HITACHI
Inspire the Next

今すぐ体験
JP1 V9.5

JP1/Cm2/Network Node Manager i

今日から使えるNNMi おためしマニュアル

ネットワーク管理が、かんたん便利に！

3020-3-T16

今すぐ体験
JP1 V9.5

JP1/Cm2/Network Node Manager i

今日から使えるNNMi おためしマニュアル

ネットワーク管理が、かんたん便利に！

3020-3-T16

Contents

マニュアルで前提とする環境

本文中の説明は、次の環境を前提とします。

・Windows Server 2008　・Windows XP　・Internet Explorer 8.0

説明中のマークの意味

参考情報を説明します。

操作時に注意することを説明します。

操作時のヒントになることを説明します。


SNMP 機器


非 SNMP 機器

マニュアルの読み方

「今日から使える NNMi※ おためしマニュアル」は、NNMi の概要や基本的な機能、操作を知っていただいたうえで、運用イメージをつかんでもらうことを目的としています。

※ NNMi は、JP1/Cm2/Network Node Manager i の略称です。

1章 NNMi を導入するとできることを、運用サイクルに沿って説明しています。

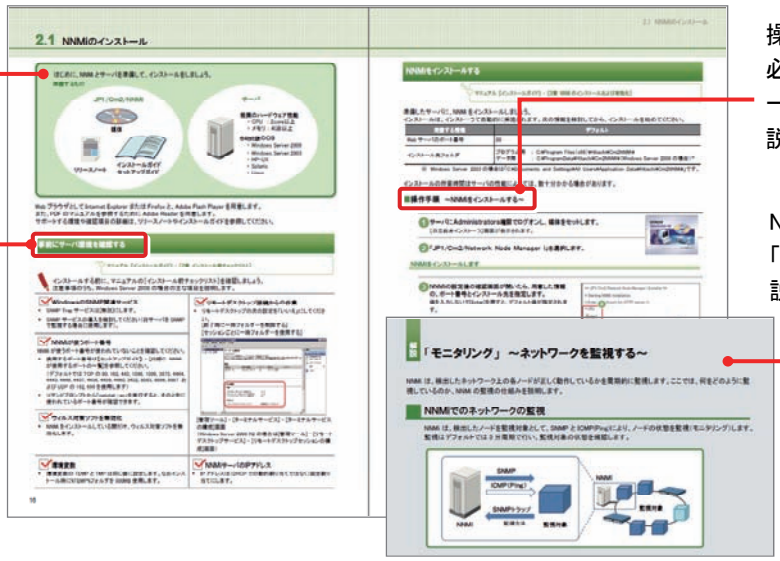
2章 **3章** NNMi の基本的な使い方の概要と、設定方法や操作手順について説明しています。 …設定と操作

4章 NNMi を使用したネットワーク管理の運用方法について説明しています。 …運用

付録 NNMi の活用方法や上級者向けの情報を説明しています。 …活用

各節の冒頭の枠内では、NNMi の機能について大まかに説明しています。

NNMi の機能を使うために実施することや、操作概要などを説明しています。



操作概要の後ろには、必要に応じて、設定の一例を操作手順として説明しています。

NNMi の重要な機能は、「解説」でさらに詳しく説明しています。

このマニュアルと関連マニュアルの活用のしかた

このマニュアルのほかにも、NNMi では製品とともに、次の関連マニュアルを提供しています。

■オンラインヘルプ

オンラインヘルプは製品のメニューから呼び出すことができます。

■マニュアル

本文中ではカッコ内のように記載します。

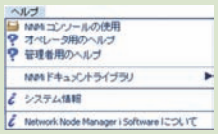
・JP1/Cm2/Network Node Manager i インストールガイド 3020-3-T01（インストールガイド）

・JP1/Cm2/Network Node Manager i セットアップガイド 3020-3-T02（セットアップガイド）

このマニュアルで具体的な参照先を記載しているので、詳しい説明を知りたいときこれらの関連マニュアルを確認してください。

NNMi の概要をわかりやすく説明

NNMi を詳しく説明



・インストールガイド
・セットアップガイド

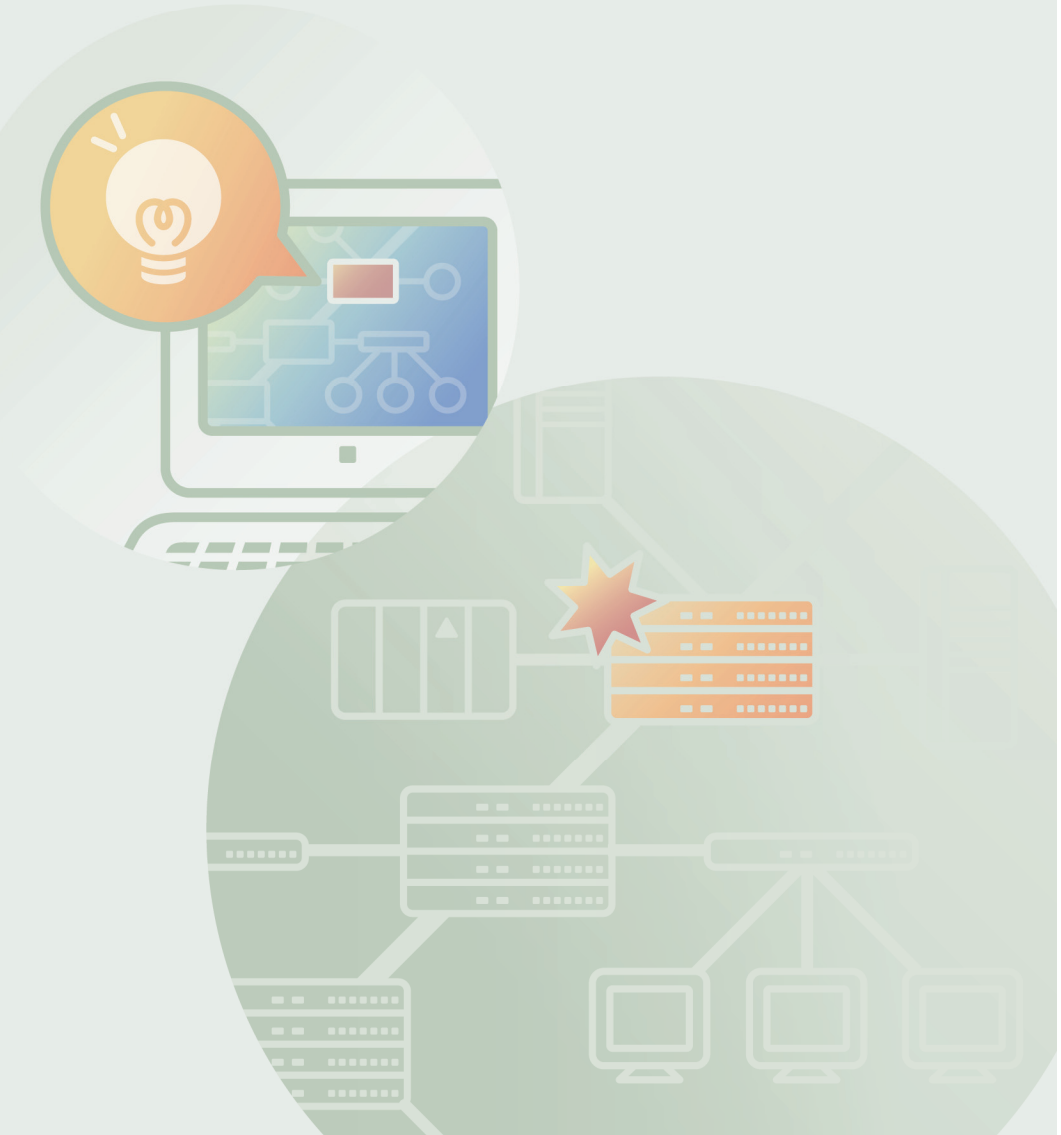
関連マニュアルへの参照指示

関連マニュアル（オンラインヘルプ、マニュアル）への具体的な参照指示は、本文中では次のような形式で記載します。

ヘルプ 【コンソールの使用】
マニュアル【インストールガイド】-［2章 インストール前チェックリスト］

1章

NNMiでできること



NNMi
導入前

従来のネットワーク管理・運用方法を見直してみませんか？

複雑化・大規模化していくネットワーク。

ネットワーク構成の把握が非効率的！

- サーバの増設など、最新のネットワーク構成を把握しておかないと、障害時、復旧に余計な時間が掛かる。しかし、最新の情報を維持するのに日頃から多くの工数はかけられない。

- 各ネットワークを把握するだけでなく、障害時にそなえて、機器間の接続関係も直感的にわかるようにしておきたい。
- 見たいネットワーク機器が探しづらい。業務や部署ごとなどに、ネットワーク機器をカテゴライズさせたい。

**ネットワーク管理の人的コストは
あまり掛けられない。
もっとかんたん便利に
管理・運用したい。**

安定した環境やサービスを提供するうえで欠かすことのできないネットワーク管理。
ネットワーク管理とひとことで言っても、ネットワーク構成の把握や障害の特定、解決など、
やるべきことはさまざまです。しかも、ネットワークが複雑化・大規模化するほど、作業も増大。
ネットワーク管理者の作業負荷を下げるため、従来の管理・運用方法を見直してみませんか？

たとえば、こんなお悩みはありませんか？

発生した障害の特定に時間がかかる！

●障害が発生すると、膨大な数のイベントが発生するため、イベントを一つ一つ調査していくのは効率が悪い。根本原因をすぐに特定したい。

障害の解決状況がわからない！

●発生した障害にはすばやく対応して、対策もれはなくしたい。
●運用担当者や対応状況などの情報をもっとかんたんに、ラクに共有したい。

ネットワーク管理でお困りのことは、
「JP1/Cm2/Network Node Manager i」
で解決しましょう。

NNMi 導入後

NNMi でネットワーク管理をかんたん便利に！

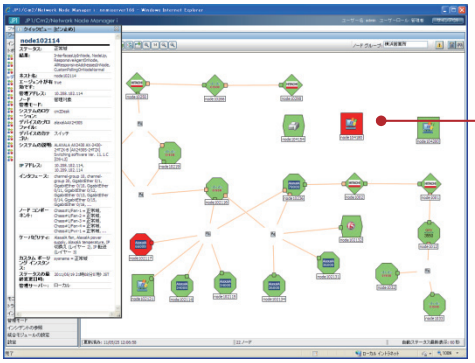
まずは事前準備！

はじめに、NNMi をインストールします。
次に、検出シードと検出範囲を設定して、把握したいネットワーク機器を自動で検出しましょう。

準備ができたら、運用開始！

ネットワーク構成をビジュアルに効率よく把握

トポロジマップ



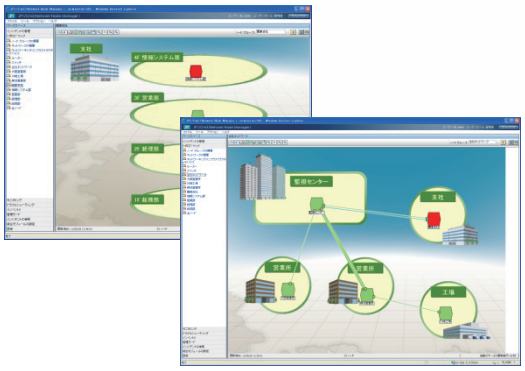
ネットワーク機器の状態を色で表現

ネットワーク機器を自動で検出すると、トポロジマップも自動生成！
さらに、ネットワーク構成の情報も最新のものに自動更新。

業界標準のSNMPプロトコルを採用

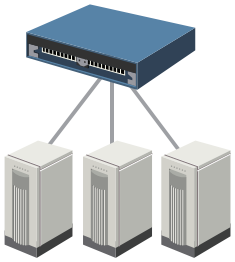
SNMP をサポートするネットワーク機器なら製品のベンダーにとらわれることなく一括管理できます。

ノードグループマップ

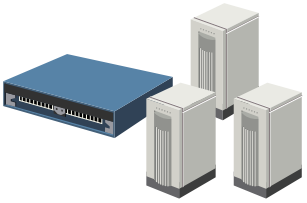


トポロジマップをカスタマイズしたマップがノードグループマップ。
ネットワーク機器をカテゴライズして、よりビジュアルに管理！ 問題の発生個所をすぐに特定でき、自由度の高い管理を実現。

レイヤー2トポロジによる管理



レイヤー3トポロジによる管理



レイヤー2 トポロジも表示できるので、ネットワークの末端にある装置間の結線（スイッチや端末など）もノードグループマップ上で直感的に把握！

P6～7でさらに詳しく説明します

NNMiで解決

NNMiを使ってネットワーク管理をはじめましょう。

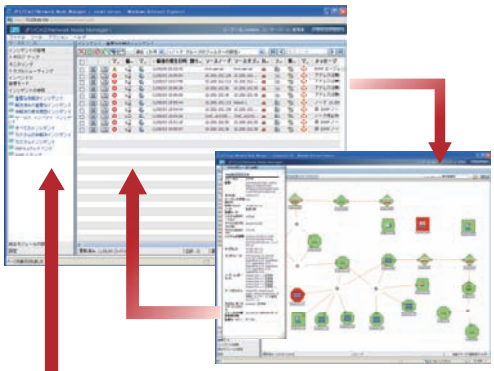
JP1のネットワーク管理製品「JP1/Cm2/Network Node Manager i」は、ネットワーク構成の把握や、障害の特定・解決など、ネットワーク管理の中でも特に作業負荷が高くなりがちな作業をかんたん便利にするための機能を用意しています。

インシデント管理で迅速に障害を特定・解決

小規模から大規模まで広範囲のネットワーク規模に対応

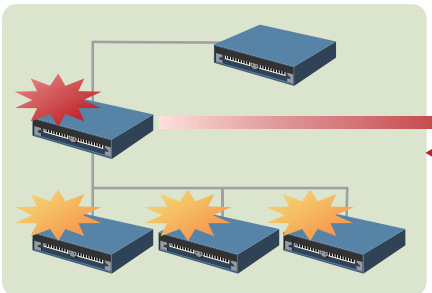
1台のNNMiで、50台から25,000台までのネットワーク機器を監視できるため、集中管理が実現できます。

インシデント管理



障害の根本原因だけをインシデントとして通知！
さらに、障害の発生個所は、トポロジマップに切り替えると、すぐに特定できる。

ポーリングによる障害監視



SNMP、ICMPプロトコルに基づいたポーリングで、ネットワーク機器を監視。幅広い障害監視が可能に！

障害の発生から解決までをライフサイクル管理

障害の発生から解決までの状況をGUIで共有！障害の対処もれの防止、対応状況の共有を効率よく実現。

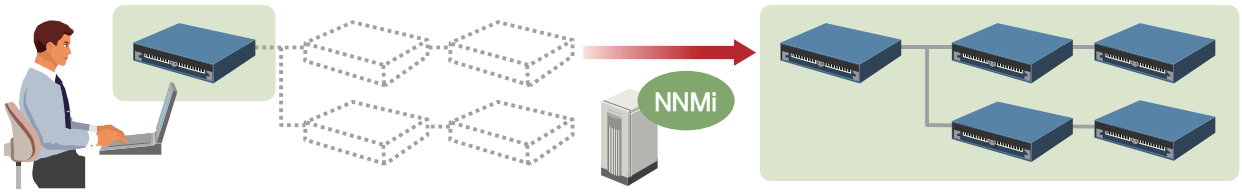
P8～9でさらに詳しく説明します

NNMi 導入後

ネットワーク構成をビジュアルに効率よく把握

ネットワーク機器の検出と把握

検出の起点となるルーターなどのネットワーク機器（**検出シード**）を設定し、IP アドレスなどで検出範囲を指定すると、NNMi は自動でネットワーク機器およびサーバを検出します。検出後にネットワーク構成を変更しても自動で更新されるため、負担なく、常に最新の情報を把握できます。



把握したいネットワーク機器を明示的に指定することも可能

対象とするネットワーク機器は、明示的に個別で指定することもできます。対象とするネットワーク機器があらかじめ明確に決まっているときには、この方法も利用してください。

トポロジマップの自動生成

検出したネットワーク機器をもとに、ネットワーク構成図（**トポロジマップ**）が自動で生成されます。このため、運用を開始した直後から、ビジュアルにネットワークの状況を把握できます。

トポロジマップ

アイコンの形、色でネットワーク機器の種類、状態を把握

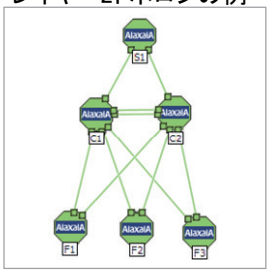
アイコンの形で、ルーターや PC などネットワーク機器の種類がわかります。
また、色で障害の発生有無などのネットワーク機器の状態を把握できます。

レイヤー2トポロジを表示

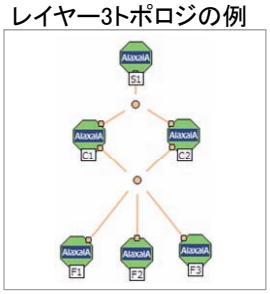
ネットワークのレイヤー3 トポロジだけでなく、レイヤー2 トポロジを表示させて確認できます。

- レイヤー2 トポロジ
  物理的な結線でネットワーク構成を表示します。
  末端のスイッチと端末間の結線を確認するときは、レイヤー2 トポロジで確認します。 レイヤー3 トポロジと併用させることによって、障害発生時の状況の確認や影響範囲の把握が直感的にできます。
- レイヤー3 トポロジ
  IP アドレスで論理的なネットワーク構成を表示します。
  基幹ネットワークの論理構成を確認するときは、レイヤー3 トポロジで確認します。

レイヤー2トポロジの例



レイヤー3トポロジの例



ノードグループマップの作成

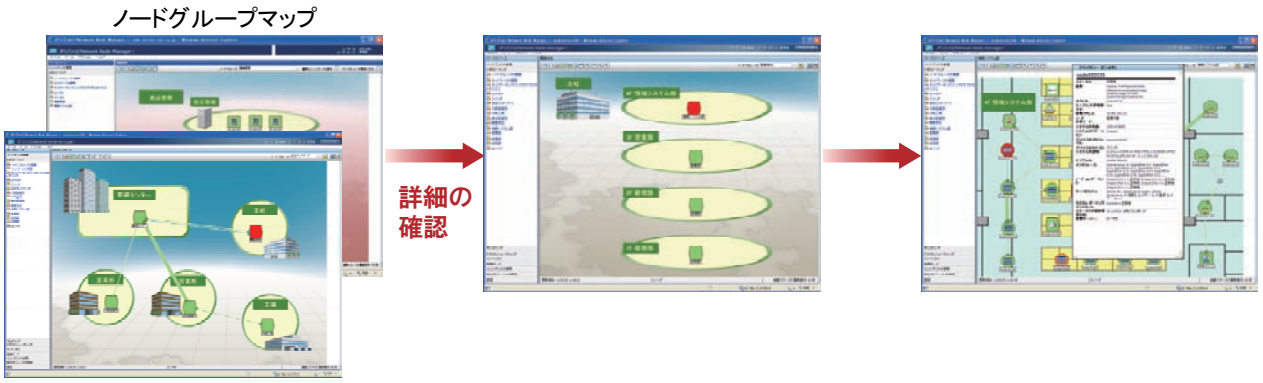
検出したネットワーク機器をカテゴライズして表示させるマップ（**ノードグループマップ**）を作成できます。このノードグループマップを作成することで、トポロジマップよりも視点を絞ってネットワーク構成が把握できるようになるため、問題の発生個所を探しやすくなり、すばやく詳細を確認できます。

ノードグループをもとに作成

検出したネットワーク機器をカテゴライズさせたものを**ノードグループ**といいます。ノードグループマップは、このノードグループをもとに作成します。ノードグループは、業務、地域、デバイスの監視方法ごとなど、観点を絞ってネットワーク機器をカテゴライズすることができます。

背景図を柔軟にカスタマイズ

ノードグループマップの背景図を、画像ファイルを使って自由に設定できます。フロアのレイアウト図を設定するなど、目的に合わせた表示方法のカスタマイズによって、より効率的なネットワークの管理を支援します。



ネットワーク構成をビジュアルに効率よく把握するための NNMi の機能や操作については、「2 章　ネットワークにあるノードを把握する」を参照してください。

NNMi 導入後

インシデント管理で迅速に障害を特定・解決

ポーリングによる監視

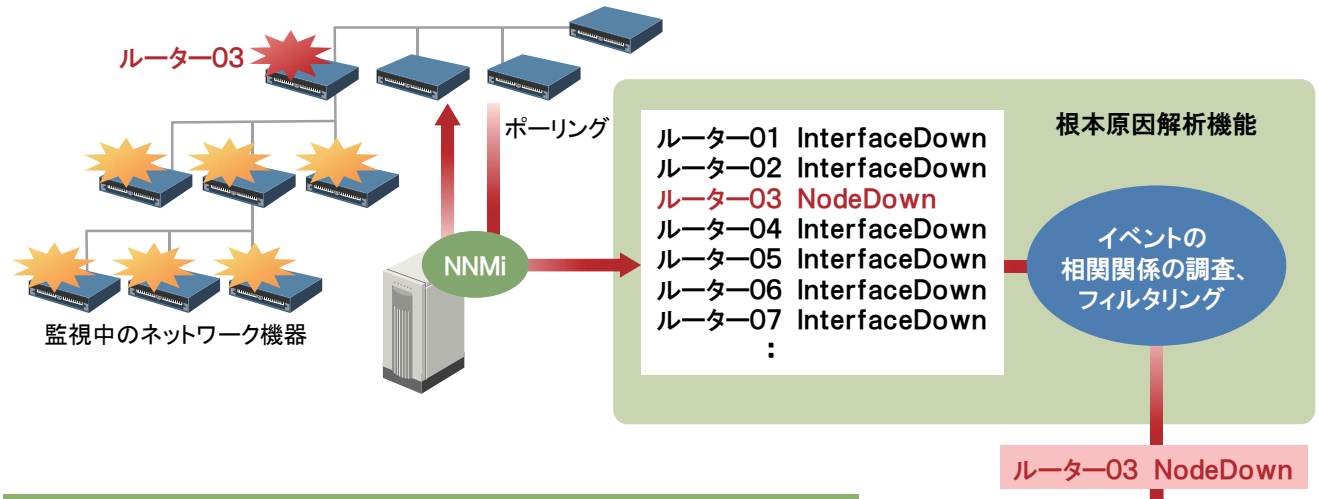
NNMi は、SNMP や ICMP プロトコルに基づいたポーリングによって、検出したネットワーク機器を監視します。ネットワーク機器の状態だけでなく、ファン・電源・電圧など、ネットワーク機器のコンポーネントの状態も対象としているため、幅広い障害監視を実現できます。なお、ポーリングは、周期（秒、分、時間、日単位）を設定することで、自動で定期的に実行されます。障害を解決した直後など、すぐにポーリングしたいときは手動でも実施できます。

ポーリングの条件を複数の範囲に対して設定

ネットワーク機器ごと、ノードグループごとなど、複数の範囲に対して、それぞれ異なるポーリングの条件を設定できます。
このため例えば、監視対象の重要度ごとにポーリングの実施周期を変えるなどの運用ができます。

障害の根本原因の解析

NNMi は障害発生時に、**根本原因解析**（RCA：Root Cause Analysis）**機能**によって、大量に発生するイベントの相関関係を調査し、フィルタリングします。さらに、レイヤー2 トポロジに基づいた障害の解析によって、根本原因を特定します。



障害の根本原因の通知と特定

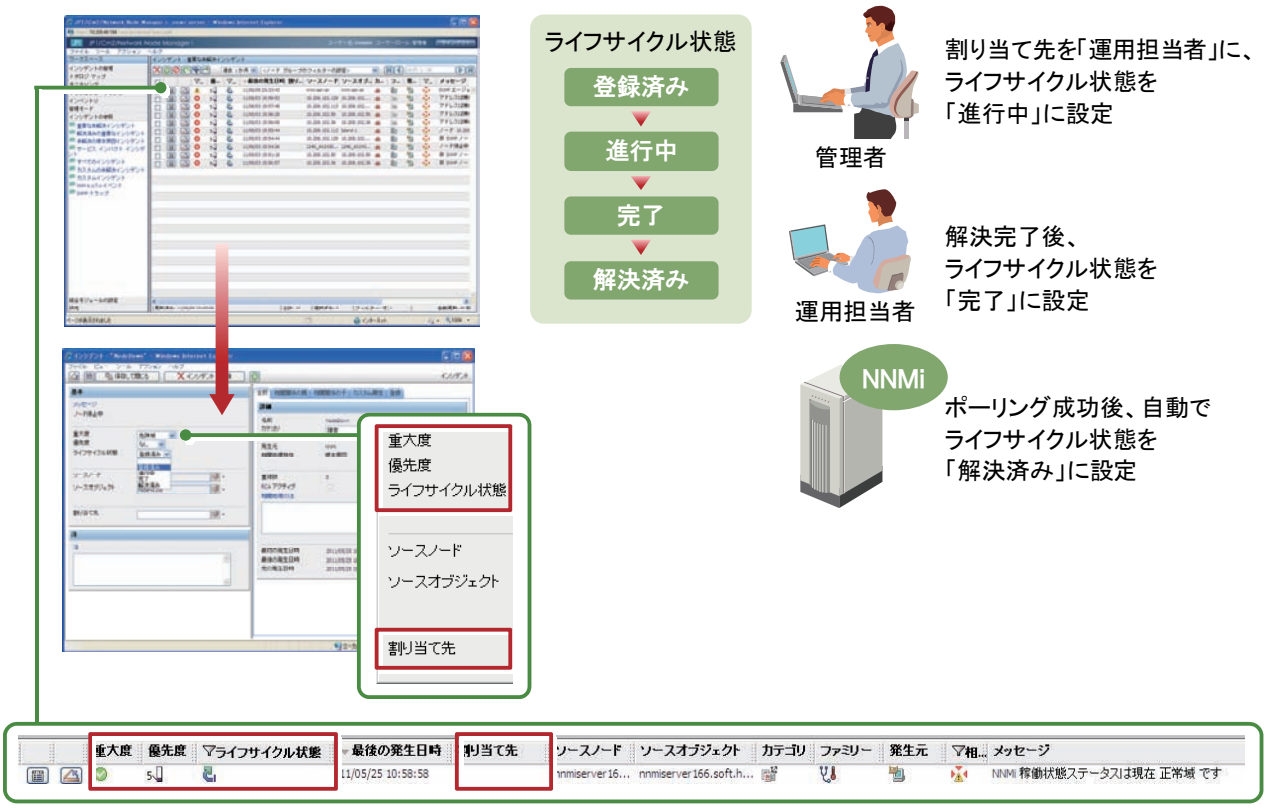
解析後、根本原因は**インシデント**として通知されます。
インシデントとは、ネットワークで発生した事象について管理者に通知する必要がある重要性の高い情報のことです。NNMi のインシデントによる管理を**インシデント管理**といいます。
通知されたインシデントはインシデントの参照画面で確認します。なお、トポロジマップで参照すると、アイコンの色から直感的にネットワーク機器の状態を把握できるので、すぐに根本原因となる障害の発生個所を特定することができます。

障害の対応状況の管理

NNMi のインシデント管理は障害を通知するだけでなく、通知した直後から解決にいたるまでの進行状況も GUI で管理します。未対応のインシデントは、フィルタリングして把握できるため、対処もれを防げます。
通知直後の**ライフサイクル状態**には「登録済み」が設定されていますが、管理者や運用担当者が「進行中」や「完了」などに更新していくことによって、GUI で障害の対応状況を共有することができます。また、ポーリングの成功によって、障害が解決済みであることを NNMi が確認すると、ライフサイクル状態が「解決済み」に自動的に更新されます。

運用担当者（割り当て先）の指定

複数人で分担して管理をする場合、自分以外の運用担当者（割り当て先）を指定できるので、障害の解決作業を開始したときに GUI 上で作業を分担することができます。



インシデント管理で迅速に障害を特定・解決するためのNNMiの機能や操作については、「3 章　把握したノードを監視する」を参照してください。

NNMi 機能概要

機能一覧

NNMi の機能概要について次の表で説明します。

構成管理

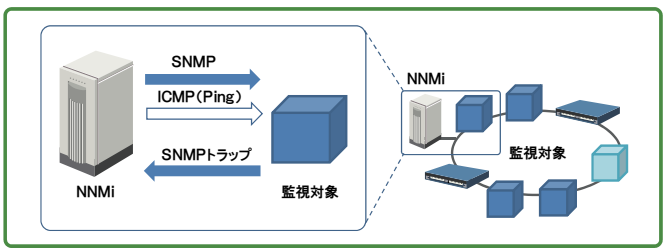
機能	説明
ノードの検出	設定したルールに従い、ノードを自動検出します。 また、手動でノードを追加することもできます。
ノードを構成するオブジェクトの自動検出	ノードを構成するオブジェクトを自動的に検出します。 ・SNMP エージェント ・カード、ポート ・インタフェース ・IPv4 アドレス、IPv6 アドレス ・電源、ファン 参考 検出できるオブジェクトは、機器のベンダーや機種によって異なります。
トポロジの検出・表示	レイヤー3 トポロジ（論理的なネットワーク構成）に加え、レイヤー2 トポロジ（物理的な結線によるネットワーク構成）を自動検出し、マップに表示します。 レイヤー2 トポロジは手動で定義することもできます。 参考 レイヤー2 トポロジを自動検出するためには、LLDP などの隣接するデバイスを検出するためのプロトコルを有効化する必要があります。
冗長化技術への対応	冗長化されたルータ・グループ（VRRP など）を自動検出します。 またリンクアグリゲーションを自動検出します。

構成管理の機能については、「2 章 ネットワークにあるノードを把握する」で説明します。

参考 「ポーリング」

NNMi は、SNMP と ICMP(Ping)を使って、ネットワークの検出や監視を周期的に行います。これをポーリングといいます。

ポーリングには次の 2 種類があります。
- 検出のためのポーリング
- 監視のためのポーリング



ポーリングについて、NNMi の画面、オンラインヘルプおよびマニュアルでは、さまざまな用語や表記を用いていますが、大きく分けると検出と監視の 2 種類です。

NNMi には次の 2 種類があります。
・JP1/Cm2/Network Node Manager i
・JP1/Cm2/Network Node Manager i Advanced
機能一覧表のうち、下線の機能は NNMi Advanced で使用できる機能です。
NNMi Advanced については、「付録 NNMi Advanced の紹介」で説明します。

障害管理

機能	説明
ICMP/SNMP ポーリングによる監視	ICMP/SNMP ポーリングによって、次のオブジェクトの状態監視を行います。 ・SNMP エージェント ・カード ・インタフェース ・IPv4 アドレス、IPv6 アドレス ・電源、ファン、電圧、温度 ・冗長化ルータ・グループ ・リンクアグリゲーション
SNMP トラップによる監視	SNMP トラップにより障害を監視します。
根本原因解析 （RCA：Root Cause Analysis）	検出したレイヤー2 トポロジに基づいて、障害の根本原因を解析します。
インシデント管理	ポーリングや SNMP トラップによって検出した障害をインシデントとして通知します。
自動アクション	インシデントの状態に応じて、任意のコマンドを自動アクションとして実行することができます。

障害管理の機能については、「3 章 把握したノードを監視する」で説明します。

性能管理

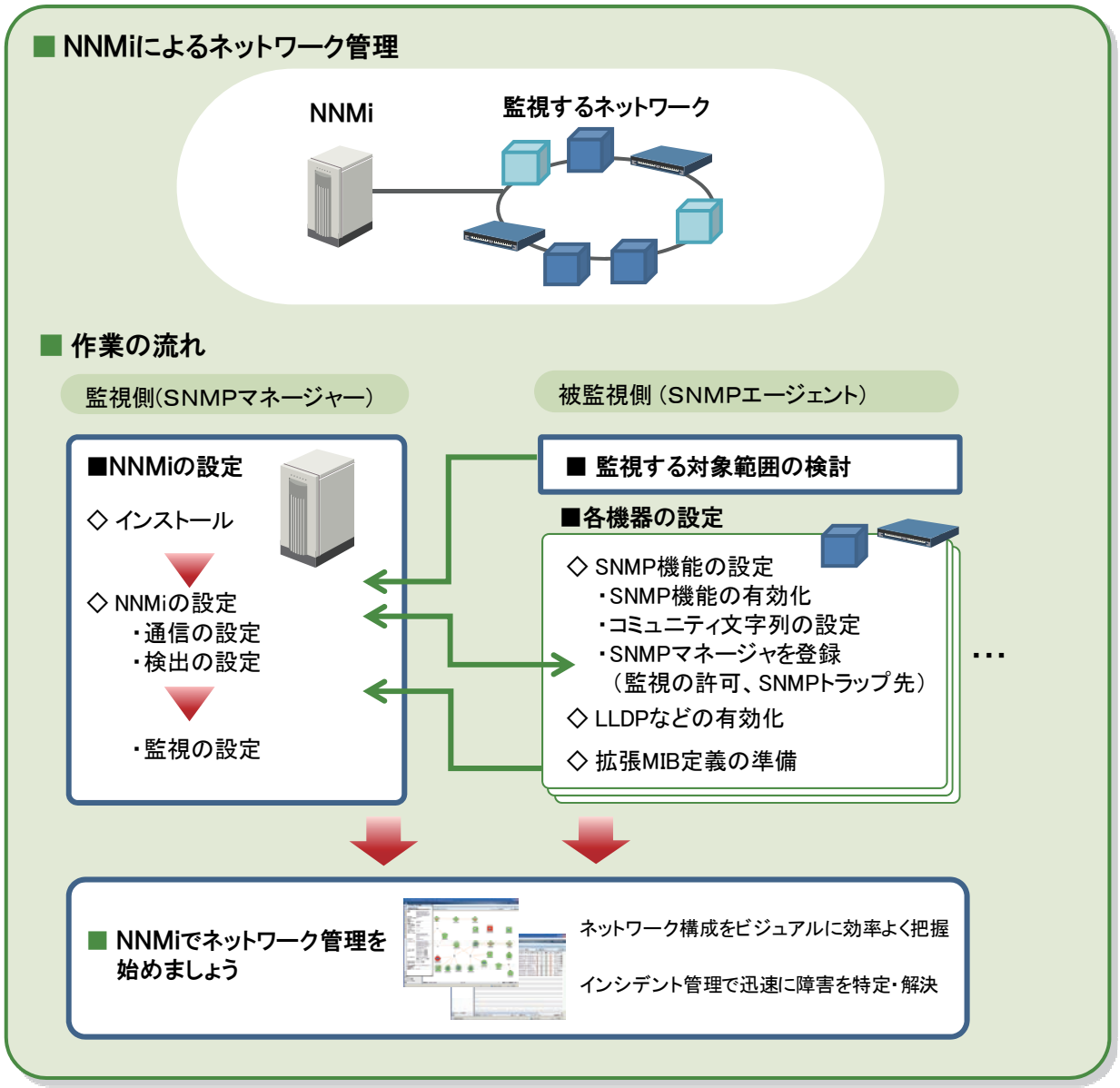
機能	説明
MIB 収集と保存	任意の MIB オブジェクトを収集します。 収集したオブジェクトは、CSV ファイルに保存できます。
しきい値監視	設定した MIB オブジェクトのしきい値（上限値、下限値）によって判定します。しきい値を超えた場合はインシデントとして通知したりマップ上のシンボル・ステータスに反映したりできます。
グラフ表示	MIB データを収集し、リアルタイムにグラフ表示することができます。

性能管理の機能については、「付録 カスタムポーラーによる監視」で説明します。

導入までの流れ

NNMi導入までの流れ

NNMi を使ったネットワーク管理を始めるために、設定することおよび準備することの全体像を説明します。



［凡例］ ：本書で説明する範囲

ネットワーク管理を始めるための準備作業には、大きく分けて監視側と被監視側の作業があります。

監視側である NNMi は、サーバを用意して NNMi をインストールし、本書の「2 章　ネットワークにあるノードを把握する」と「3 章　把握したノードを監視する」に沿って設定を進めます。

被監視側（監視対象のネットワーク）では、監視する対象範囲を決めます。
また、監視する各機器について、SNMP で監視できるように SNMP 機能を有効化します。各機器の SNMP 設定の一般的な作業項目は図のとおりです。詳しくは各機器のマニュアルを参照してください。
LLDP などの隣接デバイス検出プロトコルの機能がある場合は有効化を検討します。NNMi は LLDP などの情報を収集することで機器の接続（L2 トポロジ）を検出します。
機器固有の MIB 定義情報がある場合は、MIB ファイルを準備して NNMi に登録します。

これらの設定を完了させて、「4 章　ネットワーク管理を始めよう」を参考に運用を始めましょう。

プランニングシート ： NNMiの設定に必要な基本情報

設定作業を始める前に決めておくべき基本的な情報をプランニングシート形式で説明します。

■NNMi サーバの情報

確認項目	説明	本書の例
NNMi サーバの ホスト名、IP アドレス	NNMi を導入するサーバのホスト名(FQDN)および IP アドレス。	• ホスト名：nnmiserver • IP アドレス：192.168.100.24
NNMi インストール時の構成情報	NNMi のインストールに関する情報。 • インストール先フォルダ（プログラム用とデータ用の 2 種類）。 • NNMi の Web サーバのポート番号。	・インストール先フォルダ （プログラム用）：デフォルト値を使用 （データ用）：デフォルト値を使用 ・ポート番号：デフォルト値を使用 デフォルト値は 「2.1 NNMi のインストール」で説明します。
NNMi のユーザー	ユーザー名、パスワード、ロール。 • 管理用のシステムアカウント(system)が設定済み、パスワードだけを指定します。 • 管理者ロールのユーザーを一つ以上作成します。	ユーザー名 / パスワード / ロール system / password / － nnmiadm / password / 管理者 nnmiope / password / オペレータレベル 2

■監視対象／監視方法の情報　（これらの情報は NNMi に設定します）

確認項目		説明	本書の例
コミュニティ文字列		監視対象の SNMP 読み取り要求のコミュニティ名。	public
監視対象の検出方法		監視対象のノードを検出する方法。 自動検出と、監視対象を明示的に指定する方法があります。複数のルールを指定したり、両方を組み合わせたりすることもできます。次の項目を決めます。	自動検出
	自動検出の場合	• 自動検出ルールの名前 • 検出する IP アドレスの範囲 • 検出シード（検出の起点） • 検出対象範囲 □ルータとスイッチだけ(デフォルト) □SNMP デバイスを追加 □非 SNMP デバイスを追加	• ルール名 ： システム部 • IP の範囲 ： 10.208.102.2-254 • 検出シード： 10.208.102.116 • 検出範囲 ： すべて（SNMP デバイスと非 SNMP デバイスを追加）
	明示的に指定の場合	• 対象機器の一覧 （IP アドレス一覧を用意してシードファイルにします。）	―
監視対象のグループ化 （ノードグループ）		監視対象をグループ化したい場合に定義します。 • ノードグループの名前 • ノードグループの対象（フィルタ条件） • ノードグループマップ	• ノードグループ名： システム部 • 対象 ：10.208.102.2-254 IP 範囲指定 • マップについては「2.5 ノードグループの設定」を参照してください。
監視対象の機器の拡張 MIB 定義		監視対象の機器に独自の MIB 定義があれば準備します。	―
自動アクション		インシデントに自動アクションを設定します。 • 対象インシデント • 実行契機 • 自動アクションの内容（コマンドと引数）	• 対象：NodeDown(ノード停止中)※ • 実行契機：登録時 • 内容：msg.exe コマンドで通知

※操作練習で、ノードを停止して(または LAN ケーブルを抜いて)擬似障害を発生させます。

2章

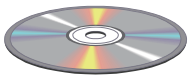
ネットワークにある ノードを把握する

2.1 NNMiのインストール

はじめに、NNMi とサーバを準備して、インストールをしましょう。

準備するもの

JP1/Cm2/NNMi

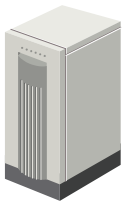


媒体

リリースノート

インストールガイド
セットアップガイド

サーバ



推奨のハードウェア性能
- CPU ：2core以上
- メモリ：4GB以上

64bit版のOS
- Windows Server 2008
- Windows Server 2003
- HP-UX
- Solaris
- Linux

Web ブラウザとして Internet Explorer または Firefox と、Adobe Flash Player を用意します。
また、PDF のマニュアルを参照するために Adobe Reader を用意します。
サポートする環境や確認項目の詳細は、リリースノートやインストールガイドを参照してください。

事前にサーバ環境を確認する

マニュアル【インストールガイド】-［2章 インストール前チェックリスト］

インストールする前に、マニュアルの［インストール前チェックリスト］を確認しましょう。
注意事項のうち、Windows Server 2008 の場合の主な項目を説明します。

WindowsのSNMP関連サービス

- SNMP Trap サービスは[無効]にします。
- SNMP サービスの導入を検討してください（自サーバを SNMP で監視する場合に使用します）。

NNMiが使うポート番号

NNMi が使うポート番号が使われていないことを確認してください。

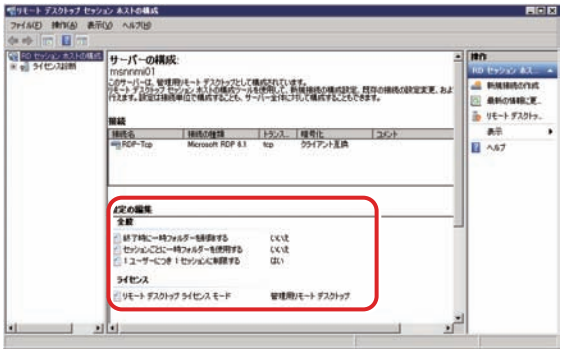
- 使用するポート番号は【セットアップガイド】－［付録C NNMi が使用するポートの一覧］を参照してください。
  （デフォルトでは TCP の 80, 162, 443, 1098, 1099, 3873, 4444, 4445, 4446, 4457, 4458, 4459, 4460, 5432, 8083, 8886, 8887 および UDP の 162, 696 を使用します）
- コマンドプロンプトから「netstat -an」を実行すると、そのときに使われているポート番号が確認できます。

ウィルス対策ソフトを無効化

- NNMi をインストールしている間だけ、ウィルス対策ソフトを無効化します。

リモートデスクトップ接続からの作業

- リモートデスクトップの次の設定を「いいえ」にしてください。
  ［終了時に一時フォルダーを削除する］
  ［セッションごとに一時フォルダーを使用する］



［管理ツール］－［ターミナルサービス］－［ターミナルサービスの構成］画面
（Windows Server 2008 R2 の場合は［管理ツール］－［リモートデスクトップサービス］－［リモートデスクトップセッションの構成］画面）

環境変数

- 環境変数の TEMP と TMP は同じ値に設定します。なおインストール時に%TEMP%フォルダを 500MB 使用します。

NNMiサーバのIPアドレス

- IP アドレスは（DHCP での動的割り当てではなく）固定割り当てにします。

NNMiをインストールする

マニュアル【インストールガイド】-［3章 NNMi のインストールおよび有効化］

準備したサーバに、NNMi をインストールしましょう。
インストールは、インストーラで自動的に実施されます。次の情報を検討してから、インストールを始めてください。

用意する情報	デフォルト
Web サーバのポート番号	80
インストール先フォルダ	プログラム用　：C:¥Program Files（x86）¥Hitachi¥Cm2NNMi¥ データ用　：C:¥ProgramData¥Hitachi¥Cm2NNMi¥（Windows Server 2008 の場合）※

※ Windows Server 2003 の場合は「C:¥Documents and Settings¥All Users¥Application Data¥Hitachi¥Cm2NNMi¥」です。

インストールの所要時間はサーバの性能によっては、数十分かかる場合があります。

■操作手順　～NNMiをインストールする～

1 サーバにAdministrators権限でログオンし、媒体をセットします。
［日立総合インストーラ］画面が表示されます。

2 「JP1/Cm2/Network Node Manager i」を選択します。

NNMiをインストールします

3 NNMiの設定値の確認画面が開いたら、用意した情報の、ポート番号とインストール先を指定します。
値を入力しないで[Enter]を押すと、デフォルト値が指定されます。

参考 インストール先フォルダ（データ用）には、NNMi の設定ファイル、データベース、ログファイルなどが格納されます。

4 「yes」を入力して[Enter]を押します。
「Installing NNMi ...」と表示され、NNMi のインストールが開始されます。
完了すると自動でコマンドプロンプトが閉じます。

「no」を入力すると 3 の設定値の入力に戻ります。

```
** JP1/Cm2/Network Node Manager i Installer **
* Starting NNMi installation.
* Enter 3 lt port for HTTP server =>
* [80]
(Enter)
* Enter program install directory =>
* [C:¥Program Files (x86)¥Hitachi¥Cm2NNMi¥]
(Enter)
* Enter program data directory =>
* [C:¥ProgramData¥Hitachi¥Cm2NNMi¥]
(Enter)
* port : 80
* install directory : C:¥Program Files (x86)¥Hitachi¥Cm2NNMi¥
* data directory : C:¥ProgramData¥Hitachi¥Cm2NNMi¥
* Do you start installation with above settings you entered ? (yes/no)
* If you need 4 hange the settings, please enter no.
yes (Enter)
Installing NNMi ...
```

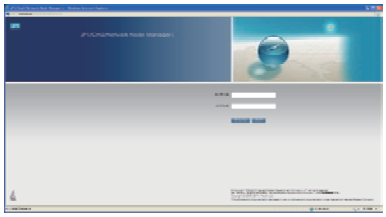
これでNNMiのインストールの操作は完了です。

NNMi の環境変数がシステムに追加されています。
画面上に開いているコマンドプロンプトがある場合は一度閉じてから開き直して、NNMi の環境変数を反映させてください。

2.2 NNMiへのアクセス

Web ブラウザから NNMi コンソールにアクセスして、運用を始めましょう。
アクセスしたら、まずはユーザーアカウントを作成します。作成しながら、基本操作も覚えましょう。

Webブラウザから NNMiにアクセスします。※



ユーザーアカウントを作成します。

（例）

管理者

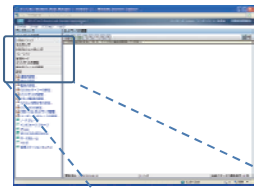
名前: nnmiadm
ロール: 管理者

運用担当者

名前: nnmiope
ロール: オペレータ レベル2

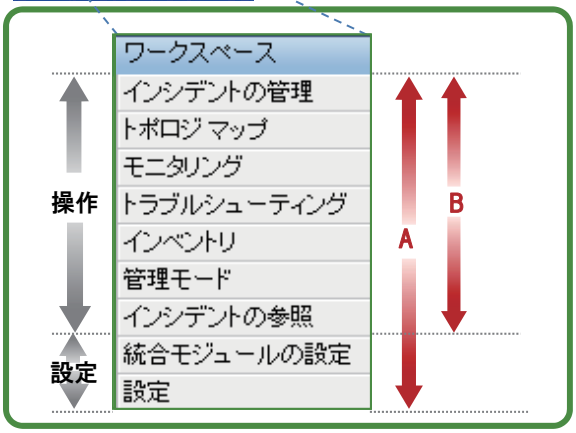
※ 初回はシステムアカウントでアクセスします。

NNMiコンソール



主な操作は「ワークスペース」から実施します。

ユーザーアカウントの「ロール」で操作できる範囲を設定します。



A：「管理者」が操作できる範囲
B：「オペレータ レベル2」が操作できる範囲

WebブラウザからNNMiにアクセスする

ヘルプ　【コンソールの使用】
マニュアル【インストールガイド】-［4章 NNMi 入門］

Web ブラウザから NNMi にアクセスしてみましょう。
最初はユーザーアカウントを作成していないため、システムアカウントを使って NNMi にアクセスします。

■操作手順　～WebブラウザからNNMiにアクセスする～

システムアカウントのパスワードを設定します

1 NNMiサービスを停止します（ovstop -cを実行）。

コマンドプロンプトを開いて実行します。NNMi が停止します。
なお、インストール直後は NNMi は停止した状態のため、「ovspmd が動作していません」と表示されます。

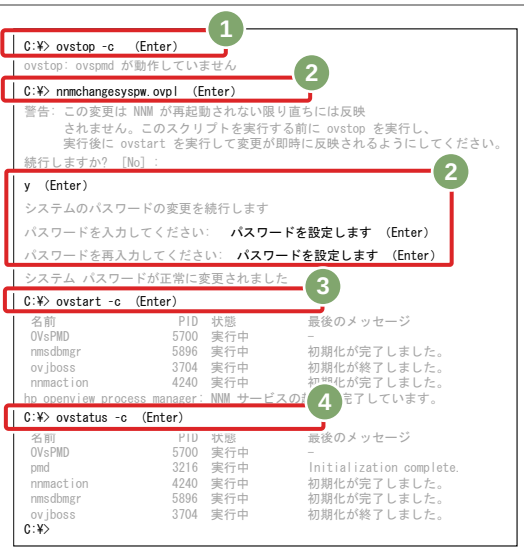
2 パスワードを設定します（nnmchangesyspw. ovpl を実行）。

「y」を入力後、メッセージに従ってパスワードに任意の文字列を指定します。
（例）　パスワード ： password

3 NNMiを起動します（ovstart -cを実行）。

4 NNMiの状態を確認します（ovstatus -cを実行）。

すべての「状態」が「実行中」になっていれば正常です。



NNMiにアクセスします

Web ブラウザから NNMi にアクセスします。あらかじめ Web ブラウザは次の設定をしてください。

- ポップアップを許可（ポップアップブロックを無効）にします。
- アクティブスクリプトの実行および Cookie の保存を有効にします。
- IE 9 の場合は互換表示を有効にしてください。

5 WebブラウザからNNMiにアクセスします。 URL： http://ホスト名:ポート番号/nnm/

NNMi コンソールのサインイン画面が表示されます。

参考

ホスト名 ：NNMi をインストールしたサーバのホスト名（FQDN）です。
ホスト名の代わりに IP アドレスも指定できます。
ポート番号 ：NNMi のインストール時に指定した Web サーバのポート番号を指定します。

参考

サインイン画面のほかにもう 1 枚画面が表示されますが、この画面はサインイン後に閉じてもかまいません。

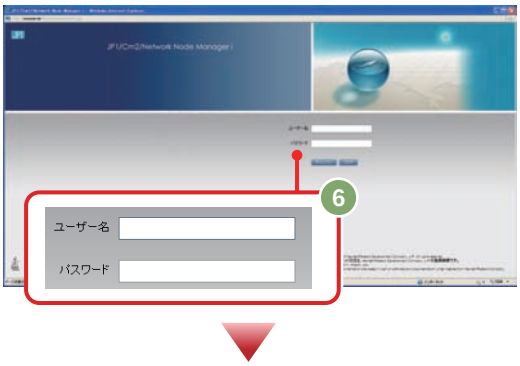
6 NNMiにサインインします。

ユーザーアカウントの作成前のためシステムアカウントを使ってサインインします。

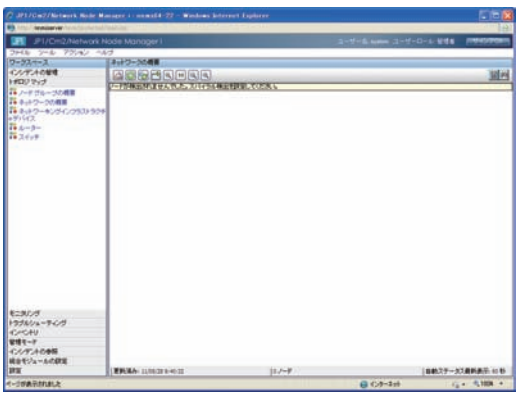
ユーザー名 ： system

パスワード ： 2 で設定した値

入力したあと、 サインイン をクリックします。



サインインが成功すると、NNMi コンソールが表示されます。



参考

システムアカウントのユーザー名「system」は固定値です。
システムアカウントは、初期設定やメンテナンス作業だけで使用します。

これでWebブラウザからNNMiにアクセスできました。

ユーザーアカウントを設定する

ヘルプ　【管理者用ヘルプ】- [NNMi ユーザーインタフェースを設定する] - [NNMiへのアクセスを制御する]

管理者と運用担当者のユーザーアカウントを、それぞれ設定しましょう。

管理者

名前　：nnmiadm
ロール：管理者

運用担当者

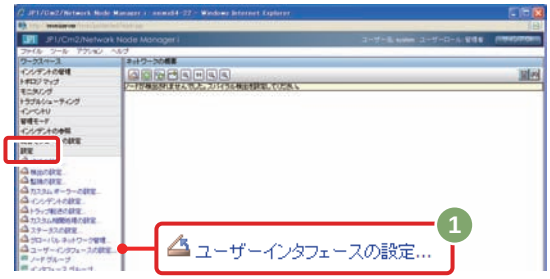
名前　：nnmiope
ロール：オペレータ レベル2

■操作手順　～ユーザーアカウントを設定する～

まず管理者ロールのユーザーを作成し、そのユーザーでサインインし直します。
その後、運用担当者のユーザーを作成します。

1 ワークスペースの[設定] - [ユーザーインタフェースの設定]を選択します。

[ユーザーインタフェースの設定]画面が表示されます。

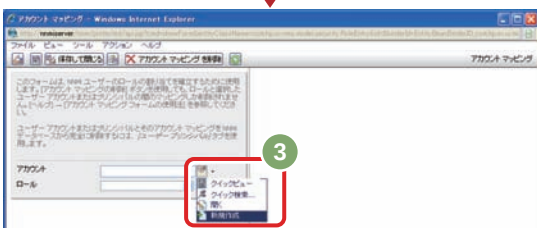


2 [ユーザーアカウント]タブを選択して、[ ]（新規作成）をクリックします。

[アカウント マッピング]画面が表示されます。

3 [アカウント]の[ ]から[新規作成]をクリックします。

[ユーザーアカウント]画面が表示されます。



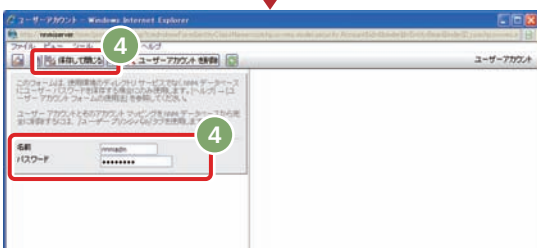
4 「名前」と「パスワード」を入力して、[保存して閉じる]をクリックします。

（例）管理者
　　名前 ： nnmiadm　　パスワード ： password

（例）運用担当者
　　名前 ： nnmiope　　パスワード ： password

ユーザー名とパスワードが設定されて、[ユーザーアカウント]画面が閉じます。

運用担当者の「nnmiope」は、管理者の「nnmiadm」を作成したあと、「nnmiadm」でサインインし直してから作成してください。



5 [アカウント マッピング]画面で、「ロール」のプルダウンメニューからロールを選択して、[保存して閉じる]をクリックします。

（例）nnmiadm ： 管理者

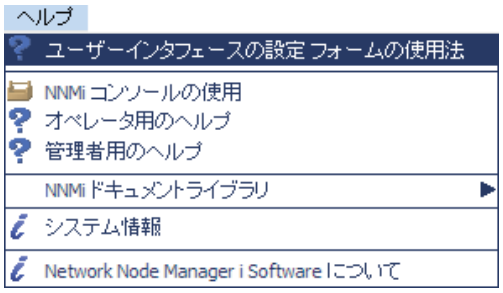
nnmiope ： オペレータ レベル2

ユーザーアカウントが設定されて、[アカウント マッピング]画面が閉じます。

ヒント

[ヘルプ]メニューを選択すると、一番上に操作中の画面に関連したトピックが表示されます。
このトピックを参照すると、指定できる文字数や文字の種類など、設定項目について知りたいことがすぐに確認できて便利です。

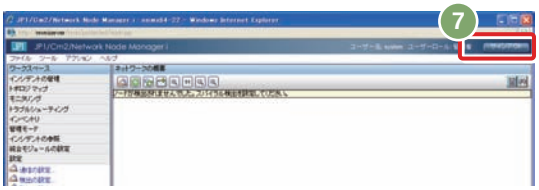
ヘルプは、ファイル一式をコピーすることで、
NNMi の動作していない PC でも参照できます。
【管理者用ヘルプ】－[NNMi ヘルプをどこでもいつでも使用する]を参照してください。



6 [ユーザーインタフェースの設定]画面の[ユーザーアカウント]タブで、設定したユーザーアカウントが表示されていることを確認して、[保存して閉じる]をクリックします。

7 システムアカウント(system)で作業している場合は、[サインアウト]をクリックしてサインアウトします。

システムアカウントは、初期設定だけで使用するユーザーです。管理者ロールのアカウント（例：nnmiadm）を作成したら、サインインし直してください。



これでユーザーアカウントを設定する操作は完了です。

困ったときは パスワードを忘れてしまった

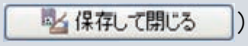
ユーザーアカウントのパスワードを忘れてしまった

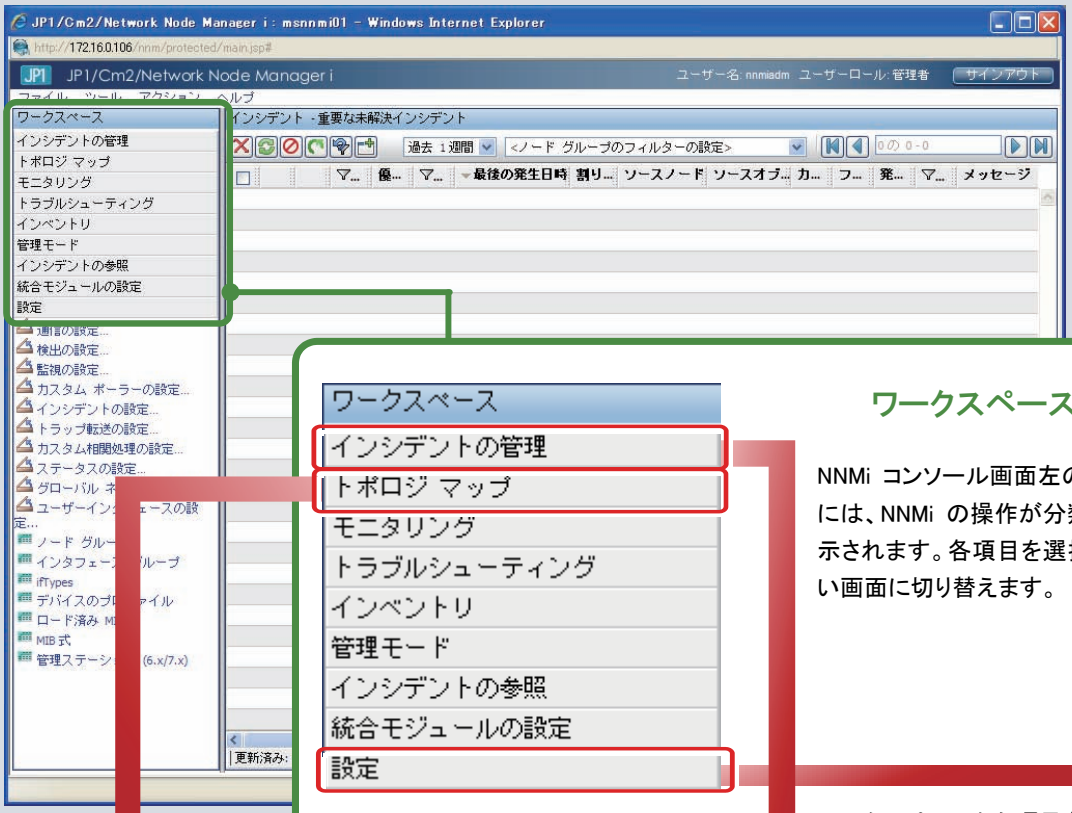
次に示すオンラインヘルプを参照して、パスワードを再設定してください。
【管理者用ヘルプ】－[NNMi ユーザーインタフェースを設定する]－[NNMi へのアクセスを制御する]－[サインインアクセスを設定する]－[NNMi アカウントでアクセスを制御する]－[パスワード、名前、またはロールの割り当てを変更する]

システムアカウントのパスワードを忘れてしまった

nnmchangesyspw.ovpl コマンドでパスワードを再設定してください。nnmchangesyspw.ovpl コマンドについては、「2.2 NNMi へのアクセス」の操作手順「WebブラウザからNNMiにアクセスする」を参照してください。

解説「NNMiコンソールの操作」

NNMi へアクセスすると、NNMi コンソールが表示されます。NNMi コンソールを使って、基本操作に慣れておきましょう。保存（  、  ）や削除（  ）をクリックしなければ、設定は変更されないため、自由に操作してみましょう。

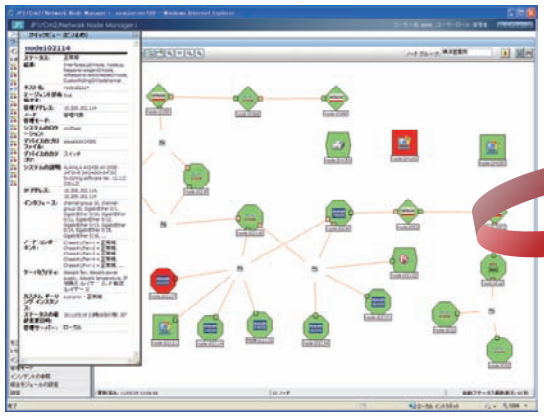


ワークスペース

NNMi コンソール画面左のワークスペースには、NNMi の操作が分類・整理されて表示されます。各項目を選択して、操作したい画面に切り替えます。

ワークスペースから項目を選択

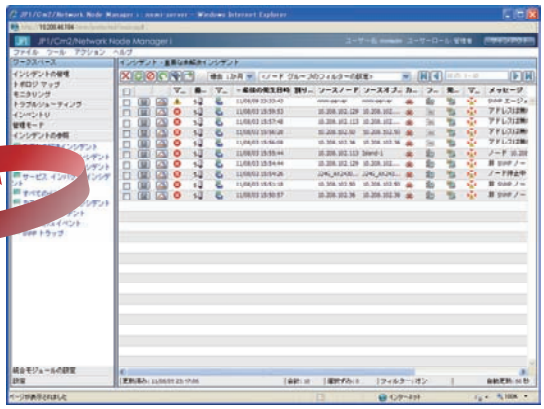
[トポロジ マップ]を選択



[ネットワークの概要]画面

トポロジマップが表示される画面で、ネットワーク構成と各ノードの状態をビジュアルに把握できます。

[インシデントの管理]を選択



[インシデント － 重要な未解決インシデント]画面

通知されたインシデントを参照し、管理することで、障害の対応状況を把握できます。

運用シーンに合わせて、画面を切り替えて使ってください。

操作の基本パターン

NNMi コンソールでは、アイコンを操作して情報を参照したり、定義を設定したりします。アイコンにカーソルを置くと、アイコンの説明が表示されます。よく使う基本の操作の流れを次に示します。

1 **画面を開きます**

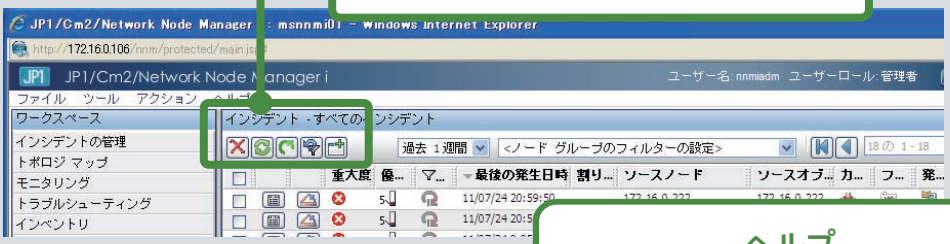
既存を開く　新規に開く　別画面で開く

2 **設定します**
参照します

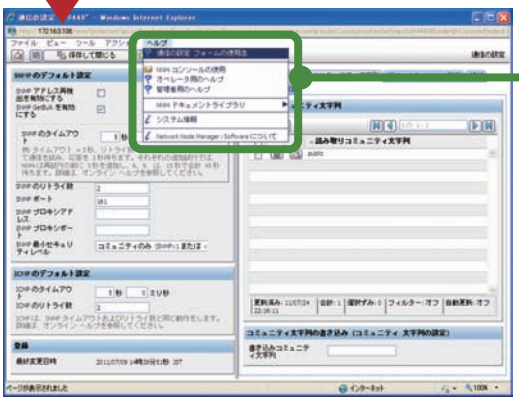
各画面で操作　変更を保存　項目を削除　表示を更新

3 **画面を閉じます**

（保存しないで）画面を閉じる　（保存して）画面を閉じる



[設定]を選択



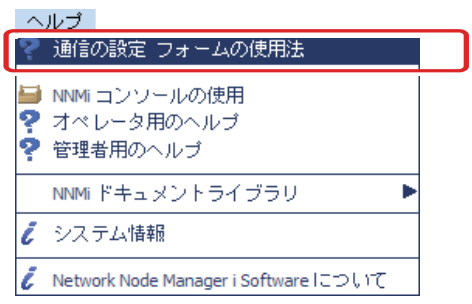
[通信の設定]画面

NNMi の環境設定をします。

ヘルプ

メニューから[ヘルプ]を選択すると、NNMiの次のオンラインヘルプが参照できます。

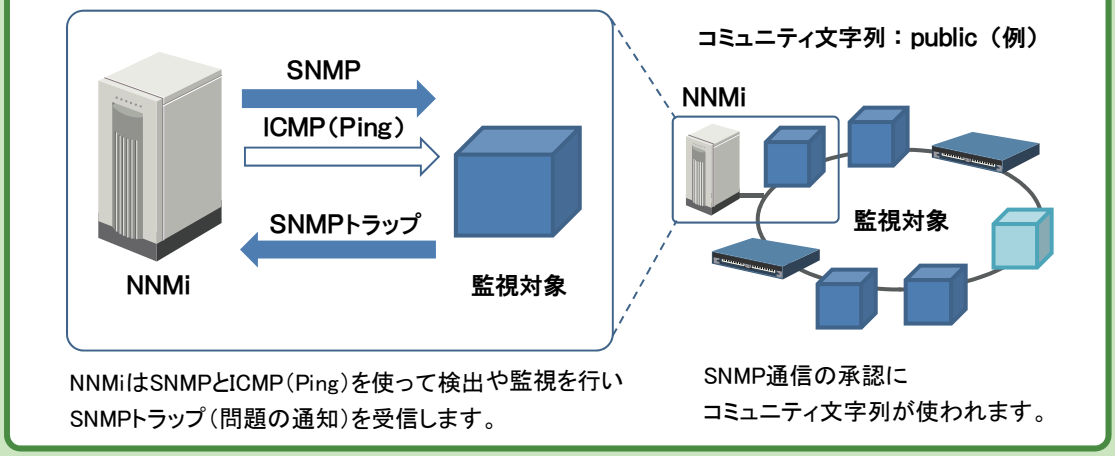
・オペレータ用のヘルプ
・管理者用のヘルプ



一番上には、操作中の画面に関するトピックが表示されるため、知りたい情報がすぐに検索、確認できるようになっています。

2.3 通信の設定

NNMi がネットワークの検出や監視で使う通信プロトコル「SNMP」、「ICMP（Ping）」の動作について設定します。



通信プロトコルを設定する

ヘルプ　【管理者用ヘルプ】-［通信プロトコルを設定する］
マニュアル【セットアップガイド】-［3章 NNMi 通信］

NNMi がネットワークの検出や監視で使う通信プロトコル「SNMP」、「ICMP（Ping）」の動作について設定します。

■操作手順　～通信プロトコルを設定する～

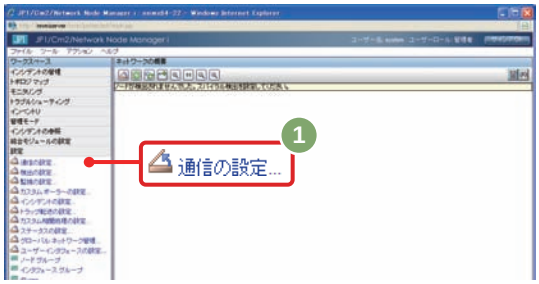
ここでの操作手順は、次の設定内容を例に説明します。

設定内容	設定値
SNMP および ICMP のタイムアウトとリトライ数の設定	デフォルトのまま※
SNMP 最小セキュリティレベル	デフォルトのまま
読み取りコミュニティ文字列	public

※　通常のネットワークでは適切な値です。運用後、必要に応じて調整してください。

1 ワークスペースの[設定] - [通信の設定]を選択します。

[通信の設定]画面が表示されます。



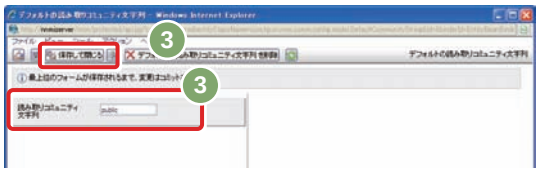
2 [デフォルトのSNMPv1/v2コミュニティ文字列]タブの[ ]([新規作成])をクリックします。

[デフォルトの読み取りコミュニティ文字列]画面が表示されます。

3 [読み取りコミュニティ文字列]を入力し、[保存して閉じる]をクリックします。

（例） 読み取りコミュニティ文字列 : public

[デフォルトの読み取りコミュニティ文字列]画面が閉じます。



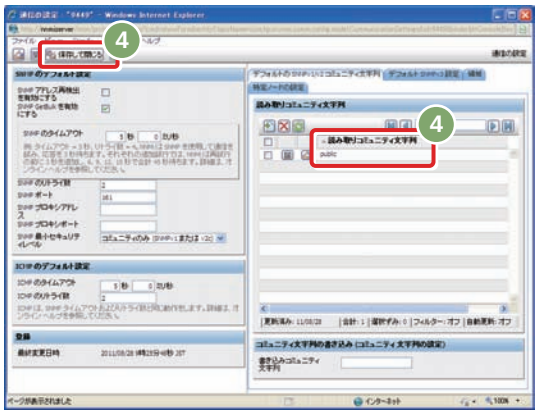
参考

監視するネットワークが複数のコミュニティ文字列を使っている場合は、2 ～ 3 を繰り返して、コミュニティ文字列を複数設定してください。

NNMi は、ネットワークで設定されているコミュニティ文字列を並行してチェックし、適切な値を使います。

4 [通信の設定]画面で、設定した内容が表示されていることを確認し、[保存して閉じる]をクリックします。

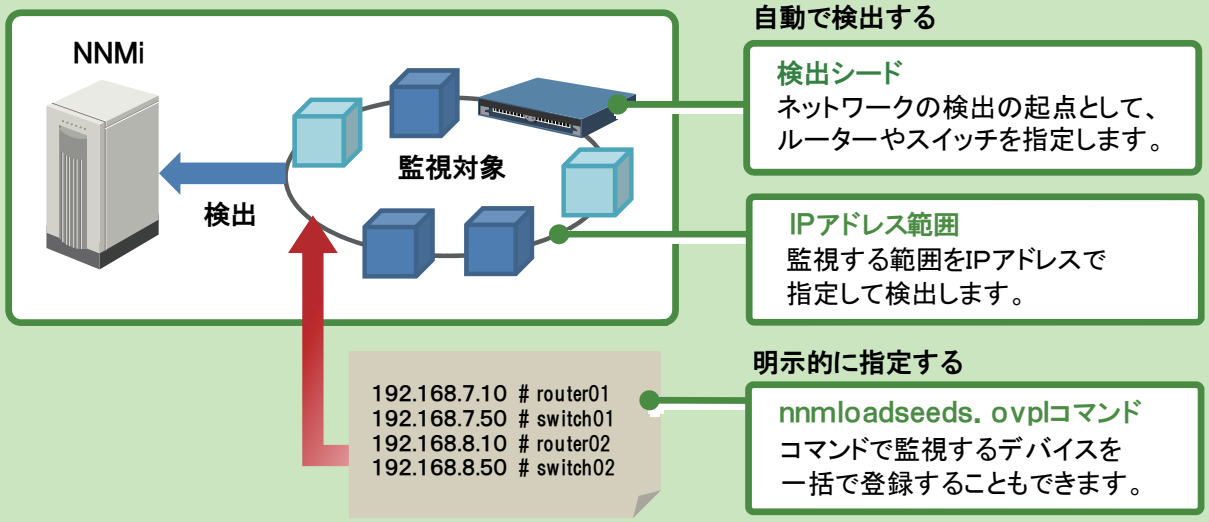
設定した内容が保存され、[通信の設定]画面が閉じます。



これで通信プロトコルを設定する操作は完了です。

2.4 ネットワークの検出

NNMi によるネットワークの検出方法は、[検出の設定]画面から設定します。監視対象の検出には、自動で検出する方法と明示的に指定する方法の 2 種類があり、これらの方法を組み合わせて設定することもできます。



自動で検出する

検出シード
ネットワークの検出の起点として、ルーターやスイッチを指定します。

IPアドレス範囲
監視する範囲をIPアドレスで指定して検出します。

明示的に指定する

nnmloadseeds. ovplコマンド
コマンドで監視するデバイスを一括で登録することもできます。

検出方法を検討する

ヘルプ　【管理者用ヘルプ】-［ネットワークの検出］-［検出のアプローチを決定する］
マニュアル【セットアップガイド】-［4.2 検出の計画］

運用にあわせてネットワークの検出方法を選びます。これらは組み合わせて運用することもできます。

検出方法	説明	こんな運用の場合に
自動で検出する	自動検出ルールを指定することで、NNMi がデバイスを自動的に検出します。	・ネットワーク変更を自動で検出したい ・大規模ネットワークで大量のデバイスがある
明示的に指定する	(検出シードとして)特定のデバイスを明示的に指定します。	・管理対象を厳密に指定したい ・ネットワーク構成が固定的である

自動で検出する場合は、検出対象とするデバイスの範囲(A～C)を決めます。
NNMi はデフォルトでは、ルーターとスイッチだけを検出します。
SNMP デバイス(SNMP に応答するデバイス)や、非 SNMP デバイス(SNMP に応答しないデバイス、ICMP で監視します)を検出するには、次の設定が必要です。

デバイスの範囲(A～C)と、[自動検出ルール]画面との対応

検出方法を設定する（自動で検出する場合）

ヘルプ　【管理者用ヘルプ】-［ネットワークの検出］-［検出の設定］
マニュアル【セットアップガイド】-［4.3 検出の設定］

ネットワークを自動で検出する場合の設定を説明します。
ここでは基本的な項目である[検出の設定]画面の［自動検出ルール］タブと［検出シード］タブの設定について設定します。

［自動検出ルール］画面

［自動検出ルール］タブから［自動検出ルール］画面を表示させて、項目を設定します。

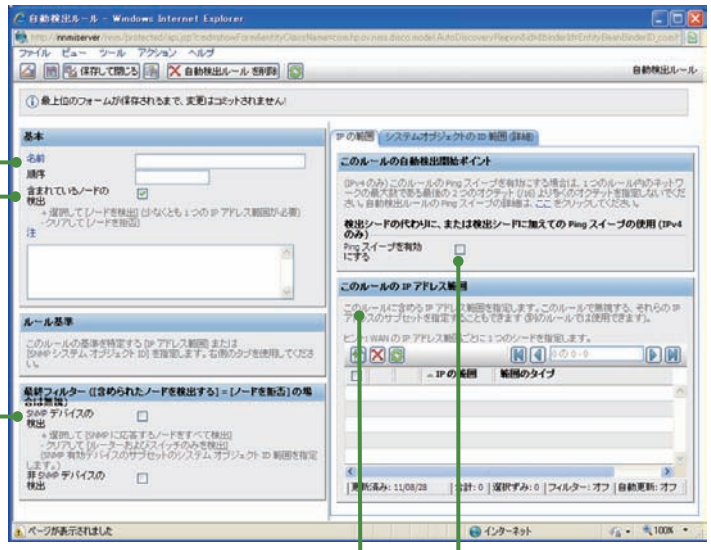
基本
自動検出ルールの「名前」、「順序」を設定します。

自動検出するデバイスの範囲を指定します

含まれているノードの検出
この画面の指定を検出対象にする。
この指定だけの場合は、ルーターとスイッチだけが検出されます。

SNMPデバイスの検出
サーバなどのSNMPデバイスが検出されます。

非SNMPデバイスの検出
非SNMPデバイスが検出されます。



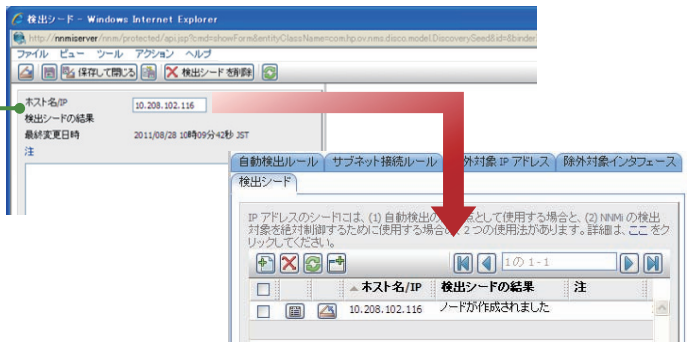
このルールのIPアドレス範囲
検出する範囲をIPアドレスで設定します。
例：10.208.*.*　192.168.30-32

Pingスイープを有効にする
有効にすると、指定したIPアドレスにICMP（Ping）を送信し、デバイスを検出します。

［検出シード］画面

［検出シード］タブから［検出シード］画面を表示させて、項目を設定します。

ホスト名/IP
検出シードをIPアドレスまたはホスト名（FQDN）で指定します。
なお、「Pingスイープを有効にする」にチェックする場合は、指定しなくてもかまいません。

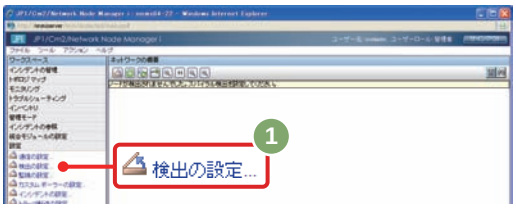


■操作手順 ～自動で検出する～

検出対象のデバイスと検出範囲を設定します

1 ワークスペースの[設定] - [検出の設定]をクリックします。

[検出の設定]画面が表示されます。

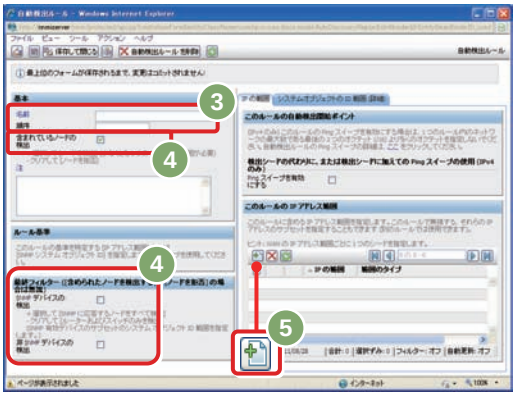


2 [検出の設定]画面で、[自動検出ルール]タブを選択し[ ](新規作成)をクリックします。

[自動検出ルール]画面が表示されます。

3 自動検出ルールの[名前]と[順序]を入力します。

（例） 名前 ： システム部
順序 ： 100



4 自動検出するデバイスの範囲を指定します。

- [含まれているノードの検出]をチェックします。
  この画面の指定範囲を自動検出します。この項目だけをチェックした場合、ルーターとスイッチだけが検出対象となります。
- [SNMP デバイスの検出]と、[非 SNMP デバイスの検出]をチェックします。
  これらをチェックすると SNMP デバイスと、非 SNMP デバイスが検出対象に加わります。

5 [このルールのIPアドレス範囲]の部分にある[ ](新規作成)をクリックします。

[IP の自動検出範囲]画面が表示されます。

6 [IPの範囲]に検出するIPアドレスの範囲を入力します。

（例）IP の範囲 ： 10.208.102.2-254
範囲のタイプ ： ルールに含める

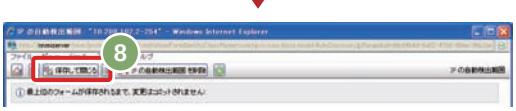
設定例についてはヘルプを参照してください。

7 [保存して閉じる]をクリックします。

設定が保存されて、[IP の自動検出範囲]画面が閉じます。

8 [自動検出ルール]画面に戻ったあと、さらに[保存して閉じる]をクリックします。

設定が保存されて、[自動検出ルール]画面が閉じます。



検出シードを設定します

9 [検出の設定]画面で、[検出シード]タブを選択し、[ ]([新規作成]をクリックします。

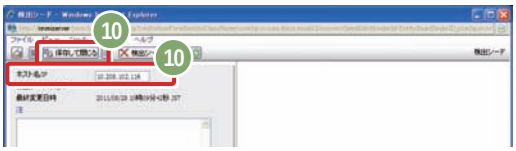
[検出シード]画面が表示されます。

10 「ホスト名/IP」に検出シードのIPアドレスを入力し、[保存して閉じる]をクリックします。

設定が保存され、[検出シード]画面が閉じます。

指定した検出シードに対して、すぐに検出が開始されます。

参考 検出シードに設定するデバイスには、隣接するデバイスの情報を多く持つ、SNMP 対応のルーターを指定してください。



11 [ ]([リフレッシュ]をクリックして、検出シードが作成されたことを確認します。

「検出シードの結果」に「ノードが作成されました」が表示されたら、[保存して閉じる]をクリックします。

[検出の設定]画面が閉じます。

検出方法を設定する(監視対象を明示的に指定する場合)

ヘルプ 【管理者用ヘルプ】-[ネットワークの検出]-[検出の設定]
-[検出ノードを指定する: 初期ルーターまたは検出対象の特定ノード] -[コンソールで検出シードを設定する]
マニュアル【セットアップガイド】-[4.3 検出の設定]

監視対象を明示的に指定する(ネットワークの自動検出を行わない)場合は、[自動検出ルール]を設定しないで、検出シードだけを設定します。

9 以降と同じ手順で、[検出の設定]画面の[検出シード]タブでの設定で、検出対象のデバイスを指定してください。

なお、次の nnmloadseeds.ovpl コマンドを使って、検出シードを一括して登録することもできます。

直接シードを指定する場合

＜形 式＞ nnmloadseeds.ovpl -n *シード△シード△・・・△シード*

△は半角スペースを入力します。

＜実行例＞ nnmloadseeds.ovpl -n 192.168.8.82 192.168.100.24

シードの一覧ファイルを指定する場合

＜形 式＞ nnmloadseeds.ovpl -f *シードファイル*

＜実行例＞ nnmloadseeds.ovpl -f c:¥jp1¥seeds.txt

＜シードファイルの例＞

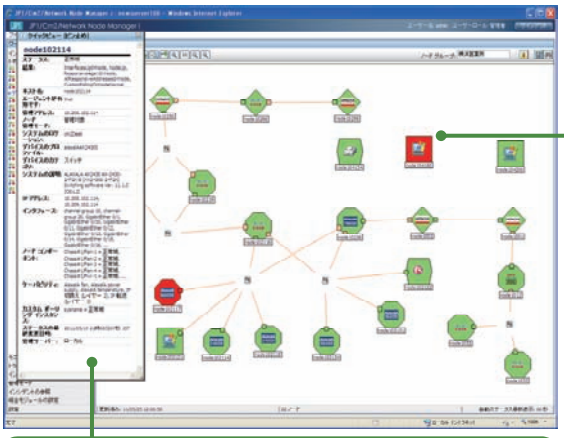
```
192.168.8.82      # node1
192.168.100.24    # node2
```

以降は[検出シード]画面の[注]の項目に表示されます。
マルチバイト文字を記入する場合は UTF-8 で記入します。

検出したネットワークを参照する

ヘルプ　【コンソールの使用】-［ビューを使用してデータを表示する］-［マップビューの使用］

トポロジマップで、検出したネットワークを参照しましょう。なお、検出の設定をした直後は、NNMi がノードを検出していく過程を参照することができます。



アイコンにカーソルを置くと、詳細が表示されます。

検出したノードは、アイコンの色で状態を確認できます。
アイコンの色の意味を次の表に示します。

アイコンの色と意味			
緑色	正常域	赤色	危険域
水色	注意域	青色	認識不能
黄色	警戒域	グレー	無効
オレンジ	重要警戒域	ベージュ	ステータスなし

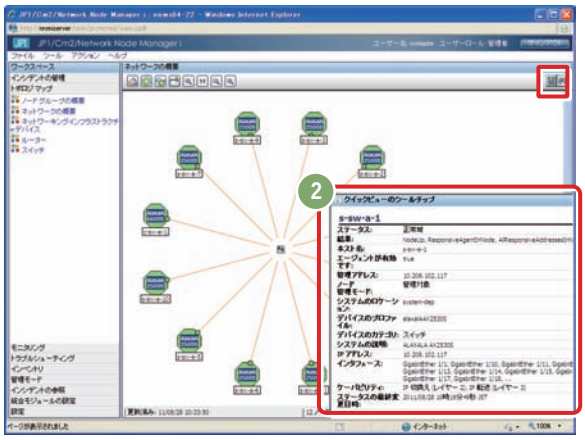
■操作手順　～検出したネットワークを参照する～

1 ワークスペースの[トポロジ マップ] - [ネットワークの概要]をクリックします。

［ネットワークの概要］画面が表示されます。

2 アイコンの色や詳細から、ノードの状態を確認します。

- アイコンをダブルクリックすると、［ノード］画面が開き、詳細を確認できます。
- アイコンにカーソルを置くと、クイックビューにより詳細が表示されます。
  クイックビューは画面右上の［ ］（クイックビューを無効にする）をクリックすると表示されなくなります。



これで検出したネットワークを参照する操作は完了です。

検出されたデバイスを確認する

ヘルプ　【管理者用ヘルプ】-［ネットワークの検出］-［検出結果を検証する］
マニュアル【セットアップガイド】-［4.4 検出の評価］

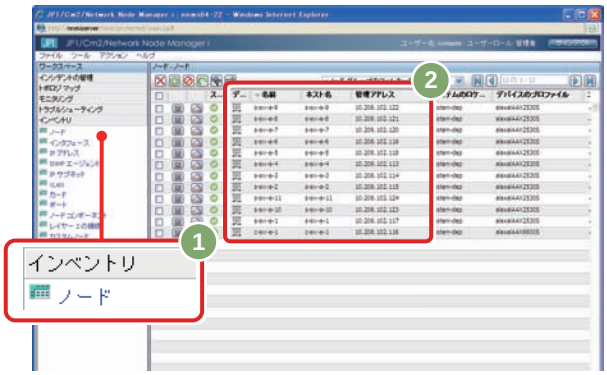
■操作手順　～検出されたデバイスを確認する～

1 ワークスペースの[インベントリ] - [ノード]をクリックします。

[ノード - ノード]画面が表示されます。

2 自動検出の対象として設定したデバイスが、正しく検出、登録されているかを確認します。

設定した IP アドレスの範囲でデバイスが表示されていれば、自動で検出する操作は問題なく実施できています。

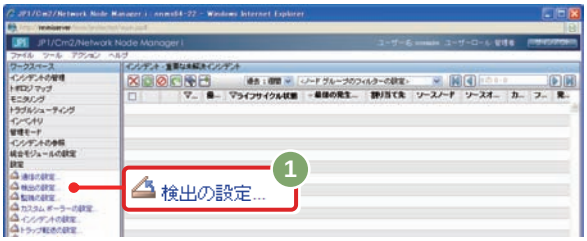


検出が完了した検出シードを削除する

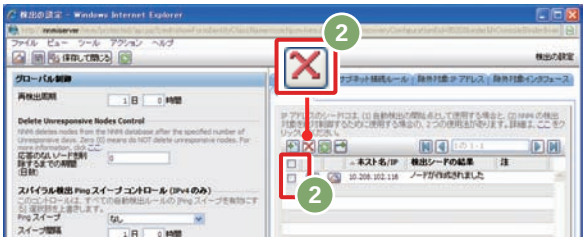
ノードの検出が完了したら検出シードを削除します。

■操作手順　～検出が完了した検出シードを削除する～

1 ワークスペースの[設定] - [検出の設定]をクリックして、[検出の設定]画面を開きます。



2 [検出シード]タブで、すべての検出シードをチェックしてから、[ ]（削除）をクリックします。



3 検出シードが削除されたことを確認して、[保存して閉じる]をクリックします。

検出したノードを削除する

ヘルプ　【管理者用ヘルプ】-［ネットワークの検出］-［トポロジを正確に維持］-［ノードの削除］

監視が不要なノードが検出された場合、そのノードを監視対象から削除することができます。

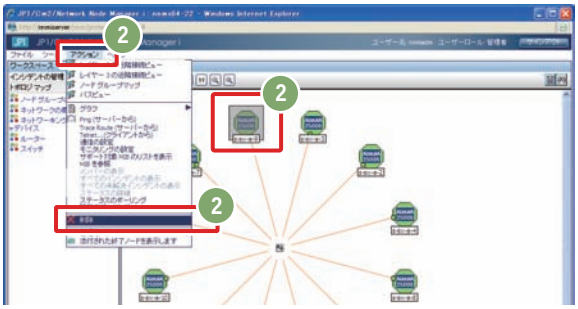
■操作手順　～検出したノードを削除する～

1 ワークスペースの[トポロジ　マップ] - [ネットワークの概要]をクリックします。

[ネットワークの概要]画面が表示されます。

2 削除するノードのアイコンをクリックし、メニューから[アクション] - [削除]をクリックします。

クリックしたノードが削除されます。



これで検出したノードを削除する操作は完了です。

困ったときは　検出したノードが削除できない

検出シードとして指定したノードは検出シード一覧からも削除してください

検出シードとして指定されたノードは、ここで説明する手順で削除しても、[検出の設定]画面の[検出シード]タブに表示される一覧からは削除されません。

＜対処方法＞

[検出の設定]画面の[検出シード]タブで直接、検出シードから削除してください。

一度削除したノードが再検出されることがあります

削除したノードが自動検出ルールの検出対象として含まれている場合は、次回の周期で再検出されます。

＜対処方法＞

再検出させたくない場合は、[検出の設定]画面の[自動検出ルール]で[IP の検出範囲]を指定するときに、検出したくない IP と検出タイプ[ルールにより無視された]を指定してください。

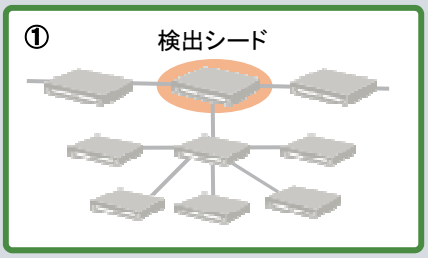
解説

「検出」 ～ネットワークを検出する～

NNMi はネットワーク上のデバイスの情報を収集し自動検出する機能によって、個々のデバイスの詳細と、ネットワーク構成（トポロジ）とを把握します。ここでは NNMi の理解を深めるために、ネットワークの検出の仕組みを説明します。

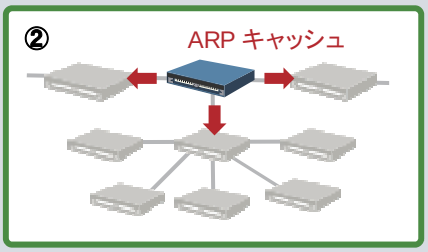
ネットワーク構成の検出

NNMi は、各デバイスの持つ ARP キャッシュ情報や LLDP（Link Layer Discovery Protocol）などのプロトコルで認識した隣接デバイスの情報を、SNMP により収集することでネットワーク全体を検出します。ここでは、ARP キャッシュによる検出を例に説明します。



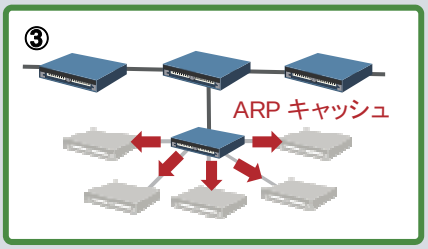
図①

「検出シード」を指定すると、NNMi は検出シードの検出処理をします。検出シードは、ネットワーク検出の起点となるデバイスです。



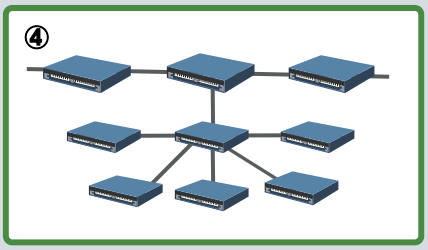
図②

次に NNMi は、検出シードに SNMP で接続し、ARP キャッシュの情報を取得します。これをもとに隣接するデバイスを検出します。



図③

NNMi は検出したデバイスに接続して、同様に情報を取得します。ARP キャッシュからさらに次のデバイスを検出します。



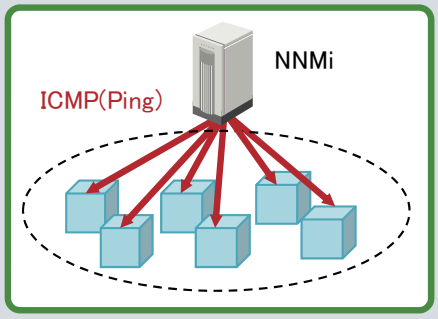
図④

この検出処理を指定された検出範囲で繰り返すことで、ネットワークに接続されたデバイスを次々と検出し、ネットワークの構成を把握します。

（凡例）  ：スイッチまたはルーター

Pingスイープによる検出

Ping スイープとは、指定された IP アドレスの範囲を ICMP（Ping）を使って監視し、応答のあったデバイスを検出する方法です。



次のようなメリット、デメリットがあります。運用に応じて Ping スイープを使ってください。

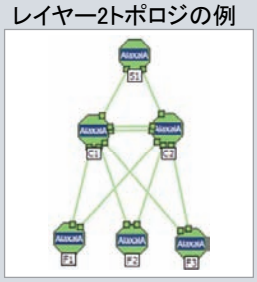
メリット　：指定したネットワークの範囲のデバイスを素早く検出できる。
デメリット：ネットワークに負荷がかかる。

Ping スイープを使うときは、対象範囲を絞ることをお勧めします。

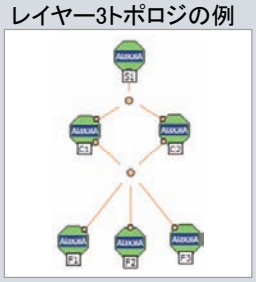
レイヤー2トポロジとレイヤー3トポロジ

NNMi は、ネットワークのトポロジ（ネットワークの構成）を、レイヤー3トポロジだけでなく、レイヤー2トポロジも認識して表示することができます。

レイヤー2トポロジの例



レイヤー3トポロジの例



■レイヤー2トポロジをどのように認識するか

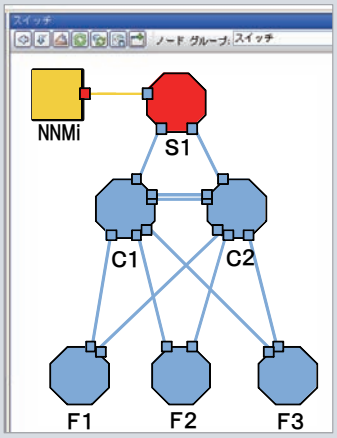
IP ネットワークの通信では、あて先を IP アドレスで指定し、通常は物理的な結線を意識しません。また、NNMi の設定作業でも、物理的な結線の情報を直接入力する必要はありません。
それでは、NNMi はどのように物理的な結線を認識するのでしょうか。
NNMi は、デバイスが LLDP などのプロトコルを使って認識している隣接デバイスの情報を、SNMP の読み取り要求により MIB(Management Information Base)情報として収集し保持します。
NNMi は、このような隣接デバイスに関する MIB 情報を収集・解析することで物理的な結線であるレイヤー2トポロジを認識します。

■レイヤー2トポロジの効果

レイヤー2 トポロジ（物理的な結線）を認識すると、ネットワークでの問題の原因をより詳しく分析できます。

例えば、NNMi が接続するスイッチ（S1）に障害が発生し、その先のネットワークと通信ができなくなった場合のレイヤー2 トポロジを右の図に示します。
IP アドレスでの通信（レイヤー3）だけで判断すると、多数のデバイスと通信できないため、広範囲なネットワーク障害と判定されてしまいます。
しかし、このレイヤー2 トポロジマップのように、物理的な結線を認識できていれば、障害が発生したスイッチと、その影響によって通信ができないデバイスを判断できます。
NNMi の根本原因解析機能では、このようなレイヤー2トポロジの情報を有効に活用して、根本原因を解析します。これについては、3章の「解説「インシデント」 ～重要な事象に絞って通知する～」の「根本原因解析」で説明します。

NNMi



■名前の由来

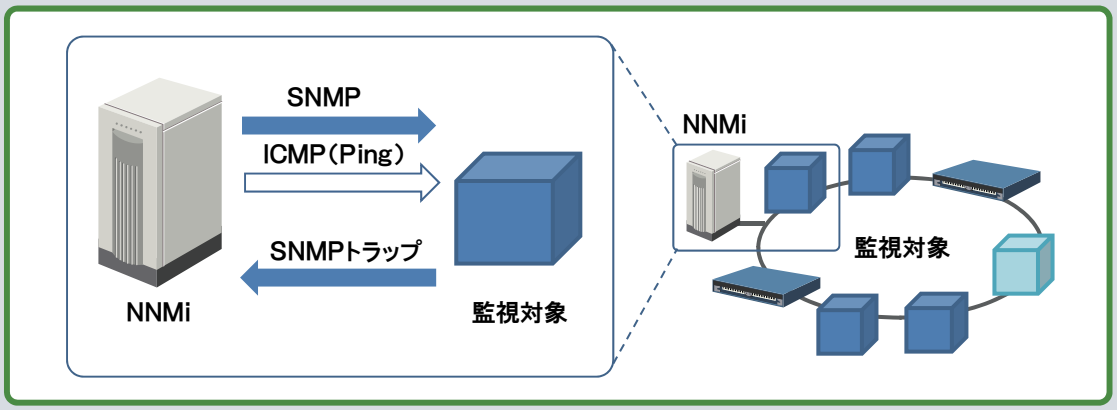
レイヤー2、レイヤー3 という名前は、OSI7 層モデルに由来しています。

レイヤー2（データリンク層）： MAC アドレスにより物理リンク間のデータ転送などを制御します。
レイヤー3（ネットワーク層）： IP アドレスによりネットワークのルート選択などを制御します。

詳細は　ヘルプ　【オペレータ用ヘルプ】 - [マップの表示（ネットワーク接続性）]

ネットワーク上のデバイスの検出

NNMi は、ネットワーク構成（トポロジ）を把握しながら、ネットワーク上にあるデバイスを検出し詳細情報を収集していきます。

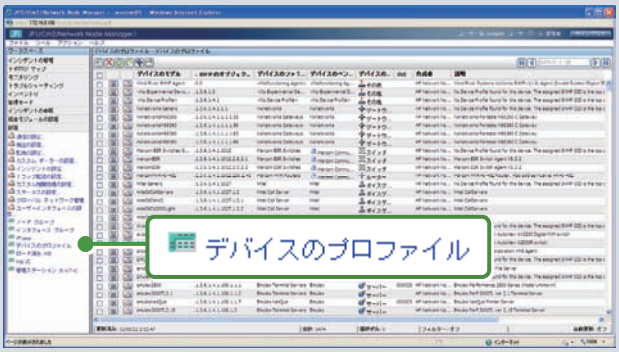


NNMi は、SNMP と ICMP（Ping）を使ってデバイスの検出を行い、各デバイスの詳細情報を収集します。
デバイスは、SNMP に応答するかどうかによって SNMP デバイスまたは非 SNMP デバイスと認識されます。

SNMPデバイス	・・・SNMP に応答するデバイス　収集した詳細情報で種別を判定する
非SNMPデバイス	・・・SNMP に応答しないデバイス

■デバイスの種類の認識

SNMP デバイスは、システムオブジェクト ID（sysObjectID）の情報を SNMP で収集してデバイスの種類（デバイスプロファイル）を判定します。
sysObjectID とは機器の種別（ベンダー、デバイスタイプ、モデル）を一意に表す情報です。
NNMi はワークスペースの［設定］－［デバイスのプロファイル］に登録された 5,000 種類以上のデバイス情報によってデバイスの種類を自動判定します。



［設定］－［デバイスのプロファイル］画面

デバイスプロファイルが決まると、分類（デバイスのカテゴリ）により、マップ画面上でのアイコン形状が決められます。

背景形状	前面形状/意味	背景形状	前面形状/意味
■	= シャーシ = コンピュータ = サーバー = ワークステーション = その他 注：「*その他*」には、非 SNMP ノードが含まれます。	⬢	= アナライザ = ファイアウォール = ロードバランサ = ネットワーク機器 = 電源 = プリンタ = ワイヤレスアクセスポイント
●	= ATM スイッチ = スイッチ	◆	= ゲートウェイ = ハブ = ルータ = スイッチルータ = ボイスゲートウェイ
■	子ノード グループ	▲	= IP フォン

［ヘルプ］－【コンソールの使用】－［ビューを使用してデータを表示する］－［マップビューの使用］－［マップについて］－［マップの記号について］

■デバイスの詳細の認識

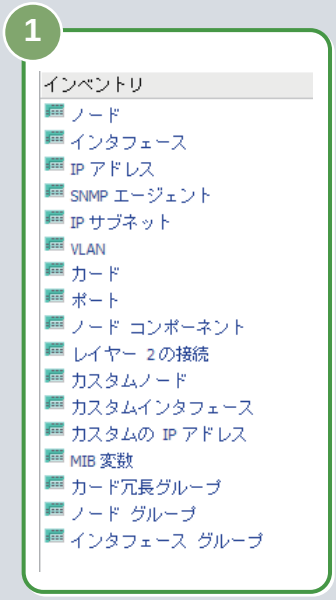
NNMi が収集したデバイスの詳細情報は、
ワークスペースの[インベントリ]で参照できます。

1 インベントリの項目

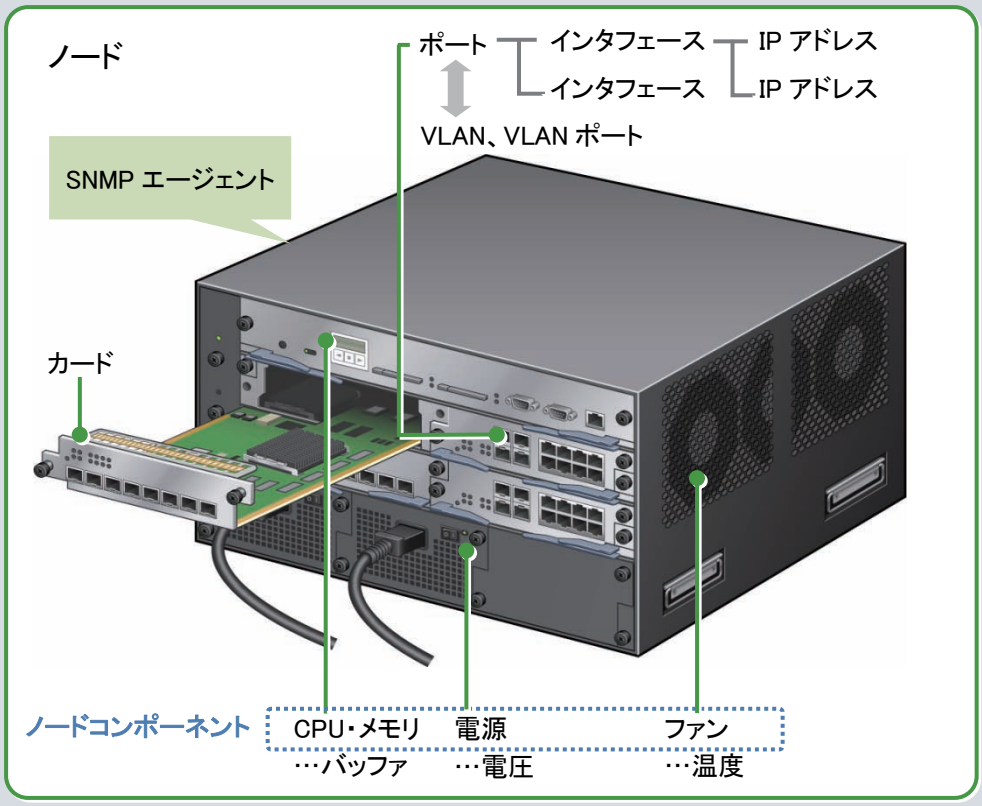
2 デバイスのカテゴリ

3 デバイスのプロファイル

実際のデバイスを NNMi がどのように認識しているか、インベントリの項目と比較して見てみましょう。



[インベントリ]画面の項目



NNMi によるデバイスの認識（概念図）

図のように、NNMi はデバイスの構成を詳細に認識し、監視を行います。
監視については、3 章の解説「モニタリング」 ～ネットワークを監視する～ で説明します。

2.5 ノードグループの設定

ノードグループは[ノード グループ]画面から設定します。
ノードグループを設定すると、検出したノードをネットワーク構成に依存しないで自由にグループ化できます。

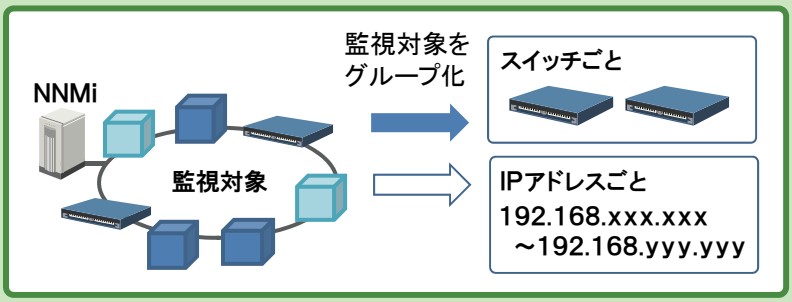
グループ化するメリット

モニタリング

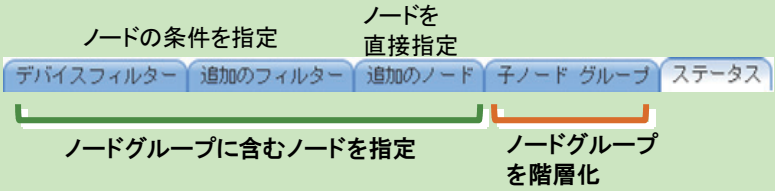
特性や運用に応じて、ノードグループ単位で適切な監視条件を設定できます。

ノードの表示

ノードグループ単位でのフィルタリングやマップの表示ができます。



[ノード グループ]画面のタブ



ノードグループは、子ノードグループを定義することで階層化できます。

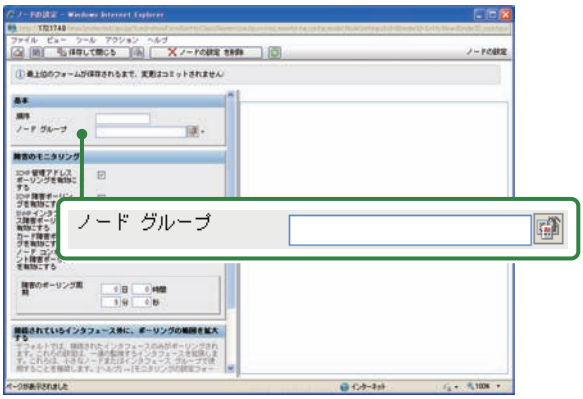
階層の深さは、5 階層までです。

ノードグループの活用方法

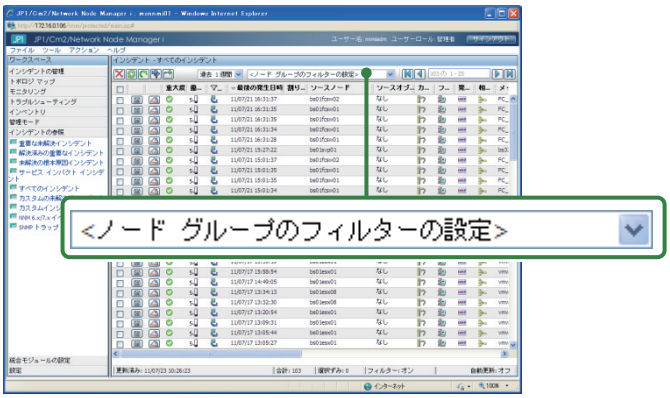
ヘルプ　【管理者用ヘルプ】-［ノードまたはインタフェースのグループ作成］

ノードグループを定義すると、ノードグループごとのモニタリングの設定やノードグループ単位でのフィルタリングができるようになります。このほか、NNMi コンソールの初期画面として任意のノードグループ画面を表示することもできます。

モニタリングの設定 - [ノードの設定]画面



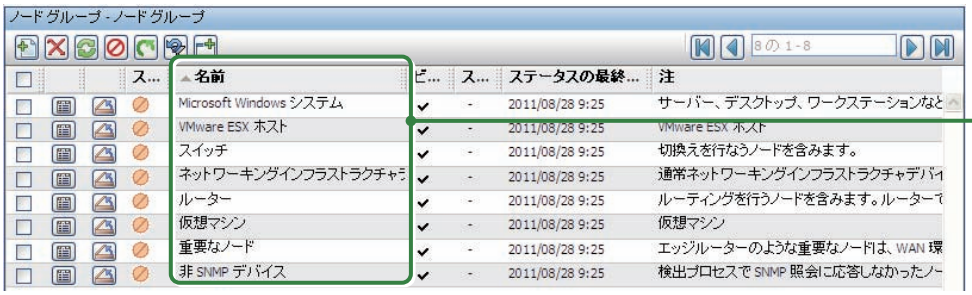
[インシデント - 重要な未解決インシデント]画面



標準のノードグループ

ヘルプ 【管理者用ヘルプ】
- [ノードまたはインタフェースのグループ作成] - [NNMiが提供するノードグループ]

Windows やルーターなど、基本的な種別ごとに適切な設定がされたノードグループが標準で用意されています。これらのノードグループの設定を使って、すぐに NNMi の運用を始めることができます。



NNMi Advanced の場合だけ[VMwareESX ホスト]と[仮想マシン]が自動認識されます。

参考

「重要なノード」ノードグループについて

使い方

重要なサーバやネットワーク機器を登録します。
「重要なノード」の応答がない場合に、SNMP デバイスは「ノード停止(NodeDown)」インシデント、非 SNMP デバイスは「非 SNMP ノードが応答なし(NonSNMPNodeUnresponsive)」が発行されます。

説明

「重要なノード」ノードグループに含めたノードは、特別な扱いになります。

NNMi は、3 章の解説「インシデント」 ～重要な事象に絞って通知する～ で説明するように、発生した事象をそのまま通知するのではなく、監視結果を解析し、根本原因に絞って通知します。この根本原因解析は、問題に迅速に対応でき、運用負担を低減する有用な機能ですが、運用上の弊害が生じるケースもあります。
例えば、ある重要なサーバが、ネットワーク経路上のルータ障害によって通信できなくなったとします。
この場合、ルータ障害は根本原因としてインシデントが通知されます。しかし、重要なサーバは通信ができなくても、ルータ障害の影響による事象(根本原因ではない)と判定されインシデントは通知されません。

無応答時に、根本原因ではなくてもインシデントを通知したいノードがある場合は、「重要なノード」に登録します。「重要なノード」に登録したノードは、根本原因解析の機能がそのノードを特別に扱い、無応答の場合に「ノード停止(NodeDown)」や「非 SNMP ノードが応答なし(NonSNMPNodeUnresponsive)」のインシデントが発行されます。

備考

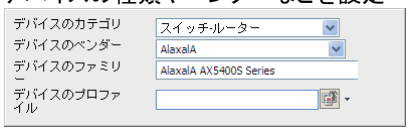
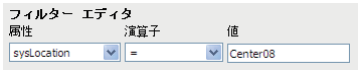
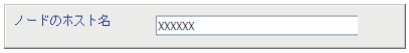
「重要なノード」ノードグループに、子ノードグループを階層化して設定した場合や、他ノードグループに含まれるノードを追加した場合でも、「重要なノード」と同じ効果(NodeDown や NonSNMPNodeUnresponsive が発行される)になります。

ノードグループを設定する

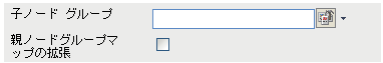
ヘルプ　【管理者用ヘルプ】-［ノードまたはインタフェースのグループ作成］
-［ノードグループの作成］-［コンソールでノードグループを作成する］

ノードグループを設定してみましょう。ノードグループは、［ノード グループ］画面で次のように設定します。

グループ化の条件

設定するタブ	設定内容	運用での活用例
［デバイスフィルター］	デバイスの種類やベンダーなどを設定 	• デバイスの重要度に応じて監視する • 機種ごとに適切な監視方法を設定する • ルーターだけ表示するなど、フィルターで絞り込んで素早く状況を把握する
［追加のフィルター］	hostedIPAddress（IP アドレス）やsysLocation（場所）などを設定 	• 設置場所や組織の単位で、監視条件を設定したり表示をフィルタリングしたりする 注　SQL の演算子(between、in、like など)を使って柔軟な条件でグループ化できる
［追加のノード］	ホスト名を直接設定 	• 特に重要なノードなどを個別に設定する • 条件指定が難しいノードを設定する

ノードグループの階層化

設定するタブ	設定内容	運用での活用例
［子ノード グループ］	子ノード グループの名前を階層順に設定 	• 職場や地域ごとにノードグループを階層化する

■操作手順　～ノードグループを設定する～

ノードグループを作成します

1 **ワークスペースの[設定] - [ノード グループ]をクリックします。**

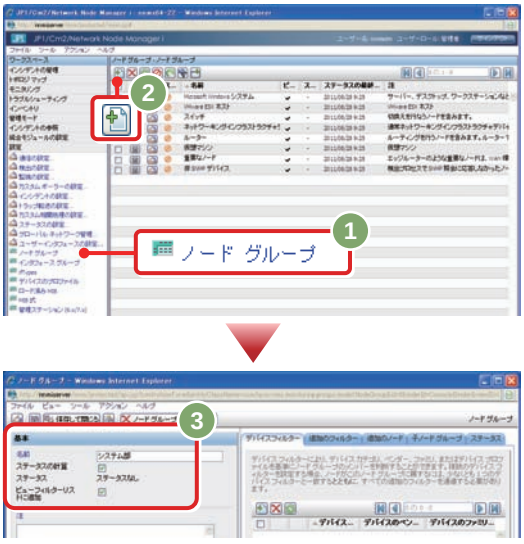
［ノード グループ - ノード グループ］画面が表示されます。

2 **[ ](新規作成)をクリックします。**

［ノード グループ］画面が表示されます。

3 **ノードグループの[名前]を設定します。**

（例）　名前　　：　システム部



参考　［ビューフィルターリストに追加］をチェックすると、［ノード］画面や［インシデント］画面の［ノードグループのフィルターの設定］欄に、作成するノードグループの名前が表示されます。

ノードグループの対象としたいノードを設定します

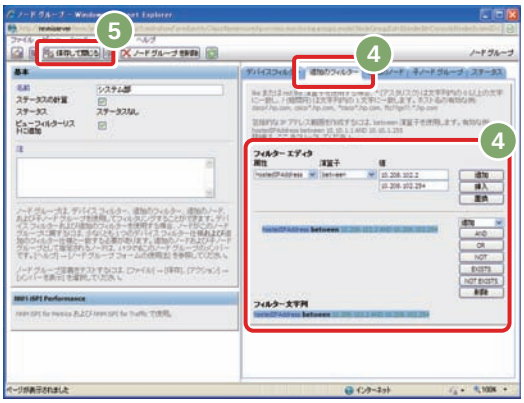
4 [追加のフィルター]タブで、ノードグループに追加するノードの条件を指定します。

- [属性][演算子]を選択して[値]を入力し、[追加]をクリックします。

  （例） 属性： hostedIPAddress、 演算子： between

  値 ： 10.208.102.2 ～ 10.208.102.254

- 指定した条件式が、[フィルター文字列]に追加されたことを確認します。
- 条件式を削除したい場合は、条件式をクリックして青色の選択状態にしたあと、[削除]をクリックします。



5 [保存して閉じる]をクリックします。

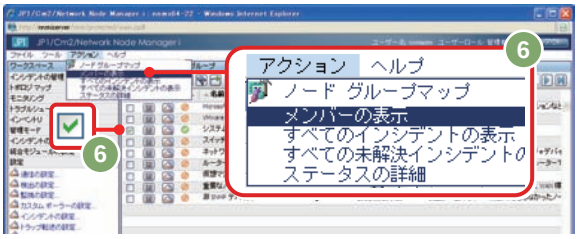
[ノード グループ]画面が閉じ、ノードグループが作成されます。

作成したノードグループを確認します

6 ノードグループのメンバーを表示します。

[ノード グループ - ノード グループ]画面で、目的のノードグループをチェック( )して、[アクション] - 「メンバーの表示」をクリックします。

[ノード － ノード]画面が表示されます。



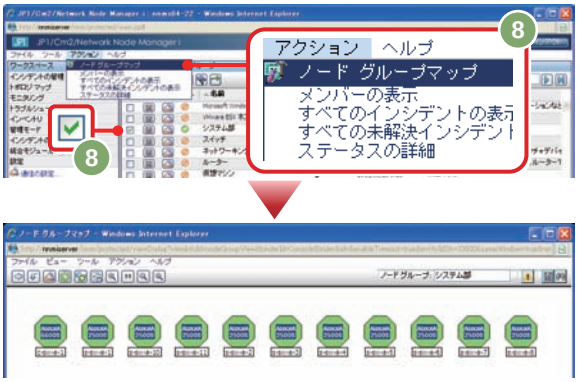
7 ノードグループに、対象として指定したノードが含まれていることを確認します。

確認後、[ノード － ノード]画面を閉じます。

8 ノードグループのマップを表示します。

6 の手順と同じように、目的のノードグループをチェック( )して、[アクション] - [ノードグループマップ]を選択します。

ノードグループがマップ形式で表示されます。

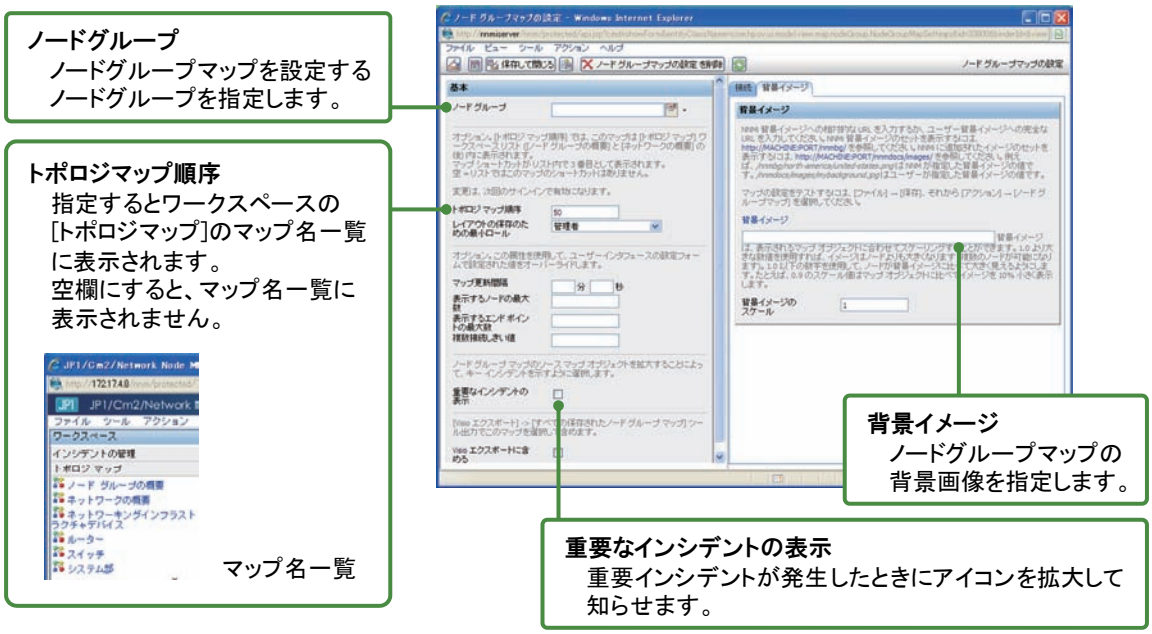


これでノードグループを設定する操作は完了です。

ノードグループマップを設定する

ヘルプ　【管理者用ヘルプ】-［NNMi ユーザーインタフェースを設定する］-［マップの設定］-［ノードグループマップの設定の定義］

ノードグループマップの設定をすると、背景イメージに任意の画像を指定できます。また、ワークスペースの[トポロジマップ]のマップ名一覧に、作成したノードグループマップを表示することができます。

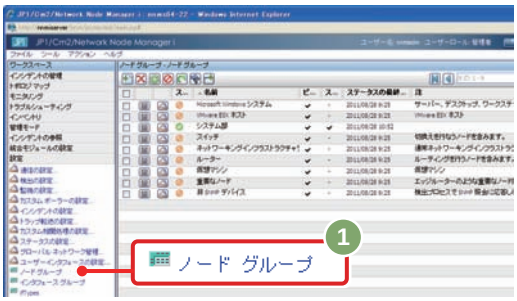


■操作手順　～ノードグループマップを設定する～

ノードグループマップを設定します

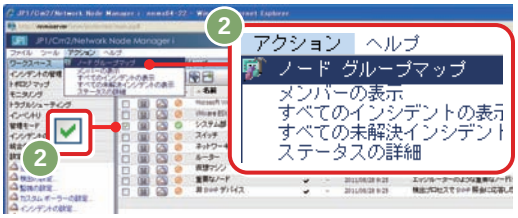
1. **ワークスペースの[設定] - [ノードグループ]をクリックします。**

   ［ノード グループ － ノード グループ］画面が表示されます。



2. **マップを設定したいノードグループをチェック( )して、[アクション] - [ノードグループマップ]をクリックします。**

   ［ノード グループマップ］画面が表示されます。



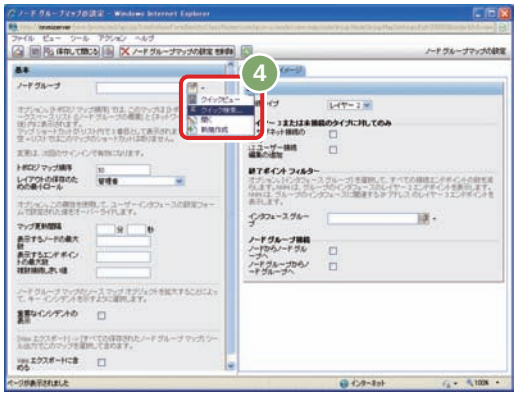
3. **メニューから[ファイル] - [ノードグループマップの設定を開く]をクリックします。**

   ［ノード グループマップの設定］画面が表示されます。

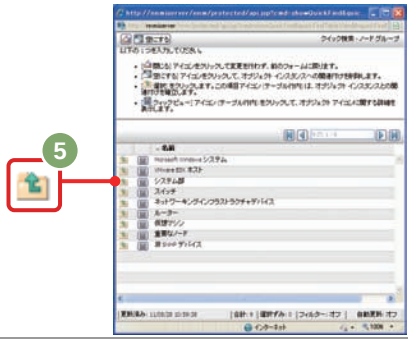
4 **ノードグループマップの設定を始めます。**

まず、[ノードグループ]を入力し、[ ]から[クイック検索]をクリックします。

[クイック検索 － ノード グループ]画面が表示されます。

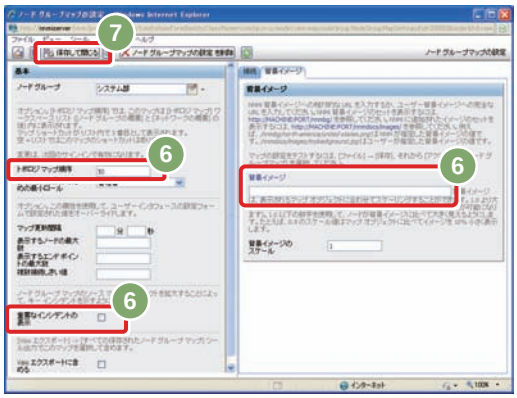


5 **対象のノードグループを選択し、[ ](この項目を選択)をクリックします。**



6 **ノードグループマップに各種設定をします。**

- **[背景イメージ]を設定します。**
  [背景イメージ]タブでマップの背景画像を指定します。Web ブラウザで表示できる gif、png、jpg などが使えます。
  画像ファイルを NNMi サーバの次のフォルダに格納します。
  インストール先フォルダ(データ用)¥shared¥nnm¥www¥htdocs¥images
  [背景イメージ]には次のように入力します。
  (例)/nnmdocs/images/画像ファイル名
- **[トポロジマップ順序]を指定します。**
  この項目を指定すると、作成したノードグループが、[トポロジマップ]ワークスペースのマップ名一覧に表示されます。
  空欄にすると、マップ名一覧に表示されません。
  これは次にサインインしたときから表示されます。
- **[重要なインシデントの表示]を指定します。**
  チェックをすると、重要なインシデントが発生したときに、マップ上のアイコンが大きく表示され、問題発生個所が見つけやすくなります。



7 **設定が終わったら[保存して閉じる]をクリックします。**

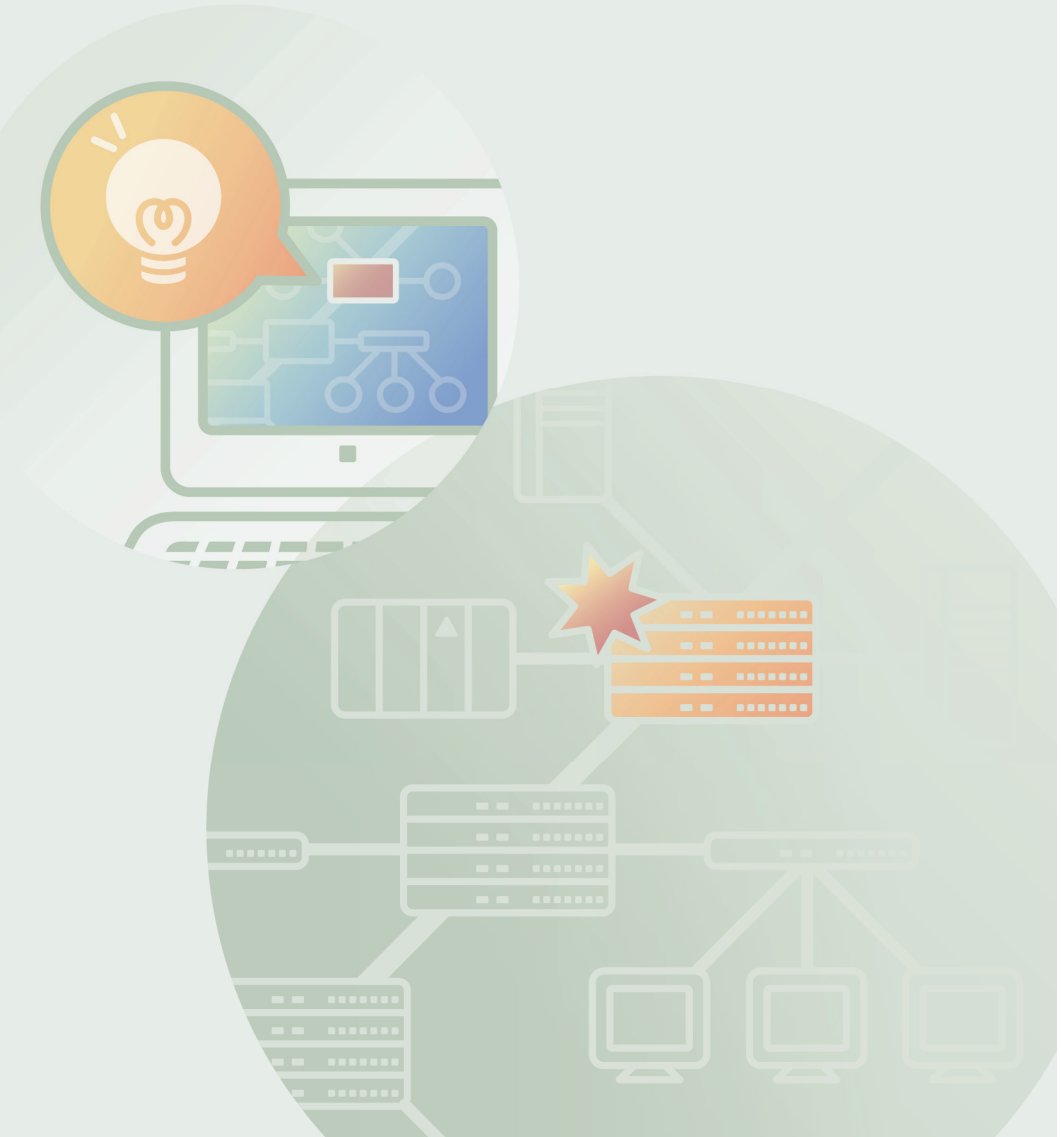
8 **アイコンの位置を調整したあと、[ ](レイアウトの保存)をクリックします。**

アイコンの位置が保存されます。

これでノードグループマップを設定する操作は完了です。

3章

把握したノードを監視する



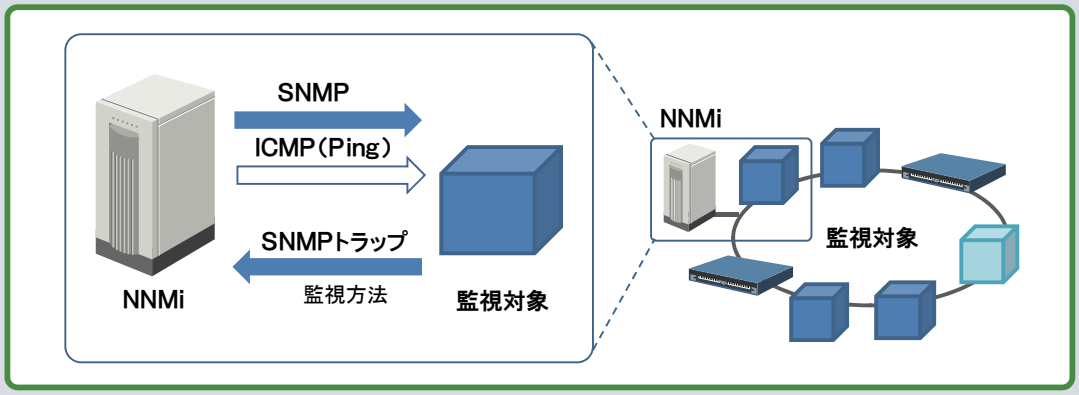
解説

「モニタリング」 ～ネットワークを監視する～

NNMi は、検出したネットワーク上の各ノードが正しく動作しているかを周期的に監視します。ここでは、何をどのように監視しているのか、NNMi の監視の仕組みを説明します。

NNMiでのネットワークの監視

NNMi は、検出したノードを監視対象として、SNMP と ICMP(Ping)により、ノードの状態を監視（モニタリング）します。監視はデフォルトでは 5 分周期で行い、監視対象の状態を確認します。



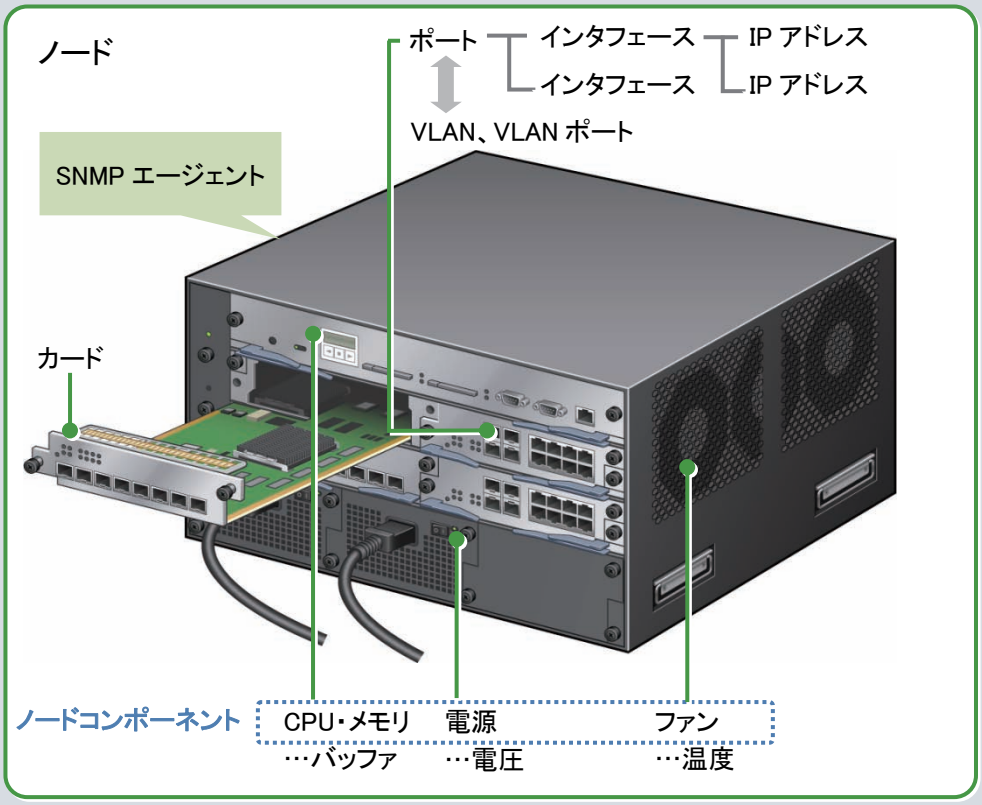
■監視対象（何を監視するか）

NNMi は、検出ポーリングによって検出したデバイスを対象として、周期的に監視（モニタリング）を行います。

SNMP デバイスの場合、デバイスの構成に合わせて SNMP により情報を収集し、監視を行います。監視方法の詳細は[モニタリングの設定]画面により設定します。

（[インベントリ]画面の項目のうち、[インタフェース]、[SNMP エージェント]、[カード]、[ノードコンポーネント]を SNMP で監視し、[IP アドレス]を ICMP（Ping）で監視します。[ノード]は最も深刻な未解決の結果がステータスに反映されます。ほかの項目は、構成を管理する情報やグループ化した情報などです。）

[インベントリ]画面の項目

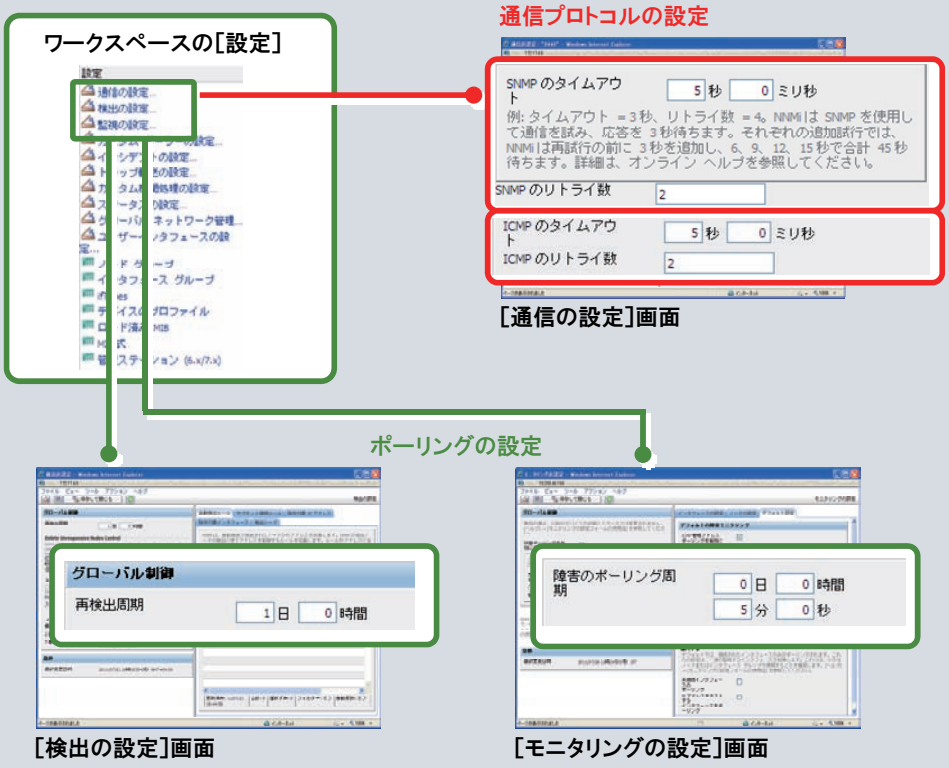


NNMi によるデバイスの認識（概念図）

デバイスの「検出」と「監視」の関係

NNMi は、検出したネットワーク上のデバイスを監視対象として、その状態を周期的に監視します。
検出と監視は連動してそれぞれが適切な周期により行われ、デフォルトの設定では、検出を 1 日に一度行い、検出したデバイスを 5 分おきに状態を監視します。
NNMi が周期的に行う「検出」と「監視」のポーリング、およびポーリングに使う通信プロトコル SNMP と ICMP(Ping) についての関係をまとめると次のようになります。

設定画面	設定対象	説明	設定項目とデフォルト値
通信の設定	SNMP と ICMP（Ping）のプロトコルについての動作	SNMP や ICMP（Ping）のプロトコルにおける、1 通信ごとのタイムアウトやリトライ数を設定します。 この設定に基づいて、検出および監視の通信が行われます。	SNMP ： 5 秒でタイムアウト（リトライ数は 2 回） ICMP（Ping） ： 5 秒でタイムアウト（リトライ数は 2 回）
検出の設定	SNMP や ICMP（Ping）を使って、ネットワーク構成を検出するときの動作	検出は、通常は構成が頻繁に変わらないため、日単位で再検出する設定にします。 検出したデバイスは、[監視の設定]により周期的に状態を監視します。	再検出周期 ： 1 日
監視の設定	SNMP や ICMP（Ping）を使って、ネットワーク状態を監視するときの動作	監視は、障害を迅速に検出するため短い周期にしますが、監視負荷を適切におさえる事も重要ですので、分単位でポーリングする設定にします。	障害ポーリング周期 ： 5 分

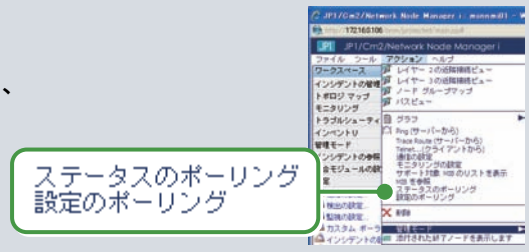


■即時のポーリングをするには

ノードを選択して、メニューの[アクション]から次の操作を行うことで、即時のポーリングが行われます。

・[ステータスのポーリング]: 状態ポーリングを行います。

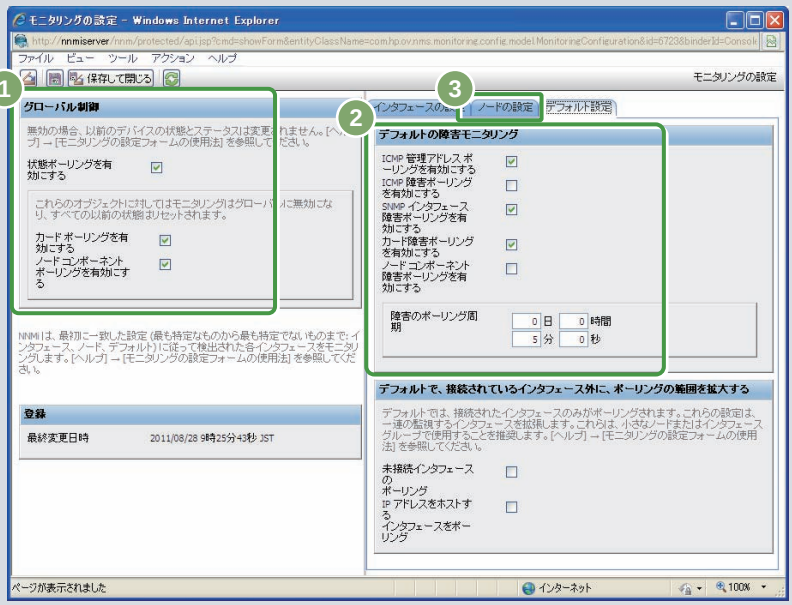
・[設定のポーリング]: 検出ポーリングを行います。

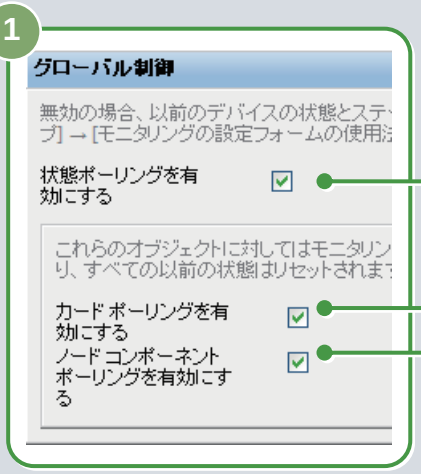


モニタリングの設定

■監視方法（どのように監視するか）

NNMi は、監視対象の状態を、
SNMP 読み取り要求および ICMP(Ping)を
使って監視します。
監視方法は、[モニタリングの設定]画面で
詳細を設定することができます。





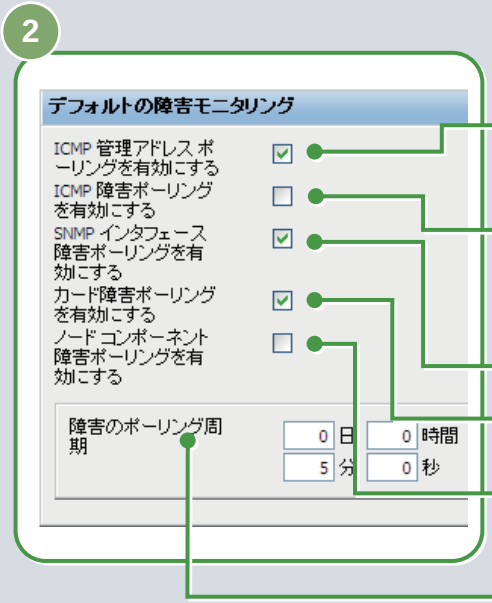
「SNMP エージェント」「インタフェース」および「IP アドレス」の稼働状態を監視します。

- ・SNMP エージェント ： SNMP で監視
- ・インタフェース ： SNMP で監視
- ・IP アドレス ： ICMP (Ping)で監視

「カード」の状態を、SNMP で監視します。

「ノードコンポーネント」の状態を、SNMP で監視します。

カードおよびノードコンポーネントは、NNMi がサポートする特定機種だけで監視できます。



管理アドレスに分類した「IP アドレス」を、ICMP(Ping)で監視します。

管理アドレスとは、NNMi がそのノードの SNMP エージェントと通信する場合に使用する IP アドレスです。

「IP アドレス」を、ICMP(Ping)で監視します。

「インタフェース」の状態を、SNMP で監視します。

「カード」の状態を、SNMP で監視します。

「ノードコンポーネント」の状態を、SNMP で監視します。

状態の監視を行う周期を指定します。

■デフォルトのモニタリング定義

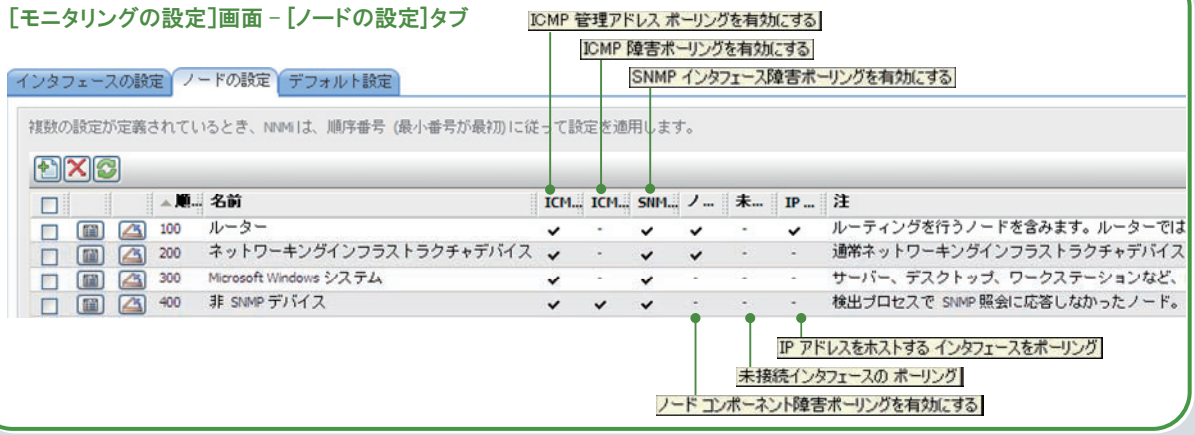
監視方法を設定するには、通常は監視対象を分類し、それぞれの特性に応じた監視方法を検討する必要があります。しかし、NNMi はここで説明するように、ネットワークを監視するための設定として、適切なモニタリング定義が標準で提供されています。

モニタリング定義とは、モニタリングするときに実行されるポーリングの種類や周期を定義したものです。このモニタリング定義によって、NNMi では導入後、すぐに適切な方法でネットワーク監視を始めることができます。

例えば、それぞれのノードに応じたモニタリングの設定をする[ノードの設定]タブには、運用を考慮し、
次のようなモニタリング定義がデフォルトで設定されています。

3

[モニタリングの設定]画面 – [ノードの設定]タブ



- **ネットワーキングインフラストラクチャデバイス**

  ネットワークの中核機器が対象となります。
  SNMP だけでなく、コンポーネント(ファン、電源など)も監視対象として設定されます。このため、コンポーネントを監視することで、問題につながる環境異常を早期に発見し対策することができます。

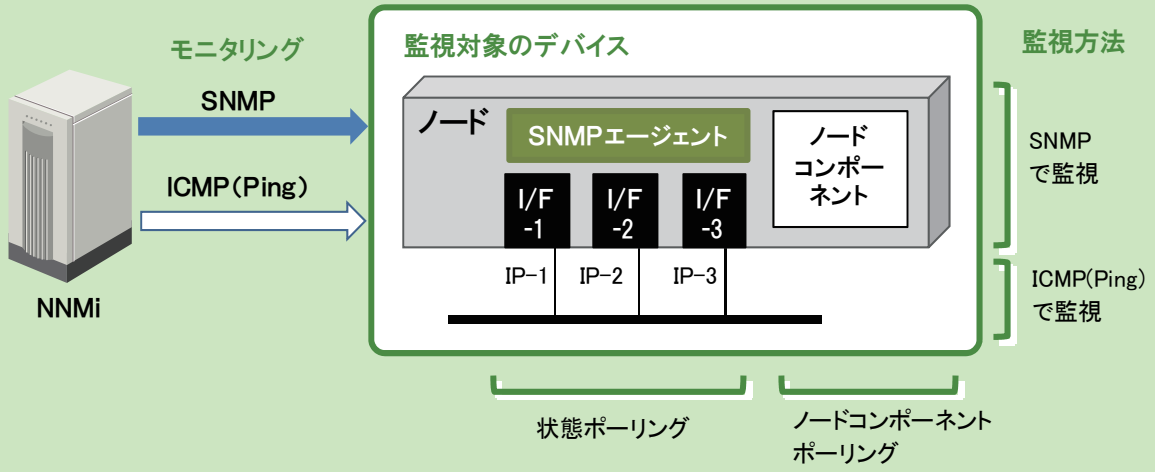
- **非SNMPデバイス**

  ネットワーク構成を検出したとき、SNMP に応答がないデバイスは、自動的に非 SNMP デバイスとして管理されます。このとき、ICMP(Ping)でモニタリングするように設定されるため、死活監視をすることができます。また、SNMP での監視も試みるよう設定されているため、SNMP への応答ができるようになったら、SNMP による管理が開始されます。

詳細は　ヘルプ　【管理者用ヘルプ】-［ネットワークの稼働状態を監視する］
マニュアル【セットアップガイド】-［5章　NNMiステータスポーリング］

3.1 モニタリングの設定

モニタリングの設定は、[モニタリングの設定]画面から設定します。
NNMi は、SNMP や ICMP によって監視対象のデバイスをモニタリングします。また、それぞれの監視対象のデバイスに応じた、複数の監視方法があります。



監視対象の SNMP エージェントや各インタフェースは SNMP によって監視をします。監視対象の各 IP アドレスは ICMP(Ping)によって監視をします。

標準のモニタリング定義を参照する

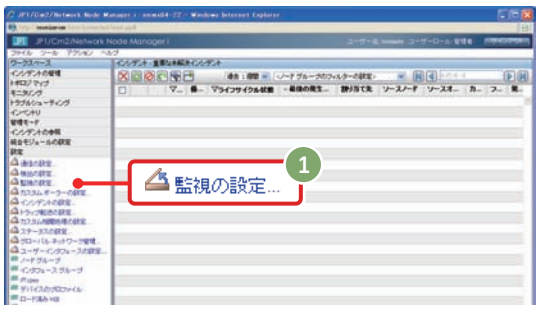
ヘルプ　【管理者用ヘルプ】-［ネットワークの稼働状態を監視する］-［モニタリング動作の設定］
マニュアル【セットアップガイド】-［5章　NNMiステータスポーリング］

NNMi では、すぐに監視を始められるように、モニタリング定義が標準で設定されています。
このため、モニタリング方法やポーリング周期をカスタマイズしなければ、特に設定を変更する必要はありません。
ただし、監視の仕組みを理解することはネットワーク監視において大変重要です。したがって、標準のモニタリング定義を参照し、監視方法を確認してみましょう。

■操作手順　～標準のモニタリング定義を参照する～

1 ワークスペースから[設定] - [監視の設定]を選択します。

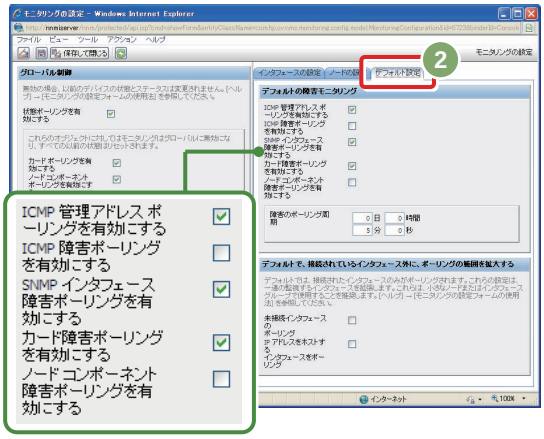
[モニタリングの設定]画面が表示されます。



2 [デフォルト設定]タブを選択し、モニタリングのデフォルトの設定を参照します。

何を監視する設定になっているか、監視間隔は何分か、確認しましょう。

各項目の意味については、3 章の解説「モニタリング」 ～ネットワークを監視する～ を参照してください。



3 ノードおよびインタフェースのモニタリングの定義を参照します。

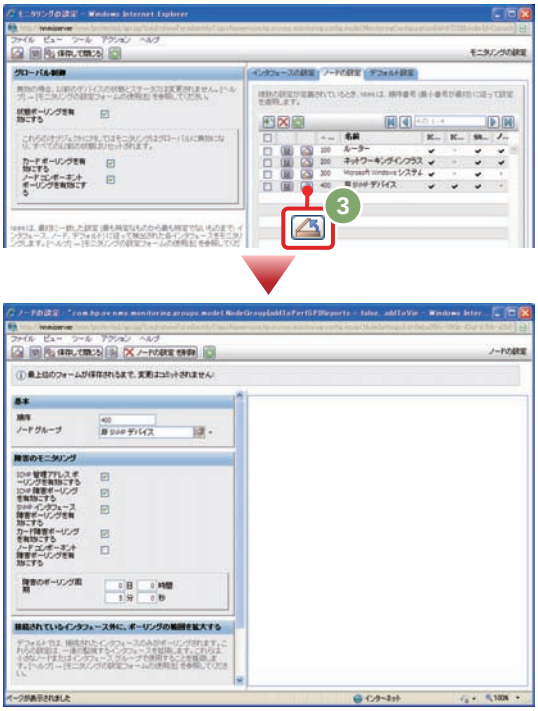
[ノードの設定]に定義されているモニタリング定義は次のとおりです。

- ルーター
- ネットワーキングインフラストラクチャデバイス
- Microsoft Windows システム
- 非 SNMP デバイス

[ノードの設定]タブを選択し、各項目の[ ]（開く）をクリックします。

それぞれのモニタリングの定義が表示されます。

ノードの種類ごとに適切なモニタリング方法が定義されています。監視対象の違いや監視間隔など、それぞれの違いを比較しながら見てみましょう。



これで標準のモニタリング定義を参照する操作は完了です。

解説

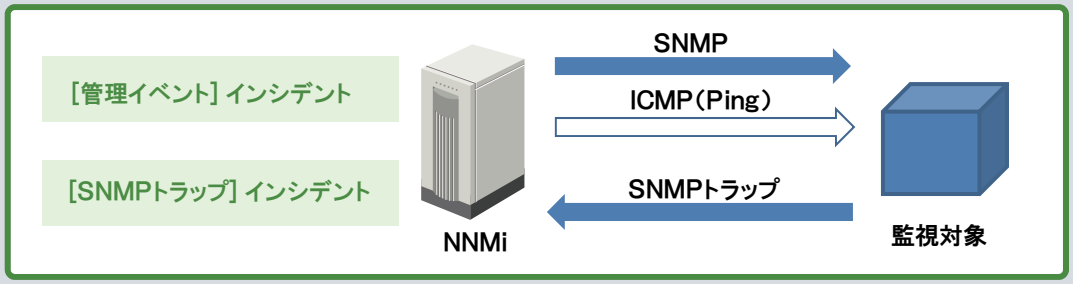
「インシデント」 ～重要な事象に絞って通知する～

NNMi は、ネットワーク構成を検出してモニタリングし、検知した問題を管理します。ここでは、NNMi のインシデント管理の仕組みについて説明します。

インシデントとは

インシデントとは、ネットワークに関連して管理者に通知する必要がある重要性の高い情報です。NNMi はネットワークを監視、発生した事象（イベント）を検知し、根本原因解析の機能によって解析することで、管理者が把握する必要がある「インシデント」に絞って通知します。

インシデントは、SNMP や ICMP（Ping）によるネットワークの監視や、SNMP トラップによる問題通知の情報をもとに根本原因解析をした結果、通知されます。



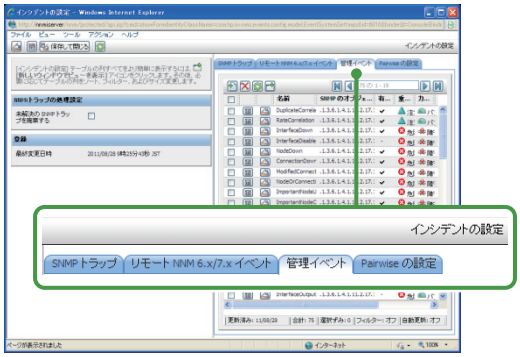
このネットワークの監視に対応したインシデント定義として標準で次の設定が提供されています。

標準のインシデント定義	説明
[管理イベント]インシデント	NNMi がネットワークを継続的に監視することで、検出した問題を解析し、根本原因をインシデントとして通知します。
[SNMP トラップ]インシデント	監視対象から、SNMP トラップによる問題発生の通知を受け取ると、インシデントとして通知します。

■インシデント定義は標準で提供されているので、すぐに活用できます

NNMi は、[管理イベント]や[SNMP トラップ]を合わせて、標準で約 140 種類インシデント定義が設定されています。これらはさまざまな事象に対応しているため、そのまま運用で使えます。
これらのインシデントのうち、ノードの種類や発生した事象に基づいて、検知した問題を適切にインシデントとして管理者へ通知します。

[インシデントの設定]画面



■ノードダウンのインシデント

例えば、ノードダウンが発生したときに発生するインシデントとして、次の内容が設定されています。
これらのうち根本原因解析の機能が状況を解析して、適切なインシデントを通知します。

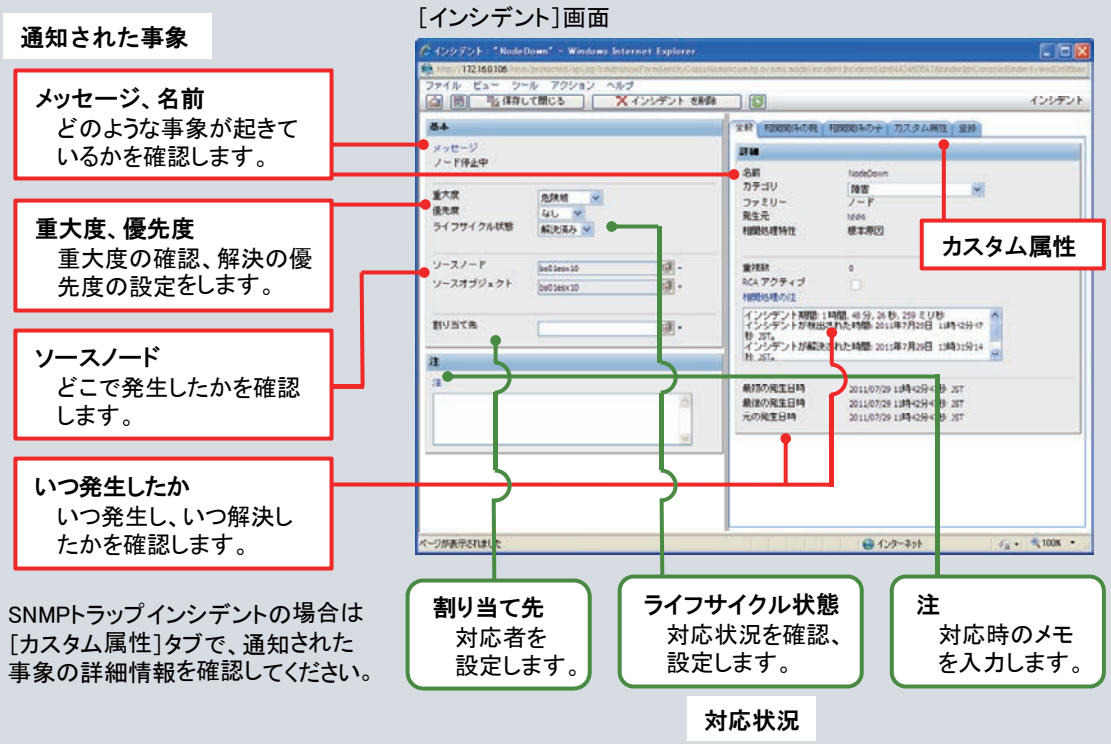
- NodeDown（ノード停止中）
- NodeOrConnectionDown（ノードまたは接続が停止中）
- NonSNMPNodeUnresponsive（非 SNMP ノードが応答なし）

■機器独自のSNMPトラップ定義

ネットワーク機器などが障害発生を SNMP トラップで通知するために、SNMP トラップの定義を拡張 MIB ファイルとして提供している場合があります。
「3.2 インシデントの設定」の設定手順を参照して、NNMi に拡張 MIB ファイルをロードして運用しましょう。

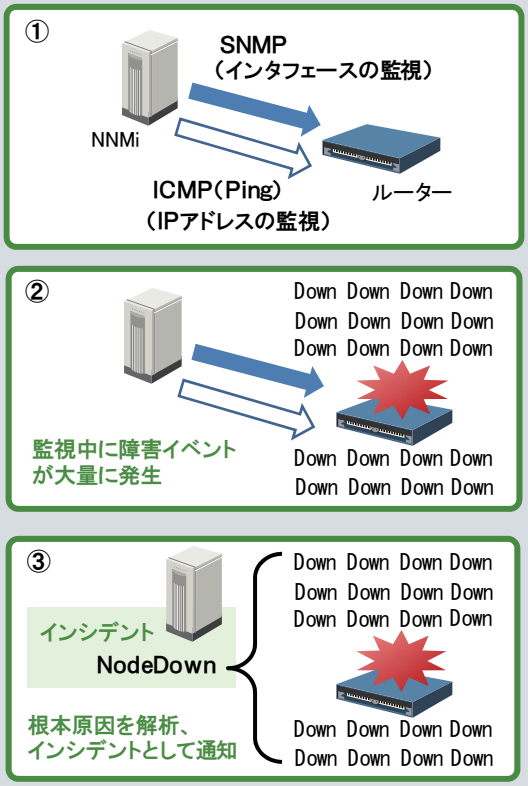
インシデントの内容

インシデントには、根本原因として通知された事象、および対応状況がわかるよう情報が記録されています。次に示す[インシデント]画面は、ネットワーク機器がノードダウンして停止したときに発生したインシデントの例です。このように、根本原因解析機能によって、根本原因の事象だけがインシデントとして通知されます。



根本原因解析

ネットワーク機器（ルーター）の監視を例にして、根本原因解析の動きを見てみましょう。



図①
ルーターを監視している場合は、インタフェースを SNMP、IP アドレスを ICMP(Ping)でポーリングして監視します。

図②
このルーターでノードダウンが発生すると、ルーターが持つ多数のインタフェースや IP アドレスが無応答となります。
このため、インタフェース障害や IP アドレスの無応答などによる障害イベントが大量に発生します。

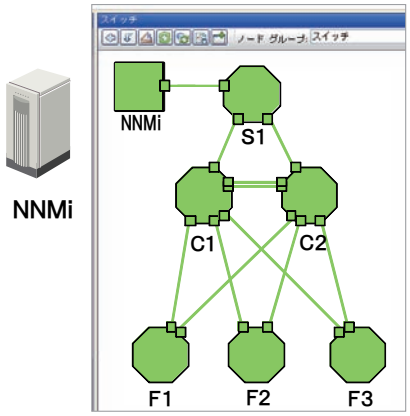
図③
この状況を NNMi の根本原因解析機能は次のように判断します。

- IP アドレスの無応答は、インタフェース障害によって発生したと判断し、インシデントを抑止する。
- 近隣ノードでの通信断の状況をもとに、ルーターにノードダウンが発生したと判断する。
- インタフェース障害はその影響と判断し、ルーターで発生したノードダウンと関連づける。

これらによって、根本原因のインシデントとしてノードダウンが通知されます。

NNMi の根本原因解析機能はネットワークを構成する複数のノードでも、レイヤー2 トポロジの情報を有効に活用することで発生している事象を解析し、根本原因のインシデントを通知します。ここでは、次のネットワーク構成を例として、根本原因解析の動きを説明します。

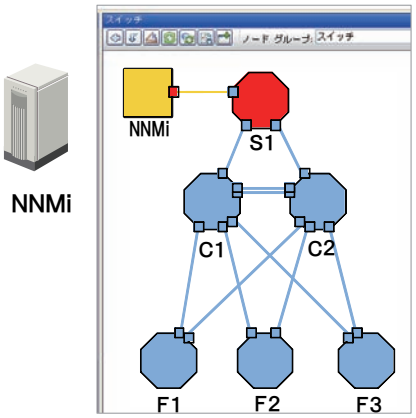
■通常時



通常時

基幹ネットワークを構成するスイッチが、図のように階層構成となっています。NNMiは最上位のスイッチ「S1」に接続されていて、監視中のネットワークはすべて正常な状態です。

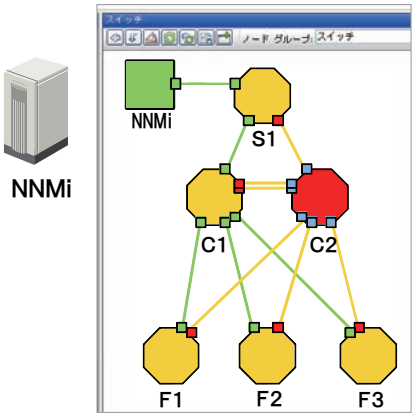
■障害発生時



最上位スイッチの障害

[想定障害　] 最上位のスイッチ「S1」がダウン
[発生イベント] ・S1と通信が不可
・S1を経由する他スイッチへの通信が不可

例えば、NNMiはこの状況を次のように判断します。
・「S1」でノード障害が発生した。
・「S1」の先も通信できないが、「S1」障害の影響と判断してインシデントを抑止し、状態不明とする。
この結果、「S1」の障害だけを根本原因のインシデントとして通知します。



中間スイッチの障害

[想定障害　] 中間のスイッチ「C2」がダウン
[発生イベント] ・C2との通信が不可
・各ノードの「C2」と接続しているインタフェースがダウン状態

例えば、NNMiはこの状況を次のように判断します。
・「C2」でノード障害が発生した。
・「C2」と接続している各インタフェースは、「C2」の障害の影響と判断してインシデントを抑止する。
この結果、「C2」の障害だけを根本原因のインシデントとして通知します。

根本原因解析機能は、ほかにも多くの事象と根本原因の対応を解析できます。

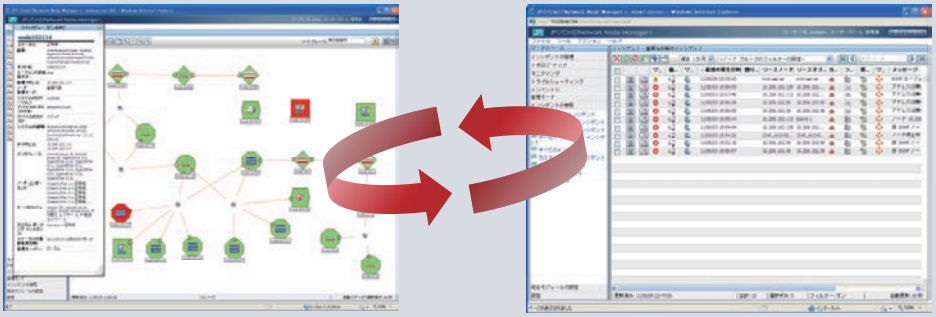
詳細は　マニュアル　【セットアップガイド】-［付録B　Causal Engine と NNMi インシデント］
ヘルプ　【オペレータ用ヘルプ】-［インシデントでの障害モニタリング］

インシデントの運用

NNMi は、監視中に発生した問題の根本原因をインシデントとして通知します。ネットワーク運用における障害の影響を最小限にするため、NNMi ではインシデントをもれなく適切に対処する次の仕組みを提供しています。

■インシデントでの障害モニタリング

インシデントが発生すると、NNMi コンソール上で通知され、表示されます。画面を切り替えながら、トポロジマップとインシデントの一覧で内容を確認し、問題に対応してください。

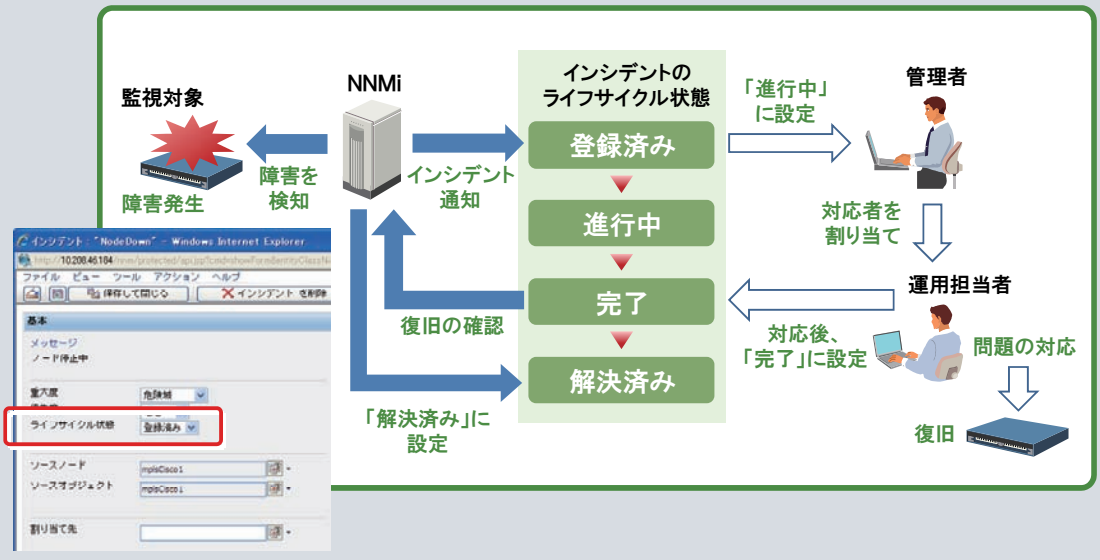


■インシデントのライフサイクル管理

NNMi は、インシデントの対応の進行状況を**ライフサイクル状態**として管理しています。ライフサイクル状態は、[インシデント]画面で確認します。

例えば、次に示す図のように、インシデントに対応する担当者の割り当て、ライフサイクル状態を変更していくことで、発生した障害に対して適切に対応するように運用できます。

なお、NNMi はインシデントが解決すると、自動的にライフサイクル状態を「解決済み」にします。例えば、ノード停止中のインシデントは、ノードが動作すると、解決済みのインシデントとして扱われます。



■インシデントの自動アクション

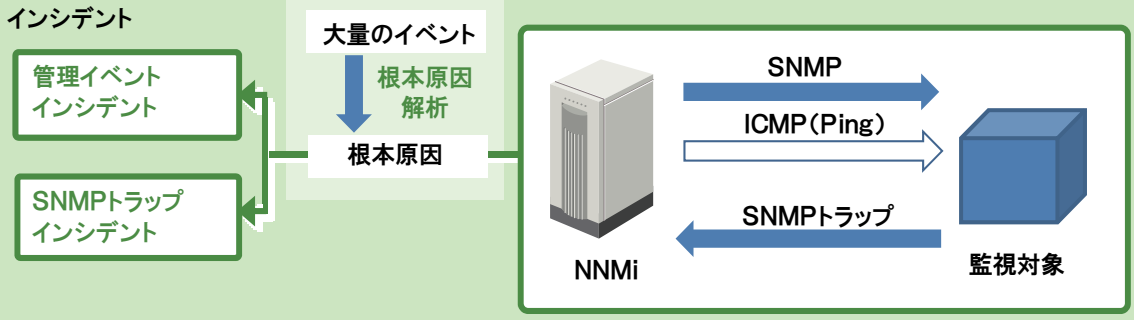
インシデントのライフサイクル状態にあわせて、自動的にアクションが実行されるように設定できます。

例えば、特定のインシデントが発生した（ライフサイクル状態が「登録済み」に設定された）ときに、発生したことをメールで通知するなどの特定のアクションが実行されます。

詳細は　ヘルプ　【管理者用ヘルプ】-［インシデントを設定する］
　　ヘルプ　【オペレータ用ヘルプ】-［インシデントでの障害モニタリング］

3.2 インシデントの設定

インシデントの設定は、[インシデントの設定]画面から設定します。
NNMi は、モニタリングで検出した問題や SNMP トラップを根本原因解決機能によって解析し、根本原因を特定すると、インシデントとして通知します。



ここでは、インシデントを設定する際の基本的な作業として、次の項目を説明します。

- 運用で使用する標準のインシデント設定（[管理イベント]や[SNMP トラップ]）の概要を参照しておく。
- ネットワーク機器などが提供する拡張 MIB ファイルをロードし、SNMP トラップのインシデントを設定する。
- 必要に応じて、インシデントに自動アクションを設定する。

標準のインシデント設定を参照する

ヘルプ　【オペレータ用ヘルプ】-［問題の調査と診断］-［根本原因インシデントの解釈］
ヘルプ　【管理者用ヘルプ】-［インシデントを設定する］
-［インシデント設定を使用してインシデントを管理する］-［NNMi が提供するインシデント設定］

インシデントの設定は、ワークスペースから[設定]-[インシデントの設定]を選択すると一覧を参照でき、[管理イベント]タブと[SNMP トラップ]タブを選択すると詳細を参照できます。標準で提供されているインシデント設定について、基本的な項目を参照してみましょう。

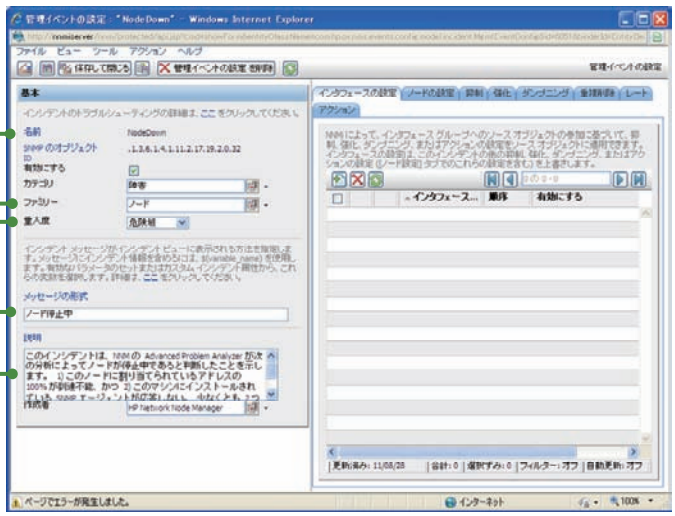
名前
インシデントの名前が表示されます。

ファミリー
どこで問題が発生しているのか、インシデントの属性が表示されます。

重大度
インシデントとして通知された問題の重大度が表示されます。

メッセージの形式
問題が発生したときのメッセージが表示されます。

説明
インシデントがどのような問題を通知するのかなど、詳細が表示されます。

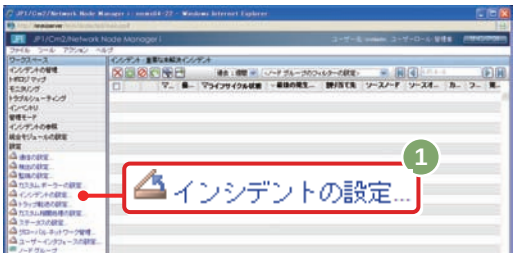


［インシデントの設定］－［管理イベントの設定］画面

■操作手順 ～標準のインシデント設定を参照する～

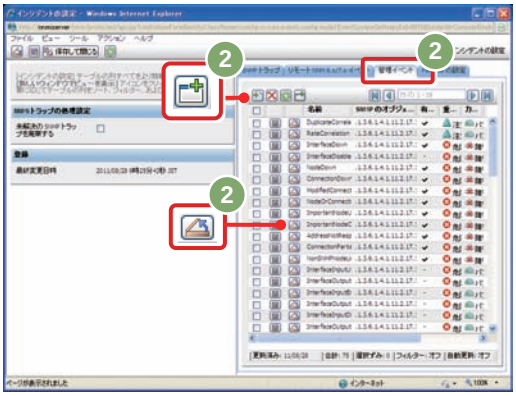
1 ワークスペースから[設定] - [インシデントの設定]を選択します。

[インシデントの設定]画面が表示されます。



2 [管理イベント]タブや[SNMPトラップ]タブを選択して、インシデントの設定を参照します。

- 「  」(新しいウィンドウでビューを表示)をクリックすると、別画面でインシデントの設定の一覧が表示されます。
- 「  」(開く)をクリックすると、設定の詳細画面が開きます。

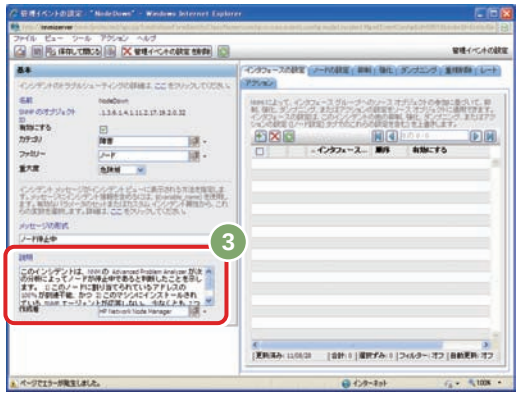


3 インシデントの設定を確認します。

ここでは例として、[管理イベント]タブの各項目の「  」(開く)をクリックして、[管理イベントの設定]画面を表示させます。ノードダウンで発生する次のインシデントを見てみましょう。

- NodeDown (ノード停止中)
- NodeOrConnectionDown (ノードまたは接続が停止中)
- NonSNMPNodeUnresponsive (非 SNMP ノードが応答なし)

インシデントの[説明]欄を確認して、理解を深めておきましょう。



これで標準のインシデント設定を参照する操作は完了です。

参考

【オペレータ用ヘルプ】 - [問題の調査と診断] - [根本原因インシデントの解釈] にはインシデントの詳しい説明が載っています。

インシデントの設定を確認するときに、合わせてヘルプを参照するとより理解を深めることができます。

ノード停止中 の説明

SNMPトラップのインシデントを設定する

ヘルプ　【管理者用ヘルプ】-［インシデントを設定する］-［SNMP トラップインシデントを設定する］

NNMi は標準で多くの SNMP トラップのインシデント定義を用意していますが、ネットワーク機器などのベンダー固有の拡張 MIB ファイルをロードして、機器独自の SNMP トラップのインシデント定義を設定することもできます。
一般的な MIB ファイルには、MIB 定義と SNMP トラップ定義が記述されています。
各ベンダーの MIB ファイルの詳細については各ベンダーのマニュアルなどを参照してください。

■操作手順　～SNMPトラップのインシデントを設定する～

NNMi での MIB ファイルのロードには nnmincidentcfg.ovpl コマンドと nnmloadmib.ovpl コマンドを使います。
NNMi データベースの同期処理を一度で済ませて処理時間を短くする手順を説明します。

1 「nnmincidentcfg.ovpl -loadTraps」を実行し、MIBファイルをロードします。

トラップ定義をロードし、同時に MIB 定義も読み込まれます。
なおトラップ定義がなく MIB 定義だけ記述された MIB ファイルをロードした場合は、「トラップ定義がない」とメッセージが表示されますが、問題ありません。

ロードする MIB ファイルが複数ある場合は、1 の手順をすべての MIB ファイルに対して行い、最後に 2 の手順を実施してください。

2 「nnmloadmib.ovpl -resynch」を実行します。

NNMi 内部の MIB ファイルとデータベースが再同期されます。

```
1
nnmincidentcfg.ovpl -loadTraps <mib_file>  -u <user> -p <password>
2
nnmloadmib.ovpl -resynch  -u <user> -p <password>
```

3 インシデントの設定を確認します。

「3.2　インシデントの設定」の操作手順「標準のインシデント設定を参照する」を参照して、ロードした SNMP トラップ定義を確認してください。

これでSNMPトラップのインシデントを設定する操作は完了です。

参考

SNMP トラップを受信するには、次の条件があります。 条件を満たさない場合、そのトラップは破棄されます。
詳しくは、【管理者用ヘルプ】-［インシデントを設定する］-［受信 SNMP トラップを管理する］ を参照してください。

＜SNMP トラップ受信の条件＞
・SNMP トラップに対応したインシデントが設定されている。かつその設定の[有効にする]がチェックされている。
・SNMP トラップを発行したソースノードが、検出されている。かつそのノードの管理モードが「管理対象」になっている。

なお、検出されていないノードが発行した SNMP トラップを受信したい場合は、【管理者用ヘルプ】-［インシデントを設定する］-［受信 SNMP トラップを管理する］の[未解決の受信トラップを処理する］ の説明を参照してください。

インシデントに自動アクションを設定する

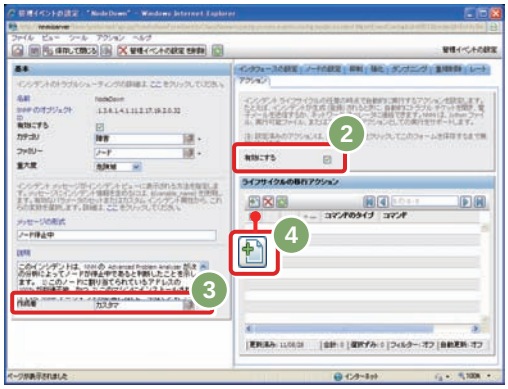
ヘルプ　【管理者用ヘルプ】-［インシデントを設定する］
　　-［インシデント設定を使用してインシデントを管理する］-［インシデントのアクションを設定する］

インシデントに自動アクションを設定すると、特定のライフサイクル状態のタイミングで、コマンドを実行できます。

■操作手順　～インシデントに自動アクションを設定する～

3.3 の操作練習（擬似障害を発生させる）で自動アクションが実行されるよう次の設定をします。
（設定例）対象インシデント　：NodeDown
　　自動アクション　　：msg コマンド

1 自動アクションを設定したいインシデント定義の設定画面を開きます。



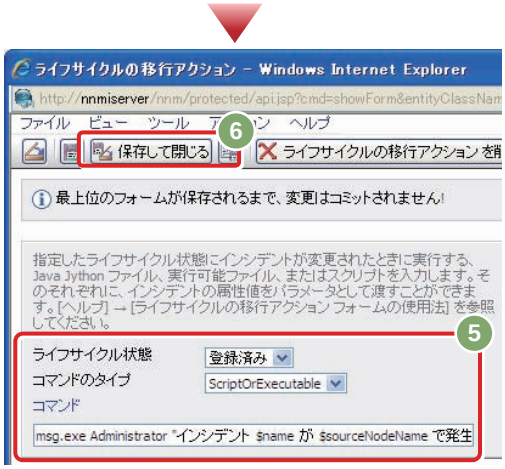
2 [アクション]タブで[有効にする]にチェックし、対象のインシデントの自動アクションを有効化します。

なお、このチェックを外すと、定義を残したままで自動アクションを一時的に抑止することができます。

3 作成者を[カスタマ]に変更します。

4 [ ]（新規作成）をクリックし、設定画面を開きます。

［ライフサイクルの移行アクション］画面が表示されます。



5 アクションの定義を入力します。

（例）ライフサイクル状態　：　登録済み
　　コマンドのタイプ　　：　ScriptOrExecutable
　　コマンド　：
「msg.exe　Administrator　"インシデント　$name が　$sourceNodeName　で発生しました。"」

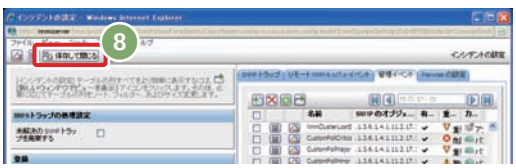
6 [保存して閉じる]をクリックします。

7 [管理イベントの設定]画面で[保存して閉じる]をクリックします。

［管理イベントの設定］画面が閉じます。

8 [インシデントの設定]画面で[保存して閉じる]をクリックします。

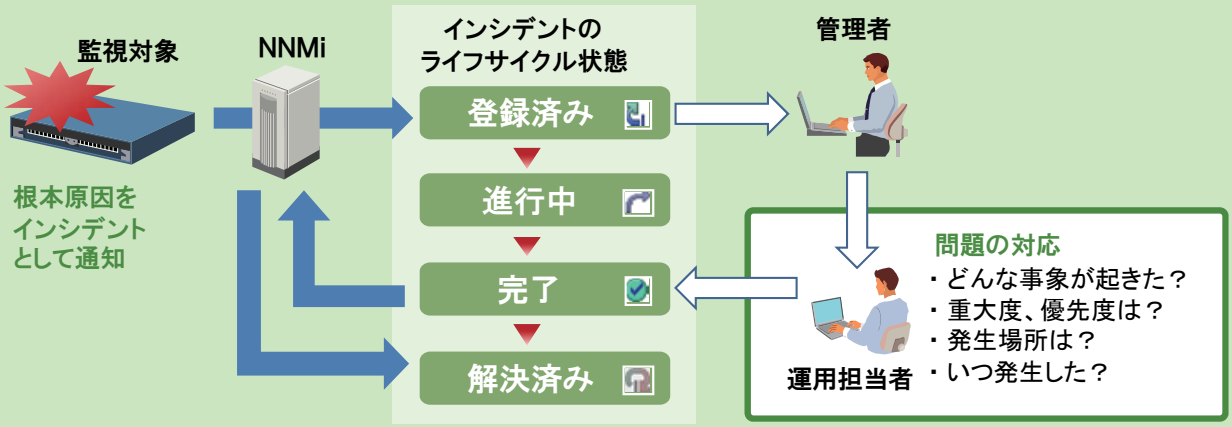
［インシデントの設定］画面が閉じて、自動アクションが設定されます。



これでインシデントに自動アクションを設定する操作は完了です。

3.3 インシデントのライフサイクル管理

インシデントはワークスペースの[インシデントの参照]から参照し、状況把握や対応を行います。各インシデントの対応の進行状況は「ライフサイクル状態」として管理しており、問題の対応漏れを防ぐことができます。



NNMi はインシデントを通知したあとも状態監視を続けており、復旧を検知した場合は自動的にインシデントを解決済みにします。例えば「ノード停止中」を通知しているノードが動作再開すると NNMi はそのインシデントを解決済みにします。

インシデントによる障害対応の管理

ヘルプ　【オペレータ用ヘルプ】-［インシデントでの障害モニタリング］

NNMi は、問題が発生すると根本原因をインシデントとして通知し、インシデントの対応の進行状況（ライフサイクル状態）を問題発生から解決まで管理しています。ここでは、問題発生から解決までの障害対応の流れを説明します。

■操作手順　～インシデントによる障害対応の管理～

ここでは、操作の練習として障害を発生させて、通知されたインシデントを確認する例を説明します。

擬似障害を発生させる

1 操作を練習するために、擬似障害を発生させます。

監視対象としているノードで障害を発生させてください。

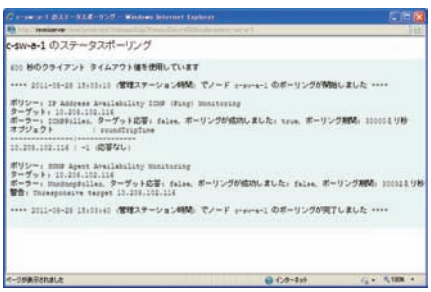
（例）・LAN ケーブルを抜く

・ノードを停止させる

業務に影響が出ないように注意してください。

2 障害を検知するまでお待ちください。

- NNMi が周期的に監視（状態ポーリング）を行い、障害発生を検知します。デフォルトの監視間隔は 5 分（Windows のノードは 10 分）です。
- すぐに検知させたい場合は、マップ画面でノードを選択して［アクション］－［ステータスポーリング］を選択してください。すぐに状態ポーリングを行います。



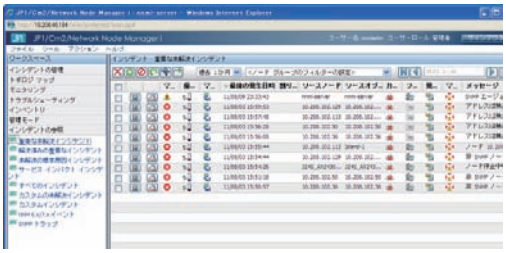
インシデントの発生状況を確認します

通常のネットワーク監視の運用では、インシデント画面またはマップ画面を開いて、監視運用を行います。
インシデントが発生した場合、それぞれ次のような操作を行ってインシデント発生の状況を確認します。

3 インシデントの発生を確認します。 ＜インシデント画面からの確認＞

ワークスペースの[インシデントの参照]をクリックします。

[重要な未解決インシデント]をクリックして、未解決のインシデントを確認します。
または、[すべてのインシデント]をクリックして、すべてのインシデントを時系列で参照します。



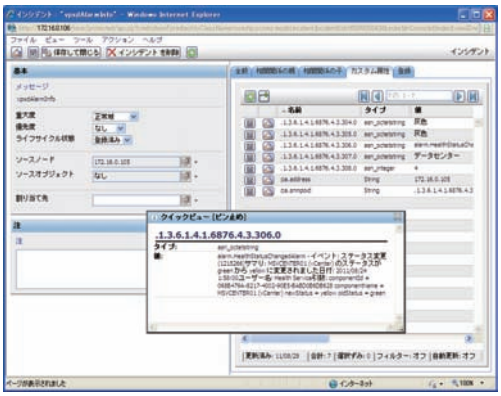
管理インシデントの場合

[インシデント]画面を開き、詳細情報を確認します。
一覧表示されている各インシデントの（開く）をクリックして、[インシデント]画面を開きます。

例えば、次の項目を確認します。

- メッセージと名前で発生したインシデントの種類を、ソースノードで発生個所を、日時で時刻を確認します。
- インシデントの意味の説明は、[アクション] － [インシデントの設定を開く]をクリックして設定画面を開くと、「説明」の欄で確認できます。
  また、[オペレータ用ヘルプ] － [問題の調査と診断] － [根本原因インシデントの解釈]も、インシデントの内容を調査するための有効な情報です。なおこのヘルプは、インシデントのメッセージを項目として記載されています（例えば NodeDown ではなく”ノード停止中”）。
- SNMP トラップインシデントの場合は、[カスタム属性]タブで詳細情報を確認します。
  カスタム属性には、SNMP トラップにより通知された情報が記録されていますので、SNMP トラップを発行した機器のマニュアル等を参照して、内容を確認します。

SNMPトラップインシデントの場合



4 インシデントの発生を確認します。 ＜マップ画面からの確認＞

ワークスペースの[トポロジマップ]をクリックします。

[ネットワークの概要]や任意に作成したノードグループマップなどを参照します。

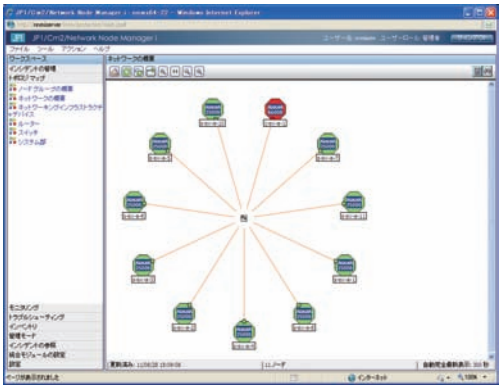
色が「正常域」以外に変化しているアイコンを確認します。

アイコンの色と意味			
緑色	正常域	赤色	危険域
水色	注意域	青色	認識不能
黄色	警戒域	グレー	無効
オレンジ	重要警戒域	ベージュ	ステータスなし

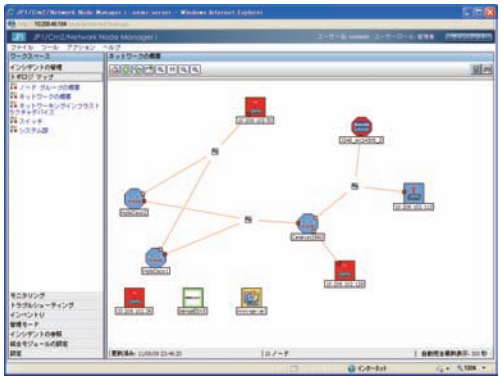
(例 2)の画面のように、あるノードの障害(赤色で表示)が近隣ノードに影響して認識不能(青色)になっている場合があります。

このように NNMi のマップ画面により、障害の原因(赤色)と影響範囲(青色)を、ビジュアルに素早く把握することができます。

(例1)マップ画面



(例 2)マップ画面

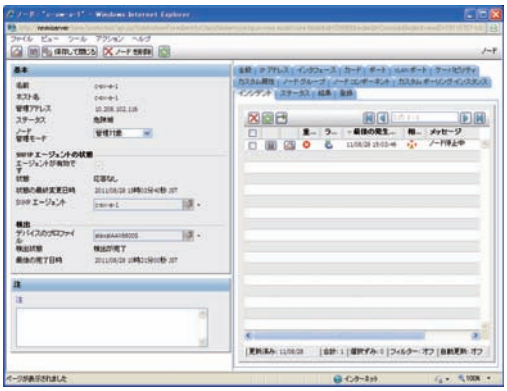


[ノード]画面を開き、詳細情報を確認します。
色が変化しているアイコンをダブルクリックして、[ノード]画面を開きます。

例えば、次の項目を確認します。

- [基本]欄で、状態と発生日時を確認します。
- [インシデント]タブで、インシデント発生状況を確認します。
- [結果]タブで、ノードステータスの遷移を確認します。

それぞれの項目で  (開く)をクリックし、詳細情報を確認します。



インシデントの対応　～「割り当て」と「ライフサイクル状態」の管理～

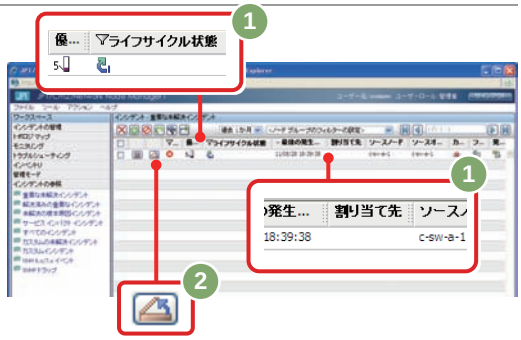
インシデントを複数名のチームで対応する場合、「割り当て先」にアカウントを設定して、作業分担の管理ができます。
また「ライフサイクル状態」により対応の進捗状況を管理できます。

1 インシデントの状態を確認します。

ワークスペースの[インシデントの参照]をクリックして[重要な未解決インシデント]を開きます。

発生したばかりのインシデントは次の状態になっています。

- ライフサイクル状態　：　（登録済み）
- 割り当て先　　：　空欄



2 インシデントの（開く）をクリックします。

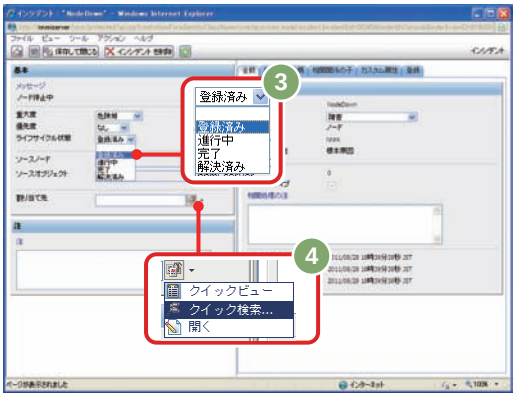
[インシデント]画面が表示されます。

3 インシデントに[ライフサイクル状態]を設定します。

[ライフサイクル状態]のプルダウンメニューから状態を選択します。

例えば、次のように[進行中]と[完了]を使って運用します。

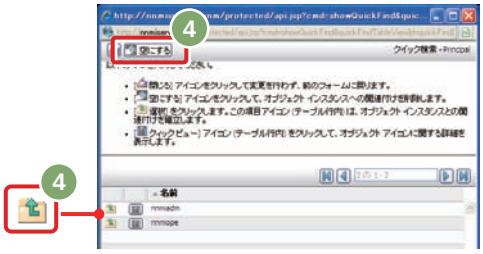
- インシデントの登録直後は[登録済み]になっています。
- 問題調査や対応を始めるときに[進行中]に、
  その後、調査や対策が完了したときに[完了]にします。
- [解決済み]は、NNMi が問題ないことを識別したときに NNMi が自動的に設定します。



4 インシデントに[割り当て先]を設定します。

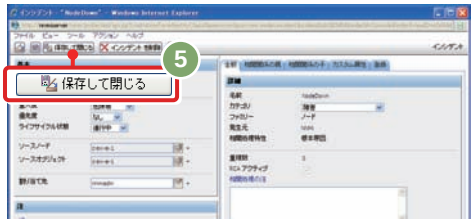
[割り当て先]の をクリックして、クイック検索画面を表示します。

- 割り当てするアカウントの をクリックします。
- 空にする をクリックすると、割り当て先が空欄に戻ります。



5 [保存して閉じる]をクリックします。

設定が保存され、[インシデント]画面が閉じます。

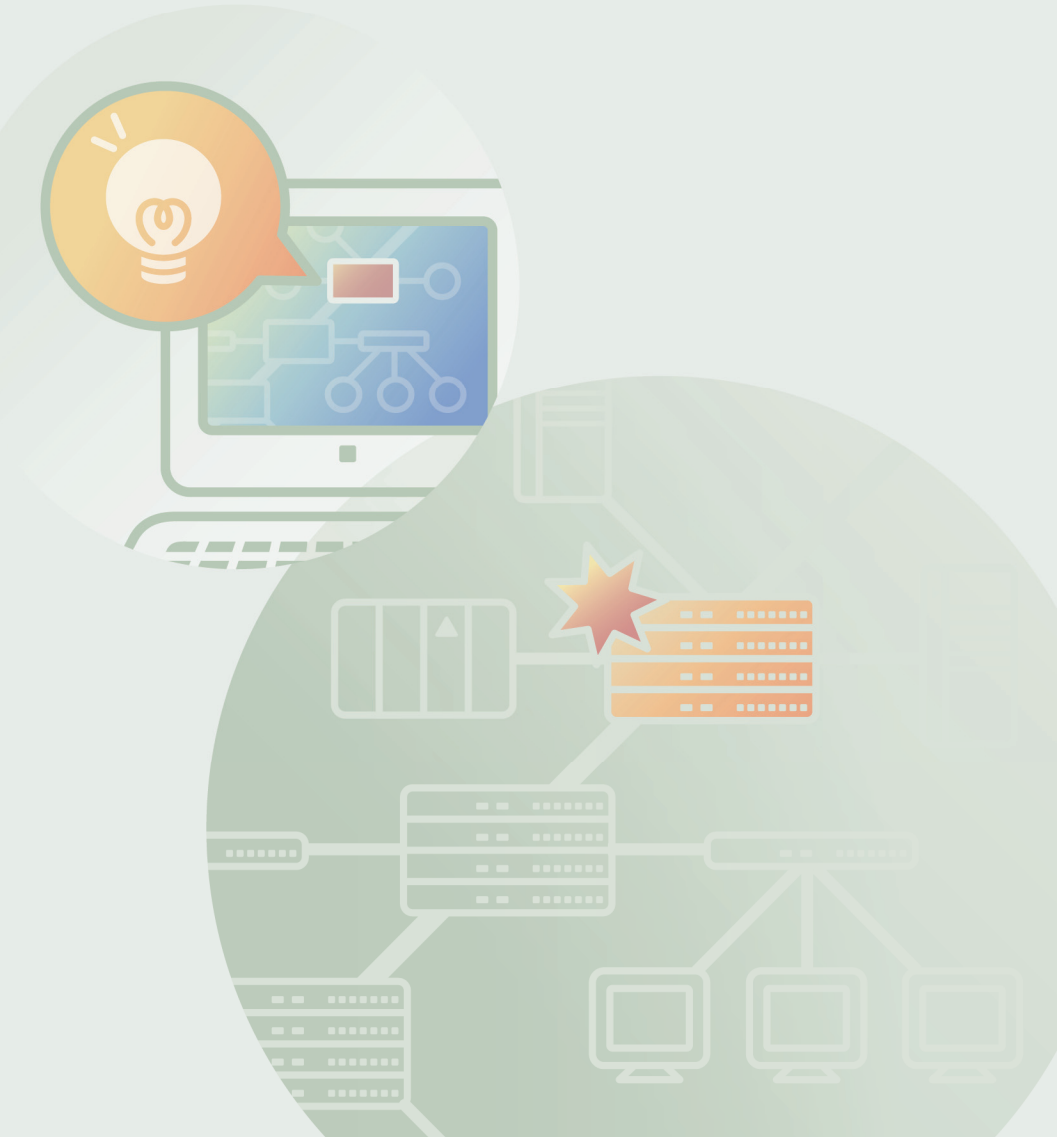


6 変更したインシデントの状態を確認します。

[インシデントの一覧]画面で、ライフサイクル状態および割り当て先が変更されていることを確認します。

4章

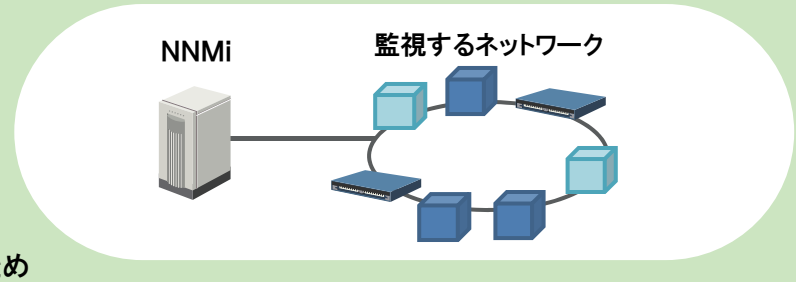
ネットワーク管理を始めよう



4.1 日頃の運用　～ネットワークの監視～

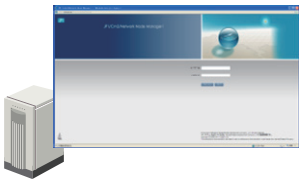
ここまでの設定により、NNMi の基本的な設定ができました。

■ NNMiによるネットワーク管理



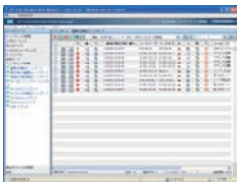
ここまでのまとめ

- NNMiが稼動開始！ ネットワークを定期監視



- ネットワーク構成を ビジュアルに把握

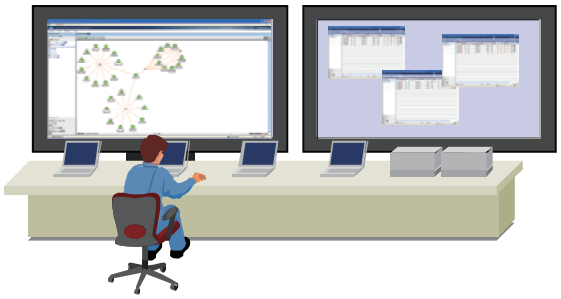
- 障害が発生しても インシデント管理で 効率よく対応



NNMi は、ネットワークの定期的な監視を始めています。
ネットワークの構成を検出し、ビジュアルなマップ画面として表示します。また、監視中に問題を検知した場合は、根本原因を解析してインシデントとして通知します。

NNMiでネットワーク管理を始めよう

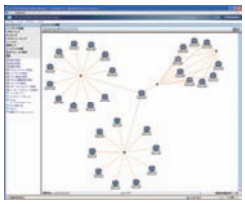
NNMi のネットワーク管理の運用方法はいくつかありますが、ここでは、マップ画面をベースに運用する方法を紹介します。例えば、運用管理センターなどでは、最も重要なマップを大型ディスプレイに常時表示して監視することがよく行われます。



トポロジマップ画面をベースに全体を監視する

[ネットワークの概要]を監視することで、ネットワーク全体の状況をビジュアルに把握できます。

P.30　検出したネットワークを参照する



ノードグループマップを定義すれば、監視したい視点で監視することができます。階層化したマップを定義することもできます。

P.40　ノードグループを設定する

画面を見て監視し続けるのは大変です。
自動アクションを設定することでメール送信やパトランプで問題発生を通知できます。

P.59　インシデントに自動アクションを設定する

ネットワーク障害に対応する

NNMi は定期的に状態ポーリングを行い、継続的にネットワークを監視しています。
もしネットワーク上で障害が発生しても、次のような運用シナリオで問題を特定して迅速に対応できます。

1 マップ画面でネットワーク状態を監視します。

監視用として常時表示する場合は、URL 指定で開いてください。

URL 指定で画面を開く方法は、このページの[参考]を参照してください。

[マップ]画面

2 障害個所をビジュアルに確認します。

障害を検知すると、マップ上のアイコンの色が変化して通知します。

マップの全体状況を確認します。マップを階層化している場合は、子ノードグループを開いて状況を確認します。

- ノードグループの状態は、最もクリティカルな状態が反映されます。
- 子ノードグループの状態は、親ノードグループにも反映されます。

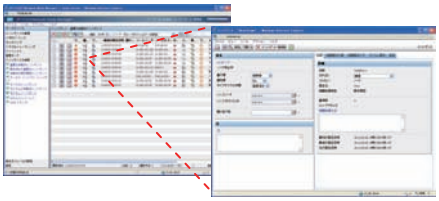
3 根本原因をインシデントで確認します。

[インシデントの参照]ワークスペースを開いて、根本原因として通知されたインシデントを確認します。

- [重要な未解決インシデント]や[すべてのインシデント]を開き、インシデントの内容を参照して、問題個所を確認します。まず、ソースノードやソースオブジェクト、カスタム属性から確認しましょう。

P.61 インシデントの発生状況を確認します

[インシデント]画面

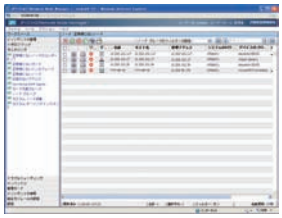


4 関連部分の状況を確認します。

ネットワークの障害は、通信経路の関連部分にも影響することが少なくありません。根本原因だけではなく、関連個所も確認します。

- マップ画面で、関連部分を確認して状況を把握します。
- [モニタリング]ワークスペースで、問題個所がないか把握します。

[モニタリング]画面



5 担当者を割り当てて対応します。

問題状況が把握できたら、インシデントの担当を割り当てて対策を進めます。

P.62 インシデントの対応～「割り当て」と「ライフサイクル状態」の管理～

参考

通常の画面は一定時間操作しないとタイムアウトします。デフォルトは 18 時間です。
URL を指定して開いたマップ画面はタイムアウトしません。監視用としてトポロジマップを常時表示する場合は、URL を指定して開きます。

・ネットワークの概要　http://ホスト名:ポート番号/nnm/launch?cmd=showNetworkOverview
・ノードグループマップ　http://ホスト名:ポート番号/nnm/launch?cmd=showNodeGroup&name=ノードグループ名※

※URL にマルチバイト文字を含める場合は URL エンコードする必要があります。
ノードグループの名前を、文字コード UTF-8 で URL エンコードして記述してください。
（例） 重要なノード → %e9%87%8d%e8%a6%81%e3%81%aa%e3%83%8e%e3%83%bc%e3%83%89

4.2 NNMiの運用

NNMi でネットワーク管理を継続的に行うためには、日頃の NNMi のメンテナンス作業が大切です。
ここでは、NNMi 自身の運用作業について説明します。

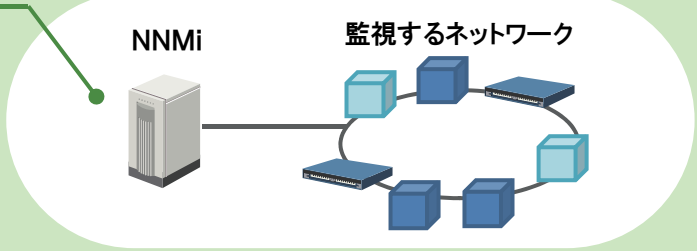
■ NNMiの保守

◇ NNMiの稼動状況の確認

◇ 設定のエクスポート
◇ バックアップ

◇ インシデントのアーカイブ

■ NNMiによるネットワーク管理



ヘルプ　【管理者用ヘルプ】- [NNMi の保守]
マニュアル　【セットアップガイド】- [14.NNMi のバックアップおよびリストアツール]
マニュアル　【セットアップガイド】- [15.NNMi の保守]

NNMiの稼動状態を確認する

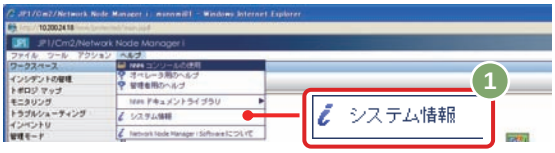
ヘルプ　【管理者用ヘルプ】- [NNMi の保守]- [NNMi の稼動状態チェック]

NNMi でネットワーク管理をするためには、まず NNMi が正常でなければなりません。NNMi の稼動状態を表示し、正常に稼動していることを確認しましょう。

1 NNMi全体の状態を確認します。

[ヘルプ] - [システム情報]をクリックします。

[システム情報]画面が表示されます。



2 [製品]タブの「ステータス」を確認します。

「ステータス」には NNMi の総合的な状態が表示されます。

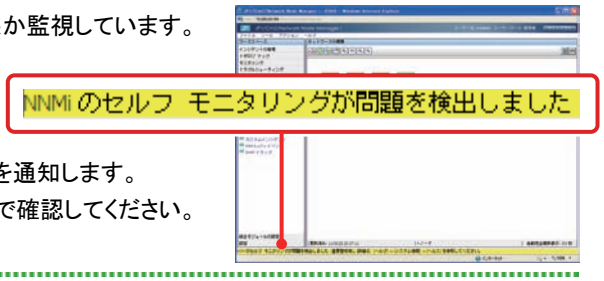
ステータスが「正常域」になっていることを確認します。

ほかに[ヘルス]タブで NNMi の詳細な状態、[StatePoller]タブで稼動状態、[データベース]タブで検出したオブジェクトの数などが確認できます。詳しくはヘルプを参照してください。

参考

NNMi は、セルフモニタリングの機能により、NNMi が正しい状態か監視しています。

もし NNMi 自体の問題を検出した場合は、
コンソールの下部に黄色で警告を表示して問題発生を知らせ、
NnmHealthOverallStatus（NNM 全体のステータス）インシデントを通知します。
このインシデントの詳細は[インシデント]画面の「カスタム属性」で確認してください。



NNMi設定のエクスポートとインポート

ヘルプ　【管理者用ヘルプ】- [NNMi の保守] - [構成設定のエクスポートとインポート]

システムの設定について重要なポイントごとに保管したり変更管理することは、運用の重要な作業です。
NNMi では nnmconfigexport.ovpl コマンドと nnmconfigimport.ovpl コマンドで、設定のエクスポートやインポートができます。
これによって現在の設定のスナップショットを取得する、設定ミスがあった場合にインポートで戻すなどを柔軟に行えます。

すべての設定をエクスポートする	nnmcomfigexport.ovpl -c all -f c:¥nnmiconf
すべての設定をインポートする	nnmconfigimport.ovpl -c all -f c:¥nnmiconf
ノードグループの設定をインポートする	nnmconfigimport.ovpl -c nodegroup -f c:¥nnmiconf

NNMiのバックアップと復元

ヘルプ　【管理者用ヘルプ】- [NNMi の保守] - [NNMi のバックアップと復元]

システム障害や操作ミスによるデータ損失などの不測の事態に備えて定期的にバックアップすることは、運用の重要な作業です。NNMi は nnmbackup.ovpl コマンドと nnmrestore.ovpl コマンドで、バックアップやリストアを行います。
ネットワーク監視を続けたままオンラインバックアップができるため、計画的にバックアップを行いましょう。

NNMi 全体をオンラインバックアップする	nnmbackup.ovpl -type online -scope all -force -target c:¥nnmi -target で指定したフォルダに nnm-bak-20110922000024 のような日時入りのフォルダが作成されます。
バックアップをリストアする	nnmrestore.ovpl -force -source c:¥nnmi¥nnm-bak-20110922000024

インシデントのアーカイブと削除

ヘルプ　【管理者用ヘルプ】- [NNMi の保守] - [インシデントのアーカイブと削除]

NNMi は、SNMP トラップインシデントの情報を 10 万件までデータベースに記録できます。データ件数が増加すると性能に影響を与え、データ件数が上限の 10 万件に達するとインシデントの保存を停止します。
このため nnmtrimincidents.ovpl コマンドを使って定期的にインシデントをアーカイブしてください。

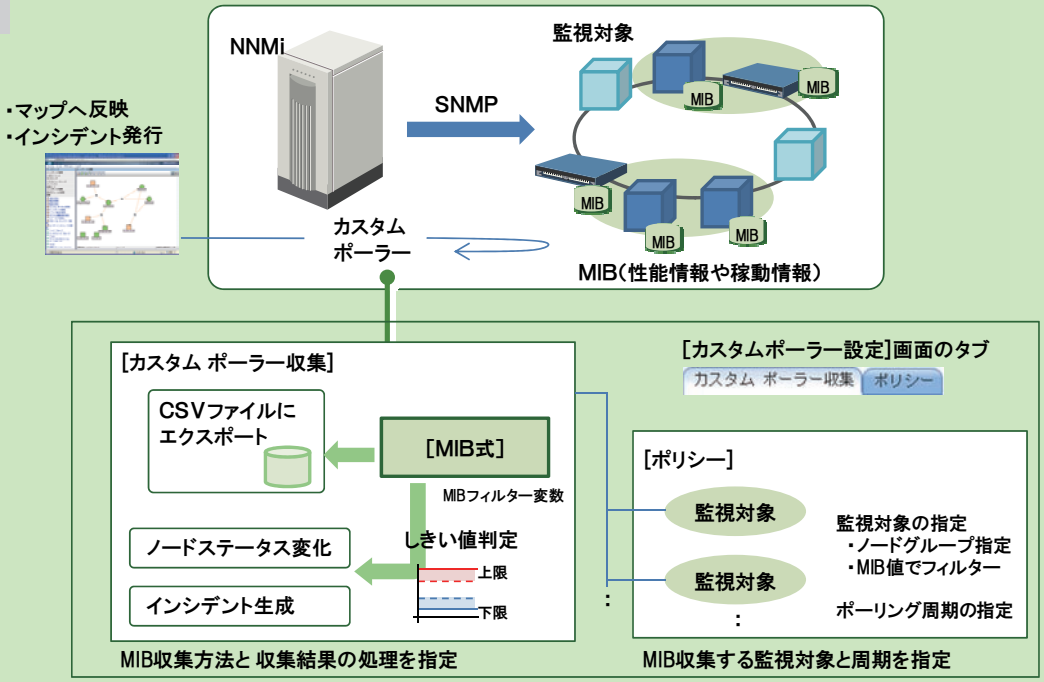
インシデント件数を確認する	NNMi のコンソール[ヘルプ] – [システム情報] – [データベース]タブのインシデントの項目に件数が表示されます。
6 日前より古く、ライフサイクル状態が解決済みのインシデントを、アーカイブに保存して削除する	nnmtrimincidents.opvl -age 6 -incr days -lifecycle Closed （例えば、新しいインシデント 1 週間分は残して処理したい場合）

参考
SNMP トラップインシデントの件数が上限の 10 万件に近づくと、次のインシデントが通知されます。
上限の 90%：SNMPTrapLimitWarning、上限の 95%：SNMPTrapLimitMajor、上限：SNMPTrapLimitCritical

付録 カスタムポーラーによる監視

上級者向け

カスタムポーラー機能によって、SNMP をサポートする監視対象から MIB 情報を収集し、性能情報や稼働情報を監視することができます。



カスタムポーラーは、[収集ルール]と[ポリシー]によって、詳細なカスタマイズや柔軟な性能監視ができます。
ここでは基本的な使い方を、通信トラフィックと通信エラーの監視を例として説明します。
(MIB 概要の知識があることを前提に説明します。MIB についてはネットワークの参考資料を参照してください)。

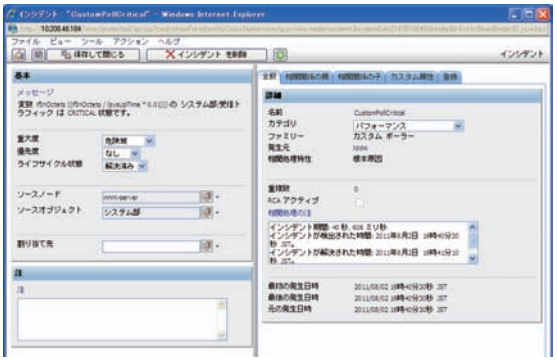
カスタムポーラーによる性能監視

ヘルプ 【管理者用ヘルプ】-[NNMi の機能を拡張する]-[カスタム ポーリングの設定]

多くのネットワークデバイスでは SNMP がサポートされ、監視に役立つ MIB が提供されています。
NNMi のカスタムポーラーを活用することで、この MIB 情報を監視対象ノードから周期的に収集し、性能監視や状態監視を行うことができます。例えば、通信トラフィック増加や通信エラーの発生、CPU 利用率などを監視し、しきい値を超えた場合にインシデントを発行して管理者に通知するなどの運用ができます。

■カスタムポーラーのメリット

・収集する MIB を柔軟に設定できます。
・しきい値を柔軟に設定できます(上限、下限、および任意の詳細定義)。
・MIB 式(MIB を組み合わせた計算式)によって、MIB 情報を
より運用に役立つ情報として提供できます。
・次の三つを組み合わせて運用に活用できます。
　・ノード状態に反映する。(例:高トラフィック時に警戒域にする)
　・インシデントを発行する。その延長で自動アクションも可能。
　・収集した MIB 情報を、CSV ファイルに出力できる。



カスタムポーラーが発行したインシデントの例
(通信トラフィックが指定したしきい値を超過)

MIBとMIB式

ヘルプ【管理者用ヘルプ】- [NNMi の機能を拡張する]- [使用可能な MIB と MIB 変数を検証する]
ヘルプ【管理者用ヘルプ】- [NNMi の機能を拡張する]- [MIB 式を設定する]

NNMi のカスタムポーラーは、SNMP デバイスがサポートする任意の MIB 情報を収集し、柔軟に性能情報や稼働情報の監視を行うことができます。この MIB について、見てみましょう。

■MIB

通信トラフィックや通信エラーの監視には、次のようなインタフェース関連の MIB 情報を参照します。
例えば、ifInOctets は一つのインタフェースが受信したバイト総数で、通信トラフィックを監視できます。
ifInErrors は一つのインタフェースが受信したエラーパケット総数で、エラー発生を監視できます。

名称	OID	型	説明
ifInOctets	.1.3.6.1.2.1.2.2.1.10	Counter32	そのインタフェースの受信オクテット総数
ifHCInOctets	.1.3.6.1.2.1.31.1.1.1.6	Counter64	そのインタフェースの受信オクテット総数 *1
ifInErrors	.1.3.6.1.2.1.2.2.1.14	Counter32	エラーがあったインバウンドパケット総数
ifOutOctets	.1.3.6.1.2.1.2.2.1.16	Counter32	そのインタフェースの送信オクテット総数
ifHCOutOctets	.1.3.6.1.2.1.31.1.1.1.10	Counter64	そのインタフェースの送信オクテット総数 *1
ifOutErrors	.1.3.6.1.2.1.2.2.1.20	Counter32	エラーがあったアウトバウンドパケット総数

*1：ifInOctets などの 32 ビットカウンタ（Counter32 型）の場合、値がラップする最短時間は 100Mbps では 5.7 分、1Gbps では 34 秒であるため、高速なインタフェースでもカウンタの値がラップしないよう ifHCInOctets など 64 ビットカウンタ（Counter64 型）の MIB が定義されています。

参考
スイッチなどは、一つのノードに複数のインタフェースがあります。このような場合は MIB 情報も各インタフェースに対応した複数の値（インスタンスと呼びます）があります。
MIB の各インスタンスは連番が振られており、OID の末尾にインターフェース番号（.1 .2 …）を付けた OID（例：ifInOctets.1 (.1.3.1.2.1.2.2.1.10.1)）により MIB 値を取得します。


スイッチ：複数のインタフェースを持つ

注意
カスタムポーラーで使用するMIBの定義は、あらかじめ NNMi にロードしておく必要があります。

■MIB式（MIB expression）

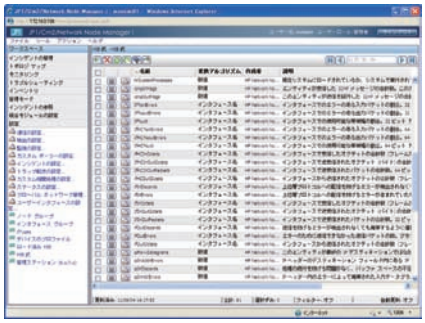
MIB 式は、MIB 情報を組み合わせた計算式です。収集した MIB は MIB 式によって、監視運用に使いやすいように加工されます。例えば、ifInOctets をそのまま参照する場合と、MIB 式を活用する場合を比較して説明します。

MIB 情報	ifInOctets	ノードを起動してから受信したバイト総数。　　値の例：4,011,828,891[バイト]
MIB 式	ifInOctets	MIB 式の定義：（ifInOctets / sysUpTime *0.01）　　値の例：10,024.8[バイト/秒] MIB 変数の ifInOctets は型がカウンタ（累計値）であるため自動的に「最新の値－直前の値」を求め、これを時間で割り算をして通信速度を求める。これらは NNMi が MIB 式の処理として自動的に行う。

MIB の ifInOctets の値そのままでは通信速度はわからないため、2 回測定して、値の差分を求めて時間で割る必要があります。
MIB 式の ifInOctets を使えば通信速度に加工した値が表示されるため、そのまま監視運用に使えます。

このように MIB 式を使って、収集した MIB 情報を性能監視・状態監視に有効に活用できます。

MIB 式は、標準で 30 以上のよく使われる設定が定義済みであるため、NNMi を導入してすぐに使えます。また、任意の MIB 式を定義することもできます。


ワースペースの[設定] - [MIB 式]画面

MIB の説明で示した ifInOctets などは、同じ名前の MIB 式として標準提供されており、すぐに使用できます。

■操作手順　～MIBを参照する・MIBに慣れる～

カスタムポーラーの定義では MIB を操作して設定をします。ここではまず準備として NNMi の操作で MIB を参照しながら MIB の扱いに慣れておきましょう。
ifInOctets（oid= .1.3.6.1.2.1.2.2.1.10　：インタフェースの受信した総バイト数）の参照を例に説明します。

MIBを参照する

1 MIBを参照するノードを選択します。

[トポロジマップ]ワークスペースの[ネットワークの概要]をクリックし、マップ画面を開きます。

MIB を参照したいノードのアイコンをクリックして選択状態にします。

2 MIBブラウザを開き、選択したノードのMIBを参照します。[アクション] - [MIBを参照]を選択します。

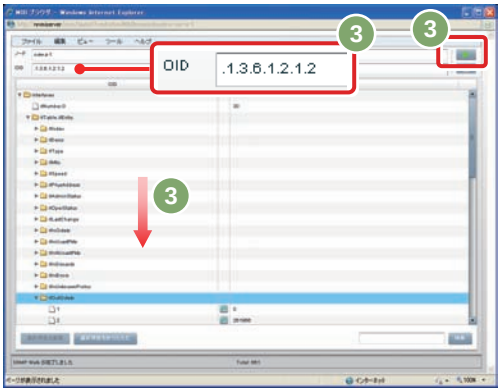
MIB ブラウザ画面が表示されます。

3 [OID]欄に参照したいMIBのOIDなどを入力し、[▶]をクリックします。

（例） OID ：　.1.3.6.1.2.1.2.2.1.10　…OID で指定

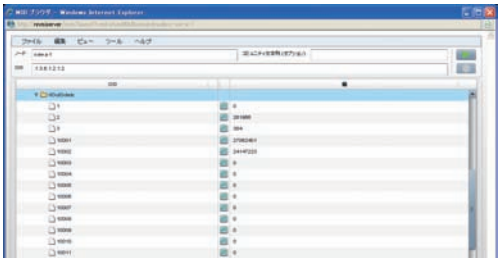
ifInOctets　…名前で指定

図のように MIB ツリーの上位の値（例：.1.3.6.1.2.1.2）を入力し、順にドリルダウンして参照することもできます。



4 表示されたMIB情報を参照します。

複数のインタフェースがあるノードの場合は、MIB の値も複数表示されます。



参考

関連する MIB も参照してみましょう。

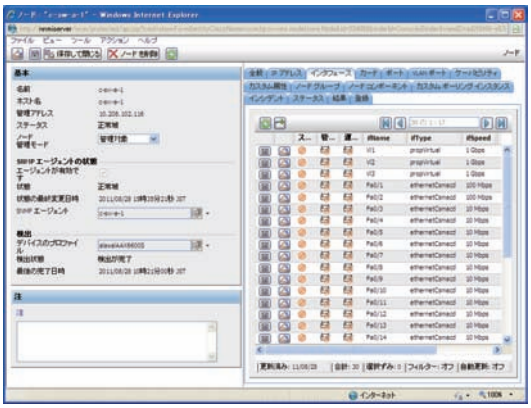
・ifIndex（.1.3.6.1.2.1.2.2.1.1）　インタフェース識別子　（一意に指定できるが、機器によっては再起動で割り当てが変わる）
・ifType（.1.3.6.1.2.1.2.2.1.3）　インタフェース種別　（vlan や EthrernetCsmacd など種別でフィルタリングする）
・ifConnectorPresent（.1.3.6.1.2.1.31.1.1.1.17）物理回線との接続状態　1:true 2:false　（論理インタフェースを省いて表示）

（ ）内の説明は、P.74 で説明するカスタムポーラーで[MIB フィルター変数]に指定するときの参考情報です。

5 MIB情報とインベントリ情報を見比べます。

MIB ブラウザで表示された MIB 情報が、NNMi のインベントリ情報とどのように対応しているか、画面を見比べてみましょう。

1 で開いたマップ画面で、MIB を参照しているノードをダブルクリックし、[ノード]画面を開きます。例えば[インタフェース]タブを参照すると、ifName や ifType という項目がありますが、これは ifName (.1.3.6.1.2.1.31.1.1.1.1)や ifType(.1.3.6.1.2.1.2.2.1.3)を MIB ブラウザで参照した値と対応していることが確認できます。

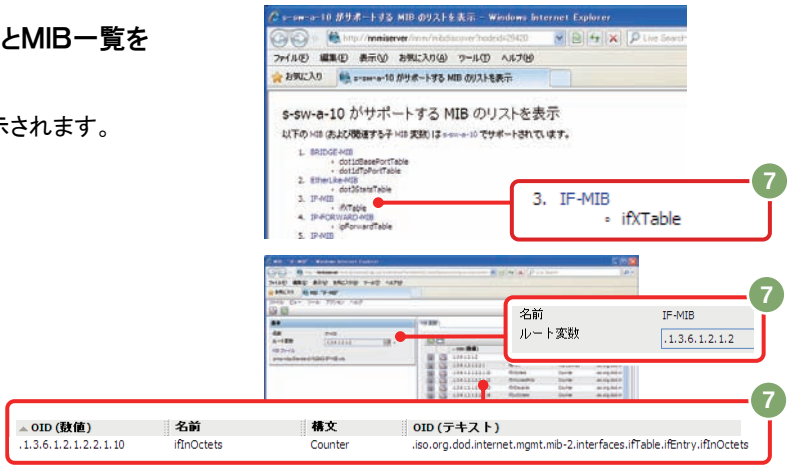


6 デバイスがサポートするMIBを参照します。[アクション] - [サポート対象 MIBリストを表示]を選択します。

ここまでは一つ一つの MIB を参照してきましたが、全体を把握する意味で、各デバイスのサポート MIB 一覧を参照してみましょう。1 で開いたマップ画面でノードを選択して、[アクション] – [サポート対象 MIB リストを表示]を選択すると、選択したノードがサポートする MIB のリストの画面が表示されます。

7 MIBのリストをクリックして、MIBリストとMIB一覧を参照します。

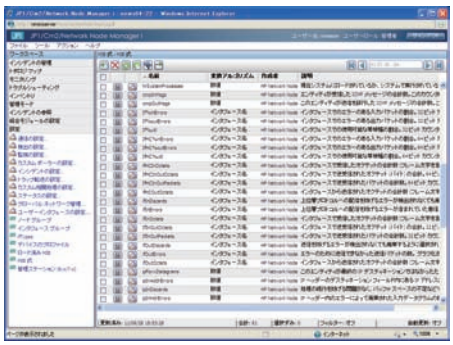
MIB 詳細説明の画面が別ウィンドウで表示されます。



8 標準の[MIB式]を参照します。

最後に、カスタムポーラーで使う MIB 式を参照しましょう。

ワークスペースの[設定] – [MIB 式]をクリックします。



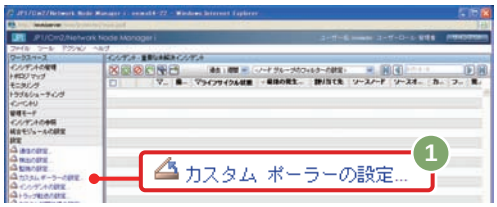
MIB 情報を MIB ブラウザで参照しましたが、カスタムポーラーはこのような MIB 情報の値を収集することで、性能監視や状態監視ができます。インタフェースのように複数のデータがある場合は、収集対象を MIB で条件指定してフィルタリングできます。

■操作手順　～カスタムポーラーを設定する～

カスタムポーラーの設定を開きます

1 ワークスペースの[設定] - [カスタムポーラーの設定]をクリックします。

[カスタムポーラー設定]画面が表示されます。



カスタムポーラーで収集するデータを設定します

2 [カスタムポーラーを有効化します]をチェックします。

カスタムポーラー機能が有効化されます。

3 [カスタムポーラー収集]タブを開いて、[ ](新規作成)をクリックします。

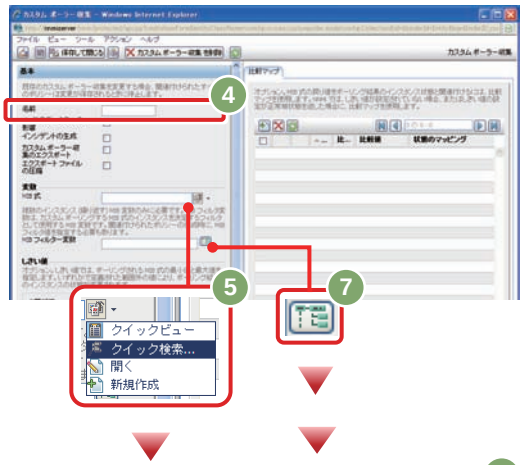
4 [名前]に収集項目の名前を入力します。

この名前は、インシデントのメッセージや、ノード画面のカスタムポーリングインスタンスの項目として表示されます。収集内容がわかりやすい名前を指定してください。

（例） 名前　：受信トラフィック

5 収集するデータである[MIB式]を指定します。
[ ]から[クイックサーチ]を選択します。

MIB 式を選択する画面が表示されます。



6 収集するMIB式の[ ]をクリックします。

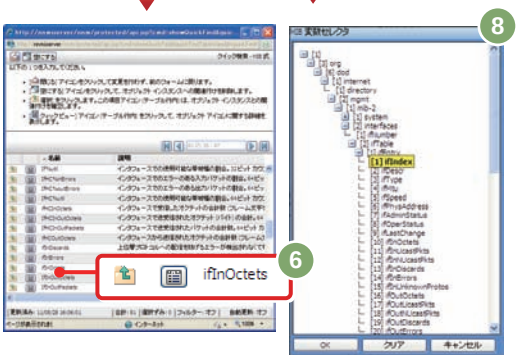
MIB 式が選択され、元の画面に戻ります。

7 [カスタムポーラー収集]画面で[ ]をクリックします。

[MIB 変数セレクタ]画面が表示されます。

8 [MIBフィルター変数]を指定します。

この MIB フィルター変数は、収集した MIB 情報が複数の値を持っている場合に、収集対象にする MIB をフィルタリングするために使います。OID 番号を順にクリックして、目的の MIB をクリックすると黄色の選択状態になります。[OK]をクリックします。

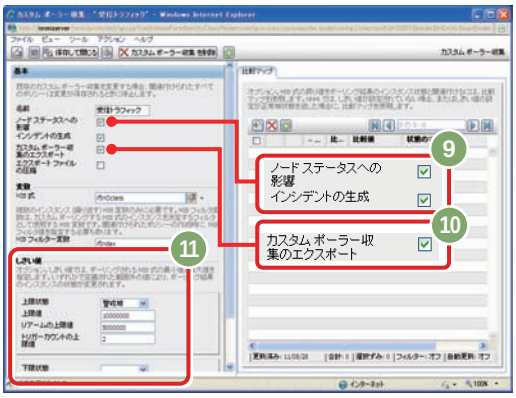


例えば、次の[MIB フィルター変数]を指定します。これは手順 15 で指定する[MIB フィルター]と対応します。
あとで設定する[ポリシー]では条件にする値を指定します。P.72 の[参考]も参照してください。
（例）[MIB フィルター変数] - [ポリシー] - [MIB フィルター]で設定する条件の値
・ifIndex（OID：.1.3.6.1.2.1.2.2.1.1 ）　1 , 2 , *（意味：インタフェースの番号で絞り込む）
・ifType（OID：.1.3.6.1.2.1.2.2.1.3 ）　vlan*（意味：インタフェースの種別で絞り込む）
・ifConnectorPresent(OID：.1.3.6.1.2.1.31.1.1.1.17 ）　1（意味：物理インタフェースだけに絞り込む）
1 は true（物理回線に接続）という意味です。
初めて試す場合は、すべてのインタフェースを収集対象にしてみましょう。この場合は、[MIB フィルター変数] ifIndex 、[MIB フィルター]の値を * に指定します。

9 [ノードステータスへの影響]や[インシデントの生成]を、運用に合わせてチェックします。

収集した MIB 式が、しきい値を超えたと判定したときの処理を指定します。

（例） 両方の項目をチェックする



10 [カスタムポーラー収集のエクスポート]を、運用に合わせてチェックします。

チェックすると、収集した MIB 式のデータを CSV ファイルに出力します。

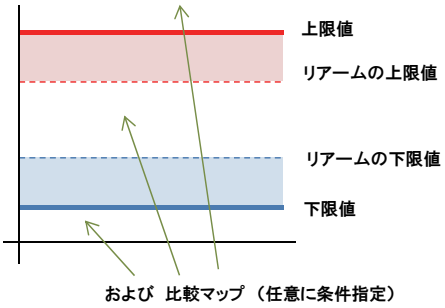
（例） 収集のエクスポートだけチェックする

11 [しきい値]の各項目を入力します。

次の例では、上限値の 10,000,000 を 2 回超えると警戒域となります。

9 の設定がされていれば、ノードステータスへ反映したり、インシデントを発行したりします。リアームの上限値である 5,000,000 を下回ると、警戒域が解除されます。

（例）　上限状態 ： 警戒域
　　上限値　 ： 10,000,000
　　リアームの上限値 ： 5,000,000
　　トリガーカウントの上限値 ： 2



参考

[しきい値]の上限値の動作について説明します。カスタムポーラーが収集した MIB 式の値が[上限値]を[トリガーカウントの上限値]の回数超えると、[上限状態]の状態になります。[リアームの上限値]の値を1度下回ると[上限状態]が解除されます。
[しきい値]の下限値も上下を逆にして同様な動作になります。
なお、比較マップ（MIB 式と条件を比較した結果を、状態としてマッピングする機能）を使うと、さらに詳しく任意の条件指定ができます。比較マップの設定についてはヘルプを参照してください。

12 [保存して閉じる]をクリックします。

カスタムポーラー収集に対応する［ポリシー］を設定します

13 [カスタムポーラー設定]画面に戻ったあと、[ポリシー]タブを開いて、[ ]（新規作成）をクリックします。

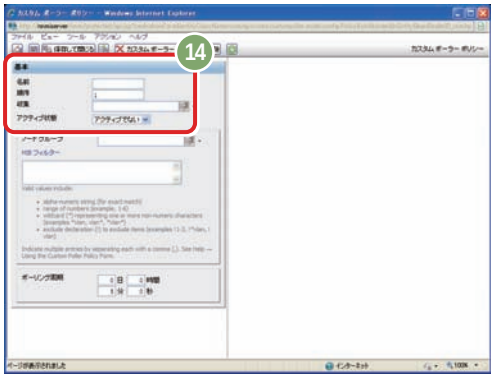
[カスタムポーラー　ポリシー]画面が表示されます。

14 ポリシーの基本項目を入力します。

- [名前]:　　収集する名前を入力します。
- [順序]:　　収集の順序を指定します（小さい値が優先）。
- [収集]:　　収集方法を選びます。[カスタムポーラー収集]画面で設定した[名前]の一覧から選択します。
- [アクティブ状態]:「アクティブ」にすると、収集を行います。

次は、システム部のデバイスを監視する例です。

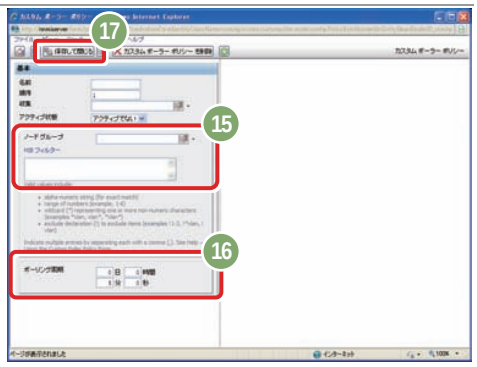
（例）[名前]:　システム部
　　[順序]:　1
　　[収集]:　受信トラフィック　手順 4 の設定
　　[アクティブ状態]:　アクティブ



15 カスタムポーリングの収集対象の条件を指定します。

- [ノードグループ]:　カスタムポーリングの対象となるノードグループを選択します。
- [MIB フィルター]:　[カスタムポーリング収集]の[MIB フィルター変数]の設定を参照して、条件を指定します。

設定する値は、手順 8 を参照してください。



16 カスタムポーリングの収集の周期を指定します。

デフォルトの周期（5 分）のままにします。

17 [保存して閉じる]をクリックします。

これでカスタムポーラーを設定する操作は完了です。

カスタムポーラーの収集データを参照する

設定したカスタムポーラーによって収集しているデータを参照してみましょう。

リアルタイムでグラフを参照する

カスタムポーラーで収集しているデータは、リアルタイムにグラフ表示することができます。

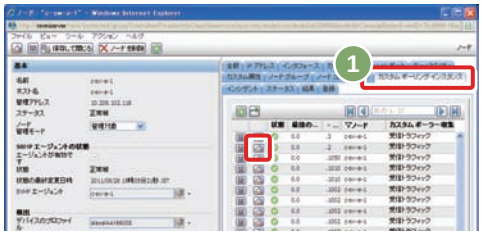
1 ノード画面の[カスタムポーリング　インスタンス]タブを選択し、インスタンスを開きます。

マップ画面などからノード画面を開き、[カスタムポーリングインスタンス]タブを選択します。

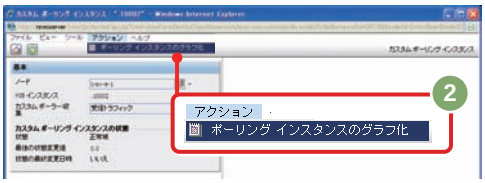
参照したい行の[]をクリックすると、[カスタムポーリングインスタンス]画面が開きます。

インスタンスが表示されない場合は、次の点を確認しましょう。

- [カスタムポーラーを有効化します]がチェックされているか。
- [MIB フィルター変数]と[MIB フィルター]の対応が正しいか。
- [MIB フィルター]の値が適切か。

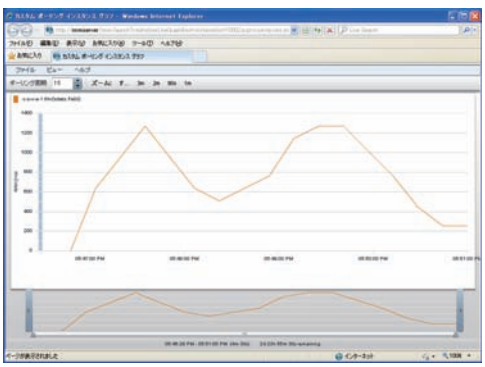


2 [カスタムポーリングインスタンス]画面で、[アクション] - [ポーリングインスタンスのグラフ化]を選択し、グラフ画面を開きます。



3 グラフを参照します。

その時点でカスタムポーラーが収集しているデータがグラフに表示されます。



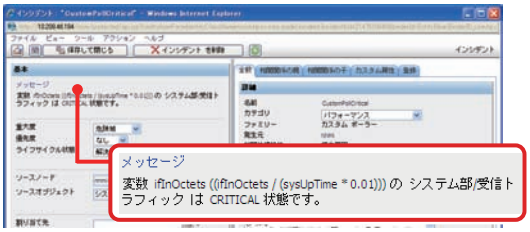
ノードステータスへの反映(カスタムポーリングインスタンス)を参照する

ノード画面を開き、[カスタムポーリングインスタンス]タブを開くと、カスタムポーラーの状態や値が表示されます。

画面には、状態が変化したときの値が表示されています。(収集した最新値ではありません)
最新の値を参照するには、CSV 出力ファイルを参照するか、リアルタイムグラフを参照してください。

カスタムポーラーのインシデントを参照する

設定したカスタムポーラーのしきい値を超えた場合、右図のようなインシデントが発行されます。
カスタムポーラーの[収集ルール]画面や[ポリシー]画面で指定した[名前]は、インシデントのメッセージ欄に表示されます。



CSVファイルを参照する

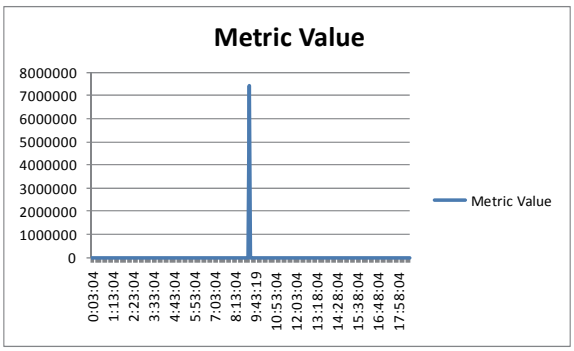
[カスタムポーラー収集]で、CSV ファイルへの出力を有効にすると、収集した MIB を「MIB 式」で加工した結果がファイルに出力されます。

ファイル出力先 *1	インストール先フォルダ(データ用)¥shared¥nnm¥databases¥custompoller¥export¥final
ファイル名称	(カスタムポール収集の名前)_(タイムスタンプ).csv (例)　受信トラフィック_20110922183744947.csv
出力方法　*1	[カスタムポール収集]の名前ごとにファイルに出力する。出力の周期はデフォルトで 5 分おき。 出力先フォルダが 1,000MB を超えると古いファイルが上書きされる。
出力項目　*2	Node UUID,　IP Address,　Node Name,　MIB Expression,　Time Stamp (ms),　Poll Interval (ms), MIB Instance,　Metric Value

*1:マニュアル【セットアップガイド】－[15.1 カスタムポーラー収集のエクスポートの管理]でカスタマイズ方法を説明しています。
*2:【管理者用ヘルプ】－[NNMi の機能を拡張する]－[カスタムポーリングの設定]－[カスタムポーラー収集の作成]
　－[カスタムポーラー収集に関する基本設定]に形式の説明があります。

ヒント　表計算ソフトを使用してグラフ化する

(例)時刻と測定値のグラフ



1. **CSVファイルが出力間隔ごとに分割されているので、例えば1日分を1ファイルに結合します。**
   C:¥> type (収集名)_(日付)*.csv　> graph.csv
2. **結合したCSVファイルを、表計算ソフトで開きます。**
3. **TimeStamp が 1970/1/1 00:00:00 からのミリ秒数の値なので表計算ソフトの日時形式に加工します。**
   (例)Excel の日時形式(シリアル値)にする場合の式
   ((TimeStamp/1000) +32400) /86400 +25569
4. **表計算ソフトのフィルタ機能などで、NodeName、MIB Instanceを条件に行を絞り込みます。**
5. **時刻(TimeStamp)と測定値(MetricValue)でグラフ化します。**
   項目が多くエラーになる場合は、対象データだけをコピーしてグラフ化します。

付録 NNMi Advancedの紹介

NNMi Advanced は、高度なネットワーク技術に対応した監視を提供する NNMi の上位製品です。

NNMi Advanced 機能一覧

機能	説明
グローバルネットワーク管理	拠点ごとの監視を行うリージョナルマネージャと、それらをまとめるグローバルマネージャによる集中管理ができます。
IPv6 ネットワークの管理	IPv6 と IPv4 を混在して管理できるため、次世代ネットワークと既存ネットワークを効率的に一元管理できます。
VMware ESX サーバの管理	ルータやスイッチを自動的に識別するように、ESX ホストと仮想マシンを自動識別し、インベントリ情報をリスト形式で管理できます。
リンクアグリゲーションの管理	アグリゲーションされたリンク構成を自動的に認識します。また、マップ上では、アグリゲーションされたリンクが太い線で表示されます。
冗長化ルーターの管理	冗長化されたルータグループの構成を自動認識します。また、ルータグループがパケットを適切にルーティングしているかどうかを監視できます。

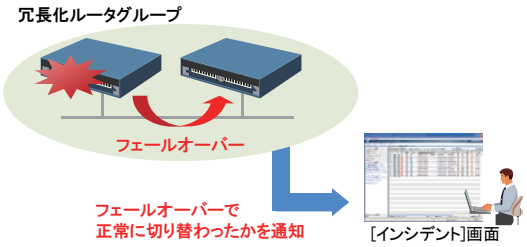
高度なネットワークに対応した管理

ネットワークのパフォーマンスや可用性・信頼性を確保するための、ルーターの冗長化や※1やリンクアグリゲーション※2に対応した高度なネットワークを管理できます。

※1：複数のルーターをルータグループ（RRG：Router Redundancy Group）に所属させ、障害時のフェールオーバーや負荷分散をする。
※2：複数の Ethernet リンクを束ねて一つの論理的なリンクを構成して、障害時のフェールオーバーや負荷分散をする。

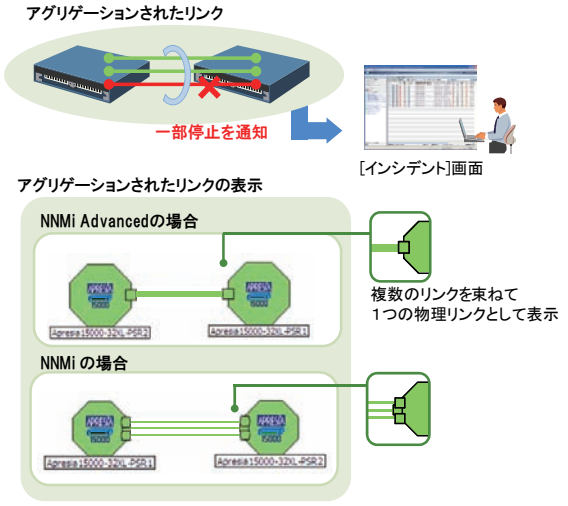
冗長化ルーターの管理

- 冗長化されたルータグループの構成を自動的に認識できます。
- ルータグループがパケットを適切にルーティングしているかどうかを監視できます。
- フェールオーバーで、正常にルーターが切り替わったかなど、ルータグループの状態変更がインシデントとして通知されます。



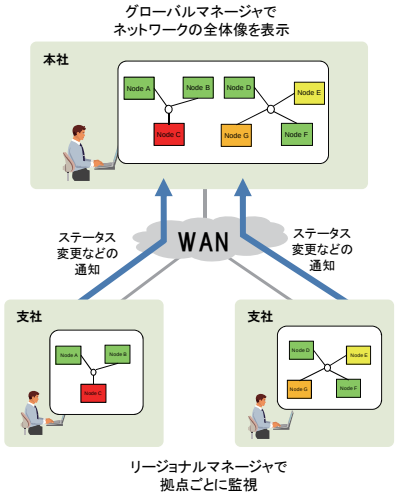
リンクアグリゲーションの管理

- アグリゲーションされたリンク構成を自動的に認識できます。
- アグリゲーションされたリンクは、マップ上で太い線で表示されるため、ほかのリンクと見分けることができます。
- リンクに異常があった場合、アグリゲーションされている一部が停止しているのか、またはすべて停止しているのかがインシデントで確認できます。



グローバルネットワーク管理

大規模なネットワーク環境で、拠点ごとの監視を行うリージョナルマネージャと、それらをまとめるグローバルマネージャを設置することによって、一元的な集中管理ができます。
グローバルマネージャでは最大 65,000 ノードまで監視できます。



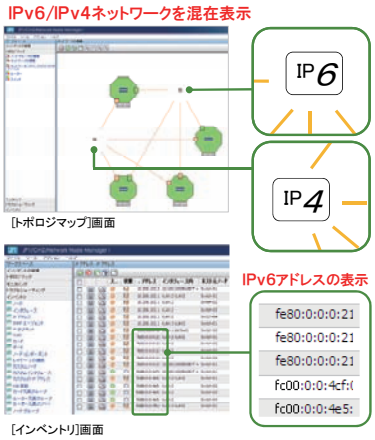
大規模なネットワークを集中管理

グローバルマネージャでは、企業のネットワーク全体を把握できるので、ネットワーク管理の運用性向上が期待できます。

- グローバルマネージャと拠点間はセキュアな通信（HTTPS）を選択できるので、保護された環境での運用ができます。
- グローバルマネージャはリージョナルマネージャ経由でノードのステータスを監視するため、管理のためのトラフィック(SNMP や ICMP)が拠点間で発生しません。
- リージョナルマネージャには NNMi または NNMi Advanced を選択できます。どちらを使用してもグローバルネットワーク管理機能に差異はありません。

IPv6 ネットワークの管理（UNIX/Linux版のみ）

次世代の IPv6 と既存の IPv4 が混在するネットワークのステータス監視やノード情報（構成情報、設定情報など）の管理を実現できます。



IPv6とIPv4の混在を一元管理

IPv6 ネットワークと IPv4 ネットワークを一元管理できるので、運用性の向上が図れます。

- IPv6 ネットワークの構成情報取得とレイヤ 3 トポロジマップを自動生成します。
- IPv6 アドレスの応答監視と IPv6 アドレスが設定されているインタフェースの状態を並行して監視できます。

NNMi は IPv6/IPv4 デュアルスタックのマシンにインストールする必要があります。

VMware ESXサーバの管理

VMware ESX または VMware ESXi のホストと仮想マシンを自動認識し、ステータス監視やノード情報の管理を実現できます。

VMwareホストや仮想マシンを管理

VMware ESX ホストや仮想マシンが何台あるかなどのノード情報の管理が容易にできるので、運用性の向上が図れます。

- 管理ノード一覧の画面で、フィルター機能を使って、ESX ホストや仮想マシンだけをリストアップできます。

VMware ESX Server の管理を行うためには、監視対象となる VMware ESX または VMware ESXi 上で SNMP エージェントを動作させておく必要があります。

付録 逆引き NNMi活用ガイド

NNMi を使ったネットワーク管理について、逆引き形式で説明します。
ポイントだけを簡単に説明していますので、詳しい説明は参照欄のページまたは関連資料を参照してください。

まず動かして使いながら試してみたい　今すぐ 1・2・3で始められないか

説明	まず次の 3 ステップで始めてみてください。操作方法は下記の参照欄のページをご覧ください。 ① [通信の設定]で SNMP コミュニティ文字列を設定する。 ② [検出の設定]で自動検出する IP アドレスの範囲を指定、ping スイープを有効化、SNMP ノード検出を有効化する。 ③ [トポロジマップ]の[ネットワークの概要]を開いて運用開始する。
参照	P.24　2.3 通信の設定　…[通信の設定]の操作方法 P.26　2.4 ネットワークの検出　…[検出の設定]の操作方法

監視するノードを一括登録したい

説明	監視するノードの IP アドレス一覧のファイルを作って、検出シードとして登録しましょう。 ① 一覧ファイルを作成　② nnmloadseeds.ovpl で登録　③ 検出が完了したらシードを削除
参照	P.26　2.4 ネットワークの検出　…「明示的に指定する」検出方法

監視しないノードを指定したい

説明	監視しないノードを、検出したあとで管理対象外にする方法と、検出しない方法とがあります。 (方法 1)検出したノードを管理対象外にする [インベントリ] – [ノード]などで対象ノードを選択し、[アクション] – [管理モード] – [非管理対象]を選択します。 (方法 2)対象のノードを検出しない [検出の設定] – [自動検出ルール]で、監視しないノードを検出範囲に指定しない、 または[自動検出ルール]で[IP の検出範囲]を指定するときに、検出しない IP を指定して 範囲のタイプを[ルールにより無視された]にするとその IP が検出対象外となります。 ※類似機能の[検出の設定] – [除外対象 IP]タブは、検出したノードから特定の IP アドレスだけを除外する場合に使います。監視しないノードの指定に使うとノードが残ったまま IP が消える現象などが発生します。用途により使い分けてください。
参照	【管理者用ヘルプ】 – [ネットワークの検出] – [検出の設定] – [除外対象 IP アドレスフィルターを設定する] 【管理者用ヘルプ】 – [ノード、インタフェース、カード、アドレス、またはノードコンポーネントの管理を停止または再起動する]

ノードが全く検出されません

説明	[検出の設定]で、検出対象の IP アドレス範囲と、検出の起点となる検出シードを指定してください。検出の状況は、トポロジマップ画面やインベントリ画面で確認します。また検出の処理状況をヘルプ – [システム情報] – [StatePoller]で確認できます。 なお JP1V8 までの NNM では、インストール後に NNM のあるセグメントから自動的に検出を行いましたが、検出の起点の変更などはできませんでした。 JP1V9 の NNMi では、[検出の設定]で任意の検出範囲を細かく設定することができます。
参照	P.26　2.4 ネットワークの検出

ルータやスイッチしか検出されないのですが・・・

説明	デフォルトの設定では、ルータやスイッチだけを検出します。 [検出の設定]で、[SNMP デバイスの検出]や[非 SNMP デバイスの検出]を有効化してください。
参照	P.26　2.4 ネットワークの検出

クラスタシステムを監視したい　（論理 IP の監視）

説明	クラスタシステムを監視する場合は、論理 IP アドレスを監視しないように「除外対象 IP アドレス」として設定してください。この設定をしないと、論理 IP アドレスが移動したときに、ノードが削除されたり、別ノードの状態が反映されたりするなどの現象が発生します。詳細はリリースノートを参照してください。
参照	リリースノート　「クラスタ構成のノードの監視」で検索してください。

snmpwalk コマンドはありますか

説明	nnmsnmpwalk.ovpl コマンドを使ってください。
参照	ヘルプ – [NNMi ドキュメントライブラリ] – [リファレンスページ] – nnmsnmpwalk.ovpl

監視するノードをグループ化したい

説明	ノードグループを設定してください。 （方法）グループ化の条件は、IP アドレスの範囲、デバイスの種類、設置場所(sysLocation)などを指定できます。ノードグループは 5 階層まで定義できます。 （用途）ノードグループを使うと、次のことができます。 • ノードグループ用のマップを定義できる　…[ノードグループマップ] • ノードグループごとに監視方法を調整できる　…[監視の設定] – [ノードの設定] • カスタムポーラで ノードグループ単位に性能監視ができる　…[カスタムポーラ]
参照	P.38　2.5 ノードグループの設定

ノードグループを定義したら、トポロジマップ名の表示が多過ぎて見づらい

説明	ノードグループマップの「トポロジマップ順序」を空欄にすると、ワークスペースの[トポロジマップ]のマップ名一覧に表示されなくなります。
参照	P.42　2.5 ノードグループの設定 …ノードグループマップを設定する

メンテナンス中は監視を一時停止したい

説明	ノードの管理モードを「サービス停止中」にすると、監視や再検出をしなくなります。 （方法 1）マップ画面などノードを選択します。 …[アクション] – [管理モード] – [サービス停止中] （方法 2）nnmmanagementmode.ovpl コマンドで管理モードをサービス停止中にします。 非管理対象にしたノードを一覧表示するには？ （方法）ワークスペースの[管理モード] – [管理対象外ノード]を参照します。 監視を再開するには？ （方法 1）マップ画面などノードを選択します。 …[アクション] – [管理モード] – [管理対象（すべてをリセット）] （方法 2）nnmmanagementmode.ovpl コマンドで管理モードを管理対象にします。
参照	【管理者用ヘルプ】 – [ノード、インタフェース、カード、アドレス、またはノードコンポーネントの管理を停止または再起動する]

監視（状態ポーリング）をしているのか見えない、監視状況を確認したい

説明	状態のポーリングは、NNMi の“State Poller“機能が処理しています。この機能の稼動状態統計情報を次の個所で確認できます。 （方法）NNMi コンソール画面のメニューから[ヘルプ] – [システム情報] – [StatePoller]タブを選択します。 なお、NNMi 自体に問題が発生した場合は、コンソール画面の下部に黄色で警告表示がされ、NnmHealthOverallStatus インシデントが発行されます。運用中にこのインシデントが通知された場合は、NNMi の状態を確認してください。
参照	P.66　4.1 日頃の運用～ネットワークの監視～

ノードと通信できないが危険域ではなく認識不能（アイコンが青色）になった

説明	例えば、ネットワーク経路途中のスイッチに障害が起きて、あるノードと通信できなくなった場合、NNMi は、スイッチを障害の根本原因としてインシデントを通知します。また、その影響で通信できなくなったノードは認識不能などと判定します。 通信できなくなった場合にインシデントを通知したい場合は、「重要なノード」を使ってください。
参照	P.52　解説「インシデント」 ～重要な事象に絞って通知する～ P.39　2.5 ノードグループの設定 …「重要なノード」ノードグループについて

SNMP マネージャ（NNMi）の IP アドレスは？

説明	SNMP エージェント側の SNMP 設定で、SNMP マネージャの IP アドレスを指定（接続を許可）する場合、NNMi サーバの IP アドレスを一通り設定してください。これは OS のネットワークのルーティング設定によって、通信先 IP に応じた IP アドレスが動的に使い分けされるためです。 IP アドレスを固定したい場合は、リリースノートを参照して、ov.conf ファイルの NNM_INTERFACE に IP アドレスを指定してください。これによって、SNMP 通信時に使う IP アドレスが固定されます。固定した IP アドレスで通信できるように OS のルーティング設定を調整してください。
参照	リリースノート　「NNM_INTERFACE」をキーワードに検索してください

SNMP トラップを発行したがインシデントとして通知されない

説明	SNMP トラップを NNMi が受信したとき、インシデントとして通知するには次の条件があります。 （条件）ノードを検出済み、当該 SNMP トラップのインシデントが定義済みで有効に設定します。 検出されていないノードからのトラップをインシデント化するには？ （方法）[インシデントの設定]の[未解決の SNMP トラップを廃棄する]をオフにします。
参照	【管理者用ヘルプ】 – [インシデントを設定する] – [受信 SNMP トラップを管理する] – [未解決の受信トラップを処理する]

SNMP トラップの状況を確認したい

説明	（方法 1）SNMP トラップインシデントを確認します。 （方法 2）nnmtrapdump.ovpl コマンドで表示します。 （例）nnmtrapdump.ovpl –source (IPaddr)　…IPaddr からの受信トラップを表示 nnmtrapdump.ovpl –t　…受信トラップを連続表示（設定時の確認などでご利用ください）
参照	【オペレータ用ヘルプ】 – [インシデントでの障害モニタリング] – [NNMi に用意されているインシデント ビュー] – [SNMP トラップ ビュー] ヘルプ – [NNMi ドキュメントライブラリ] – [リファレンスページ] – nnmtrapdump.ovpl

障害を検知したときに 自動アクションを実行したい

説明

インシデントに対して、自動アクションの実行を設定することができます。
(方法)ワークスペースの[設定]－[インシデントの設定]を開き
　　任意のインシデントの画面を開いて[アクション]タブで設定します。

自動アクションを実行するタイミングは、アクション設定のライフサイクル状態で指定できます。

- アクション設定のライフサイクル状態を「登録済み」に指定すると、インシデントが発生して登録されたときに自動アクションが実行されます。
- 「ノードが停止したのち回復して起動したタイミングで通報システムと連動したい」という場合は、ライフサイクル状態を「完了」に指定した自動アクションを指定します。

参照

P.56　3.2 インシデントの設定

障害を検知したときに メール送信やパトランプで通知したい

説明

インシデントの自動アクションとして、メール送信やパトランプ連携を実行するよう設定してください。

参照

P.56　3.2 インシデントの設定

自動アクションの内容をノードによって変えたい

説明

自動アクションの設定はインシデント設定画面で行いますが、設定を行うタブにより、アクションを実行する対象について条件指定することができます。

[インタフェースの設定]タブ －[アクション]タブ	…対象 :インタフェースグループで条件指定
[ノードの設定]タブ －[アクション]タブ	…対象 :ノードグループで条件指定
[アクション]タブ	…対象 :指定なし

優先度は［インタフェースの設定］＞［ノードの設定］＞ 普通の[アクション］の順です。高い優先度のアクション設定がほかの設定を上書きするため、アクションは 1 度だけ実行されます。
これを応用して、ノード全般への自動アクションを設定し、特定のノードグループだけは別の自動アクションを実行するなどができます。

参照

【管理者用ヘルプ】－[インシデントを設定する]

自動アクションの実行状況を確認したい

説明

自動アクションの実行状況をみるには、次のどちらかでログを確認します。
(方法 1)マップ画面で ［ツール］－[インシデントアクションログ]を見ます。

(方法 2)ログファイル %NnmDataDir%¥log¥nnm¥incidentActions.*.*.log を参照します。

＜ログの出力例＞

```
8　28,　2011　11:01:05.223　午 後　[ThreadID:10]　FINE:　com.hp.ov.nms.events.actionlog.ActionLogger
addActionResponseToCompletedList:
********************************************************************************
Command: ""msg.exe" "Administrator" "インシデント NodeDown が nodeesx04 で発生しました。""
Incident Name: NodeDown
Incident UUID: 767f6182-f5fc-4ed9-a253-7417f42a8bd2
Command Type: ScriptOrExecutable
Lifecycle state: com.hp.nms.incident.lifecycle.InProgress
Exit Code: 0
Standard Output:
Standard Error:
Execution Status: Finished execution
********************************************************************************
```

(備考)アクション設定の「有効にする」のチェックを忘れていると、自動アクションが実行されずログにも履歴が出ません。実行されない場合は、まず有効になっているか確認してみましょう。

参照

【管理者用ヘルプ】－[インシデントを設定する]

どのインシデントが通知されますか？

説明	障害の状況によります。NNMi の根本原因解析の機能が、監視状況を解析して根本原因と判定したインシデントを通知します。 例えば、ノードがダウンしたときは、NodeDown(ノード停止中)、NodeOrConnectionDown(ノードまたは接続が停止中)、NonSNMPNodeUnresponsive(非 SNMP ノードが応答なし) のうち根本原因の解析結果に適切なインシデントが通知されるか、またはほかに根本原因があると判定してインシデントの通知を抑止します。 詳細は参照欄の資料を参照してください。 シンプルに運用する方法の一つとしては、「重要なノード」ノードグループに含める方法があります。「重要なノード」が無応答になると NodeDown または NonSNMPNodeUnresponsive のインシデントが発行されるため、これを監視します。
参照	P.52　解説「インシデント」 ～重要な事象に絞って通知する～ P.56　3.2 インシデントの設定 マニュアル【セットアップガイド】 - [付録 B Causal Engine と NNMi インシデント]

インシデントの状況を確認したい

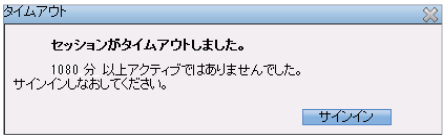
説明	ワークスペースの[インシデント] - [すべてのインシデント]で解決済みを含めたインシデントを確認できます。 対象のノードを開いて、[インシデント]タブを開くと、時系列でインシデント発生を確認できます。まず「相関処理の注」を確認して状況を見ましょう。
参照	P.60　3.3 インシデントのライフサイクル管理

画面を複数開きたい（例：マップ画面とインシデント画面を両方開く）

説明	(方法 1)[](新しいウィンドウでビューを表示)をクリックすると別画面が表示されます。 (方法 2)URL を入力して画面を開きます。 (例)[トポロジマップ]の[ネットワークの概要]画面を開く http://ホスト名:ポート番号/nnm/launch?cmd=showNetworkOverview&newWindow=true
参照	P.66　4.1 日頃の運用 ～ネットワークの監視～

画面を開いたままにしていたら、タイムアウトした

説明	一定時間操作しないとタイムアウトします。 (方法)タイムアウト時間を設定するには ワークスペースの[設定] - [ユーザーインタフェースの設定]のコンソールタイムアウトに設定します。デフォルトは 18 時間です。 (方法)URL 起動で表示したマップ画面は、タイムアウトしません。 常時監視するマップ画面などは、URL 起動で表示します。
参照	P.66　4.1 日頃の運用 ～ネットワークの監視～



サインインしたときの初期画面を設定したい

説明	[ユーザーインタフェースの設定]の初期ビューで指定できます。 （例）・インシデントを見たい　…「重要な未解決インシデント」を指定します。 ・マップを見たい　…「ネットワークの概要」や「トポロジマップ　ワークスペース内の最初のノードグループ」などを指定します。 なお、ユーザーが作成したノードグループマップを初期ビューにできますが、マップ一覧の最初または最後しか指定できないため、ノードグループマップの設定の[順序]を調整してください。
参照	【管理者用ヘルプ】－[NNMi ユーザー インタフェースを設定する]　…初期ビュー

クイックビュー（アイコンにマウスをかざすと出るウィンドウ）を消したい

説明	[]（クイックビューを無効にする）をクリックすると、クイックビューが表示されなくなります。
参照	P.30　2.4 ネットワークの検出　…検出したネットワークを参照する

サーバー覧やインシデント一覧など 一覧表を作成したい

説明	インベントリ画面などテーブル形式でデータを一覧表示する画面では、HTML 形式でデータを画面に出力できます。 例えば、ワークスペースの[インベントリ]から[ノード]画面を開いて、次の操作を行います。 （操作）1. テーブル内の任意のセルまたは列を、右クリックします。 2. メニューが表示されるので[プリント可能バージョン]－[可視行]を選択します。 HTML 形式のデータが別ウィンドウで開きます。 これをファイルに保存したり、表計算ソフトにコピー＆ペーストしたりすることによって、一覧表などを作成してください。 よく使われる用途と、参照する画面を紹介します。 • ノード一覧を作成する　…ワークスペースの[インベントリ]－[ノード] • インシデント一覧を作成する　…ワークスペースの[設定]－[管理イベントの設定]
参照	ヘルプ【コンソールの使用】－[ビューを使用してデータを表示する]－[テーブルビューを使用する]－[テーブル情報の印刷]

ポーリングの種類がたくさんあるようですが・・・

説明	ポーリングとは、SNMP や ICMP(Ping)を使ってネットワークの検出や監視を周期的に行うことです。これには大きく分けて 2 種類があります。 • 検出のためのポーリング • 監視のためのポーリング 実質的にはこの 2 種類ですが、NNMi の各種資料では、目的や状況によって次のように表記されます。 • 検出のためのポーリング ・検出ポーリング ・再検出ポーリング（検出済みのノードを構成変更がないか定期的に再検出するポーリング） ・設定ポーリング（設定を検出するためのポーリング） ・発見ポーリング（「検出」の別の言い方が「発見」。ノードを発見するためのポーリング） • 監視のためのポーリング ・ステータスポーリング（ステータスを監視するためのポーリング） ・状態ポーリング（状態を監視するためのポーリング） ・障害ポーリング（障害が発生していないか監視するためのポーリング） ・デマンドポーリング（手動操作などを契機に即時に監視を行うポーリング） なお、カスタムポーラーによるポーリングは、監視のためのポーリングですが、性能監視のためにユーザ指定の任意の MIB を取得するポーリングであるため、別に分類する場合もあります。
参照	－

用語解説

英字

ARPキャッシュ
ARPプロトコルにおいて、IPアドレスをMACアドレスに関連づけるため、PCやネットワーク機器のメモリ内に一時的に作成されるテーブルのことです。一定の時間が経つとクリアされ、再度作成されます。

Causal Engine
ネットワーク上のノード、インタフェース、IPアドレス、SNMPエージェントなどの稼働状態から、障害の根本原因を解析する機能です。

FQDN
完全修飾ドメイン名のことです。TCP/IPネットワーク上で、ドメイン名、サブドメイン名、およびホスト名を省略しないですべて指定した記述形式を指します。

ICMP(Ping)
IPプロトコルでエラーメッセージや制御メッセージを転送するためのプロトコルのことです。NNMiは、ノードを監視する状態ポーリングにICMP(Ping)とSNMPを使用します。

JP1/Cm2/Network Node Manager i
業界標準のSNMPを採用し、ネットワークの構成管理、障害管理を実現するソフトウェアです。IPネットワーク上のノードを自動で発見して構成を管理できます。また、ネットワークの障害を検知してシステム管理者に警告することができます。

NNMi
JP1/Cm2/Network Node Manager iの略称です。

NNMiコンソール
NNMiに対する操作を実施するメイン画面のことです。NNMiの設定をしたり、監視対象の情報を表示したりします。

Pingスイープ
ICMP(Ping)を複数のIPアドレスに送信し、応答するノードにどのアドレスが割り当てられているかを調べます。Pingスイープを有効にすると、自動検出ルールで定義されたIPアドレスの範囲にICMP(Ping)を送信して、応答のあるノードを監視対象に追加します。

SNMP
IPネットワーク上のネットワーク機器をネットワーク経由で監視・制御するためのプロトコルです。NNMiはSNMPv1、SNMPv2c、およびSNMPv3に対応しています。このため、SNMPをサポートするネットワーク機器であれば、ベンダーを問わず一元管理できます。

SNMPトラップ
SNMPエージェントに障害が発生したときに、SNMPエージェントからSNMPマネージャに情報を通知する処理のことです。

あ

イベント
ネットワークで発生するさまざまな事象のことです。

インシデント
ネットワークで発生するさまざまな事象（イベント）のうち、管理者に通知する必要がある重要性の高い情報のことです。NNMiはネットワークで発生するイベントの根本原因を解析し、インシデントとして通知します。

インシデント管理
ネットワークへの影響が大きい障害の通知から、その障害の解決までをインシデントによって管理することです。

インタフェース
複数の機器を接続してデータをやり取りするときの、機器と機器の間を取り持つ接続用プログラムやハードウェアを指します。NNMiではノード間の接続を指す場合もあります。

か

検出シード
監視対象ノードを検出する際の起点となるノードのことです。自動で検出する場合、検出シードのARPキャッシュを使用して、隣接するデバイスを検出します。検出シードには、隣接するデバイスの情報を多く持つルーターなどを指定します。

コミュニティ文字列
SNMPv1またはSNMPv2cによるモニタリングにおいて、ノードを検出するかどうかを判定するために使う文字列です。NNMiマネージャと監視対象のノードの両方に同じコミュニティ文字列が設定されているとき、ノードを検出します。

根本原因解析（RCA）
ネットワーク障害によって発生するさまざまなイベントの相関関係を調査・フィルタリングし、レイヤー2トポロジに基づいて障害を解析することで、障害の原因を特定することです。

さ

システムアカウント
NNMiコンソールに最初にアクセスするときに使用する管理者アカウントです。このほか、システムアカウントはユーザーアカウントを忘れてしまったなどの復旧作業で使用します。

自動アクション
インシデントのライフサイクル状態に応じて、自動で任意のコマンドを実行させる機能のことです。

自動検出ルール
監視対象ノードを自動で検出するときに、検出対象となるネットワークの範囲や検出の対象のデバイスなどを指定した定義のことです。

重大度
インシデントの障害への影響度を示す値のことです。

状態ポーリング
SNMPエージェント、インタフェースおよびIPアドレスの稼働状態を監視するポーリングのことです。

た

デバイス
ルーター、スイッチ、PC、プリンタなどのIT機器のことです。

トポロジマップ
検出したネットワーク機器の状態や接続関係をビジュアル化したネットワーク構成図のことです。

な

ノード
NNMiで監視するデバイスのことです。

ノードグループ
検出したネットワーク機器をIPアドレスやデバイス種別などの条件でグループ化、階層化したものです。

ノードグループマップ
業務・地域ごとなど、ノードグループ別にネットワーク機器をカテゴライズして表示させるマップのことです。

は

ビュー
NNMiコンソールのワークスペースから選択できる個々の操作項目のことです。

ポーリング
NNMiから監視対象に対して、監視対象の状態を周期的に問い合わせる処理のことです。

ま

モニタリング
SNMPやICMP(Ping)を使って、周期的に監視対象の稼働状態を確認することでネットワークを監視することです。

や

ユーザーアカウント
NNMiコンソールを使用するアカウントです。アカウントに割り当てるロール（権限）によって、操作できるNNMiコンソールのワークスペース、フォーム、およびアクションが異なります。

優先度
インシデントに対しての緊急性を示す値のことです。インシデントの優先度は1（最上位）～5（なし）まであり、管理者が任意で設定できます。

ら

ライフサイクル管理
インシデントをライフサイクル状態によって管理し、適切に対処することです。

ライフサイクル状態
インシデントの進行状況を確認するための属性です。状態には、「登録済み」、「進行中」、「完了」および「解決済み」があり、インシデントの対策状況に応じて更新します。

レイヤー2トポロジ
OSI参照モデルのデータリンク層からみたネットワークの接続関係のことです。末端のスイッチと端末間の結線などを表しています。

レイヤー3トポロジ
OSI参照モデルのネットワーク層からみたネットワークの接続関係のことです。ネットワークの論理構成を表しています。

ロール
ユーザーアカウントに割り当てる権限のことです。ロールには、「管理者」「オペレータ レベル2」「オペレータ レベル1」「ゲスト」があり、それぞれ操作できるNNMiコンソールのワークスペース、フォーム、およびアクションが異なります。

わ

ワークスペース
NNMiコンソールでビューを集約し、一覧で表示させたものです。作業対象や作業範囲など、関連するビューごとにカテゴライズされています。

このマニュアルでの表記

このマニュアルでは、日立製品およびそのほかの製品の名称を省略して表記しています。
製品の正式名称と、このマニュアルでの表記を次に示します。

このマニュアルでの表記			正式名称
Adobe Flash Player			Adobe(R) Flash(R) Player
Firefox			Mozilla Firefox(R)
HP-UX			HP-UX 11i v3(IPF)
Internet Explorer			Microsoft(R) Internet Explorer
			Windows(R) Internet Explorer(R)
Linux			Red Hat Enterprise Linux(R) AS4(AMD64& Intel EM64T)
			Red Hat Enterprise Linux(R) ES4(AMD64& Intel EM64T)
			Red Hat Enterprise Linux(R) 5 Advanced Platform(AMD/Intel64)
			Red Hat Enterprise Linux(R) 5(AMD/Intel64)
			Red Hat Enterprise Linux 6(AMD/Intel64)
JP1/Cm2/NNM i			JP1/Cm2/Network Node Manager i 09-50
NNMi			
NNMi Advanced			JP1/Cm2/Network Node Manager i Advanced 09-50
Solaris			Solaris 10(SPARC)
Windows	Windows Server 2008	64bit 版 の Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Enterprise
			Microsoft(R) Windows Server(R) 2008 Standard
			Microsoft(R) Windows Server(R) 2008 R2 Datacenter
			Microsoft(R) Windows Server(R) 2008 R2 Enterprise
			Microsoft(R) Windows Server(R) 2008 R2 Standard
	Windows Server 2003	Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
			Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
		Windows Server 2003 R2 (x64)	Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
			Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
	Windows XP		Microsoft(R) Windows(R) XP

このマニュアルで使用する英略語

このマニュアルで使用する英略語を、次の表に示します。

このマニュアルでの表記	正式名称
ARP	Address Resolution Protocol
FQDN	Fully Qualified Domain Name
ICMP	Internet Control Message Protocol
IE	Internet Explorer
LLDP	Link Layer Discovery Protocol
MIB	Management Information Base
OSI	Open Systems Interconnection
RCA	Root Causal Analysis
SNMP	Simple Network Management Protocol
VRRP	Virtual Router Redundancy Protocol

索引

か

き

く

け

こ

さ

し

そ

つ

て

ね

の

は

ひ

へ

ほ

め

も

ゆ

ら

れ

本製品を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

なお、ご不明な場合は、弊社担当営業にお問い合わせください。

2011年 9月 発行