今すぐ体験
JP1

JP1/Cm2/Network Node Manager i

はじめての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-T03

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 7.0

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

「はじめての 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。

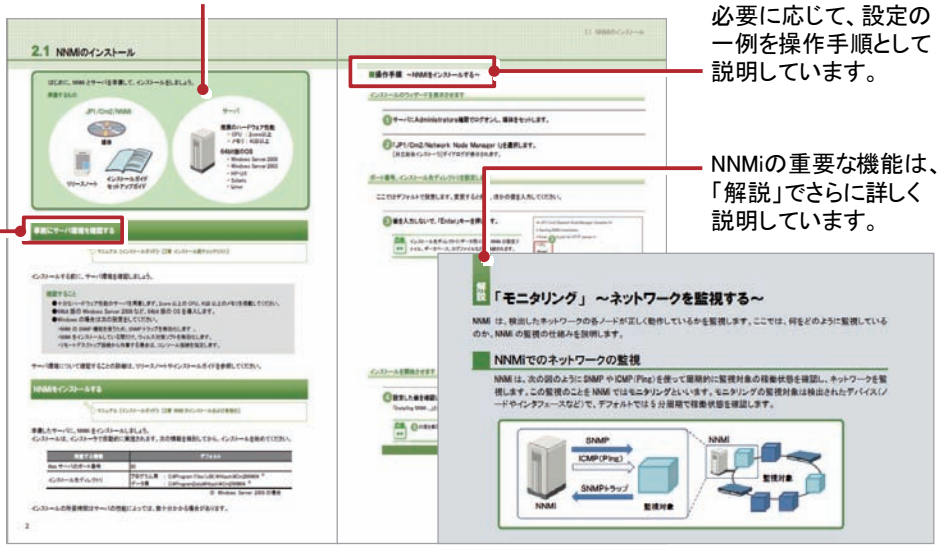
2章 **3章** 節ごとに、NNMi の基本的な使い方の概要と、操作手順について説明しています。

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。

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。

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。



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

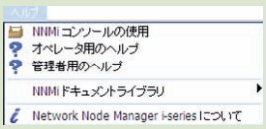
本文中ではカッコ内のように記載します。

- 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

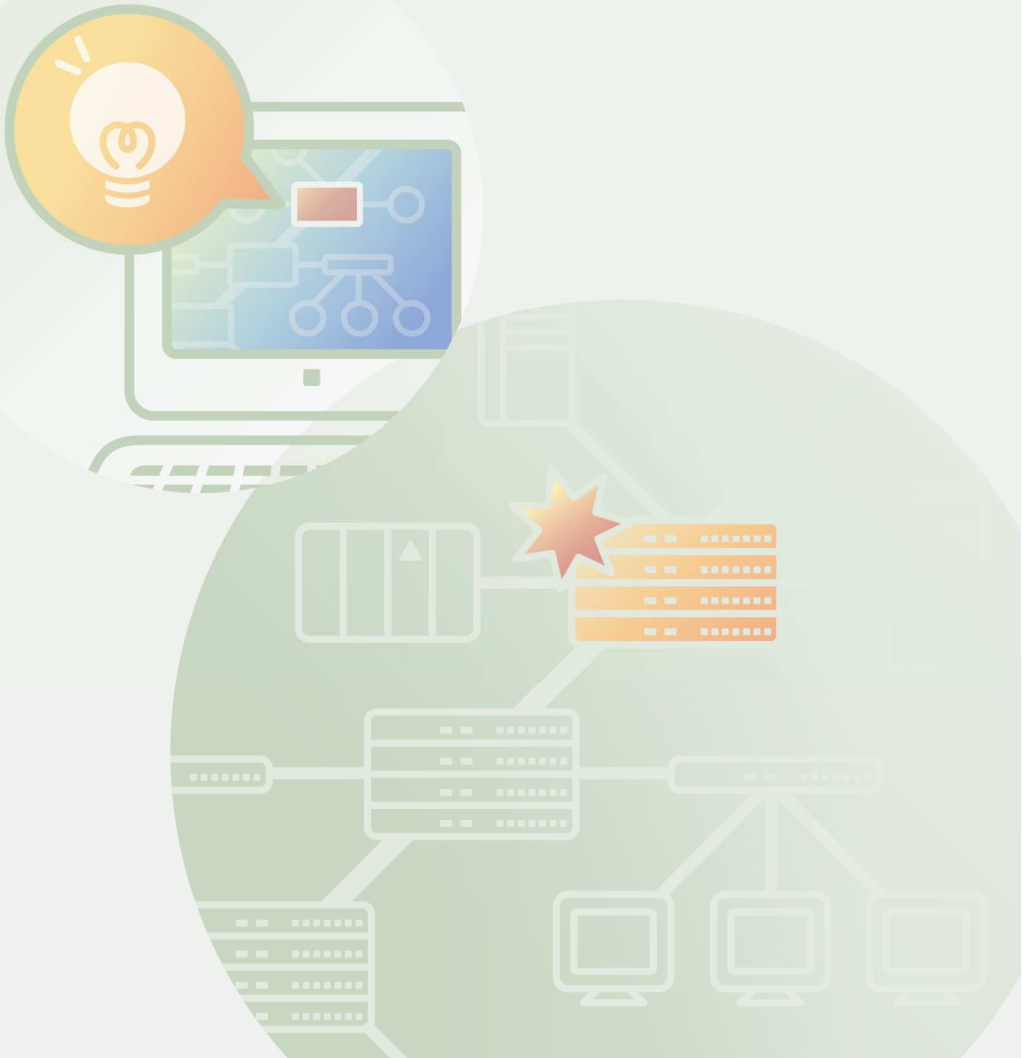
関連マニュアルへの参照指示

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 【NNMi コンソールの使用】
マニュアル【セットアップガイド】-［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。

悩み

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！

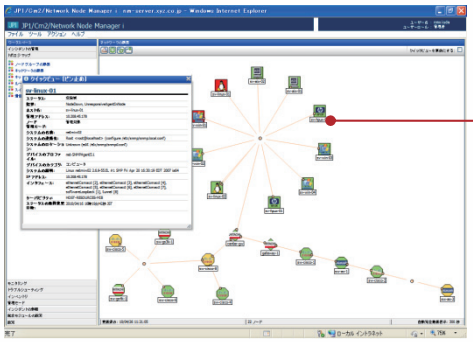
まずは事前準備！

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



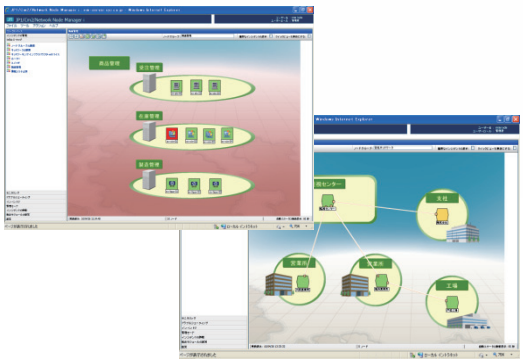
ネットワーク機器の状態を色で表現

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

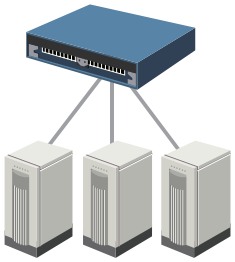
SNMP をサポートするネットワーク機器なら製品のベンダーにとらわれることなく一括管理できます。

ノードグループマップ

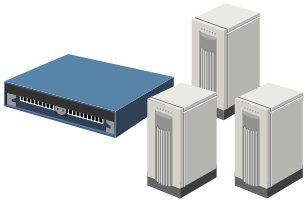


トポロジマップをカスタマイズしたマップがノードグループマップ。
ネットワーク機器をカテゴライズして、よりビジュアルに管理！　問題の発生個所をすぐに特定でき、自由度の高い管理を実現。

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。

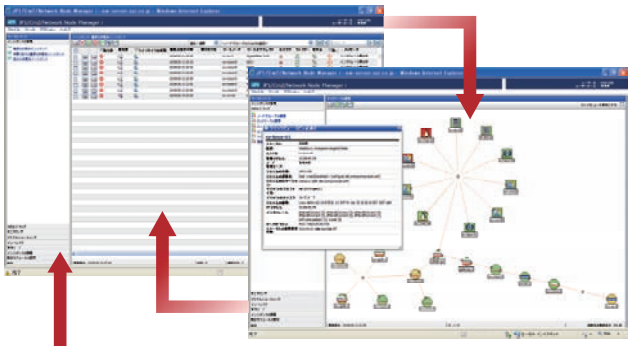
JP1のネットワーク管理製品「JP1/Cm2/Network Node Manager i」は、ネットワーク構成の把握や、障害の特定・解決など、ネットワーク管理の中でも特に作業負荷が高くなりがちな作業をかんたん便利にするための機能を用意しています。

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

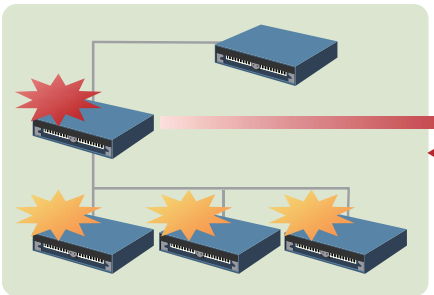
1台のNNMiで、50台から18,000台までのネットワーク機器を監視できるため、集中管理が実現できます。

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プロトコルにもと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

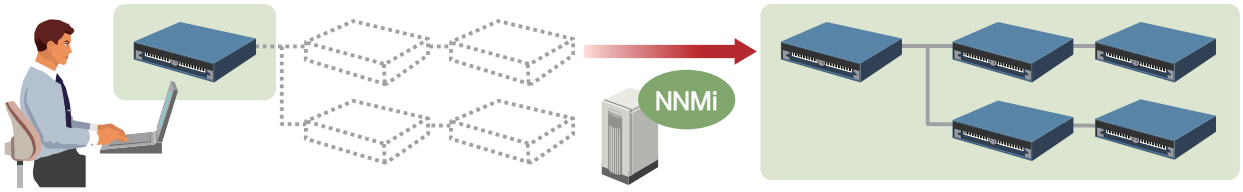
ネットワーク構成をビジュアルに効率よく把握

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。



検出シードを設定　　自動で検出　　設定完了！

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

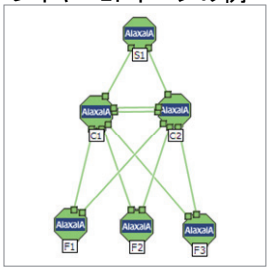
アイコンの形で、ルーターや PC などネットワーク機器の種類がわかります。
また、色で障害の発生有無などのネットワーク機器の状態を把握できます。

レイヤー2トポロジを表示

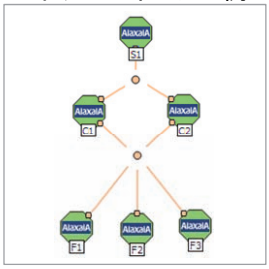
ネットワークのレイヤー3 トポロジだけでなく、レイヤー2 トポロジを表示させて確認できます。

- 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

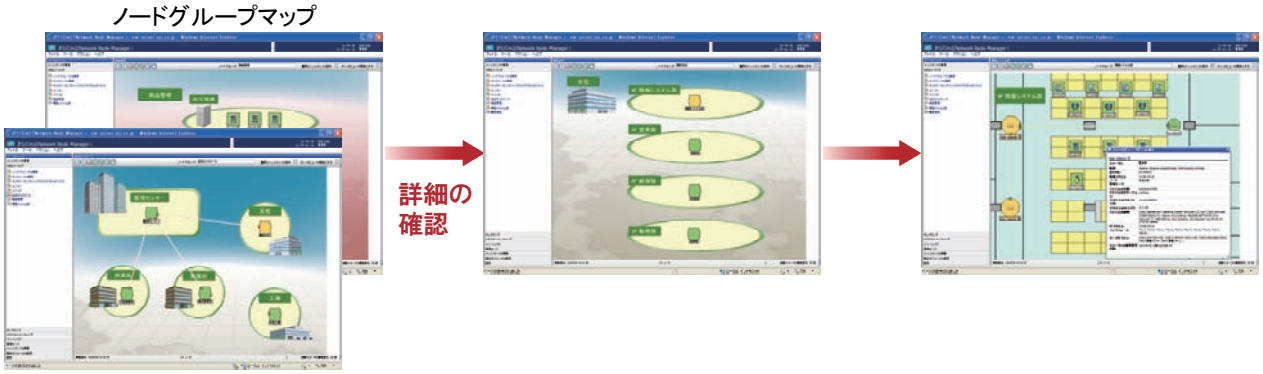
検出したネットワーク機器をカテゴライズして表示させるマップ（**ノードグループマップ**）を作成できます。このノードグループマップを作成することで、トポロジマップよりも視点を絞ってネットワーク構成が把握できるようになるため、問題の発生個所を探しやすくなり、すばやく詳細を確認できます。

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

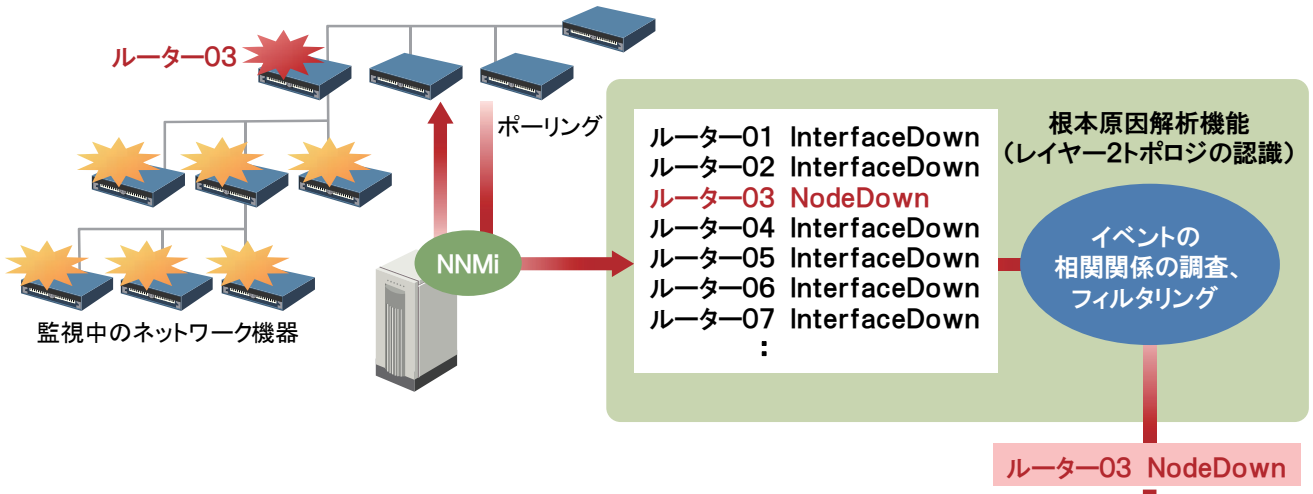
NNMi は、SNMP や ICMP プロトコルにもとづいたポーリングによって、検出したネットワーク機器を監視します。ネットワーク機器の状態だけでなく、ファン・電源・電圧など、ネットワーク機器のコンポーネントの状態も対象としているため、幅広い障害監視を実現できます。なお、ポーリングは、周期（秒、分、時間、日単位）を設定することで、自動で定期的に実行されます。障害を解決した直後など、すぐにポーリングしたいときは手動でも実施できます。

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トポロジにもと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。

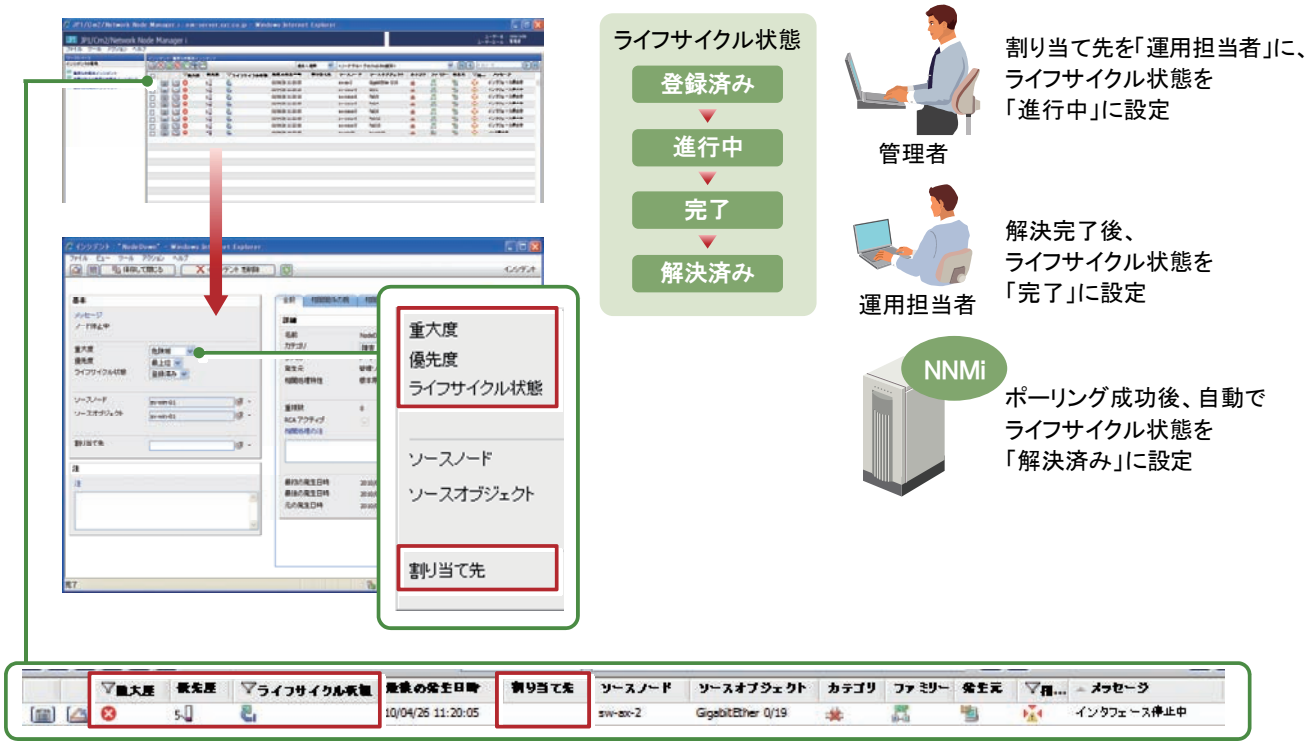
トポロジマップの表示画面

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

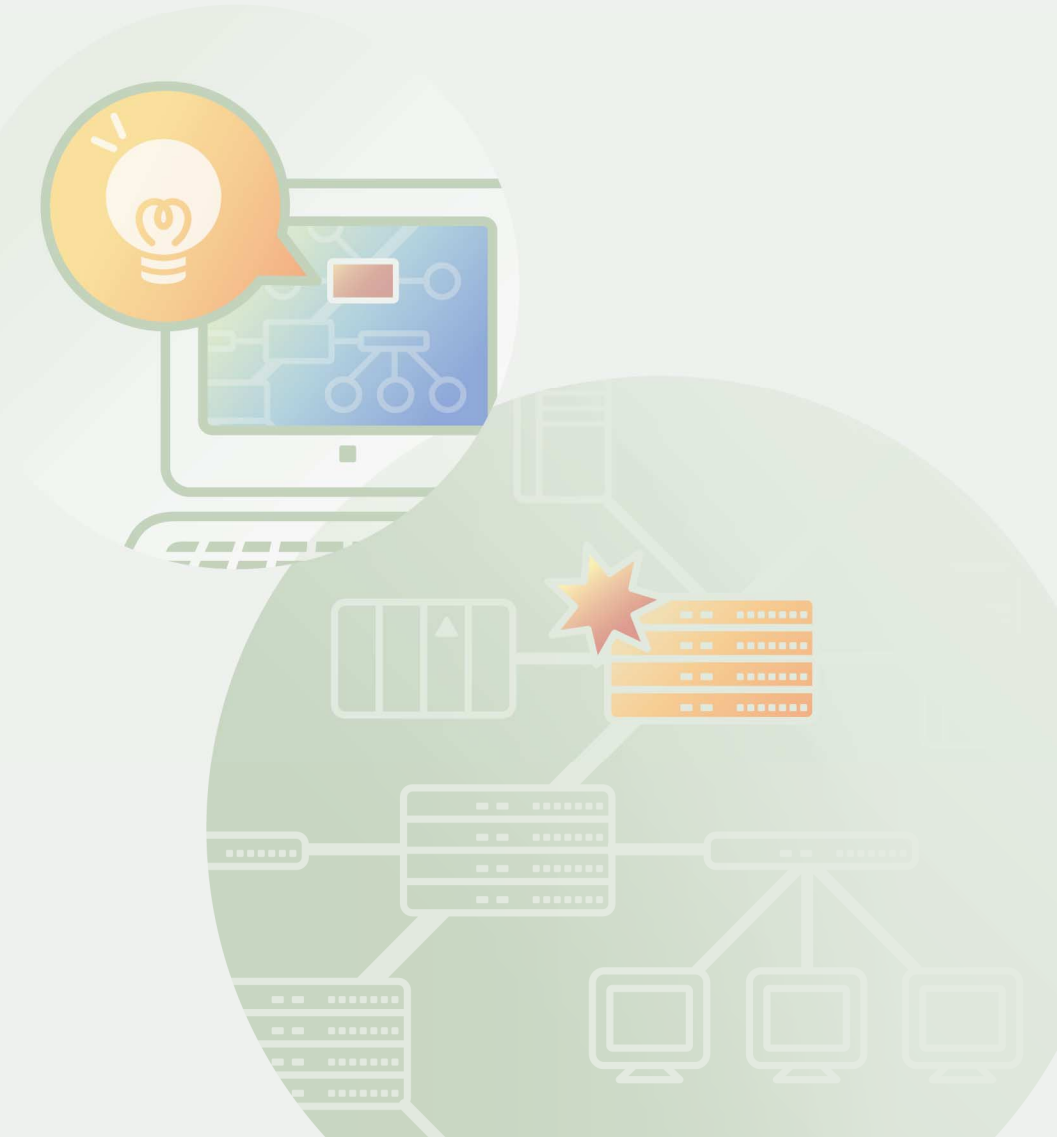
複数人で分担して管理をする場合、自分以外の運用担当者（割り当て先）を指定できるので、障害の解決作業を開始したときにGUI 上で作業を分担することができます。



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。

2章

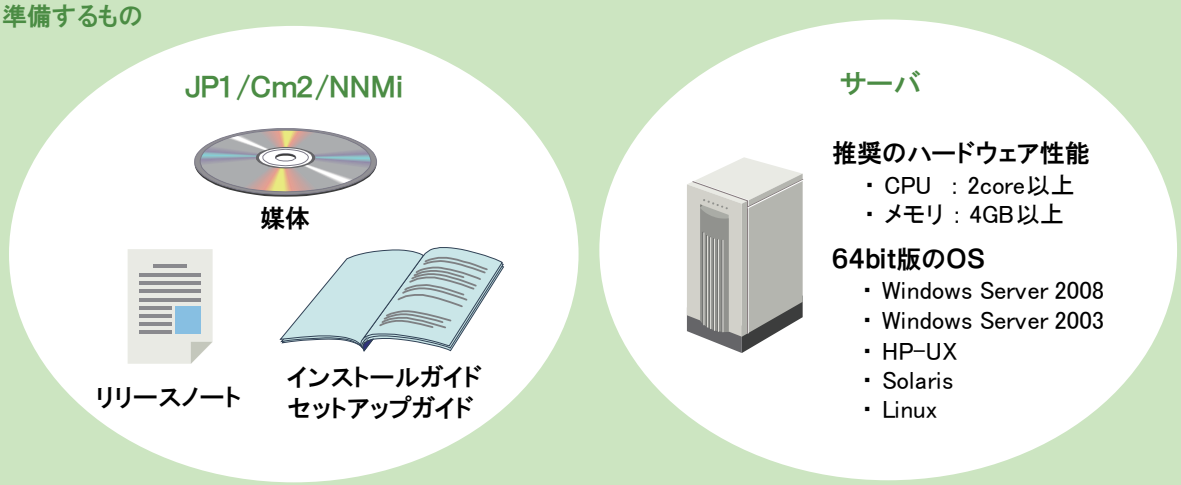
ネットワークにある ノードを把握する



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



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、サーバ環境を確認しましょう。

確認すること

●十分なハードウェア性能のサーバを用意します。2core 以上の CPU、4GB 以上のメモリを搭載してください。
●64bit 版の Windows Server 2008 など、64bit 版の OS を導入します。
●Windows の場合は次の設定をしてください。
・NNMi の SNMP 機能を使うため、SNMP トラップを無効化します。
・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作業する場合は、コンソール接続を指定します。

サーバ環境について確認することの詳細は、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。

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
インストール先ディレクトリ	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

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～

インストールのウィザードを表示させます

1 サーバにAdministrators権限でログオンし、媒体をセットします。

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

［日立統合インストーラ］ダイアログが表示されます。

ポート番号、インストール先ディレクトリを設定します

ここではデフォルトで設定します。変更するときは、ほかの値を入力してください。

3 値を入力しないで、「Enter」キーを押します。

参考 インストール先ディレクトリ（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。

```
** 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 ...
```

インストールを開始させます

4 設定した値を確認したあと「yes」を入力し、「Enter」キーを押します。

「Installing NNMi ...」と表示され、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。

参考 3 の値を修正したい場合は「no」を入力し、設定し直してください。

これでNNMiのインストールの操作は完了です。

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。

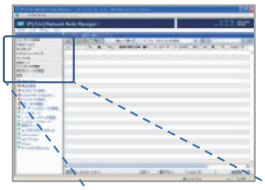
（例）

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

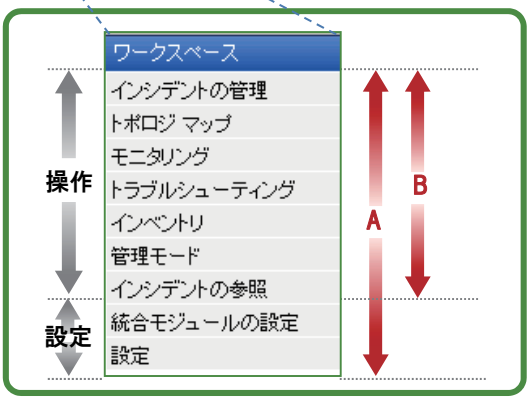
※ 初回はシステムアカウントでアクセスします。

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　【NNMi コンソールの使用】
マニュアル【セットアップガイド】-［2章 インストール前チェックリスト］

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を設定します

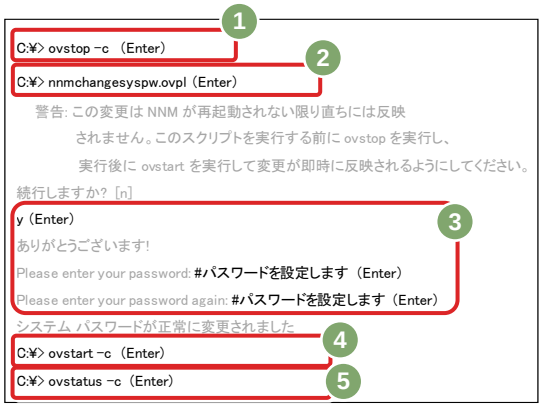
1 コマンドプロンプトで「ovstop -c」を実行します。
NNMi が停止します。

2 「nnmchangesyspw. ovpl」を実行します。

3 「y」を入力後、メッセージに従ってパスワードを設定します。
システムアカウントのパスワードは任意の文字列を指定できます。ここでは「password」（任意）を設定します。

4 「ovstart -c」を実行します。
NNMi が起動します。

5 「ovstatus -c」を実行します。
NNMi の起動状況が表示されます。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。

- Internet Explorer 8 を使用する場合は、Internet Explorer 7 との互換モードを設定します。
- 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。

6 Webブラウザから、「http://ホスト名:ポート番号/nnm/」にアクセスします。

NNMi コンソールのサインイン画面が表示されます。

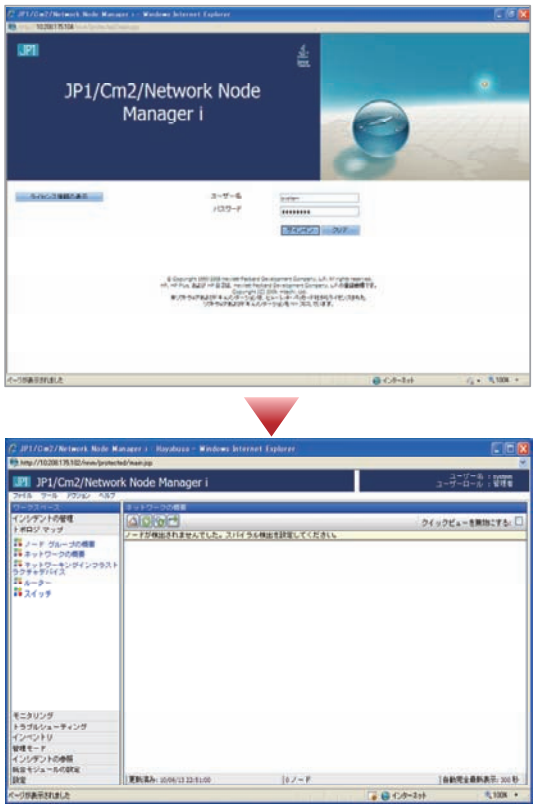
参考
ホスト名　　:ドメイン名を含んだ FQDN 名を指定します。ホスト名の代わりに IP アドレスも指定できます。
ポート番号　:インストール時に指定した番号を指定します。

注意
サインイン画面のほかにもう 1 枚画面が表示されます。閉じないで、表示させたままにしてください。

7 「ユーザー名」には「system」、「パスワード」には「password」を入力し、「サインイン」ボタンをクリックします。

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。
パスワードは 3 で設定した値を入力します。



これでWebブラウザからNNMiにアクセスする操作は完了です。

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へのアクセスを削除する］

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

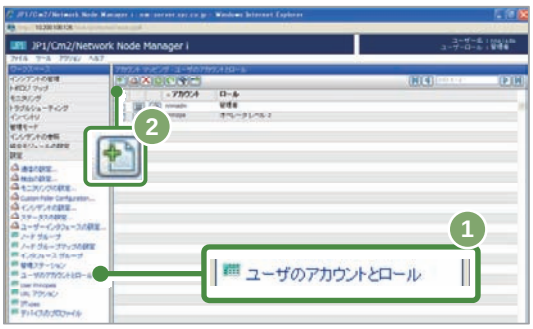
■操作手順　～ユーザーアカウントを設定する～

ユーザーアカウントのパスワードを設定できるのは、システムアカウントまたは管理者のロールを持つユーザーアカウントです。したがって、次の流れで操作します。

1. システムアカウントで、ユーザーアカウント「管理者」を設定する。
2. サインアウトする。
3. 管理者アカウントで、ユーザアーカウント「運用担当者」を設定する。

1 ワークスペースの[設定] - [ユーザのアカウントとロール]を選択します。

[アカウント マッピング - ユーザのアカウントとロール]画面が表示されます。

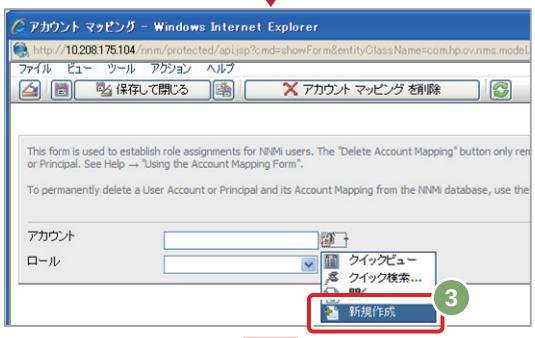


2 [ ]（新規作成）をクリックします。

[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。

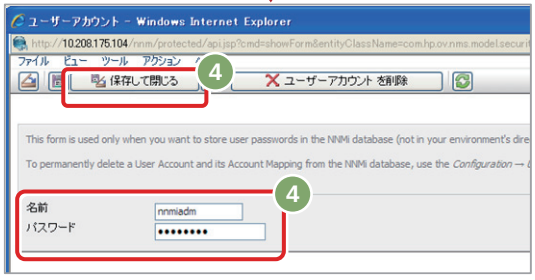
[ユーザーアカウント]画面が表示されます。



4 「名前」には「nnmiadm」を、「パスワード」は任意の値を入力し、[保存して閉じる]をクリックします。

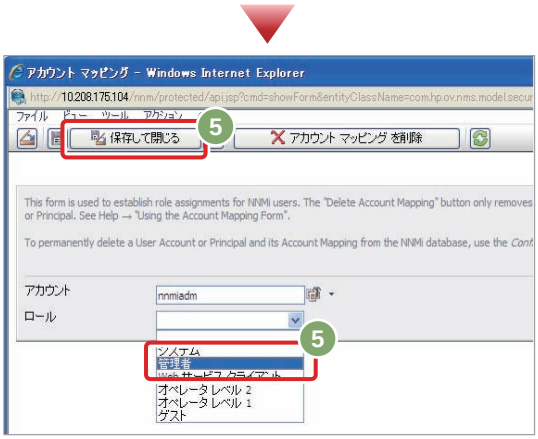
[ユーザーアカウント]画面が閉じ、ユーザー名とパスワードが設定されます。

参考　2 回目に設定するユーザーアカウント（運用担当者）の「名前」には「nnmiope」を入力してください。



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[管理者]を選択し、[保存して閉じる]をクリックします。

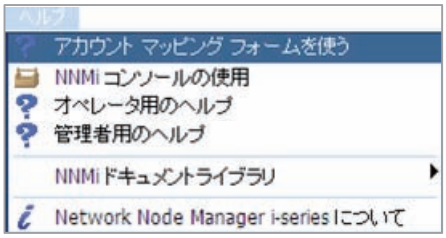
[アカウント マッピング]画面が閉じ、ユーザーアカウントが設定されます。



参考 2 回目に設定するユーザーアカウント(運用担当者)の「ロール」では[オペレータ レベル 2]を選択します。

参考 システムアカウントでユーザーアカウント「管理者」を設定したら、一度サインアウトしてください。サインアウトは、メニューから[ファイル] - [サインアウト]をクリックします。

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。



6 [アカウント マッピング - ユーザのアカウントとロール]画面で、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ます。

参考 [ ]の上にカーソルを置くと、ユーザーアカウントの設定内容が表示されます。

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

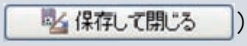
ユーザーアカウントのパスワードを忘れてしまった

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 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] - [パスワード、名前、またはロールの変更]

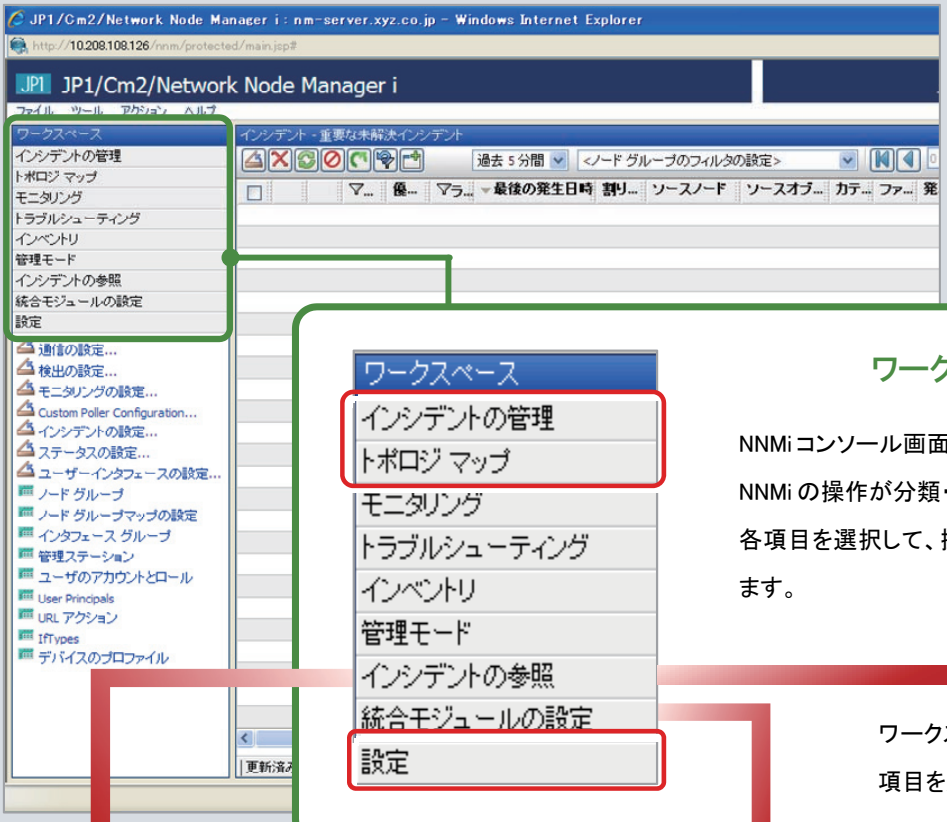
システムアカウントのパスワードを忘れてしまった

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（  、 

）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。

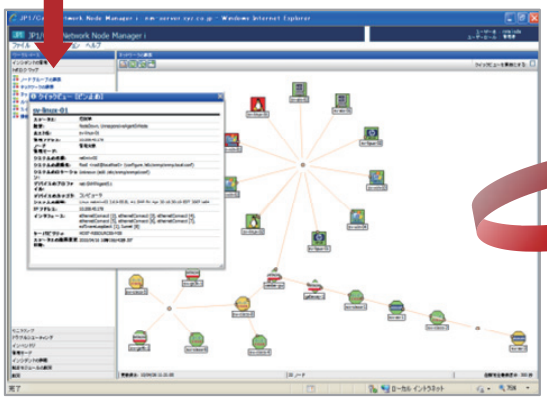


ワークスペース

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

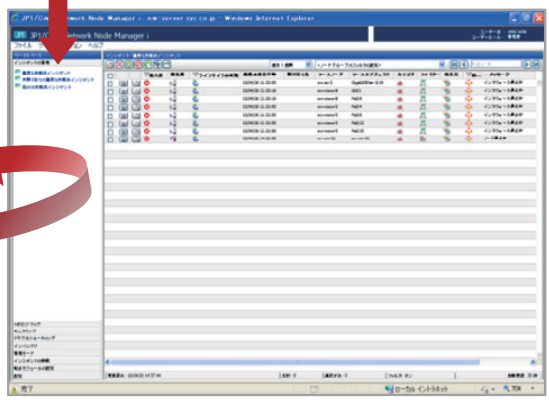
[トポロジ マップ]を選択



[ネットワークの編集]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

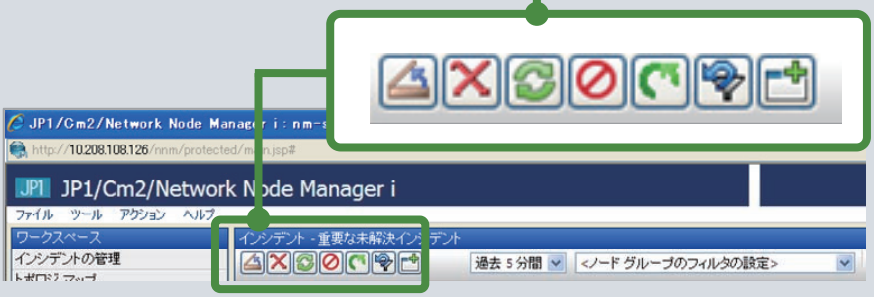
通知されたインシデントを参照し、管理することで、障害の対応状況を把握できます。

運用シーンにあわせて、画面を切り替えて使ってください。

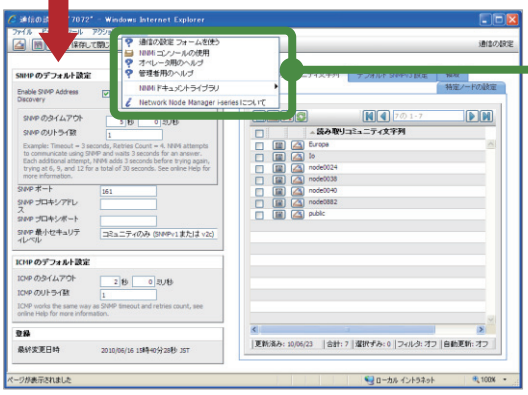
操作の基本パターン

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
2. **設定します**
   参照します
   - 設定・参照 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

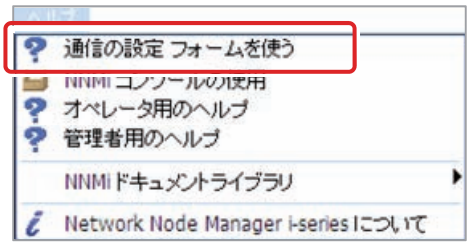
NNMi の環境設定をします。

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

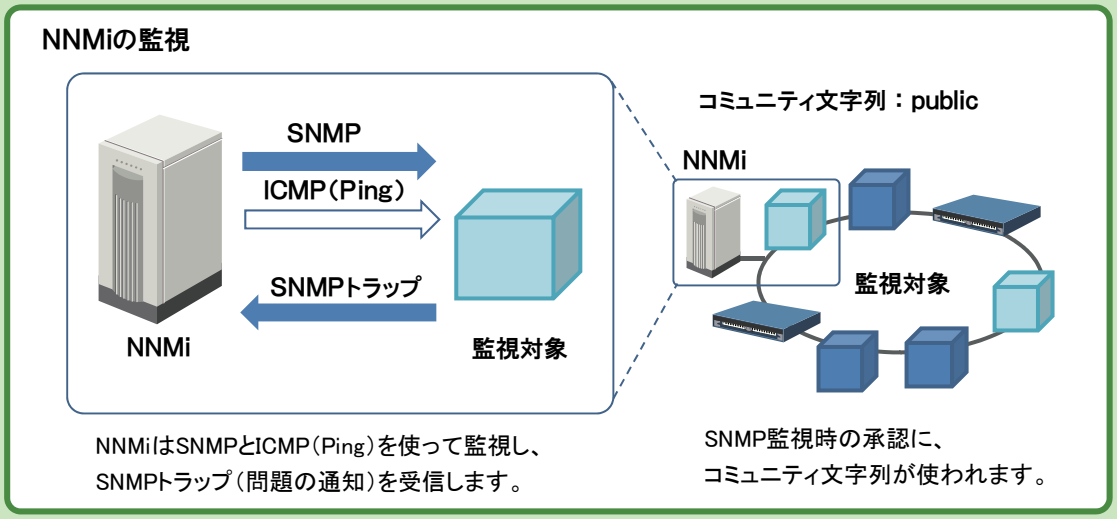
・管理者用のヘルプ



一番上には、操作中の画面に関するトピック（上の図では「通信の設定フォームを使う」）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 が監視で使う通信プロトコル「SNMP」、「ICMP（Ping）」の動作について、［通信の設定］画面で設定します。



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～

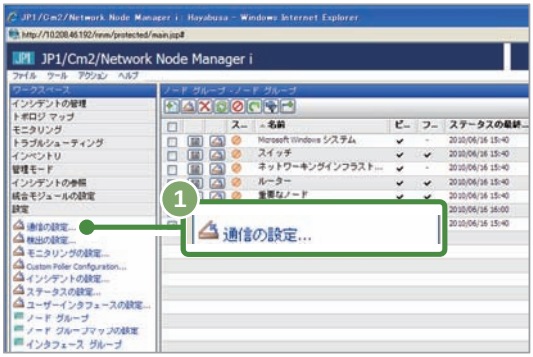
ここでの操作手順は、次の設定内容を例に説明します。

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。

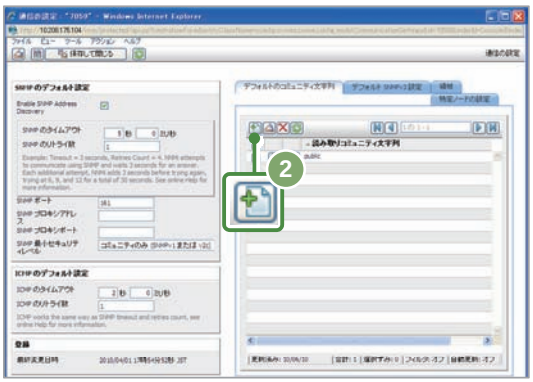
1 ワークスペースの[設定] - [通信の設定]を選択します。

[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]に「public」を入力し、[保存して閉じる]をクリックします。

「デフォルトのコミュニティ文字列」画面が閉じます。

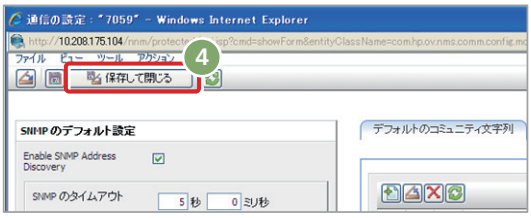
参考

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、さらに[保存して閉じる]をクリックします。

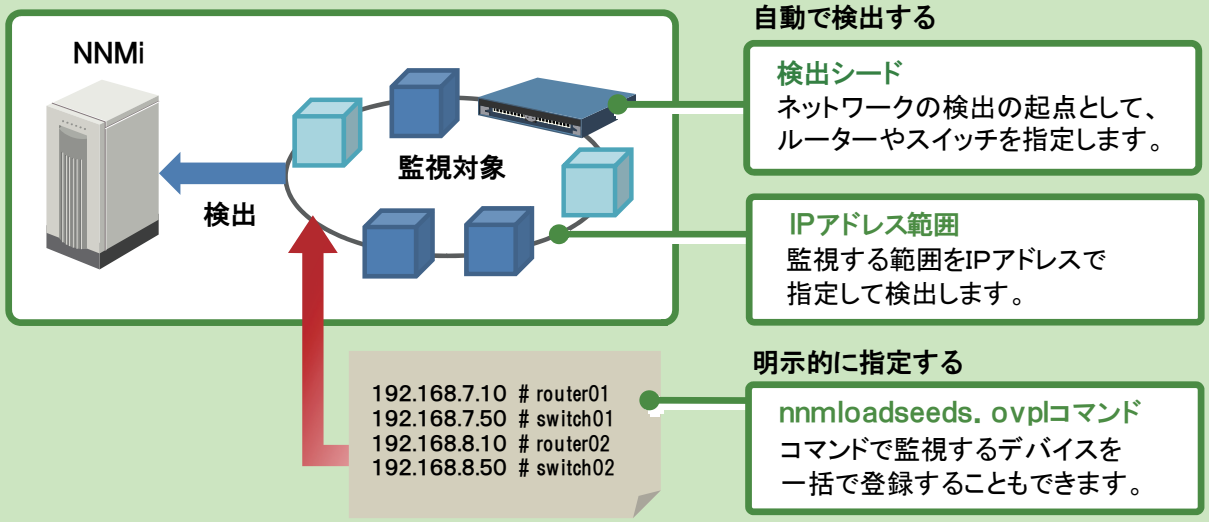
[通信の設定]画面が閉じて、設定した内容が保存されます。



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

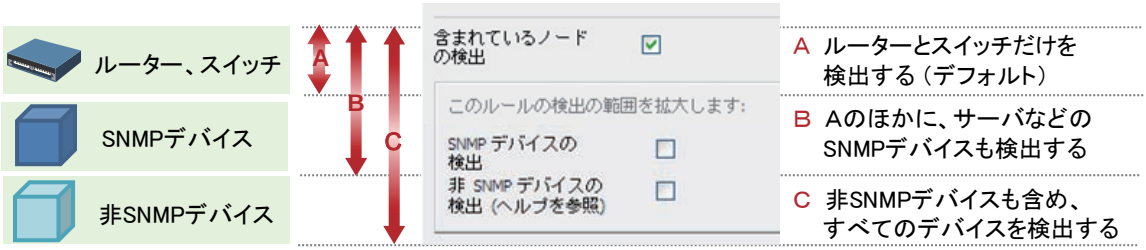
ヘルプ　【管理者用ヘルプ】-［ネットワークの検出］-［検出のアプローチを決定する］
マニュアル【セットアップガイド】-［4章 検出の計画］

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。

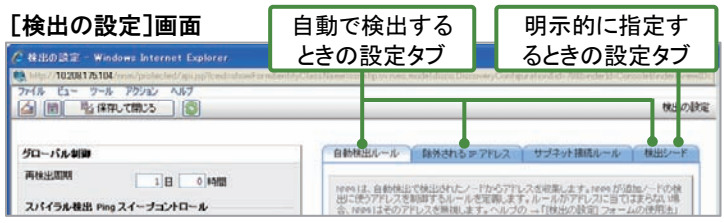
検出方法	説明	こんな運用の場合に
自動で検出する	自動検出ルールを指定することで、NNMi がデバイスを自動的に検出します。	・ネットワーク変更を自動で検出したい ・大規模ネットワークで大量のデバイスがある
明示的に指定する	(検出シードとして)特定のデバイスを明示的に指定します。	・管理対象を厳密に指定したい ・ネットワーク構成が固定的である

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。デフォルトは、ルーターとスイッチだけを検出します。

デバイスの範囲(A～C)と、[自動検出ルール]画面 - [このルールの自動検出]設定との対応



[検出の設定]画面



自動で検出する

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］

［検出の設定］画面の［自動検出ルール］、［除外される IP アドレス］、［検出シード］タブから、基本的な項目を設定します。

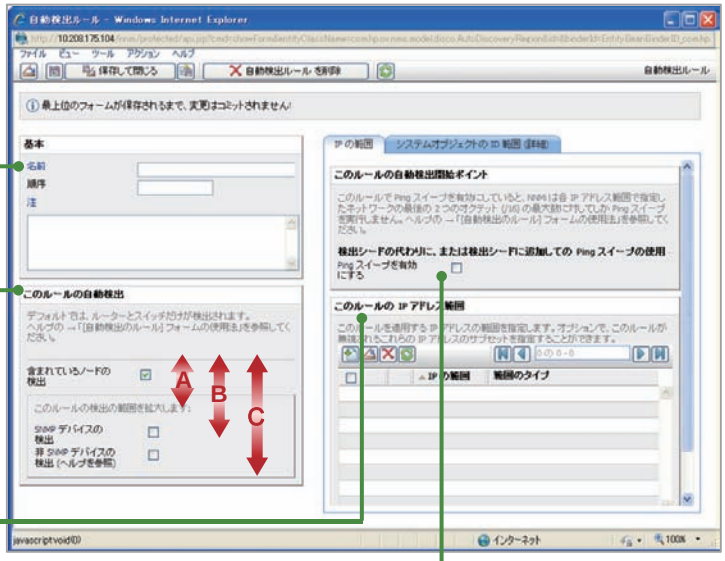
［自動検出ルール］画面

［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」、「注」を設定します。

このルールの自動検出
検出対象としたいデバイスの範囲を設定します。
含まれているノードの検出（デフォルト）
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（ヘルプを参照）
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.*.*　192.168.11.30-32

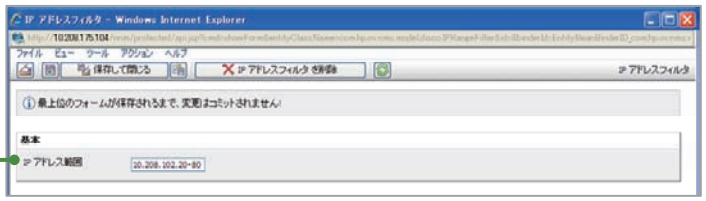


Pingスイープを有効にする
有効にすると、指定されたIPアドレスの範囲をICMP（Ping）を使って監視し、応答のあったデバイスを検出します。

［IPアドレスフィルタ］画面

［除外される IP アドレス］タブから［IP アドレスフィルタ］画面を表示させて項目を設定します。

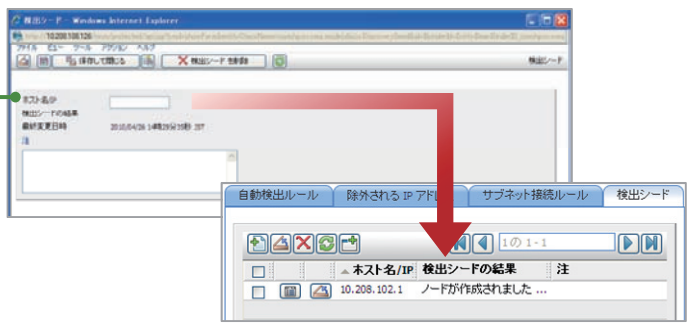
IPアドレス範囲
検出対象外にしたいデバイスがある場合は、除外したい範囲をIPアドレスで設定します。
例：10.208.10.20-80



［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FQDNホスト名で指定します。
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。

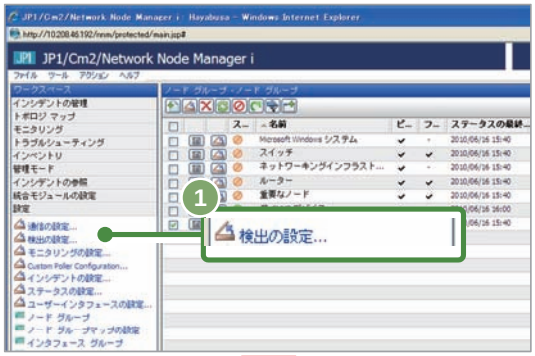


■操作手順　～自動で検出する～

検出対象のデバイスと検出範囲を設定します

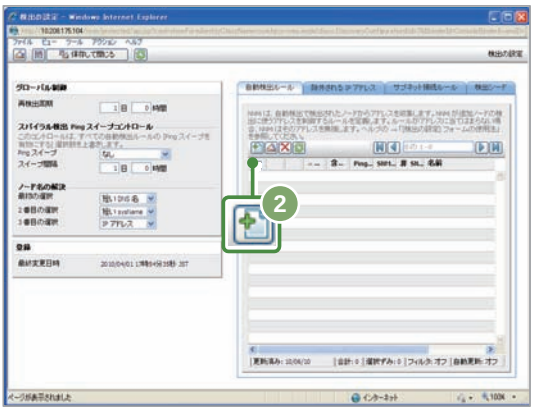
1 ワークスペースの[設定] - [検出の設定]をクリックします。

[検出の設定]画面が表示されます。



2 [自動検出ルール]タブの[ ]([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。

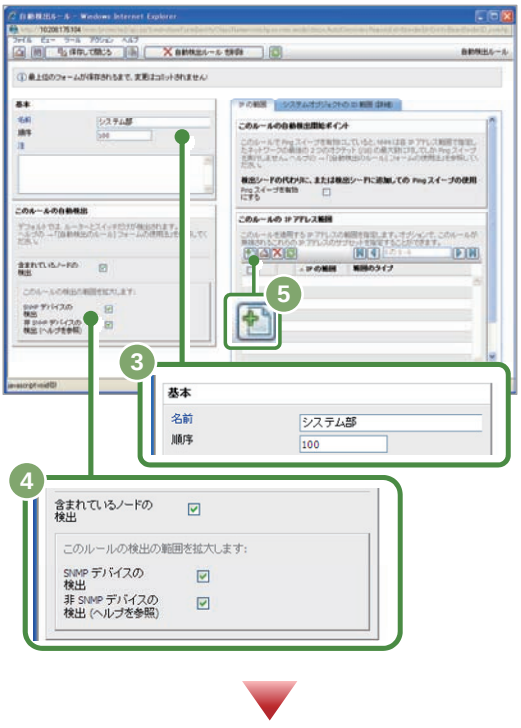


3 [名前]には「システム部」、[順序]には「100」を入力します。

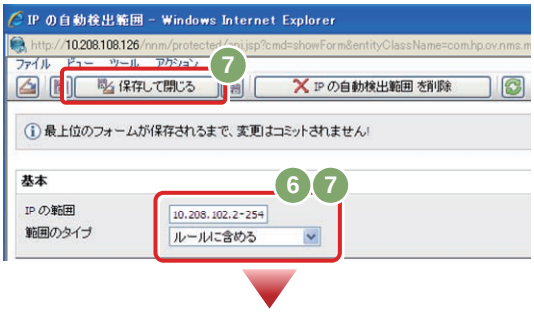
4 [含まれているノードの検出]、[SNMPデバイスの検出]、[非SNMPデバイスの検出(ヘルプを参照)]をチェックします。

5 [ ]([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]に検出したいIPアドレスの範囲を入力します。**



> **参考** 例えば、「10.208.102.2」から「10.208.102.254」の範囲で検出したい場合は、「10.208.102.2-254」と指定してください。
> 「*」(ワイルドカード)での指定もできます。「10.208.102.1」から「10.208.102.255」の範囲で検出したい場合は「10.208.102.*」と指定してください。

7 **[範囲のタイプ]のプルダウンメニューから[ルールに含める]を選択し、[保存して閉じる]をクリックします。**

[IP の自動検出範囲]画面が閉じます。

8 **[自動検出ルール]画面で、さらに[保存して閉じる]をクリックします。**

[自動検出ルール]画面が閉じて、設定した内容が保存されます。

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]タブをクリックします。**

10 **[ ](新規作成)をクリックします。**

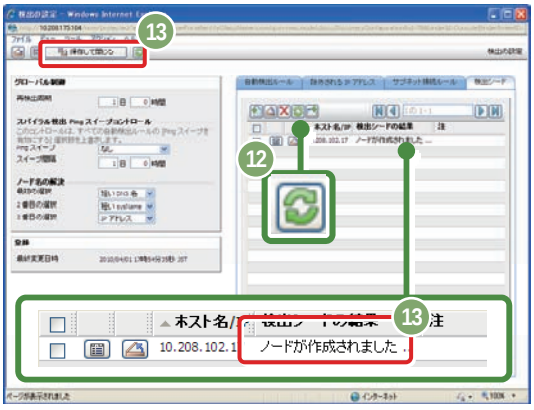
[検出シード]画面が表示されます。

11 **「ホスト名/IP」に検出シードに設定したいデバイスのIPアドレスを入力し、[保存して閉じる]をクリックします。**

[検出シード]画面が閉じます。また、検出シードの設定が保存され、検出されたデバイスの監視が開始されます。

> **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。

12 **[検出の設定]画面の[検出シード]タブの[ ](リフレッシュ)をクリックします。**



13 **11 で設定した検出シードの「検出シードの結果」に「ノードが作成されました」が表示されていることを確認したら、[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。

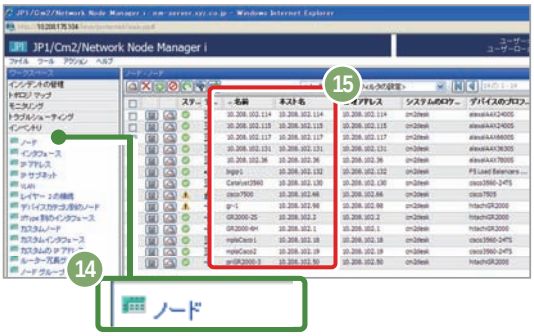
検出されたデバイスを確認します

14 ワークスペースから[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。

15 6 で設定したIPアドレスを対象として、正しくデバイスが検出、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。



これで自動で検出する操作は完了です。

監視対象を明示的に指定する

ヘルプ　【管理者用ヘルプ】-［ネットワークの検出］-［検出の設定］-［検出シードの設定］
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ときは、[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、デバイスを一括して登録することもできます。

形式

シードの一覧ファイルを指定する場合

nnmloadseeds.ovpl –f *シードファイル*

直接シードを指定する場合

nnmloadseeds.ovpl –n *シード△シード△・・・△シード*

コマンド実行例

```
nnmloadseeds.ovpl –f c:¥jp1¥seeds.txt
nnmloadseeds.ovpl –n 192.168.8.82 192.168.100.24
```

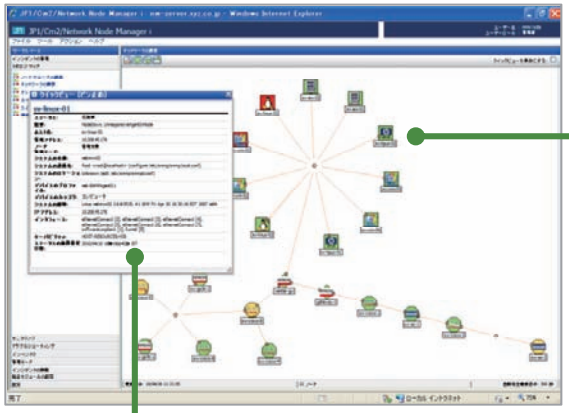
シードファイルの例

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

検出したネットワークを参照する

ヘルプ　【NNMi コンソールの使用】-［データを表示するためのレビューの使用］-［マップレビューの使用］
マニュアル【セットアップガイド】-［4.4 検出の評価］

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。

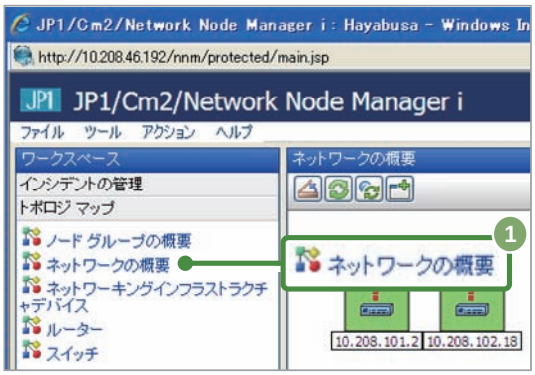
検出したノードは、アイコンの色で状態を確認できます。
アイコンの色の意味を次の表に示します。

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

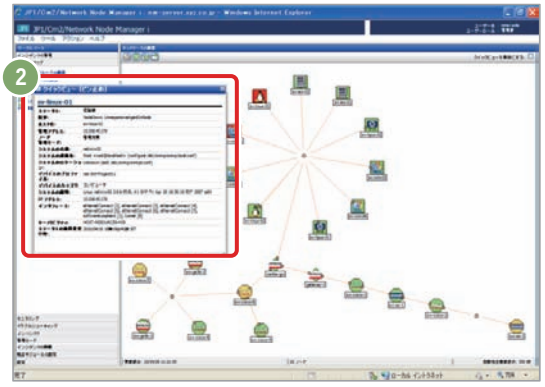
■操作手順　～検出したネットワークを参照する～

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。



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

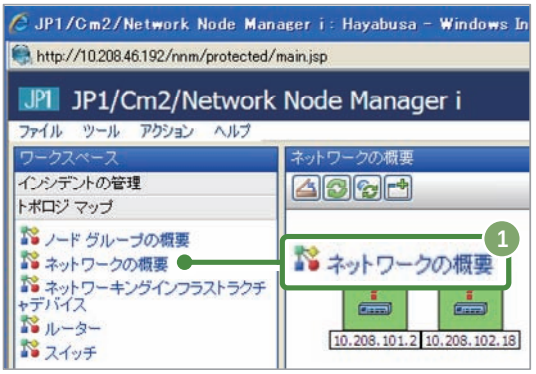
ヘルプ　【管理者用ヘルプ】-［ネットワークの検出］-［トポロジ正確に維持］-［ノードの削除］
マニュアル【セットアップガイド】-［4.4 検出の評価］

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～

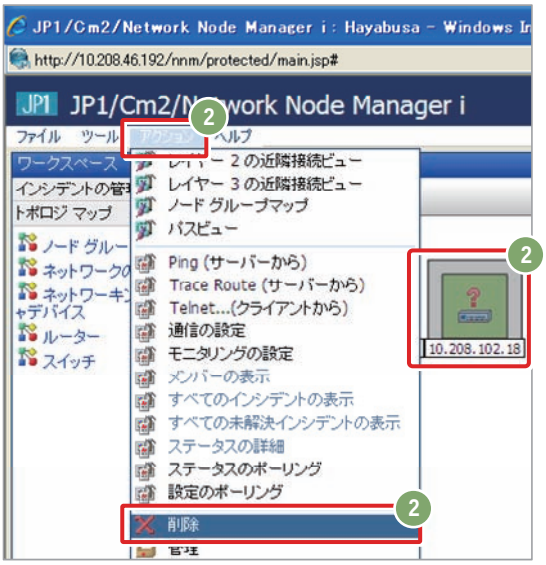
1 ワークスペースの[トポロジ　マップ] - [ネットワークの概要]をクリックします。

[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[除外される IP アドレス]タブで、検出から除外するノードを指定し、検出の対象外としてください。

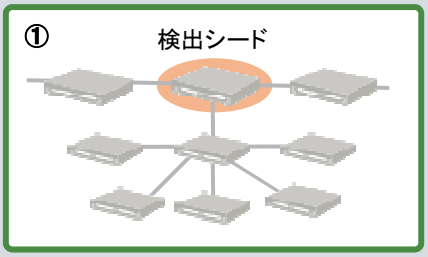
解説

「検出」 ～ネットワークを検出する～

NNMi は監視対象のデバイスを自動で検出する機能によって、ネットワーク構成を把握します。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。

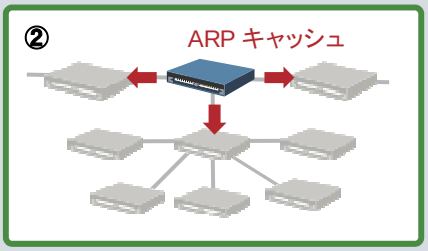
NNMiでのネットワーク構成の検出

NNMi は ARP キャッシュ情報や CDP（Cisco Discovery Protocol）などのプロトコルによって隣接デバイスの情報を収集し、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。



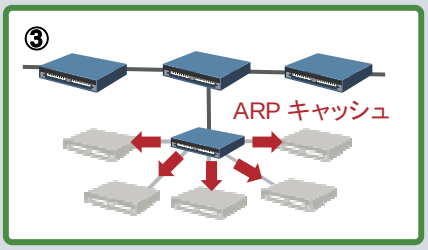
図①

「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。



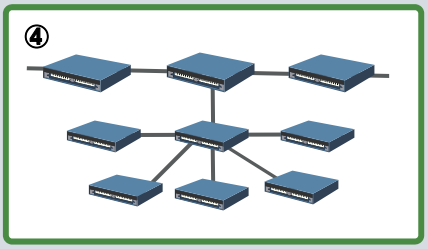
図②

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。ARP キャッシュに含まれる MAC アドレス情報は、ケーブルで接続されたノードの情報です。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。



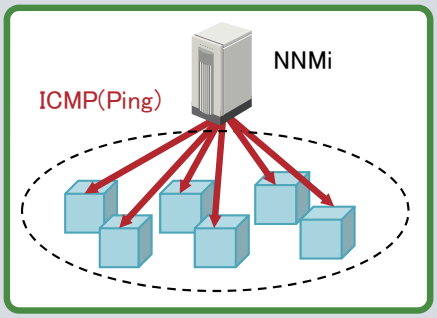
図④

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。



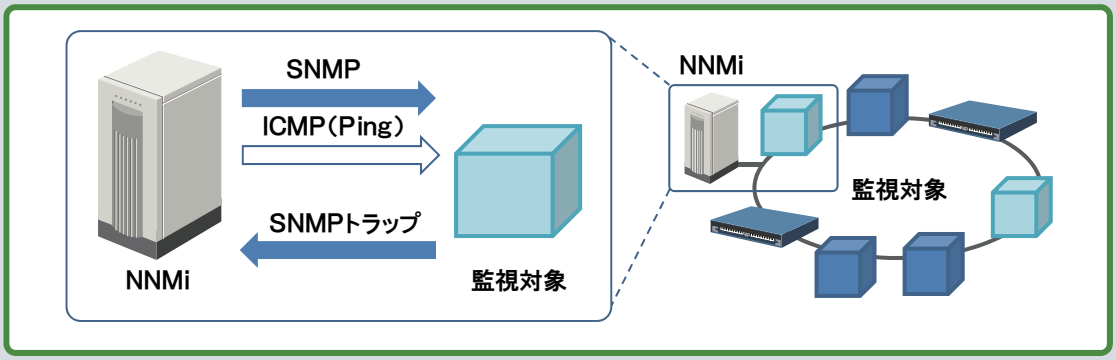
次のようなメリット、デメリットがあります。運用に応じて Ping スイープを使ってください。

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。

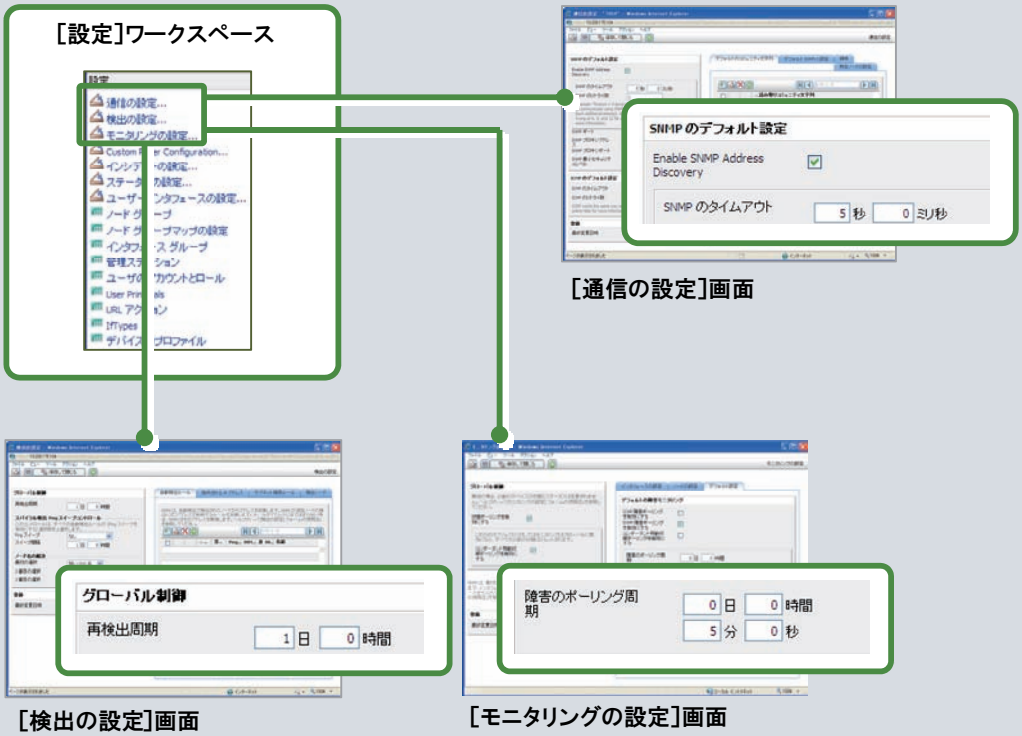
Ping スイープを使うときは、対象範囲を絞ることをお勧めします。

ネットワークの検出と監視の設定の違い

NNMi でのネットワーク管理では、SNMP と ICMP（Ping）を使ってネットワークの検出や監視を行います。これらの動作の違いについて、設定画面と対応づけて説明します。



設定画面	設定対象	設定対象	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。	SNMP ： 5 秒でタイムアウト（リトライ数は 1 回） ICMP（Ping） ： 2 秒でタイムアウト（リトライ数は 1 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	• SNMP や ICMP によってネットワーク構成を検出するときのルールを設定します。 • 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。	再検出周期 ： 1 日
モニタリングの設定	SNMP や ICMP（Ping）を使って監視するときのポーリングの動作	• SNMP や ICMP によって各ノードの状態を監視するときの設定をします。 • 各ノードの監視は、障害を迅速に検出し、監視負荷を適切におさえるため、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



[通信の設定]画面

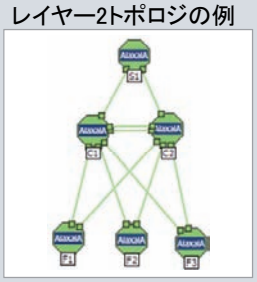
[検出の設定]画面

[モニタリングの設定]画面

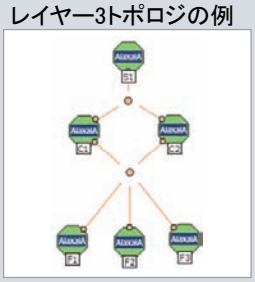
レイヤー2トポロジとレイヤー3トポロジ

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 はネットワーク構成の検出において、検出したデバイスの情報を収集します。また、ARP キャッシュや CDP プロトコルによって、隣接デバイスの情報を収集し、複数のデバイス間の接続関係を解析します。この解析結果から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

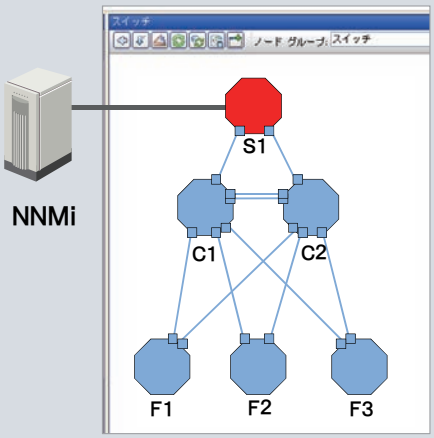
レイヤー2 トポロジ（物理的な結線）を認識すると、ネットワークでの問題の原因をより詳しく分析できます。

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。



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 【管理者用ヘルプ】-［ネットワークの検出］
マニュアル【セットアップガイド】-［4章 NNMi検出］

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。

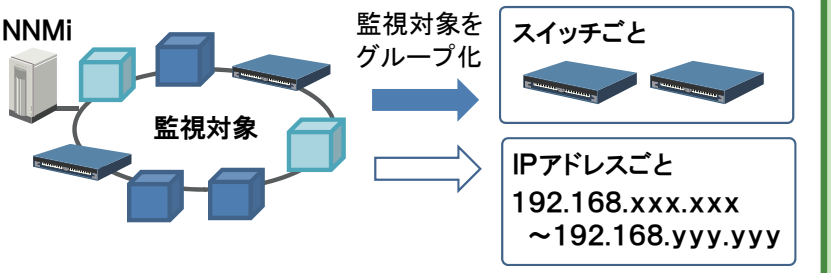
グループ化するメリット

モニタリング

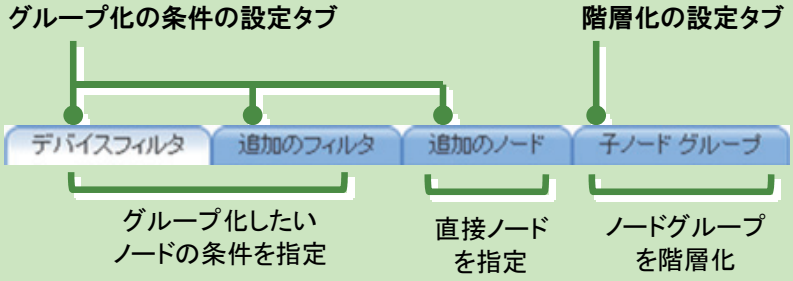
特性や運用に応じて、ノードグループ単位で適切な監視条件を設定できます。

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]画面に表示されるタブ

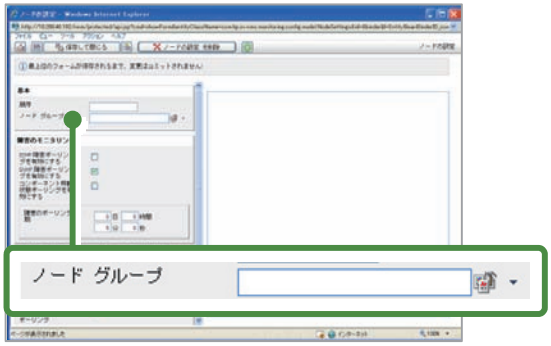


ノードグループの活用方法

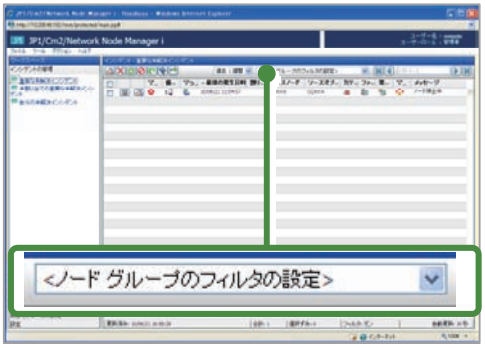
ヘルプ　【管理者用ヘルプ】-［ノードまたはインタフェースのグループ作成］

例えば、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 によって提供されたノードグループ]

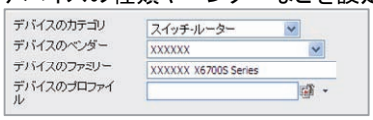
次に示す[ノード グループ – ノード グループ]画面図に表示されているノードグループが、標準で設定されています。Windows やルーターなど、基本的な種別ごとに適切な設定が用意されているため、これらのノードグループの設定を使って、すぐに NNMi の運用を始めることができます。

ノードグループを設定する

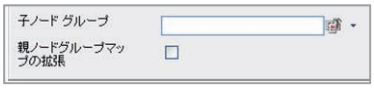
ヘルプ 【管理者用ヘルプ】- [ノードまたはインタフェースのグループ作成] - [ノードグループを定義する]

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]	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 • ルーターだけなど、表示を絞り込んで素早く状況を把握する
[追加のフィルタ]	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する 注 オペレータ(between、in、like など)を使えるため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～

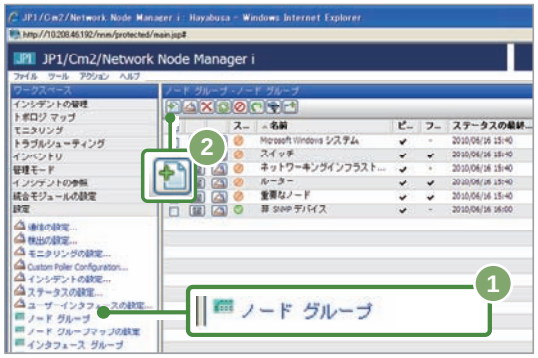
ノードグループの名前を作成します

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。

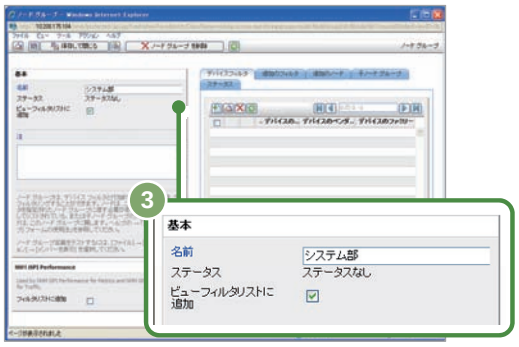
2 [ ](新規作成)をクリックします。

[ノード グループ]画面が表示されます。



3 [名前]に「システム部」を入力します。

参考 [ビューフィルタリストに追加]をチェックすると、[トポロジ マップ]ワークスペースに入力した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]タブをクリックします。

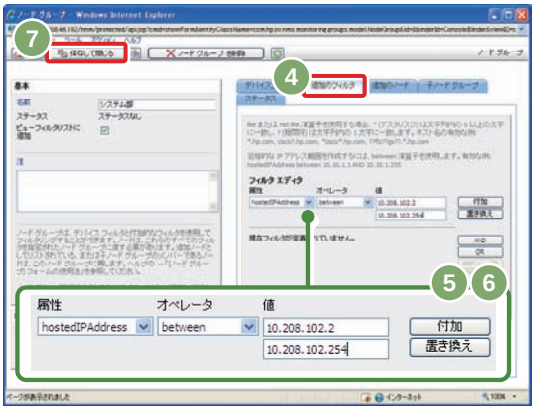
5 [属性]、[オペレータ]のプルダウンメニューから、それぞれ「hostedIPAddress」と「between」を選択します。

6 [値]にIPアドレスの範囲を入力して、[付加]をクリックします。

IP アドレスの範囲は、「2.4 ネットワークの検出」の「操作手順～自動で検出する～」で設定した値を入力してください。

7 [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。

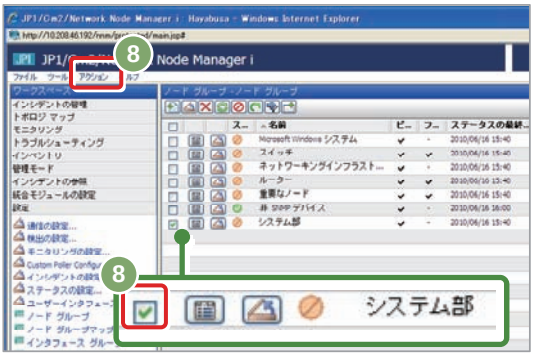


作成したノードグループを確認します

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。

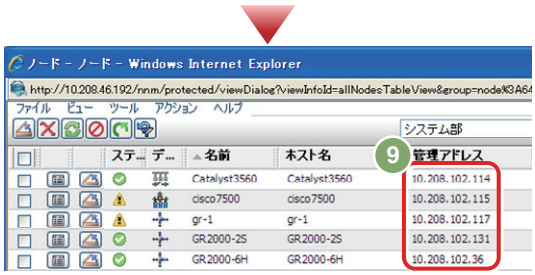
8 [ノード グループ - ノード グループ]画面で「システム部」にチェックして、[アクション] - 「メンバーの表示」をクリックします。

[ノード - ノード]画面が表示されます。



9 6 で設定したIPアドレスを対象として、ノードグループが作成されているかを確認します。

設定した IP アドレスの範囲でノードが表示されていれば、ノードグループを設定する操作は問題なく実施できています。



これでノードグループを設定する操作は完了です。

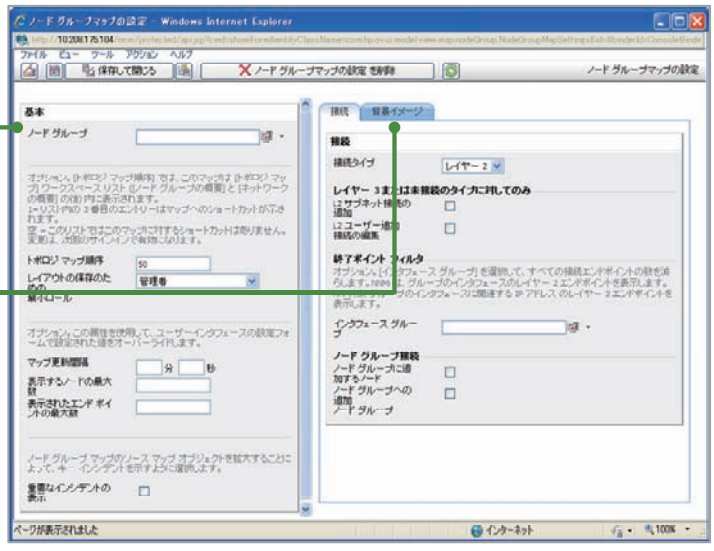
ノードグループマップを設定する

ヘルプ　【管理者用ヘルプ】-［マップの設定］-［ノードグループマップ設定を定義する］

作成したノードグループ固有のマップ（ノードグループマップ）を設定できます。
ノードグループマップは、[ノード グループマップの設定]画面で設定します。

ノードグループ
ノードグループマップを設定するノードグループを指定します。

背景イメージ
ノードグループマップの背景図を指定します。



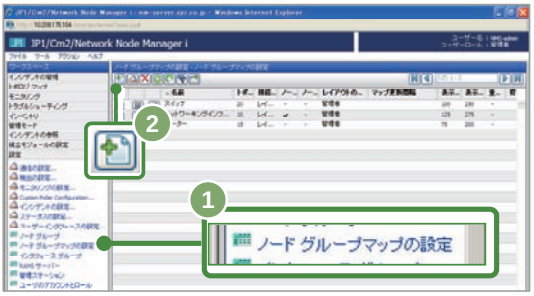
[ノード グループマップの設定]画面

■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

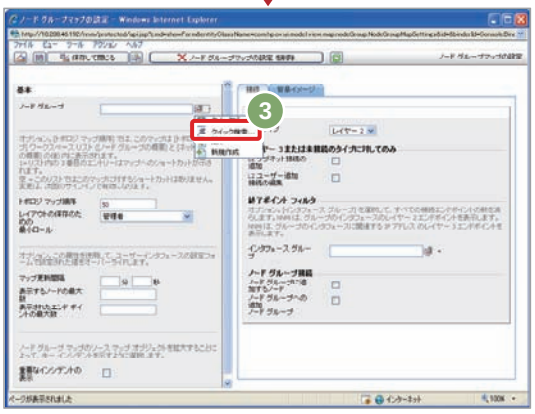
1 ワークスペースの[設定] - [ノード グループマップの設定]をクリックします。

[ノード グループマップの設定 - ノード グループマップの設定]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 グループマップの設定]画面が表示されます。



3 [ノード グループ]の[ ]から[クイック検索]をクリックします。

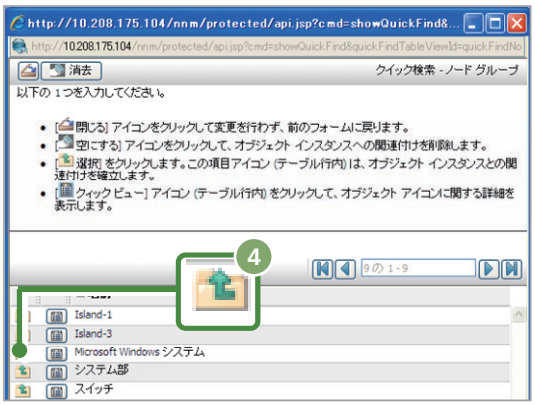
[クイック検索 - ノード グループ]画面が表示されます。

参考 [背景イメージ]タブで、ノードグループマップの背景図を設定することもできます。

4 「システム部」の[ ](この項目を選択)をクリックします。

「2.5 ノードグループの設定」の「操作手順 ～ノードグループを設定する～」で作成したノードグループを選択してください。

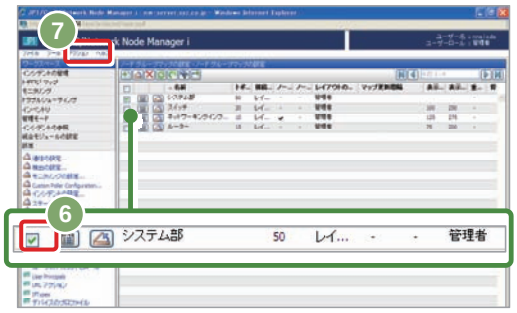
[クイック検索 - ノード グループ]画面が閉じます。



5 [ノード グループマップの設定]画面で[保存して閉じる]をクリックします。

設定したノードグループマップを確認します

6 [ノード グループマップの設定 - ノード グループマップの設定]画面で「システム部」にチェックします。

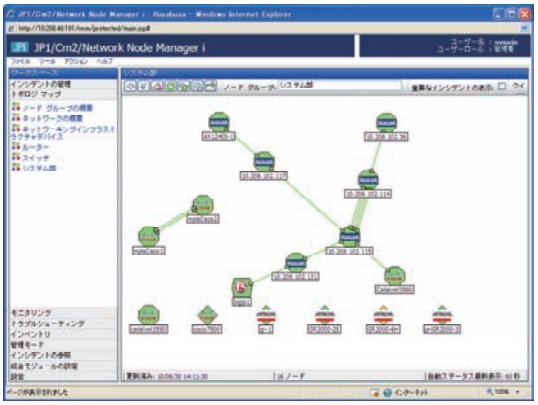


7 メニューから[アクション] - [ノード グループマップ]をクリックします。

[ノード グループマップ]画面が表示されます。

8 「システム」部のノードグループマップが表示されているかを確認します。

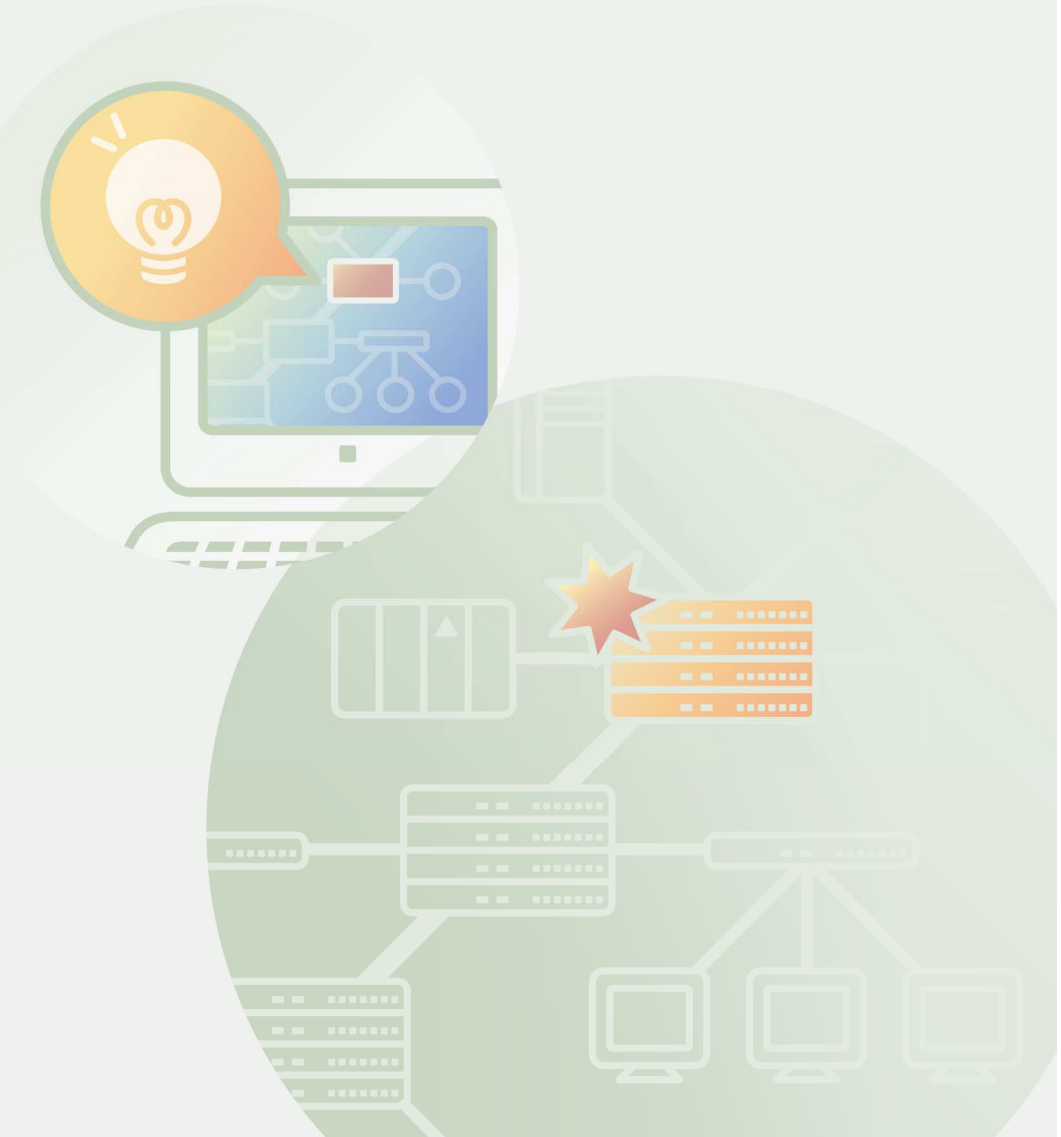
「システム部」のノードグループマップが表示されていれば、ノードグループマップの設定の操作は問題なく実施できています。



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



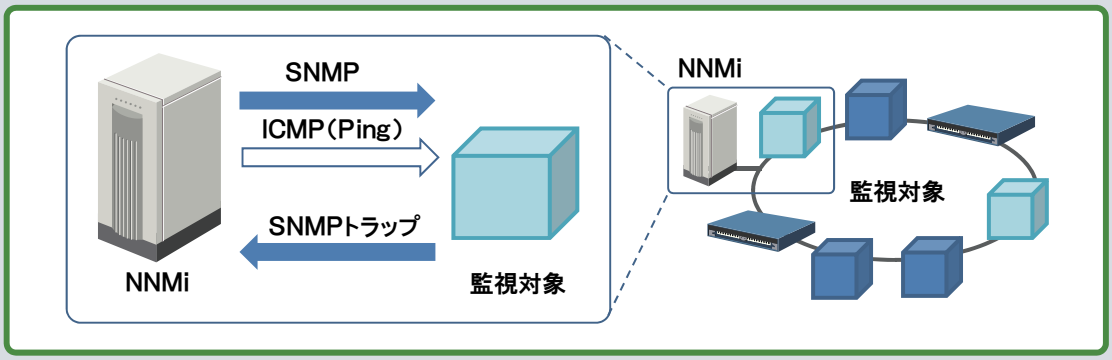
解説

「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の各ノードが正しく動作しているかを監視します。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。

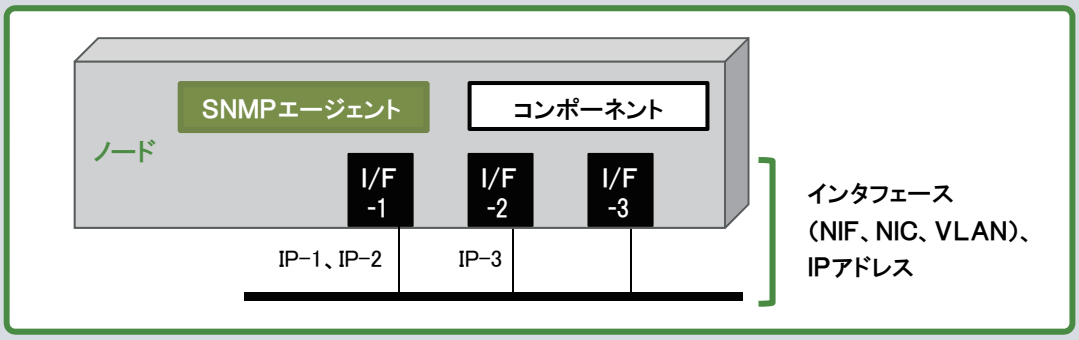
NNMiでのネットワークの監視

NNMi は、次の図のように SNMP や ICMP（Ping）を使って周期的に監視対象の稼働状態を確認し、ネットワークを監視します。この監視のことを NNMi では**モニタリング**といいます。モニタリングの監視対象は検出されたデバイス（ノードやインタフェースなど）で、デフォルトでは 5 分周期で稼働状態を確認します。

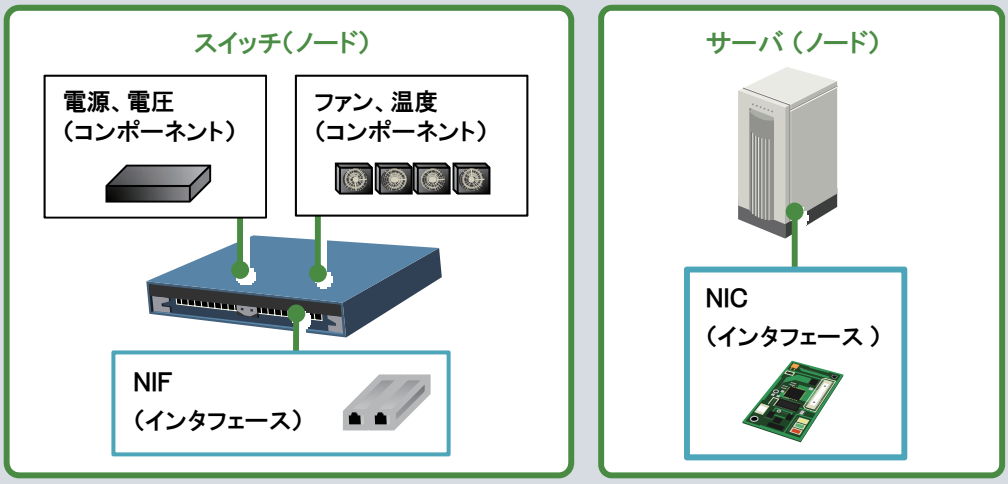


■モニタリングにおける監視対象

NNMi は監視対象のデバイスを次に示す図のような構成で認識します。



スイッチやサーバを例にすると、これらの構成は次の個所に対応しています。インタフェースは NIF や NIC などの物理的なインタフェースと、VLAN 定義のように論理的なインタフェースがあります。また、コンポーネントは、電源や温度などに相当します。



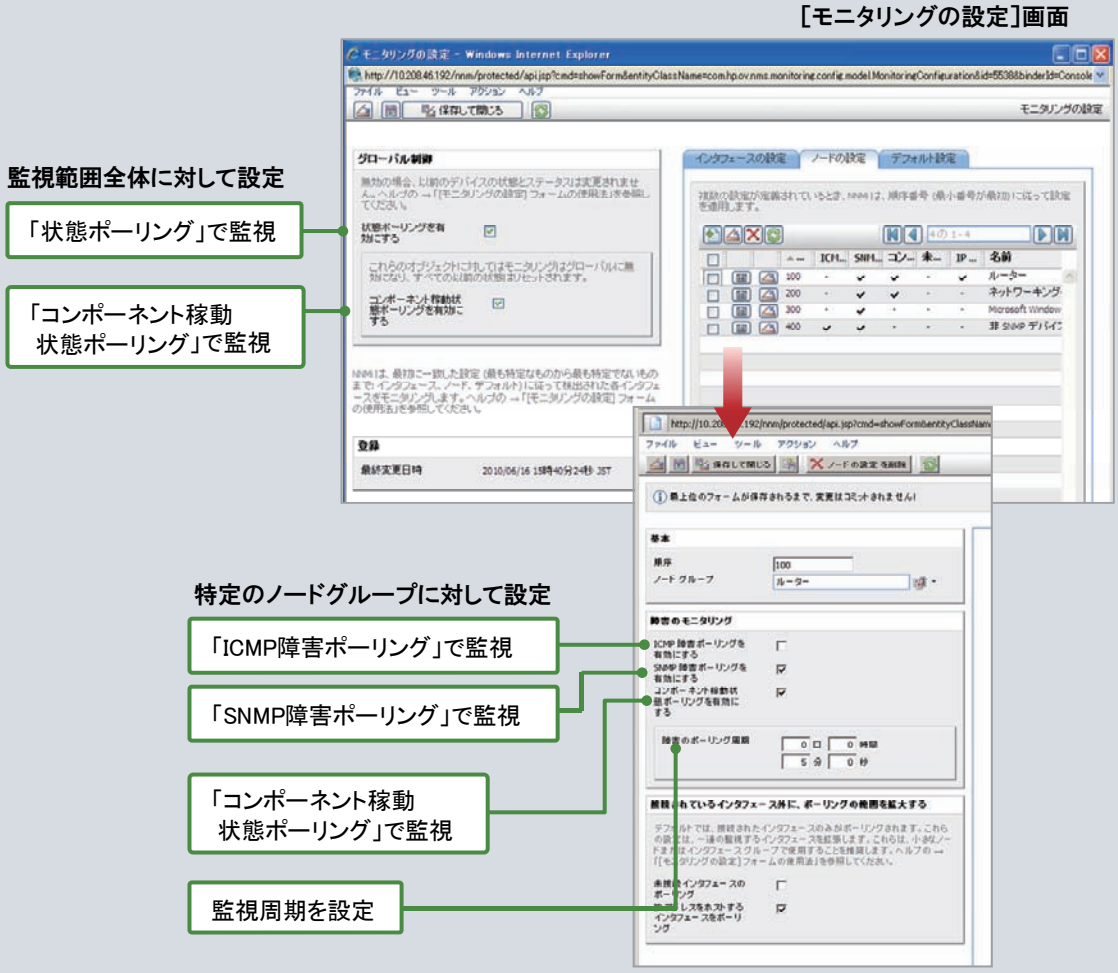
■モニタリングにおける監視方法

NNMi は、監視対象のデバイスに対してポーリングを実行して監視します。ポーリングには次の種類があります。

ポーリングの種類		意味
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します。 • SNMP エージェントは、SNMP 読み取り要求によって確認します。 • IP アドレスは ICMP 障害ポーリングで確認します。 • インタフェースは SNMP 障害ポーリングで確認します。
	ICMP 障害ポーリング	IP アドレスが、ICMP(Ping)に応答していることを確認します。
	SNMP 障害ポーリング	インタフェースの状態を、SNMP 読み取り要求によって確認します。
コンポーネント稼動状態ポーリング		コンポーネント（電源、電圧、ファン、温度）の状態を SNMP で監視します。 ただし、NNMi がサポートする特定機種だけ監視可能です。

これらの監視方法は、次に示す[モニタリングの設定]画面で設定します。
複数の範囲に対し、それぞれ異なる監視方法を設定できるため、監視対象の特性に応じて適切な監視方法を組み合わせて定義してください。

[モニタリングの設定]画面



モニタリングの設定

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してから設定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。

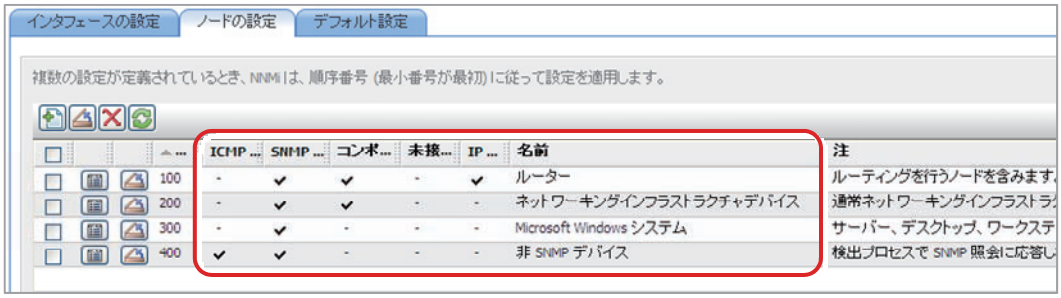
■デフォルトのモニタリング定義

デフォルトでは、次に示すモニタリング定義が提供されています。

[モニタリングの設定]画面

[インタフェースの設定]タブ

[ノードの設定]タブ



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。

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。

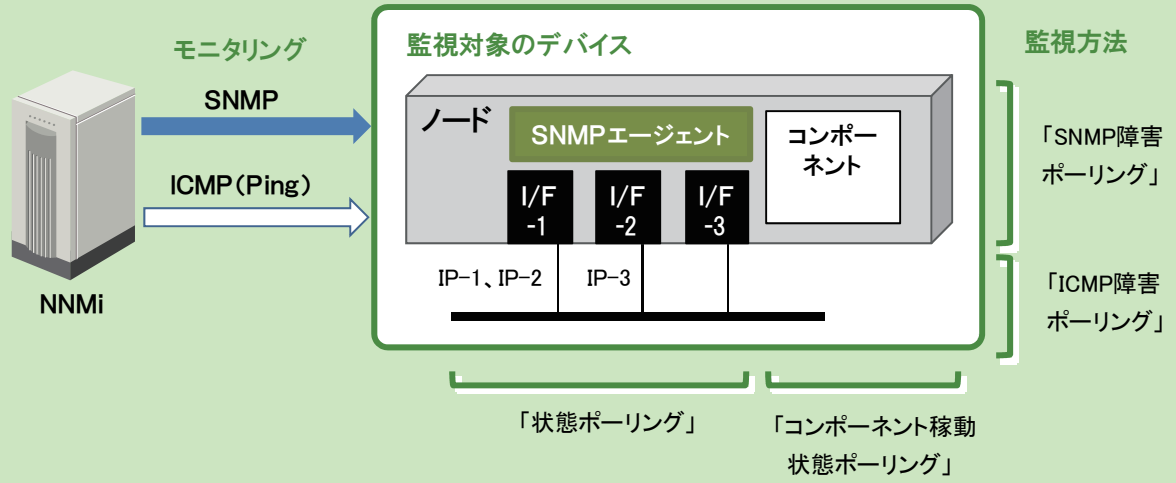
非SNMPデバイス

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】-［ネットワークの稼動状態のモニタリング］
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。



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】-［ネットワークの稼動状態のモニタリング］-［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］

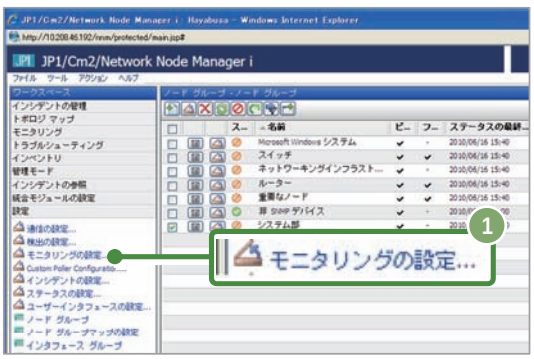
NNMi では、すぐに監視を始められるように、モニタリング定義が標準で設定されています。
このため、モニタリング方法やポーリング周期をカスタマイズしなければ、特に設定を変更する必要はありません。
ただし、監視の仕組みを理解することはネットワーク監視において大変重要です。したがって、標準のモニタリング定義を参照し、監視方法を確認してみましょう。

■操作手順　～標準のモニタリング定義を参照する～

ここでは、標準で提供されているモニタリング定義のうち、「ルーター」のモニタリング定義を参照する手順について説明します。

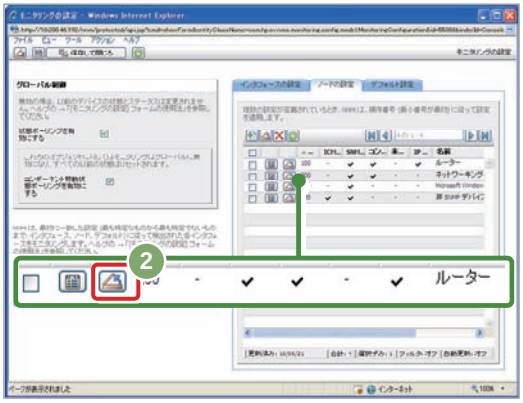
1 ワークスペースから[設定] - [モニタリングの設定]を選択します。

[モニタリングの設定]画面が表示されます。

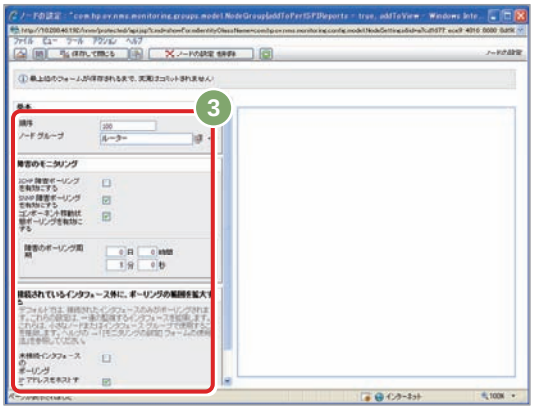


2 **[ノードの設定]タブで「ルーター」のモニタリング定義の [ ]（開く）をクリックします。**

[ノードの設定]画面が表示されます。



3 **「ルーター」のモニタリング定義で監視方法の設定項目を確認します。**



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

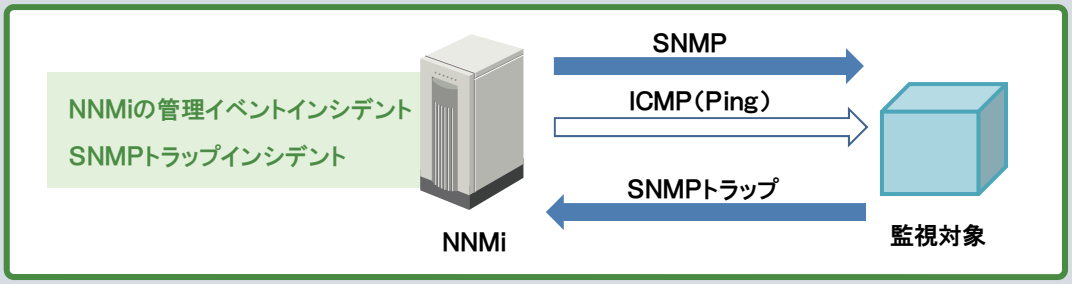
「インシデント」 ～重要な事象に絞って通知する～

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
NNMi の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、NNMi 管理イベントや SNMP トラップをあわせて、標準で約 120 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。

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。

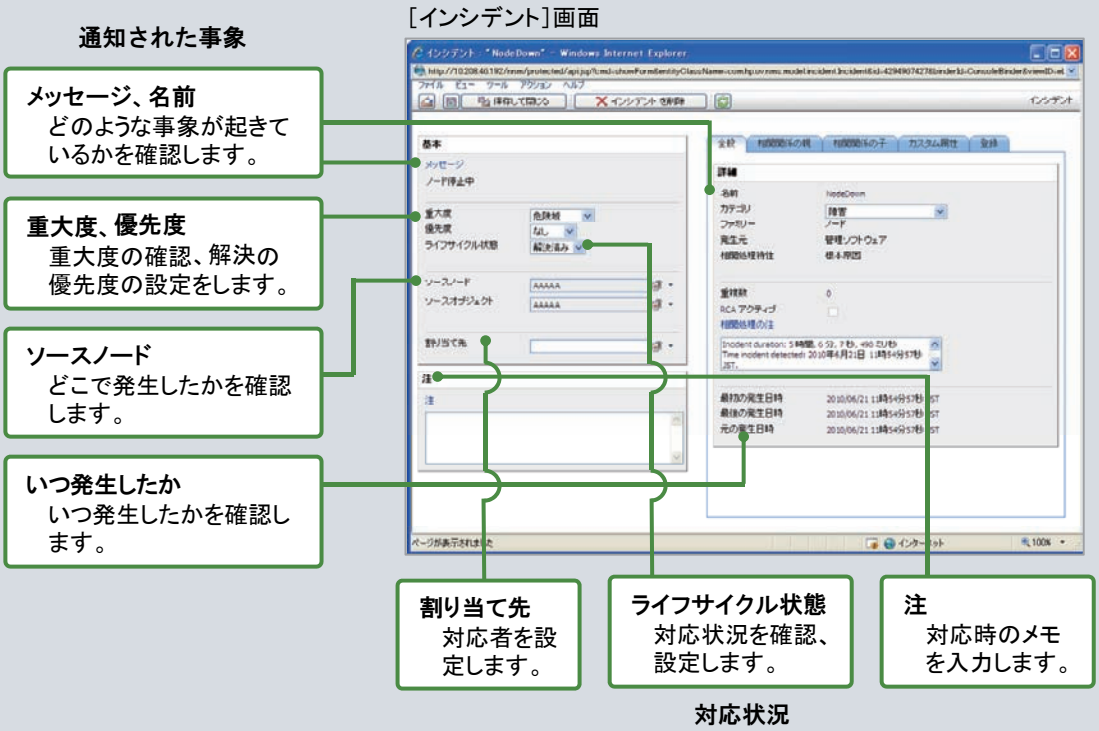
- NodeDown（ノード停止中）
- NodeOrConnectionDown（ノードまたは接続が停止中）
- NonSNMPNodeUnresponsive（非 SNMP ノードが応答なし）

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もとづいて、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]画面の
[管理イベントの設定]タブ

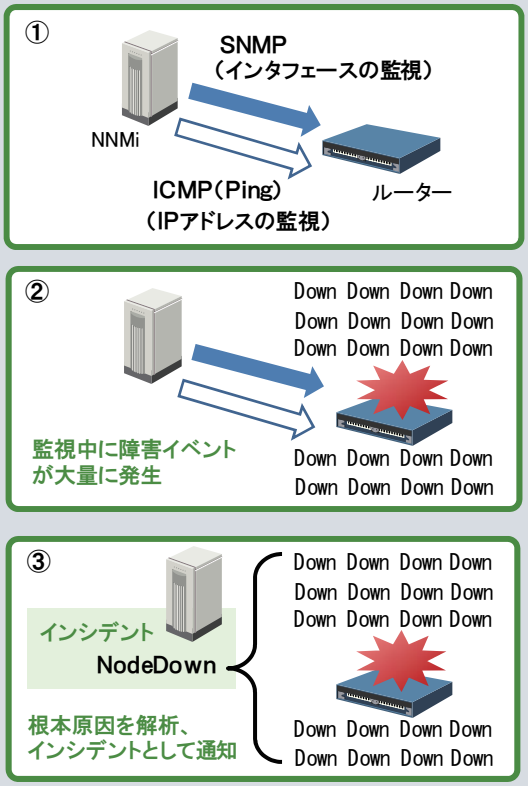
インシデントの内容

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

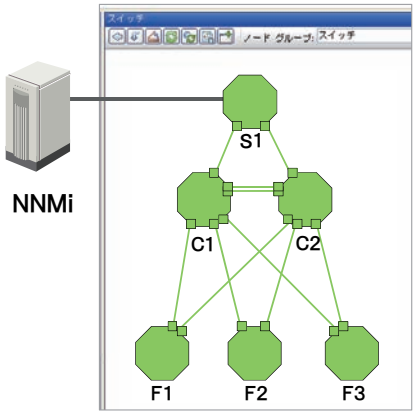
この状況を NNMi の根本原因解析機能は次のように判断します。

- 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。

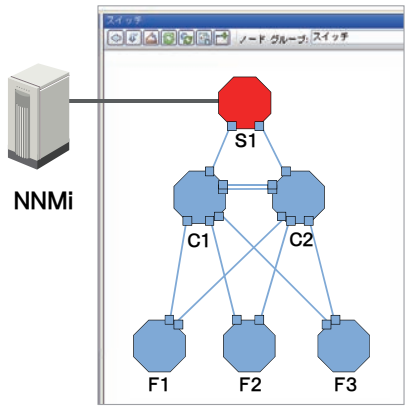
NNMi の根本原因解析機能はネットワークを構成する複数のノードでも、レイヤー2 トポロジの情報を有効に活用することで発生している事象を解析し、根本原因のインシデントを通知します。ここでは、次のネットワーク構成を例として、根本原因解析の動きを説明します。

■通常時



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

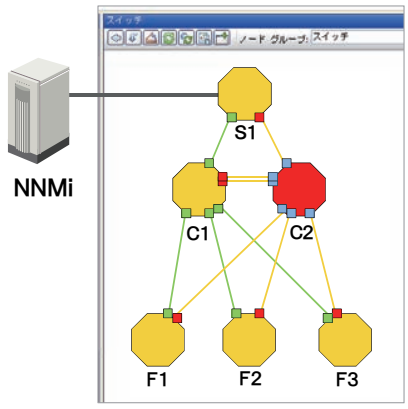


最上位スイッチの障害

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。

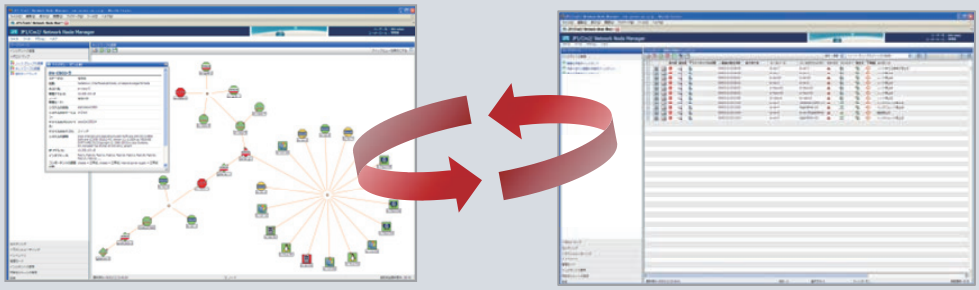
根本原因解析機能は、ほかにも多くの事象と根本原因の対応を解析できます。
詳細は、セットアップガイド「付録B　Causal Engine と NNMi インシデント」を参照してください。

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。

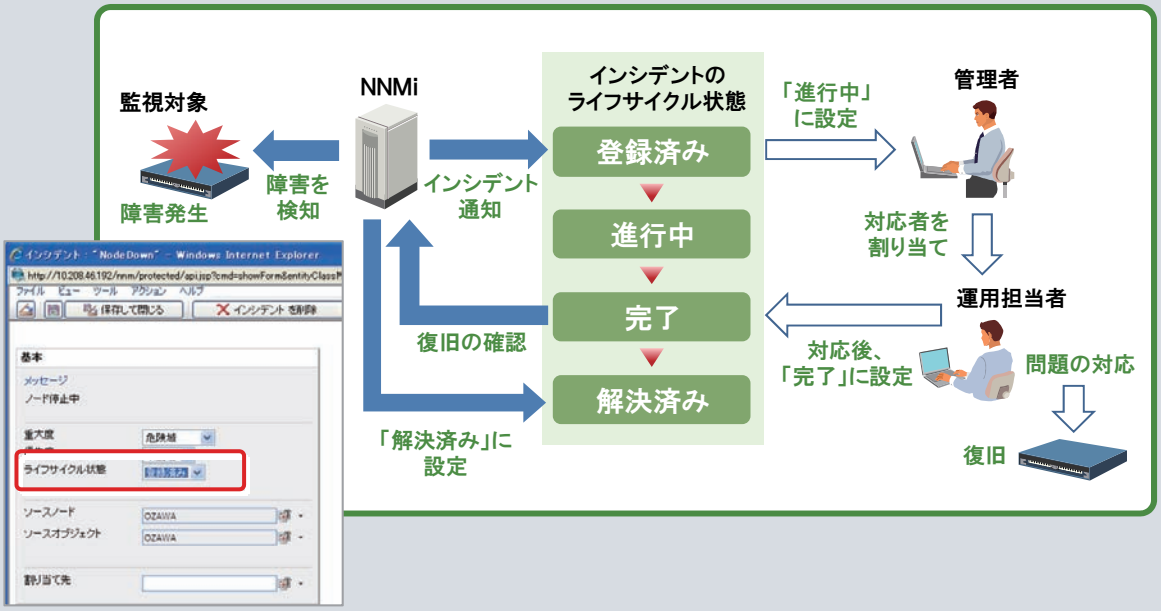


■インシデントでのライフサイクル管理

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

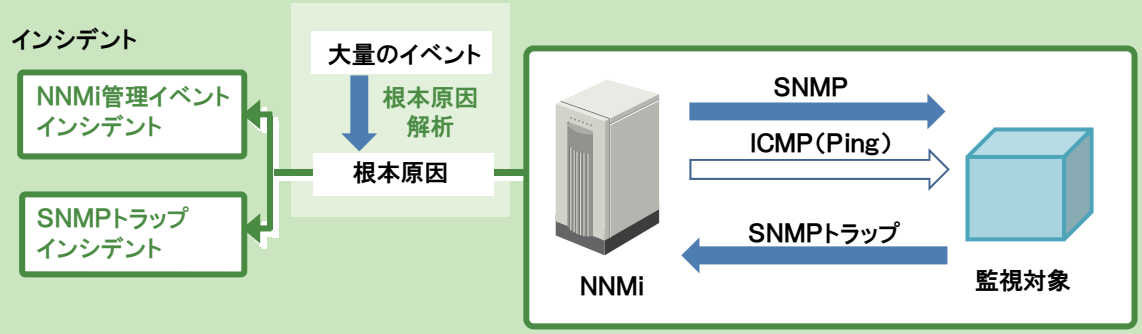
インシデントのライフサイクル状態にあわせて、自動的にアクションが実行されるように設定できます。

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。
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、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。

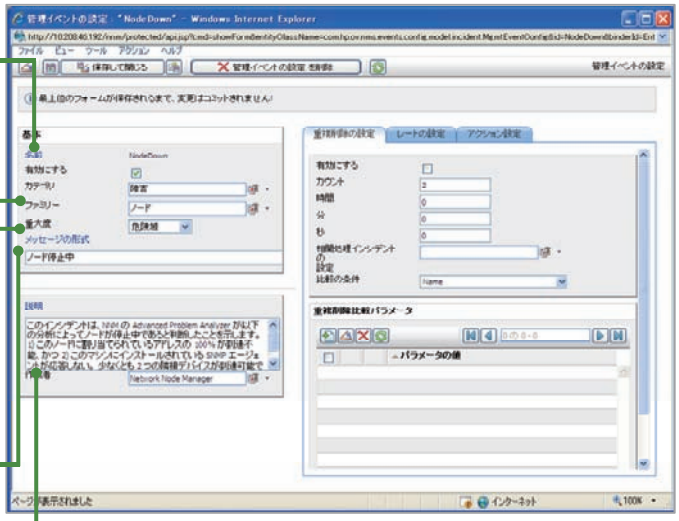


標準のインシデント定義を参照する

ヘルプ　【管理者用ヘルプ】-［インシデントを設定する］-［NNMi が提供するインシデント設定］

[インシデントの設定]画面や[管理イベントの設定]画面では、各インシデントの内容を確認できます。
標準で提供されているインシデント定義について、次の基本的な項目を参照してみましょう。

［インシデントの設定］画面



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。

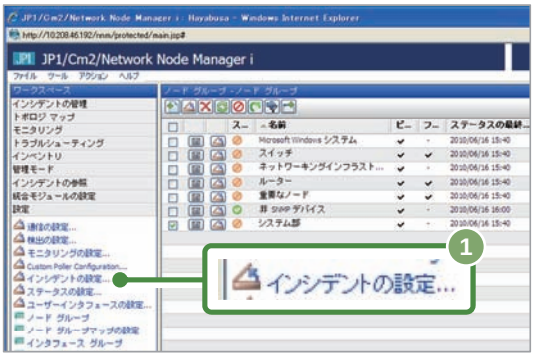
［管理イベントの設定］画面

■操作手順 ～標準のインシデント定義を参照する～

ここでは、標準で提供されているインシデント定義のうち、「NodeDown」インシデントを参照する手順について説明します。

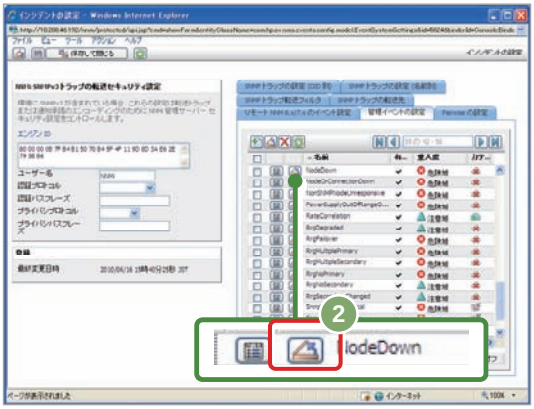
1 ワークスペースから[設定] - [インシデントの設定]を選択します。

[インシデントの設定]画面が表示されます。

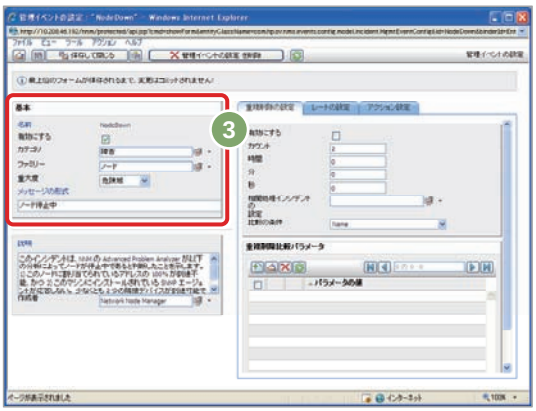


2 [管理イベントの設定]タブにある[NodeDown]の[ ]（開く）をクリックします。

「NodeDown」インシデントの[管理イベントの設定]画面が表示されます。



3 「NodeDown」インシデントで設定されている項目を確認します。



これで標準のインシデント定義を参照する操作は完了です。

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、ベンダー固有の MIB をもとにして 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。

■操作手順　～SNMPトラップのインシデントを設定する～

1 「nnmloadmib. ovpl」を実行し、MIBをロードします。

NNMi のデータベースに MIB が登録されます。

なお、各ベンダーで提供されている MIB については、各ベンダーのマニュアルを参照してください。

2 「nnmincidentcfg. ovpl」を実行します。

SNMP トラップのインシデント定義が NNMi に登録されます。

```
1
nnmloadmib.ovpl  -load <mib_file>  -u <user> -p <password>
2
nnmincidentcfg.ovpl -loadTraps  <mib_file>  -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定義を参照する～」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。

参考　ロードした SNMP トラップ定義をカスタマイズすることもできます。

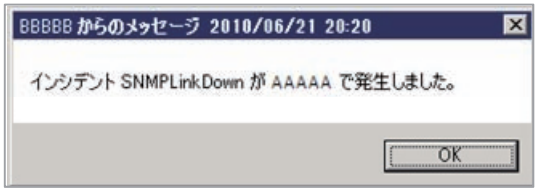
これでSNMPトラップのインシデントを設定する操作は完了です。

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、コマンドを実行させることができます。

例えば、msg コマンドを自動アクションとして設定すると、インシデントが登録されたタイミングで msg コマンドのメッセージ（右図）を表示させることができます。

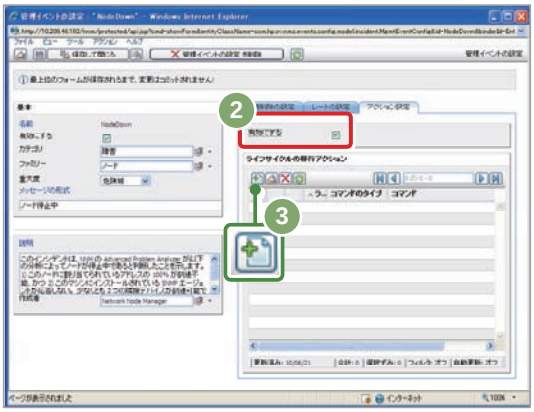


■操作手順 ～インシデントに自動アクションを設定する～

ここでは、自動アクションとして msg コマンドを設定し、PC のデスクトップ上にメッセージを表示させる手順について説明します。

1 自動アクションを設定したいインシデント定義を選択し、[管理イベントの設定]画面を表示します。

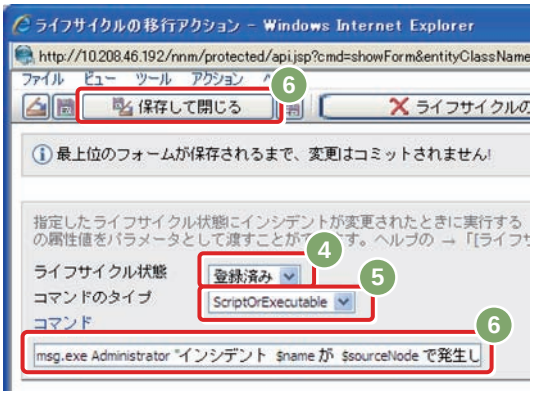
[管理イベントの設定]画面の表示方法は、「3.2 インシデントの設定」の「操作手順 ～標準のインシデント定義を参照する～」を参照してください。



2 [アクション設定]タブで[有効にする]にチェックします。

3 [ ](新規作成)をクリックします。

[ライフサイクルの移行アクション]画面が表示されます。



4 [ライフサイクル状態]のプルダウンメニューから[登録済み]を選択します。

5 [コマンドのタイプ]のプルダウンメニューから[ScriptOrExecutable]を選択します。

6 [コマンド]に表示させたいメッセージ(msg コマンド)を設定して、[保存して閉じる]をクリックします。

[ライフサイクル移行アクション]画面が閉じます。

参考

この手順では msg コマンドを使って、次の記述を[コマンド]に設定しています。

「msg.exe Administrator "インシデント $name が $sourceNodeName で発生しました。"」

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。

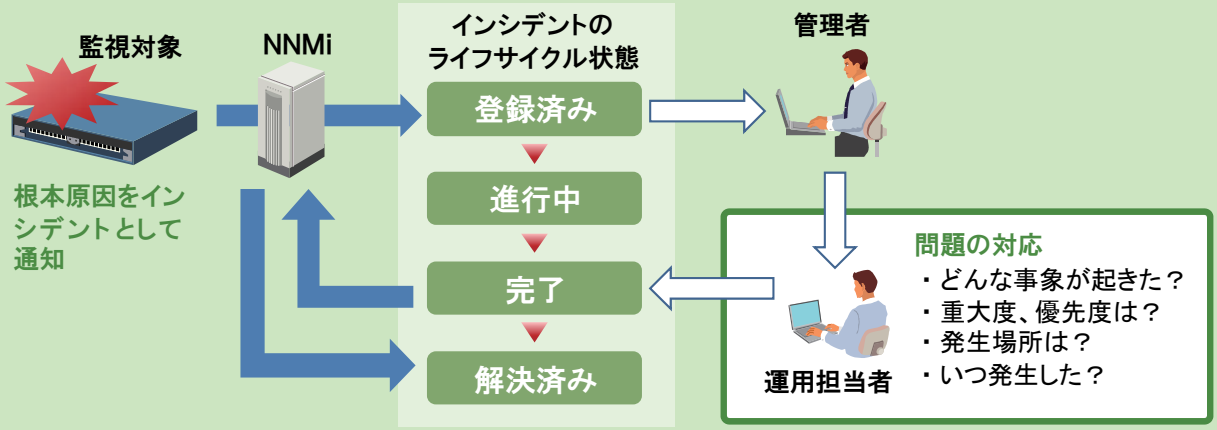
8 [インシデントの設定]画面で[保存して閉じる]をクリックします。

[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 インシデントによるライフサイクル管理

通知されたインシデントは、ライフサイクルに沿って、障害の発生から解決まで[インシデント]画面の「ライフサイクル状態」で管理できます。このため、解決が必要な障害はもれなく対応し、運用できます。



ライフサイクル管理に沿って障害を解決する

ヘルプ　【管理者用ヘルプ 】-［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］

インシデントとして問題が通知されてから解決するまでをライフサイクルに沿って管理します。運用を検討する段階で、インシデントが通知されたときの対応方法を検討しておきましょう。

■操作手順　～ライフサイクル管理に沿って障害を解決する～

未解決のインシデントを確認します

ここでは、ホストのノードダウン障害がインシデントとして通知されてきたことを想定した手順について説明します。このため、あらかじめ擬似的に障害を発生させる設定をしてください。

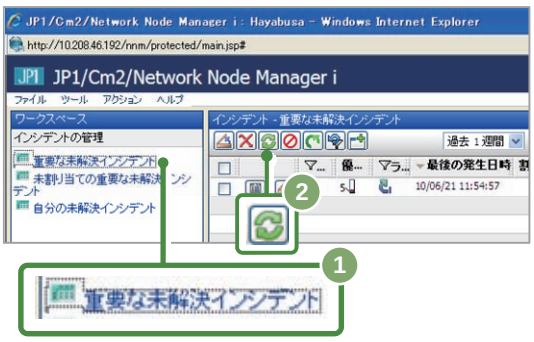
監視中のホストのSNMPサービスを停止させます

監視中のホストの SNMP サービスを 1 台停止させ、擬似的にノードダウン障害を発生させます。以降の操作手順では、このホストを**対象ホスト**と呼びます。
ポーリングが実行されたあとにノードダウン障害が NNMi によって検知されるため、しばらく時間が経過してから操作手順を実施してください。なお、ポーリングは 5 分間隔（デフォルトの場合）で実行されます。

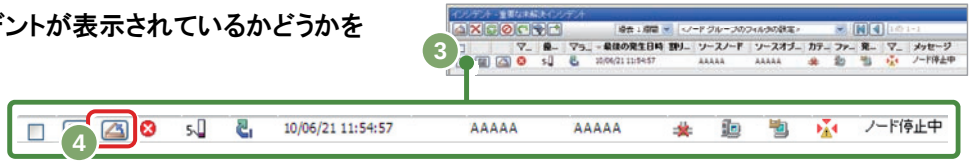
1 **ワークスペースから[インシデントの管理] - [重要な未解決インシデント]を選択します。**

[インシデント － 重要な未解決インシデント]画面が表示されます。

2 [ ]（リフレッシュ）をクリックします。



3 対象ホストのインシデントが表示されているかどうかを確認します。



4 対象ホストのインシデントの[ ](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。

ヒント

[管理イベントの設定]画面など、インシデント定義を参照する画面の[説明]欄には、該当するインシデントの説明が書かれています。インシデントとして通知された問題を解決するときに参照してください。

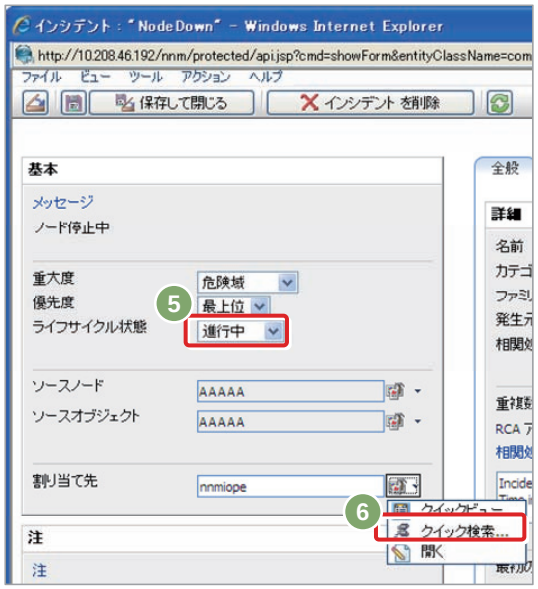
[管理イベントの設定]画面は、[インシデント定義]画面の[アクション]-[Open Incident Configration]を選択すると表示されます。

運用担当者と進行状況を設定します

管理者は通知されたインシデントをもとに、障害に対応する運用担当者を設定します。ここでは、運用担当者として、「2.2 NNMi へのアクセス」の「操作手順 ～ユーザーアカウントを設定する～」の操作手順で作成した「運用担当者(nnmiope)」を設定します。

管理者

5 [ライフサイクル状態]のプルダウンメニューから「進行中」を選択します。

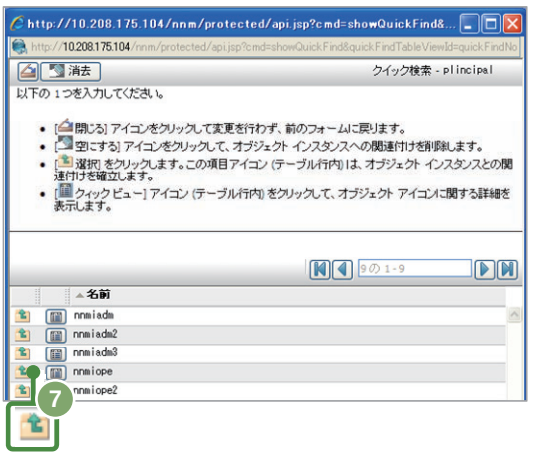


6 [割り当て先]の[ ]から[クイック検索]を選択します。

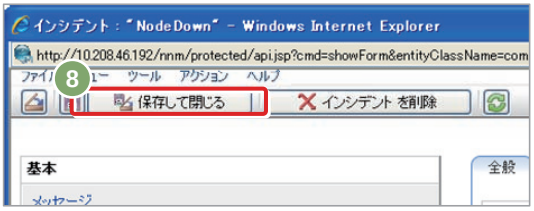
[クイック検索 - Principal]画面が表示されます。

7 「操作手順～ユーザーアカウントを設定する」で作成した「運用担当者(nnmiope)」の[ ](この項目を選択)をクリックします。

[クイック検索 - Principal]画面が閉じます。



8 [インシデント]画面で[保存して閉じる]をクリックします。



インシデントをもとに障害を解決します

9～14の操作は、管理者が[割り当て先]に指定したユーザーアカウントで実施する操作です。
「運用担当者（nnmiope）」のユーザーアカウントで NNMi にアクセスし直してから実施してください。

運用担当者

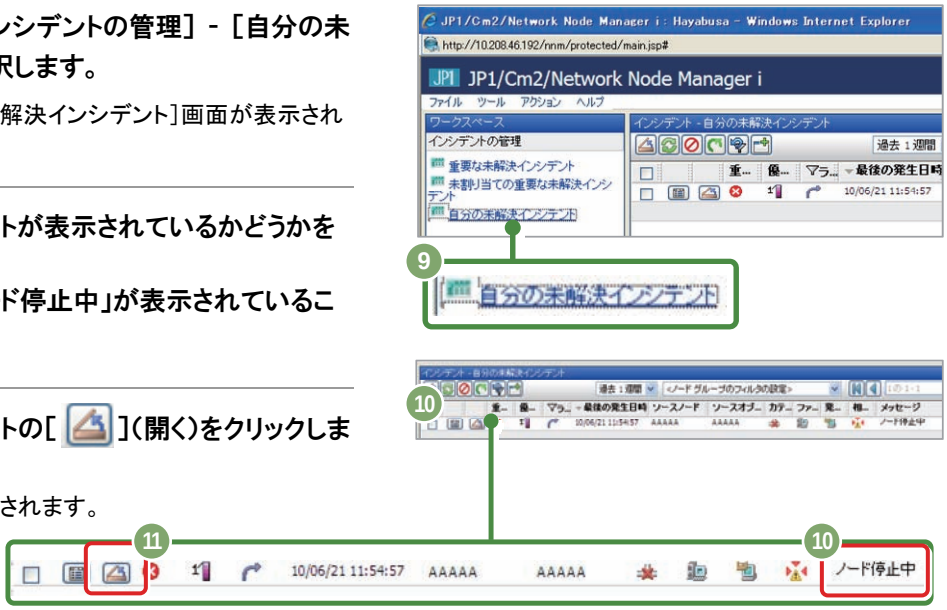
9 ワークスペースから[インシデントの管理] - [自分の未解決インシデント]を選択します。

[インシデント - 自分の未解決インシデント]画面が表示されます。

10 対象ホストのインシデントが表示されているかどうかを確認します。
また、メッセージに「ノード停止中」が表示されていることも確認します。

11 対象ホストのインシデントの[ ]（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。

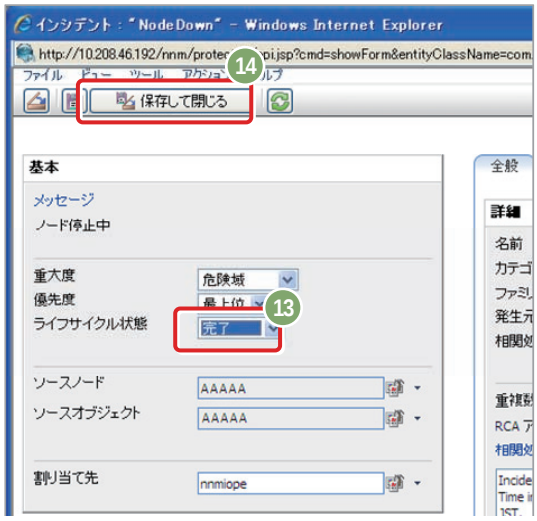


12 インシデントの情報をもとに障害を解決します。

ここでは、対象ホストの SNMP サービスを開始させて、擬似的に発生させた障害を解決します。

13 [ライフサイクル状態]のプルダウンメニューから[完了]を選択します。

14 [インシデント]画面で[保存して閉じる]をクリックします。



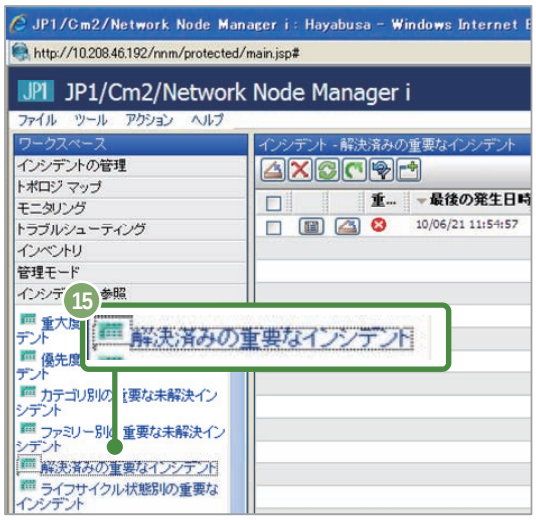
障害が解決されていることを確認します

15～18の操作は、管理者のアカウントで実施する操作です。「管理者（nnmiadm）」のユーザーアカウントで NNMi にアクセスし直してから実施してください。

15 ワークスペースから[インシデントの参照] - [解決済みの重要なインシデント]を選択します。

[インシデント - 解決済みの重要なインシデント]画面が表示されます。

参考 NNMi が対象ホストのポーリングをして、障害が解決したことを認識すると、インシデントのライフサイクル状態は「解決済み」になります。したがって、次のポーリング（デフォルトは 5 分間隔）を待ってから操作をしてください。

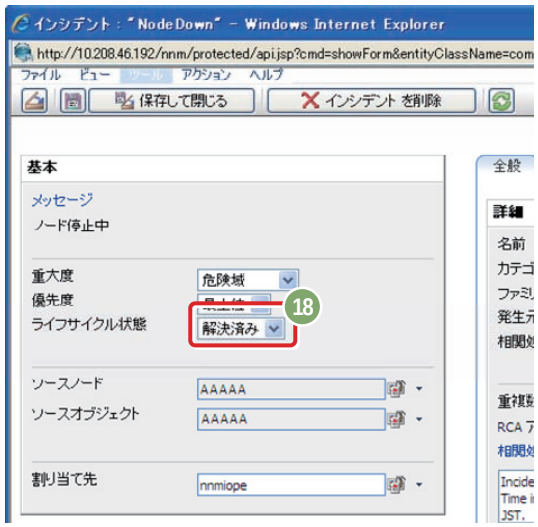


16 対象ホストのインシデントが表示されていることを確認します。

17 対象ホストのインシデントの[ ]（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。

18 対象ホストのインシデントの[ライフサイクル状態]が「解決済み」になっていることを確認してください。



これでライフサイクル管理に沿って障害を解決する操作は完了です。

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をする機能です。

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、SMMPv2c、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トポロジにもと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
HP-UX			HP-UX 11i v3(IPF)
Internet Explorer			Microsoft(R) Internet Explorer(R)
Linux			Red Hat Enterprise Linux AS4(AMD64& Intel EM64T)
			Red Hat Enterprise Linux ES4(AMD64& Intel EM64T)
			Red Hat Enterprise Linux 5 Advanced Platform(AMD/Intel64)
			Red Hat Enterprise Linux 5(AMD/Intel64)
JP1/Cm2/NNM i			JP1/Cm2/Network Node Manager i 09-10
NNMi			
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
CDP	Cisco Discovery Protocol
FQDN	Fully Qualified Domain Name
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
OSI	Open Systems Interconnection
PC	Personal Computer
RCA	Root Causal Analysis
SNMP	Simple Network Management Protocol

常用漢字以外の漢字の使用について

このマニュアルでは、常用漢字を使用することを基本としていますが、次に示す用語については、常用漢字以外の漢字を使用しています。

個所（かしょ）

索引

け

こ

さ

し

せ

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。

・HP-UXは、米国Hewlett-Packard Companyのオペレーティングシステムの名称です。
・Linuxは、Linus Torvalds氏の日本およびその他の国における登録商標または商標です。
・Microsoftは，米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。
・Solarisは、米国Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。
・Windowsは，米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。
・Windows Serverは，米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

2010年 7月 第1版 発行