WebSAM Network Management
Web コンソール
スタートアップガイド

Linux 環境用

IMS0LSJ0320-01

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、Web コンソールを利用するために必要な IMS コンポーネント (バージョン 3.2) のセットアップ、および、環境設定について説明します。また、Web コンソールの基本的な操作方法についても説明します。Web コンソールを利用するための環境構築を行う前に、本書をよくお読みください。

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動作環境（1 ページ）」	Web コンソールの概要と動作環境について説明します。	User
「第 2 章　IMS コンポーネントのセットアップ（11 ページ）」	Web コンソールを利用するための環境のセットアップ手順について説明します。	Admin
「第 3 章　運用開始前の準備（47 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 4 章　基本操作（58 ページ）」	Web コンソールの基本的な操作について説明します。	User
「第 5 章　IMS コンポーネントのアップグレード（80 ページ）」	Web コンソールの利用環境をアップグレードする手順について説明します。	Admin
「第 6 章　IMS コンポーネントのアンインストール（84 ページ）」	Web コンソールの利用環境をアンインストールする手順について説明します。	Admin
付録	Web コンソールの利用環境の構築作業に関連する補足情報について説明します。	Admin

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:

/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。

目次

第 1 章
Web コンソールの概要と動作環境

Web コンソールの概要と動作環境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。

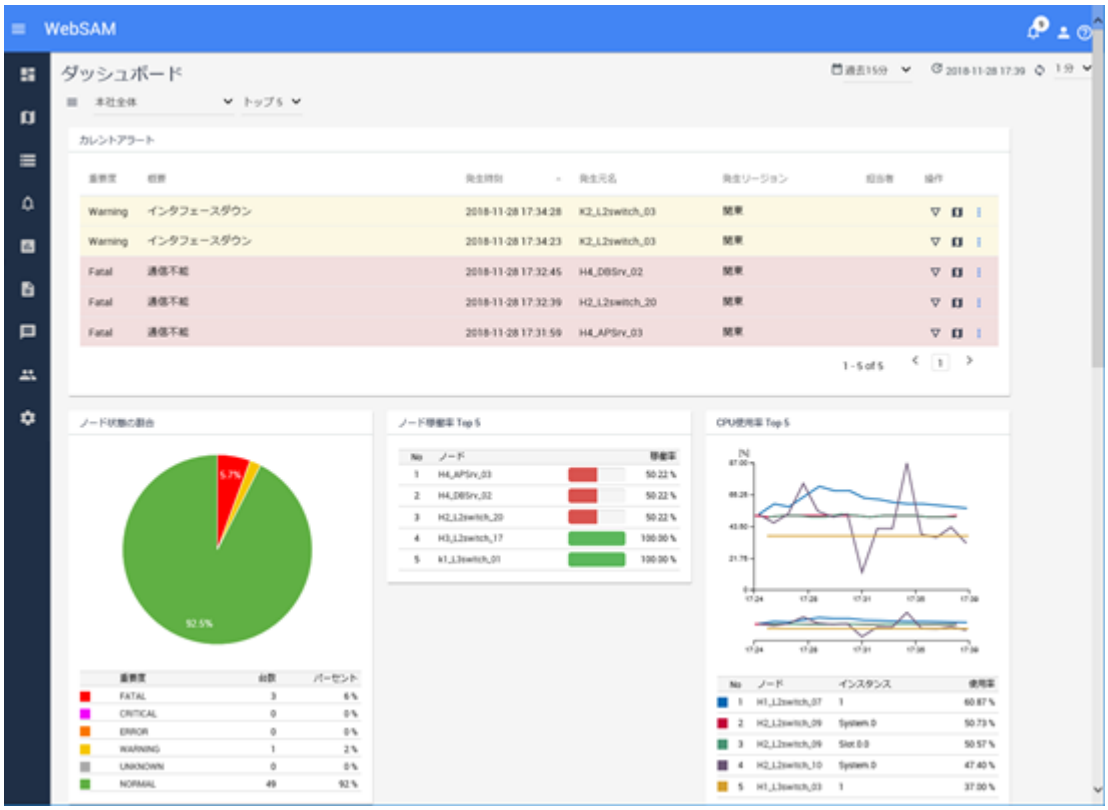

図 1-1　ダッシュボード表示

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。

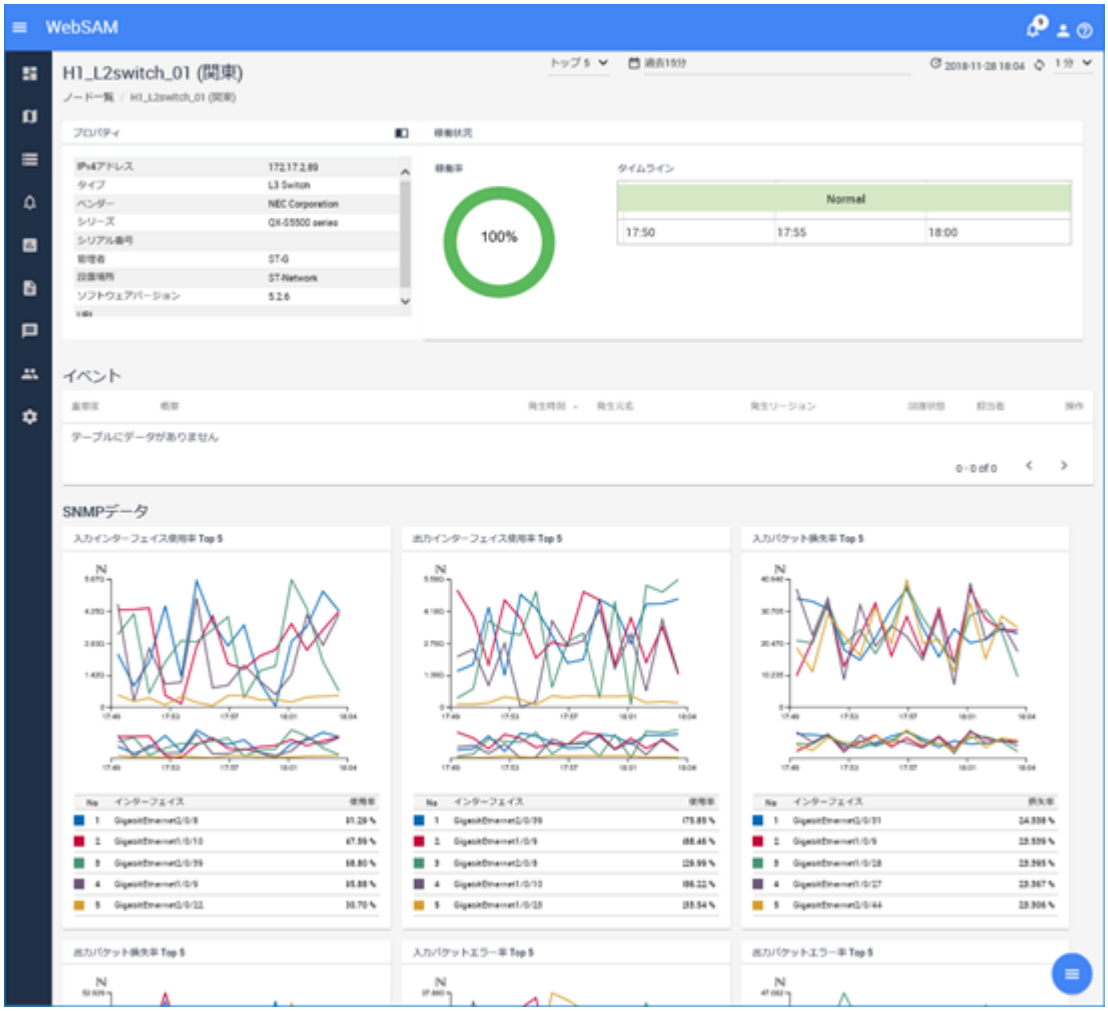

図 1-2　ノード詳細表示

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。

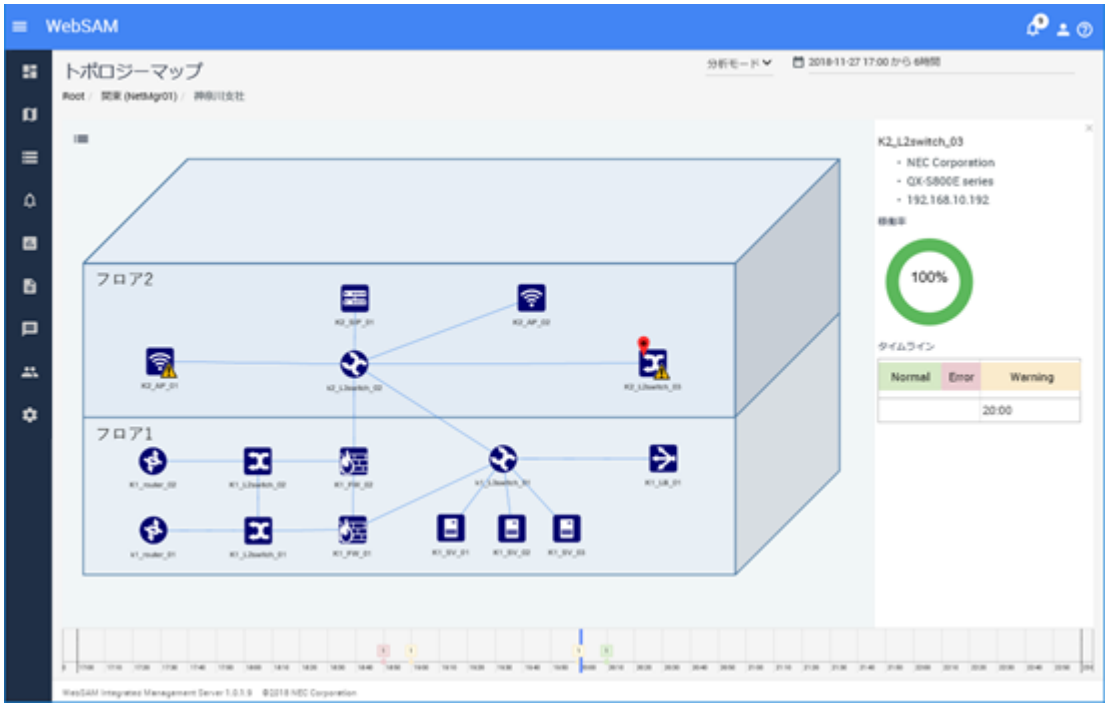

図 1-3　トポロジーマップ表示

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。

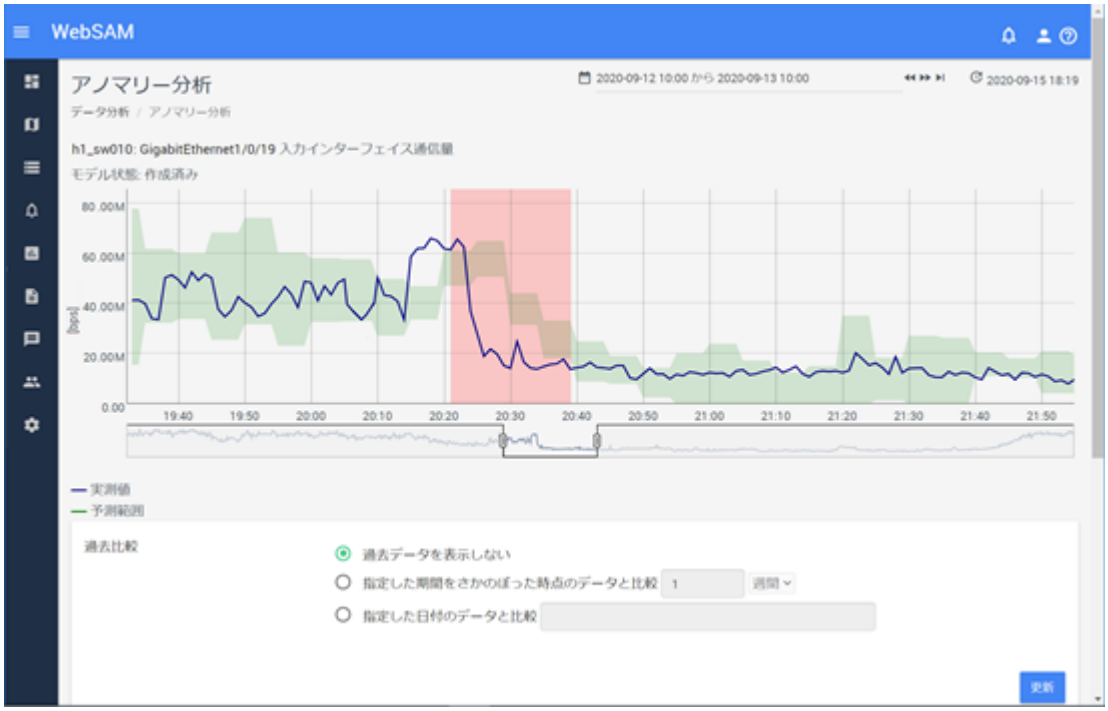

図 1-5　アノマリー分析

1.2　動作環境

Web コンソールの利用に関する動作環境について説明します。

1.2.1　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。

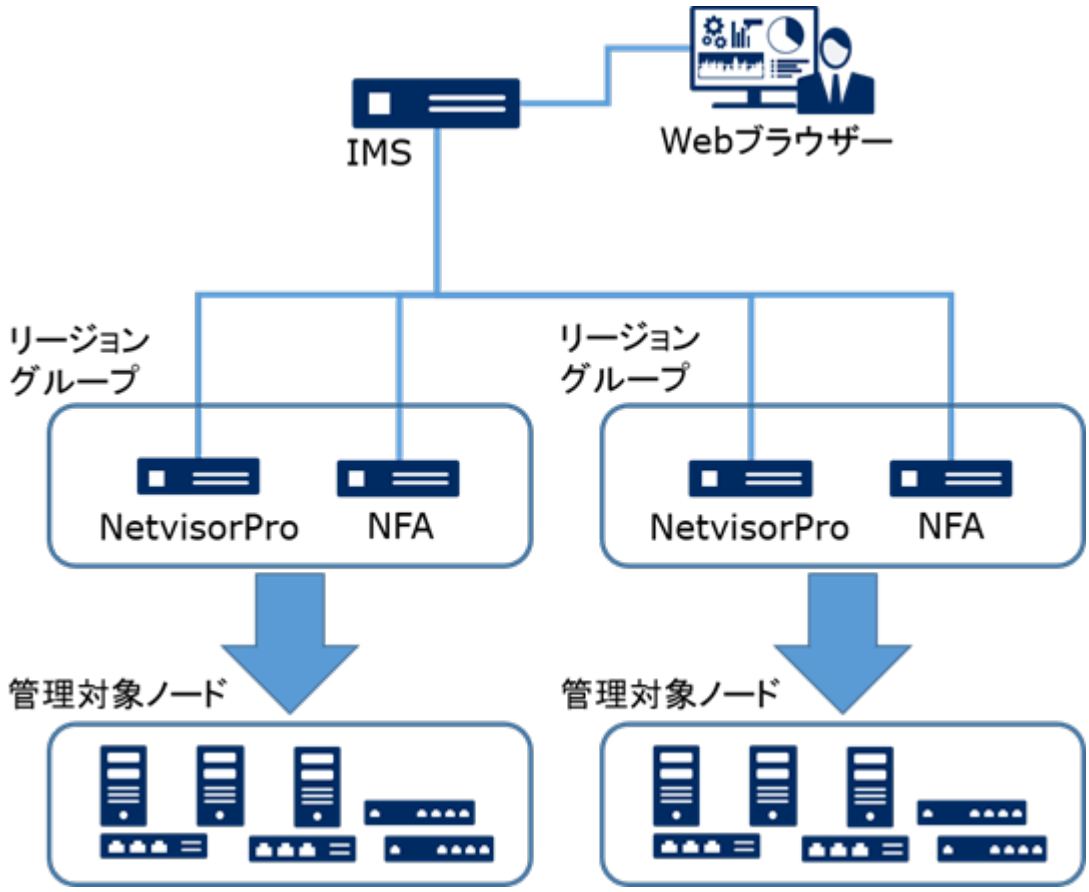

図 1-6　システム構成図

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。

1.2.2　対応製品バージョン

IMS コンポーネント (バージョン 3.2) と接続可能なネットワーク運用管理製品について、サポートするバージョンを以下に示します。

表 1-1　IMS コンポーネント バージョン 3.2 と製品バージョンの互換性

製品名	サポート バージョン	備考
WebSAM NetvisorPro V	9.0 ～ 9.6	連携アプリケーションは、3.2 のみサポート。
WebSAM Network Flow Analyzer	2.0 ～ 3.3	連携アプリケーションは、3.2 のみサポート。

⚠ 注意

- WebSAM NetvisorPro V 9.0, 9.1 においては、WebSAM SystemManager G 10 以上へのイベント通知を行うことができません。WebSAM SystemManager G 10 以上へのイベント通知が必要な場合は、WebSAM NetvisorPro V 9.2 (9.2.0.8) 以上にアップグレードする必要があります。
- WebSAM NetvisorPro V 9.3 以下においては、SyslogDiagnosis 機能を利用している場合であっても Syslog の検索、閲覧操作ができません。Syslog の検索、閲覧の機能が必要な場合は、WebSAM NetvisorPro V 9.4 以上にアップグレードする必要があります。
- WebSAM NetvisorPro V 9.5 以下においては、ネットワークインターフェイスの状態の表示、ネットワークインターフェイス詳細画面のウィジェットでのしきい値の表示は行えません。これらの機能を利用する場合は WebSAM NetvisorPro V 9.6 以上にアップグレードする必要があります。
- WebSAM Network Flow Analyzer 2.0, 2.1 においては、データ分析機能(アノマリー分析、トレンドライン分析)を利用することができません。データ分析機能を利用する場合は、WebSAM Network Flow Analyzer 2.2 以上にアップグレードする必要があります。

1.2.3　システム要件

Web コンソールの利用に必要なシステム要件、および、サポート環境について以下に示します。

表 1-2　IMS コンポーネントのシステム要件

項目	内容
CPU	Intel クアッドコア Xeon 以上、または同等の互換プロセッサを推奨
システムメモリ	最低 2GB 以上 (8GB 以上を推奨) 注 1
ディスク容量	インストールパス: 2GB 以上
	データパス: 最低 20GB 以上 (200GB 以上を推奨)
OS	• Red Hat Enterprise Linux 9 (x86_64) 注 2 注 3 (9.2 以上をサポート) • Red Hat Enterprise Linux 8 (x86_64) 注 2 注 3

注

1. データ分析において、500 件以上の分析対象を登録する場合は、システムメモリとして、16GB 以上が利用できる環境である必要があります。
2. SELinux は無効（disabled）に設定する必要があります。
3. 以下のパッケージをインストールする必要があります。
   - python3
   - glibc-langpack-en
   - libicu

表 1-3　Web ブラウザーの要件

項目	内容
対応ブラウザー	Windows 上で動作する以下の Web ブラウザー • Microsoft Edge 104 以上 • Google Chrome 104 以上
CPU	Intel Core i3 (第 6 世代) 以上、または同等の互換プロセッサを推奨
システムメモリ	最低 1GB 以上 (3GB 以上を推奨)

ヒント

Web ブラウザーに最新の修正プログラムを適用した上でご利用いただくことを推奨します。修正プログラム未適用の場合、一部機能が正常動作しない場合があります。

第 2 章
IMS コンポーネントのセットアップ

Web コンソールを利用する際に必要な IMS コンポーネントのセットアップ手順について説明します。

目次

2.1　IMS コンポーネントのセットアップ作業の流れ

IMS コンポーネントのセットアップ作業の流れについて説明します。

IMS コンポーネントのセットアップ作業の流れを、「表 2-1 IMS コンポーネントのセットアップ作業の流れ（12 ページ）」に示します。

表 2-1　IMS コンポーネントのセットアップ作業の流れ

番号	概要	説明
1	インストールパラメーターの決定	「2.2.1　セットアップパラメーターの設計を行う（13 ページ）」 IMS コンポーネントのインストール作業に必要なパラメーターを確認し、その値を決定します。
2	インストール先の環境確認	「2.2.2　インストール先の環境確認を行う（19 ページ）」 インストール先となるサーバーにおいて、IMS コンポーネントのシステム要件を満たしていることを確認します。
3	IMS コンポーネントのインストール	「2.3　インストール処理を実行する（19 ページ）」 インストールメディアに収録されたインストーラーを実行し、IMS コンポーネントをインストールします。
4	製品接続のための設定	「2.4　製品接続のための設定を行う（21 ページ）」 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ための IMS コンポーネント側の設定を行います。
5	Web コンソールの通信方式の設定	「2.5　Web コンソールの通信方式を設定する（25 ページ）」 Web コンソールへのアクセスに、HTTPS 通信を用いる場合は、HTTPS 通信の有効化のための設定と SSL サーバー証明書を用意する必要があります。 **ヒント** Web コンソールへのアクセスに、HTTP 通信を用いる場合は、本作業を行う必要はありません。
6	使用するポート番号の確認	「2.6　通信ポート番号をデフォルト値から変更する（31 ページ）」 IMS コンポーネントが使用するポート番号と、共存する他のソフトウェアが使用するポート番号とが干渉しないことを確認します。
7	SystemManager G 連携のための設定	「2.7　連携対象の SystemManager G 情報を登録する（33 ページ）」 必要に応じて、検出したイベントのメッセージを SystemManager G に連携するための設定を行います。
8	ファイアウォールの設定	「2.8　ファイアウォールの設定を変更する（36 ページ）」 IMS コンポーネントが、外部と適切に通信できるように、ファイアウォールの設定を確認し、必要に応じて設定変更します。
9	インストール環境への追加設定	「2.9　インストール環境への追加の設定を行う（36 ページ）」 IMS コンポーネントのインストール環境に対して、追加の環境設定を行います。
10	IMS コンポーネントのサービス起動	「2.10　IMS コンポーネントのサービスを起動する（40 ページ）」 IMS コンポーネントのサービスが正常に起動することを確認します。
11	接続製品のセットアップ	「2.11　接続製品のセットアップを行う（41 ページ）」 IMS コンポーネントと接続する WebSAM のネットワーク運用管理製品側のセットアップを行います。

2.2　事前準備を行う

IMS コンポーネントをセットアップする前の準備作業について説明します。

2.2.1　セットアップパラメーターの設計を行う

IMS コンポーネントのセットアップ作業に先立ち、作業に必要なパラメーターを準備します。

インストーラー実行時に必要なパラメーター

IMS コンポーネントのインストーラーを実行する際に、必要となるパラメーターを以下に示します。IMS コンポーネントのインストール前に、インストーラーで指定するパラメーターの準備を行ってください。

表 2-2　インストーラー実行時に必要なパラメーター

パラメーター名	説明	デフォルト値
インストールパス	IMS コンポーネントの実行ファイルをインストールするディレクトリです。 最大で 128 文字まで指定することができます。半角英数字、および "_", "-", "." のみ使用可能です。	/opt/nec/ims
データパス	環境設定や蓄積データを保存するディレクトリです。 最大で 128 文字まで指定することができます。半角英数字、および "_", "-", "." のみ使用可能です。 インストールパスとは異なるパスを指定することを推奨します。 データパスには、構成情報やイベントなどのデータを蓄積します。運用環境に依存して、多くの空き容量を必要とする場合があります。	/opt/nec/ims

製品接続の設定に必要な共通パラメーター

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際に、必要となるパラメーターを以下に示します。システム構成に合わせてパラメーターの準備を行ってください。

表 2-3　製品接続の設定に必要な共通パラメーター

パラメーター名	説明	例
region id	本パラメーターは、IMS コンポーネントの設定で必要となります。 接続する製品をグルーピングするリージョングループを識別するために、システムで一意の ID を半角英数字で指定します。 **⚠ 注意** セットアップ作業で指定した ID は、その後、変更することはできません。	tokyo

パラメーター名	説明	例
	複数のリージョングループで運用することを想定している場合は、複数の ID を準備します。	
region name	本パラメーターは、IMS コンポーネントの設定で必要となります。 [**region id**]に対し、表示上のリージョングループの名前を任意の文字列で指定します。システムで一意の名前となるように指定する必要があります。 Web コンソールの操作画面では、ここで指定する名前が、リージョングループの名前として表示されます。	東京
manager id (InstanceID)	本パラメーターは、IMS コンポーネントと接続する製品の両方の設定で必要となります。 IMS コンポーネントが、接続する製品(製品インスタンス)を適切に識別できるように、同一製品内で一意となる ID を半角英数字で指定します。 **⚠ 注意** セットアップ作業で指定した ID は、その後、変更することはできません。 複数製品を接続して運用することを想定している場合は、複数の ID を準備します。 例えば、2 つの NetvisorPro で構成する場合に、重複しない 2 つの ID を準備する必要があります。 NetvisorPro と NFA など異なる製品においては ID が重複しても問題ありません。 [**manager id**]を準備する際に、どの[**region id**](リージョングループ)に所属させるのかについても、あわせて設計しておく必要があります。	nvpro01 ([**tokyo**]に所属させる)
manager host name	本パラメーターは、IMS コンポーネントの設定で必要となります。 [**manager id**]に対応するホスト名を任意の文字列で指定します。 運用面を考慮し、実際のサーバーのホスト名に合わせることを推奨します。 Web コンソールの操作画面では、ここで指定する名前が、製品インスタンス名として表示されます。	NetMgr01
ims ip address	本パラメーターは、IMS コンポーネントに接続する製品側の設定で必要となります。 IMS コンポーネントをインストールするサーバーの IPv4 アドレスを指定します。 **ヒント** 複数の IPv4 アドレスを持つサーバーの場合は、必ず、接続する製品側から接続可能な IPv4 アドレスを調べておいてください。	192.168.1.200

NetvisorPro との接続に必要なパラメーター

IMS コンポーネントと NetvisorPro とを接続するために必要なパラメーターを以下に示します。

表 2-4　NetvisorPro との接続設定に必要なパラメーター

パラメーター名	説明	例
manager ip address	本パラメーターは、IMS コンポーネントの設定で必要となります。 接続する NetvisorPro のマネージャ機能をインストールするサーバーの IPv4 アドレスを指定します。 **ヒント** 複数の IPv4 アドレスを持つサーバーの場合は、必ず、IMS コンポーネント側から接続可能な IPv4 アドレスを調べておいてください。	192.168.1.100

IMS コンポーネントは、NetvisorPro の制御のため、NetvisorPro の Web API を利用します。NetvisorPro 側の Web API に関連するパラメーターをデフォルト値から変更する場合は、パラメーターの準備を行ってください。

表 2-5　NetvisorPro の Web API 関連のパラメーター

パラメーター名	説明	デフォルト値
webapi port number	本パラメーターは、IMS コンポーネントと NetvisorPro の両方の設定で必要となります。 NetvisorPro の Web API の通信ポート番号を指定します。	20100
webapi ssl flag ([**[HTTPS で暗号化する]チェックボックス**])	本パラメーターは、IMS コンポーネントと NetvisorPro の両方の設定で必要となります。 NetvisorPro の Web API の通信において、HTTPS を利用するかどうかを以下のように指定します。 • true (オン): HTTPS を利用します。 • false (オフ): HTTPS を利用せず、HTTP を利用します。	false (チェックボックス: オフ)

NFA との接続に必要なパラメーター

IMS コンポーネントと NFA とを接続するために必要なパラメーターを以下に示します。

表 2-6　NFA との接続設定に必要なパラメーター

パラメーター名	説明	例
nfa web url	本パラメーターは、IMS コンポーネントの設定で必要となります。 接続する NFA の Web コンソールにアクセスするための URL を指定します。	https://nfa01.nec.com/nfa/
ims web url	本パラメーターは、NFA の設定で必要となります。 IMS コンポーネントの Web コンソールにアクセスするための URL を指定します。	http://ims.nec.com

通信に関するパラメーター

Web コンソールへのアクセスにおいては、HTTP、および、HTTPS の 2 つのプロトコルをサポートしており、デフォルトの設定では、HTTP を利用します。また、IMS コンポーネントでは、外部、および、内部との通信において、いくつかの通信ポートを利用します。以下に通信ポート番号のデフォルト値を示します。

通信に関する各パラメーターにおいて、デフォルト値からの変更の必要性について、事前に確認しておいてください。

表 2-7　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。 デフォルトでは、HTTP 通信が有効になっています。
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。 デフォルトでは、HTTPS 通信は無効になっています。
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 2-8　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。

SSL 証明書の作成に必要なパラメーター

Web コンソールへのアクセスに、HTTPS 通信を用いる場合は、SSL サーバー証明書を作成する必要があります。SSL サーバー証明書を作成するために必要となるパラメーター、および、証明書の識別名 (Distinguished Name) に関するパラメーターを事前に準備しておきます。

ヒント

Web コンソールへのアクセスに、HTTP 通信を用いる場合は、本作業を行う必要はありません。

SSL サーバー証明書を公的な認証局に発行してもらう場合、使用する認証局によっては、鍵の暗号化アルゴリズムや識別名など、一部のパラメーターに条件が指定されている場合があります。事前に、認証局が提示している条件を確認してください。

表 2-9　SSL サーバー証明書に関するパラメーター

パラメーター名	説明	デフォルト値
キーストアのパスワード	SSL サーバー証明書を格納するキーストアのパスワードです。	なし
エントリーの別名	SSL サーバー証明書を格納するエントリーの表示名です。 特別な理由がない限り、デフォルト値をそのまま使用することをお勧めします。	tomcat
鍵の暗号化アルゴリズム	SSL サーバー証明書の鍵の暗号化アルゴリズムです。 自己署名証明書を利用する場合など、通常はデフォルト値のままで問題ありません。指定可能な値の詳細は「A.1　ims-ssl-keytool（86 ページ）」を参照してください。	RSA
生成する鍵のサイズ	SSL サーバー証明書の鍵のサイズです。 自己署名証明書を利用する場合など、通常はデフォルト値のままで問題ありません。指定可能な値の詳細は「A.1　ims-ssl-keytool（86 ページ）」を参照してください。	2048
署名アルゴリズム	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です。 通常はデフォルト値のままで問題ありません。指定可能な値の詳細は「A.1　ims-ssl-keytool（86 ページ）」を参照してください。 公的な認証局に証明書を発行してもらう場合、発行依頼時に指定できる場合があります。詳細は、認証局にお問い合わせください。	SHA256withRSA
自己署名証明書の有効期限	自己署名証明書を利用する場合に指定する、証明書の有効期限です。作成時点からの有効日数を指定します。 公的な認証局に証明書を発行してもらう場合、通常、有効期限は認証局により決められるため、この値を準備する必要はありません。	3650 日 (約 10 年)

表 2-10　SSL サーバー証明書の識別名 (Distinguished Name) に関するパラメーター

パラメーター名	説明	例
サーバーの FQDN	IMS コンポーネントをインストールするサーバーの完全修飾ドメイン名 (FQDN) です。SSL サーバー証明書の Common Name に相当します。 Web コンソールにアクセスする全ての Web ブラウザーはこのドメイン名を URL に指定してアクセスするため、全ての Web ブラウザーが解決可能な名前である必要があります。	ims.nec.com
部署名	製品を所有し運用する組織の部署名です。SSL サーバー証明書の Organizational Unit に相当します。	IT Operation Division
組織名	製品を所有し運用する組織の名称です。SSL サーバー証明書の Organizational Name に相当します。 通常、法律上の正式な英文組織名称を指定します。	NEC Corporation
市区町村名	製品を所有し運用する組織の属する市区町村の名前です。SSL サーバー証明書の Locality に相当します。 例えば、東京都港区の場合は Minato-ku と指定します。	Minato-ku
都道府県名	製品を所有し運用する組織の属する都道府県の名前です。SSL サーバー証明書の State に相当します。 例えば、東京都の場合は Tokyo と指定します。	Tokyo

パラメーター名	説明	例
国コード	製品を所有し運用する組織が属する国のコード名です。SSL サーバー証明書の Country に相当します。 日本の場合は、通常、JP と指定します。	JP

SystemManager G との連携に必要なパラメーター

SystemManager G と連携するために必要なパラメーターを以下に示します。SystemManager G との連携設定を行うことで、検出したイベントを SystemManager G に通知することができます。

表 2-11　SystemManager G 連携のためのパラメーター

パラメーター名	説明	例
manager id	本パラメーターは、IMS コンポーネントの設定で必要となります。 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。 **⚠ 注意** セットアップ作業で指定した ID は、その後、変更することはできません。	1
manager name	本パラメーターは、IMS コンポーネントの設定で必要となります。 [**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。	統合管理サーバ
manager host name	本パラメーターは、IMS コンポーネントの設定で必要となります。 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。	sysmgr01.nec.com
webapi port number	本パラメーターは、IMS コンポーネントの設定で必要となります。 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指定します。 0～65535 の範囲で指定することができ、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 **⚠ 注意** 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。	42524

パラメーター名	説明	例
url scheme	本パラメーターは、IMS コンポーネントの設定で必要となります。 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。 省略した場合は、「http」を指定したものとして動作します。	https
compatible mode	本パラメーターは、IMS コンポーネントの設定で必要となります。 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。 省略した場合は、「false」を指定したものとして動作します。 メッセージフォーマットの詳細については、「付録 E　SystemManager G 連携のメッセージフォーマット（115 ページ）」を参照してください。	false

2.2.2　インストール先の環境確認を行う

IMS コンポーネントをインストールするサーバーの環境が、インストール要件を満たしているか確認します。

インストール先のサーバーが、「1.2.3　システム要件（9 ページ）」で示す IMS コンポーネントのシステム要件を満たしていることを事前に確認します。

また、「通信に関するパラメーター（16 ページ）」で確認した通信ポートが、インストール先のサーバーで利用可能なことを確認します。もしも利用できない通信ポートが見つかった場合は、IMS コンポーネントが利用するポート番号の見直し、または、他の製品が利用するポート番号の変更を行ってください。

⚠ 注意

インストール先となるサーバーに Event Adapter コンポーネントがインストールされている場合は、IMS コンポーネントをインストールして動作させることができません。Event Adapter コンポーネントをアンインストールしてから、IMS コンポーネントのセットアップ作業を実施してください。

2.3　インストール処理を実行する

インストールメディアに収録されているインストーラーを実行し、IMS コンポーネントをインストールします。

1. インストールメディアの ISO イメージをマウントします。

ここでは、インストールメディアのマウントポイントを/media として説明します。別の場所にマウントした場合は、適宜読み替えてください。

2. インストーラーを起動します。

   インストール先の OS に合わせて、以下のコマンドを実行します。

   - Red Hat Enterprise Linux 9 (x86_64)

     ```
     # /media/IMS/Linux/ims-install-rhel9
     ```

   - Red Hat Enterprise Linux 8 (x86_64)

     ```
     # /media/IMS/Linux/ims-install-rhel8
     ```

   ヒント

   - 利用するインストールメディアの種類によって、インストーラーを配置するパスが異なります。WebSAM Media の場合は、以下のパスにインストーラーを収録しています。

     インストールメディア内: /Linux/Tools/NvPRO/IMS/

   - インストーラーの起動後、途中で中止したい場合は、Ctrl+C を入力することで、中止することができます

   ⚠ 注意

   インストール先の OS に対応していないコマンドを実行した場合は、インストール処理が失敗するため注意してください。

   インストーラーの起動後、インストール環境のチェックが行われます。すでにインストール済みの場合は、ここでインストール処理が中止されます。

3. インストールパスを入力します。

   ```
   Input installation path [default: /opt/nec/ims]
    >
   ```

   1 行目の右にはデフォルト値が表示されます。デフォルト値から変更しない場合は、何も入力せずに Enter キーを押します。

4. データパスを入力します。

   ```
   Input data installation path [default: /opt/nec/ims]
    >
   ```

   1 行目の右にはデフォルト値が表示されます。デフォルト値から変更しない場合は、何も入力せずに Enter キーを押します。

5. IMS コンポーネントに組み込むアプリケーションを選択します。

   ```
   Install application of WebSAM NetvisorPro V? (y/[N]): y
   Install application of WebSAM Network Flow Analyzer? (y/[N]): y
   ```

   組み込むアプリケーションに対し y を入力し Enter キーを押します。

ヒント

- IMS コンポーネントにアプリケーションを組み込んでいない場合は、IMS コンポーネントとそれに対応する製品との接続を行うことはできません。
- 必要なアプリケーションの選択をし忘れてしまった場合は、IMS コンポーネントのインストール後に、ims-app コマンドを用いて組み込みます。ims-app コマンドの詳細は、「A.4　ims-app（91 ページ）」を参照してください。

  アプリケーションファイルの格納先は以下になります。

  インストールメディア内: /IMS/Linux/app 配下

6. インストールを開始します。

   設定した各パラメーターが表示されます。内容に間違いがなければ、y を入力し Enter キーを押してインストールを開始します。n を入力すると、再度、パラメーターを入力するプロンプトが表示され、内容を修正することができます。

```
----- Confirmation -----------------------------------------
Installation path      : /opt/nec/ims
Data installation path : /opt/nec/ims
Applications           : WebSAM NetvisorPro V
                       : WebSAM Network Flow Analyzer
------------------------------------------------------------

Is it OK to install? (y/[N]): y
```

⚠ 注意

開始後は、Ctrl+C などで処理を中断しないでください。

次のメッセージが表示されれば、インストール処理は完了です。

```
Installing package ...... done
```

インストール処理の途中でエラーメッセージが表示された場合は、「C.1　インストーラー実行時のエラーと対策（109 ページ）」を参照し、対処を行ってください。

2.4　製品接続のための設定を行う

Web コンソールでの運用を行うためには、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させる必要があります。

IMS コンポーネントと各製品とを接続するためには、双方で接続のための設定を行います。ここでは、IMS コンポーネント側の設定について説明します。

IMS コンポーネントでの設定は、「2.2.1　セットアップパラメーターの設計を行う（13 ページ）」で準備したパラメーターを元に、以下の設定ファイル (ims-conf.ini) の内容を変更し、上書きして保存します。

設定ファイルのパス

<%データパス%>/conf/ims-conf.ini

ヒント

設定ファイル (ims-conf.ini) の変更内容は、サービスの起動時に反映されます。

設定ファイル (ims-conf.ini) に対し行う設定は以下の通りです。

- 「リージョングループに関するパラメーター設定（22 ページ）」

  接続する製品をグルーピングするリージョングループの設定を行います。

- 「製品の接続に関する共通のパラメーター設定（23 ページ）」

  接続する製品を識別するための設定を行います。

- 「NetvisorPro との接続のためのパラメーター設定（23 ページ）」

  NetvisorPro 固有の設定を行います。

- 「NFA との接続のためのパラメーター設定（24 ページ）」

  NFA 固有の設定を行います。

- 「シングルサインオンのためのパラメーター設定（25 ページ）」

  IMS コンポーネントが提供する Web コンソールから、接続する製品の Web コンソールにシングルサインオンでアクセスするための設定を行います。

具体的な設定内容については、以下に示します。

⚠ 注意

各パラメーターにおいて、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。

リージョングループに関するパラメーター設定

リージョングループに関するパラメーターに対する指定形式を以下に示します。

```
noms.core.regions.<region id>.name = <region name>
```

<region id>

リージョングループに対する ID を指定します。「製品接続の設定に必要な共通パラメーター（13 ページ）」で準備した[**region id**]パラメーターを指定します。

<region name>

[**region id**]パラメーターに対応するリージョングループの名前を指定します。「製品接続の設定に必要な共通パラメーター（13 ページ）」で準備した[**region name**]パラメーターを指定します。

設定例:

```
noms.core.regions.tokyo.name = 東京
```

上記の例では、「tokyo」という ID に、「東京」という名前を指定しています。

製品の接続に関する共通のパラメーター設定

各製品と接続するための共通的なパラメーターに対する指定形式を以下に示します。

```
noms.<type>.managers.<manager id>.name = <manager host name>
noms.<type>.managers.<manager id>.region-id = <region id>
```

<type>

接続する製品の種別を以下のように指定します。

- NetvisorPro の場合: nvp
- NFA の場合: nfa

<manager id>

接続する製品を識別するための ID を指定します。「製品接続の設定に必要な共通パラメーター（13 ページ）」で準備した[**manager id**]パラメーターを指定します。

<manager host name>

[**manager id**]パラメーターに対応するホスト名を指定します。「製品接続の設定に必要な共通パラメーター（13 ページ）」で準備した[**manager host name**]パラメーターを指定します。

<region id>

指定した[**manager id**]パラメーターに対応する製品を所属させるリージョングループの ID ([**region id**]パラメーター) を指定します。

設定例:

```
noms.nvp.managers.nvpro01.name = NetMgr01
noms.nvp.managers.nvpro01.region-id = tokyo
```

```
noms.nfa.managers.nfa01.name = FlowMgr01
noms.nfa.managers.nfa01.region-id = tokyo
```

上記の例では、ホスト名「NetMgr01」の NetvisorPro に、「nvpro01」という ID を割り当て、ホスト名「FlowMgr01」の NFA に、「nfa01」という ID を割り当てています。また、それぞれを「tokyo」という ID のリージョングループに所属させるように指定しています。

NetvisorPro との接続のためのパラメーター設定

NetvisorPro との接続で必要なパラメーターに対する指定形式を以下に示します。

```
noms.nvp.managers.<manager id>.ip-address = <manager ip address>
```

<manager id>

設定対象の NetvisorPro を示す ID ([**manager id**]パラメーター) を指定します。

<manager ip address>

NetvisorPro のマネージャ機能をインストールするサーバーの IPv4 アドレスを指定します。「NetvisorPro との接続に必要なパラメーター（14 ページ）」で準備した[**manager ip address**]パラメーターを指定します。

NetvisorPro のマネージャ機能をクラスタシステムにインストールしている場合は、クラスタシステムのフローティング IP を指定します。

IMS コンポーネントは、NetvisorPro の制御のため、NetvisorPro の Web API を利用します。NetvisorPro 側の Web API のパラメーターをデフォルト値から変更する場合は、以下の指定を追加で行います。

```
noms.nvp.managers.<manager id>.webapi-port = <webapi port number>
noms.nvp.managers.<manager id>.webapi-use-ssl = <true|false>
```

<webapi port number>

デフォルト値からの変更後の Web API の通信ポート番号を指定します。「NetvisorPro との接続に必要なパラメーター（14 ページ）」で準備した通信ポート番号を指定します。

<true|false>

Web API における HTTPS 通信の利用有無を以下のように指定します。

- true : HTTPS を利用します。
- false : HTTPS は利用せず、HTTP を利用します。

「NetvisorPro との接続に必要なパラメーター（14 ページ）」で準備した内容を指定します。

設定例:

```
noms.nvp.managers.nvpro01.ip-address = 192.168.1.100
noms.nvp.managers.nvpro01.webapi-port = 20110
noms.nvp.managers.nvpro01.webapi-use-ssl = true
```

上記の例では、ID 「nvpro01」の NetvisorPro の IPv4 アドレスとして「192.168.1.100」を指定しています。また、Web API の利用においては、「HTTPS」を用いて、通信ポート「20110」で通信するように指定しています。

NFA との接続のためのパラメーター設定

NFA との接続で必要なパラメーターに対する指定形式を以下に示します。

```
noms.nfa.managers.<manager id>.url = <nfa web url>
```

<manager id>

設定対象の NFA を示す ID ([**manager id**]パラメーター) を指定します。

<nfa web url>

NFA の Web コンソールにアクセスするための URL を指定します。「NFA との接続に必要なパラメーター（15 ページ）」で準備した[**nfa web url**]パラメーターを指定します。

設定例:

```
noms.nfa.managers.nfa01.url = https://nfa01.nec.com/nfa/
```

上記の例では、ID 「nfa01」の NFA の Web コンソールの URL として「 https://nfa01.nec.com/nfa/ 」を指定しています。

シングルサインオンのためのパラメーター設定

接続製品の Web コンソールへのシングルサインオンアクセスで必要なパラメーターに対する指定形式を以下に示します。

```
ssolite.server.permitted-domains[n] = <web url>/sso-login
```

n

シングルサインオンの設定は、複数指定することができ、設定ごとに「0」からの連番を指定します。

<web url>

接続する製品の Web コンソールの URL を指定します。

設定例:

```
ssolite.server.permitted-domains[0] = https://nfa01.nec.com/nfa//sso-login
ssolite.server.permitted-domains[1] = https://nfa02.nec.com/nfa//sso-login
```

上記の例では、接続する 2 つの NFA に対し、Web コンソールへのシングルサインオンが有効になるように指定しています。

2.5 Web コンソールの通信方式を設定する

Web コンソールへのアクセスにおいては、HTTP 通信、または、HTTPS 通信のいずれかを選択することができます。

IMS コンポーネントのインストール直後のデフォルトの設定では、HTTP 通信を利用する設定になっています。

HTTPS 通信を利用する場合は、以下の設定を行う必要があります。

- HTTPS 通信を有効するための設定ファイル (ims-conf.ini) の更新
- SSL サーバー証明書の準備

ヒント

Web コンソールへのアクセスにおいて、HTTP 通信を利用する場合は、特別な設定はありません。

2.5.1　HTTPS 通信を有効にする

Web コンソールへのアクセスにおいて、HTTPS 通信を用いる場合の設定ファイルの指定方法について説明します。

Web コンソールへのアクセスにおいて、HTTPS 通信を用いる場合は、設定ファイル (ims-conf.ini) の内容を変更し、上書きして保存します。

設定ファイルのパス

<%***データパス***%>/conf/ims-conf.ini

指定形式

以下にパラメーターの指定形式を示します。

```
noms.tomcat.http.enabled = <true|false>
```

```
noms.tomcat.https.enabled = <true|false>
```

以下のように指定することで、HTTP 通信が無効になり、HTTPS 通信が有効になります。

```
noms.tomcat.http.enabled = false
```

```
noms.tomcat.https.enabled = true
```

ヒント

- SSL サーバー証明書の準備の際に用いる `ims-ssl-keytool genkeypair` コマンドを実行すると、ims-conf.ini ファイル内の noms.tomcat.https.enabled の設定値が、自動で「true」に書き換えられます。
- 設定ファイル (ims-conf.ini) の変更内容は、サービスの起動時に反映されます。

2.5.2　SSL サーバー証明書を準備する

HTTPS を用いて Web コンソールにアクセスする場合は、SSL サーバー証明書を準備する必要があります。

SSL サーバー証明書には、次の 2 種類があります。

- 自己署名証明書
- 公的な認証局に発行してもらう証明書

また、Java keytool などを使って、他で作成した証明書を流用して使用することもできます。

それぞれの場合の準備手順を説明します。

- 「2.5.2.1　自己署名証明書を準備する（27 ページ）」
- 「2.5.2.2　公的な認証局が発行する証明書を準備する（28 ページ）」
- 「2.5.2.3　他で作成した証明書を使用する（30 ページ）」

⚠ 注意

サポートする証明書の形式は、Java keytool で扱える形式と同等の、X.509 形式の証明書です。この形式は多くの認証局がサポートしている形式ですが、ご利用予定の認証局がサポートしているかどうか、念のため事前に確認してください。

2.5.2.1　自己署名証明書を準備する

SSL サーバー証明書として、自己署名証明書を作成する手順を説明します。

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（86 ページ）」を参照してください。

作成した証明書は、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、インポートします。

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-ssl-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 server domain name? (FQDN)
  [ims.nec.com]:
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=ims.nec.com, OU=IT Operation Division,
 O=NEC Corporation, L=Minato-ku, ST=Tokyo, C=JP correct?
  [No]:  yes
```

ヒント

- `ims-ssl-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.1　ims-ssl-keytool（86 ページ）」を参照し、オプション引数を指定してください。

  鍵のアルゴリズムを ECDSA、鍵のサイズを 256bit に設定する場合の実行例:

```
# cd /opt/nec/ims/bin
# ./ims-ssl-keytool genkeypair -keyalg EC -keysize 256
```

- 鍵の内容を変更して再度作成するには、`ims-ssl-keytool delete` コマンドを実行してから再度 `ims-ssl-keytool genkeypair` コマンドを実行します。

  コマンドの詳細は、「A.1　ims-ssl-keytool（86 ページ）」を参照してください。

作成された証明書は、自己署名された状態になります。

2. 次のコマンドを実行し、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>
```

<*filename*>には任意のファイル名を指定できますが、Web ブラウザー側で簡単に証明書をインポートするために、ファイルの拡張子に`.cer` を指定することを強く推奨します。

コマンドの実行に成功すると、指定したファイルにバイナリー符号化方式の証明書が出力されます。

`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、「3.1.2　Web ブラウザーに SSL サーバー証明書をインポートする（48 ページ）」を参照してください。

2.5.2.2　公的な認証局が発行する証明書を準備する

SSL サーバー証明書として、公的な認証局に署名済み証明書を発行してもらう手順を説明します。

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（86 ページ）」を参照してください。

サポートする証明書の形式は、Java keytool で扱える形式と同等の、X.509 形式の証明書です。この形式は多くの認証局がサポートしている形式ですが、ご利用予定の認証局がサポートしているかどうか、念のため事前に確認してください。

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-ssl-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 server domain name? (FQDN)
  [ims.nec.com]:
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=ims.nec.com, OU=IT Operation Division,
 O=NEC Corporation, L=Minato-ku, ST=Tokyo, C=JP correct?
  [No]:  yes
```

ヒント

- `ims-ssl-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.1　ims-ssl-keytool（86 ページ）」を参照し、オプション引数を指定してください。

  鍵のアルゴリズムを ECDSA、鍵のサイズを 256bit に設定する場合の実行例:

  ```
  # cd /opt/nec/ims/bin
  # ./ims-ssl-keytool genkeypair -keyalg EC -keysize 256
  ```

- 鍵の内容を変更して再度作成するには、`ims-ssl-keytool delete` コマンドを実行してから再度 `ims-ssl-keytool genkeypair` コマンドを実行します。

  コマンドの詳細は、「A.1　ims-ssl-keytool（86 ページ）」を参照してください。

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-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。

3. 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。

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-ssl-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、認証局にお問い合わせください。

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-ssl-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-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。

IMS コンポーネント側の証明書の準備は、これで完了です。

使用する認証局によっては、Web ブラウザー側に別途、認証局の証明書をインポートするなどの作業が必要となる場合があります。詳細は、認証局の指示に従ってください。

2.5.2.3　他で作成した証明書を使用する

SSL サーバー証明書として、他で作成した証明書を流用して使用する手順を説明します。

事前に PKCS12 形式のキーストアを準備し、キーストア内に有効な鍵と証明書を作成しておいてください。また、準備したキーストアのファイルは、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配置しておいてください。

1. 次のテキストファイルを開きます。

   <%データパス%>/conf/ims-conf.ini

2. 以下の内容を ims-conf.ini ファイルに記載します。

```
noms.tomcat.https.keyAlias = 鍵を含むエントリの別名
noms.tomcat.https.keystoreFile = キーストアファイルの絶対パス
noms.tomcat.https.keystorePass = キーストアのパスワード
```

⚠ 注意

- パラメーター noms.tomcat.https.keystoreFile の記載における注意事項
  - 記載するパスに半角スペースが含まれる場合でも、シングルクォーテーション(')やダブルクォーテーション(")でパスを囲う必要はありません。

  記述例：

  ```
  noms.tomcat.https.keystoreFile = /path to/keystore.jks
  ```

- ims-conf.ini ファイルに、外部のキーストアを使用する設定を記載した場合、`ims-ssl-keytool` コマンドは使用できなくなります。代わりに、Java keytool コマンドなどを直接使用して管理してください。

  Java keytool コマンドは、IMS コンポーネントと共にインストールされます。

  `<%`***インストールパス***`%>/jre/bin/keytool`

自己署名証明書の場合などは、バイナリー符号化形式の証明書 (.cer) を出力し、Web ブラウザーにインポートしてください。

2.6　通信ポート番号をデフォルト値から変更する

IMS コンポーネントが利用するポート番号を、デフォルト値から変更する場合の設定ファイルの指定方法について説明します。

「2.2.1　セットアップパラメーターの設計を行う（13 ページ）」において、IMS コンポーネントで利用するポート番号をデフォルト値から変更する判断を行った場合は、以下の内容に従って、変更対象の通信ポートに対応した設定ファイルを変更し、上書きして保存します。

ヒント

通信ポート番号をデフォルト値のまま運用する場合は、本作業を行う必要はありません。

表 2-12　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`

用途	指定形式
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を行います。詳細は、「2.11　接続製品のセットアップを行う（41 ページ）」に示します。
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

用途	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。

ヒント

各設定ファイルの変更内容は、サービスの起動時に反映されます。

2.7　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。

ヒント

SystemManager G との連携を行わない場合は、本作業を行う必要はありません。

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。

ここへは、「SystemManager G との連携に必要なパラメーター（18 ページ）」で準備した[**manager id**]を指定します。

<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。

ここへは、「SystemManager G との連携に必要なパラメーター（18 ページ）」で準備した[**manager name**]を指定します。

<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。

ここへは、「SystemManager G との連携に必要なパラメーター（18 ページ）」で準備した[**manager host name**]を指定します。

<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。

ここへは、「SystemManager G との連携に必要なパラメーター（18 ページ）」で準備した[**webapi port number**]を指定します。

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。

ここへは、「SystemManager G との連携に必要なパラメーター（18 ページ）」で準備した[**url scheme**]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。

ここへは、「SystemManager G との連携に必要なパラメーター（18 ページ）」で準備した[**compatible mode**]を指定します。

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。

ヒント

設定ファイル (ims-conf.ini) の変更内容は、サービスの起動時に反映されます。

2.8　ファイアウォールの設定を変更する

IMS コンポーネントが利用する通信ポートを、ファイアウォールによってブロックされないように、ファイアウォールの設定を変更します。

IMS コンポーネントが利用する通信ポートのデフォルト値は、「表 2-13 通信ポート番号一覧 (外部通信)（36 ページ）」、「表 2-14 通信ポート番号一覧 (内部通信)（36 ページ）」の通りです。

「2.6　通信ポート番号をデフォルト値から変更する（31 ページ）」の手順により、利用する通信ポート番号を変更している場合は、通信ポート番号を適宜読み替えてください。

表 2-13　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。 デフォルトでは、HTTP 通信が有効になっています。
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。 デフォルトでは、HTTPS 通信は無効になっています。
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 2-14　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がファイアウォールによってブロックされないよう、ファイアウォールの設定内容を確認し、必要に応じて、設定を変更します。

ヒント

ここでのファイアウォールとは、以下の 2 つのことを指します。

- IMS コンポーネントをインストールしたサーバー上のパーソナルファイアウォール
- 通信経路上のファイアウォール

2.9　インストール環境への追加の設定を行う

IMS コンポーネントのインストール環境に対して行う、追加の設定について説明します。

2.9.1　通報時および SAML 認証に用いる URL を設定する

通報処理および SAML 認証で用いる Web コンソールの URL の設定について説明します。

Web コンソールは以下の用途で、Web コンソールの URL を使用します。

- 通報処理

  Web コンソールでは、接続する製品が検知したイベント(アラート)を契機に、メールやコマンドでの通報を行う仕組み(イベントアクション機能)を提供しています。この機能の中で、検知したイベントの詳細情報を示す画面(イベント詳細画面)の URL を通知することができます。詳細は、「WebSAM Network Management Web コンソール リファレンスマニュアル」を参照してください。

- SAML 認証

  Web コンソールでは、IdP と連携し認証を行う SAML 認証機能を提供しています。SAML 認証では Web コンソールの URL を設定することで、IdP との認証情報の連携が行えます。

ここでは、通報処理および SAML 認証で用いる Web コンソールの URL を設定します。

⚠ 注意

- 通報時にイベント詳細画面の URL を通知する場合は、通報を受け取った場所からアクセス可能な URL を指定する必要があります。
- SAML 認証を利用する場合は、IdP からアクセス可能な URL を指定する必要があります。

Web コンソールの URL 設定は、以下の設定ファイル (ims-conf.ini) の内容を変更し、上書きして保存します。

設定ファイルのパス

<%***データパス***%>/conf/ims-conf.ini

指定形式

以下にパラメーターの指定形式を示します。

```
noms.core.url.external-base-url = <base url>
```

設定例:

```
noms.core.url.external-base-url = http://ims.nec.com
```

ヒント

設定ファイル (ims-conf.ini) の変更内容は、サービスの起動時に反映されます。

2.9.2 データ分析用のデータ保持期間をデフォルト値から変更する

アノマリー分析、および、トレンド分析の利用において、蓄積するデータの保持期間をデフォルト値から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. 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。

ヒント

保持期間の変更内容は、サービスの起動時に反映されます。

⚠ 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。

2.9.3　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. 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。

ヒント

保持期間の変更内容は、サービスの起動時に反映されます。

2.9.4　Web サーバーのログを自動削除する設定を行う

IMS コンポーネントに含まれている Web サーバーのログを、定期的に自動削除するための設定について説明します。

Web コンソールのアクセスログは、以下のディレクトリに蓄積されます。このログについては、自動での削除は行われません。必要に応じて、「cron」などを利用して、古いログを自動的に削除するように設定してください。

- <%*インストールパス*%>/tomcat/logs/localhost_access_log.*yyyy-mm-dd*.txt

yyyy-mm-dd は、Web サーバーの日付を表します。例えば、localhost_access_log.2018-10-31.txt は、2018/10/31 の Web コンソールに対するアクセスログファイルです。

設定例

以下は、30 日以上経過したログファイルを、毎日深夜 1 時にチェックして削除する cron 設定の例です。

```
0 1 * * *    /usr/bin/find /opt/nec/ims/tomcat/logs/
   -type f -regex '^.*\.[0-9]+-[0-9]+-[0-9]+\.txt$'
   -mtime +30 -exec /bin/rm -f {} \;
```

cron の設定に関する詳細は、OS の提供するマニュアルを参照してください。

2.9.5　ウイルス対策ソフトウェアの設定を変更する

IMS コンポーネントをインストールしたサーバーに、ウイルス対策ソフトウェアをインストールしている場合は、IMS コンポーネントの動作に影響を与えないように、ウイルス対策ソフトウェアの設定を見直す必要があります。

IMS コンポーネントは動作の際、インストールパス、および、データパスとして指定したディレクトリ配下に対し、ファイルの読み込み、書き込み等を実施します。また、サーバー外部に配置する WebSAM のネットワーク運用管理製品と接続して通信を行います。

共存するウイルス対策ソフトウェアが、この動作のいずれかを阻害する場合、Web コンソールでの運用を適切に行うことができません。必ず、共存するウイルス対策ソフトウェアの仕様を確認し、必要に応じて、IMS コンポーネントの動作を阻害しないように設定を見直してください。

2.10　IMS コンポーネントのサービスを起動する

ここまでのセットアップ作業が適切に行えていれば、IMS コンポーネントのサービスを起動することができます。

IMS コンポーネントのサービスは、起動コマンド (systemctl) を実行するか、OS の再起動によって起動することができます。

ここでは、起動コマンドを実行してサービスを起動する方法について説明します。

1. root ユーザーでサーバーにログインします。
2. サービス起動のためのコマンドを実行します。

```
# systemctl start nec-ims
```

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。

正常に起動できなかったプロセスは、[OK]の代わりに[NG]と表示されます。

3. デーモンプロセスの起動状態を確認します。

しばらく時間をあけ、デーモンプロセスが起動し続けているかを以下のコマンドで確認します。

```
# <%インストールパス%>/bin/ims-ctl status
```

すべてのデーモンプロセ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...
```

すべてのデーモンプロセ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
```

2.11　接続製品のセットアップを行う

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させるためには、IMS コンポーネントと接続する各製品側でもセットアップ作業が必要になります。

IMS コンポーネントと接続する製品側での接続設定は、各製品によって手順が異なります。運用環境に合わせて、製品ごとの説明を確認してください。

2.11.1　NetvisorPro の接続設定を行う

IMS コンポーネントと NetvisorPro とを接続させるために実施する、NetvisorPro 側の設定方法について説明します。

設定は、NetvisorPro のセットアップ後に追加で行います。NetvisorPro のセットアップ作業については、NetvisorPro の各環境に対する「セットアップガイド」を参照し、実施してください。

NetvisorPro では、以下の設定を行います。

- 設定ファイル (NvPROIms.ini) の更新
- Web API 通信の有効化

設定ファイルの更新

NetvisorPro をインストールすると、設定ファイル (NvPROIms.ini) が作成されます。この設定ファイルの内容を更新し、上書きして保存します。

- 設定ファイルのパス

  `NetvisorPro の<%データパス%>/Manager/sg/NvPRO/NvPROIms.ini`

- 指定形式

```
[NOMS]
InstanceID=<manager id>
MessageQueueIP=<ims ip address>
MessageQueuePort=<port number>
[EVENT]
sendEvent=<1|0>
```

<manager id>

IMS コンポーネントが、接続する NetvisorPro を識別するための ID を指定します。「製品接続の設定に必要な共通パラメーター（13 ページ）」で準備した[**manager id**]パラメーターの値を指定します。

デフォルト値は空です。

本パラメーターは、「2.4　製品接続のための設定を行う（21 ページ）」で実施した IMS コンポーネント側の設定ファイル (ims-conf.ini) の設定値と一致させる必要があります。

<ims ip address>

IMS コンポーネントをインストールするサーバーの IPv4 アドレスを指定します。「製品接続の設定に必要な共通パラメーター（13 ページ）」で準備した[**ims ip address**]パラメーターの値を指定します。

デフォルト値は、「127.0.0.1」が指定されています。

<port number>

IMS コンポーネントの Message Queue との通信で利用する通信ポート番号を指定します。

デフォルト値は、「28110」が指定されています。

本パラメーターは、「2.6　通信ポート番号をデフォルト値から変更する（31 ページ）」でデフォルトの通信ポート番号を変更した場合に、修正が必要になります。

<1|0>

NetvisorPro で検出したアラート情報を IMS コンポーネントに通知するかどうかを以下のように指定します。

- 1 : アラート情報を通知します。基本的には、「1」を指定します。
- 0 : アラート情報を通知しません。

デフォルト値は、「1」が指定されています。

設定例:

```
InstanceID=nvpro01
MessageQueueIP=192.168.1.200
MessageQueuePort=28110
[EVENT]
sendEvent=1
```

ヒント

設定ファイル (NvPROIms.ini) の以下のパラメーターについては、修正する必要はありません。

```
[SnmpDataDb]
Port=28100
ShiftTimeZone=+0900
```

- [**Port**]

  Performance Database で設定している通信ポート番号と一致した値を指定します。通常、設定値を変更することはありません。

- [**ShiftTimeZone**]

  本パラメーターは、UTC (協定世界時) に対する時差を指定します。日本国内で運用する場合は、「+0900」 (+9 時間)であるため、修正の必要はありません。

⚠ 注意

設定ファイル (NvPROIms.ini) の更新内容を反映させるためには、NetvisorPro 関連のすべてのサービスを再起動する必要があります。

Web API 通信の有効化

IMS コンポーネントから NetvisorPro の Web API を利用できるように、NetvisorPro の Web API 通信を有効化します。

本設定は、NetvisorPro の監視端末から以下のように実施します。

1. 定義モードに遷移します。

   メインメニューの [**設定**] >[**定義モード**] メニューをクリックします。

2. オプション設定ダイアログを表示します。

   メインメニューの [**設定**] >[**オプション**] メニューをクリックします。

   オプション設定ダイアログが表示されます。

3. [**Web 監視画面機能**]タブをクリックします。
4. Web API 通信を有効化します。

   [**Web API 機能を使用する**]チェックボックスをオンにします。
5. Web API 関連のパラメーター値を変更します。

   デフォルト値から変更を行う場合は、「2.4　製品接続のための設定を行う（21 ページ）」での IMS コンポーネントの設定ファイル (ims-conf.ini) の指定内容と一致した値を指定してください。

   - [**ポート番号**]

     Web API の通信ポート番号を指定します。
   - [**HTTPS で暗号化する**]チェックボックス
     - オン : HTTPS を利用します。
     - オフ : HTTPS は利用せず、HTTP を利用します。
6. [**OK**]ボタンをクリックして、設定内容を保存します。

2.11.2　NFA の接続設定を行う

IMS コンポーネントと NFA とを接続させるために実施する、NFA 側の設定方法について説明します。

設定は、NFA のセットアップ後に追加で行います。NFA のセットアップ作業については、NFA の「スタートアップガイド」を参照し、実施してください。

NFA では、以下の設定を行います。

- IMS コンポーネントと NFA との接続設定
- IMS の Web コンソールから NFA の Web コンソールをシングルサインオンで起動するための設定

上記の設定は、NFA の以下の設定ファイル (controller.properties) を更新することで行います。

設定ファイルのパス

`NFA の<%データパス%>/controller/conf/controller.properties`

⚠ 注意

- 設定ファイル (controller.properties) が存在しない場合は、新規に作成してください。
- 設定ファイル (controller.properties) の更新内容を反映させるためには、NFA のサービスを再起動する必要があります。

接続設定の指定形式

設定ファイル (controller.properties) の以下のパラメーターを編集し、上書きして保存します。

```
ims.application-instance-id = <manager id>
ims.msgqueue.host = <ims ip address>
ims.msgqueue.port = <port number>
```

<manager id>

IMS コンポーネントが、接続する NFA を識別するための ID を指定します。「製品接続の設定に必要な共通パラメーター（13 ページ）」で準備した[**manager id**]パラメーターの値を指定します。

デフォルト値は、未定義になっています。

本パラメーターは、「2.4　製品接続のための設定を行う（21 ページ）」で実施した IMS コンポーネント側の設定ファイル (ims-conf.ini) の設定値と一致させる必要があります。

<ims ip address>

IMS コンポーネントをインストールするサーバーの IPv4 アドレスを指定します。「製品接続の設定に必要な共通パラメーター（13 ページ）」で準備した[**ims ip address**]パラメーターの値を指定します。

デフォルト値は、「127.0.0.1」が指定されています。

<port number>

IMS コンポーネントの Message Queue との通信で利用する通信ポート番号を指定します。

デフォルト値は、「28110」が指定されています。

本パラメーターは、「2.6　通信ポート番号をデフォルト値から変更する（31 ページ）」でデフォルトの通信ポート番号を変更した場合に、修正が必要になります。

設定例:

```
ims.application-instance-id = nfa01
ims.msgqueue.host = 192.168.1.200
ims.msgqueue.port = 28110
```

シングルサインオン設定の指定形式

設定ファイル (controller.properties) の以下のパラメーターを編集し、上書きして保存します。

```
ims.webserver.base-url = <ims web url>
ims.sso.enabled = <true|false>
```

<ims web url>

IMS コンポーネントが提供する Web コンソールにアクセスするための URL を指定します。「NFA との接続に必要なパラメーター（15 ページ）」で準備した[**ims web url**]パラメーターの値を指定します。

デフォルト値は、「http://localhost」が指定されています。

⚠ 注意

本パラメーターは、ブラウザー側および NFA 側からアクセス可能な URL を指定する必要があります。

<true\|false>

シングルサインオンの動作を有効にするかどうかを以下のように指定します。

- true : シングルサインオンの動作を有効にします。
- false : シングルサインオンの動作を無効にします。

デフォルト値は、「false」が指定されています。IMS コンポーネントとの接続時においては、「true」を指定します。

設定例:

```
ims.webserver.base-url = http://ims.nec.com
ims.sso.enabled = true
```

第 3 章
運用開始前の準備

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

3.1　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。

3.1.1　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（48 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。

3.1.2　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（86 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。

3.2　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。

事前に「3.1　Web コンソールを使用するための準備を行う（48 ページ）」に記載の、Web ブラウザーの設定を行っておく必要があります。

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。

   初期ユーザー名は「admin」、初期パスワードは「password」です。

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、admin ユーザーの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。

3.3　ユーザーを登録する

Web コンソールの利用には、アクセスするためのユーザー登録が必要です。

ここでは、ユーザー管理の概要と、ユーザー登録の手順について説明します。

3.3.1　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。

3.3.2　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、「3.3.1　グループとユーザー（51 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。

3.3.3　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。

3.4　構成情報の同期を行う

Web コンソールを用いて運用を開始する前に、IMS コンポーネントに管理対象ノードの情報を適切に登録しておく必要があります。

IMS コンポーネントと各製品を接続する前に、製品側において管理対象ノードの情報を登録していた場合は、構成情報の同期を実施する必要があります。構成情報の同期は、Web コン

ソールの構成情報同期画面で実施することができます。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 3-1　構成情報同期画面

構成情報同期画面の製品インスタンス一覧の[**同期**]ボタンをクリックすることで、対象製品の構成情報の同期を行うことができます。

構成情報同期の詳細については、「リファレンスマニュアル」の「構成情報を同期する」を参照してください。

初回の同期処理の完了後は、IMS コンポーネントと各製品とが接続した状態にあれば、各製品側で行った構成情報の更新操作(ノード追加やプロパティ更新)の内容が、適切に IMS コンポーネントに自動反映されます。

3.5　管理対象のノード情報を確認する

Web コンソールを用いて運用を開始する前に、IMS コンポーネントに管理対象ノードの情報が、適切に登録されていることを確認しておく必要があります。

IMS コンポーネントに登録された管理対象ノードの情報は、Web コンソールのノード一覧画面で確認することができます。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。

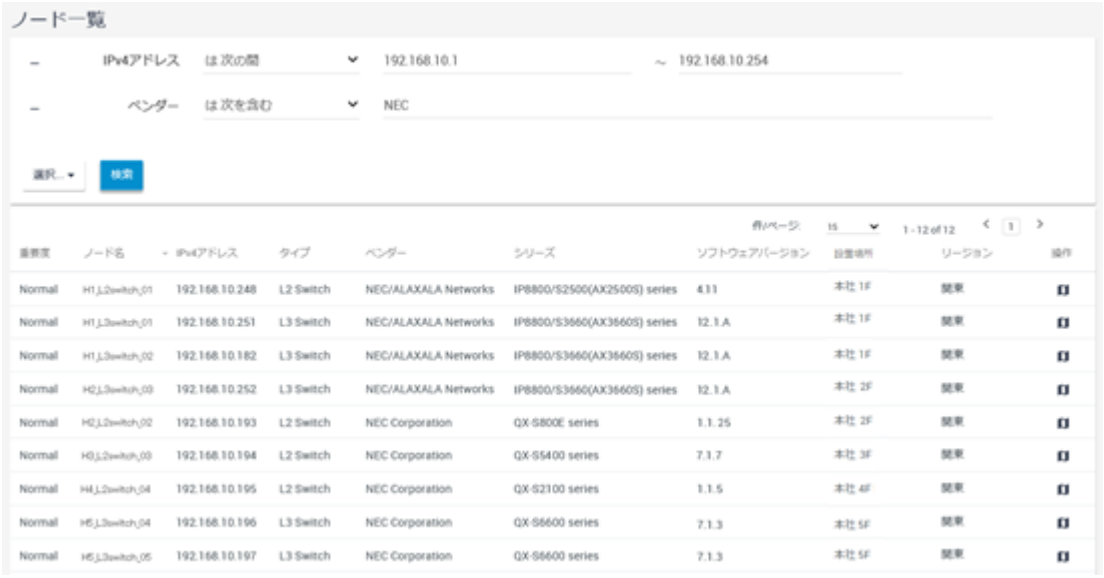

図 3-2　ノード一覧画面

セットアップ作業の関係で、IMS コンポーネントのサービスを停止した状態で、各製品での構成情報の更新作業を実施した場合は、IMS コンポーネントに正しく構成情報が反映されません。このような場合は、再度、構成情報の同期を行います。

構成情報の同期については、「リファレンスマニュアル」の「構成情報を同期する」を参照してください。

ヒント

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、各製品で管理するノードが、物理的に同一のノードかどうかを自動で判断します。

同一ノードの判定方法の詳細については、「リファレンスマニュアル」の「ノード情報のマッピング」を参照してください。

3.6　トポロジーマップの構成を確認する

Web コンソールを利用する前に、トポロジーマップの構成が適切かを確認し、必要に応じて編集する必要があります。

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。

ヒント

- トポロジーマップ画面は、NetvisorPro を利用している場合にのみ、表示することができます。そのため、NetvisorPro を利用していない場合は、本作業を行う必要はありません。
- マップに配置するノードのアイコン位置を、上記の編集作業により決定していない場合は、Web コンソールが表示処理の際に、適切なアイコン位置を自動算出します。そのため、NetvisorPro 側で新たなノードのアイコンを登録すると、それまでのアイコン配置と異なる表示になる場合があります。

第 4 章
基本操作

Web コンソールの基本的な操作について説明します。

目次

4.1　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 4-1 Web コンソールの画面構成（59 ページ）」で示す 4 つの領域で構成されています。

図 4-1　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。

4.2　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。

4.3　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。

4.4　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 4-2 折れ線グラフ表示タイプのウィジェット（65 ページ）」に示します。

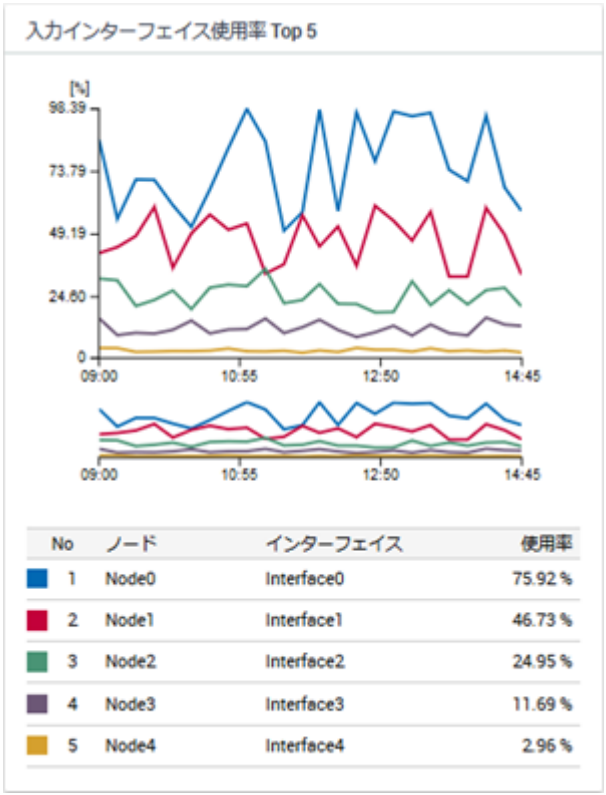

図 4-2　折れ線グラフ表示タイプのウィジェット

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 4-3 円グラフ表示タイプのウィジェット（66 ページ）」に示します。

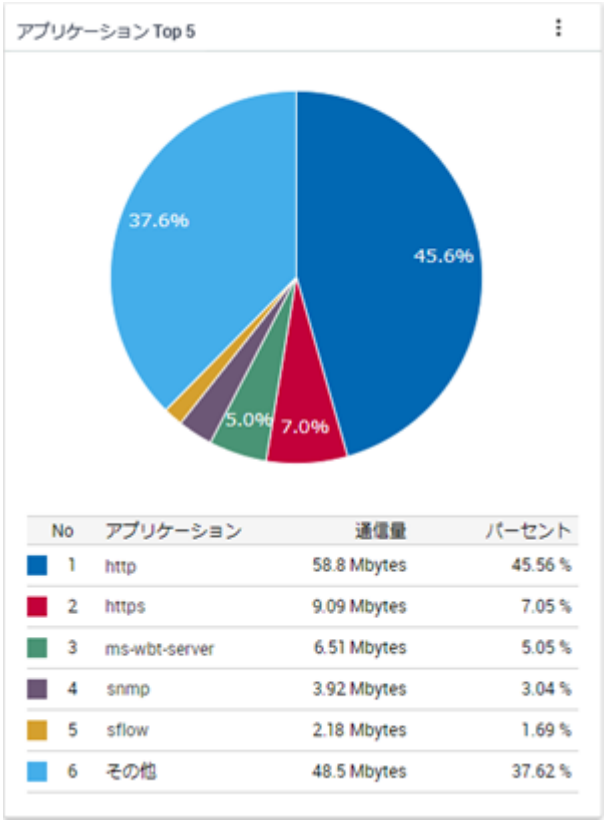

図 4-3　円グラフ表示タイプのウィジェット

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 4-4 一覧表示タイプのウィジェット（67 ページ）」に示します。

図 4-4　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 4-5 その他の表示タイプのウィジェット（68 ページ）」に示します。

図 4-5　その他の表示タイプのウィジェット

4.5　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

4.6　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。

4.6.1　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。

4.6.2　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。

4.6.3　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。

4.6.4　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。

4.6.5　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。

4.6.6　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。

4.6.7　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。

4.7　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。

4.7.1　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。

4.7.1.1　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。

   - [**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。

4.7.1.2　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。

4.7.1.3　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。

4.7.2　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 5 章
IMS コンポーネントのアップグレード

Web コンソールを利用する際に必要な IMS コンポーネントをアップグレードする手順について説明します。

目次

5.1　アップグレードする

インストールメディアに収録されているインストーラーを実行し、IMS コンポーネントをアップグレードします。アップグレードにより、古いバージョンから最新バージョンへ更新されます。

⚠ 注意

バージョンアップに伴い、必須パッケージが追加になっている場合があります。「1.2.3　システム要件（9 ページ）」の内容を確認し、事前に必要なパッケージのインストールを行っておいてください。

1. 万が一に備え、事前にバックアップを取得します。

   バックアップは、`ims-backup` コマンドにより取得できます。万が一の場合には、取得したバックアップから、`ims-restore` コマンドを使用することで環境を復元することができます。

   バックアップ・リストア作業の詳細は、「付録 D　運用環境をバックアップ、リストアする（112 ページ）」を参照してください。

2. インストールメディアの ISO イメージをマウントします。

   ここでは、インストールメディアのマウントポイントを`/media` として説明します。別の場所にマウントした場合は、適宜読み替えてください。

3. IMS コンポーネントのサービスを停止します。

```
# systemctl stop nec-ims
```

4. アップグレードインストーラーを起動します。

   インストール先の OS に合わせて、以下のコマンドを実行します。

   - Red Hat Enterprise Linux 9 (x86_64)

```
# /media/IMS/Linux/ims-upgrade-rhel9
```

   - Red Hat Enterprise Linux 8 (x86_64)

```
# /media/IMS/Linux/ims-upgrade-rhel8
```

ヒント

- 利用するインストールメディアの種類によって、インストーラーを配置するパスが異なります。WebSAM Media の場合は、以下のパスにインストーラーを収録しています。

  インストールメディア内: `/Linux/Tools/NvPRO/IMS/`

- インストーラーの起動後、途中で中止したい場合は、`Ctrl+C` を入力することで、中止することができます

⚠ 注意

インストール先の OS に対応していないコマンドを実行した場合は、アップグレード処理が失敗するため注意してください。

インストーラーの起動後、インストール環境のチェックが行われます。古いバージョンがインストールされていない場合や、すでにアップグレード済みの場合は、ここでアップグレード処理が中止されます。

5. アップグレードを開始します。

   アップグレード対象のバージョン情報が表示されます。バージョン番号に間違いがなければ、y を入力し Enter キーを押してアップグレードを開始します。n を入力すると、アップグレードが中止されます。

```
----- Confirmation -----------------------------------------
Version      : 3.1.0.6 -> 3.2.0.6
Applications : WebSAM NetvisorPro V  3.1.0.6 -> 3.2.0.6
               WebSAM Network Flow Analyzer  3.1.0.6 -> 3.2.0.6
------------------------------------------------------------

Is it OK to upgrade? (y/[N]): y
```

⚠ 注意

開始後は、Ctrl+C などで処理を中断しないでください。

次のメッセージが表示されれば、アップグレードの適用は完了です。

```
Upgrading package ... done
```

アップグレード処理の途中でエラーが発生した場合は、エラーメッセージが表示されます。エラーメッセージが表示された場合は、「C.1　インストーラー実行時のエラーと対策（109 ページ）」を参照し、対処を行ってください。

適用後に、IMS コンポーネントのサービスを起動させてください。

```
# systemctl start nec-ims
```

⚠ 注意

IMS 1.0 からのアップグレードの場合は、アップグレードに合わせて、Web ブラウザー上のキャッシュをクリアする必要があります。詳細は、「5.2　Web ブラウザーのキャッシュをクリアする（83 ページ）」を参照してください。

アップグレードを機にアプリケーションを追加したい場合、IMS コンポーネントのアップグレード後に、ims-app コマンドを用いて組み込みます。ims-app コマンドの詳細は、「A.4　ims-app（91 ページ）」を参照してください。

アプリケーションファイルの格納先は以下になります。

インストールメディア内: /IMS/Linux/app 配下

ヒント

アップグレード作業中に問題が発生し、旧バージョンへ切り戻しを行う場合は、以下の手順で行ってください。

1. 一旦、IMS コンポーネントをアンインストールします。
2. 旧バージョンの IMS コンポーネントを再インストールします。
3. 事前に取得したバックアップデータを用いて、リストアを行います。
4. IMS コンポーネントのサービスが正常に起動できることを確認します。

5.2　Web ブラウザーのキャッシュをクリアする

IMS のアップグレード後、使用する Web ブラウザー上のキャッシュをクリアします。

IMS の Web サーバーからダウンロードされる一部のファイルは、表示を高速化するために Web ブラウザー上にキャッシュされます。IMS のアップグレード後、画面が正常に表示されるように、この Web ブラウザー上のキャッシュをクリアしてください。キャッシュのクリアに関する詳細は、各 Web ブラウザーのヘルプを参照してください。

ヒント

Web ブラウザーのキャッシュクリア作業は、IMS 1.0 からのアップグレードの場合のみ必要です。バージョン 1.1 以降からのアップグレードの場合は、キャッシュは自動で破棄されます。

Google Chrome

1. Web ブラウザーの任意の画面で、Ctrl + Shift + Del を同時に押します。
2. [**期間**]を[**全期間**]に設定後、[**キャッシュされた画像とファイル**]の項目をチェックし、キャッシュを削除します。

第 6 章
IMS コンポーネントのアンインストール

IMS コンポーネントをアンインストールする手順について説明します。

目次

6.1　アンインストールにおける注意事項

IMS コンポーネントをアンインストールする際の注意事項について説明します。

- インストールパスとデータパスを分けてインストールしていた場合、アンインストーラーでは、データパスの削除を行いません。別途、手動で削除する必要があります。
- インストールパスとデータパスが同じ場合、アンインストーラーにより、すべてのデータが削除されます。

6.2　アンインストールする

IMS コンポーネントのアンインストール手順について説明します。

1. root ユーザーでログインします。
2. IMS コンポーネントのサービスを停止します。

```
# systemctl stop nec-ims
```

3. IMS コンポーネントをアンインストールします。

```
# rpm -e nec-ims
```

4. インストールパスとデータパスを分けていた場合、データパスを手動で削除します。

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。

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（98 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（99 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（99 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（103 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（106 ページ）」 「B.3.4　IdP で SAML 認証の設定を行う（103 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。

  「2.9.1　通報時および SAML 認証に用いる URL を設定する（37 ページ）」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「2.5　Web コンソールの通信方式を設定する（25 ページ）」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「3.3　ユーザーを登録する（51 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（93 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（93 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（93 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（93 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（102 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（105 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（103 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（93 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

IMS コンポーネントのセットアップ作業中に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　インストーラー実行時のエラーと対策

インストーラー実行時に発生するエラーとその対策を説明します。

Non-root user cannot access the install path

次のようなメッセージが表示された場合、インストールパスに、OS の管理者権限を持たないユーザーがアクセスできないことが原因です。

```
ERROR: Non-root user cannot access the install path: <%インストールパス%>
       Check the permission of the install destination.
```

インストールパスとして指定したディレクトリ、および、その途中のディレクトリについて、OS の管理者権限を持たないユーザーがアクセスできるように、権限の設定変更を行ってください。その後、再度、インストーラーを実行してください。

installing package nec-ims-3.2.0.6-1.x86_64 needs *XXX*MB on the / file system

次のようなメッセージが表示された場合、インストールパスに指定したファイルシステム上の空き容量が足りないか、ファイルシステムが書き込み可能でないことが原因です。

```
Installing package ...... failed
ERROR: Failed to install package: code=1
        installing package nec-ims-3.2.0.6-1.x86_64 needs XXXMB
        on the / file system.
```

インストールパスには、十分な空き容量を持った書き込み可能な場所を指定してください。空き容量を確保した後、再度インストーラーを実行してください。

Failed to initialize data. Directory exists

次のようなメッセージが表示された場合、データパスに指定したディレクトリ中に、インストール時に作成するディレクトリが既に存在していることが原因です。

```
Installing package ...... failed
ERROR: Failed to initialize data.
       ERROR: Directory exists: <%データパス%>/conf
```

`Failed to initialize data` が表示されると、その下に、以下のようなリカバリー用のコマンドが表示されます。

```
Try to run the following command later.
    <%インストールパス%>/bin/ims-init -data <%データパス%>
```

表示されたコマンドを OS の管理者権限を持つユーザーで実行してください。

その他のエラー

上記以外のエラーを表示する場合があります。エラーメッセージと共にリカバリー用のコマンドが表示されている場合は、表示された内容に従い、コマンドを実行して対処してください。

リカバリー用のコマンド表示例:

```
Try to run the following command later.
    <%インストールパス%>/bin/ims-app install
    -silent /media/IMS/Linux/app/nvp.war
```

対処方法が不明なエラーが発生した場合は、NEC カスタマーサポートセンターに問い合わせてください。

C.2　サービス起動時のエラーと対策

IMS コンポーネントのサービス起動時に発生する可能性のあるエラーとその対策を説明します。

インストール直後のサービス起動に失敗した場合

データパスの初期化が、正常に行われていない可能性があります。

次の手順で対処を行ってください。

1. IMS コンポーネントのサービスを停止します。

   ```
   # systemctl stop nec-ims
   ```

2. データパスの状態を確認します。

   以下のコマンドを実行します。

   ```
   # <%インストールパス%>/bin/ims-init -data <%データパス%>
   ```

   データパスのディレクトリが空でない場合、次のようなエラーが表示される場合があります。

   ```
   ERROR: Directory exists: <%データパス%>/conf
   ```

エラーが表示された場合は、表示されたディレクトリを削除し、再度、コマンドを実行してください。

3. 必要に応じて、SSL サーバー証明書を作成します。

   HTTPS を用いて、Web コンソールにアクセスする環境の場合は、「2.5.2　SSL サーバー証明書を準備する（26 ページ）」の手順を実施してください。

4. IMS コンポーネントのサービスを再度、起動します。

```
# systemctl start nec-ims
```

Web サーバーの待ち受けポート 443/tcp が存在しないか LISTEN 状態ではない場合

HTTPS を用いて、Web コンソールにアクセスする環境において、IMS コンポーネントの Web サーバーの待ち受けポート 443/tcp の状態を確認しても、開かれたポートが存在しない場合、SSL 証明書が正常に作成されていない可能性があります。

次の手順で対処を行ってください。

1. SSL サーバー証明書を作成します。

   「2.5.2　SSL サーバー証明書を準備する（26 ページ）」の手順を実施してください。

2. IMS コンポーネントのサービスを再起動します。

```
# systemctl restart nec-ims
```

OS 起動時にサービスが自動で起動しない場合

IMS コンポーネントのサービスを手動で起動することはできるが、OS 起動時に IMS コンポーネントのサービスが自動で起動しない場合、`systemctl` コマンドで自動起動設定が変更されている可能性があります。

OS 起動時の自動起動を有効にしたい場合は、次のコマンドを実行し対処を行ってください。

```
# systemctl enable nec-ims
```

付録 D　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。

D.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（89 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。

D.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、「D.1　運用環境をバックアップする（112 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（90 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。

5. 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。構成情報同期の詳細については、「リファレンスマニュアル」の「構成情報を同期する」を参照してください。

付録 E　SystemManager G 連携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。

E.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、「E.2　互換モードのメッセージフォーマット（117 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 E-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** 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。

プロパティ	通知内容
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（116 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 E-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
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。

E.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 E-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、「E.3　互換モードのメッセージフォーマットを変更する（120 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（119 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 E-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 E-5 パラメーター(置換文字列)の説明（120 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、「E.3　互換モードのメッセージフォーマットを変更する（120 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 E-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。

E.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.m
essage-text.other = [ID={id}]{summary}(D={detail})(IP={ip
Address})
```

指定可能な置換文字列の詳細は、「表 E-5 パラメーター(置換文字列)の説明（120 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。

WebSAM Network Management
Web コンソール
スタートアップガイド
Linux 環境用

IMS0LSJ0320-01

2024 年 10 月 第 1 版 発行

日本電気株式会社