した項目ごとに異なります。

  - チェックボックスによる指定

    チェックボックスを用いて、検索条件を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**モデル状態**]

  - キーワードの指定

    選択した項目に対して、キーワードと照合方法を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**データ種別**]、[**概要**]、[**ノード名**]、[**分析箇所**]、[**リージョン**]、[**分析ポリシー**]

    照合方法については、以下を指定することができます。

    * 照合方法：

      [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

条件を指定した後、[**検索**]ボタンをクリックすると、検索条件に合致した分析対象の一覧が表示されます。

分析対象一覧

- [**データ種別**]

  分析対象のデータ種別を表示します。

- [**概要**]

分析対象の概要を表示します。

- [**ノード名**]

  分析対象のノードの名前を表示します。

- [**分析箇所**]

  分析対象のインターフェイス名、または、CPU やメモリのインスタンス番号などの分析箇所に関する情報を表示します。

- [**リージョン**]

  分析対象のノードが属するリージョングループの名前を表示します。

- [**分析ポリシー**]

  アノマリー分析を行うために適用した分析ポリシーの名前を表示します。

- [**モデル状態**]

  アノマリー分析を行うための分析モデルの状態を表示します。以下のいずれかを表示します。

  - [**対象外**]

    分析ポリシーを適用していない状態であり、アノマリー分析の対象外であることを示します。

  - [**蓄積中**]

    分析モデルを作成するために必要なデータを蓄積している状態であることを示します。分析モデルの作成前の状態であり、アノマリー分析は行えません。

  - [**作成済み**]

    分析モデルの作成が完了している状態であることを示します。アノマリー分析を適切に行うことができる状態です。

  - [**再作成中**]

    分析モデルの作成中であることを示します。分析モデルの再作成を実行し、処理が未完了の場合に表示されます。

  - [**要再作成**]

    分析モデルの再作成が必要であることを示します。分析モデルに関係する分析ポリシーのパラメーターを変更した場合に表示されます。

- [**分析**]

  各アイコンをクリックすることで、データ分析結果を表示します。

  - [**アノマリー分析**]アイコン

適用した分析ポリシーに従ったアノマリー分析の結果を表示します。[**アノマリー分析**]アイコンをクリックすると、アノマリー分析画面が表示されます。詳細は、「4.5.1　アノマリーの発生状況を確認する（168 ページ）」を参照してください。

- [**トレンドライン分析**]アイコン

  トレンドライン分析の結果を表示します。[**トレンドライン分析**]アイコンをクリックすると、トレンドライン分析画面が表示されます。詳細は、「4.5.2　トレンドラインを確認する（170 ページ）」を参照してください。

- [**操作**]

[ ]アイコンをクリックすることで、分析対象に対する以下のメニューを選択することができます。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、[**操作**]欄が表示され、メニュー操作を行うことができます。

- [**概要の編集**] メニュー

  分析対象に対する概要を変更します。 [**概要の編集**] メニューを選択すると、概要編集ダイアログが表示されます。詳細は、「3.3.1.3　分析対象の概要を更新する（99 ページ）」を参照してください。

- [**分析ポリシーの適用**] メニュー

  分析対象に分析ポリシーを適用します。すでに分析ポリシーを適用している場合は、分析ポリシーを変更することができます。 [**分析ポリシーの適用**] メニューを選択すると、分析ポリシーの適用ダイアログが表示されます。詳細は、「3.3.3.1　分析ポリシーを適用する（108 ページ）」を参照してください。

- [**削除**] メニュー

  分析対象の定義、および、分析のために蓄積したデータを削除します。詳細は、「3.3.1.4　分析対象を削除する（99 ページ）」を参照してください。

1 ページに表示する分析対象の数は、プルダウンメニュー([**15**]、[**50**]、[**100**])から選択します。デフォルト値は、[**15**]です。

検索条件に合致したすべての分析対象を 1 ページで表示できない場合は、ページを切り替えて、分析対象の情報を確認します。

3.3.1.2　分析対象を追加する

新規に分析対象を追加する手順について説明します。

ここでは、「スイッチ 03」のネットワークインターフェイス「Gi1/0/1」、および、「Gi1/0/2」を通る業務サーバー「192.168.2.100」からの「https」の通信フローを分析対象として追加する例を用いて、具体的な操作手順を説明します。

1. データ分析画面を表示します。

   [ **データ分析**] メニューをクリックします。

2. [ **分析対象を追加**]ボタンをクリックします。

   分析対象追加画面が表示されます。

3. 分析対象追加画面で適切な値を指定します。

   a. 分析対象の基本情報を指定します。

      - [**製品名**]

        分析対象とするデータを収集している製品の名前をプルダウンメニューから選択します。

      - [**リージョン**]

        分析対象のノードが属するリージョングループの名前をプルダウンメニューから選択します。

      - [**データ種別**]

        分析対象とするデータの種別をプルダウンメニューから選択します。プルダウンメニューの表示内容は、[**製品名**]の選択内容に依存します。

        - WebSAM NetvisorPro V を選択している場合

          以下のデータ種別を選択することができます。

          * [**CPU 使用率**]
          * [**メモリ使用率**]
          * [**入力インターフェイス使用率**]
          * [**入力インターフェイス使用量**]
          * [**出力インターフェイス使用率**]
          * [**出力インターフェイス使用量**]
          * [**入力パケット損失率**]
          * [**入力パケット損失数**]
          * [**出力パケット損失率**]
          * [**出力パケット損失数**]
          * [**入力パケットエラー率**]
          * [**入力パケットエラー数**]
          * [**出力パケットエラー率**]
          * [**出力パケットエラー数**]

* [**応答時間(IPv4)**]
* [**応答時間(IPv6)**]

また、NetvisorPro で任意のデータ種別を設定している場合は、その値も指定することができます。

- WebSAM Network Flow Analyzer を選択している場合

以下のデータ種別を選択することができます。

* [**アプリケーション**]
* [**入力インターフェイス通信量**]
* [**出力インターフェイス通信量**]
* [**DSCP**]
* [**IP プロトコル**]

[**アプリケーション**]、[**DSCP**]、[**IP プロトコル**]を選択した場合は、さらに、[**データ種別の詳細条件**]を選択します。[🔍]欄にキーワードを指定することで、キーワードを含む選択肢のみが一覧に表示されます。表示された一覧から詳細条件を選択します。

[**製品名**]で WebSAM Network Flow Analyzer を選択している場合は、以下の[**フィルター条件**]を指定することで、より具体的な通信フローを指定することができます。

* [**送信元 IP アドレス**]
* [**宛先 IP アドレス**]
* [**送信元エンドポイントグループ**]
* [**宛先エンドポイントグループ**]
* [**送信元 AS**]
* [**宛先 AS**]

- [**概要**]

分析対象の内容に対する概要を指定します。最大文字数は、256 文字です。

ヒント

分析対象の内容を識別する際に活用する情報となります。データ種別の詳細条件などの情報をできるだけ分かり易く明記することを推奨します。

ここでは、以下の内容を指定します。

- [**製品名**]： WebSAM Network Flow Analyzer
- [**リージョン**]： 関東地区

- [**データ種別**]：[**アプリケーション**]
- [**データ種別の詳細条件**]：https
- [**フィルター条件**]：[**送信元 IP アドレス**]=192.168.2.100
- [**概要**]：

  本社コアスイッチを経由する業務サーバーの https 通信の分析

b. 分析箇所を指定します。

分析箇所となるノードやネットワークインターフェイス、分析項目のインスタンスを表示された一覧から選択します。

ここでは、「スイッチ 03」のネットワークインターフェイス「Gi1/0/1」、および、「Gi1/0/2」を選択します。

ヒント

NFA 3.2 以降を利用している場合、分析箇所のネットワークインターフェイスに対して、対象とするフローの方向を指定することができます。

c. 必要に応じて分析ポリシーを指定します。

表示されている分析ポリシーの一覧から、適用する分析ポリシーを選択します。

本操作は、アノマリー分析を実施する場合で、かつ、適用する分析ポリシーが作成済みである場合に実施します。トレンドライン分析のみを実施する場合、または、後から分析ポリシーを適用する場合は、本操作を行う必要はありません。

ヒント

分析ポリシーを適用せずに、分析対象を登録した場合、当該分析対象のアノマリー分析画面には、分析対象データのグラフのみが表示されます。アノマリー分析画面に表示された分析対象データのグラフから、挙動の周期性を確認した後に、適切な分析ポリシーを作成して適用する運用を推奨します。

4. 設定内容を確認します。

ヒント

分析対象の指定内容を保存すると、[**概要**]、および、[**分析ポリシー**]の指定内容以外は、更新することができません。十分に指定内容を確認してから保存してください。

5. 分析対象の内容を保存します。

[**保存**]ボタンをクリックします。

指定した内容で、新規に分析対象が追加されます。

データ分析画面で、指定した内容の分析対象が追加されていることを確認します。

3.3.1.3　分析対象の概要を更新する

分析対象の概要内容を更新する手順について説明します。

1. データ分析画面を表示します。

   [**データ分析**] メニューをクリックします。

2. 概要を編集する分析対象の [**概要の編集**] メニューを選択します。

   [**操作**]欄の[⋮]アイコンをクリックすると、 [**概要の編集**] メニューが表示されます。

   [**概要の編集**] メニューを選択すると、概要編集ダイアログが表示されます。

3. 概要内容を変更します。

   概要の最大文字数は 256 文字です。

4. 変更内容を保存します。

   変更内容を確認し、[**保存**]ボタンをクリックします。

   指定した内容で、分析対象の概要が更新されます。

3.3.1.4　分析対象を削除する

登録済みの分析対象を削除する手順について説明します。

分析対象を削除すると、分析のために蓄積したデータも削除されます。

1. データ分析画面を表示します。

   [**データ分析**] メニューをクリックします。

2. 削除を行う分析対象の [**削除**] メニューを選択します。

   [**操作**]欄の[⋮]アイコンをクリックすると、 [**削除**] メニューが表示されます。

   [**削除**] メニューを選択すると、削除処理に対する確認のためのダイアログが表示されます。

3. 削除を実行します。

   確認のためのダイアログの[**OK**]ボタンをクリックします。

   データ分析画面の分析対象一覧から、指定した分析対象の情報が削除されます。

3.3.2　アノマリー検知のための分析ポリシーを定義する

アノマリー検知を行うための分析ポリシーの定義について説明します。

3.3.2.1　分析ポリシー一覧画面

分析ポリシー一覧画面について説明します。

分析ポリシー一覧画面では、分析ポリシーの内容確認、および、操作(追加、編集、削除)を行います。

分析ポリシー一覧画面は、データ分析画面の [**分析ポリシー一覧**] アイコンをクリックして表示します。データ分析画面は、 [**データ分析**] メニューをクリックして表示します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、分析ポリシー一覧画面を表示することができます。

図 3-9　分析ポリシー一覧画面

- [**分析ポリシーの追加**]ボタン

  分析ポリシーを新規に追加します。[**分析ポリシーの追加**]ボタンをクリックすると、分析ポリシー追加画面が表示されます。詳細は、「3.3.2.2　分析ポリシーを追加する（101 ページ）」を参照してください。

分析ポリシー一覧

- [**名前**]

  分析ポリシーの名前を表示します。

- [**説明**]

  分析ポリシーの説明を表示します。

- [**除外期間**]

  分析処理を除外する期間を示すスケジュールの名前を表示します。

- [**操作**]

  各アイコンをクリックすることで、分析ポリシーに対する操作を行うことができます。

  - [**編集**]アイコン

分析ポリシーの登録内容を変更します。[**編集**]アイコンをクリックすると、分析ポリシー編集画面が表示されます。詳細は、「3.3.2.3　分析ポリシーを更新する（104 ページ）」を参照してください。

- [**削除**]アイコン

  分析ポリシーを削除します。詳細は、「3.3.2.4　分析ポリシーを削除する（108 ページ）」を参照してください。

- [**分析対象検索**]アイコン

  分析ポリシーを適用している分析対象を検索し、表示します。[**分析対象検索**]アイコンをクリックすると、検索条件に、当該分析ポリシーが指定された状態で、データ分析画面が表示されます。データ分析画面の詳細は、「3.3.1.1　データ分析画面（91 ページ）」を参照してください。

1 ページに表示する分析ポリシーの数は、プルダウンメニュー([**15**]、[**50**]、[**100**])から選択します。デフォルト値は、[**15**]です。

分析ポリシーを 1 ページで表示できない場合は、ページを切り替えて、分析ポリシーの情報を確認します。

3.3.2.2　分析ポリシーを追加する

新規に分析ポリシーを追加する手順について説明します。

ここでは、1 週間ごと(曜日ごと)におおよその周期性が見られる分析対象を想定した分析ポリシーを作成する例を用いて、具体的な操作手順を説明します。

1. 分析ポリシー一覧画面を表示します。
   a. データ分析画面を表示します。

      [**データ分析**] メニューをクリックします。

   b. データ分析画面の [**分析ポリシー一覧**] アイコンをクリックします。

      分析ポリシー一覧画面が表示されます。

2. [**分析ポリシーの追加**]ボタンをクリックします。

   分析ポリシー追加画面が表示されます。

3. 分析ポリシー追加画面で適切な値を指定します。
   a. 基本情報を指定します。

      - [**名前**]

        一意に識別できる分析ポリシーの名前を指定します。最大文字数は、64 文字です。

        以下に示す文字は指定することができません。

- 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
- 先頭および末尾への半角スペース

- [**説明**]

  分析ポリシーの内容の説明を指定します。最大文字数は、1024 文字です。

ここでは、以下の内容を指定します。

- [**名前**]： 1 週間周期データの分析(イベント通知なし)
- [**説明**]：

  1 週間ごとに周期性がみられるデータに対する分析ポリシー。アノマリー検知時のイベント通知は OFF。

b. [**アノマリー分析設定**]の内容を指定します。

- [**周期**]

  分析対象となるデータのおおよその周期性を指定します。以下のいずれかを指定します。

  デフォルト値は、[**1 週間**]です。

  - [**1 日**]

    24 時間ごとにデータ変動のおおよその周期性が見られる場合に使用します。

  - [**1 週間**]

    曜日ごとや 7 日間ごとにデータ変動のおおよその周期性が見られる場合に使用します。

- [**予測範囲係数**]

  アノマリー分析では、過去の蓄積データを元に、次に収集して得られるデータがどの範囲の値になるのかを予測し、アノマリー判定を行います。[**予測範囲係数**]は、データの予測範囲の幅を決定する係数です。係数の値が大きいと予測範囲の幅も大きくなり、データの細かな挙動に対してはアノマリー判定は行われにくくなります。

  係数は、1~5 の範囲で指定でき、デフォルト値は、[**3**]です。

- [**判定条件**]

  予測範囲に対し、実際に収集した値がどのような場合にアノマリーと判定するのかを以下のいずれかで指定します。

  デフォルト値は、[**外れたら**]です。

  - [**外れたら**]

    実際に収集した値が、予測範囲よりも大きい値、もしくは、小さい値の場合にアノマリーと判定します。

- [**上回ったら**]

  実際に収集した値が、予測範囲よりも大きい値の場合にのみ、アノマリーと判定します。

- [**下回ったら**]

  実際に収集した値が、予測範囲よりも小さい値の場合にのみ、アノマリーと判定します。

- [**検知のタイミング**]

  [**判定条件**]で指定した条件に合致した場合に、即座に、アノマリーと判定するかどうかを指定します。

  デフォルト値は、[***15* 分以上満たした場合にアノマリーを検知する**]です。

  - [**直ちにアノマリーを検知する**]

    [**判定条件**]に合致した場合、直ちにアノマリーを検知します。

  - [***<n>* 分以上満たした場合にアノマリーを検知する**]

    [**判定条件**]に合致する状態が指定時間継続した場合にのみ、アノマリーを検知します。<*n*>部分に 1 以上の数値を指定します。デフォルト値は、「15」です。

  ヒント

  インターフェイスの使用率や特定の通信フローなど、データの収集ごとに値が大きく変動するような性質のデータを分析対象とする場合は、[***<n>* 分以上満たした場合にアノマリーを検知する**]を選択し、複数のデータの挙動からアノマリーを判断する運用を推奨します。

  上記に対し、メモリ使用率など、データの収集ごとに値が大きく変動しない性質のデータに対しは、[**直ちにアノマリーを検知する**]の適用が妥当かどうかを収集済みのデータの挙動から判断してください。

- [**除外期間**]

  事前に登録済みのスケジュールを選択して、分析処理の除外期間を設定します。

  スケジュールの詳細は、「2.2　運用スケジュールを管理する（44 ページ）」を参照してください。

ここでは、以下の内容を指定します。

- [**周期**]：[**1 週間**]
- [**予測範囲係数**]：2
- [**判定条件**]：[**外れたら**]
- [**検知のタイミング**]：[***10* 分以上満たした場合にアノマリーを検知する**]
- [**除外期間**]：

事前に作成しておいた 2020 年､2021 年の祝日をすべて登録したスケジュールを設定

c. [**イベント設定**]の内容を指定します。

アノマリー検知時に、イベント通知を行うかどうかを指定します。

- [**アノマリー検知イベント**]

  [**発行する**]、[**発行しない**]のいずれかを選択します。デフォルト値は、[**発行しない**]です。

  ヒント

  分析開始直後は、蓄積データ量や[**予測範囲係数**]の値に関連し、アノマリーの誤検知が発生する場合があります。初期の段階では､[**アノマリー検知イベント**]を[**発行しない**]とし、アノマリー検知状況を確認してから、[**アノマリー検知イベント**]を[**発行する**]に変更する運用を推奨します。

- [**重要度**]

  [**アノマリー検知イベント**]において[**発行する**]を選択した場合にのみ指定します。

  通知するイベントの重要度を[**Critical**]、[**Error**]、[**Warning**]のいずれかから選択します。デフォルト値は、[**Warning**]です。

- [**自動回復**]

  [**アノマリー検知イベント**]において[**発行する**]を選択した場合にのみ指定します。

  アノマリー検知後､[**判定条件**]に合致しない状態に戻った場合､自動的に回復処理を行うかについて、[**する**]、[**しない**]のいずれかを選択します。デフォルト値は、[**しない**]です。

ここでは、以下の内容を指定します。

- [**アノマリー検知イベント**]：[**発行しない**]

4. 分析ポリシーの内容を保存します。

内容を確認し、[**保存**]ボタンをクリックします。

指定した内容で、新規に分析ポリシーが追加されます。

分析ポリシー一覧画面で、指定した内容の分析ポリシーが追加されていることを確認します。

3.3.2.3　分析ポリシーを更新する

登録済みの分析ポリシーの内容を更新する手順について説明します。

ここでは、[**アノマリー分析設定**]の内容は変更せず、アノマリー検知時にイベントを通知する設定に変更する例を用いて、具体的な操作手順を説明します。

1. 分析ポリシー一覧画面を表示します。
   a. データ分析画面を表示します。

      [**データ分析**] メニューをクリックします。

   b. データ分析画面の [**分析ポリシー一覧**] アイコンをクリックします。

      分析ポリシー一覧画面が表示されます。

2. 更新対象の分析ポリシーの[**編集**]アイコンをクリックします。

   分析ポリシー編集画面が表示されます。

3. 分析ポリシー編集画面で適切な値を指定します。
   a. 基本情報を指定します。

      - [**名前**]

        一意に識別できる分析ポリシーの名前を指定します。最大文字数は、64 文字です。

        以下に示す文字は指定することができません。

        - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
        - 先頭および末尾への半角スペース

      - [**説明**]

        分析ポリシーの内容の説明を指定します。最大文字数は、1024 文字です。

      ここでは、以下の内容に変更します。

      - [**名前**]： 1 週間周期データの分析(イベント通知あり)
      - [**説明**] :

        1 週間ごとに周期性がみられるデータに対する分析ポリシー。アノマリー検知時はイベントを Warning レベルで通知。

   b. [**アノマリー分析設定**]の内容を指定します。

      - [**周期**]

        分析対象となるデータのおおよその周期性を指定します。以下のいずれかを指定します。

        - [**1 日**]

          24 時間ごとにデータ変動のおおよその周期性が見られる場合に使用します。

        - [**1 週間**]

曜日ごとや 7 日間ごとにデータ変動のおおよその周期性が見られる場合に使用します。

- [**予測範囲係数**]

  アノマリー分析では、過去の蓄積データを元に、次に収集して得られるデータがどの範囲の値になるのかを予測し、アノマリー判定を行います。[**予測範囲係数**]は、データの予測範囲の幅を決定する係数です。係数の値が大きいと予測範囲の幅も大きくなり、データの細かな挙動に対してはアノマリー判定は行われにくくなります。

  係数は、1~5 の範囲で指定できます。

- [**判定条件**]

  予測範囲に対し、実際に収集した値がどのような場合にアノマリーと判定するのかを以下のいずれかで指定します。

  - [**外れたら**]

    実際に収集した値が、予測範囲よりも大きい値、もしくは、小さい値の場合にアノマリーと判定します。

  - [**上回ったら**]

    実際に収集した値が、予測範囲よりも大きい値の場合にのみ、アノマリーと判定します。

  - [**下回ったら**]

    実際に収集した値が、予測範囲よりも小さい値の場合にのみ、アノマリーと判定します。

- [**検知のタイミング**]

  [**判定条件**]で指定した条件に合致した場合に、即座に、アノマリーと判定するかどうかを指定します。

  - [**直ちにアノマリーを検知する**]

    [**判定条件**]に合致した場合、直ちにアノマリーを検知します。

  - [**<*n*> 分以上満たした場合にアノマリーを検知する**]

    [**判定条件**]に合致する状態が指定時間継続した場合にのみ、アノマリーを検知します。<*n*>部分に 1 以上の数値を指定します。

ヒント

インターフェイスの使用率や特定の通信フローなど、データの収集ごとに値が大きく変動するような性質のデータを分析対象とする場合は、[**<*n*> 分以上満たした場合にアノマリーを検知する**]を選択し、複数のデータの挙動からアノマリーを判断する運用を推奨します。

上記に対し、メモリ使用率など、データの収集ごとに値が大きく変動しない性質のデータに対しは、[**直ちにアノマリーを検知する**]の適用が妥当かどうかを収集済みのデータの挙動から判断してください。

- [**除外期間**]

  事前に登録済みのスケジュールを選択して、分析処理の除外期間を設定します。

  スケジュールの詳細は、「2.2　運用スケジュールを管理する（44 ページ）」を参照してください。

ここでは、指定内容を変更しません。

c. [**イベント設定**]の内容を指定します。

アノマリー検知時に、イベント通知を行うかどうかを指定します。

- [**アノマリー検知イベント**]

  [**発行する**]、[**発行しない**]のいずれかを選択します。

  ヒント

  分析開始直後は、蓄積データ量や[**予測範囲係数**]の値に関連し、アノマリーの誤検知が発生する場合があります。初期の段階では、[**アノマリー検知イベント**]を[**発行しない**]とし、アノマリー検知状況を確認してから、[**アノマリー検知イベント**]を[**発行する**]に変更する運用を推奨します。

- [**重要度**]

  [**アノマリー検知イベント**]において[**発行する**]を選択した場合にのみ指定します。

  通知するイベントの重要度を[**Critical**]、[**Error**]、[**Warning**]のいずれかから選択します。

- [**自動回復**]

  [**アノマリー検知イベント**]において[**発行する**]を選択した場合にのみ指定します。

  アノマリー検知後、[**判定条件**]に合致しない状態に戻った場合、自動的に回復処理を行うかについて、[**する**]、[**しない**]のいずれかを選択します。

ここでは、以下の内容に変更します。

- [**アノマリー検知イベント**]：[**発行する**]
- [**重要度**]：[**Warning**]
- [**自動回復**]：[**する**]

4. 分析ポリシーの内容を保存します。

内容を確認し、[**保存**]ボタンをクリックします。

指定した内容で、分析ポリシーが更新されます。

分析ポリシー一覧画面で、分析ポリシーの[**名前**]や[**説明**]の内容が更新されていることを確認します。

3.3.2.4　分析ポリシーを削除する

登録済みの分析ポリシーを削除する手順について説明します。

⚠ 注意

分析対象に適用中の分析ポリシーは、削除することができません。

1. 分析ポリシー一覧画面を表示します。
   a. データ分析画面を表示します。

      [**データ分析**] メニューをクリックします。

   b. データ分析画面の [**分析ポリシー一覧**] アイコンをクリックします。

      分析ポリシー一覧画面が表示されます。
2. 削除対象の分析ポリシーの[**削除**]アイコンをクリックします。

   削除処理に対する確認のためのダイアログが表示されます。
3. 削除を実行します。

   確認のためのダイアログの[**OK**]ボタンをクリックします。

   分析ポリシー一覧画面から、指定した分析ポリシーの情報が削除されます。

3.3.3　アノマリー検知のための設定を行う

アノマリー検知を行うためのアノマリー分析の設定について説明します。

アノマリーを検知するためには、分析対象に対して分析ポリシーを適用し、アノマリー分析のための分析モデルの作成を行う必要があります。ここでは、分析ポリシーの適用手順、および、分析モデルの作成手順について説明します。

3.3.3.1　分析ポリシーを適用する

分析対象に対し、分析ポリシーを適用する手順について説明します。

分析対象への分析ポリシーの適用は、分析対象の追加時に併せて実施することができますが、ここでは、分析対象の追加後に、分析ポリシーを適用する手順を説明します。

適用済みの分析ポリシーを別の分析ポリシーに変更する、または、分析ポリシーを未適用の状態にする場合も本手順で操作します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ本操作を行うことができます。

1. データ分析画面を表示します。

   [**データ分析**] メニューをクリックします。

2. 分析対象の [**分析ポリシーの適用**] メニューを選択します。

   [**分析ポリシーの適用**] メニューは、当該分析対象の[⋮]アイコンをクリックすることで表示されます。

   [**分析ポリシーの適用**] メニューを選択すると、分析ポリシー選択ダイアログが表示されます。

3. 分析ポリシーを選択します。

   適用する分析ポリシーのチェックボックスをオンにします。

   分析ポリシーを未適用に変更する場合は、[**(選択なし)**]のチェックボックスをオンにします。

4. 選択内容を反映します。

   分析ポリシー選択ダイアログの[**OK**]ボタンをクリックします。

   分析ポリシーの適用処理に対する確認のためのダイアログが表示されます。

   確認ダイアログの[**OK**]ボタンをクリックすると選択内容が反映されます。

データ分析画面で、選択した分析ポリシーが適用されていることを確認します。

適用する分析ポリシーを変更すると、[**モデル状態**]が[**要再作成**]に変化する場合があります。この場合は、モデルの再作成を実施してください。詳細は、「3.3.3.2　分析モデルを再作成する（109 ページ）」を参照してください。

ヒント

分析対象に対し、本手順で初めて分析ポリシーを適用した場合は、「3.3.3.2　分析モデルを再作成する（109 ページ）」と同様の手順で、分析モデルの作成を行う必要があります。

3.3.3.2　分析モデルを再作成する

アノマリー分析のための分析モデルを再作成する手順について説明します。

データ分析画面の分析対象一覧において、[**モデル状態**]が[**要再作成**]の場合に、モデルの再作成を実施します。

以下のような操作を実施した場合に、[**モデル状態**]が[**要再作成**]となります。

- 分析対象に初めて分析ポリシーを適用した場合、または、適用する分析ポリシーを変更した場合
- 適用している分析ポリシーの[**アノマリー分析設定**]の内容を変更した場合
- [**除外期間**]の更新により、過去に収集したデータを分析利用から除外した場合

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ本操作を行うことができます。

1. データ分析画面を表示します。

   [**データ分析**] メニューをクリックします。

2. [**モデル状態**]が[**要再作成**]の分析対象のみを一覧表示します。

   a. [**選択...**]ボタンをクリックします。

   b. プルダウンメニューから[**モデル状態**]を選択します。

   c. [**要再作成**]チェックボックスをオンにします。

   d. [**検索**]ボタンをクリックします。

3. [**モデル再作成**]ボタンをクリックします。

   モデルの再作成処理に対する確認のためのダイアログが表示されます。[**OK**]ボタンをクリックするとモデルの再作成処理が開始されます。

   モデルの再作成は、現在、[**要再作成**]と表示されている分析対象のみ実行されます。

   すべての[**要再作成**]の分析対象が表示できていない場合は、表示件数を増やす、もしくは、ページを切り替えて、再度、[**モデル再作成**]ボタンをクリックします。

データ分析画面で、[**モデル状態**]が[**再作成中**]に変化したことを確認します。

3.4　各種一覧画面における一覧表の列の表示設定を行う

以下の一覧画面で表示される一覧表においては、ユーザーごとに表示する列や列の位置、デフォルトのソート列などを設定することができます。

- 「4.2.1.1　イベント画面（129 ページ）」
- 「4.4.1　ネットワークインターフェイス一覧画面（156 ページ）」

ここでは、一覧表の表示設定に関する操作について説明します。

一覧表の表示設定

一覧表の表示設定を行うための手順について説明します。

1. 各種一覧画面にて、一覧表の[**設定**]アイコンをクリックします。
2. 表示設定ダイアログにて設定を行います。設定の詳細を以下に示します。
   - 列の表示/非表示

[**表示**]列にて、表示する列をチェックボックスで指定します。

- デフォルトのソート列

  [**昇順**]列、[**降順**]列のラジオボタンにて、デフォルトのソート列に設定する列と昇順/降順を選択します。

- 文字の折り返し設定

  表示する文字列が列幅を超えた場合の表示方法を以下から選択します。

  - 折り返しなし

    文字列を折り返さずに表示します。文字列の長さに応じて列幅が自動的に広がります。

  - 折り返す(英単語の途中で改行しない)

    列幅を超えた場合は改行して表示されます。その際、英単語の途中では改行されません。

  - 折り返す(英単語の途中で改行する)

    列幅を超えた場合は改行して表示されます。その際、英単語の途中であっても列幅に合わせて改行します。

  - 省略記号

    列幅を超えた場合は省略記号が表示され、必ず 1 行で表示されます。

- 列幅

  各列の幅を指定します。指定方法には、表全体の幅に対する当該列の幅の割合を指定する方法(例：20%)と、px 単位での固定的な列幅を指定する方法(例：150px)を利用できます。

- 列の表示順序

  [↑**上へ移動**][↓**下へ移動**]ボタンで列の順序を変更することで、列の表示順序を設定します。

3. 表示設定を保存します。

一覧画面で、表示設定が反映されていることを確認します。

第 4 章
運用操作

Web コンソールによる運用操作の方法について説明します。

目次

4.1　現在のネットワークの状況を確認する

現在のネットワーク状況を即座に把握するための Web コンソールの操作方法について説明します。

Web コンソールでは、現在のネットワーク状況を即座に把握するために、以下の 3 つの操作画面を提供します。

- ダッシュボード画面

  ネットワークの全体的な状況把握のために利用します。ランキング形式(TopN)で表示されたデータから、各ノードの負荷や通信状況に対する問題の有無を確認します。

- トポロジーマップ画面([**通常モード**]での表示)

  ネットワーク構成の把握や障害発生箇所の特定、影響確認などに利用します。階層化したマップをドリルダウンで調べていき、障害発生ノードの周辺の構成を確認します。

- ノード一覧画面

  管理対象のノードのプロパティ情報や現在の状態(重要度)を確認する際に利用します。検索条件を指定して、条件に合致するノードの状態や情報を確認します。

4.1.1　ダッシュボードで全体状況を確認する

ダッシュボード画面では、様々な情報をランキング形式(TopN)などで表示し、現在の状況を確認することができます。ここでは、ダッシュボード画面の操作方法について説明します。

ダッシュボード画面で確認できる情報は、以下の通りです。

- 管理対象ノードの CPU やメモリなどのリソースの使用率
- 管理対象ノードのネットワークインターフェイスに関する情報(使用率、パケット損失率、エラー率)
- ネットワークを流れる通信フローに関する情報
- 障害発生状況やノードの稼働率に関する情報

ダッシュボード画面では、値の高さや低さのランキングデータから全体の状況を把握していきます。例えば、すべての管理対象ノードに対する CPU 使用率の高い Top10 を表示し、表示された 10 ノードのすべてで、問題のない CPU 使用率の値だった場合、ネットワーク全体で CPU 使用率に対する問題はないということが把握できます。

4.1.1.1　ダッシュボード画面

ダッシュボード画面について説明します。

ダッシュボード画面は、様々なランキング形式(TopN)の情報から、ネットワーク全体の状況を把握するために利用します。

ダッシュボード画面は、 [**ダッシュボード**] メニューをクリックして表示します。

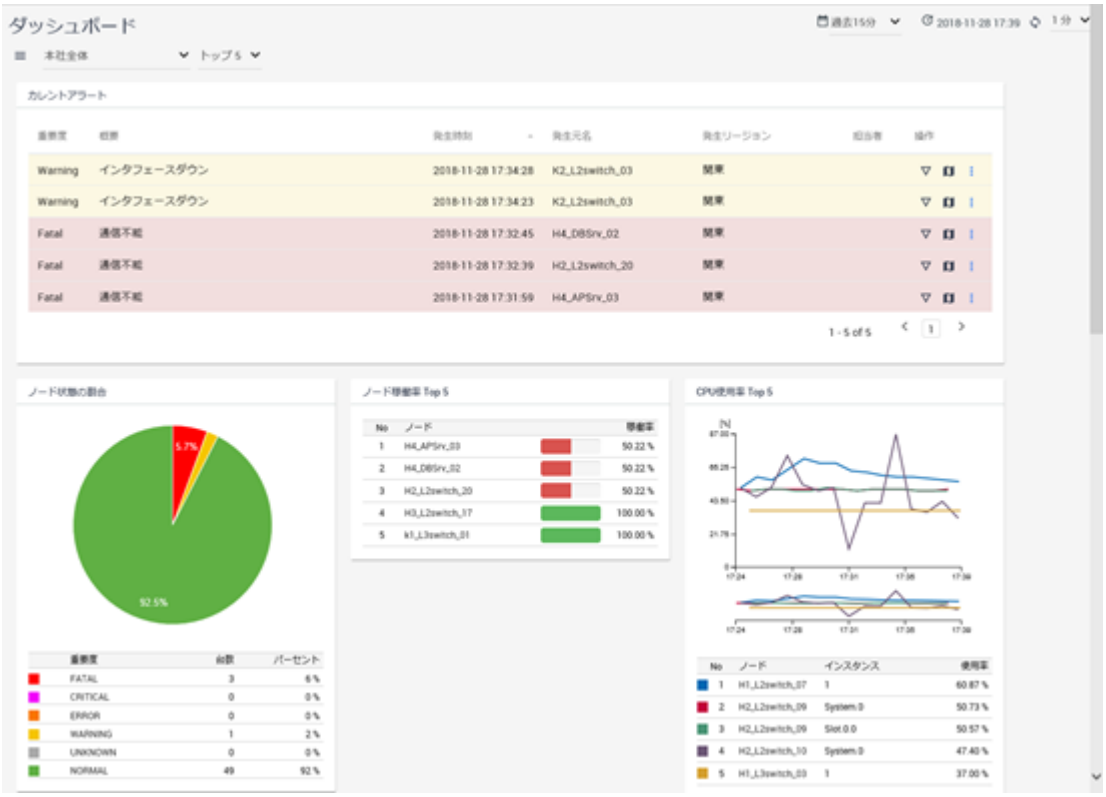

図 4-1　ダッシュボード画面

画面操作領域

- [**ダッシュボード一覧**]アイコン

  ダッシュボード一覧画面を表示します。ダッシュボード一覧画面では、ダッシュボードの定義内容の確認、および、操作(追加、編集、削除)を行うことができます。詳細は、「3.1.1　ダッシュボード一覧画面（73 ページ）」を参照してください。

  ヒント

  アドミニストレーターの役割を持つグループのユーザーのみ、[**ダッシュボード一覧**]アイコンの表示や選択を行うことができます。

- [**ダッシュボード**]

  プルダウンメニューから登録済みのダッシュボード名を選択することで、ダッシュボード画面に表示する情報を切り替えることができます。

- [**件数**]

  ダッシュボードの各ウィジェットで表示する、ランキングデータの表示件数をプルダウンメニュー([**トップ 5**]、[**トップ 10**]、[**トップ 20**])から選択します。

- [**期間**]

ダッシュボードで表示するデータの表示期間をプルダウンメニュー([**過去 15 分**]、[**過去 30 分**]、[**過去 1 時間**]、[**過去 6 時間**]、[**過去 24 時間**]、[**過去 48 時間**]、[**過去 72 時間**])から選択します。

- [**最終更新時刻**]

  画面更新を実施した日時を表示します。

- [**更新**]アイコン

  画面表示を最新の内容に更新します。

- [**更新間隔**]

  画面表示の更新間隔をプルダウンメニュー([**1 分**]、[**5 分**]、[**15 分**]、[**なし**])から選択します。

ウィジェット表示領域

ウィジェットを表示します。ダッシュボードに表示する各ウィジェットの操作については、「1.2.8　ウィジェットの基本操作（22 ページ）」、または、「1.2.9　特定ウィジェットによる固有操作（27 ページ）」を参照してください。

4.1.1.2　ダッシュボードの表示内容を切り替える

ダッシュボード画面の各パラメーターを変更していくことで、様々な観点で、ネットワークの状況を確認していくことができます。

ここでは、「本社ネットワーク」と「支社ネットワーク」の 2 つのダッシュボードを切り替えながら、ネットワーク全体の状況を確認していく操作例を用いて、ダッシュボードの具体的な操作手順を説明します。

操作例での 2 つのダッシュボードは、以下の内容として説明します。

- 本社ネットワーク

  [**期間**]は[**過去 1 時間**]で、[**件数**]は[**トップ 5**]が指定されており、表示するウィジェットは以下の通り。

  - 基幹スイッチの CPU 使用率
  - 基幹スイッチの入力インターフェイスの使用率

- 支社ネットワーク

  [**期間**]は[**過去 1 時間**]で、[**件数**]は[**トップ 5**]が指定されており、表示するウィジェットは以下の通り。

  - 支社 WAN ルーターの CPU 使用率
  - 支社の WAN ルーターの出力インターフェイスの使用率

1. ダッシュボード画面を表示します。

[**ダッシュボード**] メニューをクリックします。

ダッシュボード画面には、初期表示ダッシュボードとして登録されているダッシュボードの内容が表示されます。

本操作例では、ダッシュボード「本社ネットワーク」が表示されたとして説明します。

2. [**更新間隔**]を[**なし**]に設定します。

   細かく状況を確認する場合は、操作中、意図しないタイミングで画面表示が更新されないように、[**更新間隔**]のプルダウンメニューから[**なし**]を選択しておきます。

3. 各ウィジェットの内容を確認します。

   各ウィジェットで表示するランキングデータの上位の状況から問題の有無を判断します。

   例えば、ウィジェット「基幹スイッチの CPU 使用率」において、ランキング 1 位のスイッチの CPU 使用率が「60%」だったとします。この場合、その他すべてのスイッチの CPU 使用率が、「60%以下」と把握できるため、対象となるすべてのスイッチの CPU 使用率は、高くない状況であると判断できます。

   もう 1 つの例として、ウィジェット「基幹スイッチの入力インターフェイスの使用率」を確認した場合に、ランキング 5 位の入力インターフェイスの使用率が「90%」を超えていたとします。この状況から、ウィジェットで表示している 5 つのネットワークインターフェイスすべてで高負荷であることが把握できます。このような場合は、[**件数**]を[**トップ 20**]などのデフォルト値よりも大きい値に変更し、どの範囲まで高負荷なのかを確認します。

   必要に応じて、ノード詳細画面やネットワークインターフェイス詳細画面、または、トポロジーマップ画面を表示し、ネットワークインターフェイスの負荷の影響確認や原因調査を行います。

4. 別のダッシュボードに切り替えます。

   一通りの確認が完了した後、別の観点で状況確認を行うため、プルダウンメニューから別のダッシュボード名を選択します。ダッシュボード画面の表示が、選択したダッシュボードの情報に切り替わります。

   ここでは、ダッシュボード「支社ネットワーク」に切り替えて、支社のネットワーク状況について確認します。

5. [**更新間隔**]を[**なし**]に設定します。

   ダッシュボードを切り替えると、ダッシュボード画面の各パラメーターが選択したダッシュボードのデフォルト値に変わります。そのため、再度、[**更新間隔**]のプルダウンメニューから[**なし**]を選択します。

6. 各ウィジェットの内容を確認します。

   同様に、各ウィジェットで表示するランキングデータの上位の状況から問題の有無を判断します。

例えば、「支社の WAN ルーターの出力インターフェイスの使用率」において、現在から 30 分前までの期間は通常状態だが、それ以前で高負荷な傾向が見られたとします。このような場合は、[**期間**]を[**過去 6 時間**]などのデフォルト値よりも大きい値に変更し、いつから高負荷だったのかを確認します。

必要に応じて、当該ネットワークインターフェイスに対するネットワークインターフェイス詳細画面を表示して、高負荷の原因を調査します。

ヒント

NFA を利用している場合は、ネットワークインターフェイス詳細画面に当該ネットワークインターフェイスを流れる通信フローのアプリケーションの内容やカンバセーション(通信を行う 2 点間の情報)の内容を確認することができます。

ネットワークの状況確認は、上述の通り、ダッシュボード画面にて、ダッシュボードを切り替えながら全体状況を把握していきます。そして、細かな調査については、各ウィジェットから、詳細な情報表示を行う各画面に遷移していき、実施します。

4.1.2　トポロジーマップ（通常モード）による状況確認

トポロジーマップ画面では、現在の状況を表示する[**通常モード**]とノードの過去の状態(重要度)を表示する[**分析モード**]の 2 つの[**表示モード**]を使い分けて状況確認を行っていきます。ここでは、現在の状況を表示する[**通常モード**]の操作について説明します。

トポロジーマップ画面では、ネットワーク構成を示すマップから、ノード間の物理的な接続関係や、建物、または、フロアでのノードの配置を確認することができます。階層化したマップは、ドリルダウンで配下のマップを表示していくことができます。[**通常モード**]で表示している場合は、現在の各ノードの状態を確認することができます。また、サイドパネルを利用することで、ネットワーク構成とともに、各ノードの現在の負荷状況を確認していくことができます。

4.1.2.1　トポロジーマップ画面(通常モード)

トポロジーマップ画面の[**通常モード**]について説明します。

トポロジーマップ画面では、ネットワークの構成とともに、各ノードの状態、および、負荷状況を確認することができます。

トポロジーマップ画面は、 [**トポロジーマップ**] メニューをクリックして表示します。

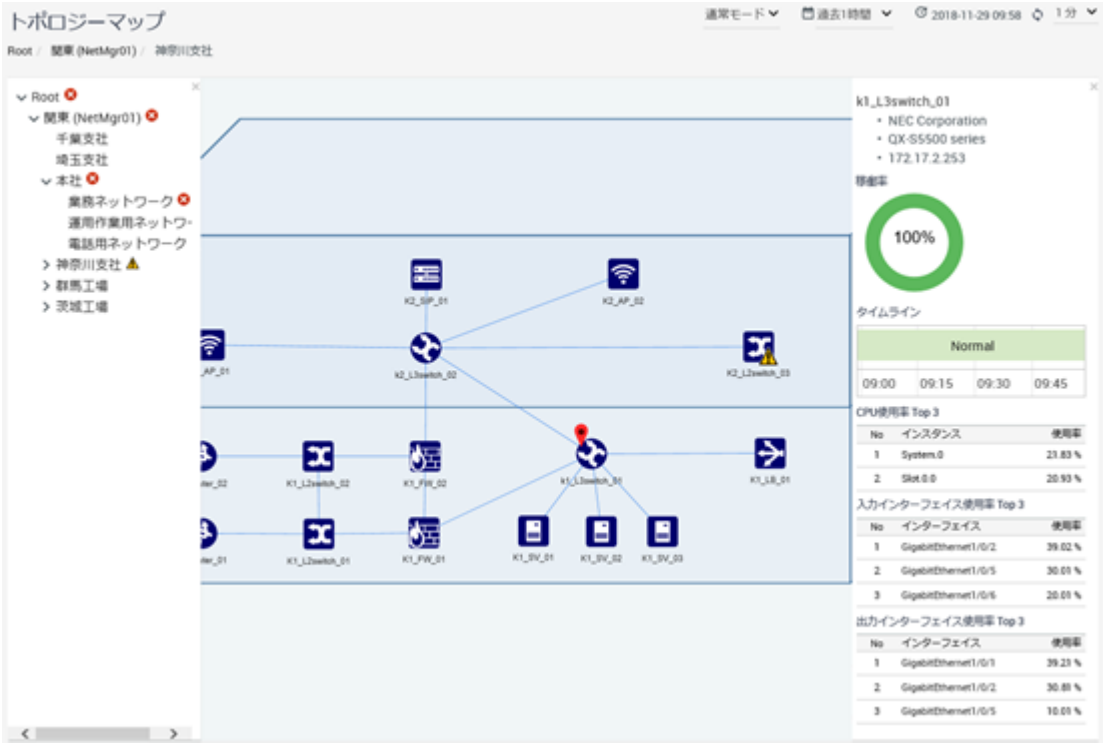

図 4-2　トポロジーマップ画面(通常モード)

画面操作領域

- [**表示モード**]

  プルダウンメニューから以下のいずれかを選択し、[**表示モード**]を切り替えます。

  - [**通常モード**]

    現在のネットワークの状態(重要度)を確認する場合に選択します。 [**トポロジーマップ**] メニューからトポロジーマップ画面を表示した場合は、必ず、[**通常モード**]となります。

  - [**分析モード**]

    過去のネットワークの状態(重要度)を確認する場合に選択します。過去の期間を表示するノード詳細画面、または、イベント画面からトポロジーマップ画面を表示した場合は、[**分析モード**]となります。

  - [**編集モード**]

    トポロジーマップの表示内容を編集する場合に選択します。

    ヒント

    アドミニストレーターの役割を持つグループのユーザーのみ、[**編集モード**]へ切り替えることができます。

- [**期間**](通常モード)

サイドパネルで表示するデータの表示期間をプルダウンメニュー([**過去 15 分**]、[**過去 30 分**]、[**過去 1 時間**]、[**過去 6 時間**]、[**過去 24 時間**]、[**過去 48 時間**]、[**過去 72 時間**])から選択します。デフォルト値は、[**過去 1 時間**]です。

- [**最終更新時刻**]

  画面更新を実施した日時を表示します。

- [**更新**]アイコン

  画面表示を最新の内容に更新します。

- [**更新間隔**]

  画面表示の更新間隔をプルダウンメニュー([**1 分**]、[**5 分**]、[**15 分**]、[**なし**])から選択します。デフォルト値は、[**1 分**]です。

ツリービュー

マップの階層構成をツリー形式で表示します。ツリービューは、通常、最小化しており、マップビュー上の[ ]アイコンをクリックして表示します。

NetvisorPro のツリービュー同様に、マップ内のノードで障害が発生した場合は、それを示す重要度の情報が、[**マップ**]アイコンに伝搬します。また、当該[**マップ**]アイコンの上位にあたる[**マップ**]アイコンにもその情報が伝搬します。

マップビュー

ツリービューで選択した[**マップ**]アイコンに対するマップを表示します。マップビューに表示するマップには、管理対象ノードを示す[**ノード**]アイコンやそのノード間の接続関係を示す[**接続線**]、下位のマップを示す[**マップ**]アイコンを表示します。

[**接続線**]の端点となるネットワークインターフェイスの状態がどちらか一方でも DOWN 状態の場合には、接続線の色が赤く表示されます。ネットワークインターフェイスの状態については、「4.4.1　ネットワークインターフェイス一覧画面（156 ページ）」を参照してください。

ヒント

ノード間において、複数の物理的な接続関係があったとしてもマップビューでは、1 本の接続線で接続関係を表現します。物理的な接続関係の詳細は、[**接続線**]を選択した際に表示するサイドパネルで確認することができます。

マップビューでは、表示内容に対し、以下の操作を行うことができます。

- 表示の拡大、縮小

  [**拡大**]ボタンをクリックするとマップが拡大表示し、[**縮小**]ボタンをクリックするとマップが縮小表示します。

また、マウスホイールを操作することでも、マップを拡大表示、縮小表示することができます。

- 表示箇所の移動

  マップをドラッグすることで、表示箇所を移動することができます。マップを拡大表示した状態で表示箇所を移動する場合に利用します。

- 表示内容の最適化

  [Fit]アイコンをクリックすると、マップビュー上のすべての[**ノード**]アイコンや[**マップ**]アイコンが表示できる位置や縮尺に、マップビューの表示内容を切り替えます。

- 上位、および、下位のマップへの画面遷移

  マップビューの上部には、ツリービューで選択した[**マップ**]アイコンに対するツリー上の位置を示すパス情報のリンクが表示されます。このリンクをクリックすることで、マップビューの表示を上位のマップに切り替えることができます。また、マップビューに表示する下位のマップを示す[**マップ**]アイコンをダブルクリックすることで、マップビューの表示を下位のマップに切り替えることができます。

  上記の操作を利用することにより、マップビューのみでマップの表示を切り替えて、運用していくことができます。

サイドパネル

マップビューで表示する[**ノード**]アイコンや[**マップ**]アイコン、[**接続線**]を選択すると、サイドパネルが表示されます。サイドパネルでは、選択したアイコンの詳細情報を表示します。詳細は、「4.1.2.2　マップビューのサイドパネル（120 ページ）」を参照してください。

4.1.2.2　マップビューのサイドパネル

サイドパネルについて説明します。

サイドパネルは、ネットワーク構成を見ながら、ノードの負荷状況を調べたり、ノード間の接続関係を確認する場合に利用します。

サイドパネルは、マップビューに表示する[**ノード**]アイコンや[**マップ**]アイコン、[**接続線**]を選択した場合に表示され、選択したノードやマップ、接続線の情報が表示されます。

サイドパネルで表示する内容は、選択対象に応じて大きく異なります。

図 4-3　サイドパネル

ノードの表示内容

[**ノード**]アイコンを選択した場合、サイドパネルには、以下の情報が表示されます。

- [**ノード名**]

  ノード名を表示します。リンクをクリックすると、当該ノードに対するノード詳細画面を表示します。

- [**ベンダー名**]

  ノードのベンダー情報を表示します。

- [**シリーズ名**]

  ノードの機種に関する情報を表示します。

- [**IPv4 アドレス**]

  監視処理で用いている代表の IPv4 アドレスの情報を表示します。

- [**IPv6 アドレス**]

  監視処理で用いている代表の IPv6 アドレスの情報を表示します。

トポロジーマップ画面の[**期間**]の設定値に対応する以下の情報を表示します。ランキングデータとしては、Top3 までの情報を表示します。

- [**稼働率**]

  ノードの稼働率と、状態(重要度)の推移を表示します。

- [**CPU 使用率**]

  CPU 使用率の状況を表示します。

- [**入力インターフェイスの使用率**]

  ネットワークインターフェイスの入力側の使用率の状況を表示します。

- [**出力インターフェイスの使用率**]

  ネットワークインターフェイスの出力側の使用率の状況を表示します。

ヒント

[**CPU 使用率**]、[**入力インターフェイスの使用率**]、[**出力インターフェイスの使用率**]を表示するには、事前に、NetvisorPro のデータ収集機能において、収集設定を行っておく必要があります。

マップの表示内容

[**マップ**]アイコンを選択した場合、サイドパネルには、以下の情報が表示されます。

- [**マップ名**]

  マップ名を表示します。

- [**IPv4 アドレス**]

  マップに設定されている IPv4 のネットワークアドレスの情報を表示します。

- [**IPv6 アドレス**]

  マップに設定されている IPv6 のネットワークアドレスの情報を表示します。

- [**管理者**]

  マップに設定されている管理者の情報を表示します。

- [**設置場所**]

  マップに設定されている場所の情報を表示します。

- [**URL**]

  マップに設定されている URL の情報を表示します。

接続線の表示内容

[**接続線**]を選択した場合、サイドパネルには、以下の情報が表示されます。

- 接続関係の情報

接続する 2 つのノードの情報を以下の形式で表示します。

```
<ノード名 1>
to <ノード名 2>
```

- 接続するネットワークインターフェイスの情報

  接続関係の情報で示したノード間をどのネットワークインターフェイスで接続しているのかを以下の形式で表示します。

```
<ネットワークインターフェイス名 1>(<回線速度>)
to <ネットワークインターフェイス名 2>(<回線速度>)
```

ヒント

- 上段は、<*ノード名 1*>のネットワークインターフェイスの情報を示し、下段は、<*ノード名 2*>のネットワークインターフェイスの情報を示します。
- <*回線速度*>は、各ノードから取得したネットワークインターフェイスの帯域速度の情報を表示します。
- 複数のネットワークインターフェイスで接続がある場合は、すべての接続するネットワークインターフェイスの情報を同様に表示します。

4.1.2.3　トポロジーマップで障害箇所を確認する

マップをドリルダウンしていくことで、障害箇所、および、その周辺の状況を確認することができます。

ここでは、ネットワーク全体を表示する上位のマップから、ドリルダウンして障害箇所を確認する手順について説明します。

1. トポロジーマップ画面を表示します。

   [**トポロジーマップ**] メニューをクリックします。

2. マップビューで、障害発生を示す[**マップ**]アイコンを確認します。

   トポロジーマップ画面の表示直後は、最上位のマップビューが表示されます。配下のノードで障害が発生している[**マップ**]アイコンには、障害の重要度を示す情報が伝搬して表示されます。

   ヒント

   最上位のマップビューには、IMS コンポーネントと接続する NetvisorPro を示す[**マップ**]アイコンが表示されます。

3. 障害が発生している[**マップ**]アイコンをダブルクリックします。

   クリックした[**マップ**]アイコンに対するマップが、マップビューに表示されます。

4. マップビューで、障害発生を示すアイコンを確認します。

障害発生を示すアイコンが[**マップ**]アイコンの場合は、さらにダブルクリックして、ドリルダウンしていきます。

障害発生を示すアイコンが[**ノード**]アイコンの場合は、当該ノードが障害発生箇所になります。

5. 障害発生を示す[**ノード**]アイコンの周辺の構成を確認します。

   障害が発生したノードの周辺の構成を見ることで影響範囲を確認することができます。

6. 障害発生を示すノードの状態を確認します。

   障害発生を示す[**ノード**]アイコンをクリックし、サイドパネルを表示します。サイドパネルの情報から、現在の負荷状況や状態(重要度)の変化の推移を確認します。

発生したイベントの内容の確認など、詳細な調査が必要な場合は、サイドパネルに表示するノード名のリンクをクリックし、当該ノードに対するノード詳細画面を表示します。

4.1.3　ノードの状態を一覧で確認する

検索条件に合致するノードのプロパティ情報や状態(重要度)を一覧表示するノード一覧画面の操作方法について説明します。

ノード一覧画面では、様々な検索条件を指定して、条件に合致するノードのプロパティ情報(IP アドレス、ベンダー、シリーズ、バージョンなど)や現在の状態(重要度)を即座に確認することができます。

例えば、検索条件に、[**ベンダー**]や[**シリーズ**]を指定して、特定機種で表示を絞り込むことで、同一機種のノードにおいて、バージョンアップ作業に漏れがないかなどを確認することができます。

上記のように、すべての管理対象ノードに対し、様々な条件での検索を行うことで、ノード情報の詳細確認を効率的に実施していくことができます。

4.1.3.1　ノード一覧画面

ノード一覧画面について説明します。

ノード一覧画面は、管理対象ノードの情報を、様々な観点で確認、調査する際に利用します。

ノード一覧画面は、[ **ノード一覧**] メニューをクリックして表示します。

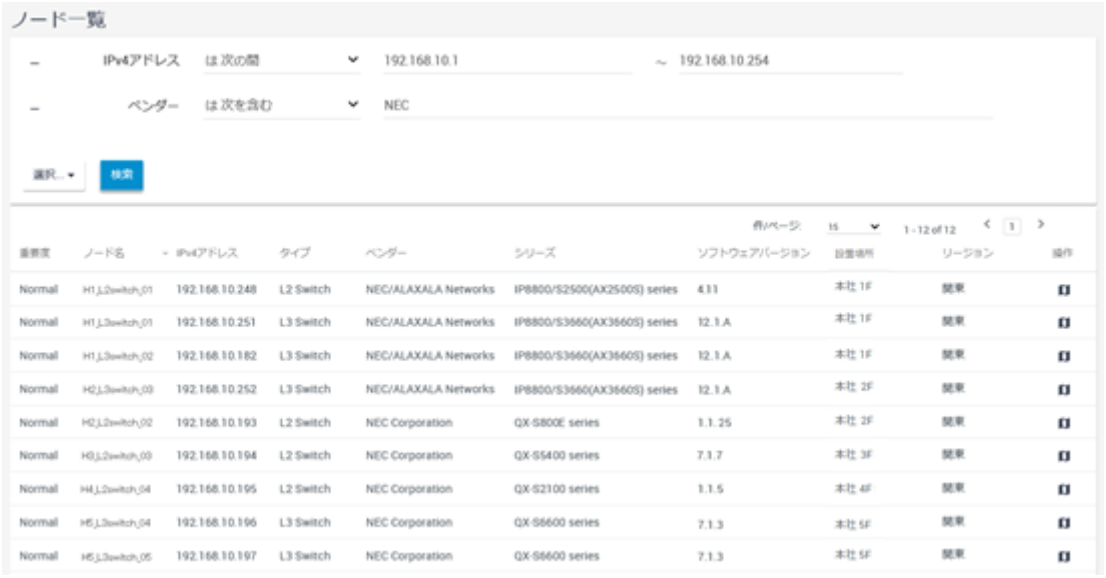

図 4-4　ノード一覧画面

検索条件の指定

ノード一覧で表示する各項目の内容に対し、条件を指定して、表示するノードを絞り込むことができます。

- 条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。

  追加した条件の先頭に表示する[−]アイコンをクリックすると追加した条件を取り消すことができます。

- 条件指定

  ノード一覧で表示する各項目に対し、以下の 3 つの方法で、検索条件を指定します。検索条件の指定方法は、選択した項目ごとに異なります。

  - チェックボックスによる指定

    チェックボックスを用いて、検索条件を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**重要度**]

  - キーワードの指定

    選択した項目に対して、キーワードと照合方法を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**ノード名**]、[**タイプ**]、[**ベンダー**]、[**シリーズ**]、[**ソフトウェアバージョン**]、[**設置場所**]、[**リージョン**]

照合方法については、以下を指定することができます。

* 照合方法：

  [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

- 値の範囲指定

  検索条件として、値、もしくは、値の範囲を指定します。対象項目は以下の通りです。

  * 対象項目：

    [**IPv4 アドレス**]

  * 照合方法：

    [**は次と等しい**](一致)、[**は次の間**](範囲内)

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

条件を指定した後、[**検索**]ボタンをクリックすると、検索条件に合致したノードの一覧が表示されます。

ノード一覧

- [**重要度**]

  ノードの現在の状態を表示します。

- [**ノード名**]

  ノードの名前を表示します。ノード名のリンクをクリックすると、当該ノードに対するノード詳細画面を表示します。

- [**IP アドレス**]

  ノードの監視処理で用いている代表の IPv4 アドレスを表示します。

- [**タイプ**]

  ノードの種類に関する情報を表示します。[**タイプ**]は、NetvisorPro で指定している[**アイコンタイプ**]の情報や、NetvisorPro が MIB から取得した[**sysObjectID**](機種を示す ID)の値から判断します。

- [**ベンダー**]

  ノードの製造元となる会社名を表示します。[**ベンダー**]は、NetvisorPro が MIB から取得した[**sysObjectID**](機種を示す ID)の値から判断しています。

ヒント

[**ベンダー**]は、IANA(Internet Assigned Numbers Authority)によって定義された、ベンダー ID と会社名の情報に従って表示を行います。

- [**シリーズ**]

  ノードの機種シリーズについての情報を表示します。[**シリーズ**]は、NetvisorPro が MIB から取得した[**sysObjectID**](機種を示す ID)の値から判断します。

- [**ソフトウェアバージョン**]

  ノードのソフトウェアバージョンの情報を表示します。

- [**設置場所**]

  ノードが設置されている場所に関する情報を表示します。

- [**リージョン**]

  ノードが属するリージョングループの名前を表示します。

- [**操作**]

  アイコンをクリックすることで、ノードに対する操作を行います。

  - [**トポロジーマップ**]アイコン

    当該ノードを配置しているマップを[**通常モード**]で表示します。

    ヒント

    - [**トポロジーマップ**]アイコンは、NetvisorPro を利用している場合に表示されます。
    - 当該ノードのアイコンを複数のマップに配置している場合は、表示するマップの選択画面が表示されます。

1 ページに表示するノード情報の件数は、プルダウンメニュー([**15**]、[**50**]、[**100**])から選択します。デフォルト値は、[**15**]件です。

検索条件に合致したすべてのノード情報を 1 ページで表示できない場合は、ページを切り替えて、ノード情報を確認します。

4.1.3.2　障害が発生しているノードを一覧で確認する

ノード一覧画面では、様々な検索条件を指定して、条件に合致するノードの情報を確認していくことができます。

ここでは、ノードの状態が、「Warning 以上」のノードを検索する操作例を用いて、ノード一覧画面の具体的な操作手順を説明します。

1. ノード一覧画面を表示します。

   [**ノード一覧**] メニューをクリックします。

2. 検索対象の項目を選択します。

   プルダウンメニュー([**重要度**]、[**ノード名**]、[**IP アドレス**]、[**タイプ**]、[**ベンダー**]、[**シリーズ**]、[**ソフトウェアバージョン**]、[**設置場所**]、[**リージョン**])から検索対象とする項目を選択します。

   ここでは、プルダウンメニューから[**重要度**]を選択します。

3. 選択した項目に対する検索条件を指定します。

   [**重要度**]を選択した場合は、各重要度のチェックボックスが表示されます。条件とする重要度のチェックボックスをオンにします。

   ここでは、現在、「Warning 以上」の状態のノードを検索したいため、[**Fatal**]、[**Critical**]、[**Error**]、[**Warning**]に対するチェックボックスをクリックし、オンにします。

4. [**検索**]ボタンをクリックします。

   検索条件に合致するノードの情報が、ノード一覧に表示されます。

5. 検索結果を確認します。

   ノード一覧に表示された情報を確認します。1 ページで、すべての検索結果が表示されていない場合は、ページを切り替えて結果を確認します。

   必要に応じて、[**選択...**]ボタンのプルダウンメニューから検索条件を追加して、情報の絞り込みを行います。

ノード一覧に表示されたノードに対し、さらに細かく調べたい場合は、ノード名のリンクをクリックし、ノード詳細画面を表示します。ノード詳細画面では、当該ノードのすべてのプロパティ情報や現在の負荷状況などを確認することができます。

4.2　イベントの発生状況を確認する

Web コンソールにおけるイベント発生状況の確認方法について説明します。

Web コンソールでは、イベントの発生状況を確認するために、以下の 3 つの操作画面を利用します。

- イベント画面

  発生したイベントの情報を時系列で確認したり、イベントの詳細情報を確認する際に利用します。イベントの発生時間帯を検索条件に指定して、過去のイベント発生状況の確認を行うこともできます。

- トポロジーマップ画面([**分析モード**]での表示)

  過去に発生したイベントの影響範囲や当時の負荷状況を確認する際に利用します。任意の期間を指定し、タイムラインを操作することで、イベント発生当時の各ノードの状態をマップで再現することができます。

- Syslog 画面

NetvisorPro のシスログサーバー機能(SyslogDiagnosis 機能ライセンス)で受信、蓄積した Syslog の内容を確認する際に利用します。期間やノード名、Syslog に含まれている文字列などを検索条件に指定して、障害発生前後の詳細な状況を調査することができます。

ヒント

Web コンソールの操作中におけるイベントの発生有無については、[ **新着通知**]アイコンの状態から確認することができます。また、[ **新着通知**]アイコンをクリックすることで、発生したイベントの概要情報の確認を行うこともできます。詳細は、「1.2.5　新着イベントを確認する (17 ページ)」を参照してください。

4.2.1　発生したイベントの内容を確認する

Web コンソールでは、発生したすべてのイベントの内容をイベント画面で確認します。

イベント画面では、発生したイベントに対し、以下の操作を行うことができます。

- 特定条件に合致したイベントの検索

  検索条件を指定することで、条件に合致したイベントだけ一覧表示することができます。

  例えば、未回復状態のイベントを確認する場合や、自身が調査担当として割り当てられているイベントを確認する場合などで利用します。

- イベントの詳細情報の確認

  イベント画面から、指定したイベントに対するイベント詳細画面を表示することで、当該イベントの詳細な情報を確認することができます。

- 調査担当者の割り当て

  発生したイベントに対し、調査担当者を割り当てていくことができます。複数の運用者でネットワークを管理している場合に、障害対応の責任区分を明確にしたり、イベント内容が確認済みであることを他の運用者に示すなどの用途で利用します。

- イベントの回復操作

  発生した障害イベント(重要度が、 Unknown、および、Warning 以上)に対し、回復処理を行うことができます。原因調査、復旧作業の完了後に回復操作を行います。

  ヒント

  イベントを検出した製品の仕様に依存して、イベントによっては、自動で回復状態を検出し、回復処理が行われます。

4.2.1.1　イベント画面

イベント画面について説明します。

イベント画面では、発生したイベントの内容確認、および、操作(担当者割り当て、回復、削除)を行います。

イベント画面は、[**イベント**] メニューをクリックして表示します。

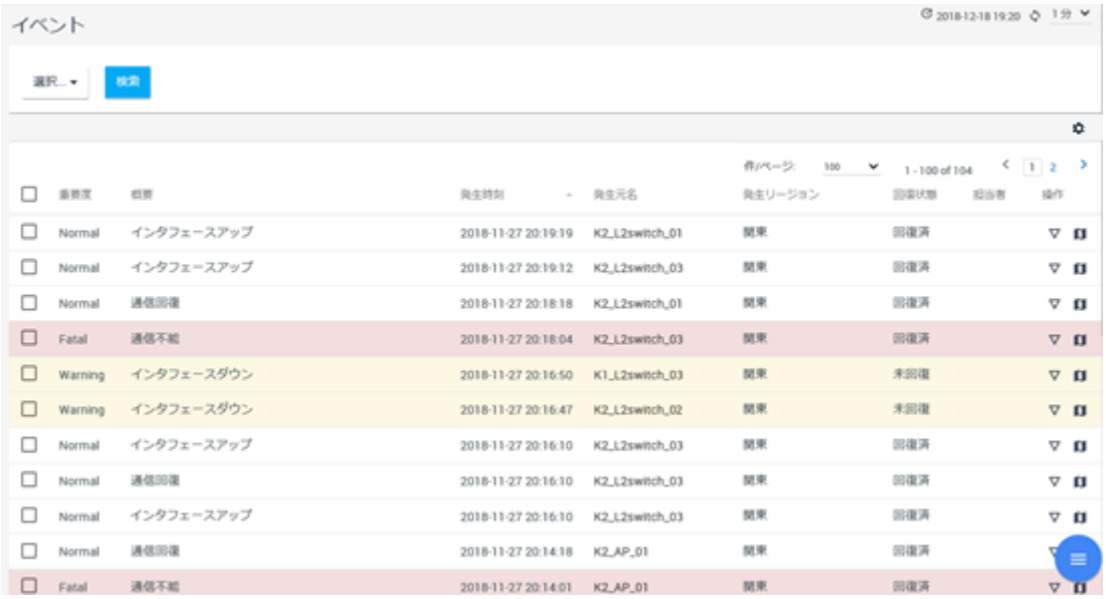

図 4-5　イベント画面

画面操作領域

- [**最終更新時刻**]

  画面更新を実施した日時を表示します。

- [**更新**]アイコン

  画面表示を最新の内容に更新します。

- [**更新間隔**]

  画面表示の更新間隔をプルダウンメニュー([**1 分**]、[**5 分**]、[**15 分**]、[**なし**])から選択します。デフォルト値は、[**1 分**]です。

検索条件の指定

イベント一覧で表示する各項目の内容に対し、条件を指定して、表示するイベントの情報を絞り込むことができます。

- 条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。

  追加した条件の先頭に表示する[−]アイコンをクリックすると追加した条件を取り消すことができます。

- 条件指定

イベント一覧で表示する各項目に対し、以下の 3 つの方法で、検索条件を指定します。検索条件の指定方法は、選択した項目ごとに異なります。

- チェックボックスによる指定

  チェックボックスを用いて、検索条件を指定します。対象項目は以下の通りです。

  * 対象項目：

    [**重要度**]、[**回復状態**]、[**Syslog Severity**]

- キーワードの指定

  選択した項目に対して、キーワードと照合方法を指定します。対象項目は以下の通りです。

  * 対象項目：

    [**概要**]、[**詳細**]、[**対処**]、[**発生元名**]、[**発生リージョン**]、[**担当者**]、[**TRAP Enterprise**]

  照合方法については、以下を指定することができます。

  * 照合方法：

    [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

    [**発生元名**]、および、[**担当者**]に対しては、[**は定義されていない**]を指定することができます。

- 時刻の範囲指定

  選択した項目に対して、*YYYY-MM-DD hh:mm* の形式で時間範囲を指定します。対象項目は以下の通りです。

  * 対象項目：

    [**発生時刻**]

- 値の範囲指定

  検索条件として、値、もしくは、値の範囲を指定します。対象項目は以下の通りです。

  * 対象項目：

    [**TRAP GenericCode**]、[**TRAP SpecificcCode**]

  * 照合方法：

    [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次の値以上**](以上)、[**は次の値以下**](以下)、[**は次の間**](範囲内)

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

条件を指定した後、[**検索**]ボタンをクリックすると、検索条件に合致したイベントの一覧が表示されます。

⚠ 注意

- [**発生元名**]に対する検索を行う場合は、以下の点に注意してください。
  - イベントの発生元となるノードの[**ノード名**]を変更しても、イベントの[**発生元名**]の情報は、イベントの発生当時のままになります。
  - IMS コンポーネントが発行したイベントには、[**発生元名**]の情報がありません。IMS コンポーネントが発行したイベントを検索する場合は、[**発生元名**]に対し、照合方法として、[**は定義されていない**]を指定してください。
- [**概要**]、[**詳細**]、[**対処**]に対する検索では、改行文字を含んだ文字列は検索できません。イベント一覧の[**概要**]列、[**詳細**]列、[**対処**]列のメッセージをコピーして検索条件に指定する場合には、改行部分を含まないように指定してください。
- 検索条件には、一覧表に表示されている項目のみが指定可能です。非表示となっている項目は検索条件として指定できません。

イベント一覧

- [**チェックボックス**]

  [**選択したイベントに対し:**]ボタンにカーソルを重ねると表示する、各ボタンの操作対象イベントを指定します。

  [**チェックボックス**]をオンにしたイベントに対し、以下の操作を実行することができます。

  ヒント

  オブザーバーの役割を持つグループにしか属さないユーザーでは、[**選択したイベントに対し:**]ボタンは表示されず、以下の操作を行うことはできません。

  - [**担当者に自分を割り当てる**]ボタン

    イベントに対し、自分を担当者として割り当てます。

  - [**担当者を解除する**]ボタン

    イベントに対し割り当てられていた担当者を解除します。自分以外の担当者の割り当ても解除することができます。

  - [**回復する**]ボタン

イベントを回復状態にします。

- [ **削除する**]ボタン

  イベントを削除します。

- [**重要度**]

  イベントの重要度を表示します。Web コンソールで表示するイベントの重要度の詳細については、「4.2.1.3　イベント重要度（137 ページ）」を参照してください。

- [**概要**]

  イベントの概要情報を表示します。

- [**発生時刻**]

  イベントの発生時刻を表示します。

- [**発生元名**]

  イベントの発生元となるノード名、および、ネットワークインターフェイス名を表示します。

- [**発生リージョン**]

  イベントの発生元となるノードが属するリージョングループの名前を表示します。

- [**詳細**]

  イベントの詳細情報を表示します。

- [**対処**]

  イベントの対処方法の情報を表示します。

- [**IPv4 アドレス**]

  イベントの発生元となるノードの IPv4 アドレスを表示します。

- [**IPv6 アドレス**]

  イベントの発生元となるノードの IPv6 アドレスを表示します。

- [**TRAP Enterprise**]

  SNMP トラップの EnterpriseOID を表示します。

- [**TRAP GenericCode**]

  SNMP トラップの Generic Code を表示します。

- [**TRAP SpecificCode**]

  SNMP トラップの Specific Code を表示します。

- [**Syslog Facility**]

  Syslog の Facility を表示します。

- [**Syslog Severity**]

  Syslog の Severity を表示します。

- [**回復状態**]

  イベントの回復状態を表示します。現在発生中のイベントに対しては、[**未回復**]の表示になります。

- [**担当者**]

  当該イベントの対応を担当するユーザー名(表示名)を表示します。誰も担当者として割り当てられていない場合は、空欄となります。

- [**操作**]

  各アイコンをクリックすることで、イベントに対応する操作画面を表示します。

  - [**イベント詳細**]アイコン

    イベントに対するイベント詳細ダイアログを表示します。

  - [**トポロジーマップ**]アイコン

    イベントの発生元となるノードを配置しているマップを[**分析モード**]で表示します。

    ヒント

    - [**トポロジーマップ**]アイコンは、NetvisorPro を利用している場合に表示されます。
    - 当該ノードのアイコンを複数のマップに配置している場合は、表示するマップの選択画面が表示されます。

1 ページに表示するイベントの件数は、プルダウンメニュー([**50**]、[**100**]、[**250**])から選択します。デフォルト値は、[**100**]です。

検索条件に合致したすべてのイベント情報を 1 ページで表示できない場合は、ページを切り替えて、イベント情報を確認します。

[**設定**]アイコンをクリックすることで、列の表示設定を行うことができます。詳細は「3.4　各種一覧画面における一覧表の列の表示設定を行う（110 ページ）」を参照してください。

ヒント

保持できるイベントの最大件数は、1,000,000 件です。1,000,000 件を超えると、最も古いイベントを削除し、新しいイベントを保持していきます。

4.2.1.2　イベント詳細ダイアログと画面

イベントの詳細内容を表示するイベント詳細ダイアログとイベント詳細画面について説明します。

イベント詳細ダイアログ、および、イベント詳細画面では、選択したイベントの詳細な情報を確認することができます。

イベント詳細ダイアログは、イベント情報を表示する各画面から、イベントに対する[▽**イベント詳細**]アイコンをクリックして表示します。

イベント詳細画面は、イベント詳細ダイアログの右上に配置している[**印刷用画面を開く**]アイコンをクリックして表示します。また、イベントアクションによるメール通報において、メール本文にイベント詳細画面の URL を埋め込んでいた場合に、その URL からもイベント詳細画面を表示することができます。

図 4-6　イベント詳細画面

ヒント

- イベント詳細ダイアログとイベント詳細画面とでは、表示するイベント情報の内容は同じです。イベント詳細画面のみ、操作ボタンによるイベント操作を行うことができます。
- イベント情報の内容を印刷したい場合は、イベント詳細画面を表示し、Web ブラウザーの印刷機能を用いて印刷を行ってください。

- [**概要**]

  イベントの概要情報を表示します。

- [**重要度**]

イベントの重要度を表示します。Web コンソールで表示するイベントの重要度の詳細については、「4.2.1.3　イベント重要度（137 ページ）」を参照してください。

- [**回復状態**]

  イベントの回復状態を表示します。現在発生中のイベントに対しては、[**未回復**]の表示になります。

- [**発生元名**]

  イベントの発生元となるノード名、および、ネットワークインターフェイス名を表示します。また、当該ノードの IP アドレスの情報と所属するリージョングループの情報も表示します。

  ⚠ 注意

  イベントの発生元として通知する IP アドレスの値は、イベントを検知した製品で管理する IP アドレスの値となります。そのため、環境によっては、Web コンソールのノード詳細画面などに表示している IMS コンポーネントで管理する IP アドレスの値とは異なる場合があります。

  [**トポロジーマップ**]アイコンをクリックすることで、イベントの発生元となるノードを配置しているマップを表示します。

  ヒント

  - [**トポロジーマップ**]アイコンは、NetvisorPro を利用している場合に表示されます。
  - [**カレントアラート**]ウィジェットから起動したイベント詳細ダイアログの場合は、現在の状況を表示する[**通常モード**]でトポロジーマップ画面を表示します。それ以外の場合は、イベント発生当時の状況を表示することができる[**分析モード**]でトポロジーマップ画面を表示し、イベントの発生時刻を中心とした[**期間**]が設定されます。
  - 当該ノードのアイコンを複数のマップに配置している場合は、表示するマップの選択画面が表示されます。

- [**発生時刻**]

  イベントの発生時刻を表示します。

- [**担当者**]

  当該イベントの対応を担当するユーザー名(表示名)を表示します。誰も担当者として割り当てられていない場合は、空欄となります。

- [**詳細**]

  イベントの詳細情報を表示します。

- [**対処**]

  イベントの対処方法の情報を表示します。

- [**SNMP トラップ Enterprise**]、[**Generic Code**]、[**Specific Code**]

SNMP トラップの情報を表示します。本項目は SNMP トラップのイベントでのみ表示されます。

- [**Syslog Facility**]、[**Severity**]

  Syslog の情報を表示します。本項目は Syslog のイベントでのみ表示されます。

- [**アプリケーション名**]

  イベントを検知したアプリケーション名(IMS コンポーネントと接続する製品名)を表示します。

操作ボタン

イベント詳細画面では、以下のボタンを用いて、イベントに対する操作を行うことができます。

ヒント

オブザーバーの役割を持つグループにしか属さないユーザーでは、操作ボタンは、表示されず、イベントに対する操作を行うことはできません。

- [**担当者に自分を割り当てる**]ボタン

  イベントに対し、自分を担当者として割り当てます。

- [**担当者を解除する**]ボタン

  イベントに対し割り当てられている担当者を解除します。

- [**回復する**]ボタン

  イベントを回復状態にします。

  ヒント

  イベントを検出した製品の仕様に依存して、イベントによっては、自動で回復状態を検出し、回復処理が行われます。

4.2.1.3　イベント重要度

Web コンソールに通知するイベントの重要度について説明します。

Web コンソールのイベント重要度

Web コンソールでは、各製品が検知したイベントに対し、以下の 6 つの重要度を割り当てて通知します。以下は重要度が高い順に記載しています。

- [ **Fatal**]

  システムダウンなど致命的な問題が発生したことを示します。

ヒント

Web コンソールの各画面で表示する稼働率は、[Fatal]のイベントが発生していた期間を「ノードの停止期間」と判断し、算出しています。

- [Critical]

  システムダウンなどの致命的な状況ではないが、至急の対処を必要とする問題が発生したことを示します。

- [Error]

  システム動作に影響する可能性がある一般的なエラーが発生したことを示します。

- [Warning]

  注意、確認が必要な事象が発生したことを示します。

- [Unknown]

  重要度が不明な事象が発生したことを示します。イベントを検知した製品側で重要度の定義が行われていない場合に[Unknown]での通知になります。

- [Normal]

  障害ではなく、システムの状況の変化を示すイベント、または、発生していた事象の回復を示すイベントなど、運用に関する情報が通知されたことを示します。

各製品の重要度との対応

Web コンソールでは、各製品でのイベント重要度と表現が異なっている部分があります。「表 4-1 各製品の重要度との対応状況（138 ページ）」に対応状況を示します。

表 4-1　各製品の重要度との対応状況

Web コンソール	NetvisorPro	NFA
Fatal	異常	-
Critical	MAJOR	-
Error	MINOR	異常
Warning	警告	警告
Unknown	不明	-
Normal	正常	正常

4.2.1.4　イベントの表示内容を絞り込む

イベント画面では、条件指定を行うことで、様々な観点でイベントを絞り込み状況確認していくことができます。

ここでは、夜間(2018/10/01 22:00:00 ~ 2018/10/02 03:00:00)に発生したイベントを検索する操作例を用いて、イベント画面の具体的な操作手順を説明します。

1. イベント画面を表示します。

   [**イベント**] メニューをクリックします。

2. 検索条件を入力します。

   プルダウンメニューから条件の対象となる項目を選択します。プルダウンメニューで対象項目を選択すると、選択した項目に対応する入力欄が表示されます。

   ここでは、プルダウンメニューから [**発生時刻**] を選択し、入力欄には、「2018-10-01 22:00:00」 ~ 「2018-10-02 03:00:00」を指定します。

   ヒント

   - [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。追加した条件の先頭に表示する[ー]アイコンをクリックすると追加した条件を取り消すことができます。
   - 異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

3. [**検索**]ボタンをクリックします。

   イベント画面に検索結果が表示されます。

4.2.1.5　イベント対応の担当者を割り当てる

自分が対応を担当するイベントの管理手順について説明します。

Web コンソールに通知されたイベントに対し、担当者として割り当てる操作を行うことで、自分が担当するイベントをイベント画面で管理していくことができます。

ヒント

オブザーバーの役割を持つグループにしか属さないユーザーでは、本操作を行うことはできません。

1. イベント画面を表示します。

   [**イベント**] メニューをクリックします。

2. 対応作業を担当するイベントを選択します。

   イベント画面のチェックボックスをオンにすることで、担当するイベントを選択します。

3. 担当者の割り当てを実施します。

   a. [**選択したイベントに対し:**]ボタンにカーソルを重ねます。

      [**担当者に自分を割り当てる**]ボタンが表示されます。

   b. [**担当者に自分を割り当てる**]ボタンをクリックします。

      確認ダイアログが表示されます。

   c. 確認ダイアログで内容を確認し、[**OK**]ボタンをクリックします。

   チェックボックスをオンにしたイベントの[**担当者**]欄に、自身のユーザー名が登録されます。

4. 担当者でイベント一覧を絞り込みます。

   a. 検索対象の項目を選択します。

      プルダウンメニューから [**担当者**] を選択します。

   b. 照合方法を選択します。

      プルダウンメニューから [**は次と等しい**] を選択します。

   c. 検索キーワードを指定します。

      自分のユーザー名(表示名)を指定します。

   d. 検索を実行します。

      指定した内容を確認し、[**検索**]ボタンをクリックします。

      担当者として割り当てられているイベントが、イベント一覧に表示されます。

   上記の手順で、自分が担当者となっているイベントを確認しながら、イベントの対応を行っていきます。

ヒント

- チェックボックスでオンになっているイベントに対し、[**担当者を解除する**]ボタンの操作を行うと、担当者の割り当てを解除することができます。
- すでに別のユーザーが担当者として割り当てられているイベントに対し、[**担当者に自分を割り当てる**]ボタンの操作を行うと、担当者を自分に変更することができます。

4.2.1.6　イベントの回復操作を行う

イベントを回復する手順について説明します。

発生していたイベントの対応が完了した後、当該イベントに対し回復操作を実施します。

ここでは、NetvisorPro が検知した「ルーター 01」の「ファン異常」(SNMP トラップ)のイベントに対する操作例を用いて、具体的な操作手順を説明します。

ヒント

- オブザーバーの役割を持つグループにしか属さないユーザーでは、本操作を行うことはできません。
- イベントを検出した製品（NetvisorPro、NFA）の仕様に依存して、イベントによっては自動で回復状態を検出し、回復処理が行われます。

  製品側で回復し、IMS コンポーネント側で回復しなかったイベントについては、改めて本操作を行ってください。
- イベントの回復操作を実施すると、イベントを検知した製品側においても回復操作が行われます。

1. イベント画面を表示します。

   [**イベント**] メニューをクリックします。

2. 回復対象のイベントを選択します。

   イベント画面のチェックボックスをオンにすることで、回復させたいイベントを選択します。

   必要に応じて、イベントの表示内容を絞り込んでから、選択を行います。

   ここでは、NetvisorPro が検知した「ルーター 01」の「ファン異常」のイベントのチェックボックスをオンにします。

3. イベントを回復します。

   a. [**選択したイベントに対し:**]ボタンにカーソルを重ねます。

      [**回復する**]ボタンが表示されます。

   b. [**回復する**]ボタンをクリックします。

      確認ダイアログが表示されます。

   c. 確認ダイアログで内容を確認し、[**OK**]ボタンをクリックします。

   NetvisorPro において、「ルーター 01」の「ファン異常」のアラートに対し、回復が実行されます。

   同時に、Web コンソールのイベント画面において、チェックボックスをオンにした「ルーター 01」の「ファン異常」のイベントの[**回復状態**]欄が、[**回復済**]に変わります。

4.2.1.7　イベントを削除する

イベントを削除する手順について説明します。

ネットワークの構成変更などの作業で通知された、管理、対応が不要なイベントに対しては、手動で削除することができます。

ヒント

オブザーバーの役割を持つグループにしか属さないユーザーでは、本操作を行うことはできません。

1. イベント画面を表示します。

   [**イベント**] メニューをクリックします。

2. 削除対象のイベントを選択します。

   イベント画面のチェックボックスをオンにすることで、削除したいイベントを選択します。

   必要に応じて、イベントの表示内容を絞り込んでから、選択を行います。

3. イベントを削除します。

   a. [**選択したイベントに対し:**]ボタンにカーソルを重ねます。

      [**削除する**]ボタンが表示されます。

   b. [**削除する**]ボタンをクリックします。

      確認ダイアログが表示されます。

   c. 確認ダイアログで内容を確認し、[**OK**]ボタンをクリックします。

   イベント画面において、チェックボックスをオンにしたイベントが削除されます。

4.2.2　トポロジーマップ（分析モード）によるイベント確認

トポロジーマップ画面では、現在の状況を表示する[**通常モード**]とノードの過去の状態(重要度)を表示する[**分析モード**]の 2 つの[**表示モード**]を使い分けて状況確認を行っていきます。ここでは、ノードの過去の状態を表示する[**分析モード**]の操作について説明します。

トポロジーマップ画面を[**分析モード**]で表示すると、タイムラインが表示されます。このタイムラインと、[**期間**]の指定により、各ノードの過去の状態をマップに反映して見ることができます。また、サイドパネルでは、指定ノードの過去の負荷状況を確認することができます。

[**分析モード**]の利用方法としては、例えば、深夜に障害が発生し、朝に状況を確認した時点で、自動復旧により回復状態になっていた事象が発生した場合に、深夜の障害発生時の状況をトポロジーマップ画面上で再現し、視覚的に状況を確認するといったことが挙げられます。

4.2.2.1　トポロジーマップ画面(分析モード)

トポロジーマップ画面の[**分析モード**]について説明します。

トポロジーマップ画面では、ネットワークの構成とともに、各ノードの状態、および、負荷状況を確認することができます。また、[**表示モード**]を[**分析モード**]に切り替えることで、各ノードの過去の状態をマップに反映して、当時の状況を調査することができます。

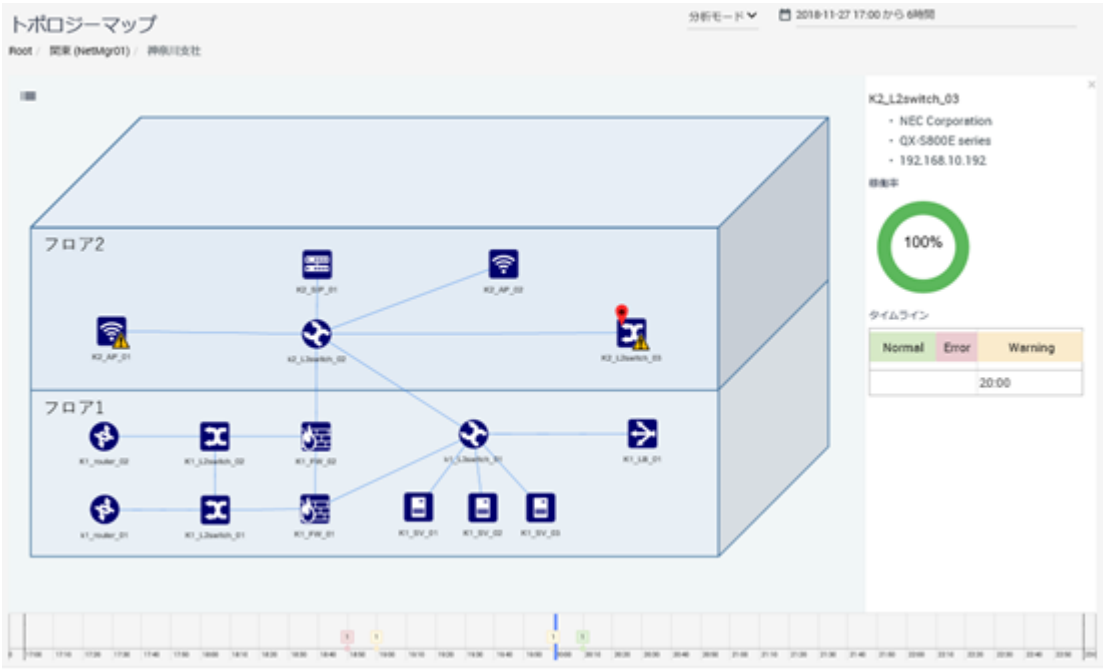

図 4-7　トポロジーマップ画面(分析モード)

画面操作領域

[**表示モード**]を[**分析モード**]に切り替えると、画面表示の自動更新が停止し、[**期間**]で指定した範囲のデータが表示されます。

- [**期間**](分析モード)

  タイムライン、および、サイドパネルを含むトポロジーマップ画面で表示するデータの表示期間を、起点となる過去の日時と期間(現在の方向)のプルダウンメニューで指定します。デフォルト値は、[**起点日時**]が「1 時間前の日時」で、[**期間**]が「1 時間」になります。

タイムライン

マップビューに表示する各ノードの状態変化を時系列で表示します。表示範囲は、[**期間**]で指定した範囲で、[**スライダー**]を動かすことで、その時点での各ノードの状態がマップに反映されます。また、ツリービュー上の[**マップ**]アイコンの状態も合わせて変化します。

過去の障害発生時のマップ、および、ノードの状態を視覚的に再現し、当時の影響範囲の確認や障害発生の関連性などの調査をサポートします。

⚠ 注意

タイムラインでは、イベントの発生履歴をもとに、過去における各ノードの重要度の状況を表示しますが、マップは、現在の構成のみを表示し、過去からの変更状況は表示しません。そのため、

マップの構成を変更していた場合に、変更前の重要度に対するノード数とマップの表示状況が一致しない場合があります。

その他の表示

ツリービュー、マップビュー、サイドパネルの表示内容、および、操作方法については、[**通常モード**]時と同様です。詳細は、「4.1.2.1　トポロジーマップ画面(通常モード) (117 ページ)」を参照してください。

⚠ 注意

[**分析モード**]は、ネットワークインターフェイスの状態に応じた接続線の色の変化には対応していません。

4.2.2.2　過去のイベント発生の影響をトポロジーマップで確認する

過去のイベント発生による影響をトポロジーマップで視覚的に確認する手順について説明します。

トポロジーマップ画面を[**分析モード**]で表示することで、過去に発生したイベントに対し、発生当時のネットワークの状態や各ノードのイベント発生の関係性をマップ上で確認することができます。

ここでは、「2018/10/01 00:00:00」前後に発生したイベントからマップでの影響確認を実施する操作例を用いて、トポロジーマップ画面(分析モード)の具体的な操作手順を説明します。

1. イベント画面を表示します。

   [**イベント**] メニューをクリックします。

2. 検索条件を入力します。

   ここでは、プルダウンメニューから [**発生時刻**] を選択します。また、「2018/10/01 00:00:00」前後に発生したイベントを確認したいため、入力欄には、「2018-09-30 23:00:00」～「2018-10-01 01:00:00」を指定します。

3. [**検索**]ボタンをクリックします。

   イベント画面に検索結果が表示されます。

4. イベント画面の検索結果を確認します。

   イベントの内容や発生の関連性を、イベント一覧の表示内容などから確認します。

5. イベントからトポロジーマップを表示します。

   イベントの[**トポロジーマップ**]アイコンをクリックすることで、イベントの発生元となるノードが配置されているマップを表示することができます。

   ここでは、複数発生しているイベントの中で、最も重要度が高いイベントの[**トポロジーマップ**]アイコンをクリックします。

[**トポロジーマップ**]アイコンをクリックすると、トポロジーマップ画面を[**分析モード**]で表示します。

6. 必要に応じて、[**期間**]の設定値を見直します。

   イベントからトポロジーマップ画面を表示した場合は、イベント発生時刻を含んだ表示期間を自動的に設定します。表示期間が適切ではない場合は、[**期間**]を改めて指定します。

   本例においては、[**起点日時**]に「2018-09-30 23:00:00」、[**期間**]に「2 時間」を指定し、「2018-09-30 23:00:00 ~ 2018-10-01 01:00:00」の状況を表示します。

7. 指定期間におけるノードの状態変化の状況を確認します。

   タイムラインで、各ノードがどの時間帯で状態変化しているのかや、どれくらいのノードで状態変化が発生しているのかを確認します。

8. ノード状態の時間的な変化の状況を確認します。

   タイムラインの[**スライダー**]を動かして、マップへの状態反映を行っていき、イベントが発生した時間帯における各ノードの状態と周辺システムへの影響を調べます。

ヒント

- このとき、ツリービューを表示して、[**スライダー**]操作を行うことで、同時間帯で、別のマップに配置するノードの状態変化の有無も確認することができます。
- 細かな状況変化を調べたい場合は、[**期間**]を可能な限り狭めて設定します。

発生しているイベントがノードの負荷と関連している場合は、マップ上の当該ノードのアイコンをクリックし、サイドパネルを表示することで、状況確認を行うことができます。また、特定ノードに対して、詳細な調査が必要になってきた場合は、サイドパネルで表示するノード名のリンクをクリックし、当該ノードに対するノード詳細画面を表示します。

4.2.3　Syslog の発生状況を確認する

Web コンソールでは、NetvisorPro のシスログサーバー機能(SyslogDiagnosis 機能ライセンス)で受信、蓄積した Syslog の内容を Syslog 画面で確認することができます。

Syslog 画面では、必ず、[**リージョン**]、および、[**受信時刻**]の条件を指定して、Syslog を表示します。また、[**ノード名**]や[**メッセージ**]などの条件を加えていくことで、表示する Syslog を絞り込んでいくことができます。

例えば、障害が発生した時刻から 6 時間前までの Syslog の中から、メッセージに特定の IP アドレスの情報を含んだもののみに絞り込んで、Syslog の発生状況、内容を調べるといった操作を行うことができます。

上記のように、すべての蓄積した Syslog に対し、様々な条件での検索を行うことで、指定期間内でのシステムの状況を効率的に調べていくことができます。

4.2.3.1　Syslog 画面

Syslog 画面について説明します。

Syslog 画面は、NetvisorPro に蓄積されている Syslog を、様々な観点で確認、調査する際に利用します。

Syslog 画面は、[**Syslog**] メニューをクリックして表示します。

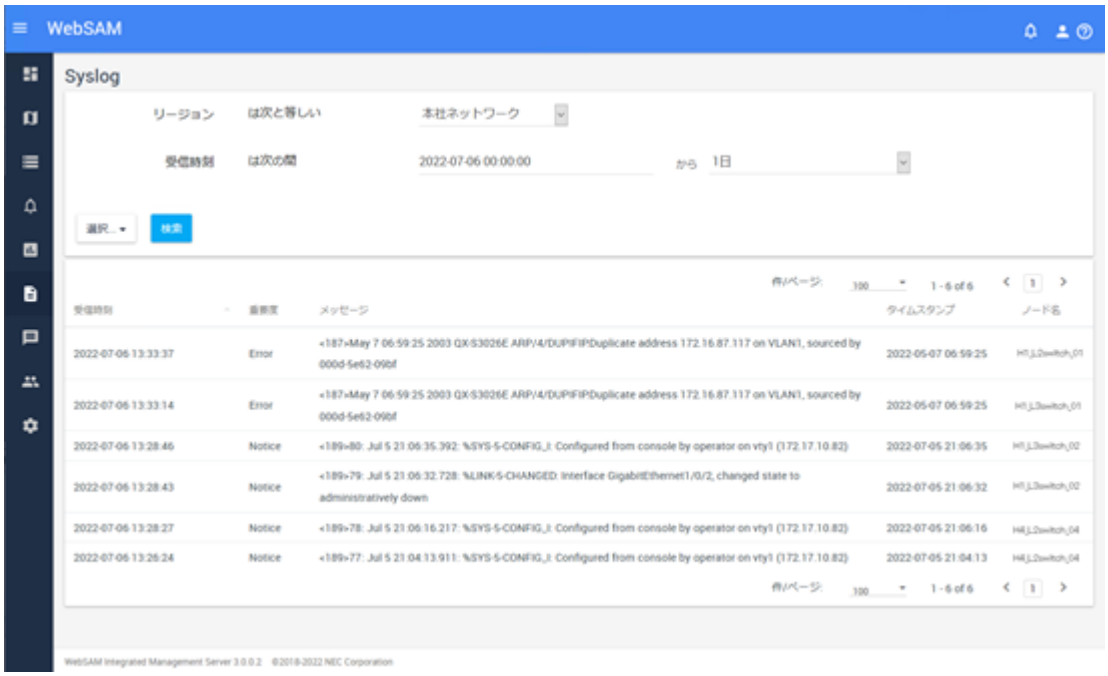

図 4-8　Syslog 画面

検索条件の指定

Syslog 一覧で表示する各項目の内容に対し、条件を指定して、表示する Syslog を絞り込むことができます。

以下の 2 つの項目については、条件指定が必須となります。

- [**リージョン**]

  リージョングループ名を指定し、表示対象の Syslog を絞り込みます。

- [**受信時刻**]

  表示対象の Syslog の受信期間を起点となる過去の日時と期間(現在の方向)のプルダウンメニューで指定します。デフォルト値は、[**起点日時**]が「画面表示した日の 0:00」で、[**期間**]が「1 日」になります。

その他の項目に対する検索条件の指定方法については、以下の通りです。

- 条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。

追加した条件の先頭に表示する[ー]アイコンをクリックすると追加した条件を取り消すことができます。

- 条件指定

  Syslog 一覧で表示する各項目に対し、以下の 3 つの方法で、検索条件を指定します。検索条件の指定方法は、選択した項目ごとに異なります。

  - チェックボックスによる指定

    チェックボックスを用いて、検索条件を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**重要度**]

  - キーワードの指定

    選択した項目に対して、キーワードと照合方法を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**メッセージ**]、[**ノード名**]

    照合方法については、以下を指定することができます。

    * 照合方法：

      [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

  - 時刻の範囲指定

    選択した項目に対して、*YYYY-MM-DD hh:mm* の形式で時間範囲を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**タイムスタンプ**]

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

条件を指定した後、[**検索**]ボタンをクリックすると、検索条件に合致した Syslog の一覧が表示されます。

Syslog 一覧

- [**受信時刻**]

  NetvisorPro が Syslog を受信した時刻を表示します。

- [**重要度**]

Syslog の重要度を表示します。

イベントの重要度とは異なり、[**Emergency**]、[**Alert**]、[**Critical**]、[**Error**]、[**Warning**]、[**Notice**]、[**Informational**]、[**Debug**]の 8 種類の重要度で表現されます。

- [**メッセージ**]

  Syslog のメッセージ内容を表示します。

- [**タイムスタンプ**]

  Syslog の送信元で記録された Syslog の発生時刻を表示します。

- [**ノード名**]

  Syslog の送信元であるノード名を表示します。

1 ページに表示する Syslog の件数は、プルダウンメニュー([**50**]、[**100**]、[**250**])から選択します。デフォルト値は、[**100**]です。

検索条件に合致したすべての Syslog を 1 ページで表示できない場合は、ページを切り替えて確認します。

ヒント

検索条件において 6 時間以上の期間を指定した場合、性能を考慮して条件に合致する Syslog の件数は表示しません。件数の把握を行いたい場合は、検索条件の期間を狭めて検索を行ってください。

4.2.3.2　障害発生前後の Syslog を調査する

Syslog 画面では、条件指定を行うことで、様々な観点で Syslog を絞り込み状況確認していくことができます。

ここでは、リージョングループ「関東地区」で、2022/10/10 15:30 頃に障害が発生したとし、その前後の Syslog を調査する操作例を用いて、Syslog 画面の具体的な操作手順を説明します。

1. Syslog 画面を表示します。

   [**Syslog**] メニューをクリックします。

2. リージョングループの条件を入力します。

   プルダウンメニューから条件の対象となるリージョングループを選択します。

   ここでは、プルダウンメニューから [**関東地区**] を選択します。

3. 受信時刻の条件を入力します。

   表示対象の Syslog を受信した時間帯を指定します。

   ここでは障害発生前後の時間範囲になるように、起点になる日時として、「2022/10/10 15:00」を指定し、期間としてプルダウンメニューから[**1 時間**]を選択します。

4. その他の検索条件を入力します。

   プルダウンメニューから条件の対象となる項目を選択します。プルダウンメニューで対象項目を選択すると、選択した項目に対応する入力欄が表示されます。

   ここでは、プルダウンメニューから [**ノード名**] を選択し、照合方法として、[**は次と等しい**]を選択します。また、入力欄には、障害が発生したノードの名前を指定します。

   ヒント

   - [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。追加した条件の先頭に表示する[ー]アイコンをクリックすると追加した条件を取り消すことができます。
   - 異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

5. [**検索**]ボタンをクリックします。

   Syslog 画面に検索結果が表示されます。

   調査対象とする Syslog の内容に合わせて、必要に応じて検索条件を変更し、表示する Syslog を絞り込み、Syslog の発生状況を確認します。

⚠ 注意

指定した条件に合致する Syslog の件数が多い場合、処理に時間がかかり、タイムアウトを示すメッセージが表示される場合があります。この場合は、表示対象とする Syslog の条件内容を見直してください。

4.3　ノードの状態を詳細に確認する

ノード詳細画面では、指定したノードに特化したダッシュボード表示を行います。

ノード詳細画面では、指定したノードに対し、以下の情報を確認することができ、ノードの詳細状況を即座に把握することができます。

- プロパティ情報
- 稼働率情報
- イベント一覧
- ランキング形式(TopN)によるフロー情報
- ランキング形式(TopN)による CPU、メモリ、ネットワークインターフェイス関連の負荷情報、および、応答時間情報

4.3.1　ノード詳細画面

指定したノードに対するダッシュボードを表示するノード詳細画面について説明します。

ノード詳細画面は、様々な観点の情報からノードの詳細状況を把握するために利用します。

ノード詳細画面は、各画面で表示するノード名のリンクをクリックすることで表示します。

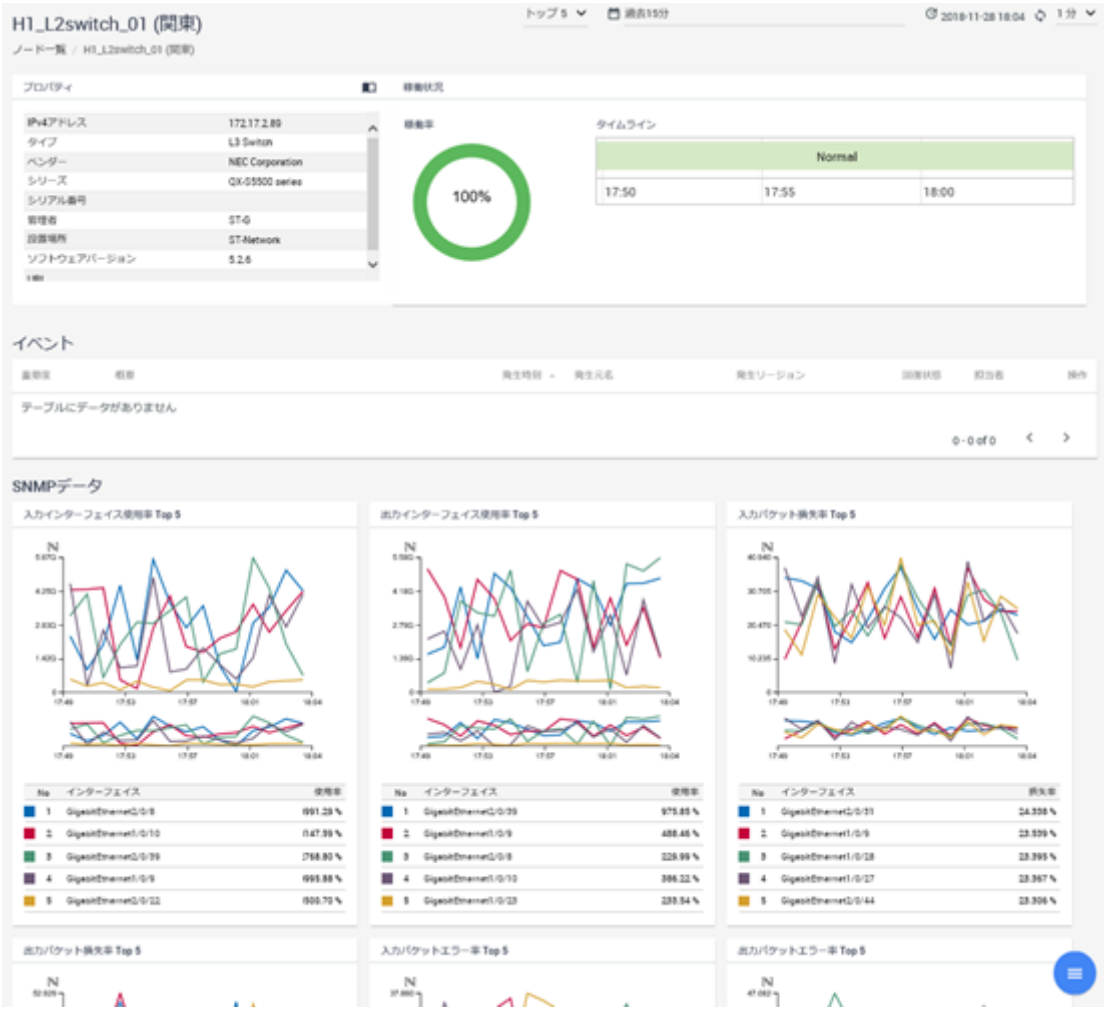

図 4-9　ノード詳細画面

ノード詳細画面の右下に配置する[**MENU**]ボタンにカーソルを重ねると以下の操作ボタンが表示されます。以下の操作ボタンをクリックすることで、当該ノードに対する各画面を表示することができます。

- [**フロー分析**]ボタン

  当該ノードをエクスポーターとして登録している NFA のエクスポーター分析画面を表示します。本ボタンは、NFA を利用している場合に表示します。

- [**トポロジーマップ**]ボタン

  当該ノードを配置しているマップを表示します。本ボタンは、NetvisorPro を利用している場合に表示します。

ヒント

当該ノードのアイコンを複数のマップに配置している場合は、表示するマップの選択画面が表示されます。

- [**IPV6 アドレス一覧**]ボタン

  当該ノードに対する IPv6 アドレス一覧画面を表示します。本ボタンは、NetvisorPro を利用している場合に表示します。

- [**ネットワークインターフェイス一覧**]ボタン

  当該ノードに対するネットワークインターフェイス一覧画面を表示します。

画面操作領域

- [**件数**]

  各ウィジェットで表示する、ランキングデータの表示件数をプルダウンメニュー([**トップ 5**]、[**トップ 10**]、[**トップ 20**])から選択します。デフォルト値は、[**トップ 5**]です。

- [**期間**]

  ウィジェットで扱うデータの表示期間を以下の 2 つの方法で指定します。

  - [**既定の期間から選択**](デフォルト値)

    データの表示期間をプルダウンメニュー([**過去 15 分**]、[**過去 30 分**]、[**過去 1 時間**]、[**過去 6 時間**]、[**過去 24 時間**]、[**過去 48 時間**]、[**過去 72 時間**])から選択します。デフォルト値は、[**過去 1 時間**]です。

  - [**特定の日時と期間を指定**]

    データの表示期間を起点となる過去の日時と期間(現在の方向)のプルダウンメニューで指定します。デフォルト値は、[**起点日時**]が「1 時間前の日時」で、[**期間**]が「1 時間」になります。

- [**最終更新時刻**]

  画面更新を実施した日時を表示します。

- [**更新**]アイコン

  画面表示を最新の内容に更新します。

- [**更新間隔**]

  画面表示の更新間隔をプルダウンメニュー([**1 分**]、[**5 分**]、[**15 分**]、[**なし**])から選択します。デフォルト値は、[**1 分**]です。

ウィジェット表示領域

指定したノードに関するウィジェットを表示します。ノード詳細画面では、以下のウィジェットを表示します。

- [**プロパティ**]ウィジェット

  ノードのプロパティ情報を表示します。[ ]アイコンをクリックすると、プロパティ詳細ダイアログが表示されます。

  ノードのプロパティ情報は、NetvisorPro、または、NFA に登録している情報を統合して表示します。

  ヒント

  - NetvisorPro において、ノードのプロパティの[**URL**]を登録している場合、Web コンソールでは、リンク形式で登録した URL 情報を表示します。そのため、URL をクリックするだけで、当該サイトにアクセスすることができます。
  - プロパティ詳細ダイアログでは、NetvisorPro が、ノードの MIB から収集した以下の情報を表示します。
    - [**説明**]

      ノードの sysDescr (1.3.6.1.2.1.1.1)から取得した機種情報の説明を表示します。
    - [**sysObjectID**]

      ノードの sysObjectID (1.3.6.1.2.1.1.2)から取得した機種を識別するための ID を表示します。

- [**稼働状況**]ウィジェット

  ノードの稼働率、および、状態変化を示すタイムラインを表示します。

  本ウィジェットは、NetvisorPro を利用している場合に表示されます。

- [**イベント**]ウィジェット

  当該ノードで発生したイベントの一覧を表示します。[**イベント詳細**]アイコンをクリックすると、当該イベントに対するイベント詳細画面を表示します。

- フローデータ

  フローデータの各ウィジェットは、NFA を利用している場合に表示されます。

  - [**アプリケーション**]ウィジェット

    当該ノードを経由した通信フローにおける、アプリケーションの通信量に対するランキングデータを表示します。
  - [**IP プロトコル**]ウィジェット

    当該ノードを経由した通信フローにおける、IP プロトコルの通信量に対するランキングデータを表示します。
  - [**DSCP**]ウィジェット

当該ノードを経由した通信フローにおける、DSCP(IP パケットの優先度設定)の設定値毎の通信量に対するランキングデータを表示します。

- [**カンバセーション**]ウィジェット

  当該ノードを経由した通信フローにおける、カンバセーション(通信を行う 2 点間の情報)の通信量に対するランキングデータを表示します。

- SNMP データ

  SNMP データの各ウィジェットは、NetvisorPro を利用している場合に表示されます。

  - [**CPU 使用率**]ウィジェット

    ノードの CPU 使用率に対するランキングデータを表示します。

  - [**メモリ使用率**]ウィジェット

    ノードのメモリ使用率に対するランキングデータを表示します。

  - [**入力インターフェイス使用率**]ウィジェット

    ノードが保持するネットワークインターフェイスの入力側の使用率に対するランキングデータを表示します。

  - [**入力インターフェイス使用量**]ウィジェット

    ノードが保持するネットワークインターフェイスの入力側の使用量に対するランキングデータを表示します。

  - [**出力インターフェイス使用率**]ウィジェット

    ノードが保持するネットワークインターフェイスの出力側の使用率に対するランキングデータを表示します。

  - [**出力インターフェイス使用量**]ウィジェット

    ノードが保持するネットワークインターフェイスの出力側の使用量に対するランキングデータを表示します。

  - [**入力パケット損失率**]ウィジェット

    ノードが保持するネットワークインターフェイスの入力側のパケット損失率に対するランキングデータを表示します。

  - [**入力パケット損失数**]ウィジェット

    ノードが保持するネットワークインターフェイスの入力側のパケット損失数に対するランキングデータを表示します。

  - [**出力パケット損失率**]ウィジェット

    ノードが保持するネットワークインターフェイスの出力側のパケット損失率に対するランキングデータを表示します。

  - [**出力パケット損失数**]ウィジェット

ノードが保持するネットワークインターフェイスの出力側のパケット損失数に対するランキングデータを表示します。

- [**入力パケットエラー率**]ウィジェット

  ノードが保持するネットワークインターフェイスの入力側のパケットエラー率に対するランキングデータを表示します。

- [**入力パケットエラー数**]ウィジェット

  ノードが保持するネットワークインターフェイスの入力側のパケットエラー数に対するランキングデータを表示します。

- [**出力パケットエラー率**]ウィジェット

  ノードが保持するネットワークインターフェイスの出力側のパケットエラー率に対するランキングデータを表示します。

- [**出力パケットエラー数**]ウィジェット

  ノードが保持するネットワークインターフェイスの出力側のパケットエラー数に対するランキングデータを表示します。

- [**応答時間(IPv4)**]ウィジェット

  ノードの ICMP ECHO に対する応答時間を表示します。

- [**応答時間(IPv6)**]ウィジェット

  ノードの ICMPv6 ECHO に対する応答時間を表示します。

- 任意のデータ種別のウィジェット

  NetvisorPro で任意のデータ種別を設定している場合は、それに応じたデータを表示します。

⚠ 注意

SNMP データ、および、フローデータの各ウィジェットにおいては、NetvisorPro、および、NFA 側でデータを収集する設定を行っていない場合、非表示となります。

4.3.2　ノードの過去の状態を確認する

ノード詳細画面を利用して、特定のノードの過去の状態を調査する方法を説明します。

ノード詳細画面では、[**期間**]に過去の期間を指定することで、ノードの過去の状態を各ウィジェットで確認することができます。

ここでは、昨夜の「23：00」頃に「ルーター 01」で発生したイベントを起点に、「ルーター 01」の当時の状態を調べる例を用いて、具体的な操作手順について説明します。

1. イベント画面を表示します。

   [**イベント**] メニューをクリックします。

2. 障害調査対象のノードを検索します。

   a. プルダウンメニューから [**発生元名**] を選択します。

   b. 照合方法として、[**は次と等しい**]を選択します。

   c. 調査対象のノード名を入力します。

      ここでは、「ルーター 01」と入力します。

   d. [**検索**]ボタンをクリックします。

   イベント画面に、「ルーター 01」で発生したイベントが一覧表示されます。

3. イベントの内容を確認します。

   例えば、昨夜の「23：00」頃に「CPU 使用率のしきい値超過」のイベントが発生していたとします。以降の手順では、「CPU 使用率のしきい値超過」のイベントの調査について説明していきます。

4. イベントの発生元であるノードに対するノード詳細画面を表示します。

   [**発生元名**]欄のノード名のリンクをクリックします。

   ここでは、「ルーター 01」のリンクをクリックします。

   リンクをクリックすると、「ルーター 01」に対するノード詳細画面が表示されます。また、[**期間**]には、「CPU 使用率のしきい値超過」のイベントが発生した昨夜の「23：00」を含む過去の期間が設定されます。

5. 指定期間でのノードの状態を確認します。

   [**CPU 使用率**]ウィジェットからは、当時の CPU の挙動を確認することができます。

   [**入力インターフェイス使用率**]ウィジェット、または、[**出力インターフェイス使用率**]ウィジェットから、当時の通信量の多さを確認することができます。

   [**アプリケーション**]ウィジェット、または、[**カンバセーション**]ウィジェットからは、「ルーター 01」を経由した通信内容を確認することができ、CPU 負荷に影響を与えるものがないかを調査することができます。

   通信状況に問題が見つからない場合は、[**プロパティ**]ウィジェットで表示する[**ソフトウェアバージョン**]から、既存の問題が含まれていないかを「ルーター 01」のサポート窓口に問い合わせを行うなどの対応も考えられます。

CPU 使用率が高くなった原因として、通信状況が関係している可能性がある場合は、NFA による詳細なフロー分析が効果的です。[**アプリケーション**]ウィジェット、または、[**カンバセーション**]ウィジェット内のリンクや、[**フロー分析**]ボタンをクリックすることで、NFA のエクスポーター分析画面を簡単に表示することができます。

4.4　ネットワークインターフェイスの状態を確認する

Web コンソールでは、指定したノードが保持するネットワークインターフェイスの詳細情報を確認するための仕組みを提供しています。

ネットワークインターフェイスの詳細情報を確認するための方法として、具体的には、以下の画面を操作します。

- ネットワークインターフェイス一覧画面

  ノードが保持するすべてのネットワークインターフェイスのプロパティ情報を表示します。

- IPv6 アドレス一覧画面

  ノードのネットワークインターフェイスに割り当てられている IPv6 アドレスの詳細情報を表示します。

- ネットワークインターフェイス詳細画面

  指定したネットワークインターフェイスの様々なデータを表示し、ネットワークインターフェイスの通信状況の確認を行うことができます。

4.4.1　ネットワークインターフェイス一覧画面

ネットワークインターフェイス一覧画面について説明します。

ネットワークインターフェイス一覧画面では、ノードが保持するすべてのネットワークインターフェイスのプロパティ情報を確認することができます。

ネットワークインターフェイス一覧画面は、ノード詳細画面の[**ネットワークインターフェイス一覧**]ボタンをクリックして表示します。ノード詳細画面は、各画面で表示するノード名のリンクをクリックすることで表示します。

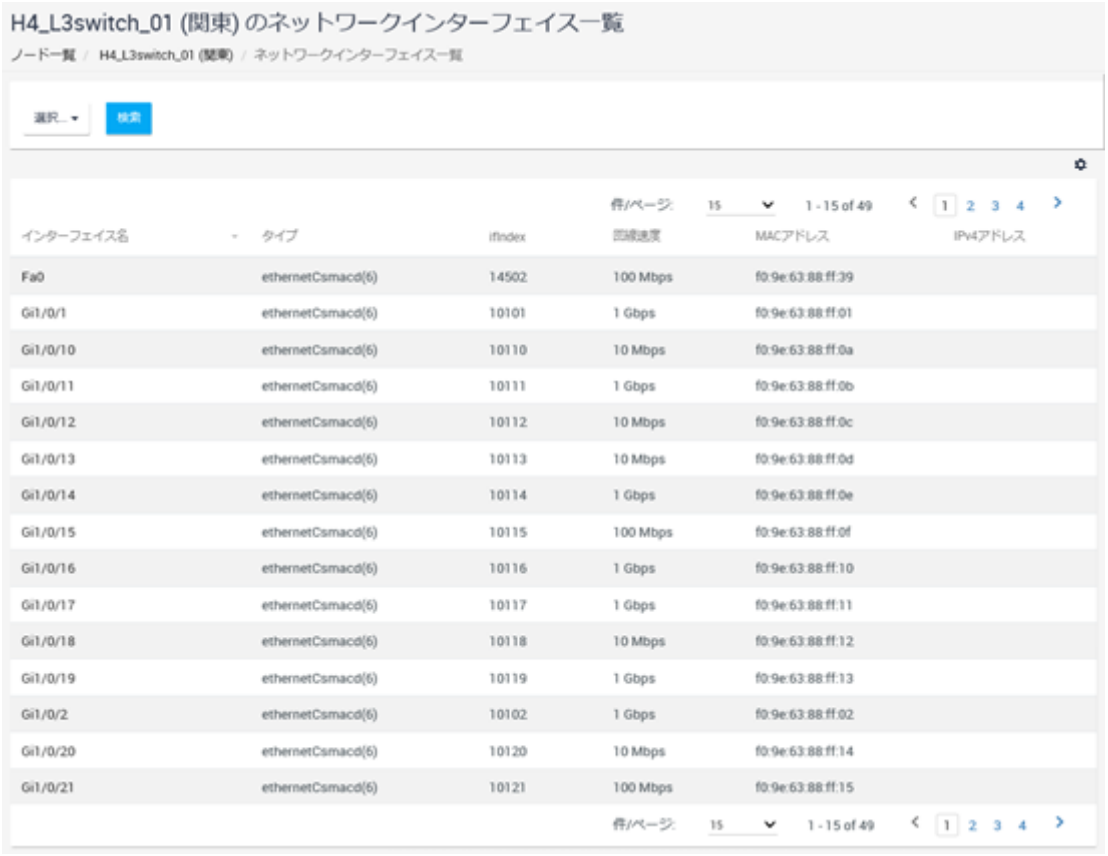

図 4-10　ネットワークインターフェース一覧画面

検索条件の指定

ネットワークインターフェイス一覧で表示する各項目の内容に対し、条件を指定して、表示するネットワークインターフェイスを絞り込むことができます。

- 条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。

  追加した条件の先頭に表示する[ー]アイコンをクリックすると追加した条件を取り消すことができます。

- 条件指定

  ネットワークインターフェイス一覧で表示する各項目に対し、以下の 3 つの方法で、検索条件を指定します。検索条件の指定方法は、選択した項目ごとに異なります。

  - チェックボックスによる指定

    チェックボックスを用いて、検索条件を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**状態**]

  - キーワードの指定

選択した項目に対して、キーワードと照合方法を指定します。対象項目は以下の通りです。

* 対象項目：

  [**インターフェイス名**]、[**タイプ**]、[**別名**]、[**説明**]、[**MAC アドレス**]

照合方法については、以下を指定することができます。

* 照合方法：

  [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

- 値の範囲指定

  検索条件として、値、もしくは、値の範囲を指定します。対象項目は以下の通りです。

  * 対象項目：

    [**ifIndex**]、[**回線速度**]、[**IPv4 アドレス**]

  * 照合方法：

    [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次の値以上**](以上)、[**は次の値以下**](以下)、[**は次の間**](範囲内)

    [**IPv4 アドレス**]に対しては、[**は次と等しい**](一致)、[**は次の間**](範囲内)のみ指定することができます。

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

⚠ 注意

検索条件には、一覧表に表示されている項目のみが指定可能です。非表示となっている項目は検索条件として指定できません。

条件を指定した後、[**検索**]ボタンをクリックすると、検索条件に合致したノードの一覧が表示されます。

ネットワークインターフェイス一覧

- [**状態**]

  ネットワークインターフェイスの状態を表示します。Web コンソールで表示するネットワークインターフェイスの状態の詳細については、「4.4.2　ネットワークインターフェイスの状態（159 ページ）」を参照してください。

- [**インターフェイス名**]

ネットワークインターフェイスの名前を表示します。インターフェイス名のリンクをクリックすると、当該ネットワークインターフェイスに対するネットワークインターフェイス詳細画面を表示します。

- [**タイプ**]

  ネットワークインターフェイスのタイプ情報を表示します。

  ヒント

  表示する値は、MIB の ifType(1.3.6.1.2.1.2.2.1.3)から取得したものであり、IANA(Internet Assigned Numbers Authority)によって定義された表記で表示します。

- [**ifIndex**]

  ネットワークインターフェイスを一意に識別するための ID 値を表示します。

- [**別名**]

  ネットワークインターフェイスの別名(ifAlias)を表示します。

- [**説明**]

  ネットワークインターフェイスの説明(ifDescr)を表示します。

- [**回線速度**]

  ネットワークインターフェイスの回線速度を表示します。

- [**MAC アドレス**]

  ネットワークインターフェイスに割り当てられている MAC アドレスを表示します。

- [**IP アドレス**]

  ネットワークインターフェイスに割り当てられている IPv4 アドレスを表示します。

1 ページに表示するネットワークインターフェイス情報の件数は、プルダウンメニュー([**15**]、[**50**]、[**100**])から選択します。デフォルト値は、[**15**]件です。

すべてのネットワークインターフェイス情報を 1 ページで表示できない場合は、ページを切り替えて、ネットワークインターフェイス情報を確認します。

[**設定**]アイコンをクリックすることで、列の表示設定を行うことができます。詳細は「3.4　各種一覧画面における一覧表の列の表示設定を行う（110 ページ）」を参照してください。

4.4.2　ネットワークインターフェイスの状態

ネットワークインターフェイスの状態について説明します。

ネットワークインターフェイスの状態

Web コンソールでは、各製品でのネットワークインターフェイスに対する監視結果を統合して、ネットワークインターフェイスの状態として管理します。

状態は以下の 4 つの種類があります。複数の状態に当てはまる場合は、以下の優先順位によって状態が決まります。

表 4-2　状態の種類

状態	説明	優先順位
[**DOWN**]	ポートがダウンし、利用できない状態を示します。 トポロジーマップ画面の[**通常モード**]において、DOWN 状態のネットワークインターフェイスを端点とする接続線は赤色で表示されます。 NetvisorPro においては、状態監視機能や SNMP トラップの受信によってポートのダウンを検知した場合に該当します。	1
[**しきい値異常**]	しきい値での監視によって異常状態となっていることを示します。 NetvisorPro においては、データ収集機能での当該ネットワークインターフェイスに対するしきい値監視で超過が起き、重要度が異常のアラートが発生した場合に該当します。	2
[**しきい値警告**]	しきい値での監視によって警告状態となっていることを示します。 NetvisorPro においては、データ収集機能での当該ネットワークインターフェイスに対するしきい値監視で超過が起き、重要度が MAJOR、MINOR、警告のアラートが発生した場合に該当します。	3
[-](Unknown)	障害が発生していない、または、監視を行っていない状態を示します。	4

4.4.3　IPv6 アドレス一覧画面

IPv6 アドレス一覧画面について説明します。

IPv6 アドレス一覧画面では、ノードのネットワークインターフェイスに割り当てられている IPv6 アドレスの情報を確認することができます。

IPv6 アドレス一覧画面は、ノード詳細画面の[**IPV6 アドレス一覧**]ボタンをクリックして表示します。ノード詳細画面は、各画面で表示するノード名のリンクをクリックすることで表示します。

図 4-11　IPv6 アドレス一覧画面

IPv6 アドレス定義一覧

- [**ipv6ifIndex**]

  IPv6 インターフェイスを一意に識別するための ID を表示します。

- [**下位レイヤー**]

  ネットワークインターフェイスが動作するプロトコルレイヤーを識別するための ID を表示します。

- [**MAC アドレス**]

  IPv6 インターフェイスに割り当てられている MAC アドレスを表示します。

- [**IPv6 アドレス**]

  IPv6 インターフェイスに割り当てられている IPv6 アドレスを表示します。

- [**説明**]

  IPv6 インターフェイスに対する説明を表示します。

4.4.4　ノードに割り当てられている IPv6 アドレスを確認する

ノードのネットワークインターフェイスに割り当てられているすべての IPv6 アドレスを確認する方法について説明します。

ここでは、「ルーター 01」の IPv6 アドレスを確認する操作例を用いて、具体的な操作手順を説明します。

1. ノード一覧画面を表示します。

   [**ノード一覧**] メニューをクリックします。

2. 確認対象のノードを選択します。

   ここでは、[**ノード名**]欄の「ルーター 01」のリンクをクリックします。

「ルーター 01」に対するノード詳細画面が表示されます。

3. 監視処理で利用している代表の IPv6 アドレスを確認します。

   [**プロパティ**]ウィジェットの[▽]アイコンをクリックし、プロパティ詳細ダイアログを表示します。プロパティ詳細ダイアログでは、[**IPv6 アドレス**]欄に、監視処理で利用している代表の IPv6 アドレスを表示します。

4. IPv6 アドレス一覧画面を表示します。

   IPv6 アドレス一覧画面では、その他の IPv6 アドレスの割り当て状況を確認することができます。

   ノード詳細画面の[**IPV6 アドレス一覧**]ボタンをクリックします。

5. IPv6 アドレス一覧の内容を確認します。

   IPv6 アドレス一覧には、監視処理で利用する代表の IPv6 アドレスを含め、ノードのネットワークインターフェイスに割り当てられているすべての IPv6 アドレスの情報を表示します。

4.4.5　ネットワークインターフェイス詳細画面

指定したネットワークインターフェイスの通信状況を示す様々なデータを表示するネットワークインターフェイス詳細画面について説明します。

ネットワークインターフェイス詳細画面は、様々な観点の情報からネットワークインターフェイスの詳細状況を把握するために利用します。

ネットワークインターフェイス詳細画面は、各画面で表示するネットワークインターフェイス名のリンクをクリックすることで表示します。

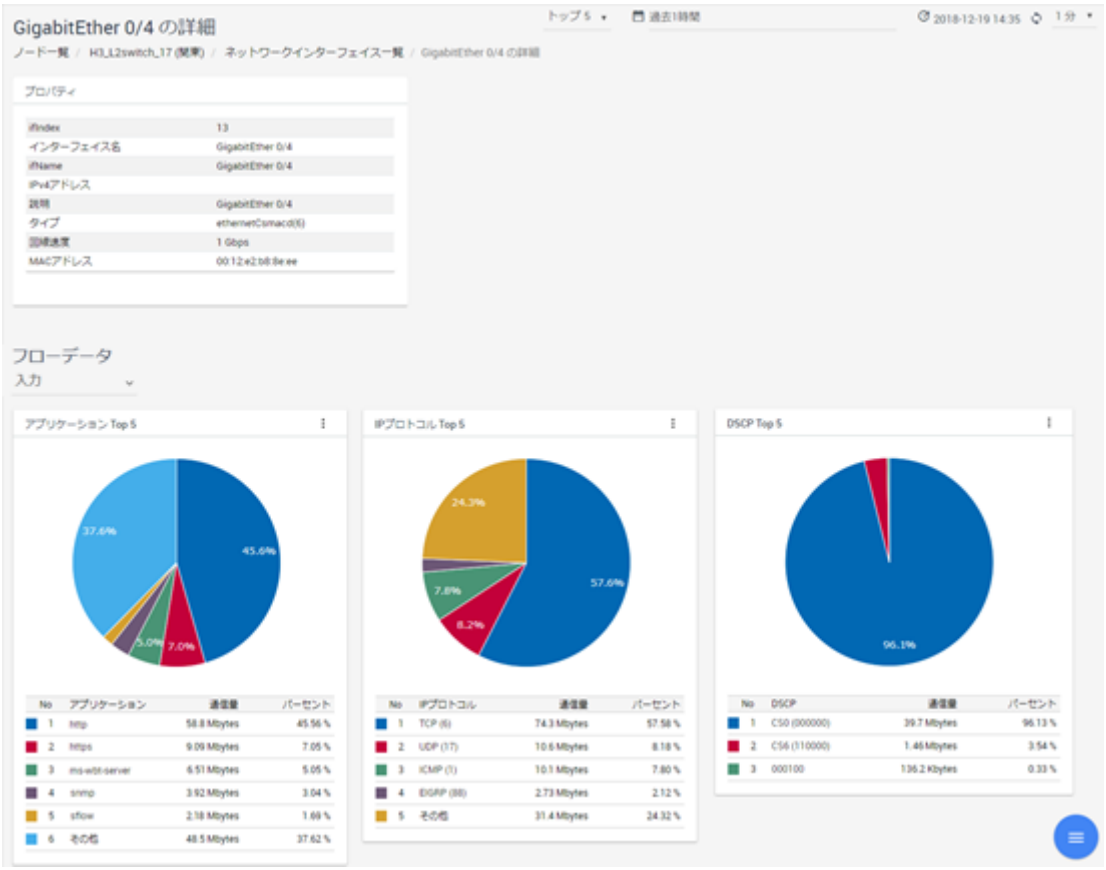

図 4-12　ネットワークインターフェイス詳細画面

ネットワークインターフェイス詳細画面の右下に配置する[**MENU**]ボタンにカーソルを重ねると以下の操作ボタンが表示されます。

- [**フロー分析**]ボタン

  当該ネットワークインターフェイスを登録している NFA のエクスポーター分析画面を表示します。本ボタンは、NFA を利用している場合に表示します。

画面操作領域

- [**件数**]

  フロー情報を扱うウィジェットで表示する、ランキングデータの表示件数をプルダウンメニュー([**トップ 5**]、[**トップ 10**]、[**トップ 20**])から選択します。デフォルト値は、[**トップ 5**]です。

  ヒント

  NFA を利用していない場合、[**件数**]は表示されません。

- [**期間**]

  ウィジェットで扱うデータの表示期間を以下の 2 つの方法で指定します。

  - [**既定の期間から選択**](デフォルト値)

データの表示期間をプルダウンメニュー([**過去 15 分**]、[**過去 30 分**]、[**過去 1 時間**]、[**過去 6 時間**]、[**過去 24 時間**]、[**過去 48 時間**]、[**過去 72 時間**])から選択します。デフォルト値は、[**過去 1 時間**]です。

- [**特定の日時と期間を指定**]

  データの表示期間を起点となる過去の日時と期間(現在の方向)のプルダウンメニューで指定します。デフォルト値は、[**起点日時**]が「1 時間前の日時」で、[**期間**]が「1 時間」になります。

- [**最終更新時刻**]

  画面更新を実施した日時を表示します。

- [**更新**]アイコン

  画面表示を最新の内容に更新します。

- [**更新間隔**]

  画面表示の更新間隔をプルダウンメニュー([**1 分**]、[**5 分**]、[**15 分**]、[**なし**])から選択します。デフォルト値は、[**1 分**]です。

ウィジェット表示領域

指定したネットワークインターフェイスに関するウィジェットを表示します。ネットワークインターフェイス詳細画面では、以下のウィジェットを表示します。

- [**プロパティ**]ウィジェット

  ネットワークインターフェイスのプロパティ情報を表示します。

- フローデータ

  フローデータの各ウィジェットは、NFA を利用している場合に表示されます。

  - [**アプリケーション**]ウィジェット

    当該ネットワークインターフェイスを経由した通信フローにおける、アプリケーションの通信量に対するランキングデータを表示します。

  - [**IP プロトコル**]ウィジェット

    当該ネットワークインターフェイスを経由した通信フローにおける、IP プロトコルの通信量に対するランキングデータを表示します。

  - [**DSCP**]ウィジェット

    当該ネットワークインターフェイスを経由した通信フローにおける、DSCP(IP パケットの優先度設定)の設定値毎の通信量に対するランキングデータを表示します。

  - [**カンバセーション**]ウィジェット

当該ネットワークインターフェイスを経由した通信フローにおける、カンバセーション(通信を行う 2 点間の情報)の通信量に対するランキングデータを表示します。

ヒント

NFA 3.2 以降を利用している場合、当該ネットワークインターフェイスに対して、抽出するフローの方向を指定することができます。

- SNMP データ

  SNMP データの各ウィジェットは、NetvisorPro を利用している場合に表示されます。

  - [**入力インターフェイス使用率**]ウィジェット

    ネットワークインターフェイスの入力側の使用率を表示します。

  - [**入力インターフェイス使用量**]ウィジェット

    ネットワークインターフェイスの入力側の使用量を表示します。

  - [**出力インターフェイス使用率**]ウィジェット

    ネットワークインターフェイスの出力側の使用率を表示します。

  - [**出力インターフェイス使用量**]ウィジェット

    ネットワークインターフェイスの出力側の使用量を表示します。

  - [**入力パケット損失率**]ウィジェット

    ネットワークインターフェイスの入力側のパケット損失率を表示します。

  - [**入力パケット損失数**]ウィジェット

    ネットワークインターフェイスの入力側のパケット損失数を表示します。

  - [**出力パケット損失率**]ウィジェット

    ネットワークインターフェイスの出力側のパケット損失率を表示します。

  - [**出力パケット損失数**]ウィジェット

    ネットワークインターフェイスの出力側のパケット損失数を表示します。

  - [**入力パケットエラー率**]ウィジェット

    ネットワークインターフェイスの入力側のパケットエラー率を表示します。

  - [**入力パケットエラー数**]ウィジェット

    ネットワークインターフェイスの入力側のパケットエラー数を表示します。

  - [**出力パケットエラー率**]ウィジェット

    ネットワークインターフェイスの出力側のパケットエラー率を表示します。

  - [**出力パケットエラー数**]ウィジェット

    ネットワークインターフェイスの出力側のパケットエラー数を表示します。

- 任意のデータ種別のウィジェット

  NetvisorPro で任意のデータ種別を設定している場合は、それに応じたデータを表示します。

ヒント

NetvisorPro にて、各ウィジェットに該当するデータ収集機能の取集エントリでしきい値監視を設定している場合には、しきい値を表す線がグラフに表示されます。

しきい値の線は、上限のしきい値が赤、下限のしきい値が青で表示されます。

⚠ 注意

SNMP データ、および、フローデータの各ウィジェットにおいては、NetvisorPro、および、NFA 側でデータを収集する設定を行っていない場合、非表示となります。

4.4.6　ネットワークインターフェイスの過去の状態を確認する

ネットワークインターフェイス詳細画面を利用して、特定のネットワークインターフェイスの過去の状態を調査する方法を説明します。

ネットワークインターフェイス詳細画面では、[**期間**]に過去の期間を指定することで、ネットワークインターフェイスの過去の状態を各ウィジェットで確認することができます。

ここでは、昨夜の「23：00」頃に「スイッチ 01」で発生したイベントを起点に、「GigabitEthernet1/0/1」の当時の状態を調べる例を用いて、具体的な操作手順について説明します。

1. イベント画面を表示します。

   [**イベント**] メニューをクリックします。

2. 障害調査対象のノードを検索します。

   a. プルダウンメニューから [**発生元名**] を選択します。

   b. 照合方法として、[**は次と等しい**]を選択します。

   c. 調査対象のノード名を入力します。

      ここでは、「スイッチ 01」と入力します。

   d. [**検索**]ボタンをクリックします。

   イベント画面に、「スイッチ 01」で発生したイベントが一覧表示されます。

3. イベントの内容を確認します。

   例えば、昨夜の「23：00」頃に「入力インターフェイス使用率のしきい値超過」のイベントが発生していたとします。以降の手順では、「入力インターフェイス使用率のしきい値超過」のイベントの調査について説明していきます。

4. イベントの発生元であるノードに対するノード詳細画面を表示します。

[**発生元名**]欄のノード名のリンクをクリックします。

ここでは、「スイッチ 01」のリンクをクリックします。

リンクをクリックすると、「スイッチ 01」に対するノード詳細画面が表示されます。また、[**期間**]には、「入力インターフェイス使用率のしきい値超過」のイベントが発生した昨夜の「23：00」を含む過去の期間が設定されます。

5. 指定期間でのノードの状態を確認します。

   [**入力インターフェイス使用率**]ウィジェットから、しきい値超過したネットワークインターフェイス名とそのしきい値超過発生前後の挙動を確認することができます。また、[**CPU 使用率**]ウィジェットや[**メモリ使用率**]ウィジェットから、ネットワークインターフェイス負荷に関連した異常が発生していないかの確認を行うことができます。

6. 問題のあるネットワークインターフェイスのネットワークインターフェイス詳細画面を表示します。

   [**入力インターフェイス使用率**]ウィジェットのネットワークインターフェイス名のリンクをクリックします。

   ここでは、ランキング 1 位となっている「GigabitEthernet1/0/1」のリンクをクリックします。

   「GigabitEthernet1/0/1」に対するネットワークインターフェイス詳細画面が表示されます。ネットワークインターフェイス詳細画面の[**期間**]には、ノード詳細画面で設定されていた内容が、そのまま引き継がれます。

7. 指定期間でのネットワークインターフェイスの状態を確認します。

   「GigabitEthernet1/0/1」の入力側の使用率だけではなく、それに関連して、パケット損失やエラーが発生していないかを[**入力パケット損失率**]ウィジェットや[**入力パケットエラー率**]ウィジェットから確認することができます。

   NFA を利用している場合は、[**アプリケーション**]ウィジェットからネットワークインターフェイスの負荷を高めているアプリケーション通信の内容を調査することができます。また、[**カンバセーション**]ウィジェットからは、どの IP アドレス間での通信が多いのかを確認することができます。

さらに詳細な通信フロー内容の調査が必要な場合は、ネットワークインターフェイス詳細画面の[**フロー分析**]ボタンをクリックすることで、NFA のエクスポーター分析画面を簡単に表示することができます。

4.5　データ分析の結果を確認する

データ分析の結果を確認する手順について説明します。

4.5.1　アノマリーの発生状況を確認する

分析対象のアノマリー発生状況を確認する手順について説明します。

アノマリー分析画面を操作することで、分析対象のデータ挙動の状態を詳細に確認することができます。

ヒント

本分析結果からは、分析対象のデータ挙動が普段と異なっていることを検知、確認することができますが、必ずしもシステム障害に関係しているものとは限りません。普段とは異なるシステムのメンテナンスやオペレーションを行った場合もアノマリーを検知する場合があります。分析結果を元に、関連したシステムの運用内容の確認を実施し、問題有無を確認してください。

1. データ分析画面を表示します。

   [**データ分析**] メニューをクリックします。

2. 分析対象の[**アノマリー分析**]アイコンをクリックします。

   アノマリー分析画面が表示されます。

3. アノマリーの発生状況を確認します。

   a. 分析範囲の期間を選択します。

      画面右上の[**期間**]をクリックし、表示されたダイアログから分析範囲の期間を指定します。期間の指定には、以下の 2 つの方法があります。

      - [**既定の期間から選択**] (デフォルト値)

        プルダウンメニュー([**過去 1 時間**]、[**過去 6 時間**]、[**過去 1 日**]、[**過去 2 日**]、[**過去 3 日**]、[**過去 7 日**]、[**過去 30 日**])から分析期間を選択します。デフォルト値は、[**過去 7 日**]です。

      - [**特定の期間を指定**]

        グラフの開始日時となる[**起点日時**]とグラフの終了日時となる[**終点日時**]を指定します。

      ヒント

      [◀◀]および[▶▶]をクリックすると、現在の指定期間の幅を保ったまま、前後の期間のグラフを表示することができます。

      [▶|]をクリックすると、[**既定の期間から選択**]から、現在表示している期間幅に最も近いプルダウンメニューを選択し、現在時刻を含むグラフを表示します。

   b. 分析内容を確認します。

      - グラフ表示領域：

        グラフ表示領域には、指定期間の実測データと共に、分析モデルを元に算出した予測範囲のグラフが表示されます。

アノマリーを検知した場合は、アノマリーと判定されている区間が強調されて表示されます。また、スケジュール定義による[**除外期間**]を指定している場合は、その除外の区間もグラフ上に重ねて表示されます。

ヒント

ダッシュボード画面のウィジェットと同様に、[**レンジセレクター**]を操作することでグラフの表示をズームインすることができますが、アノマリー分析画面においては、グラフ表示領域で範囲指定するだけで、グラフの表示をズームインすることができます。また、グラフ表示領域をダブルクリックすることで、元の表示状態に戻すことができます。

- [**過去比較**]：

  [**期間**]で指定した期間よりも過去の期間を指定して、2 つの期間でのデータの挙動を比較表示します。

  - [**過去比較を行わない**] (デフォルト値)

    過去期間のデータとの比較表示は行いません。

  - [**比較対象データ： *<n> <日前\|週間前>***]

    [**期間**]で指定したデータに対し、どれくらい前のデータと比較するのかを指定します。

  - [**比較対象データの起点日： *<yyyy-mm-dd>***]

    比較対象とするデータの期間を具体的な起点の日付で指定します。おおよその周期性が 1 週間の分析対象については、[**期間**]で指定した起点日と同じ曜日になるよう比較対象データの起点日を指定してください。

  [**更新**]ボタンをクリックすると、グラフ表示領域に比較対象のグラフが表示されます。

  ヒント

  [**過去比較**]は、分析ポリシーを適用する前に、登録した分析対象の周期性を確認する際にも活用できます。例えば、1 週間前のデータ挙動を重ねて表示させることで、1 週間でのおおよその周期性がみられるかが確認できます。

- [**分析対象**]：

  分析対象の詳細情報を表示します。[**分析対象**]をクリックすることで、表示の開閉操作を行うことができます。

- [**分析ポリシー**]：

  アノマリー分析に用いた分析ポリシーの内容を表示します。[**分析ポリシー**]をクリックすることで、表示の開閉操作を行うことができます。[**除外期間**]には、[**期間**]で指定した期間に該当するスケジュール情報のみが表示されます。

4.5.2　トレンドラインを確認する

分析対象のトレンドラインの状況を確認する手順について説明します。

トレンドライン分析画面を操作することで、現在までに収集したデータから、将来のデータの増減傾向について確認することができます。

本分析結果は、リソースのキャパシティ管理を行う際の指標として活 用することができます。

1. データ分析画面を表示します。

   [**データ分析**] メニューをクリックします。

2. 分析対象の[**トレンドライン分析**]アイコンをクリックします。

   トレンドライン分析画面が表示されます。

3. トレンドラインの状況を確認します。

   a. 分析範囲の期間を選択します。

      画面右上の[**期間**]のプルダウンメニューから、分析範囲の期間として以下のいずれかを選択します。

      デフォルト値は、[**現在時刻の前後 30 日**]です。

      - [**現在時刻の前後 1 時間**]
      - [**現在時刻の前後 6 時間**]
      - [**現在時刻の前後 1 日**]
      - [**現在時刻の前後 2 日**]
      - [**現在時刻の前後 3 日**]
      - [**現在時刻の前後 7 日**]
      - [**現在時刻の前後 30 日**]
      - [**現在時刻の前後 90 日**]
      - [**現在時刻の前後 360 日**]

   b. 分析内容を確認します。

      - グラフ表示領域：

        指定期間における現在までの実測データのグラフの表示と共に、表示されている実測データから算出したトレンドラインのグラフを表示します。

      - [**分析対象**]：

        分析対象の詳細情報を表示します。[**分析対象**]をクリックすることで、表示の開閉操作を行うことができます。

4.6　イベントアクションの実行状況を確認する

イベントアクションの実行結果は、すべてアクションログとして記録します。ここでは、アクションログの確認方法について説明します。

アクションログの内容を確認することで、定義したイベントアクションが、適切に実行されていることや、実行したイベントアクションの中で呼び出した処理が、正しく完了できていたのかを確認することができます。

4.6.1　アクションログ一覧画面

アクションログ画面について説明します。

アクションログ画面では、イベントアクションの定義に従ったアクションの実行状況を確認することができます。

アクションログ画面は、[**イベントアクション設定**] >[**アクションログ**] メニューをクリックして表示します。

図 4-13　アクションログ画面

画面操作領域

- [**最終更新時刻**]

  画面更新を実施した日時を表示します。

- [**更新**]アイコン

  画面表示を最新の内容に更新します。

- [**更新間隔**]

  画面表示の更新間隔をプルダウンメニュー([**1 分**]、[**5 分**]、[**15 分**]、[**なし**])から選択します。デフォルト値は、[**1 分**]です。

検索条件の指定

アクションログ一覧で表示する各項目の内容に対し、条件を指定して、表示するアクションログの情報を絞り込むことができます。

- 条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。

  追加した条件の先頭に表示する[ー]アイコンをクリックすると追加した条件を取り消すことができます。

- 条件指定

  アクションログ一覧で表示する各項目に対し、以下の 3 つの方法で、検索条件を指定します。検索条件の指定方法は、選択した項目ごとに異なります。

  - チェックボックスによる指定

    チェックボックスを用いて、検索条件を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**結果**]

  - キーワードの指定

    選択した項目に対して、キーワードと照合方法を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**イベントアクション名**]、[**アクション概要**]

    照合方法については、以下を指定することができます。

    * 照合方法：

      [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

  - 時刻の範囲指定

    選択した項目に対して、*YYYY-MM-DD hh:mm* の形式で時間範囲を指定します。対象項目は以下の通りです。

    * 対象項目：

      [**アクション開始時刻**]、[**アクション終了時刻**]

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

条件を指定した後、[**検索**]ボタンをクリックすると、検索条件に合致したアクションログの一覧が表示されます。

アクションログ一覧

- [**結果**]

  イベントアクションの実行結果(成功、失敗)を表示します。

  ヒント

  イベントアクションでコマンド実行を行った場合は、戻り値が「0」の場合に、「成功」と判断し、それ以外の場合は、「失敗」と判断します。

- [**アクション開始時刻**]

  イベントアクションの処理を開始した日時を表示します。

- [**アクション終了時刻**]

  イベントアクションの処理を終了した日時を表示します。

- [**イベントアクション名**]

  実行したイベントアクションの定義名を表示します。イベントアクション名のリンクをクリックすると、イベントアクション編集画面が表示され、当該イベントアクション定義の修正を行うことができます。

- [**アクション概要**]

  イベントアクションの実行状況の概要を表示します。

- [**操作**]

  各アイコンをクリックすることで、実行したイベントアクションに関連する詳細情報を表示します。

  - [**アクションログ詳細**]アイコン

    イベントアクションから呼び出したアクションの処理内容を示すアクションログ詳細ダイアログを表示します。

  - [**イベント詳細**]アイコン

    イベントアクションの実行契機となったイベントに対するイベント詳細ダイアログを表示します。

1 ページに表示するアクションログの件数は、プルダウンメニュー([**50**]、[**100**]、[**250**])から選択します。デフォルト値は、[**100**]です。

検索条件に合致したすべてのアクションログの情報を 1 ページで表示できない場合は、ページを切り替えて、アクションログの情報を確認します。

ヒント

保持できるアクションログの最大件数は、10,000 件です。10,000 件を超えると、最も古いアクションログを削除し、新しいアクションログを保持していきます。

4.6.2　アクションログ詳細ダイアログ

アクションログ詳細ダイアログについて説明します。

アクションログ詳細ダイアログでは、イベントアクションから呼び出したアクションの処理内容を示す詳細なログを確認することができます。

アクションログ詳細ダイアログは、アクションログ画面の[**アクションログ詳細**]アイコンをクリックして表示します。アクションログ画面は、[**イベントアクション設定**] >[**アクションログ**] メニューをクリックして表示します。

図 4-14　アクションログ詳細ダイアログ

- [**アクション概要**]

  イベントアクションの実行状況の概要を表示します。

- [**アクション開始時刻**]

  イベントアクションの処理を開始した日時を表示します。

- [**アクション終了時刻**]

  イベントアクションの処理を終了した日時を表示します。

- [**結果**]

  イベントアクションの実行結果(成功、失敗)を表示します。

  ヒント

  イベントアクションでコマンド実行を行った場合は、戻り値が「0」の場合に、「成功」と判断し、それ以外の場合は、「失敗」と判断します。

- [**イベントアクション名**]

  実行したイベントアクションの定義名を表示します。

- [**アクション名**]

  イベントアクションで定義している実行したアクション名を表示します。

- [**アクション詳細**]

コマンド実行の場合は、標準出力や標準エラーの内容を表示し、メール通報の場合は、エラー発生時に出力されたログ情報などが表示されます。

4.6.3　イベントアクションの実行結果を詳細に確認する

イベントアクションの実行結果を詳細に確認する手順について説明します。

イベントアクションの[**結果**]が、[**失敗**]だった場合に、アクションログの詳細情報を確認することで、アクションの実行状況を調査できる場合があります。

ここでは、イベントアクション名「接点出力コマンドの実行」の実行内容を確認する操作例を用いて、具体的な操作手順を説明します。

1. アクションログ画面を表示します。

   [**イベントアクション設定**] >[**アクションログ**] メニューをクリックします。

2. 調査対象のアクションログを検索します。

   a. プルダウンメニューから [**イベントアクション名**] を選択します。

   b. 照合方法として、[**は次と等しい**]を選択します。

   c. 調査対象のイベントアクション名を入力します。

      ここでは、「接点出力コマンドの実行」と入力します。

   d. [**検索**]ボタンをクリックします。

   アクションログ一覧に、「接点出力コマンドの実行」に対するアクションログが表示されます。

3. アクションの実行内容を確認します。

   [**結果**]が[**失敗**]となっているアクションログに対する[**アクションログ詳細**]アイコンをクリックします。

   アクションログ詳細ダイアログが表示されます。

4. アクションログの詳細内容を確認します。

   [**アクション詳細**]には、実行したコマンドの標準出力、および、標準エラーの内容が記録されています。

   ここでは、呼び出した「接点出力コマンド」の標準出力、標準エラーの内容とコマンド仕様を照らし合わせて、失敗原因を調査します。

4.7　ユーザーの操作履歴を確認する

Web コンソールでは、各ユーザーのログインや操作の状況を証跡ログとして記録しています。

証跡ログを活用することで、意図せず設定が変更されていた場合に、誰がいつ変更したのかを追跡調査することができます。

証跡ログは、IMS コンポーネントをインストールしたサーバーの以下のパスにテキストファイルとして出力されます。また、証跡ログは、以下のファイル名で、日ごとに記録するファイルが切り替わります。

出力パス

<%***データパス***%>\auditlog\

ファイル名

audit_log.*YYYY-MM-DD*.txt

証跡ログの詳細なフォーマットについては、「証跡ログフォーマット（176 ページ）」を参照してください。

証跡ログファイルの保持期間のデフォルト値は、3 年間(1095 日間)となっています。保持期間の変更方法については、「5.2.8　証跡ログの保持期間を変更する（201 ページ）」を参照してください。

ヒント

証跡ログファイルは、任意のテキストエディターを用いて参照することができます。

証跡ログフォーマット

証跡ログは、以下のフォーマットで、1 操作に対し 1 行で記録されます。

```
<操作日時>\t<操作>\t<結果>\t<ユーザー名>\t<本文>
```

\t : タブ文字を示します。

<操作日時>

操作を行った日時を示します。以下の形式となります。

- YYYY-MM-DD HH:mm:ss.SSS

<操作>

操作の種類を示します。以下のいずれかとなります。

- 追加
- 編集
- 削除
- 情報

<結果>

操作の結果を示します。以下のいずれかとなります。

- 成功
- 失敗

<ユーザー名>

操作を行ったユーザー名を示します。

システムの動作によるログやログインの失敗などでユーザー名が特定できなかった場合のログでは、「(none)」となります。

<本文>

操作の具体的な内容を示します。

以下に証跡ログの出力例を示します。

```
2021-09-02 17:49:20.002　追加　成功　admin　ダッシュボードを追加しました。（ダッシュボード名=全体管理ダッシュボード）
```

第 5 章
システムメンテナンス

Web コンソールの利用環境に対するメンテナンス方法について説明します。

目次

5.1　ノードの管理情報のマッピング状況を管理する

1 つのリージョングループに複数の製品を登録している場合、各製品での管理対象ノードが、物理的に同一のノードかどうかを自動判定し、IMS コンポーネントに登録しています。ここでは、同一ノードの判定結果の確認方法や処理の不正が見つかった場合の修正方法について説明します。

5.1.1　ノード情報のマッピング

同一ノードかどうかの判定処理は、同一リージョングループに属する各製品の管理対象ノードに対し行います。ここでは、同一ノードの判定処理の詳細について説明します。

1 つのリージョングループに複数の製品を登録している場合は、各製品で管理する以下のノード情報を用いて、各製品で管理するノードが同一のノードかどうかを判定して、IMS コンポーネントに登録します。

- ノードの IP アドレス(IPv4 アドレス、および、IPv6 アドレス)
- ノードの MIB から取得した sysName(1.3.6.1.2.1.1.5)の値

例えば、「図 5-1 同一ノードの判定処理（179 ページ）」に示すように、NetvisorPro と NFA とで、同一のノードを管理している場合、各製品の管理情報から IP アドレス、sysName の値を確認し、同一ノードとして、IMS コンポーネントに登録します。

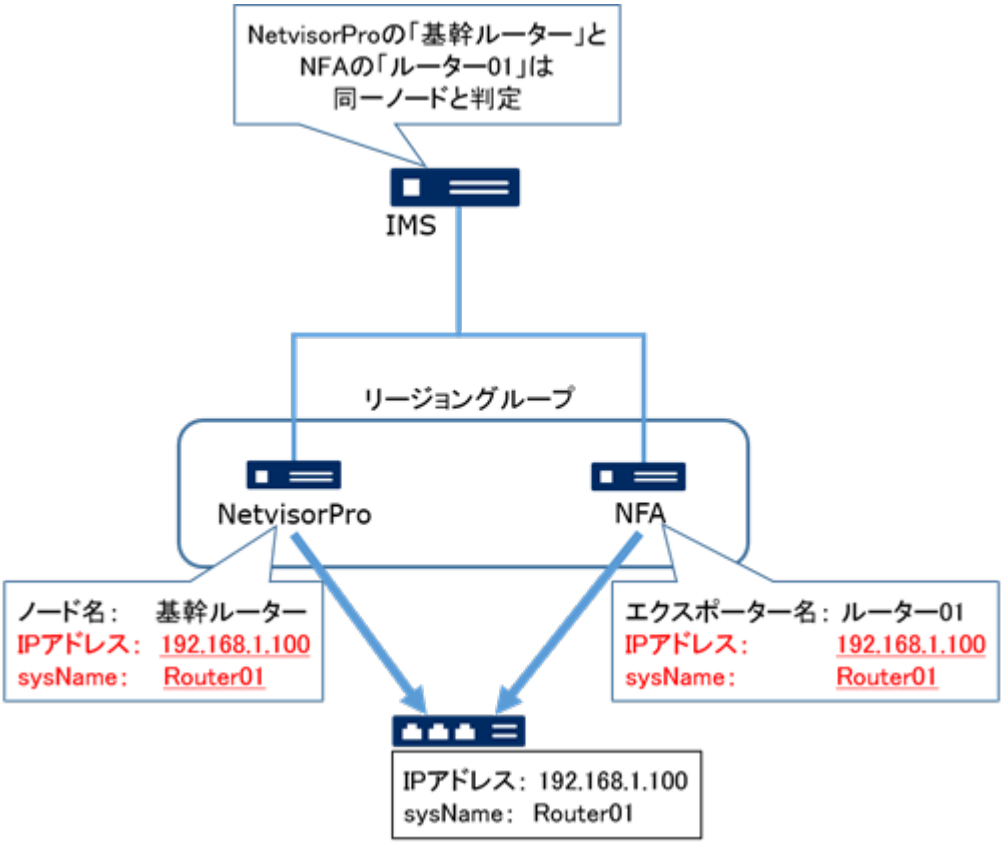

図 5-1　同一ノードの判定処理

ヒント

同一ノードと判定した場合、IMS コンポーネントには、1 つのノードとして情報を統合して登録します。この時、「図 5-1 同一ノードの判定処理（179 ページ）」に示したように、NetvisorPro と NFA とでノード名が異なっている場合は、NetvisorPro でのノード名(「基幹ルーター」)を採用し、IMS コンポーネントに登録します。

同一ノードの判定結果については、ノードマッピング画面で確認することができます。同一ノードの判定結果が不正な場合は、ノードマッピング画面から正しく修正することができます。

5.1.1.1　ノードマッピング画面

ノードマッピング画面について説明します。

ノードマッピング画面では、複数製品で管理するノードに対する同一ノードの判定結果の確認、および、修正操作を行うことができます。

ノードマッピング画面は、[**システム設定**] >[**ノードマッピング**] メニューをクリックして表示します。

ヒント

- アドミニストレーターの役割を持つグループのユーザーのみ、ノードマッピング画面を表示することができます。
- 同一リージョングループに複数製品を登録して運用していない場合は、本画面の操作は不要です。

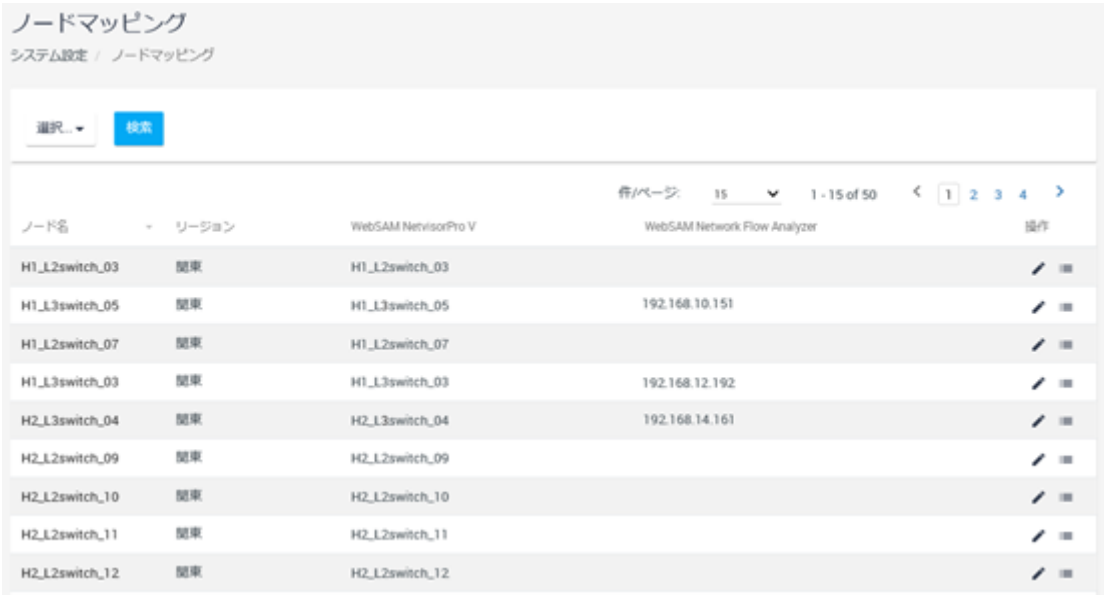

図 5-2　ノードマッピング画面

検索条件の指定

ノードマッピング一覧で表示する各項目の内容に対し、条件を指定して、表示するノードの情報を絞り込むことができます。

- 条件追加と解除

  [**選択...**]ボタンのプルダウンメニューから新しい条件を追加することができます。

  追加した条件の先頭に表示する[ー]アイコンをクリックすると追加した条件を取り消すことができます。

- 条件指定

  ノードマッピング一覧で表示する各項目に対し、キーワードと照合方法を指定します。

  - 対象項目：

    [**ノード名**]、[**リージョン**]、[**<*製品名*>:ノード名**]

  - 照合方法：

    [**は次と等しい**](一致)、[**は次と異なる**](不一致)、[**は次を含む**](含む)、[**は次を含まない**](含まない)、[**は次で始まる**](前方一致)、[**は次で終わる**](後方一致)

ヒント

異なる項目の条件を追加した場合は、AND 条件として設定し、同じ項目に対し複数の条件を指定した場合は、OR 条件として設定します。

条件を指定した後、[**検索**]ボタンをクリックすると、検索条件に合致したノードのマッピング情報の一覧が表示されます。

⚠ 注意

[**<*製品名*>:ノード名**]に対する検索においては、指定した製品(<*製品名*>)で管理するノードの中から条件に合致するものを表示します。指定した製品(<*製品名*>)で管理していないノードの情報は、検索結果としては表示されません。

ノードマッピング一覧

- [**ノード名**]

  Web コンソールでのノード名を表示します。

- [**リージョン**]

  ノードが属するリージョングループの名前を表示します。

- [**<*製品名*>**]

  各製品でのノード名を表示します。NetvisorPro で管理するノード名は、[**WebSAM NetvisorPro V**]欄に、NFA で管理するノード名は、[**WebSAM Network Flow Analyzer**]欄に表示します。

- [**操作**]

  各アイコンをクリックすることで、ノードのマッピング情報に対応する操作画面を表示します。

  - [**編集**]アイコン

    同一ノードの判定内容を修正します。[**編集**]アイコンをクリックすると、ノードマッピング編集画面が表示されます。詳細は、「5.1.1.2　ノードのマッピング状況を変更する（182 ページ）」を参照してください。

  - [**ネットワークインターフェイスマッピング**]アイコン

    ノードが保持するネットワークインターフェイスの同一判定結果を表示します。

    [**ネットワークインターフェイスマッピング**]アイコンをクリックすると、ネットワークインターフェイスマッピング画面が表示されます。詳細は、「5.1.2.1　ネットワークインターフェイスマッピング画面（184 ページ）」を参照してください。

1 ページに表示するノードのマッピング情報の件数は、プルダウンメニュー([**15**]、[**50**]、[**100**])から選択します。デフォルト値は、[**15**]件です。

検索条件に合致したすべてのノードのマッピング情報を 1 ページで表示できない場合は、ページを切り替えて、ノードのマッピング情報を確認します。

5.1.1.2　ノードのマッピング状況を変更する

Web コンソールで表示するノード情報において、同一ノードの判定結果を修正する手順について説明します。

同一ノードかどうかの判定処理が誤っていた場合は、手動で正しい状態に修正する必要があります。

ここでは、物理的に同一のノードが、誤って異なるノードと判定されてしまった場合の操作例を用いて、具体的な操作手順を説明します。

⚠ 注意

ノードのマッピングを更新する前に、当該ノードにおいてイベントが発生していた場合、マッピングの更新操作後も、当該イベントの発生元情報は、変化しません。そのため、以下のような状況になる場合があります。

- マッピング済みのノードを分離する操作を行った場合:

  イベント発生を検知したはずのノードであっても、IMS コンポーネントで管理するノード名が変わってしまうと、もう一方の名前が変わっていないノードの方で当該イベントが発生したこととして処理される。

- 手動でマッピングを行い 1 つのノードにした場合:

  イベント発生を検知したノードのノード名が、マッピング操作によって変わってしまうと、マッピングされたノードには結びつかないイベントとして処理される。

ノードのマッピング状況を変更する場合は、上記の仕様を元に、イベントの発生元を適切に読み替えて、対応を実施してください。

1. ノードマッピング画面を表示します。

   [**システム設定**] >[**ノードマッピング**] メニューをクリックします。

2. 更新対象のノードを検索します。

   a. プルダウンメニューから[**リージョン**]を選択します。

   b. 照合方法として、[**は次と等しい**]を選択します。

   c. 更新対象のノードが所属するリージョングループ名を入力します。

   d. プルダウンメニューから[**ノード名**]を選択します。

   e. 照合方法として、[**は次と等しい**]を選択します。

   f. 更新対象のノード名を入力します。

   g. [**検索**]ボタンをクリックします。

   検索結果が、ノードマッピング一覧に表示されます。

3. 更新対象のノード名の[**編集**]アイコンをクリックします。

   当該ノードに対するノードマッピング編集画面が表示されます。

4. ノードのマッピング情報を更新します。

   各製品のノード情報に対する以下のボタンを操作して、マッピング情報を更新します。

   - [**編集**]アイコン

     ノード選択の画面が表示されます。ノード選択の画面には、当該ノードが所属するリージョングループ内の選択製品が管理するノードの情報が一覧で表示されます。ノード選択の画面で、変更後のノードを選択し、[**OK**]ボタンをクリックすると、ノードマッピング編集画面に選択したノードの情報が反映されます。

   - [**削除**]アイコン

     ノードのマッピング状況を解除します。

   ここでは、誤って異なるノードとして判定されてしまったノードを、ノード選択の画面から選択します。

   ノードマッピング編集画面において、当該ノードのマッピング関係が修正されます。

5. ノードマッピングの変更内容を登録します。

   変更内容を確認し、ノードマッピング編集画面の[**OK**]ボタンをクリックします。

   ノードマッピング画面に更新した内容が反映されます。

5.1.2　ネットワークインターフェイスのマッピング

同一ノードの判定を行い、複数製品で管理するノードの情報を統合して IMS コンポーネントに登録する際に、ネットワークインターフェイスの情報も同一のものかどうかを判断して登録します。

ネットワークインターフェイスに関しては、各製品が当該ノードの MIB から取得した ifIndex(1.3.6.1.2.1.2.2.1.1)の値を元に、同一のネットワークインターフェイスかどうかを判定し、登録します。

同一ネットワークインターフェイスの判定結果については、ネットワークインターフェイスマッピング画面で確認することができます。同一ネットワークインターフェイスの判定結果が不正な場合は、ネットワークインターフェイスマッピング画面から正しく修正することができます。

ヒント

- 基本的に、ネットワークインターフェイス名と ifIndex 値は 1 対 1 で対応しているため、同一ノードの判定結果が誤っていない限り、ネットワークインターフェイスの同一化処理が誤ることはありません。

  ただし、装置仕様によっては、装置の再起動で ifIndex 値が変化する場合があり、各製品の監視処理を含め、ネットワークインターフェイスの管理に大きな影響を与えます。このような仕様の装置に対しては、ifIndex を固定化 (持続)するための設定を必ず行ってください。
- NFA では、LAG(Link Aggregation Group)の仕組みで論理的に束ねたネットワークインターフェイスから直接、フロー情報を送信する設定ができない機種の管理に対応するため、複数の物理的なネットワークインターフェイスを NFA 側で、グルーピングして、フロー情報を集計する仕組みを提供しています。NFA では、グルーピングしたネットワークインターフェイスに対して、ifIndex 値の管理を行っていないため、NetvisorPro 側で LAG インターフェイスの ifIndex 値を取得している場合に、同一ネットワークインターフェイスとしての判定が行えません。このような場合は、本機能を利用して、手動で同一ネットワークインターフェイスとしての登録を行います。

5.1.2.1　ネットワークインターフェイスマッピング画面

ネットワークインターフェイスマッピング画面について説明します。

ネットワークインターフェイスマッピング画面では、複数製品で管理するノードに対する同一ノード判定後に実施する同一ネットワークインターフェイスの判定結果の確認、および、修正操作を行うことができます。

ネットワークインターフェイスマッピング画面は、ノードマッピング画面のノードに対する[**ネットワークインターフェイスマッピング**]アイコンをクリックして表示します。ノードマッピング画面は、[**システム設定**] >[**ノードマッピング**] メニューをクリックして表示します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、ネットワークインターフェイスマッピング画面を表示することができます。

図 5-3　ネットワークインターフェイスマッピング画面

ネットワークインターフェイスマッピング一覧

- [**インターフェイス名**]

  IMS に登録されているネットワークインターフェイス名を表示します。

- [***<製品名>　<ノード名>***]

  各製品で管理するノードに対するネットワークインターフェイス名を表示します。列の項目名は、製品名と、その製品におけるノード名になります。

- [**操作**]

  アイコンをクリックすることで、ネットワークインターフェイスのマッピング情報に対応する操作画面を表示します。

  - [**編集**]アイコン

    同一ネットワークインターフェイスの判定内容を修正します。[**編集**]アイコンをクリックすると、ネットワークインターフェイスマッピング編集画面が表示されます。詳細は、「5.1.2.2　ネットワークインターフェイスのマッピングを変更する（186 ページ）」を参照してください。

1 ページに表示するネットワークインターフェイスのマッピング情報の件数は、プルダウンメニュー([**15**]、[**50**]、[**100**])から選択します。デフォルト値は、[**15**]件です。

すべてのネットワークインターフェイスのマッピング情報を 1 ページで表示できない場合は、ページを切り替えて、ネットワークインターフェイスのマッピング情報を確認します。

5.1.2.2　ネットワークインターフェイスのマッピングを変更する

Web コンソールで表示するネットワークインターフェイス情報において、同一ネットワークインターフェイスの判定結果を修正する手順について説明します。

同一ネットワークインターフェイスかどうかの判定処理が誤っていた場合は、手動で正しい状態に修正する必要があります。

ここでは、NFA で、グルーピングしたネットワークインターフェイスの情報と、NetvisorPro で、LAG(Link Aggregation Group)インターフェイスとして管理するネットワークインターフェイスを同一ネットワークインターフェイスとして登録する操作例を用いて、具体的な操作手順を説明します。

1. ノードマッピング画面を表示します。

   [**システム設定**] >[**ノードマッピング**] メニューをクリックします。

2. 更新対象のネットワークインターフェイスを保持するノードを検索します。

   a. プルダウンメニューから[**リージョン**]を選択します。

   b. 照合方法として、[**は次と等しい**]を選択します。

   c. 更新対象のノードが所属するリージョングループ名を入力します。

   d. プルダウンメニューから[**ノード名**]を選択します。

   e. 照合方法として、[**は次と等しい**]を選択します。

   f. 更新対象のノード名を入力します。

   g. [**検索**]ボタンをクリックします。

   検索結果が、ノードマッピング一覧に表示されます。

3. 更新対象のネットワークインターフェイスを保持するノード名の[**ネットワークインターフェイスマッピング**]アイコンをクリックします。

   当該ノードに対するネットワークインターフェイスマッピング画面が表示されます。

4. 更新対象のネットワークインターフェイスに対するネットワークインターフェイスマッピング編集画面を表示します。

   NFA でグルーピングしたネットワークインターフェイスの[**編集**]アイコン、または、NetvisorPro で、LAG(Link Aggregation Group)インターフェイスとして管理するネットワークインターフェイスの[**編集**]アイコンをクリックします。

   ここでは、NFA でグルーピングしたネットワークインターフェイスの[**編集**]アイコンをクリックします。

NFA でグルーピングしたネットワークインターフェイスに対するネットワークインターフェイスマッピング編集画面が表示されます。

5. ネットワークインターフェイスのマッピング情報を更新します。

   各製品のネットワークインターフェイス情報に対する以下のボタンを操作して、マッピング情報を更新します。

   - [**編集**]アイコン

     ネットワークインターフェイス選択の画面が表示されます。ネットワークインターフェイス選択の画面には、選択製品が管理する当該ノードのネットワークインターフェイス情報が一覧で表示されます。ネットワークインターフェイス選択の画面で、変更後のネットワークインターフェイスを選択し、[**OK**]ボタンをクリックすると、ネットワークインターフェイスマッピング編集画面に選択したネットワークインターフェイスの情報が反映されます。

   - [**削除**]アイコン

     ネットワークインターフェイスのマッピング状況を解除します。

   ここでは、NetvisorPro が管理するネットワークインターフェイス情報に対する[**編集**]アイコンをクリックします。表示されたネットワークインターフェイス選択の画面から、対応する LAG(Link Aggregation Group)インターフェイスとして管理しているネットワークインターフェイスを選択します。

   NFA でグルーピングしたネットワークインターフェイスと NetvisorPro で、LAG(Link Aggregation Group)インターフェイスとして管理するネットワークインターフェイスが同一ネットワークインターフェイスとして、ネットワークインターフェイスマッピング編集画面に設定されます。

6. ネットワークインターフェイスマッピングの変更内容を登録します。

   変更内容を確認し、ネットワークインターフェイスマッピング編集画面の[**OK**]ボタンをクリックします。

   ネットワークインターフェイスマッピング画面に更新した内容が反映されます。

5.2　システムの環境をメンテナンスする

システム環境をメンテナンスする手順について説明します。

5.2.1　関連コンポーネントのバージョン情報を確認する

IMS コンポーネント、および、各製品の連携プラグインモジュールのバージョン情報を確認する手順について説明します。

Web コンソールの動作に関して、NEC カスタマーサポートセンターに問い合わせを行う場合や、NEC カスタマーサポートセンターから入手したアップデートモジュールを適用する場合に、運用中の IMS コンポーネントや組み込んでいる各製品のアプリケーションの正確なバージョン情報を確認する必要があります。

IMS コンポーネントのバージョンについては、Web コンソールから確認する方法と、コマンドから確認する方法があります。組み込んでいる各製品のアプリケーションについてのバージョンは、コマンドからのみ確認することができます。

- IMS コンポーネントのバージョンを Web コンソールから確認する
  1. Web コンソールにログインします。
  2. 画面のフッター領域のバージョン情報を確認します。

     表示形式は以下の通りです。

     WebSAM Integrated Management Server <バージョン番号>.<リビジョン番号>.<ビルド番号>
- IMS コンポーネント、および、アプリケーションのバージョンをコマンドから確認する
  1. IMS コンポーネントをインストールしているサーバーにログインします。
  2. Windows 環境の場合、コマンドプロンプトを起動します。
  3. カレントディレクトリを移動します。

     ```
     > cd <%インストールパス%>/bin
     ```
  4. バージョン確認のコマンドを実行します。

     ```
     > ims-app list
     ```
  5. 表示結果からバージョン情報を確認します。

     表示形式は以下の通りです。

     ```
     WebSAM Integrated Management Server version 4.0.0.1

       ID  | Application Name              | Version
       ------------------------------------------------
       nvp | WebSAM NetvisorPro V          | 4.0.0.1
       nfa | WebSAM Network Flow Analyzer | 4.0.0.1
     ```

5.2.2　サービスを起動、停止する

IMS コンポーネントのサービスを手動で起動、停止する手順について説明します。

IMS コンポーネントのサービスは、OS の起動、停止に連動して、自動で起動、停止します。

IMS コンポーネントのメンテナンスのため、OS を起動したまま、IMS コンポーネントのサービスのみを停止したり、再び起動したい場合は、以下の手順を実施します。

⚠ 注意

サービス起動前に、設定ファイルや証跡ログファイルなどにおいて、ファイルロックが発生していないことを確認してください。ファイルロックが発生した状態でサービス起動を行うと、Web コンソールへアクセスできない状態になる場合があります。

Windows 環境の場合

Windows OS の[**管理ツール**]を用いて、サービスの制御を行います。

1. コントロールパネル画面を開き、[**管理ツール**]を検索します。
2. 管理ツール画面の[**サービス**]を表示します。
3. 以下の操作を行います。
    - サービスを起動する場合、すべてのサービスが停止していることを確認してから、サービス画面のサービス一覧から、以下のサービスを順番に選択し、[**サービスの開始**]を実行します。
        a. WebSAM IMS Message Queue
        b. WebSAM IMS System Database
        c. WebSAM IMS TimeSeries Database
        d. WebSAM IMS Key Store
        e. WebSAM IMS Web Server
        f. WebSAM IMS Event Manager
    - サービスを停止する場合、サービス画面のサービス一覧から、以下のサービスを順番に選択し、 [**サービスの停止**]を実行します。
        a. WebSAM IMS Event Manager
        b. WebSAM IMS Web Server
        c. WebSAM IMS Key Store
        d. WebSAM IMS TimeSeries Database
        e. WebSAM IMS System Database
        f. WebSAM IMS Message Queue

Linux 環境の場合

IMS コンポーネントが提供する以下のコマンドを用いて、サービスの制御を行います。

- `systemctl {start | stop} nec-ims`

ヒント

本コマンドは、IMS コンポーネントをインストールしたサーバーに、root ユーザーでログインして実行する必要があります。

- サービスを起動する場合、引数 `start` を付けてコマンドを実行します。

  IMS の全てのデーモンプロセスの起動に成功すれば、コマンドは戻り値として 0 を返します。

```
# systemctl start nec-ims
```

- サービスを停止する場合、引数 `stop` を付けてコマンドを実行します。

  IMS の全てのデーモンプロセスの停止に成功すれば、コマンドは戻り値として 0 を返します。

```
# systemctl stop nec-ims
```

- 製品の提供する `ims-ctl` コマンドを、引数 `status` を付けて実行することで、サービスの状態を確認することができます。

```
# <%インストールパス%>/bin/ims-ctl status
```

  サービスが起動していれば、次のようなメッセージを表示します。また、コマンドは戻り値として 0 を返します。

```
message queue (pid 12341) is running...
systemdb (pid 12342) is running...
timeseriesdb (pid 12343) is running...
key store (pid 12344) is running...
web server (pid 12345) is running...
event manager (pid 12346) is running...
```

  サービスが停止していれば、次のようなメッセージを表示します。また、コマンドは戻り値として 3 を返します。

```
message queue is stopped
systemdb is stopped
timeseriesdb is stopped
key store is stopped
web server is stopped
event manager is stopped
```

5.2.3　利用する通信ポート番号を変更する

IMS コンポーネントが利用するポート番号を変更する手順を説明します。

IMS コンポーネントが利用するポート番号については、「D.1　利用するポート番号の一覧（230 ページ）」を参照してください。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

IMS コンポーネントが利用する各ポート番号の変更手順は、以下の通りです。

1. IMS コンポーネントをインストールしているサーバーにログインします。
2. IMS コンポーネントのサービスを停止します。
3. 変更したいポート番号に対する設定ファイルを変更し、上書きして保存します。

   設定ファイルと変更のための指定形式を「表 5-1 通信ポート番号の設定（191 ページ）」に示します。

表 5-1　通信ポート番号の設定

用途	指定形式

HTTP 通信	• 設定ファイル
	`<%データパス%>\conf\ims-conf.ini`
	• 指定形式
	`noms.tomcat.http.port = <ポート番号>`
	同ファイル内の以下の設定値を「true」にすることで、上記の設定が有効になります。
	「false」の場合は、通信ポートを開きません。
	`noms.tomcat.http.enabled = true`

HTTPS 通信	• 設定ファイル
	`<%データパス%>\conf\ims-conf.ini`
	• 指定形式
	`noms.tomcat.https.port = <ポート番号>`
	同ファイル内の以下の設定値を「true」にすることで、上記の設定が有効になります。
	「false」の場合は、通信ポートを開きません。
	`noms.tomcat.https.enabled = true`

Message Queue 通信	• 設定ファイル
	`<%データパス%>\conf\ims-conf.ini`
	• 指定形式
	以下の設定項目を追記し、ポート番号を指定します。
	`amqphub.amqp10jms.remote-url = amqps://localhost:<ポート番号>?transport.trustAll=true`
	IMS コンポーネントに接続する各製品においても、上記の設定変更したポート番号に合わせて設定変更する必要があります。
	NetvisorPro の場合
	• 設定ファイル
	`NetvisorPro の<%データパス%>\Manager\sg\NvPRO\NvPROIms.ini`
	• 指定形式

用途	指定形式
	[NOMS] MessageQueuePort=<*ポート番号*> 設定ファイルを更新する場合は、サービスの再起動が必要です。 NFA の場合 • 設定ファイル NFA の<%*データパス*%>/controller/conf/controller.properties • 指定形式 ims.msgqueue.port = <*ポート番号*> 設定ファイルを更新する場合は、サービスの再起動が必要です。
System Database 通信	• 設定ファイル <%*データパス*%>\conf\ims-conf.ini • 指定形式 以下の設定項目を追記し、ポート番号を指定します。 noms.tomcat.jndi.port = <*ポート番号*> 上記に合わせて、以下の設定ファイルの内容も更新します。 • 設定ファイル <%*データパス*%>\conf\systemdb-extra.conf • 指定形式 port = <*ポート番号*>
Key Store 通信	• 設定ファイル <%*データパス*%>\conf\ims-conf.ini • 指定形式 以下の設定項目を追記し、ポート番号を指定します。 spring.redis.port = <*ポート番号*> 上記に合わせて、以下の設定ファイルの内容も更新します。 • 設定ファイル <%*データパス*%>\conf\redis-extra.conf • 指定形式 port = <*ポート番号*>
TimeSeries Database 通信	• 設定ファイル <%*データパス*%>\conf\ims-conf.ini • 指定形式 以下の設定項目を追記し、ポート番号を指定します。 noms.timescale.datasource.port = <*ポート番号*> 上記に合わせて、以下の設定ファイルの内容も更新します。 • 設定ファイル <%*データパス*%>\conf\timescaledb-extra.conf • 指定形式 port = <*ポート番号*>

⚠ 注意

- 1 つの項目について 2 つ以上の設定ファイルが記載されているポートは、すべての設定ファイルを同時に編集し、同じ値を設定してください。関連する設定ファイル間でポート番号が異なると、正常に動作しません。
- パラメーターの末尾に不要なスペースが含まれている場合、末尾のスペースも含めてパラメーター値と判断するため、意図した通りの処理が行えません。

  設定ファイルの保存前に、パラメーター末尾に不要なスペースが含まれていないことを確認してください。

4. 必要に応じて、ファイアウォールの設定を見直します。

   特に外部通信用のポート番号は、ファイアウォールによってブロックされている場合が多いため、ポート番号変更の際には、ファイアウォールの設定が適切かどうかを確認してください。

5. IMS コンポーネントのサービスを起動します。

   サービスの起動後、ポート番号の変更内容が IMS コンポーネントに反映されます。

5.2.4　ドメイン名 (FQDN) を変更する

IMS コンポーネントをインストールするサーバーのドメイン名 (FQDN) を変更した場合に必要となる、環境設定の変更作業について説明します。

5.2.4.1　通報用の URL を変更する

IMS コンポーネントをインストールするサーバーのドメイン名 (FQDN) を変更した場合、通報用の URL 設定の内容を変更する必要があります。

イベントアクションによる通報においては、発生したイベントに対するイベント詳細画面の URL をメール本文などに記載することができます。記載する URL は、設定ファイル(ims-conf.ini)で指定した URL を元にしているため、IMS コンポーネントをインストールしているサーバーのドメイン名 (FQDN) を変更した場合は、それに合わせて設定ファイル(ims-conf.ini)の内容も変更する必要があります。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

1. IMS コンポーネントをインストールしているサーバーにログインします。
2. IMS コンポーネントのサービスを停止します。
3. 設定ファイルの内容を変更し、上書きして保存します。
   - 設定ファイル

     <%***データパス***%>\conf\ims-conf.ini

- 指定形式

```
noms.core.url.external-base-url = <URL>
```

例：

```
noms.core.url.external-base-url = http://ims.nec.com:8080/
```

4. IMS コンポーネントのサービスを起動します。

   サービスの起動後、URL の変更内容が IMS コンポーネントに反映されます。

5.2.4.2　SSL サーバー証明書のドメイン名 (CN) を変更する

HTTPS を用いて Web コンソールにアクセスしている環境においては、IMS コンポーネントをインストールするサーバーのドメイン名 (FQDN) を変更した場合、SSL サーバー証明書の更新作業が必要になります。

SSL サーバー証明書の中には、ドメイン名 (識別名の CN) が含まれており、IMS コンポーネントをインストールしているサーバーのドメイン名 (FQDN) に合わせて変更を行います。

ヒント

HTTP を用いて、Web コンソールにアクセスする環境の場合は、以下のような作業を行う必要はありません。

SSL サーバー証明書に関する操作は、製品が提供する `ims-ssl-keytool` コマンドを使用します。詳細は、「A.1　ims-ssl-keytool（205 ページ）」を参照してください。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

1. IMS コンポーネントをインストールしているサーバーにログインします。
2. 次のコマンドを実行し、出力されたメッセージの中から Owner 情報を確認します。

```
> <%インストールパス%>/bin/ims-ssl-keytool list -v
```

Windows での実行例:

```
> cd C:\Program Files\NEC\IMS\bin
> ims-ssl-keytool list -v | findstr Owner
Owner: CN=ims.nec.com, OU=IT Operation Division, O=NEC Corporation,
 L=Minato-ku, ST=Tokyo, C=JP
```

3. `ims-ssl-keytool selfcert` コマンドを`-dname`, `-dns` オプション付きで実行し、識別名を更新します。

```
> <%インストールパス%>/bin/ims-ssl-keytool selfcert -dname <dname>
 -dns <FQDN>
```

確認した Owner 情報のうち、ドメイン名に関係する CN の値を変更して実行します。

Windows での実行例:

```
> ims-ssl-keytool selfcert -dname "CN=new-ims.nec.com,
 OU=IT Operation Division, O=NEC Corporation, L=Minato-ku,
 ST=Tokyo, C=JP" -dns "new-ims.nec.com"
```

4. 公的な認証局に証明書を発行してもらっていた場合、証明書の再発行を依頼します。

   a. 次のコマンドを実行し、認証局に送付するための証明書署名要求 (CSR) をファイルに出力します。

   ```
   > <%インストールパス%>/bin/ims-ssl-keytool certreq -dns <FQDN>
    <filename>
   ```

   指定したファイルに、CSR の内容がテキストで出力されます。

   b. 証明書署名要求 (CSR) を認証局に提出します。

   ims-ssl-keytool certreq コマンドで出力した CSR ファイルの内容を、認証局に提出します。

   認証局は、CSR の内容を元に、証明書に署名し、返送します。署名済み証明書の返送には、認証局によっては数日かかる場合があります。

   c. 認証局から返送された署名済み証明書をインポートします。

   ims-ssl-keytool importcert コマンドを、-alias オプションは指定せずに実行します。

   ```
   > <%インストールパス%>/bin/ims-ssl-keytool importcert <filename>
   ```

   実行時に Failed to establish chain from reply というメッセージが表示された場合、証明書のチェーンが解決できなかったことを表しています。認証局のルート証明書や中間証明書がインポートされていない可能性があります。認証局に、インポートが必要な証明書を問い合わせてください。

5. IMS コンポーネントのサービスを再起動します。

6. 自己署名証明書を使用している場合、ims-ssl-keytool exportcert コマンドで、Web ブラウザーにインポートするための証明書をファイルに出力します。

```
> <%インストールパス%>/bin/ims-ssl-keytool exportcert <filename>
```

ims-ssl-keytool exportcert コマンドで出力した証明書ファイルは、Web コンソールにアクセスするすべての Web ブラウザーに配布し、インポートしてください。Web ブラウザーに証明書をインポートすることで、IMS コンポーネントの Web サーバーに成りすますフィッシング攻撃などを予防することができます。

Web ブラウザーに証明書をインポートする方法は、「1.2.1.2　Web ブラウザーに SSL サーバー証明書をインポートする（9 ページ）」を参照してください。

5.2.4.3　シングルサインオンの設定を変更する

IMS コンポーネントをインストールするサーバーのドメイン名 (FQDN) を変更した場合、シングルサインオン設定を行っている製品側の設定内容を変更する必要があります。

IMS コンポーネントの Web コンソールから、NFA などの Web コンソールをシングルサインオンで起動することができます。シングルサインオンでの Web コンソールの起動に際しては、事前に、接続、または、連携する製品側で、IMS コンポーネントの Web コンソールの URL を登録しておく必要があります。このため、IMS コンポーネントをインストールしているサーバーのドメイン名 (FQDN) を変更した場合は、それに合わせて、接続、または、連携する製品側のシングルサインオン設定の内容も変更する必要があります。

ここでは、例として、NFA での変更手順を説明します。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

1. NFA をインストールしているサーバーにログインします。
2. NFA のサービスを停止します。
3. 設定ファイル(controller.properties)の内容を変更し、上書きして保存します。
   - 設定ファイル

     NFA の<%データパス%>/controller/conf/controller.properties
   - 指定形式

     ```
     ims.webserver.base-url = <ims web url>
     ```

     例：

     ```
     ims.webserver.base-url = http://chg-ims.nec.com/
     ```
4. NFA のサービスを起動します。

   サービスの起動後、URL の変更内容が NFA に反映されます。

5.2.5　IP アドレスを変更する

IMS コンポーネントをインストールするサーバーの IP アドレスを変更する場合の作業について説明します。

IMS コンポーネントをインストールしているサーバーの IP アドレスを変更する場合は、必ず、IMS コンポーネントのサービスをすべて停止してから作業を行ってください。

また、IMS コンポーネントをインストールしているサーバーの IP アドレスを変更した場合は、IMS コンポーネントに接続する各製品側の設定変更が必要になります。

以下に、IMS コンポーネントに接続する NetvisorPro、および、NFA の設定の変更方法を示します。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

1. IMS コンポーネントに接続する製品をインストールしているサーバーにログインします。
2. 接続製品のサービスを停止します。
3. 設定ファイルの内容を変更し、上書きして保存します。
   - NetvisorPro の場合
     - 設定ファイル

       NetvisorPro の<%データパス%>\Manager\sg\NvPRO\NvPROIms.ini

     - 指定形式

       ```
       [NOMS]
       MessageQueueIP=<ims ip address>
       ```

   - NFA の場合
     - 設定ファイル

       NFA の<%データパス%>/controller/conf/controller.properties

     - 指定形式

       ```
       ims.msgqueue.host = <ims ip address>
       ```

4. 接続製品のサービスを起動します。

   サービスの起動後、変更内容が反映されます。

5.2.6　ノードの構成情報を同期する

作業によって、IMS コンポーネントと各製品との間で、ノードの構成情報の差異が生じる場合があります。

例えば、以下のような場合に、ノードの構成情報の差異が生じます。

- IMS コンポーネントのサービスが停止している状態で、NetvisorPro 側で管理対象ノードのプロパティ情報を変更したり、NFA 側でエクスポーターを新たに追加したりした場合
- IMS コンポーネントにおいて、古いバックアップをリストアした場合

このような場合は、構成情報同期画面から、ノードの構成情報に差異がある製品インスタンスとの間で同期を実施します。

5.2.6.1　構成情報同期画面

構成情報同期画面について説明します。

構成情報同期画面では、指定した製品のインスタンスとの間で、ノードの構成情報の同期を行うことができます。

構成情報同期画面は、[**システム設定**] >[**構成情報同期**] メニューをクリックして表示します。

ヒント

アドミニストレーターの役割を持つグループのユーザーのみ、構成情報同期画面を表示することができます。

図 5-4　構成情報同期画面

製品インスタンス一覧

- [**アプリケーション名**]

  IMS コンポーネントに接続する製品名を表示します。

- [**インスタンス名**]

  IMS コンポーネントに接続する製品のインスタンス名を表示します。

- [**リージョン**]

  製品のインスタンスが属するリージョングループ名を表示します。

- [**操作**]

  アイコンをクリックすることで、製品のインスタンスに対する操作を行うことができます。

  - [**同期**]アイコン

    当該インスタンスからノードの構成情報を取得して、IMS コンポーネントに構成情報の再登録を行います。これにより構成情報の差異が解消されます。

5.2.6.2　ノードの構成情報の差異を解消する

メンテナンス作業等によって発生した IMS コンポーネントと各製品とのノードの構成情報の差異を解消するための手順について説明します。

IMS コンポーネントのサービスの停止中に、各製品のノードの構成情報を操作すると、それぞれで管理するノードの構成情報に差異が生じ、運用に支障をきたす場合があります。このような場合、ノードの構成情報の同期を実施して、IMS コンポーネントから各製品の構成情報を再取得し、差異を解消します。

ここでは、IMS コンポーネントのサービスの停止中に、リージョングループ「本社地区」に所属する NetvisorPro の製品インスタンス「NetMgr01」でノードの構成情報の変更作業を行っていた場合の例を用いて、具体的な操作手順を説明します。

1. 構成情報同期画面を表示します。

   [**システム設定**] >[**構成情報同期**] をクリックします。

2. 差異が生じているノードの構成情報を管理する製品インスタンスと同期を行います。

   製品インスタンス一覧から、該当する製品インスタンスを確認し、[**同期**]アイコンをクリックします。

   ここでは、ノードの構成情報の変更作業を行ったリージョングループ「本社地区」に所属する NetvisorPro の製品インスタンス「NetMgr01」の[**同期**]アイコンをクリックします。

   ⚠ 注意

   画面を遷移し、再度、構成情報同期画面を表示すると、同期完了を待たずして、[**同期**]アイコンが再度クリックできる状態になります。同期処理は、構成情報取得の対象製品側にも負荷を与える処理であるため、重複した同期実行を行わないようにしてください。

3. 同期処理の完了通知を確認します。

   実行した同期処理の結果は、イベントとして通知されます。新着イベント通知やイベント画面から、同期処理の完了を示すイベントの内容を確認してください。

4. ノードの構成情報が正しく同期されたことを確認します。

   ノード一覧画面の情報や、ノード詳細画面の[**プロパティ**]ウィジェット、トポロジーマップ画面から、更新した構成情報の内容が、IMS コンポーネントに反映され、Web コンソールで参照できることを確認します。

5.2.7　データ分析用データの保持期間を変更する

アノマリー分析、および、トレンド分析において利用する蓄積するデータの保持期間を変更する手順について説明します。

アノマリー分析、および、トレンド分析における蓄積データの保持期間のデフォルト値は、3 年間(1095 日間) となっています。

1 つの分析対象で利用するディスク容量の目安は、以下の計算式から算出することができます。

ディスク使用量の目安[MB] = 24 × 60 ÷ <*収集間隔（分）*> × <*保持期間(日)*> × 0.00015

<*収集間隔（分）*>：

分析対象としているデータを収集している間隔を分単位で指定します。

NetvisorPro で収集しているデータの場合は、データ収集機能のインターバル値を指定します。

NFA で収集しているフローデータの場合は、必ず、「1」を指定します。

<*保持期間(日)*>：

蓄積データの保持期間を日数で指定します。

例：

NetvisorPro のデータ収集機能において、5 分インターバルで収集している 500 件の項目を分析対象として登録する場合、ディスク使用量の目安は以下のようになります。

ディスク使用量の目安 = (24 × 60 ÷ 5 × 1095 × 0.00015) × 500 ≒ 23GB

上記のディスク使用量の見積もり結果を踏まえ、ディスク使用量の削減が必要な場合に、以下の操作を行います。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

1. IMS コンポーネントをインストールしているサーバーにログインします。
2. IMS コンポーネントのサービスを停止します。
3. 設定ファイルの内容を変更し、上書きして保存します。

   設定ファイルと変更のための指定形式は以下の通りです。

   - 設定ファイル

     <%***データパス***%>\conf\ims-conf.ini

   - 指定形式

     noms.report.raw-data.max-age = <*保持日数*>

     <*保持日数*>で指定した日数分のデータを保持します。ここには、365~1095 の数値を指定することができます。

4. IMS コンポーネントのサービスを起動します。

   サービスの起動後、保持期間の変更内容が IMS コンポーネントに反映されます。

⚠ 注意

保持期間を過ぎたデータの削除においては、各データ間の整合性の確保や処理性能を考慮したタイミングで処理を制御しています。そのため、指定した保持期間よりも最大で 7 日分多く、データが保持され続ける場合があります。

5.2.8　証跡ログの保持期間を変更する

ユーザーの操作履歴を記録する証跡ログの保持期間を変更する手順について説明します。

証跡ログの保持期間のデフォルト値は、3 年間(1095 日間) となっています。証跡ログをデフォルトの期間より長く保持したい場合は、以下の操作を行います。

ヒント

証跡ログ 1 件のデータサイズは、約 300 Bytes です。1 日の証跡ログの件数を 1,000 件と仮定した場合、1 日分のデータサイズは約 300 KBytes となります。この値を目安に、設定変更後のディスク使用量において問題がないことを事前に確認することを推奨します。

1. IMS コンポーネントをインストールしているサーバーにログインします。
2. IMS コンポーネントのサービスを停止します。
3. 設定ファイルの内容を変更し、上書きして保存します。

   設定ファイルと変更のための指定形式は以下の通りです。

   - 設定ファイル

     <%***データパス***%>\conf\ims-conf.ini

   - 指定形式

     ```
     noms.core.auditlog.max-duration = <保持日数>
     ```

     <*保持日数*>で指定した日数分のデータを保持します。ここには、1~5000 の数値を指定することができます。
4. IMS コンポーネントのサービスを起動します。

   サービスの起動後、保持期間の変更内容が IMS コンポーネントに反映されます。

5.3　運用環境をバックアップ、リストアする

IMS コンポーネントの環境設定や蓄積データをバックアップ、リストアする方法について説明します。

IMS コンポーネントでは、環境設定、および、蓄積データのすべての運用環境データをバックアップ、リストアの対象とします。

バックアップ作業、および、リストア作業は、IMS コンポーネントのサービスを停止した状態で行います。

⚠ 注意

バックアップしたデータは、同じバージョンの IMS コンポーネントにのみリストアすることができます。

5.3.1　運用環境をバックアップする

環境設定、蓄積データを一括してバックアップする手順を説明します。

バックアップ作業は、IMS コンポーネントのサービスを停止した状態でのみ実施することができます。

⚠ 注意

- バックアップデータのサイズは、*<%データパス%>*のディスク消費量と同程度になる場合があります。バックアップデータの出力先や保存先の空き容量は十分に確保した上で作業してください。
- バックアップデータのサイズに依存して、バックアップの完了まで時間がかかる場合があります。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

1. IMS コンポーネントをインストールしているサーバーにログインします。
2. バックアップ対象の現在のサイズを確認します。
   - Windows 環境の場合

     以下の 2 つのフォルダに対するプロパティダイアログを表示し、確認します。表示された[**サイズ**]の値を合算してください。

     - *<%データパス%>*\conf
     - *<%データパス%>*\db
   - Linux 環境の場合

     次のコマンドを実行して、サイズを確認します。

     ```
     # du -sm <%データパス%>/{conf,db}
     ```

     結果は、個々のディレクトリ単位に MB 単位で表示されます。表示された数字を合算してください。
3. IMS コンポーネントのサービスを停止します。
4. Windows 環境の場合、コマンドプロンプトを起動します。

   コマンドプロンプトは、 [**管理者として実行**] メニューから起動します。
5. バックアップコマンドを実行します。

   ```
   > <%インストールパス%>/bin/ims-backup <path>
   ```

   引数*<path>*には、バックアップを出力するディレクトリを指定します。バックアップ対象のサイズに対して、十分な空き容量があることを確認してから指定してください。

ims-backup コマンドの詳細については、「A.2　ims-backup（208 ページ）」を参照してください。

エラーメッセージが表示されず、コマンドが正常終了すると、指定した出力先ディレクトリにバックアップファイルが生成されています。

6. IMS コンポーネントのサービスを起動します。

5.3.2　運用環境のバックアップをリストアする

運用環境のバックアップデータをリストアする手順を説明します。

運用環境のバックアップデータのリストアは、IMS コンポーネントのサービスを停止した状態で実施する必要があります。

リストア作業を開始する前に、「5.3.1　運用環境をバックアップする（202 ページ）」で取得したバックアップディレクトリを IMS コンポーネントをインストールしているサーバーに配置しておく必要があります。

⚠ 注意

バックアップのサイズによっては、リストアの完了までに時間かかる場合があります。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

1. IMS コンポーネントをインストールしているサーバーにログインします。
2. IMS コンポーネントのサービスを停止します。
3. Windows 環境の場合、コマンドプロンプトを起動します。

   コマンドプロンプトは、[**管理者として実行**] メニューから起動します。
4. IMS コンポーネントのバックアップをリストアします。

   以下のリストアコマンドを実行します。

```
> <%インストールパス%>/bin/ims-restore <path>
```

   引数<*path*>には、バックアップが格納されているディレクトリを指定します。

   ims-restore コマンドの詳細については、「A.3　ims-restore（209 ページ）」を参照してください。

   エラーメッセージが表示されず、コマンドが正常終了すると、リストアは完了です。

   ⚠ 注意

   OS や Python のバージョンによっては、実行時に警告(Warning)が表示される場合がありますが、リストアは正常に実施されるため問題はありません。
5. 必要に応じて、SSL サーバー証明書の更新作業を行います。

本作業は、HTTPS 通信を行う環境で、かつ、バックアップ元の環境とリストア先の環境のドメイン名 (Web サーバーにアクセスするための URL) が異なる場合に実施します。

作業手順は、「5.2.4.2　SSL サーバー証明書のドメイン名 (CN) を変更する（194 ページ）」を参照してください。

6. IMS コンポーネントのサービスを起動します。

リストアの完了後、IMS コンポーネントと接続する製品との間で、管理対象ノードの構成情報に差異が生じた場合は、構成情報の同期処理を実施してください。詳細は、「5.2.6　ノードの構成情報を同期する（197 ページ）」を参照してください。

付録 A　コマンドリファレンス

IMS コンポーネントが提供するコマンドについて説明します。

A.1　ims-ssl-keytool

HTTPS 通信で使用する SSL サーバー証明書の作成、および、管理を行うコマンドです。

このコマンドは、Java keytool コマンドの機能を本製品向けに使いやすい形で提供するラッパーコマンドです。本コマンドから使用できる機能は、Java keytool コマンドの一部のみです。また、引数の名前や意味は、Java keytool コマンドに合わせています。

Java keytool コマンドとの主な相違点は以下の通りです。

- 最初の引数に genkeypair などのサブコマンド名を指定します。サブコマンドの引数名の先頭に - は付きません。
- 本コマンドでは、キーストアの形式は PKCS12 固定です。また、キーストアファイルのパスは<%***データパス***%>\conf\webserver.ks 固定です。
- genkeypair サブコマンドを実行すると、キーストアのパスワード、キーストア内のエントリーの別名が以下のファイルに記録されます。

  <%***データパス***%>\conf\ims-conf.ini

  ファイルに記録された各種情報は、各種サブコマンドで-storepass、-alias オプションを省略した際に自動で使用されます。そのため、引数の指定数を最小限に抑えてコマンドを実行することができます。
- -keyalg、-validity オプションのデフォルト値が異なります。
- initstore という独自のサブコマンドを実装しています。

⚠ 注意

本コマンドの実行には、OS の管理者権限が必要です。

パス

<%***インストールパス***%>\bin\ims-ssl-keytool

形式

```
ims-ssl-keytool genkeypair [-help] [-storepass PASS] [-alias ALIAS]
    [-keyalg KEYALG] [-keysize KEYSIZE] [-sigalg SIGALG]
    [-validity DAYS] [-dname DNAME] [-dns DNS]
```

```
ims-ssl-keytool selfcert [-help] [-storepass PASS] [-alias ALIAS]
    [-sigalg SIGALG] [-validity DAYS] [-dname DNAME] [-dns DNS]
```

```
ims-ssl-keytool certreq [-help] [-storepass PASS] [-alias ALIAS]
    [-dns DNS] FILE
```

```
ims-ssl-keytool importcert [-help] [-storepass PASS] [-alias ALIAS] FILE
```

```
ims-ssl-keytool exportcert [-help] [-storepass PASS] [-alias ALIAS] FILE
```

```
ims-ssl-keytool list [-help] [-storepass PASS] [-alias ALIAS] [-rfc | -v]
```

```
ims-ssl-keytool delete [-help] [-storepass PASS] [-alias ALIAS]
```

```
ims-ssl-keytool initstore [-help]
```

```
ims-ssl-keytool -help
```

説明

各サブコマンドの意味は次の通りです。

- genkeypair

  鍵のペア (公開鍵および関連する非公開鍵) を生成し、キーストアに格納します。また、Web サーバーが生成した鍵を使用するための情報を以下のファイルに書き出します。

  <%**データパス**%>\conf\ims-conf.ini

  ⚠ 注意

  本コマンドを実行すると、ims-conf.ini ファイル内の設定値を以下のように書き換えます。

  ```
  noms.tomcat.http.enabled = false
  noms.tomcat.https.enabled = true
  ```

- selfcert

  キーストアエントリーの鍵に対する自己署名証明書を作成します。

- certreq

  PKCS#10 形式を使って証明書署名要求 (CSR) を生成します。

- importcert

  ファイルから証明書または証明書チェーンを読み取り、キーストアに格納します。

- exportcert

  証明書をキーストアから読み取り、バイナリ符号化方式の証明書としてファイルに格納します。

- `list`

  特定のキーストアエントリー、またはキーストア全体の内容を表示します。

- `delete`

  キーストアから特定のエントリーを削除します。

- `initstore`

  キーストアファイルを削除します。また、Web サーバーが生成した鍵を使用するための情報を以下のファイルから削除します。

  `<%`**データパス**`%>\conf\ims-conf.ini`

  ⚠ 注意

  本コマンドを実行すると、ims-conf.ini ファイル内の設定値を以下のように書き換えます。

  ```
  noms.tomcat.http.enabled = true
  noms.tomcat.https.enabled = false
  ```

引数

-storepass *PASS*

キーストアのパスワードを指定します。

`genkeypair` サブコマンドの実行時に省略した場合は、コマンド実行中にパスワードの入力が求められます。それ以外のサブコマンドの実行時に省略した場合は、ims-conf.ini ファイルから読み取った値を使用します。

-alias *ALIAS*

キーストア内のエントリーの別名を指定します。

`genkeypair` サブコマンドの実行時に省略した場合は、デフォルト値の「tomcat」が使用されます。また、`list` サブコマンドの実行時に省略した場合は、すべてのエントリーが対象になります。それ以外のサブコマンドの実行時に省略した場合は、ims-conf.ini ファイルから読み取った値を使用します。

-keyalg *KEYALG*

鍵の暗号化アルゴリズムを指定します。「RSA」、「DSA」、「EC」などを指定することができます。デフォルトは「RSA」です。

`-keyalg`、および`-sigalg` に指定できるアルゴリズム一覧は、Java 暗号化アーキテクチャ (JCA) リファレンス・ガイドを参照してください。

-keysize *KEYSIZE*

生成する鍵のサイズを指定します。

指定可能な値およびデフォルト値は、Java keytool の仕様に準拠しています。

-sigalg *SIGALG*

自己署名証明書に署名を付けるときに使うアルゴリズムを指定します。

指定するアルゴリズムは、`-keyalg` と互換性のあるものでなければなりません。指定可能な値およびデフォルト値は、Java keytool の仕様に準拠しています。

-validity *DAYS*

自己署名証明書が有効と見なされる日数を指定します。0 ～ 365000 が指定できます。デフォルトは 3650 (約 10 年) です。

-dname *DNAME*

自己署名証明書の issuer フィールドと subject フィールドとして使う X.500 識別名を指定します。

識別名を指定しなかった場合は、コマンド実行中に識別名の入力を求められます。

-dns *DNS*

証明書の Subject Alternative Name (SAN) 拡張領域に登録する FQDN を指定します。

`genkeypair` サブコマンドでは、指定しなかった場合は証明書の Common Name が使用されます。

-rfc

`list` サブコマンドの出力形式指定オプションです。出力可能符号化方式で証明書の内容が出力されます。

`-v` オプションと同時に指定することはできません。

-v

`list` サブコマンドの出力形式指定オプションです。人間が読むことのできる形式で、証明書の内容詳細が出力されます。

`-rfc` オプションと同時に指定することはできません。

-help

コマンド全体、または各サブコマンドの使用方法を表示します。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

A.2　ims-backup

IMS コンポーネントの運用環境(環境設定、蓄積データ)をバックアップするコマンドです。

本コマンドは、IMS コンポーネントの運用環境をバックアップする際に実行します。

⚠ 注意

- 本コマンドの実行には、OS の管理者権限が必要です。
- 本コマンドは、IMS コンポーネントのサービスを停止した状態で実行する必要があります。
- バックアップ対象のデータサイズによっては、コマンドの完了までに時間がかかる場合があります。

パス

<%*インストールパス*%>\bin\ims-backup

形式

```
ims-backup PATH
```

```
ims-backup -help
```

説明

エラーメッセージが表示されず、コマンドが正常終了すると、指定した出力先ディレクトリにバックアップファイルが生成されています。

引数

PATH

バックアップを出力するディレクトリを指定します。

-help

コマンドの使用方法を表示します。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

A.3　ims-restore

IMS コンポーネントの運用環境(環境設定、蓄積データ)のバックアップデータをリストアするコマンドです。

本コマンドは、IMS コンポーネントの運用環境のバックアップデータをリストアする際に実行します。

⚠ 注意

- 本コマンドの実行には、OS の管理者権限が必要です。
- 本コマンドは、IMS コンポーネントのサービスを停止した状態で実行する必要があります。
- バックアップデータのサイズによっては、コマンドの完了までに時間がかかる場合があります。
- リストアは、バックアップデータと同じバージョンの IMS コンポーネントにのみ実行することができます。

パス

<%*インストールパス*%>\bin\ims-restore

形式

```
ims-restore PATH
```

```
ims-restore -help
```

説明

エラーメッセージが表示されず、コマンドが正常終了すると、バックアップのリストアが完了します。

⚠ 注意

OS や Python のバージョンによっては、実行時に警告(Warning)が表示される場合がありますが、リストアは正常に実施されるため問題はありません。

引数

PATH

バックアップが格納されているディレクトリを指定します。

-help

コマンドの使用方法を表示します。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

A.4　ims-app

IMS コンポーネントに組み込むアプリケーションを管理するためのコマンドです。

本コマンドは、以下の 4 つの作業を行う際に実行します。

- IMS コンポーネント、および、組み込んでいるアプリケーションのバージョン確認作業
- IMS コンポーネントへのアプリケーションの組み込み(インストール)作業
- IMS コンポーネントに組み込まれているアプリケーションのアップデート作業
- IMS コンポーネントに組み込んだアプリケーションのアンインストール作業

⚠ 注意

- 本コマンドの実行には、OS の管理者権限が必要です。
- インストール、アップデート、またはアンインストールの作業を行う場合は、事前に、IMS コンポーネントのサービスを停止させておく必要があります。

パス

<%***インストールパス***%>\bin\ims-app

形式

```
ims-app list
```

```
ims-app install [-help] [-silent] [-overwrite] [-ignore-dependencies]
        WAR_FILE
```

```
ims-app update [-help] [-silent] [-ignore-dependencies] WAR_FILE
```

```
ims-app uninstall [-help] [-silent] ID
```

```
ims-app -help
```

説明

各サブコマンドの意味は次の通りです。

- `list`

  IMS コンポーネントのバージョン情報と共に、IMS コンポーネントに組み込んでいるアプリケーション名、および、バージョン情報を表示します。

- `install`

  WAR_FILE で指定したアプリケーションファイル(WAR ファイル)をインストールし、IMS コンポーネントに組み込みます。

- `update`

IMS コンポーネントに組み込み済みのアプリケーションについて、*WAR_FILE* で指定したアプリケーションファイル(WAR ファイル)にアップデートします。組み込まれていないアプリケーションに対する WAR ファイルを指定した場合は、エラーとなります。

- `uninstall`

  IMS コンポーネントに組み込んでいるアプリケーションの *ID* を指定し、アンインストールします。

引数

-silent

非対話モード(サイレントモード)でコマンドを実行します。

-overwrite

`install` サブコマンドの処理に関するオプションで、非対話モード(サイレントモード)の場合に有効となります。

すでにアプリケーションがインストールされていた場合に、上書きします。

-ignore-dependencies

`install` および `update` サブコマンドの処理に関するオプションです。

アプリケーション間の依存関係を無視してインストール処理を行います。

-help

コマンドの使用方法を表示します。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

A.5　ims-saml-keytool

SAML 認証で使用するキーストアの作成、および、管理を行うコマンドです。

このコマンドは、Java keytool コマンドの機能を本製品向けに使いやすい形で提供するラッパーコマンドです。本コマンドから使用できる機能は、Java keytool コマンドの一部のみです。また、引数の名前や意味は、Java keytool コマンドに合わせています。

Java keytool コマンドとの主な相違点は以下の通りです。

- 最初の引数に `genkeypair` などのサブコマンド名を指定します。サブコマンドの引数名の先頭に - は付きません。
- 本コマンドでは、キーストアの形式は PKCS12 固定です。また、キーストアファイルのパスは`<%`***データパス***`%>\conf\saml.jks` 固定です。

- genkeypair サブコマンドを実行すると、キーストアのパスワード、キーストア内のエントリーの別名が以下のファイルに記録されます。

  <%データパス%>\conf\ims-conf.ini

  ファイルに記録された各種情報は、各種サブコマンドで-storepass、-alias オプションを省略した際に自動で使用されます。そのため、引数の指定数を最小限に抑えてコマンドを実行することができます。

- -keyalg、-validity オプションのデフォルト値が異なります。
- initstore という独自のサブコマンドを実装しています。

⚠ 注意

本コマンドの実行には、OS の管理者権限が必要です。

パス

<%インストールパス%>\bin\ims-saml-keytool

形式

```
ims-saml-keytool genkeypair [-help] [-storepass PASS] [-alias ALIAS]
    [-keyalg KEYALG] [-keysize KEYSIZE] [-sigalg SIGALG]
    [-validity DAYS] [-dname DNAME]
```

```
ims-saml-keytool selfcert [-help] [-storepass PASS] [-alias ALIAS]
    [-sigalg SIGALG] [-validity DAYS] [-dname DNAME]
```

```
ims-saml-keytool certreq [-help] [-storepass PASS] [-alias ALIAS]
    FILE
```

```
ims-saml-keytool importcert [-help] [-storepass PASS] [-alias ALIAS] FILE
```

```
ims-saml-keytool list [-help] [-storepass PASS] [-alias ALIAS] [-rfc | -v]
```

```
ims-saml-keytool delete [-help] [-storepass PASS] [-alias ALIAS]
```

```
ims-saml-keytool initstore [-help]
```

```
ims-saml-keytool -help
```

説明

各サブコマンドの意味は次の通りです。

- genkeypair

鍵のペア (公開鍵および関連する非公開鍵) を生成し、キーストアに格納します。また、SAML 認証を行うための情報を以下のファイルに書き出します。

<%***データパス***%>\conf\ims-conf.ini

- selfcert

  キーストアエントリーの鍵に対する自己署名証明書を作成します。

- certreq

  PKCS#10 形式を使って証明書署名要求 (CSR) を生成します。

- importcert

  ファイルから証明書または証明書チェーンを読み取り、キーストアに格納します。

- list

  特定のキーストアエントリー、またはキーストア全体の内容を表示します。

- delete

  キーストアから特定のエントリーを削除します。

- initstore

  キーストアファイルを削除します。また、SAML 認証を行うための情報を以下のファイルから削除します。

  <%***データパス***%>\conf\ims-conf.ini

引数

-storepass *PASS*

キーストアのパスワードを指定します。

genkeypair サブコマンドの実行時に省略した場合は、コマンド実行中にパスワードの入力が求められます。それ以外のサブコマンドの実行時に省略した場合は、ims-conf.ini ファイルから読み取った値を使用します。

-alias *ALIAS*

キーストア内のエントリーの別名を指定します。

genkeypair サブコマンドの実行時に省略した場合は、デフォルト値の「ims」が使用されます。また、list サブコマンドの実行時に省略した場合は、すべてのエントリーが対象になります。それ以外のサブコマンドの実行時に省略した場合は、ims-conf.ini ファイルから読み取った値を使用します。

-keyalg *KEYALG*

鍵の暗号化アルゴリズムを指定します。「RSA」、「DSA」、「EC」などを指定することができます。デフォルトは「RSA」です。

`-keyalg`、および`-sigalg` に指定できるアルゴリズム一覧は、Java 暗号化アーキテクチャ (JCA) リファレンス・ガイドを参照してください。

-keysize *KEYSIZE*

生成する鍵のサイズを指定します。

指定可能な値およびデフォルト値は、Java keytool の仕様に準拠しています。

-sigalg *SIGALG*

自己署名証明書に署名を付けるときに使うアルゴリズムを指定します。

指定するアルゴリズムは、`-keyalg` と互換性のあるものでなければなりません。指定可能な値およびデフォルト値は、Java keytool の仕様に準拠しています。

-validity *DAYS*

自己署名証明書が有効と見なされる日数を指定します。0 〜 365000 が指定できます。デフォルトは 3650 (約 10 年) です。

-dname *DNAME*

自己署名証明書の issuer フィールドと subject フィールドとして使う X.500 識別名を指定します。

識別名を指定しなかった場合は、コマンド実行中に識別名の入力を求められます。

-rfc

`list` サブコマンドの出力形式指定オプションです。出力可能符号化方式で証明書の内容が出力されます。

`-v` オプションと同時に指定することはできません。

-v

`list` サブコマンドの出力形式指定オプションです。人間が読むことのできる形式で、証明書の内容詳細が出力されます。

`-rfc` オプションと同時に指定することはできません。

-help

コマンド全体、または各サブコマンドの使用方法を表示します。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

付録 B　SAML 認証によるシングルサインオン

SAML 認証を利用した Web コンソールと IdP のシングルサインオンについて説明します。

B.1　SAML 認証によるシングルサインオンの概要

Web コンソールが提供する SAML 認証機能の概要について説明します。

Web コンソールは、 IdP を用いた SAML 認証に対応しています。

SAML 認証を有効化すると、Web コンソールは SP として動作し IdP に登録されたユーザー情報をもとに認証を行うことができます。これにより、IdP と連携している SystemManager G や他の SP とのシングルサインオンが可能となります。

ユーザー情報と権限

SAML 認証は Web コンソールに登録されたユーザー情報と、 IdP に登録されたユーザー情報を紐づけて認証を行います。紐づけにはユーザー名が使用され、同一のユーザー名をもつユーザーを同一ユーザーとみなします。

ユーザーに適用される権限は IdP に登録されたユーザーの持つ権限ではなく、Web コンソールに登録されたユーザーの持つ権限になります。

ヒント

対応関係にある Web コンソールと IdP に登録されたユーザー情報はユーザー名が同一であれば、パスワードは一致させる必要はありません。SAML 認証時は IdP に登録されたユーザー情報のパスワードが使用されます。

SAML 認証を利用したログアウト

SAML 認証によるシングルサインオンを行ったあとに Web コンソールでログアウトを実行すると、Web コンソール、および、 IdP からログアウトが行われます。この状態で、Web コンソールや他の SP へアクセスすると、再度、ユーザー認証を行う必要があります。

B.2　動作環境

SAML 認証の利用に関する動作環境について説明します。

システム構成

SAML 認証を利用するためには、IdP と IMS コンポーネントをセットアップし、連携設定をする必要があります。また、他の SP と IdP の連携設定を行うことで、Web コンソールと他の SP の間でシングルサインオン連携が可能になります。

システム要件

Web コンソールで SAML 認証を利用するためには、以下の条件を満たす IdP との連携が必要となります。

- SAML 2.0 SP-Initiated SSO: Redirect/POST Bindings に対応している。
- XML メタデータのインポート/エクスポートに対応している。

B.3　SAML 認証を利用するための設定作業

SAML 認証を利用する際に必要なセットアップ手順について説明します。

B.3.1　SAML 認証を利用するための設定作業の流れ

SAML 認証を利用するための設定作業の流れについて説明します。

SAML 認証を利用するための設定作業の流れを、「表 B-1 SAML 認証を利用するための設定作業の流れ（217 ページ）」に示します。

表 B-1　SAML 認証を利用するための設定作業の流れ

番号	概要	説明
1	事前準備	「B.3.2　事前準備（218 ページ）」 Web コンソールの設定確認および、SAML 認証を行うユーザーアカウントを準備します。
2	Web コンソールの SAML 認証設定	「B.3.3　Web コンソールで SAML 認証の設定を行う（218 ページ）」 Web コンソールで SAML 認証を行うための設定および XML メタデータのダウンロードを行います。
3	IdP の SAML 認証設定	「B.3.4　IdP で SAML 認証の設定を行う（222 ページ）」 IdP へ Web コンソールの情報登録、XML メタデータのダウンロードを行います。
4	Web コンソールへ IdP の情報をインポート	「B.3.5　Web コンソールへ IdP の XML メタデータをインポートする（225 ページ）」 「B.3.4　IdP で SAML 認証の設定を行う（222 ページ）」でダウンロードした IdP の XML メタデータを Web コンソールへインポートします。

B.3.2　事前準備

Web コンソールで SAML 認証を利用するための準備として、Web コンソールの設定確認、およびユーザーの準備を行います。

設定の確認

SAML 認証の設定を行う前に、以下の設定が適切に行われていることを確認します。

- SAML 認証で用いる URL の設定

  IdP と認証情報の連携を行うために用いる Web コンソールの URL の設定を確認します。

  Web コンソールの「スタートアップガイド」を参照し、URL の設定が行われていることを確認してください。Web コンソールの URL の設定をしていない場合は設定を行ってください。

- Web コンソールの通信方式の設定

  Web コンソールの通信方式の設定を確認します。

  連携を行う IdP によっては、通信方式として HTTPS 通信を有効にする必要があります。事前に IdP のマニュアルを確認し、必要な場合は Web コンソールの「スタートアップガイド」を参照して通信方式の設定を行ってください。

  例えば、Microsoft 社の ADFS (Active Directory Federation Services) を IdP として使用する場合は、HTTPS 通信を有効にする必要があります。

ユーザーの準備

SAML 認証を行うために、IdP と Web コンソールのユーザー情報の紐づけが必要となります。紐づけを行うために、IdP と Web コンソールで同一のユーザー名のアカウントを用意します。事前に SAML 認証を行うためのユーザーの選定を行い、IdP と Web コンソールへユーザー登録を行ってください。

Web コンソールのユーザー登録については「2.1　ユーザーを管理する（34 ページ）」を参照してください。

IdP へのユーザー登録については、各種 IdP のマニュアルを参照してください。

ヒント

対応関係にある Web コンソールと IdP に登録されたユーザー情報はユーザー名が同一であれば、パスワードは一致させる必要はありません。SAML 認証時は IdP に登録されたユーザー情報のパスワードが使用されます。

B.3.3　Web コンソールで SAML 認証の設定を行う

Web コンソールで SAML 認証を行うための設定について説明します。

B.3.3.1　SAML 認証の有効化とキーストアの準備をする

SAML 認証の有効化とキーストアを準備します。

SAML 認証はデフォルトの設定では無効になっているため、有効化する必要があります。また、Web コンソールと IdP の間で安全な通信を行うために、鍵と証明書を格納するキーストアの準備が必要となります。

SAML 認証の有効化と、キーストアの準備は製品が提供する ims-saml-keytool コマンドを使用することで行えます。使用するキーストアには、次の 2 種類があります。

- 自己署名証明書を含むキーストア
- 公的な認証局に発行してもらう証明書を含むキーストア

それぞれの場合の準備手順を説明します。

自己署名証明書を含むキーストアを準備する

SAML 認証に用いるキーストアとして、自己署名証明書を含むキーストアを作成する手順を説明します。

SAML 認証の有効化とキーストアに関する操作は、製品が提供する `ims-saml-keytool` コマンドを使用します。詳細は、「A.5　ims-saml-keytool（212 ページ）」を参照してください。

1. 次のコマンドを実行して、鍵のペア (公開鍵と非公開鍵) を生成し、鍵に対する証明書を作成します。

```
> <%インストールパス%>\bin\ims-saml-keytool genkeypair
```

鍵と証明書を格納するキーストアのパスワードや証明書の識別名に関する情報を入力していきます。

- [ ] 内にはデフォルト値が表示されています。何も入力せず Enter キーを押すと、デフォルト値が使用されます。

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Taro Yamada
What is the name of your organizational unit?
  [Unknown]:  IT Operation Division
What is the name of your organization?
  [Unknown]:  NEC Corporation
What is the name of your City or Locality?
  [Unknown]:  Minato-ku
What is the name of your State or Province?
  [Unknown]:  Tokyo
What is the two-letter country code for this unit?
  [Unknown]:  JP
Is CN=Taro Yamada, OU=IT Operation Division,
 O=NEC Corporation, L=Minato-ku, ST=Tokyo, C=JP correct?
  [No]:  yes
```

ヒント

- ims-saml-keytool コマンドは、いくつかの引数を取ることができます。鍵のアルゴリズムやサイズ、有効期限などを変更したい場合は、「A.5　ims-saml-keytool（212 ページ）」を参照し、オプション引数を指定してください。

作成された証明書は、自己署名された状態になります。

2. IMS コンポーネントのサービスを再起動します。

公的な認証局が発行する証明書を含むキーストアを作成する

SAML 認証に用いるキーストアとして、公的な認証局に署名済み証明書を含むキーストアを作成する手順を説明します。

SAML 認証の有効化とキーストアに関する操作は、製品が提供する ims-saml-keytool コマンドを使用します。詳細は、「A.5　ims-saml-keytool（212 ページ）」を参照してください。

1. 次のコマンドを実行して、鍵のペア (公開鍵と非公開鍵) を生成し、鍵に対する証明書を作成します。

```
> <%インストールパス%>\bin\ims-saml-keytool genkeypair
```

鍵と証明書を格納するキーストアのパスワードや証明書の識別名に関する情報を入力していきます。

- [ ] 内にはデフォルト値が表示されています。何も入力せず Enter キーを押すと、デフォルト値が使用されます。

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Taro Yamada
What is the name of your organizational unit?
  [Unknown]:  IT Operation Division
What is the name of your organization?
  [Unknown]:  NEC Corporation
What is the name of your City or Locality?
  [Unknown]:  Minato-ku
What is the name of your State or Province?
  [Unknown]:  Tokyo
What is the two-letter country code for this unit?
  [Unknown]:  JP
Is CN=Taro Yamada, OU=IT Operation Division,
 O=NEC Corporation, L=Minato-ku, ST=Tokyo, C=JP correct?
  [No]:  yes
```

ヒント

- ims-saml-keytool コマンドは、いくつかの引数を取ることができます。鍵のアルゴリズムやサイズ、有効期限などを変更したい場合は、「A.5　ims-saml-keytool（212 ページ）」を参照し、オプション引数を指定してください。

2. 次のコマンドを実行し、認証局に送付するための証明書署名要求 (CSR) をファイルに出力します。

```
> <%インストールパス%>\bin\ims-saml-keytool
 certreq <filename>
```

指定したファイルに、CSR の内容がテキストで出力されます。

3. 証明書署名要求 (CSR) を認証局に提出します。

`ims-saml-keytool certreq` コマンドで出力した CSR ファイルの内容を、認証局に提出します。

認証局は、CSR の内容を元に、証明書に署名し、返送します。署名済み証明書の返送には、認証局によっては数日かかる場合があります。

4. 認証局から署名済み証明書が届いたら、まずは、認証局のルート証明書をインポートします。

ルート証明書は、IMS コンポーネントをインストールしているサーバー上にファイルとして保存し、次のコマンドでインポートできます。

```
> <%インストールパス%>\bin\ims-saml-keytool
 importcert -alias <alias> <filename>
```

<*alias*>には任意の名前を指定できます。ルート認証局の名前など、分かりやすい名前を指定してください。

認証局によっては、ルート証明書の他に中間証明書のインポートが必要になる場合があります。インポートする証明書の詳細は、認証局に問い合わせてください。

5. ルート証明書や中間証明書をインポートした後に、署名済みの自身の証明書をインポートします。

自身の証明書のインポートにも、`ims-saml-keytool importcert` コマンドを使用します。次のように、`-alias` オプションは指定せずに実行します。

```
> <%インストールパス%>\bin\ims-saml-keytool importcert <filename>
```

実行時に `Failed to establish chain from reply` というメッセージが表示された場合、証明書のチェーンが解決できなかったことを表しています。認証局のルート証明書や中間証明書がインポートされていない可能性があります。認証局に、インポートが必要な証明書を問い合わせてください。

6. IMS コンポーネントのサービスを再起動します。

B.3.3.2 Web コンソールの XML メタデータをダウンロードする

IdP の設定で用いる Web コンソールの XML メタデータをダウンロードする手順について説明します。

1. Web コンソールの XML メタデータをダウンロードします。

Web ブラウザーで以下 URL を指定し、Web コンソールの XML メタデータをダウンロードし、サーバー上に保存します。

- HTTP 通信の場合の URL

  http://<IMS サーバーのドメイン名(FQDN)>/saml/metadata

- HTTPS 通信の場合の URL

  https://<IMS サーバーのドメイン名(FQDN)>/saml/metadata

  <IMS サーバーのドメイン名(FQDN)>は、SSL サーバー証明書の作成時に入力した名前と一致している必要があります。一致していない場合、不正な証明書として警告が表示されます。

2. XML メタデータを IdP をインストールしたサーバーへコピーします。

   ダウンロードした Web コンソールの XML メタデータを IdP がインストールされたサーバー上の任意のディレクトリへ保存します。

   保存した XML メタデータは IdP の設定で使用します。

B.3.4　IdP で SAML 認証の設定を行う

IdP で SAML 認証を行うための設定について説明します。

IdP と Web コンソールを連携し SAML 認証を利用するための設定を行います。

ここでは、IdP の設定に必要な共通の手順について説明し、具体例として、Microsoft 社の ADFS (Active Directory Federation Services) を用いた場合の設定手順を示します。

⚠ 注意

- 設定の詳細は、 IdP 製品ごとに異なるため、利用する IdP 製品のマニュアルを、必ず、確認してください。
- 具体例として示す ADFS の手順においては、ADFS の強化等により変更される場合があります。手順に変更がある場合は、本書の記載内容を参考に、ADFS のマニュアルを確認してください。

1. IdP をインストールしたサーバーにログインします。
2. IdP の管理画面を開きます。
3. Web コンソールの XML メタデータをインポートします。

   IdP と連携するために、Web コンソールの XML メタデータを Idp にインポートします。

   IdP の仕様によっては、XML メタデータとキーストアのインポートが必要になる場合があります。その場合は、IMS コンポーネントをインストールしたサーバー上のキーストアファイルを、IdP のサーバーへコピーし、インポートしてください。

   - キーストアファイル

     `<%`***データパス***`%>\conf\saml.jks`

   以下に ADFS を IdP として使用した場合の設定手順について説明します。

a. 証明書利用者信頼の追加ダイアログを開きます。

ADFS の管理画面から、 [**証明書利用者信頼の追加**] メニューを選択します。

b. 要求への対応を指定します。

証明書利用者信頼の追加ダイアログの [**ようこそ**] ステップで、[**要求に対応する**] を選択します。その後、[**開始**]ボタンをクリックします。

c. Web コンソールの XML メタデータをインポートします。

証明書利用者信頼の追加ダイアログの[**データ ソースの選択**]ステップで、[**証明書利用者についてのデータをファイルからインポートする**]を選択し、「B.3.3.2　Web コンソールの XML メタデータをダウンロードする（221 ページ）」で保存した Web コンソールの XML メタデータを指定します。その後、[**次へ**]ボタンをクリックします。

d. 表示名を指定します。

証明書利用者信頼の追加ダイアログの[**表示名の指定**]ステップで、[**表示名**] として任意の値を設定し、[**次へ**]ボタンをクリックします。

e. アクセス制御ポリシーを指定します。

証明書利用者信頼の追加ダイアログの[**アクセス制御ポリシーの選択**]ステップで、[**すべてのユーザーを許可**]を選択します。その後、[**次へ**]ボタンをクリックします。

f. 証明書利用者信頼の追加ダイアログの[**信頼の追加の準備完了**]ステップで、[**次へ**]ボタンをクリックします。

g. 証明書利用者信頼の追加ダイアログの[**完了**]ステップで、[**閉じる**]ボタンをクリックします。

証明書利用者信頼の追加ダイアログが閉じ、Web コンソールの証明書利用者信頼が登録されます。

4. Web コンソールと IdP のユーザーアカウントの紐づけに関する設定を行います。

SAML 認証時に、Web コンソールと IdP に登録されているユーザーアカウントを紐づける情報として、ユーザー名を使用するための設定を行います。

SAML 認証で使用する NameID フォーマットとして[**ユーザー名**]を指定してください。

以下に ADFS を IdP として使用した場合の設定手順について説明します。

a. 要求発行ポリシーの編集ダイアログを開きます。

ADFS の管理画面の [**証明書利用者信頼**] メニューを選択します。表示された証明書利用者信頼から、先ほど登録した Web コンソールの証明書利用者信頼を右クリックし、 [**要求発行ポリシーの編集**] メニューを選択します。

要求発行ポリシーの編集ダイアログが表示されます。

b. 要求発行ポリシーの編集ダイアログで、[**規則の追加**]ボタンをクリックします。

変換要求規則の追加ダイアログが表示されます。

c. 規則の種類の選択を行います。

変換要求規則の追加ダイアログの[**規則の種類の選択**]ステップで、[**要求規則テンプレート**]に [**LDAP 属性を要求として送信**]を選択し、[**次へ**]ボタンをクリックします。

d. 要求規則の構成を行います。

変換要求規則の追加ダイアログの[**要求規則の構成**] ステップで、[**要求規則名**]に任意の値を指定し、[**属性ストア**] に[**Active Directory**]を選択します。

その後、[**LDAP 属性の出力方向の要求の種類への関連付け**]に「表 B-2 LDAP 属性の出力方向の要求の種類への関連付け（224 ページ）」の項目を設定し、[**完了**]ボタンをクリックします。

表 B-2　LDAP 属性の出力方向の要求の種類への関連付け

LDAP 属性	出力方向の要求の種類
SAM-Account-Name	名前 ID

変換要求規則の追加ダイアログが閉じ、要求発行ポリシーの編集ダイアログが表示されます。

e. 要求発行ポリシーの編集ダイアログを閉じます。

要求発行ポリシーの編集ダイアログの[**OK**]ボタンをクリックします。

5. SAML 認証の詳細設定を行います。

SAML 認証の詳細設定として以下の設定を行います。

- デジタル署名のハッシュアルゴリズム

  Web コンソールと IdP 間の通信処理で使用するデジタル署名のハッシュアルゴリズムを設定します。

  ハッシュアルゴリズムとして SHA-256 を指定してください。

- ログアウトエンドポイント

  Web コンソールからログアウトする際、IdP からもログアウトするために IdP のログアウト URL を設定します。

  IdP 製品のマニュアルを参照し、必要に応じて URL の設定を行ってください。

以下に ADFS を IdP として使用した場合の設定手順について説明します。

a. 証明書利用者信頼のプロパティダイアログを開きます。

ADFS の管理画面から [**証明書利用者信頼**] メニューを選択します。表示された証明書利用者信頼から、先ほど登録した Web コンソールの証明書利用者信頼を右クリックし、 [**プロパティ**] メニューを選択します。

プロパティダイアログが表示されます。

b. ハッシュアルゴリズムを設定します。

プロパティダイアログの、[**詳細設定**]タブを選択し、[**セキュア ハッシュアルゴリズム**]で [**SHA-256**]を選択します。

c. ログアウトエンドポイントを設定します。

プロパティダイアログの、[**エンドポイント**]タブを選択し、各[**SAML ログアウトエンドポイント**]の項目に対して編集を行い、[**信頼された URL**]に以下の URL を指定します。

- https://<ADFS サーバーのドメイン名(FQDN)>/adfs/ls/?wa=wsignout1.0

d. プロパティダイアログを閉じます。

プロパティダイアログで[**OK**]ボタンをクリックします。

6. IdP の XML メタデータをダウンロードします。

Web コンソールへインポートを行う IdP の XML メタデータをダウンロードします。ダウンロードした XML メタデータは saml-idp-metadata.xml という名前でサーバー上に保存します。

以下に ADFS を IdP として使用した場合の設定手順について説明します。

Web ブラウザーで以下 URL を指定し、ADFS の XML メタデータをダウンロードし、saml-idp-metadata.xml という名前でサーバー上に保存します。

- https://<ADFS サーバーのドメイン名(FQDN)>/federationmetadata/2007-06/federationmetadata.xml

以上で、IdP へ行う設定は完了となります。

B.3.5　Web コンソールへ IdP の XML メタデータをインポートする

IdP の XML メタデータを Web コンソールにインポートする手順を説明します。

1. IdP の XML メタデータをコピーします。

「B.3.4　IdP で SAML 認証の設定を行う（222 ページ）」で保存した IdP の XML メタデータを、IMS コンポーネントをインストールしたサーバーへコピーしてください。コピー先のパスとファイル名を以下に示します。

- コピー先のパス

<%***データパス***%>\conf\

- ファイル名

saml-idp-metadata.xml

2. IMS コンポーネントのサービスを再起動します。
3. Web ブラウザーで、Web コンソールの URL を指定し IdP のログイン画面が表示されることを確認します。

- HTTP 通信の場合の URL

  http://<IMS サーバーのドメイン名(FQDN)>/

- HTTPS 通信の場合の URL

  https://<IMS サーバーのドメイン名(FQDN)>/

  <IMS サーバーのドメイン名(FQDN)>は、SSL サーバー証明書の作成時に入力した名前と一致している必要があります。一致していない場合、不正な証明書として警告が表示されます。

SAML 認証を利用するための設定作業は以上で完了となります。

B.4　IdP メンテナンス時のログイン

IdP メンテナンス時のログイン方法について説明します。

障害発生やメンテナンスなどにより IdP に接続できない場合、SAML 認証を利用してログインすることができなくなります。そのような場合は、ローカル認証を利用してログインすることができます。

ローカル認証では、Web コンソールに登録したユーザーのユーザー名、パスワードを使用してログインします。ローカル認証を行う場合は、以下の URL を Web ブラウザーで指定してください。

- HTTP 通信の場合の URL

  http://<IMS サーバーのドメイン名(FQDN)>/login

- HTTPS 通信の場合の URL

  https://<IMS サーバーのドメイン名(FQDN)>/login

  <IMS サーバーのドメイン名(FQDN)>は、SSL サーバー証明書の作成時に入力した名前と一致している必要があります。一致していない場合、不正な証明書として警告が表示されます。

B.5　SAML 認証の無効化

SAML 認証を有効化した後に、無効化する場合の手順を説明します。

SAML 認証の無効化に関する操作は、製品が提供する `ims-saml-keytool` コマンドを使用します。`ims-saml-keytool` コマンドの詳細は、「A.5　ims-saml-keytool（212 ページ）」を参照してください。

1. SAML 認証を無効化するためのコマンドを実行します。

```
> <%インストールパス%>\bin\ims-saml-keytool initstore
```

SAML 認証が無効化され、鍵のペア (公開鍵と非公開鍵) 、および、鍵に対する証明書が削除されます。

2. IMS コンポーネントのサービスを再起動します。

付録 C　トラブルシューティング

Web コンソールの利用において、想定されるトラブルとその対処方法について説明します。

C.1　Web コンソールにアクセスできない

事象

所定の URL を指定して、Web コンソールにアクセスしようとしたが、以下のような画面が表示されてアクセスできない。

図 C-1　画面例

原因

IMS サーバー上で、IMS コンポーネントのサービスが起動していないことが考えられます。

対処

IMS コンポーネントのサービスを起動してください。操作については、「5.2.2　サービスを起動、停止する（188 ページ）」を参照してください。

C.2　対処方法が不明なエラーダイアログが表示される

事象

Web コンソールのメニューやボタンをクリックした際に、以下のような Ajax エラーを示すエラーダイアログが表示されます。

図 C-2　画面例

原因

IMS コンポーネントのサービスが再起動されたなどにより Web コンソールの通信セッションが切断された可能性があります。

対処

Web ブラウザーを閉じるなどして、Web コンソールへのアクセスを停止し、再度、Web コンソールへアクセスしてください。

付録 D　利用するシステムリソース

IMS コンポーネントが利用するシステムリソースについて説明します。

D.1　利用するポート番号の一覧

IMS コンポーネントが利用するポート番号のデフォルト値について説明します。

IMS コンポーネントが、外部、および、内部との通信において利用するポート番号を「表 D-1 通信ポート番号一覧 (外部通信) (230 ページ)」、「表 D-2 通信ポート番号一覧 (内部通信) (230 ページ)」に示します。

表 D-1　通信ポート番号一覧 (外部通信)

名称	ポート番号	プロトコル	方向	説明
HTTP 通信ポート	80	TCP	IN	Web ブラウザーとの HTTP 通信のために利用します。
HTTPS 通信ポート	443	TCP	IN	Web ブラウザーとの HTTPS 通信のために利用します。
Message Queue 通信ポート	28110	TCP	IN	各製品とのメッセージの送受信のために利用します。

表 D-2　通信ポート番号一覧 (内部通信)

名称	ポート番号	プロトコル	方向	説明
System Database 通信ポート	28120	TCP	IN	システムデータベースとの通信に利用します。
Key Store 通信ポート	28130	TCP	IN	キーストアとの通信に利用します。
TimeSeries Database 通信ポート	28140	TCP	IN	タイムシリーズデータベースとの通信に利用します。

これらのポート番号はすべて変更することができます。利用するポート番号の変更手順は、「5.2.3　利用する通信ポート番号を変更する（190 ページ）」を参照してください。

付録 E　レポート作成用サンプルマクロ

IMS コンポーネントは、Microsoft Excel を用いて性能情報のレポートを作成するためのサンプルマクロを提供しています。

ここでは、提供するサンプルマクロの概要や使用方法について説明します。

サンプルマクロは、インストールメディアの以下のパスに格納しています。

- `\IMS\tools\report\IMS_SampleReport_V1.1.xlsm`
- `\IMS\tools\report\IMS_SampleReport_FM_V1.0.xlsm`

⚠ 注意

サンプルマクロを利用するためには、利用環境において、.NET Framework 3.5 をインストール、または、機能を有効にする必要があります。

Windows 10 においては、以下の手順で機能を有効にすることができます。

1. [**コントロール パネル**]から[**プログラムと機能**]を選択します。
2. [**Windows の機能の有効化または無効化**]を選択します。

   Windows の機能ダイアログが表示されます。
3. [**.NET Framework 3.5 (.NET 2.0 および 3.0 を含む)**]チェックボックスをオンにします。

   再起動を求められた場合は、コンピュータの再起動を実施します。

E.1　サンプルマクロの概要

提供するサンプルマクロの概要について説明します。

性能管理レポート

提供するサンプルマクロでは、Web API を用いて指定期間における SNMP データ、または、フローデータを取得し、グラフの作成、データの出力を行います。

取得可能なデータ種別は、以下の通りです。

- SNMP データ (NetvisorPro 利用時)
  - CPU 使用率
  - メモリ使用率
  - 入力インターフェイス使用率
  - 入力インターフェイス使用量
  - 出力インターフェイス使用率
  - 出力インターフェイス使用量

  - 入力パケット損失率
  - 入力パケット損失数
  - 出力パケット損失率
  - 出力パケット損失数
  - 入力パケットエラー率
  - 入力パケットエラー数
  - 出力パケットエラー率
  - 出力パケットエラー数
  - 応答時間(IPv4)
  - 応答時間(IPv6)
  - NetvisorPro で設定した任意のデータ種別
- フローデータ (NFA 利用時)
  - 通信量の多い入力インターフェイス
  - 通信量の多い出力インターフェイス
  - 通信量の多いアプリケーション (線グラフ、または、円グラフ)
  - 通信量の多い IP プロトコル (線グラフ、または、円グラフ)
  - 通信量の多い DSCP (線グラフ、または、円グラフ)
  - 通信量の多いカンバセーション (2 点間)
  - 通信量の多い送信元 IP アドレス
  - 通信量の多い宛先 IP アドレス
  - 通信量の多い送信元エンドポイントグループ
  - 通信量の多い宛先エンドポイントグループ
  - 通信量の多い送信元 AS (Autonomous System)
  - 通信量の多い宛先 AS (Autonomous System)

データの取得対象とするノード、または、インターフェイスは最大で 10 個までを同時に指定することができます。

対象件数 (TopN) の指定は、最大で 100 まで指定することができます。ただし、対象件数 (TopN) に 20 を超える値を指定した場合は、グラフの作成は行わず、グラフ作成用のデータの出力のみ行います。

障害管理レポート

提供するサンプルマクロでは、Web API を用いて指定期間におけるイベントデータを取得し、以下の情報をレポートとして出力します。

- イベントデータ集計:

  イベントの重要度ごとに重み付けした異常度を集計し、異常度の値が高いノード TopN(ランキング)を表示します。障害が発生しやすいノードの分析などに利用することができます。

- イベント発生状況グラフ:

  イベントの発生件数を時系列グラフで表示します。障害が発生しやすい時間帯の分析などに利用することができます。

- イベント一覧:

  イベントデータ集計やイベント発生状況グラフの処理で用いたイベントの一覧を表示します。指定期間に発生したイベントの記録として利用することができます。

E.2　サンプルマクロの使用方法

提供するサンプルマクロの使用方法について説明します。

サンプルマクロは、インストールメディアから任意の端末にコピーして利用します。

サンプルマクロを Microsoft Excel で開いた際、必ず、マクロの有効化(コンテンツの有効化)を実施してください。

具体的な操作手順は以下の通りです。

1. [**基本設定**]シートの Web API アクセスキーを入力します。

   [**Access Key ID**]、および、[**Secret Access Key**]は、Web コンソールのプロファイル編集画面から発行、確認することができます。

2. [**基本設定**]シートの IMS サーバーの情報を入力します。

   Web コンソールにアクセスする場合と同じ[**ドメイン名(FQDN)**]、[**ポート番号**]、[**プロトコル**]を指定します。

3. [**条件入力**]シートに取得対象データの条件を指定します。

   性能管理レポートにおいては、単一のノード、または、インターフェイスを指定する場合と複数のノードおよびインターフェイスを指定する場合とで、入力するシートが異なります。

4. グラフ作成を実行します。

   [**条件入力**]シートの右上に配置する[**グラフ作成**]アイコンをクリックするとマクロが実行され、グラフ作成処理が開始されます。

   処理が完了するとグラフおよびデータを出力するシートが作成されます。

5. 作成されたシートの内容を確認します。

上記の操作を繰り返し実施することで、様々なデータを取得することができます。

サンプルマクロが作成するグラフでは運用に支障がある場合は、得られたデータから、Microsoft Excel を用いて集計、グラフ作成等の作業を実施してください。

付録 F　SystemManager G との連携

イベントアクション機能を利用することで、検出したイベントの情報を SytemManager G へ連携することができます。

ここでは、SystemManager G と連携するための設定や SystemManager G へ通知するイベントメッセージのフォーマットについて説明します。

F.1　連携対象の SystemManager G 情報を登録する

イベントの通知先となる SystemManager G の情報を登録する方法について説明します。

検出したイベントの情報を SystemManager G へ通知するためには、事前に、通知先となる SystemManager G の情報を設定ファイル (ims-conf.ini) に登録しておく必要があります。

設定ファイルのパス

<%***データパス***%>\conf\ims-conf.ini

指定形式

以下のパラメーターを追記し、上書きして保存します。

```
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].id
 = <manager id>
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].name
 = <manager name>
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].host
 = <manager host name>
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].port
 = <webapi port number>
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].url-scheme
 = <url scheme>

noms.event.action.sysmgrg-linkage.nvp-compatible-format.enable
 = <compatible mode>
```

<manager id>

連携対象の SystemManager G を一意に識別できるようにするための ID を半角英数字で指定します。最大文字数は 64 文字です。

<manager name>

[**manager id**]に対する SystemManager G を識別する名前を任意の文字列で指定します。最大文字数は 64 文字です。

<manager host name>

連携対象の SystemManager G のホスト名、もしくは、IPv4 アドレスを指定します。本パラメーターを用いて SystemManager G との通信処理を行います。

ホスト名で指定する場合の最大文字数は、128 文字です。また、指定したホスト名で名前解決が行える必要があります。

<webapi port number>

イベントメッセージ転送の通信で利用する SystemManager G の通信ポート番号を 0～65535 の範囲で指定します。

ヒント

- 指定を省略した場合は、*<url-scheme>*の指定値に対応して、以下のデフォルト値で動作します。
  - http: 22524
  - https: 42524
- 本パラメーターは、SystemManager G のメッセージストアで利用する通信ポート番号と合わせる必要があります。

<url scheme>

SystemManager G との通信において、「http」を利用するのか「https」を利用するのかを指定します。

ヒント

指定を省略した場合は、「http」を指定したものとして動作します。

<compatible mode>

NetvisorPro の監視イベントを SystemManager G に互換モードのメッセージフォーマットで通知するかどうかを以下のように指定します。

- true (オン):

  互換モードのメッセージフォーマットで通知します。

- false (オフ):

  通常モードのメッセージフォーマットで通知します。

ヒント

指定を省略した場合は、「false」を指定したものとして動作します。

設定例:

```
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].id = 1
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].name
 = 統合管理サーバ
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].host
 = sysmgr01.nec.com
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].port = 42524
noms.event.action.sysmgrg-linkage.sysmgrg-managers[0].url-scheme
 = https
```

```
noms.event.action.sysmgrg-linkage.nvp-compatible-format.enable = false
```

⚠ 注意

パラメーターの末尾に不要なスペースが含まれている場合、末尾のスペースも含めてパラメーター値と判断するため、意図した通りの処理が行えません。

設定ファイル (ims-conf.ini) の保存前に、パラメーター末尾に不要なスペースが含まれていないことを確認してください。

設定ファイル (ims-conf.ini) の変更内容を反映させるため、サービスの再起動を行います。

F.2　メッセージフォーマット

SystemManager G に通知するイベントのメッセージフォーマットについて説明します。

ヒント

NetvisorPro の監視によって発生したイベントに対しては、2 種類のフォーマットを提供しています。

F.2.1　通常モードのメッセージフォーマット

SystemManager G に連携するイベントのメッセージは、通常、本節で説明するメッセージフォーマットで通知されます。

⚠ 注意

SystemManager G との連携設定において互換モードを選択した場合、NetvisorPro の監視によって検出したイベントに対しては異なるメッセージフォーマットで通知されます。詳細は、「F.2.2　互換モードのメッセージフォーマット（239 ページ）」を参照してください。

SystemManager G への通知内容

SystemManager G のメッセージプロパティに対する通知内容を以下に示します。

表 F-1　メッセージのプロパティ

プロパティ	通知内容
カテゴリ	Network
アプリケーション	WebSAM Integrated Management Server
オブジェクト	NetvisorPro の監視イベント以外では値なしで通知します。 NetvisorPro の監視イベントでは以下の値で通知します。 **NvPro System** NetvisorPro のシステムが発行するメッセージであることを示します。 **NvPro SNMP Trap** SNMP トラップ受信によるメッセージであることを示します。 **NvPro Syslog**

プロパティ	通知内容
	シスログ受信によるメッセージであることを示します。 **NvPro Alert** 状態監視やデータ収集によるアラート検出やアラート集約などを示すメッセージであることを示します。
メッセージ定義 ID	2300000
メッセージ ID	IMS コンポーネント内で管理するイベントの ID を通知します。
重要度	Web コンソールのイベント重要度に対応する SystemManager G の重要度を通知します。
発生日時	Web コンソールでの発生日時を通知します。
ノード名	イベント発生を検知したノード名、または、ネットワークインターフェイス名を以下の形式で通知します。 *<ノード名>(<リージョングループ名>)* *<ノード名>(<リージョングループ名>):<ネットワークインターフェイス名>* *"(<リージョングループ名>)"*を付与するかどうかはカスタマイズが可能です。詳細は、後述するヒントを参照してください。
メッセージ概要	イベントの概要情報を通知します。
メッセージテキスト	イベントの詳細情報、および、対処情報に加え、イベント詳細画面の URL を通知します。 詳細は「メッセージテキストのフォーマット（239 ページ）」を参照してください。

ヒント

*ノード名に"(<リージョングループ名>)"*を付与しないためには、以下の設定を行ってください。

- 設定ファイル

  `<%`***データパス***`%>\conf\ims-conf.ini`

- 指定形式

  ```
  noms.event.action.sysmgrg-linkage.settings.region-name-format =
  ```

  空の値を設定します。

設定ファイルの内容は、サービスの再起動により、動作に反映されます。

重要度の対応付け

SystemManager G に通知される重要度について説明します。

Web コンソールのイベント重要度と SystemManager G の重要度の対応は以下となります。

表 F-2　重要度の対応付け

Web コンソール	SystemManager G
Fatal	異常
Critical	警告
Error	警告
Warning	警告

Web コンソール	SystemManager G
Unknown	不明
Normal	正常

メッセージテキストのフォーマット

メッセージテキストは、以下のフォーマットとなります。

```
<イベントの詳細情報>

詳細:
<イベント詳細画面の URL>

対処:
<イベントの対処情報>
```

通知例:

```
通信インタフェース 519 の動作が開始したという通知を検出しました。

詳細:
http://ims.nec.com/events/1234-5678-90

対処:
対処は不要です。
```

⚠ 注意

<イベント詳細画面の URL>をメッセージ内に含めるためには、事前に、以下の設定ファイルに対して Web コンソールにアクセスするための URL を設定しておく必要があります。

- 設定ファイル

  <%***データパス***%>\conf\ims-conf.ini

- 指定形式

```
noms.core.url.external-base-url = <URL>
```

設定ファイルの内容は、サービスの再起動により、動作に反映されます。

F.2.2　互換モードのメッセージフォーマット

SystemManager G との連携設定において互換モードを選択した場合、NetvisorPro の監視によって検出したイベントに対しては、本節で説明するメッセージフォーマットで通知されます。

互換モードを選択した場合は、従来の NetvisorPro と SystemManager G (バージョン 10 未満) との連携時と互換性のあるフォーマットでイベントのメッセージを通知します。

⚠ 注意

NetvisorPro の監視以外で検出したイベントに対しては、通常モードのメッセージフォーマットが適用されます。

SystemManager G への通知内容

SystemManager G のメッセージプロパティに対する通知内容を以下に示します。

表 F-3　メッセージのプロパティ

プロパティ	通知内容
カテゴリ	Network
アプリケーション	NetvisorPro V
オブジェクト	NetvisorPro のアラート種別に合わせて以下の値で通知します。 **NvPro System** NetvisorPro のシステムが発行するメッセージであることを示します。 **NvPro SNMP Trap** SNMP トラップ受信によるメッセージであることを示します。 **NvPro Syslog** シスログ受信によるメッセージであることを示します。 **NvPro Alert** 状態監視やデータ収集によるアラート検出やアラート集約などを示すメッセージであることを示します。
メッセージ定義 ID	2300000
メッセージ ID	NetvisorPro 内で管理するアラートの ID を通知します。
重要度	Web コンソールのイベント重要度に対応する SystemManager G の重要度を通知します。
発生日時	NetvisorPro での発生日時を通知します。
ノード名	イベント発生を検知したノード名を以下の形式で通知します。 <*ノード名*>@<*ホスト名*> "@<*ホスト名*>"を付与するかどうかはカスタマイズが可能です。詳細は、「F.2.3　互換モードのメッセージフォーマットを変更する（243 ページ）」を参照してください。
メッセージ概要	イベントの概要情報を通知します。
メッセージテキスト	オブジェクトの値ごとに異なるフォーマットのメッセージを通知します。 詳細は「メッセージテキストのフォーマット（241 ページ）」を参照してください。

重要度の対応付け

SystemManager G に通知される重要度について説明します。

Web コンソールのイベント重要度と SystemManager G の重要度の対応は以下となります。

表 F-4　重要度の対応付け

Web コンソール	SystemManager G
Fatal	異常
Critical	警告
Error	警告
Warning	警告
Unknown	不明
Normal	正常

メッセージテキストのフォーマット

メッセージテキストは、オブジェクト値によってフォーマットが異なります。以下にオブジェクト値に対するメッセージテキストのフォーマットについて示します。

フォーマットの記述の中にある｛｝で囲んだパラメーター(置換文字列)の詳細については、「表 F-5 パラメーター(置換文字列)の説明（242 ページ）」に示します。

ヒント

メッセージテキストの形式は、カスタマイズすることが可能です。詳細は、「F.2.3　互換モードのメッセージフォーマットを変更する（243 ページ）」を参照してください。

- NvPro SNMP Trap : SNMP トラップを示すメッセージ

```
[ID={id}]{summary}(D={detail})(IP={ipAddress})(Enterprise={enterprise})
(Gen={genericCode})(Spec={specificCode})

<イベント詳細画面の URL>
```

通知例：

```
[ID=1114]インタフェースアップ(D=通信インタフェース 519 の動作が開始した
という通知を検出しました。)(IP=10.1.1.1)
(Enterprise=1.3.6.1.4.1.119.2.2.4.4.18.3)(Gen=6)(Spec=1)

http://ims.nec.com/events/1234-5678-90
```

- NvPro Syslog : シスログを示すメッセージ

```
[ID={id}]{summary}(D={detail})(IP={ipAddress})(A={action})
(F={facility})(Sev={severity})(K={knowledgeId})

<イベント詳細画面の URL>
```

通知例：

```
[ID=1115]IKE 機能のシスログ(WARNING)が発生しました。(D=IKE 接続先の
 10.34.17.23 から応答がありません。)(IP=10.1.1.1)
(A=接続先との通信の確認を行って下さい。)(F=IKE)(Sev=WARNING)
(K=15231)
```

```
http://ims.nec.com/events/2345-6789-01
```

- その他のオブジェクト値 (NvPro Alert, NvPro System)

```
[ID={id}]{summary}(D={detail})(IP={ipAddress})(Snd={sender})
(M={messageDefinitionId})

<イベント詳細画面の URL>
```

通知例：

```
[ID=1116]通信不能(D=コンポーネントと通信できなくなりました)(IP=10.1.1.1)
(Snd=IcmpUpDown)(M=198)

http://ims.nec.com/events/3456-7890-12
```

表 F-5　パラメーター(置換文字列)の説明

パラメーター(置換文字列)	説明
{id}	すべてのオブジェクト値に対し共通のパラメーターで、NetvisorPro のアラート管理で採番した ID に置換します。
{summary}	すべてのオブジェクト値に対し共通のパラメーターで、イベントの概要情報に置換します。
{detail}	すべてのオブジェクト値に対し共通のパラメーターで、イベントの詳細情報に置換します。
{ipAddress}	すべてのオブジェクト値に対し共通のパラメーターで、イベントを検知したノードの IP アドレスに置換します。
{enterprise}	[**NvPro SNMP Trap**]に対するパラメーターで、受信した SNMP トラップの Enterprise 値に置換します。
{genericCode}	[**NvPro SNMP Trap**]に対するパラメーターで、受信した SNMP トラップの GenericCode 値に置換します。
{specificCode}	[**NvPro SNMP Trap**]に対するパラメーターで、受信した SNMP トラップの SpecificCode 値に置換します。
{action}	[**NvPro Syslog**]に対するパラメーターで、シスログの対処情報に置換します。
{facility}	[**NvPro Syslog**]に対するパラメーターで、シスログの Facility 値（10 進表記）に置換します。
{severity}	[**NvPro Syslog**]に対するパラメーターで、シスログの Severity 値に置換します。
{knowledgeId}	[**NvPro Syslog**]に対するパラメーターで、SyslogDiagnosis 機能が提供するシスログの対処情報に対応する ID に置換します。
{sender}	[**NvPro Alert**]または、[**NvPro System**]に対するパラメーターで、NetvisorPro のアラート発行機能の情報に置換します。
{messageDefinitionId}	[**NvPro Alert**]または、[**NvPro System**]に対するパラメーターで、NetvisorPro のアラートメッセージ定義の ID に置換します。

F.2.3　互換モードのメッセージフォーマットを変更する

互換モード選択時の NetvisorPro の監視イベントに対し、メッセージフォーマットを変更する手順について説明します。

ヒント

以下の操作は、OS の管理者権限を持つユーザーで実施する必要があります。

1. IMS コンポーネントをインストールしているサーバーにログインします。
2. IMS コンポーネントのサービスを停止します。
3. 設定ファイル (ims-conf.ini) の内容を変更し上書き保存します。

   設定ファイル (ims-conf.ini) の格納先と指定形式を以下に示します。

   設定ファイルのパス

   <%***データパス***%>\conf\ims-conf.ini

   指定形式

   - メッセージテキストのフォーマットを定義する場合

     SystemManager G に通知するアラートメッセージのフォーマットは、アラートの種別(オブジェクト値)ごとに定義を行います。

     - NvPro SNMP Trap : SNMP トラップを示すメッセージ

       ```
       noms.event.action.sysmgrg-linkage.nvp-compatible-format.message-text.snmp-trap = <メッセージテキスト>
       ```

       <メッセージテキスト>の指定に利用できる置換文字列は以下の通りです。

       {id}、{summary}、{detail}、{ipAddress}、

       {enterprise}、{genericCode}、{specificCode}

       指定例

       ```
       noms.event.action.sysmgrg-linkage.nvp-compatible-format.message-text.snmp-trap = [ID={id}]{summary}(D={detail})(Enterprise:{enterprise}, Gen:{genericCode}, Spec={specificCode})(IP={ipAddress})
       ```

     - NvPro Syslog : シスログを示すメッセージ

       ```
       noms.event.action.sysmgrg-linkage.nvp-compatible-format.message-text.syslog = <メッセージテキスト>
       ```

       <メッセージテキスト>の指定に利用できる置換文字列は以下の通りです。

       {id}、{summary}、{detail}、{ipAddress}、

       {action}、{facility}、{severity}、{knowledgeId}

       指定例

```
noms.event.action.sysmgrg-linkage.nvp-compatible-format.message-text.syslog = [ID={id}]{summary}(D={detail})(A={action})(F={facility}, Sev={severity})
```

- その他のオブジェクト値 (NvPro Alert, NvPro System)

```
noms.event.action.sysmgrg-linkage.nvp-compatible-format.message-text.other = <メッセージテキスト>
```

<メッセージテキスト>の指定に利用できる置換文字列は以下の通りです。

{id}、{summary}、{detail}、{ipAddress}、

{sender}、{messageDefinitionId}

指定例

```
noms.event.action.sysmgrg-linkage.nvp-compatible-format.message-text.other = [ID={id}]{summary}(D={detail})(IP={ipAddress})
```

指定可能な置換文字列の詳細は、「表 F-5 パラメーター(置換文字列)の説明（242 ページ)」を参照してください。

- ノード名の形式を変更する場合

SystemManager G に通知するノード名に"@<ホスト名>"を付与するかどうかを設定します。

```
noms.event.action.sysmgrg-linkage.nvp-compatible-format.to-MoM = <mode>
```

<mode>

- true:

  "@<ホスト名>"を付与します。

- false:

  "@<ホスト名>"を付与しません。

ヒント

指定を省略した場合は、「true」を指定したものとして動作します。

4. IMS コンポーネントのサービスを起動します。

用語集

A - Z

■ D

■ DNS

DNS(Domain Name System)とは、ネットワーク上のホスト名、あるいは、ドメイン名と IP アドレスとの対応状況を管理するためのシステムのことを指します。

■ DSCP

DSCP(Differentiated Services Code Point)とは、パケットに優先度を付けるための仕組みのことを指します。IP ヘッダー内の ToS フィールド(8bit)のうち、6bit を利用し、64 段階の優先度を指定することができます。

■ F

■ FQDN

FQDN(Fully Qualified Domain Name/完全修飾ドメイン名)とは、ドメイン名、サブドメイン名、ホスト名等を省略せずにすべて記述したドメイン名のことを示します。

■ I

■ IANA

IANA(Internet Assigned Numbers Authority)とは、インターネットに関連する様々な番号(IP アドレス、プロトコル番号、ポート番号など)を管理している組織のことを指します。

■ IdP

IdP(Identity Provider)とは、SAML 認証において認証情報(ユーザー情報)を提供するためのシステムのことを指します。

■ ifIndex

SNMP によるネットワーク管理において、最も利用されている識別子の 1 つで、物理インターフェイスや論理インターフェイスに関連付けられる一意の識別番号のことを指します。

■ ifName

装置の物理インターフェイス、または、論理インターフェイスの名前を記録する MIB のオブジェクト名のことを指します。

■ IP プロトコル

Web コンソール、および、NFA では、IP ヘッダ中のプロトコル番号 (IP Protocol Number)で示されるプロトコルのことを指しており、具体的には、TCP、UDP、ICMP などの総称としています。

■ IPFIX

IPFIX(IP Flow Information Export)とは、ネットワークの通信状況をモニタリングするための技術で、NetFlow version 9 をもとにして拡張された IETF 標準技術です。

■ L

■ LAG

LAG(Link Aggregation Group)とは、複数の物理的なインターフェイスを仮想的に束ね、あたかも 1 本のインターフェイスであるかのように扱う技術のことで、IEEE P802.3ad で規定されています。

■ M

■ MIB

MIB(Management Information Base)とは、SNMP で管理可能なネットワーク装置が、自分の状態を外部に知らせるために公開する管理情報のことで、RFC 1156 および、RFC 1213 で規定されています。MIB の情報は、外部から SNMP を用いて、オブジェクト名を指定して値を参照することができます。

■ N

■ NetFlow

米国 Cisco Systems, Inc.が開発したネットワークの通信状況をモニタリングするための技術で、RFC3954 でバージョン 9 の仕様が公開されています。

NetFlow では、IP ベースの通信情報のみを対象としており、また、通信パケットのモニタリング方法としてフルモードとサンプリングモードの 2 つを提供しています。

■ P

■ PHB

PHB(Per Hop Behavior)とは、DSCP 値に対応するパケット転送処理の振る舞い定義のことを指します。

■ S

■ SAML

SAML(Security Assertion Markup Language)とは、異なるサービス間においてユーザー認証を行うための規格を指します。

SAML を利用することで、複数のサービスへのシングルサインオンを行うことができます。

■ sFlow

米国 InMon Corp.が開発したネットワークの通信状況をモニタリングするための技術で、RFC3176 でバージョン 4 の仕様が公開されています。

sFlow では、特定の割合で通信パケットをサンプリングし、その情報を統計分析することで、全体の通信量を算出する仕組みを提供しています。

■ SNMP

SNMP(Simple Network Management Protocol)とは、RFC1157 で規定されているネットワーク管理のためのプロトコルです。

SNMP を用いることで、TCP/IP ネットワークに接続するネットワーク装置に対し、ネットワーク経由で監視や管理を行うことができます。

■ SNMP トラップ

能動的に自分の状態を通知するための SNMP が提供する仕組みのことを指します。

■ SP

SP(Service Provider)とは、SAML 認証において IdP の認証情報(ユーザー情報)を利用するシステムのことを指します。

Web コンソールは SAML 認証において SP に分類されます。

■ sysDescr

装置に関する説明を記録する MIB のオブジェクト名のことを指します。

■ sysName

装置のホスト名を記録する MIB のオブジェクト名のことを指します。sysName の値は、装置のコンフィグにより設定することができます。

■ sysObjectID

装置の機種に関連付けられる一意の識別番号のこと、または、それを記録する MIB のオブジェクト名のことを指します。

■ T

■ ToS

ToS(Type of Service)とは、IP ヘッダーを構成するフィールドの 1 つで、パケット転送を行う各装置に対し、パケットの処理方法を伝えるために利用します。

あ - わ

■ あ

■ ウィジェット

ダッシュボード画面やノード詳細画面などの各画面の構成要素の 1 つで、グラフや一覧表の表示機能を提供します。

■ エクスポーター

NFA では、フロー(sFlow、NetFlow、IPFIX)パケットを送信することができるスイッチやルーターなどの装置、または、ソフトウェアの総称としてエクスポーターという表現を用いています。

■ エンドポイント

ネットワークに接続し、様々な通信を行うパソコンなどのネットワーク端末の総称のことを示します。

■ か

■ カンバセーション

Web コンソール、および、NFA では、特定の 2 点間の通信のやり取りのことをカンバセーションと表現しています。

■ は

■ フロー

エンドポイント間の通信の流れのこと、または、この通信の流れをエクスポーターでモニタリングし生成した情報(sFlow、NetFlow、IPFIX)のことを指します。

■ ポート番号

TCP/IP の通信を行う際に通信先のプログラムを特定するための番号のことを指します。

WebSAM Network Management
Web コンソール
リファレンスマニュアル

IMS00MJ0400-01

2025 年 5 月 第 1 版 発行

日本電気株式会社