HITACHI
Inspire the Next

JP1 Version 13

ネットワーク管理 基本ガイド

3021-3-L31

前書き

■ 対象製品

JP1/Network Node Manager i（適用 OS：Windows）

P-2942-82DL JP1/Network Node Manager i 13-00

P-2942-89DL JP1/Network Node Manager i Developer's Toolkit 13-00

JP1/SNMP System Observer（適用 OS：Windows）

P-2942-8RDL JP1/SNMP System Observer 13-00

JP1/Network Node Manager i（適用 OS：Linux）

P-8442-82DL JP1/Network Node Manager i 13-00

P-8442-89DL JP1/Network Node Manager i Developer's Toolkit 13-00

JP1/SNMP System Observer（適用 OS：Linux）

P-8442-8RDL JP1/SNMP System Observer 13-00

■ 輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

■ 商標類

この製品には，Apache Software Foundation で開発されたソフトウェアが含まれています。
(http://www.apache.org)
この製品には，Indiana University Extreme! Lab で開発されたソフトウェアが含まれています。
(http://www.extreme.indiana.edu)
この製品には，The Legion Of The Bouncy Castle によって開発されたソフトウェアが含まれています。
(http://www.bouncycastle.org)

JP1/SNMP System Observer は，米国 EMC コーポレーションの RSA BSAFE(R)ソフトウェアを搭載しています。

■ マイクロソフト製品のスクリーンショットの使用について

マイクロソフトの許可を得て使用しています。

■ 発行

2023 年 9 月 3021-3-L31

■ 著作権

変更内容

変更内容（3021-3-L31）JP1/Network Node Manager i 13-00，JP1/Network Node Manager i Developer's Toolkit 13-00，JP1/SNMP System Observer 12-00

追加・変更内容	変更個所
JP1/Network Element Manager に関する記述を削除した。	1.1，1.3，1.3.2，3.1.1
次の製品に関する記述を変更または削除した。 • JP1/Extensible SNMP Agent for Windows • JP1/Extensible SNMP Agent • JP1/SNMP System Observer - Agent for Process	1.1，1.2.1，1.2.4，1.3.5(3)，1.4.4(4)，2.1，2.3，2.3.2，3.1.1(2)，4.3
監視マネージャーの適用 OS に次の OS を追加した。 • Linux 9.1 • Oracle Linux 9.1 また，次の適用 OS を削除した。 • Windows Server 2012 • CentOS • Linux 6.1 • Oracle Linux 6.1	1.2.1
NNMi が使用する HTTP ポートおよび HTTPS ポートのデフォルト値を変更した。	1.2.1，1.3.1
Web ブラウザの Internet Explorer のサポート終了に伴い，関連する記述を削除した。	1.2.1，2.2.1
監視マネージャーとするサーバに必要なパッケージとライブラリファイルに関する説明を変更した。	1.2.3

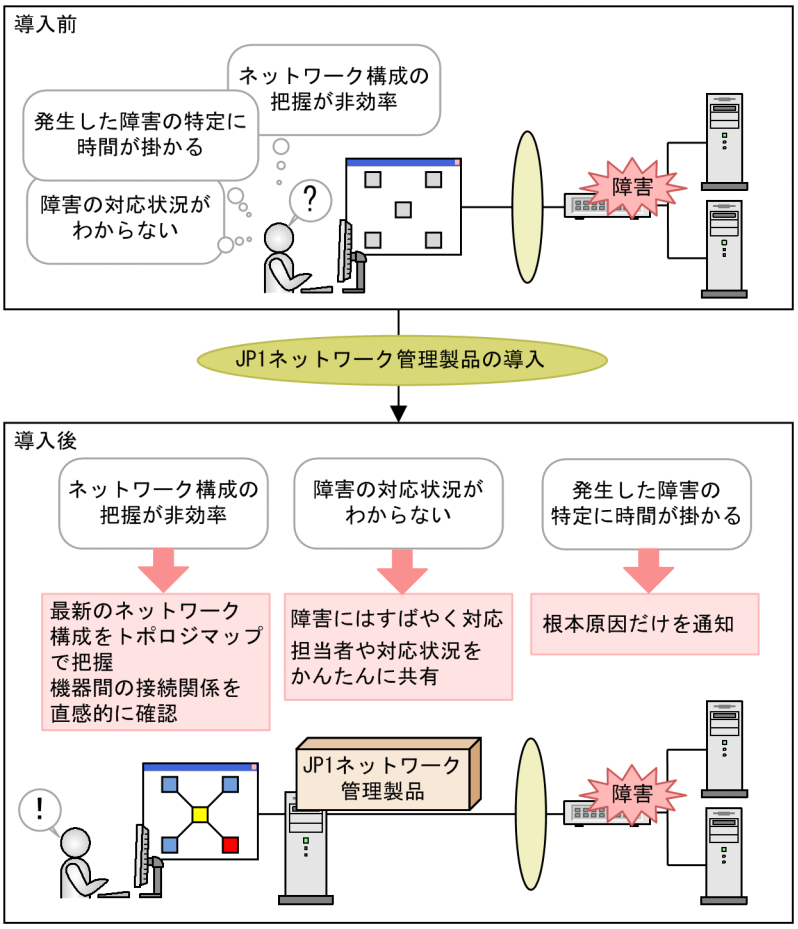
単なる誤字・脱字などはお断りなく訂正しました。

はじめにお読みください

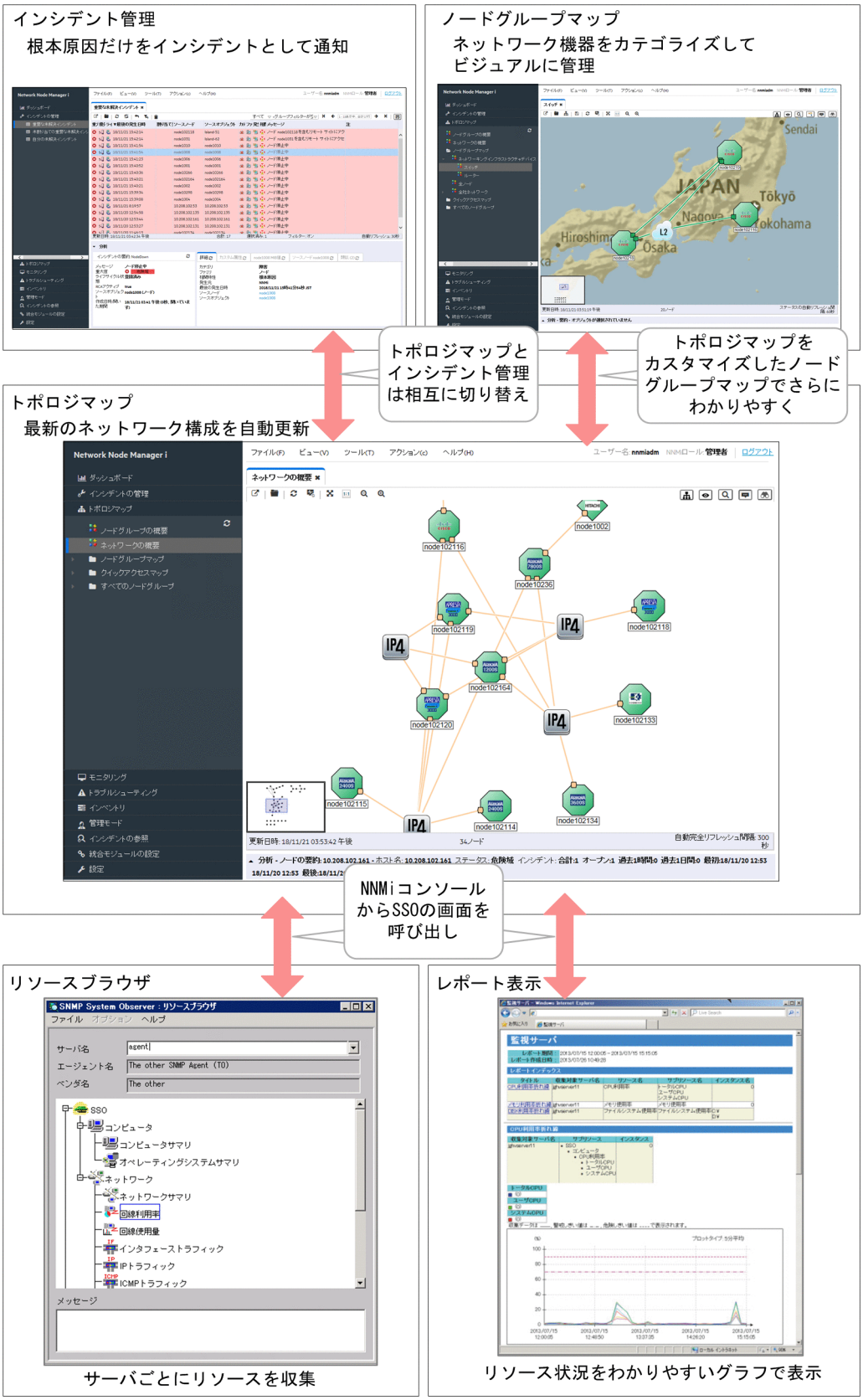
■ JP1 ネットワーク管理製品でできること

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ですが，日ごとに複雑化・大規模化していくネットワークに，管理者の作業が増大していませんか。

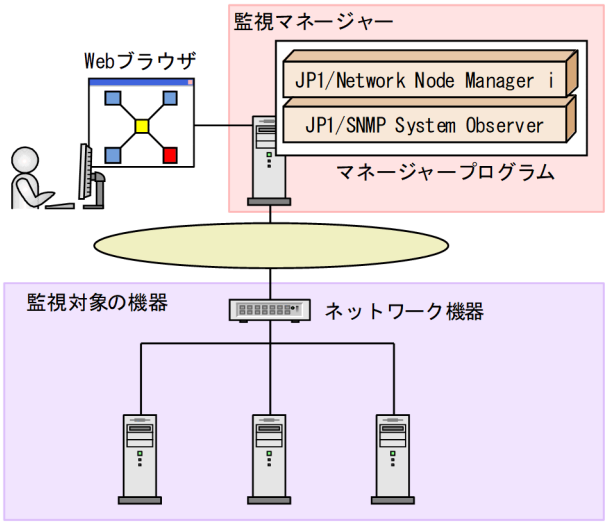
次のような悩みをお持ちなら，従来のネットワーク管理・運用方法を見直し，JP1 ネットワーク管理製品を導入しましょう。JP1 ネットワーク管理製品を導入すれば，ネットワーク構成を効率良く把握し，迅速に障害を特定・解決できます。



また，JP1 ネットワーク管理製品では，ネットワーク構成やリソース状況を直感的に把握できる多彩な画面を提供し，ネットワーク管理者の日々の業務をサポートします。



JP1 ネットワーク管理製品の基本的なシステム構成を次に示します。



JP1/Network Node Manager i（以降，NNMi と表記します）

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マネージャープログラムです。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もできます。

JP1/SNMP System Observer（以降，SSO と表記します）

SNMP をサポートするネットワーク機器を対象に，リソースを収集するマネージャープログラムです。ネットワーク機器のベンダーを意識することなく監視できます。

マネージャープログラムの主な機能は次のとおりです。

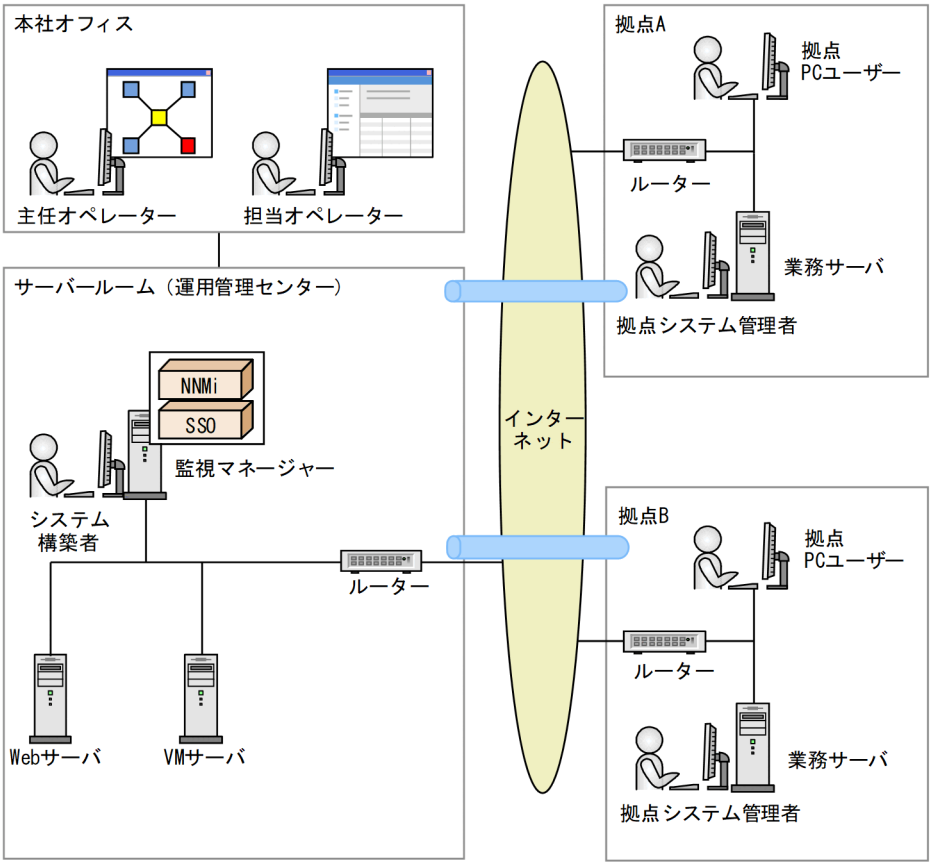
製品名	機能名	機能の説明
NNMi	ノードの検出	設定したルールに従い，ノードを自動検出します。また，手動でノードを追加することもできます。
	トポロジの検出・表示	レイヤー 3 トポロジ（論理的なネットワーク構成）に加え，レイヤー 2 トポロジ（物理的な結線によるネットワーク構成）を自動検出し，マップに表示します。
	ICMP/SNMP ポーリングや SNMP トラップによる監視	ICMP/SNMP ポーリングによって，オブジェクトの状態を監視します。また，SNMP トラップによって障害を監視します。
	根本原因解析	検出したレイヤー 2 およびレイヤー 3 トポロジに基づいて，障害の根本原因を解析します。
	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できます。

製品名	機能名	機能の説明
SSO	リソース収集	回線利用率などのネットワーク性能情報など，さまざまなシステムリソースを監視します。

■ このマニュアルで説明すること

このマニュアルでは，JP1 ネットワーク管理製品の基本的な構築方法および運用方法について説明しています。このマニュアルを読んだユーザーが，JP1 ネットワーク管理製品を使用して，日々のネットワーク管理や迅速な障害対応が行えるようになることを目指します。

このマニュアルは，次に示すシステム，および組織の構成に基づいて運用手順を説明します。



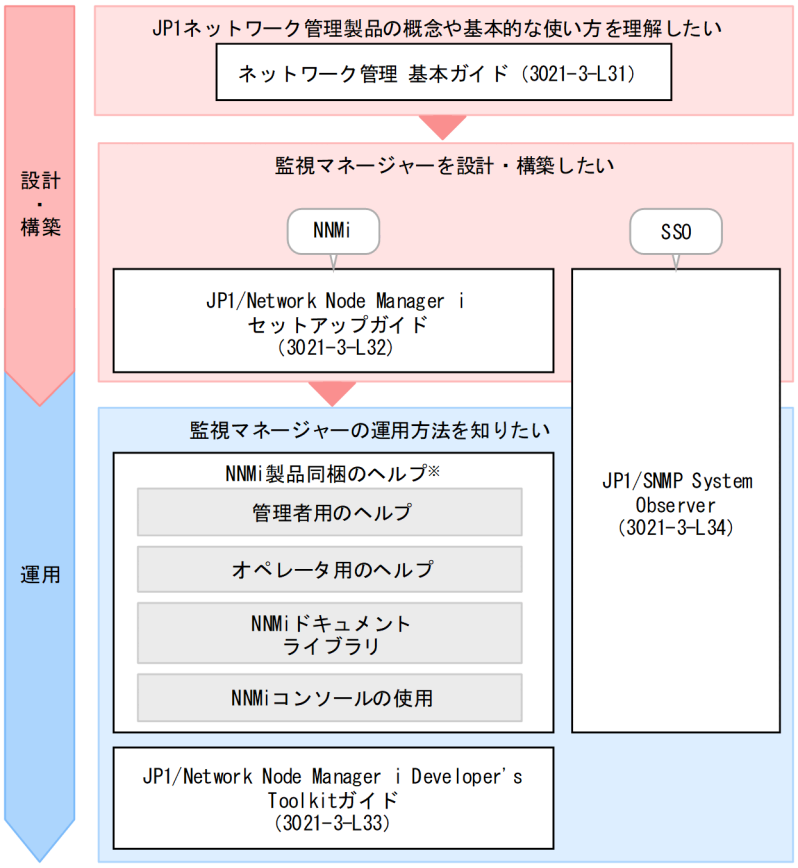
このマニュアルで説明する構築手順

1. 主任オペレーターは，システム構築者に JP1 ネットワーク管理製品の環境構築を依頼します。
2. システム構築者は，監視マネージャーとなるサーバを用意し，マネージャー環境を構築します。
3. システム構築者は，JP1 ネットワーク管理製品の設定を行います。

4. JP1 ネットワーク管理製品の設定が完了したら，システム構築者はそのことを主任オペレーターに連絡します。
5. 連絡を受けた主任オペレーターは，担当オペレーターをユーザーに登録し，JP1 ネットワーク管理製品による運用を開始します。

■ マニュアルの読み方

JP1 ネットワーク管理製品では，このマニュアルのほかにも複数のマニュアルとヘルプを提供しています。さらに応用的な機能や操作を知りたい場合は，目的に応じて次のようにお読みください。



注※　ヘルプは，NNMiコンソールの［ヘルプ］メニューから表示できます。

他マニュアルへの参照先は，『～については，マニュアル「△△」の「○○」のトピックを参照してください。』の形式で記載しています。「○○」をキーワードとしてマニュアル「△△」の索引内を検索して，該当する説明をお読みください。

このマニュアルでは，次に示す環境を前提として説明しています。

監視マネージャーでの操作

Windows の場合：Windows Server 2019 を使用している環境

Linux の場合：Linux 8.1 (x64)を使用している環境

Web ブラウザでの操作

Microsoft Edge を使用している環境

製品の改良などによって，このマニュアルに掲載されている画面はご使用の製品画面と一部異なることがあります。あらかじめご了承ください。

目次

1 JP1 ネットワーク管理製品の構築

JP1 ネットワーク管理製品をインストールして，ネットワーク監視環境を構築しましょう。

1.1　JP1 ネットワーク管理製品の構築の流れ

JP1 ネットワーク管理製品を構築するには，監視マネージャーを構築する必要があります。監視マネージャーの構築は，Windows と Linux で構築手順が異なります。

監視マネージャーの構築の流れを次に示します。

作業の概要	順番	作業内容	参照先	
			Windows	Linux
インストール前の準備	1	サーバ環境を確認する	1.2.1	
	2	監視マネージャーの前提条件を確認する	1.2.2	1.2.3
監視マネージャーの構築	3	NNMi をインストールする	1.3.1	1.4.1
	4	SSO をインストールする	1.3.2	1.4.2
	5	NNMi をセットアップする	1.3.3	1.4.3
	6	SSO をセットアップする	1.3.4	1.4.4

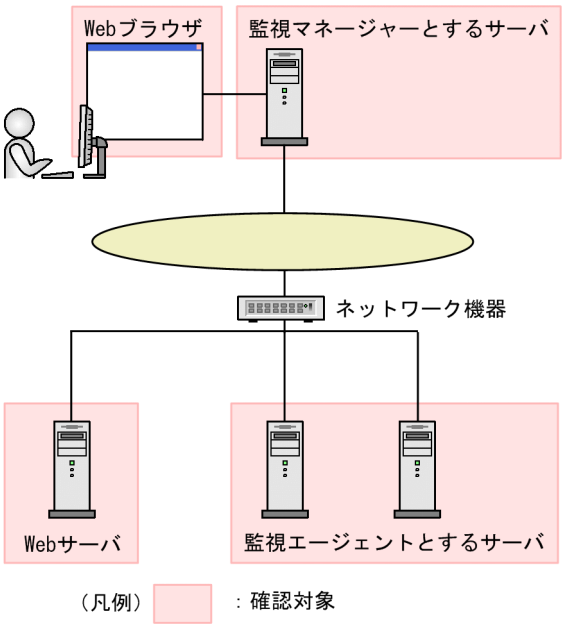
1.2　インストール前の準備

1.2.1　サーバ環境を確認する

JP1 ネットワーク管理製品をインストールする前に，運用で使用するサーバ環境が適切かどうかを確認します。

前提条件

このマニュアルで想定するシステム構成を次に示します。



操作手順

1. 監視マネージャーとするサーバの仕様が，次の条件を満たしていることを確認します。

   - OS：

     Windows の場合：Windows Server 2016，Windows Server 2019，または Windows Server 2022

     Linux の場合：Linux 7.1，Linux 8.1，Linux 9.1，Oracle Linux 7.1，Oracle Linux 8.1，Oracle Linux 9.1，または SUSE Linux 12

     なお，このマニュアルでは，Windows Server 2019 および Linux 8.1 の構築手順を説明します。

   - ディスク容量：

     Windows の場合：14.5GB 以上

     Linux の場合：14.0GB 以上

   - メモリ：

Windows の場合：4.5GB 以上
Linux の場合：6.0GB 以上

2. **監視マネージャーとするサーバの言語設定を確認します。**
   Windows の場合は，ロケールを次のとおりに設定します。
   - 日本語環境：日本語
   - 英語環境：英語
   - 中国語環境：中国語

   Linux の場合は，ロケールを次のとおりに設定します。
   - 日本語環境：ja_JP.UTF-8
   - 英語環境：C
   - 中国語環境：zh_CN.utf8

3. **Web サーバのポート番号を確認します。**
   Web サーバのポート番号は，NNMi のインストール時に使用します。デフォルトは HTTP ポートは 20480，HTTPS ポートは 20481 です。

4. **使用する Web ブラウザが，次の条件を満たしていることを確認します。**
   OS が Windows の場合：Firefox ESR，Google Chrome，または Microsoft Edge（Chromium 版）。
   詳細については，リリースノートを参照してください。

次の作業

サーバ環境に問題がないことが確認できたら，前提条件の確認に進みましょう。

関連項目

- マニュアル「NNMi セットアップガイド」の「インストール前チェックリスト」のトピック
- 1.2.2　監視マネージャーの前提条件を確認する（Windows の場合）
- 1.2.3　監視マネージャーの前提条件を確認する（Linux の場合）

1.2.2　監視マネージャーの前提条件を確認する（Windows の場合）

監視マネージャーが Windows の場合，次の設定を確認してから，JP1 ネットワーク管理製品のインストールを開始します。前提条件の詳細については，マニュアル「NNMi セットアップガイド」の「インストール前チェックリスト」のトピックを参照してください。

操作手順

1. 監視マネージャーのホスト名を確認します。
   ホスト名はトラップ宛先の設定やログイン時に使用します。

2. 監視マネージャーが使うポート番号が使われていないことを確認します。
   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。
   ポート番号の詳細については，マニュアル「NNMi セットアップガイド」の「NNMi が使用するポートの一覧」のトピックを参照してください。SSO については，リリースノートの「設定ポート番号および設定変更手順」を参照ください。

3. 監視マネージャーに固定 IP アドレスを割り当てます。
   IP アドレスは DHCP での動的割り当てではなく，固定割り当てに設定してください。

4. NNMi をインストールするフォルダを検討します。
   NNMi のインストール先フォルダは，インストール時に使用します。デフォルトを次に示します。
   - プログラム用：C:¥Program Files (x86)¥Hitachi¥Cm2NNMi¥
   - データ用：C:¥ProgramData¥Hitachi¥Cm2NNMi¥

5. NNMi のシステムアカウントのパスワードを検討します。
   NNMi のシステムアカウントは，NNMi コンソールに最初にサインインする際に使用します。
   パスワードは，1 文字以上，最大 40 文字まで入力できます。使用できる文字は，半角英数字（A-Z，a-z，0-9），およびアンダーバー（_）です。

6. SSO をインストールするフォルダを検討します。
   SSO のインストール先フォルダは，インストール時に使用します。デフォルトを次に示します。
   - C:¥Program Files¥HITACHI¥JP1SSO¥

7. ウィルス対策ソフトを無効化します。
   JP1 ネットワーク管理製品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。

8. Windows の SNMP 関連サービスの SNMP Trap サービスを「無効」にします。

9. 監視マネージャーを SNMP で監視する場合は，SNMP サービスを導入します。

10. 監視マネージャーが使用しているポート番号へのアクセスが，Windows ファイアウォールで有効になっていることを確認します。
    ポート番号へのアクセスの詳細については，マニュアル「NNMi セットアップガイド」の「ファイアウォールの通過方向」のトピックを参照してください。

11. 環境変数の TEMP と TMP に設定された値が，同じかどうかを確認します。

    環境変数の TEMP と TMP の値が異なると，NNMi のインストールに失敗することがあります。値が異なる場合は，同じ値を設定してください。なお，インストール時に%TEMP%フォルダを 500.0MB 使用します。

12. ［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 ホストの構成］で，リモートデスクトップの設定を次のように設定します。

    - 終了時に一時フォルダーを削除しない
    - セッションごとに一時フォルダーを使用しない

次の作業

前提環境に問題がないことが確認できたら，監視マネージャーの構築に進みましょう。

関連項目

- 1.3　監視マネージャーの構築（Windows の場合）

1.2.3　監視マネージャーの前提条件を確認する（Linux の場合）

監視マネージャーが Linux の場合，次の設定を確認してから，JP1 ネットワーク管理製品のインストールを開始します。前提条件の詳細については，マニュアル「NNMi セットアップガイド」の「インストール前チェックリスト」のトピックを参照してください。

操作手順

1. 監視マネージャーのホスト名を確認します。

   ホスト名はトラップ宛先の設定やログイン時に使用します。

2. 監視マネージャーが使うポート番号が使われていないことを確認します。

   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。

   ポート番号の詳細については，マニュアル「NNMi セットアップガイド」の「NNMi が使用するポートの一覧」のトピックを参照してください。

3. 監視マネージャーに固定 IP アドレスを割り当てます。

   IP アドレスは DHCP での動的割り当てではなく，固定割り当てに設定してください。

4. ウィルス対策ソフトを無効化します。

   JP1 ネットワーク管理製品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。

5. 必要なパッケージがインストールされていることを確認します。

   必要なパッケージは，OS の種類やバージョンによって異なります。詳細については，リリースノートを参照してください。

6. /etc/sysctl.conf ファイルを開き，カーネルのパラメータを設定します。

   /etc/sysctl.conf ファイルに次のエントリを追加してください。

```
# NNM settings for embedded database
kernel.shmmax = 68719476736
kernel.shmall = 68719476736
# NNM settings for UDP receive and send buffer sizes
net.core.rmem_max = 8388608
net.core.wmem_max = 2097152
```

   ここでは，共有メモリ（kernel.shmmax，kernel.shmall）64.0GB，UDP 受信バッファ（net.core.rmem_max）8.0MB，UDP 送信バッファ（net.core.wmem_max）2.0MB として設定しています。

次の作業

前提環境に問題がないことが確認できたら，監視マネージャーの構築に進みましょう。

関連項目

- 1.4　監視マネージャーの構築（Linux の場合）

1.2.4　各製品のコマンドの格納先

各製品のコマンドの格納先を次に示します。

NNMi コマンドの格納先

- Windows の場合
  NNMi のインストール先フォルダ¥bin¥
- Linux の場合
  /opt/OV/bin/

SSO コマンドの格納先

- Windows の場合
  SSO のインストール先フォルダ¥bin¥
- Linux の場合
  /opt/CM2/SSO/bin/

1.3　監視マネージャーの構築（Windows の場合）

NNMi，および SSO をインストールおよびセットアップして，Windows 環境に監視マネージャーを構築します。

1.3.1　NNMi をインストールする（Windows の場合）

監視マネージャーが Windows の場合，日立統合インストーラから，ウィザードに従って NNMi をインストールします。

操作手順

1. 監視マネージャーにするサーバに Administrators 権限でログインし，提供媒体をセットします。
2. 「JP1/Network Node Manager i」を選択します。
   NNMi の設定値の確認画面が表示されます。
3. Web サーバのポート番号を指定し，［Enter］キーを押します。
   値を入力しないで［Enter］キーを押すと，デフォルトが指定されます。デフォルトは HTTP ポートは 20480，HTTPS ポートは 20481 です。
4. NNMi のインストール先フォルダを指定します。
   値を入力しないで［Enter］キーを押すと，デフォルトが指定されます。デフォルトを次に示します。
   - プログラム用：C:¥Program Files (x86)¥Hitachi¥Cm2NNMi¥
   - データ用：C:¥ProgramData¥Hitachi¥Cm2NNMi¥

   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。
5. 「yes」を入力して［Enter］キーを押します。
   NNMi のインストールが開始されます。しばらく経過すると，システムアカウントのパスワードの設定画面が表示されます。
6. システムアカウントのパスワードを設定します。
   画面の指示に従ってパスワードを設定します。
   インストール後に設定する場合は，「¥quit」を入力します。
   設定完了後，[Enter] キーを押すと，コマンドプロンプトが閉じます。

次の作業

次は SSO をインストールしましょう。

関連項目

- 1.3.2　SSO をインストールする（Windows の場合）

1.3.2　SSO をインストールする（Windows の場合）

監視マネージャーが Windows の場合，日立統合インストーラから，ウィザードに従って SSO をインストールします。

操作手順

1. 監視マネージャーにするサーバに Administrators 権限でログインし，提供媒体をセットします。
2. 「JP1/SNMP System Observer」を選択します。
3. インストーラの指示に従って，SSO をインストールします。

次の作業

次は NNMi をセットアップしましょう。

関連項目

- 1.3.3　NNMi をセットアップする（Windows の場合）

1.3.3　NNMi をセットアップする（Windows の場合）

インストール時にシステムアカウントのパスワードの設定をスキップした場合は，NNMi のサービスを停止し，システムアカウントを設定します。そのほかのメンバーを登録する場合は，NNMi コンソールにログインしてから，ユーザーを登録してください。

前提条件

インストール前から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ください。

操作手順

1. インストール時にシステムアカウントのパスワードの設定をスキップした場合のみ，手順 a.および b.を実行します。
   a. コマンドプロンプトで ovstop -c を実行して，NNMi サービスを停止します。
      NNMi サービスが停止します。インストール直後は，NNMi サービスは停止した状態です。

b. nnmchangesyspw.ovpl を実行して，パスワードを設定します。
「y」を入力後，メッセージに従ってパスワードを指定します。

2. ovstart -c を実行して，NNMi を起動します。

3. ovstatus -c を実行して，NNMi の状態を確認します。
すべての状態が"実行"になっていれば正常です。

次の作業

次は SSO をセットアップしましょう。

関連項目

- 1.2.4　各製品のコマンドの格納先
- 2.2.3　ユーザーを登録する
- 1.3.4　SSO をセットアップする（Windows の場合）

1.3.4　SSO をセットアップする（Windows の場合）

監視マネージャーが Windows の場合，コミュニティ名や SSO の定義情報を設定して，SSO をセットアップします。

(1)　SSO から NNMi への接続情報を追加する

SSO の ssonnmsetup コマンドを実行して，NNMi と連携するための接続情報を設定します。

操作手順

1. 次のコマンドを実行します。
ssonnmsetup -add -user **ユーザー名** -password **パスワード** -port **ポート番号** -ssl
システムアカウントのユーザー名とパスワードを指定します。**ポート番号**には，Web サーバのポート番号を指定します。-ssl オプションは https で通信する場合だけ指定してください。

関連項目

- 1.2.4　各製品のコマンドの格納先
- 1.3.3　NNMi をセットアップする（Windows の場合）
- 1.2.1　サーバ環境を確認する

(2) SSO の定義情報を NNMi に設定する

コマンドを実行して，SSO の定義情報を NNMi に設定します。

操作手順

1. NNMi の nnmconfigimport.ovpl コマンドを実行して，インシデント定義を設定します。
   nnmconfigimport.ovpl -u ユーザー名 -p パスワード -f SSO のインストール先フォルダ¥incident¥ssoincident.def
   システムアカウントのユーザー名とパスワードを指定します。
   イベント通知に TCP 通信を使用しない APM をプロセス・サービス監視対象とする場合，次のインシデント定義も設定が必要です。
   nnmconfigimport.ovpl -u ユーザー名 -p パスワード -f SSO のインストール先フォルダ¥incident¥apmtrap.def
2. NNMi の nnmconfigimport.ovpl コマンドを実行して，URL アクション定義を設定します。
   nnmconfigimport.ovpl -u ユーザー名 -p パスワード -f SSO のインストール先フォルダ¥urlaction¥ssourlaction.def
   システムアカウントのユーザー名とパスワードを指定します。
3. SSO の ssoauth コマンドを実行して，SSO にユーザーを登録します。
   ssoauth -add -user ユーザー名 -password パスワード
   SSO コンソールからログインするためのユーザー名とパスワードを設定します。
4. SSO の ssostart コマンドを実行して，SSO を起動します。
5. SSO の ssostatus コマンドを実行して，SSO の状態を確認します。
   すべての状態が実行中になっていれば正常です。

関連項目

- 1.2.4 各製品のコマンドの格納先

(3) コミュニティ名を設定する

コミュニティ名とは，SNMP プロトコルで MIB オブジェクトにアクセスするためのパスワードです。リソースを収集する場合は，監視エージェントと監視マネージャーの get コミュニティ名を一致させる必要があります。

操作手順

1. SNMP 定義ファイル（SSO のインストール先フォルダ¥conf¥ssosnmp.conf）を開きます。
2. SNMP 定義ファイルを編集します。

3. 次のように ssoapcom コマンドを実行して，定義ファイルを再読み込みします。
   ssoapcom -r
4. 次のように ssocollectd コマンドを実行して，定義ファイルを再読み込みします。
   ssocollcetd -r

次の作業

これで，監視マネージャーの構築が完了しました。拠点の監視エージェントの構築が完了していることを確認しましょう。拠点の監視エージェントの構築が完了している場合は，JP1 ネットワーク管理製品の設定に進みましょう。

関連項目

- 1.2.4　各製品のコマンドの格納先
- 1.3.3　NNMi をセットアップする（Windows の場合）
- 2.　JP1 ネットワーク管理製品の設定

1.3.5　SSO の WebGUI をセットアップする（Windows の場合）

SSO コンソールを使用する Windows のマシン上に，SSO の WebGUI を準備します。

WebGUI の設定は，Administrator 権限を持つユーザーで実行してください。

操作手順

1. ssogui_fileset.zip ファイルを，SSO コンソールを使用する Windows のマシン上にコピーして，任意の場所に展開します。
   ファイルの格納先：
   SSO のインストール先フォルダ¥webgui¥ssogui_fileset.zip
2. 展開先の bin フォルダにある webguisetup.bat コマンドを，コマンドプロンプトから次のように実行します。
   展開先パス¥SSOGUI¥bin¥webguisetup.bat 展開先パス¥SSOGUI

1.4　監視マネージャーの構築（Linux の場合）

NNMi と SSO をインストールおよびセットアップして，Linux 環境に監視マネージャーを構築します。

1.4.1　NNMi をインストールする（Linux の場合）

監視マネージャーが Linux の場合，日立統合インストーラから，ウィザードに従って NNMi をインストールします。

操作手順

1. 監視マネージャーにするサーバに root 権限でログインします。
2. 環境変数「LC_ALL」，「LANG」に，次のロケールを設定します。
   - 日本語環境の場合
     # LC_ALL=ja_JP.utf8
     # export LC_ALL
     # LANG=ja_JP.utf8
     # export LANG
     または
     # LC_ALL=ja_JP.UTF-8
     # export LC_ALL
     # LANG=ja_JP.UTF-8
     # export LANG
   - 英語環境の場合
     # LC_ALL=C
     # export LC_ALL
     # LANG=C
     # export LANG
     または
     # LC_ALL=en_US.utf8
     # export LC_ALL
     # LANG=en_US.utf8
     # export LANG
     または
     # LC_ALL=en_US.UTF-8
     # export LC_ALL

LANG=en_US.UTF-8
export LANG

- 中国語環境の場合
LC_ALL=zh_CN.utf8
export LC_ALL
LANG=zh_CN.utf8
export LANG

3. NNMi の提供媒体をセットし，次のコマンドを実行します。
/提供媒体のマウントディレクトリ名/X64LIN/setup /提供媒体のマウントディレクトリ名

4. Hitachi PP Installer の初期画面で「I」を入力します。

5. 「JP1/Network Node Manager i」を選択し，「I」を入力します。
インストールを続行するか確認するメッセージが表示されます。

6. 「Y」を入力します。

7. インストーラの指示に従って情報を入力します。
値を入力しないで［Enter］キーを押すと，デフォルト値が指定されます。
次のフォルダに NNMi がインストールされます。
- プログラム用：/opt/OV/
- データ用：/var/opt/OV/

しばらく経過すると，システムアカウントのパスワードの設定画面が表示されるので，パスワードを入力します。
インストール後に設定する場合は，「¥quit」を入力します。

次の作業

次は SSO をインストールしましょう。

関連項目

- 1.4.2　SSO をインストールする（Linux の場合）

1.4.2　SSO をインストールする（Linux の場合）

監視マネージャーが Linux の場合，日立統合インストーラから，ウィザードに従って SSO をインストールします。

操作手順

1. 監視マネージャーにするサーバに root 権限でログインし，提供媒体をセットします。
2. 次のコマンドを実行します。
   /提供媒体のマウントディレクトリ名/X64LIN/setup /提供媒体のマウントディレクトリ名
3. Hitachi PP Installer の初期画面で「I」を入力します。
4. 「JP1/SNMP System Observer」を選択し，「I」を入力します。
   インストールを続行するか確認するメッセージが表示されます。
5. 「Y」を入力します。
   SSO がインストールされます。

次の作業

次は NNMi をセットアップしましょう。

関連項目

- 1.4.3　NNMi をセットアップする（Linux の場合）

1.4.3　NNMi をセットアップする（Linux の場合）

監視マネージャーが Linux の場合，システムアカウントを設定して，NNMi をセットアップします。

(1)　システムアカウントを設定する

インストール時にシステムアカウントのパスワードの設定をスキップした場合は，NNMi のシステムアカウントを設定します。設定する方法は，Windows の場合と同じです。

システムアカウントの設定が終わったら，SSO をセットアップしましょう。

関連項目

- 1.2.4　各製品のコマンドの格納先
- 1.3.3　NNMi をセットアップする（Windows の場合）
- 1.4.4　SSO をセットアップする（Linux の場合）

1.4.4　SSO をセットアップする（Linux の場合）

監視マネージャーが Linux の場合，言語環境や定義情報を設定して，SSO をセットアップします。

(1)　言語環境を設定する

SSO のインストールが完了したら，/etc/rc.d/init.d/sso ファイルに言語設定を追加する必要があります。

操作手順

1. /etc/rc.d/init.d/sso ファイルを開きます。
2. 「. /etc/rc.d/init.d/functions」行の直後に次の 2 行を追加します。
   - 日本語環境の場合
     LANG=ja_JP.UTF-8
     export LANG
   - 英語環境の場合
     LANG=C
     export LANG
   - 中国語環境の場合
     LANG=zh_CN.utf8
     export LANG
3. /etc/rc.d/init.d/sso ファイルを上書き保存します。
   これで，言語環境が設定されました。

(2)　SSO から NNMi への接続情報を追加する

NNMi と連携するための接続情報を設定します。設定する方法は，Windows の場合と同じです。

関連項目

- (1)　SSO から NNMi への接続情報を追加する

(3)　SSO の定義情報を NNMi に設定する

コマンドを実行して，SSO の定義情報を NNMi に設定します。

操作手順

1. NNMi の nnmconfigimport.ovpl コマンドを実行して，インシデント定義を設定します。
   nnmconfigimport.ovpl -u ユーザー名 -p パスワード -f /etc/opt/CM2/SSO/incident/ssoincident.def
   システムアカウントのユーザー名とパスワードを指定します。
   イベント通知に TCP 通信を使用しない APM をプロセス・サービス監視対象とする場合，次のインシデント定義も設定が必要です。
   nnmconfigimport.ovpl -u ユーザー名 -p パスワード -f SSO のインストール先フォルダ¥incident¥apmtrap.def
2. NNMi の nnmconfigimport.ovpl コマンドを実行して，URL アクション定義を設定します。
   nnmconfigimport.ovpl -u ユーザー名 -p パスワード -f /etc/opt/CM2/SSO/urlaction/ssourlaction.def
   システムアカウントのユーザー名とパスワードを指定します。
3. SSO の ssoauth コマンドを実行して，SSO にユーザーを登録します。
   ssoauth -add -user ユーザー名 -password パスワード
   SSO コンソールからログインするためのユーザー名とパスワードを設定します。
4. SSO の ssostart コマンドを実行して，SSO を起動します。
5. SSO の ssostatus コマンドを実行して，SSO の状態を確認します。
   すべての状態が実行中になっていれば正常です。

関連項目

- 1.2.4　各製品のコマンドの格納先

(4)　コミュニティ名を設定する

コミュニティ名とは，SNMP プロトコルで MIB オブジェクトにアクセスするためのパスワードです。リソースを収集する場合は，監視エージェントと監視マネージャーの get コミュニティ名を一致させる必要があります。

操作手順

1. SNMP 定義ファイル（/etc/opt/CM2/SSO/conf/ssosnmp.conf）を開きます。
2. SNMP 定義ファイルを編集します。
3. 次のように ssoapcom コマンドを実行して，定義ファイルを再読み込みします。
   ssoapcom -r

4. 次のように ssocollectd コマンドを実行して，定義ファイルを再読み込みします。

   ssocollcetd -r

次の作業

コミュニティ名を設定したら，拠点の監視エージェントの構築が完了していることを確認しましょう。拠点の監視エージェントの構築が完了している場合は，JP1 ネットワーク管理製品の設定に進みましょう。

関連項目

- 1.2.4　各製品のコマンドの格納先
- (2)　SSO の定義情報を NNMi に設定する
- 2.　JP1 ネットワーク管理製品の設定

1.4.5　SSO の WebGUI をセットアップする（Linux の場合）

SSO コンソールを使用する Windows のマシン上に，SSO の WebGUI を準備します。

WebGUI の設定は，Administrator 権限を持つユーザーで実行してください。

操作手順

1. ssogui_fileset.zip ファイルを，SSO コンソールを使用する Windows のマシン上にコピーして，任意の場所に展開します。

   ファイルの格納先：

   /etc/opt/CM2/SSO/webgui/ssogui_fileset.zip

2. 展開先の bin フォルダにある webguisetup.bat コマンドを，コマンドプロンプトから次のように実行します。

   展開先パス¥SSOGUI¥bin¥webguisetup.bat **展開先パス**¥SSOGUI

2 JP1 ネットワーク管理製品の設定

NNMi や SSO にアクセスして，ネットワーク管理を開始するための設定をしましょう。

2.1　JP1 ネットワーク管理製品の設定の流れ

JP1 ネットワーク管理製品の設定の流れを次に示します。

作業の概要	順番	作業内容	参照先
NNMi の設定	1	NNMi にアクセスする	2.2.1
	2	ユーザーを登録する	2.2.3
	3	通信プロトコルを設定する	2.2.4
	4	ネットワークを検出する	2.2.5
	5	ノードグループを設定する	2.2.6
	6	モニタリングを設定する	2.2.7
	7	インシデントを設定する	2.2.8
SSO の設定	8	SSO にアクセスする	2.3.1
	9	リソース収集を設定する	2.3.2

2.2 NNMi の設定

2.2.1 NNMi にアクセスする

Web ブラウザから NNMi にアクセスして，設定を始めましょう。

前提条件

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。

操作手順

1. **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/
   - **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。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。

   NNMi のサインイン画面が表示されます。
2. **ユーザー名とパスワードを入力します。**
   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：システムアカウントのパスワード
3. **［サインイン］をクリックします。**
   NNMi コンソールが表示されます。

> **重要**
>
> 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のためのアカウントです。コマンドによってパスワードが変更できるため，通常運用での使用はお勧めしません。

次の作業

これで，NNMi にサインインできました。NNMi の設定をしながら，基本操作を覚えましょう。

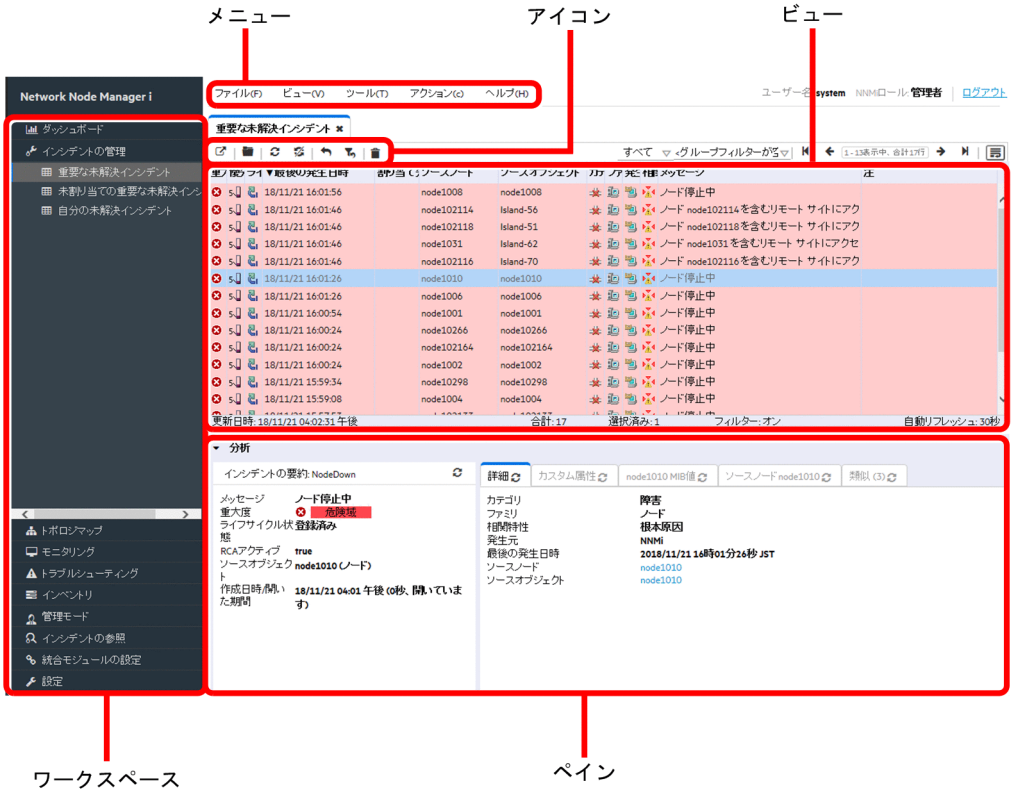
関連項目

- 1.3.3　NNMi をセットアップする（Windows の場合）
- 1.4.3　NNMi をセットアップする（Linux の場合）
- 2.1　JP1 ネットワーク管理製品の設定の流れ

2.2.2　NNMi コンソールについて

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）， （保存して閉じる）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。

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。



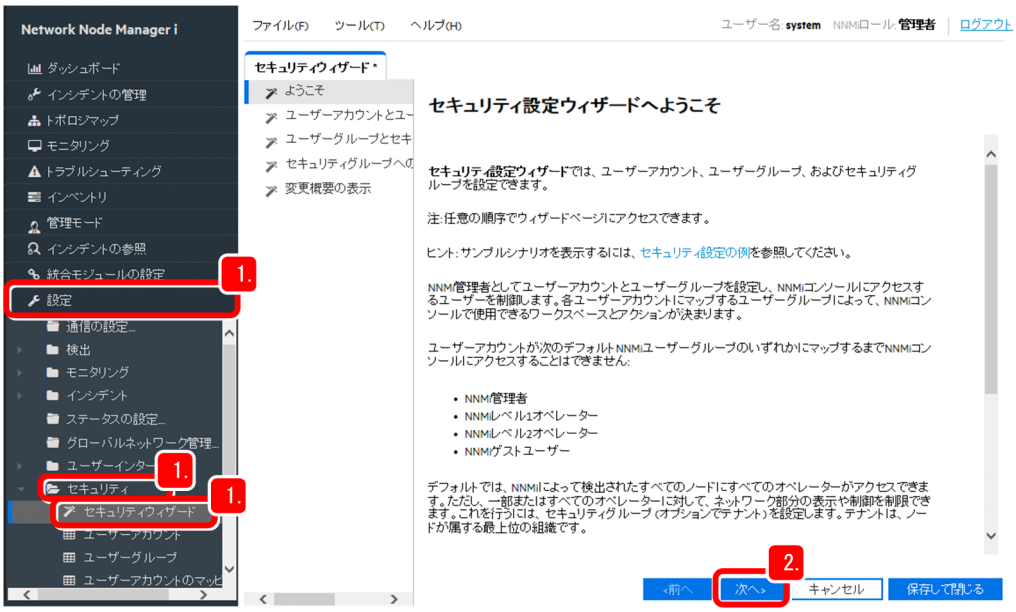
[ヘルプ] メニューを選択すると，操作中の画面に関連したトピックが表示されます。このトピックを参照すると，指定できる文字数や文字の種類など設定項目について知りたいことがすぐに確認できて便利です。

2.2.3　ユーザーを登録する

システム管理者と主任オペレーターのユーザーアカウントを作成して，ユーザーを登録しましょう。まずシステム管理者のユーザーアカウントを作成し，そのユーザーでサインインし直します。その後，主任オペレーターのユーザーアカウントを作成します。

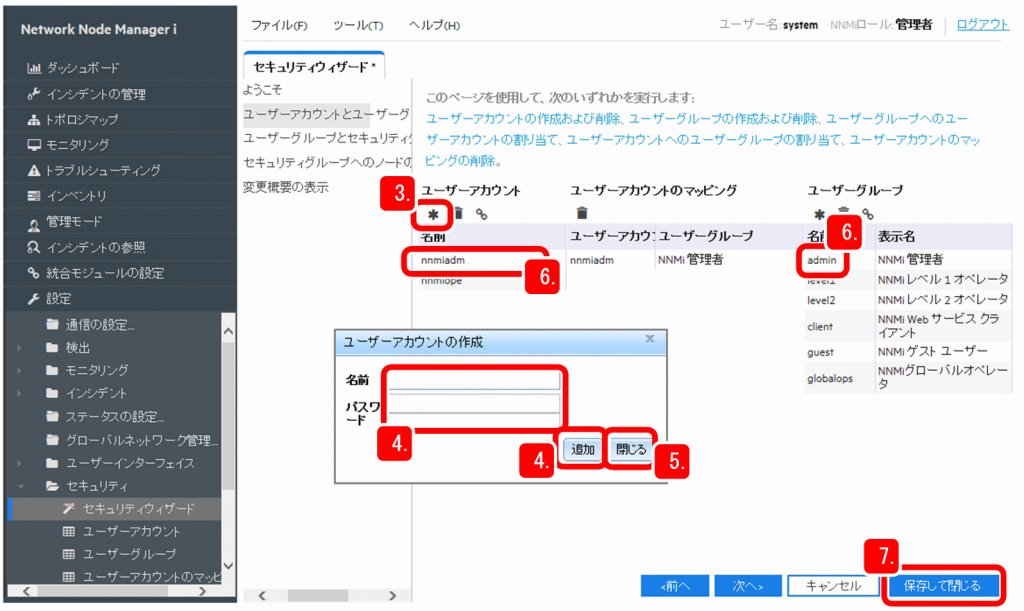
操作手順

1. [設定] ワークスペース－［セキュリティ］－［セキュリティウィザード］を選択します。



2. [セキュリティ設定ウィザードへようこそ] ビューの説明を読み，画面下の［次>］をクリックします。

3. ユーザーアカウント欄の ✱ （ユーザーアカウントの作成）をクリックします。



4. ユーザーの［名前］と［パスワード］を入力して［追加］をクリックします。

ユーザーアカウントが作成されます。

（例）

システム管理者　名前：nnmiadm，パスワード：password

主任オペレーター　名前：nnmiope，パスワード：password

5. ユーザーの追加が完了したら，［閉じる］をクリックします。

6. 作成したユーザーアカウントを選択し，対応づけたいユーザーグループをクリックします。

（例）

nnmiadm：システム管理者

nnmiope：主任オペレーター

7. ［保存して閉じる］をクリックします。

8. 確認ダイアログボックスで［OK］をクリックします。

ユーザーアカウントが設定されます。

メモ

パスワードを忘れた場合

ユーザーアカウントのパスワードの再設定については，NNMi ヘルプ「管理」の「ユーザーアカウントを設定する」の「ユーザー名とパスワードの変更」のトピックを参照してください。

システムアカウントのパスワードは，nnmchangesyspw.ovpl コマンドで再設定します。ユーザーアカウントのパスワードを変更する場合，［ファイル］メニュー－［パスワードの変更］で自ユーザーのパスワードを変更できます。

次の作業

これで，ユーザーを登録できました。［設定］ワークスペース－［セキュリティ］－［ユーザーアカウントのマッピング］を選択して，作成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しょう。

関連項目

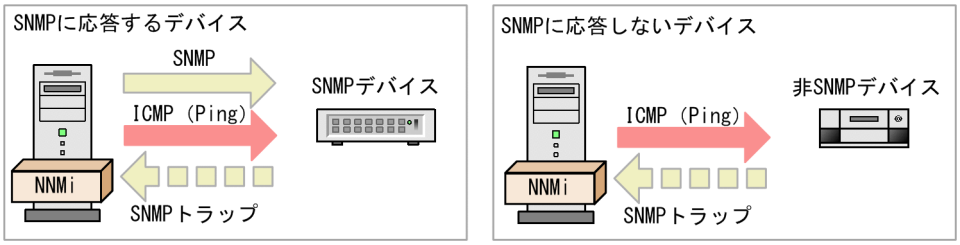
- 1.3.3　NNMi をセットアップする（Windows の場合）
- 1.4.3　NNMi をセットアップする（Linux の場合）
- 2.2.4　通信プロトコルを設定する

2.2.4　通信プロトコルを設定する

NNMi は SNMP と ICMP（Ping）を使ってデバイスの検出や監視を行い，SNMP トラップ（問題の通知）を受信します。

前提条件

デバイスは，SNMP に応答する SNMP デバイスと，SNMP に応答しない非 SNMP デバイスに分けられます。

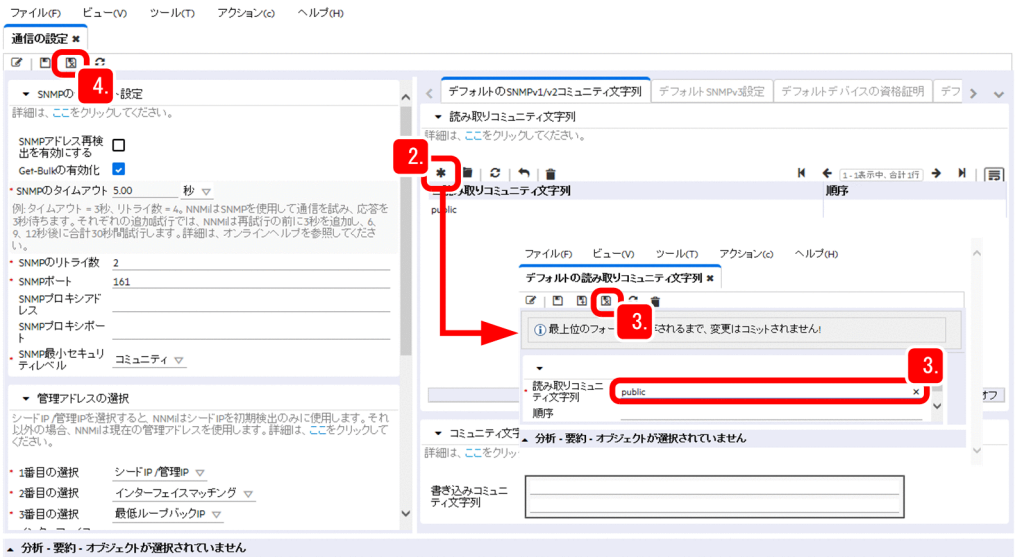


ここでは，NNMi がネットワークの検出や監視で使う通信プロトコル「SNMP」，「ICMP（Ping）」の動作を設定します。次の設定内容を例に説明します。必要に応じて，設定値を変更してください。

- 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（変更しない）
- SNMP 最小セキュリティレベル：デフォルト（変更しない）
- 読み取りコミュニティ文字列：public

操作手順

1. [設定] ワークスペース－［通信の設定］を選択します。
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。



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

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，手順 2.～手順 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] ビューで，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ます。

次の作業

これで，通信プロトコルを設定できました。次は，監視するネットワークを検出しましょう。

関連項目

- 2.2.5　ネットワークの検出

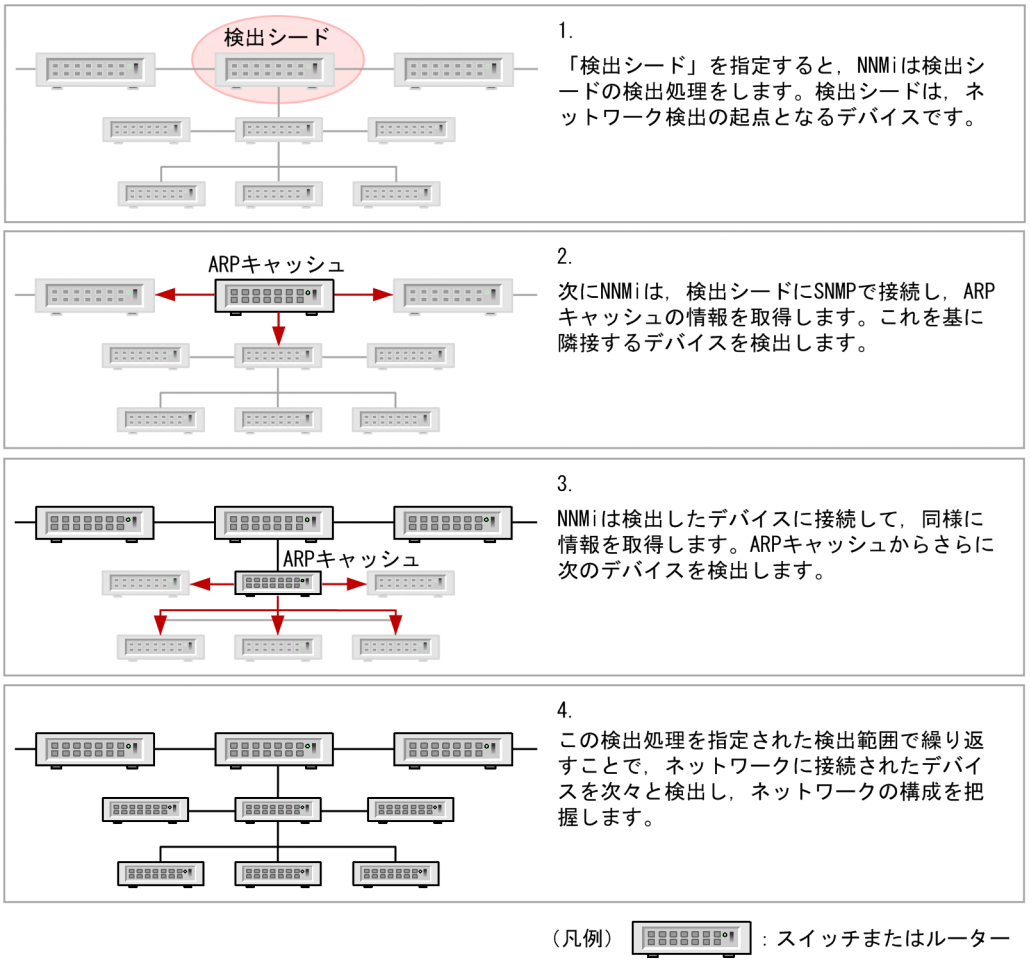
2.2.5　ネットワークの検出

NNMi は，ネットワーク上のデバイスの情報を収集し，個々のデバイスの詳細とネットワーク構成（トポロジ）を把握します。

(1)　ネットワークの検出とは

NNMi は，各デバイスの持つ ARP キャッシュ情報や LLDP などのプロトコルで認識した隣接デバイスの情報を，SNMP によって収集することでネットワーク全体を検出できます。

ここでは，ARP キャッシュによる検出を例に説明します。

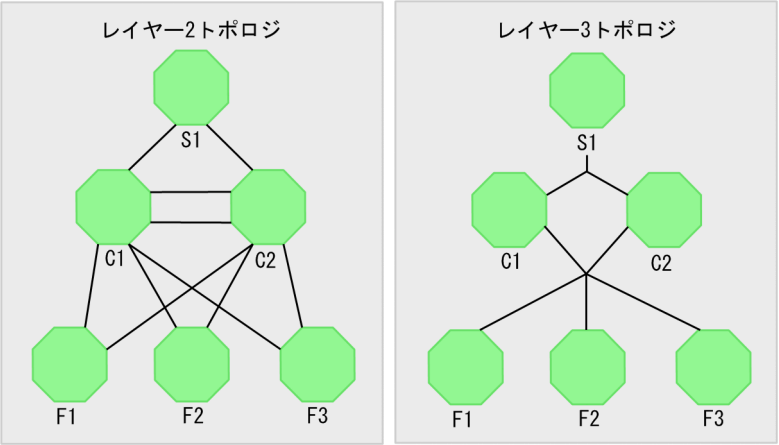


メモ

NNMi では，Ping スイープによる検出もできます。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。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ますが，ネットワークに負荷が掛かります。運用に応じて Ping スイープを使ってください。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。

(2) 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 トポロジでも認識して表示できます。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。



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 トポロジと併用することで，障害発生時の状況の確認や影響範囲が直感的に把握できます。

レイヤー 3 トポロジ

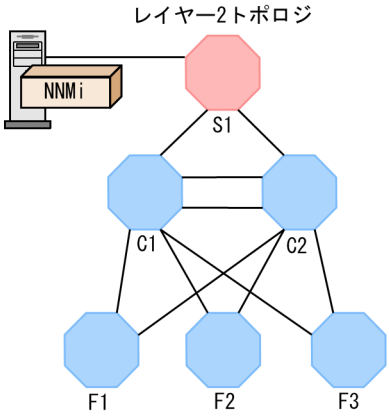
IP アドレスで論理的なネットワーク構成を表示します。

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。

> **ヒント**
>
> 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 アドレスによって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 アドレスによってネットワークのルート選択などを制御します。

IP ネットワークの通信や NNMi の設定作業では，宛先を IP アドレスで指定し，通常は物理的な結線を意識する必要はありません。NNMi は，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。

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 トポロジでの表示を次に示します。



IPアドレスでの通信（レイヤー3トポロジ）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ます。
しかし，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。

(3)　ネットワークの検出方法を設定する

監視するネットワーク上にあるネットワーク機器を検出します。ネットワークの検出は，監視エージェントの構築が完了してから，行ってください。

前提条件

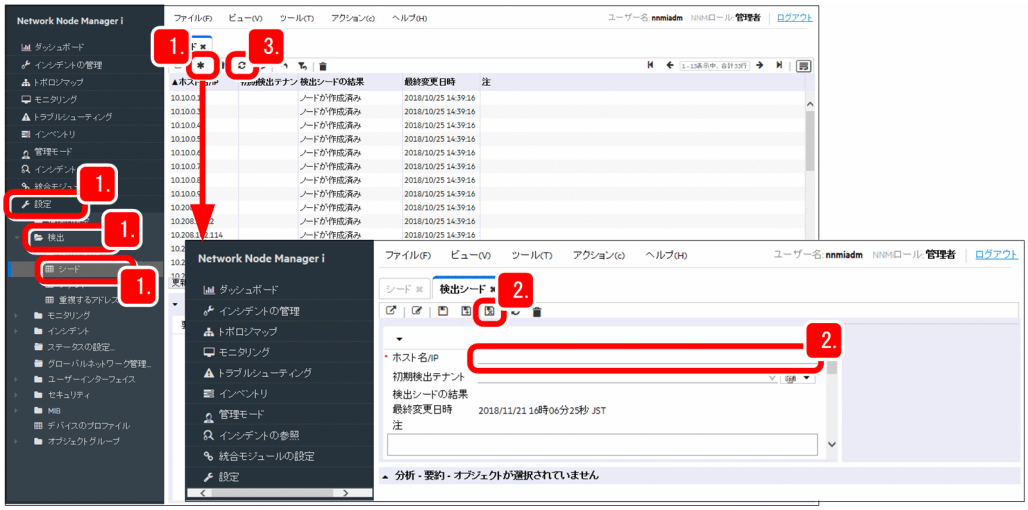
ネットワークの検出には，自動で検出する方法と明示的に指定する方法があり，これらの方法を組み合わせて設定することもできます。自動で検出する方法と明示的に指定する方法の説明と運用例を次に示します。

検出方法	説明	運用例
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

ここでは，明示的にネットワークを検出する方法について説明します。

操作手順

1. [設定] ワークスペース－ [検出] － [シード] をクリックし， （新規作成）をクリックします。



2.「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。

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。

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。

3. （リフレッシュ）をクリックします。

指定した検出シードが作成されたことを確認します。

メモ

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

（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

（例）nnmloadseeds.ovpl -f c:¥jp1¥seeds.txt

シードファイルの記入例

192.168.8.82 # node1

192.168.100.24 # node2

nnmloadseeds.ovpl コマンドについては，[ヘルプ] メニュー－ [NNMi ドキュメントライブラリ] － [リファレンスページ] － [nnmloadseeds.ovpl] のトピックを参照してください。

ヒント

自動で検出したい場合は，［設定］ワークスペース－［検出の設定］－［自動検出ルール］で設定します。［IP の範囲］を指定するときに，検出しない IP アドレス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 アドレスが検出対象外となります。

［検出の設定］－［除外対象 IP アドレス］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 アドレスが消える場合があるため，用途により使い分けてください。

自動検出の詳細については，マニュアル「NNMi セットアップガイド」の「自動検出ルールを設定する」のトピックを参照してください。

関連項目

- 1.2.4　各製品のコマンドの格納先

(4)　検出されたネットワークとデバイスを確認する

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。検出の設定をした直後は，ノードを検出していく過程を参照できます。

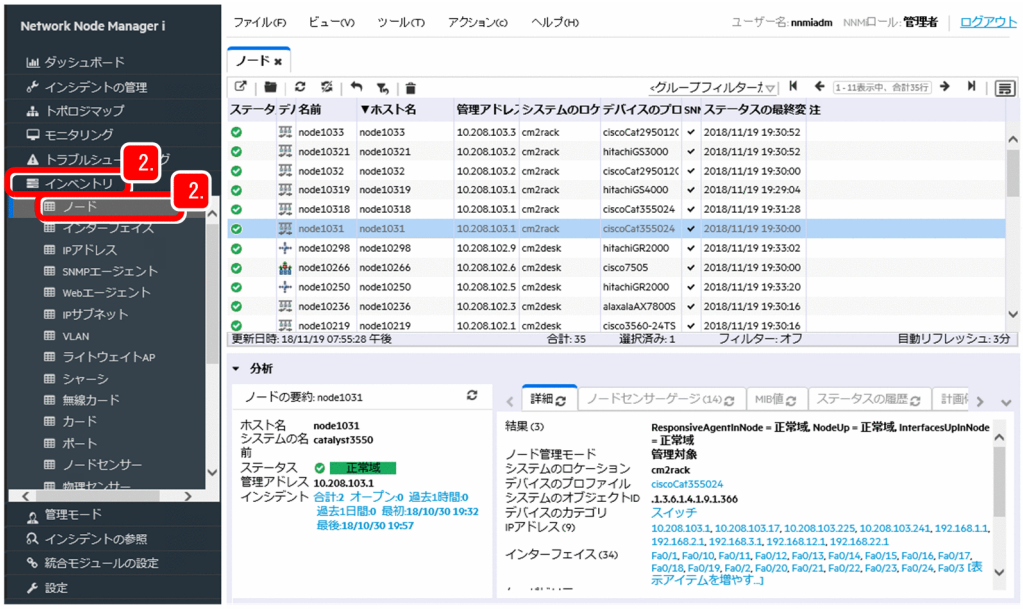
操作手順

1. ［トポロジマップ］ワークスペース－［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］ビューで，ネットワークの状態を確認します。

2. [インベントリ] ワークスペース－［ノード］をクリックします。

検出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。設定したデバイスが表示されていれば，ネットワーク検出は問題なく実施できています。

［デバイスの種類］や［デバイスのプロファイル］などを確認して，どんなデバイスが検出されているか確認しましょう。



ヒント

監視対象にクラスタシステムのノードが存在する場合は，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。

メモ

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方法と監視対象外にする方法があります。

監視対象から削除する方法

［トポロジマップ］ワークスペース－［ネットワークの概要］で，削除するノードのアイコンを選択して削除できます。ただし，検出シードとして指定されたノードは，ノードを削除しても［シード］ビューに表示される一覧からは削除されません。検出シードを削除してください。

監視対象外にする方法

［インベントリ］ワークスペース－［ノード］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。マップ上からはノードを消したくない場合や一時的に監視対象外にしたい場合などに使用します。

関連項目

- (5)　検出が完了した検出シードを削除する

(5)　検出が完了した検出シードを削除する

ネットワークの検出が完了したら，検出シードを削除します。

操作手順

1. [設定] ワークスペース－［検出］－［シード］をクリックします。
2. すべての検出シードを選択してから，　（削除）をクリックします。

   複数の行を選択するには，[Ctrl] キーを押しながら行をクリックします。
3. 検出シードが削除されたことを確認します。

次の作業

これで，ネットワークを検出できました。次は，ノードグループを設定しましょう。

関連項目

- 2.2.6　ノードグループの設定

2.2.6　ノードグループの設定

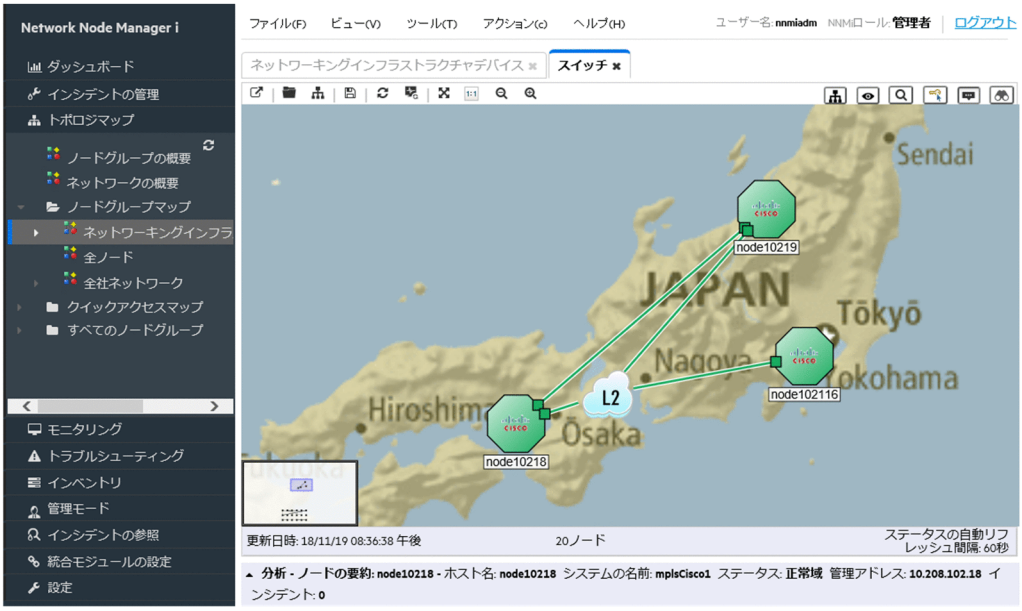
ノードグループを定義すると，ノードグループごとのモニタリングの設定やノードグループ単位でのフィルタリングができるようになります。また，NNMi コンソールの初期画面として任意のノードグループを表示することもできます。

(1)　ノードグループとは

ノードグループとは，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。NNMi では，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。ノードグループは，子ノードグループを定義することで 6 階層まで階層化できます。

また，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。

ノードグループマップ



ノードグループマップの背景図は，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。

「重要なノード」ノードグループの使い方

NNMi には，標準で「重要なノード」ノードグループが設定されています。この「重要なノード」ノードグループには，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，デバイスは「ノード停止(NodeDown)」インシデントが発行されます。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」に登録してください。

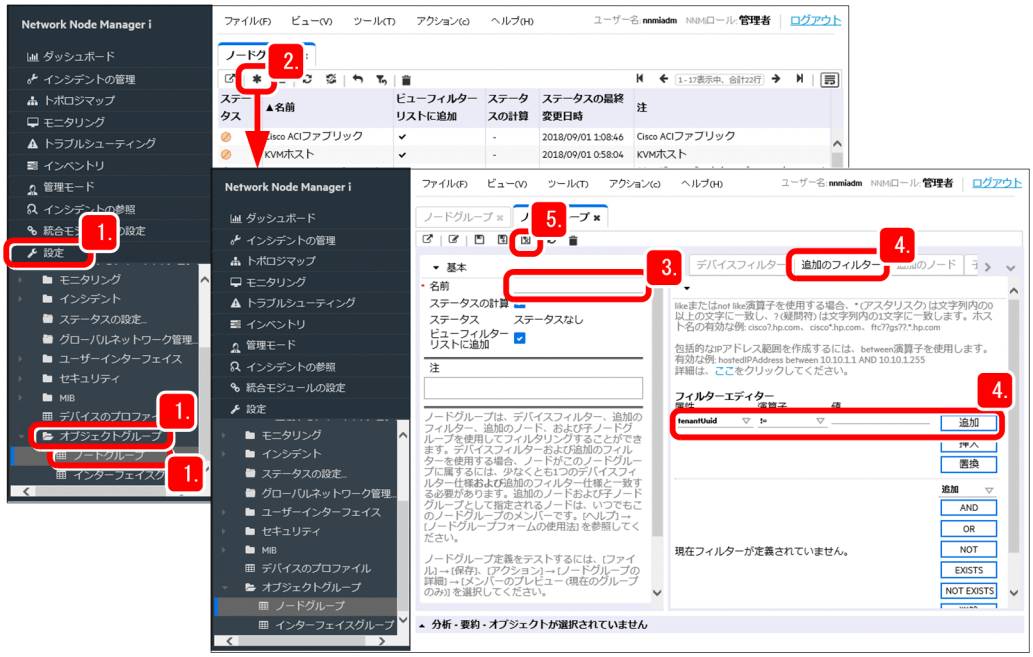
「重要なノード」ノードグループに，子ノードグループを階層化して設定した場合や，他ノードグループに含まれるノードを追加した場合でも，インシデントが発行されます。

(2)　ノードグループを設定する

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。ここでは，属性の値を指定してグループを設定する手順を説明します。

操作手順

1. [設定] ワークスペース－［オブジェクトグループ］－［ノードグループ］をクリックします。



2. ✱（新規作成）をクリックします。

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

［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］ビューや［インシデント］ビューの［<グループフィルターが空です>］に，作成するノードグループの名前が表示されます。

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］に追加されます。条件式を削除したい場合は，条件式を選択したあと，［削除］をクリックします。

ヒント

グループ化の条件は，IP アドレスの範囲，デバイスの種類，設置場所などを指定できます。SQL の演算子（between，in，like など）を使って柔軟な条件を設定することもできます。ノードグループは 6 階層までです。ノードグループは，次のように使用します。

- ノードグループ用のマップを定義する：［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する：［モニタリングの設定］－［ノードの設定］

- ノードグループ単位に性能監視する：[モニタリング] − [カスタムポーラー設定] − [カスタムポーラーポリシー]

5. （保存して閉じる）をクリックします。

[ノードグループ] ビューが閉じ，ノードグループが作成されます。

6. 作成したノードグループの行を選択し，右クリックで［ノードグループの詳細］ − ［メンバーの表示(子グループを含む)］をクリックします。

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。

7. 目的のノードグループを右クリックし，［マップ］ − ［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。

メモ

NNMi では，演算子を使った設定以外にも，さまざまなグループ化の条件を用意しています。グループ化の条件を設定するタブと運用例を次に示します。

設定するタブ	設定項目	運用例
[デバイスフィルター] タブ	• デバイスの種類 • ベンダー など	• 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，条件を絞り込んで素早く状況を把握する。
[追加のフィルター] タブ	• hostedIPAddress（IPアドレス） • sysLocation（場所） など	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。
[追加のノード] タブ	ホスト名	• 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。
[子ノードグループ] タブ	子ノードグループ（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。

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

操作手順

1. [設定] ワークスペース－［オブジェクトグループ］－［ノードグループ］をクリックします。

2. マップを設定したいノードグループを選択，右クリックでメニューを表示し，［マップ］－［ノードグループマップ］をクリックします。

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

4. 設定したいノードグループを［ノードグループ］プルダウンメニューから選択します。

5. [背景イメージ］タブで［背景イメージ］にマップの背景画像を設定します。

   ［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

   Web ブラウザで表示できる gif，png，jpg などが指定できます。画像ファイルは，監視マネージャーの次のフォルダに格納します。

   - Windows の場合

     インストール先データフォルダ¥shared¥nnm¥www¥htdocs¥images

   - Linux の場合

     /var/opt/OV/shared/nnm/www/htdocs/images

6. [トポロジマップ順序］を指定します。

   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［クイックアクセスマップ］フォルダに表示されるように設定できます。設定後，サインインし直すと表示されます。

7. [重要なインシデントを示す] をチェックします。

チェックすると，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。

8. 設定が終わったら （保存して閉じる）をクリックします。

9. アイコンの位置を調整したあと， （マップを保存）をクリックします。

アイコンの位置が保存されます。

次の作業

これで，ノードグループマップを設定できました。次は，モニタリング定義を設定しましょう。

関連項目

- 2.2.7　モニタリングの設定

2.2.7　モニタリングの設定

NNMi は，ネットワーク検出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。

(1)　モニタリングとは

モニタリングとは，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することです。NNMi は，SNMP や ICMP（Ping）によって監視対象のデバイスを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。

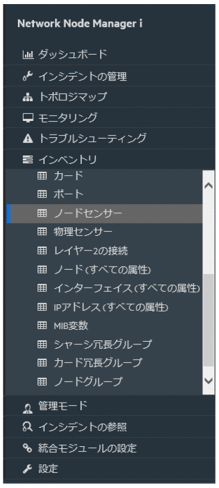
通信と検出およびモニタリングの設定と，通信プロトコル SNMP と ICMP（Ping）の関係を次に示します。

設定対象	説明	設定個所	設定項目	デフォルト値
プロトコルの動作	SNMP や ICMP（Ping）のプロトコルでの，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。	[設定] ワークスペース－［通信の設定］	SNMP	5 秒（リトライ数 2 回）
			ICMP（Ping）	
ネットワーク検出時の動作	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。	[設定] ワークスペース－［検出］－［検出の設定］	再検出間隔	1 日
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。ただし，監視負荷を適切にするため，分単位でポーリングする設定にします。	[設定] ワークスペース－［モニタリン	障害ポーリング周期	5 分

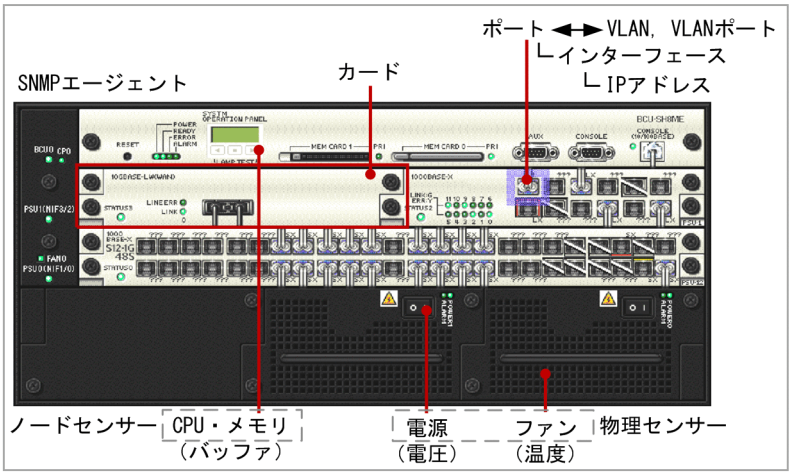
設定対象	説明	設定個所	設定項目	デフォルト値
ネットワーク状態を監視するときの動作	監視は，障害を迅速に検出するため短い周期にします。ただし，監視負荷を適切にするため，分単位でポーリングする設定にします。	グ］－［モニタリングの設定］	障害ポーリング周期	5 分

NNMi で監視できる項目は，［インベントリ］ビューに表示されます。NNMi の監視項目とデバイスとの対応を次に示します。

NNMiの監視項目の表示例



［ノード］：最も深刻な未解決の結果がステータスに反映されます。



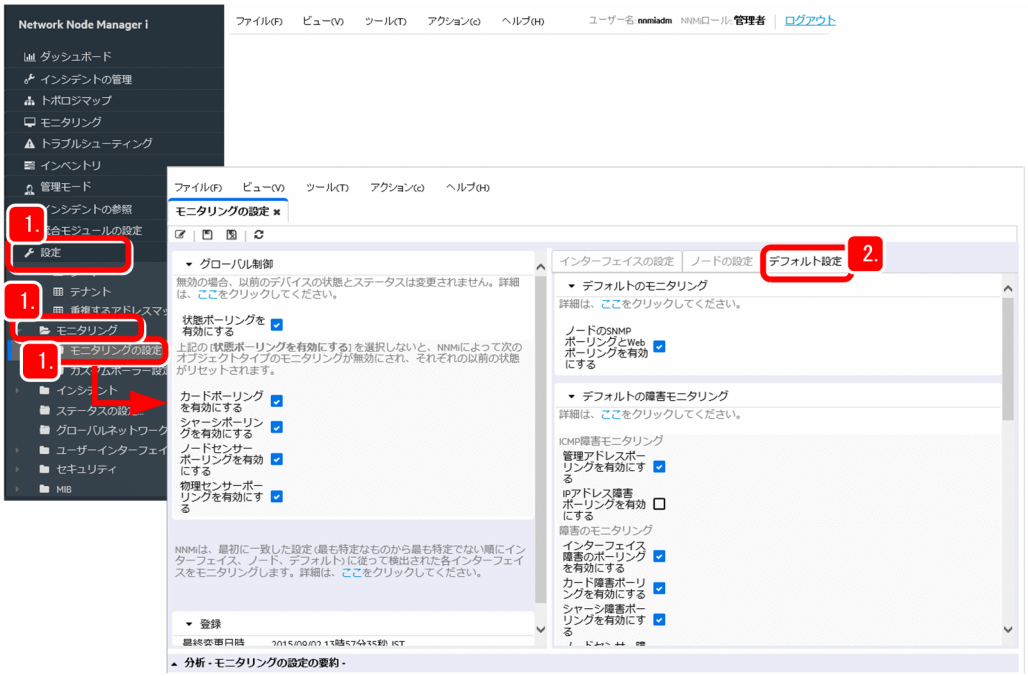
［インタフェース］，［SNMP エージェント］，［カード］，［ノードセンサー］，［物理センサー］ をSNMPで監視します。［IPアドレス］をICMP（Ping）で監視します。ほかの項目は，構成を管理する情報やグループ化した情報などです。

(2)　モニタリング定義を参照して監視方法を確認する

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。ここでは，監視の仕組みを理解するために，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

1. [設定] ワークスペース－［モニタリング］－［モニタリングの設定］を選択します。



2. [デフォルト設定] タブを選択します。

   モニタリングのデフォルトの設定が表示されます。

   何を監視する設定になっているか，監視間隔は何分間かなどを確認しましょう。

3. [インタフェースの設定] タブや［ノードの設定］タブを選択して，モニタリングの定義を参照します。

   ［ノードの設定］タブ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

4. モニタリング定義項目をダブルクリックします。

   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。

次の作業

これで，デフォルトのモニタリング定義を確認できました。次は，インシデントを設定しましょう。

関連項目

- (3)　モニタリング定義の設定項目
- 2.2.8　インシデントの設定

(3)　モニタリング定義の設定項目

NNMi には，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 を導入後，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。

監視方法は，［モニタリングの設定］ビューで設定できます。定義できる主なモニタリング定義項目について次に示します。

設定場所	モニタリング定義項目	説明
［グローバル制御］	状態ポーリングを有効にする	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

設定場所	モニタリング定義項目	説明
［グローバル制御］	カードポーリングを有効にする※	「カード」の状態を，SNMP で監視します。
	シャーシポーリングを有効にする※	「シャーシ」の状態を，SNMP で監視します。
	物理センサーポーリングを有効にする※	「物理センサー」の状態を，SNMP で監視します。
［デフォルト設定］タブ	管理アドレスポーリングを有効にする	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 アドレス障害ポーリングを有効にする	「IP アドレス」を，ICMP(Ping)で監視します。
	インタフェース障害のポーリングを有効にする	「インタフェース」の状態を，SNMP で監視します。
	カード障害ポーリングを有効にする※	「カード」の状態を，SNMP で監視します。
	シャーシ障害ポーリングを有効にする※	「シャーシ」の状態を，SNMP で監視します。
	物理センサー障害ポーリングを有効にする※	「物理センサー」の状態を，SNMP で監視します。
	障害のポーリング間隔	状態の監視を行う周期を指定します。
［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 デバイスだけでなく，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。
	非 SNMP デバイス	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。ICMP（Ping）でモニタリングするように設定されるため，死活監視ができます。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。

注※　カード，シャーシ，および物理センサーは，NNMi がサポートする特定の機種だけで監視できます。

2.2.8　インシデントの設定

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。

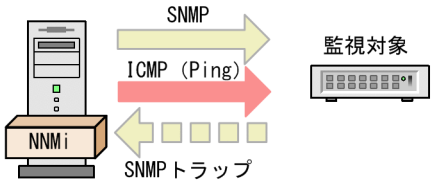
(1) インシデントとは

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基に根本原因解析をした結果，通知されます。

［管理イベント］インシデント
ネットワークを継続的に監視して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。



NNMi では，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［管理イベント］インシデントと［SNMP トラップ］インシデントなど約 150 種類の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，そのまま運用で使用できます。

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［管理イベント］インシデントに設定されています。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）

運用方法の一つとして，「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 のインシデントが発行されるため，これを監視します。

インシデントの発行例

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を次に示します。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。

ネットワーク運用での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。

機能	説明	参照先
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。	2.2.8(4)
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。トポロジマップとインシデントの参照で画面を切り替えながら，内容を確認できます。	3.1
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。	4.2

これらの機能を使用するために，インシデントを設定しましょう。

関連項目

- 2.2.6　ノードグループの設定
- (4)　インシデントに自動アクションを設定する
- 3.1　JP1 ネットワーク管理製品でのネットワーク監視
- 4.2　障害対応の仕組み

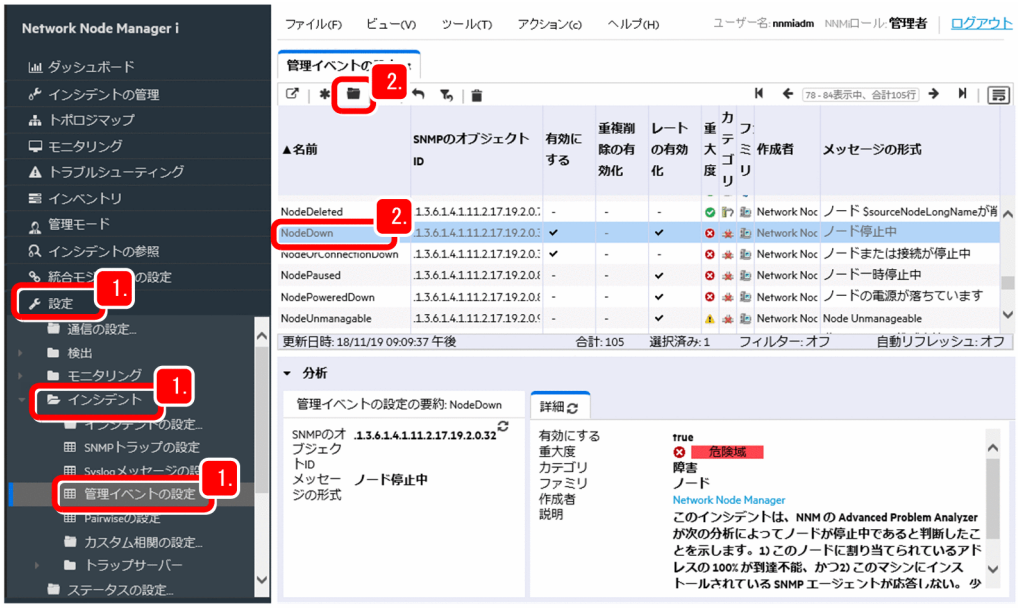
(2)　インシデント設定の内容を確認する

JP1 ネットワーク管理製品には，運用で使用する標準のインシデント設定があらかじめ設定されています。標準で提供されているインシデント設定を見て，基本的な項目を確認してみましょう。

操作手順

1. [設定] ワークスペース－［インシデント］－［SNMP トラップの設定］または［管理イベントの設定］をクリックします。

   SNMP トラップによるインシデントを確認する場合は［SNMP トラップの設定］を，NNMi がネットワーク監視時に検出したインシデントを確認する場合は［管理イベントの設定］を選択してください。



2. 参照したいインシデントの行をクリックして　（開く）をクリックします。

   インシデントの設定内容が表示されます。例えば，ノードダウンで発生する次の［管理イベント］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）

［説明］にインシデントの意味が表示されます。

インシデントの内容を確認し，理解を深めましょう。必要に応じて，SNMP トラップのインシデントを設定したり，インシデントに自動アクションを設定したりしてください。

(3) SNMP トラップのインシデントを設定する

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。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。NNMi のインストール時に標準で多くの MIB がロード済みです。ロード済み MIB の一覧は，［設定］ワークスペース－［MIB］－［ロード済み MIB］で参照できます。

前提条件

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。

- 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。

詳しくは，NNMi ヘルプ「管理」の「SNMP トラップを管理する」のトピックを参照してください。また，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，NNMi ヘルプ「管理」の「未解決の受信 SNMP トラップを管理する」のトピックを参照してください。

操作手順

1. NNMi の nnmloadmib.ovpl コマンドを実行します。

   指定例：`nnmloadmib.ovpl -load MIB ファイル名`

   MIB ファイルの内容が，NNMi にロードされます。-load オプションに，ロードする MIB ファイルを指定してください。

2. NNMi の nnmincidentcfg.ovpl コマンドを実行します。

   指定例：`nnmincidentcfg.ovpl -loadTraps MIB モジュール名`

   NNMi の MIB データベースからインシデント構成を作成します。

   -loadTraps オプションに，MIB ファイルに定義されている MIB モジュール名を指定してください。

3. ［設定］ワークスペース－［インシデント］－［SNMP トラップの設定］をクリックします。

   SNMP トラップの状況を確認できます。

メモ

SNMP トラップの状況は，nnmtrapdump.ovpl コマンドでも確認できます。

（例）

nnmtrapdump.ovpl -source IPaddr

IPaddr からの受信トラップを表示します。

nnmtrapdump.ovpl -t

受信トラップを連続表示します。設定時の確認などで使用します。

詳細は，ヘルプ「オペレータ用のヘルプ」の「[SNMP トラップ] ビュー」のトピックと，[ヘルプ] メニュー－［NNMi ドキュメントライブラリ］－［リファレンスページ］－［nnmtrapdump.ovpl］を参照してください。

メモ

MIB モジュール名は，MIB ファイルを開いてファイルの先頭付近を確認します。
「DEFINITIONS ::= BEGIN」の前に定義されている名前が MIB モジュール名です。

（例）

MIB モジュール名の例

------ MIB Simple Sample

SAMPLE-MIB DEFINITIONS ::= BEGIN

ここでは，SAMPLE-MIB が MIB モジュール名となります。

関連項目

- 1.2.4　各製品のコマンドの格納先

(4)　インシデントに自動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ときに，指定したコマンドを実行できます。

背景

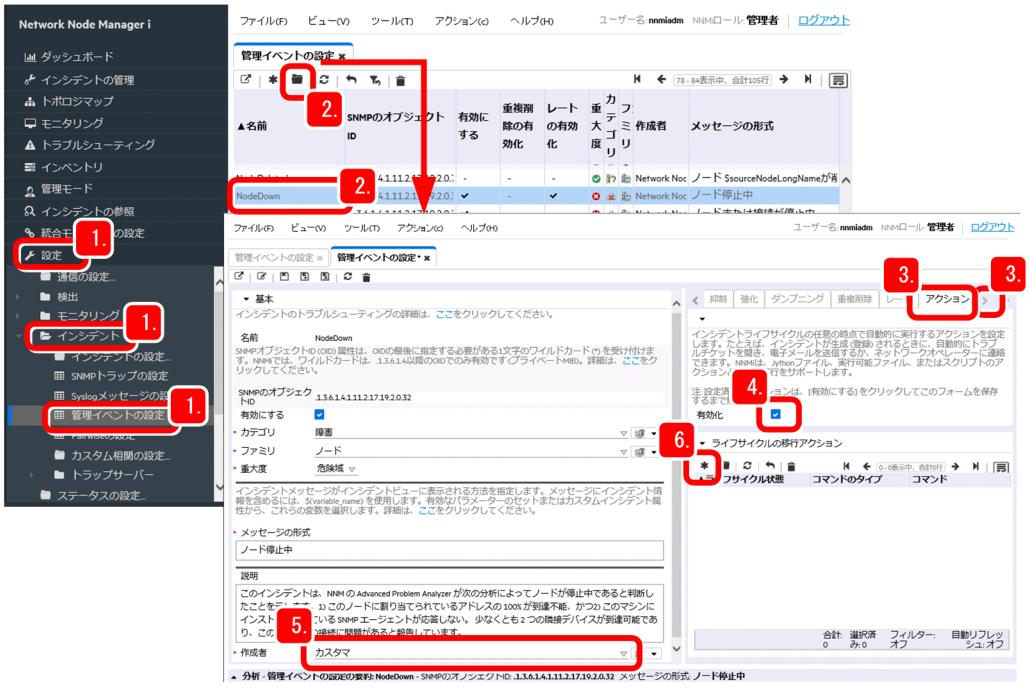
メモ

JP1/IM と連携すれば，障害発生時にメールを送信したり，パトランプを使用したりできます。

操作手順

1. [設定] ワークスペース－［インシデント］－［SNMP トラップの設定］または［管理イベントの設定］をクリックします。

   SNMP トラップによるインシデントに自動アクションを設定したい場合は［SNMP トラップの設定］を，NNMi がネットワーク監視時に検出したインシデントに自動アクションを設定したい場合は［管理イベントの設定］を選択してください。



2. 自動アクションを設定したいインシデントの行をクリックして （開く）をクリックします。

3. をクリックしてタブ表示を切り替え，［アクション］タブが表示されたらクリックします。

> **ヒント**
>
> 自動アクションの設定をノードによって変更したい場合は，設定を行うタブによって，ノードごとに条件を指定できます。
>
> - ［インタフェースの設定］タブの［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］タブの［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］タブ＞［ノードの設定］タブ＞普通の［アクション］タブの順です。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。そのため，ノード全般に自動アクションを設定し，特定のノードグループだけ別の自動アクションを実行するなどの運用ができます。

詳細は，NNMi ヘルプ「管理」の「インシデントの設定」のトピックを参照してください。

4. [有効にする] をチェックします。

この設定をしないと，インシデントが発生しても自動アクションが実行されません。

5. 作成者を「カスタマ」に設定します。

ユーザーがインシデントの設定を変更する場合は，作成者を「カスタマ」に変更する必要があります。

6. [アクション] タブの [ライフサイクルの移行アクション] で ✱ （新規作成）をクリックします。

7. 自動アクションが実行されるタイミングを [ライフサイクル状態] から選択します。

自動アクションを実行したいタイミングに応じて，次のように設定します。

- 登録済み：障害を検知し，インシデントが発行されたときに，自動アクションを実行します。
- 進行中：インシデントに担当が割り当てられたり，調査中になったりなどで，[ライフサイクル状態] が「進行中」になったときに，自動アクションを実行します。
- 完了：障害の対処が完了して，[ライフサイクル状態] が「完了」になったときに，自動アクションを実行します。
- 解決済み：障害が解決したことを NNMi が検知し，[ライフサイクル状態] が「解決済み」になったときに，自動アクションを実行します。例えば，「ノードが停止したあと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，「解決済み」を指定します。

8. [コマンドのタイプ] を選択します。

Jython コマンドを指定する場合は「Jython」，実行ファイルまたはバッチファイルを指定する場合は「ScriptOrExecutable」を選択します。

9. [コマンド] を入力します。

コマンドタイプ「ScriptOrExecutable」の場合，必要なパラメータが指定された OS 上で実行できるコマンドを入力します。

（設定例）

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

コマンドタイプ「Jython」の場合の入力方法については，NNMi ヘルプ「管理」の「インシデントのアクションを設定する」のトピックを参照してください。

10. （保存して閉じる）をクリックします。

11. [SNMP トラップの設定] ビューまたは［管理イベントの設定］ビューの （保存して閉じる）をクリックします。

設定内容が保存されます。

ヒント

自動アクションの実行状況は，［ツール］メニュー－［インシデントアクションログ］で確認します。また，次のログファイルでも確認できます。

- Windows の場合
  NNMi のインストール先データフォルダ¥log¥nnm¥incidentActions.*.*.log
- Linux の場合
  /var/opt/OV/log/nnm/public/incidentActions.*.*.log

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ましょう。詳細は，NNMi ヘルプ「管理」の「インシデントの設定」のトピックを参照してください。

次の作業

これで，インシデントに自動アクションを設定できました。次は，SSO にアクセスして，SSO の設定をしましょう。

関連項目

- 2.3　SSO の設定

2.3　SSO の設定

SSO では，リソース収集機能を使って，サーバやネットワーク機器の状態をきめ細やかにチェックできます。

2.3.1　SSO にアクセスする

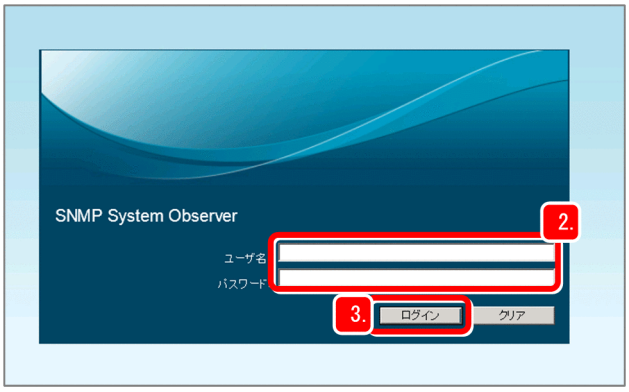
SSO にログインして，SSO の設定を始めましょう。

操作手順

1. Web ブラウザから SSO にアクセスします。
   http://**ホスト名:ポート番号**/SSOConsole/

   ホスト名は，監視マネージャーのホスト名を入力します。デフォルトのポート番号は「20393」です。

2. **ユーザー名**とパスワードを入力します。
   ユーザー名と**パスワード**は SSO の定義情報で設定した値を入力してください。



3. [ログイン] をクリックします。
   SSO コンソールが表示されます。

> **メモ**
>
> Windows の［スタート］メニューから［プログラムと機能］－［SNMP System Observer］－［SSO］を選択して表示することもできます。

次の作業

これで，SSO にログインできました。次は，SSO でリソースを収集するための設定をしましょう。

関連項目

- (2)　SSO の定義情報を NNMi に設定する
- 2.3.2　リソースの収集

2.3.2　リソースの収集

SSO では，システム上に存在する，SNMP をサポートする各種サーバ製品やネットワーク機器などからシステムリソースを収集できます。収集する時間帯，間隔，期間などを設定すると，定期的にリソースを収集し，参照できます。

(1)　リソース収集とは

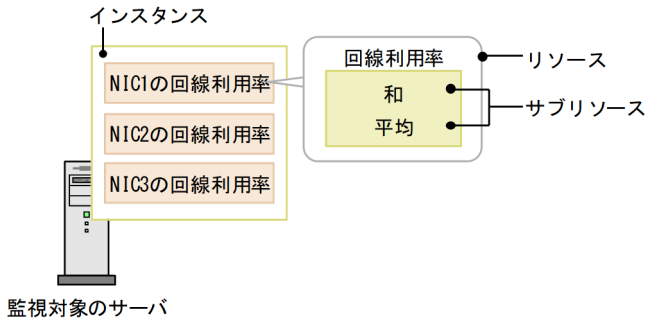
リソース収集とは，ネットワーク上のサーバのシステムリソースやユーザーが任意に設定した監視リソースを収集することです。

SSO では，OS（Windows や Linux）や SNMP をサポートする各種サーバ製品とネットワーク機器のシステムリソース（性能情報，統計情報，稼働情報）およびユーザーリソース（ユーザーが独自に定義できるリソース）を収集し，リアルタイムに監視できます。例えば，NIC の回線利用率が 90%を超えたら，インシデントを発行するなどの監視ができます。インシデント発行と合わせて，任意のアクションを自動的に実行することもできます。

収集対象のリソースを設定する場合，収集対象の候補は SSO にあらかじめ登録されているため，GUI に表示されたリソースから選択するだけで簡単に設定できます。収集の開始および終了をコマンドで実行できるため，操作を自動化することもできます。

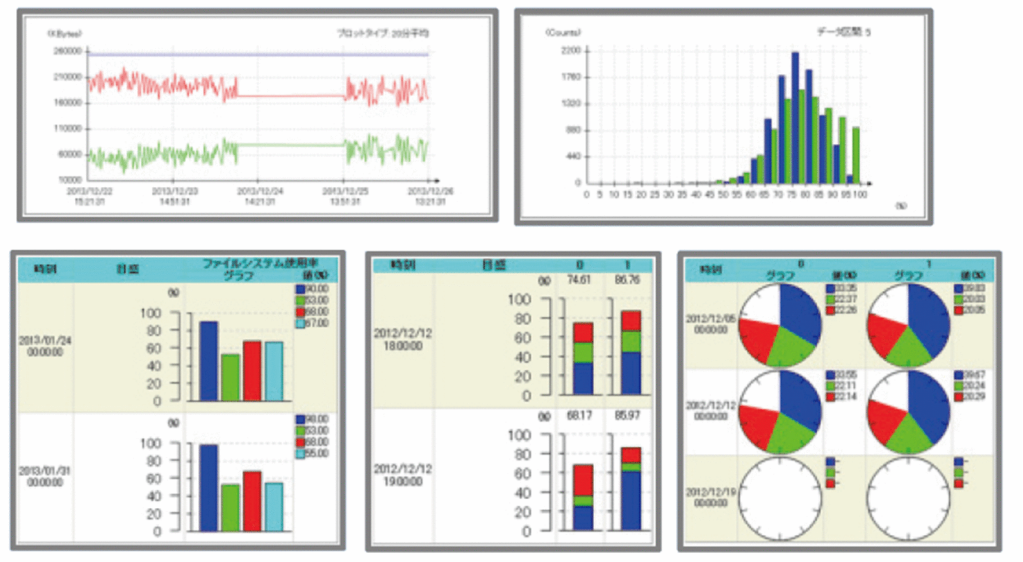
ヒント

SSO のリソース収集機能では，リソース収集元の実体をインスタンス，SNMP エージェントから取得できるリソースの最小項目をサブリソース，複数のサブリソースをグループ化したものをリソースと定義しています。



メモ

収集したリソースで，月単位や時間単位など任意の期間でレポートを作成できます。レポートを確認すれば，SNMP をサポートする各種サーバ製品やネットワーク機器などの動作傾向が把握できるため，システム運用の計画を立てやすくなります。レポートは，CSV 形式，または HTML 形式で出力できます。さまざまな形式のグラフが選択できるため，用途に合ったレポートを出力できます。



関連項目

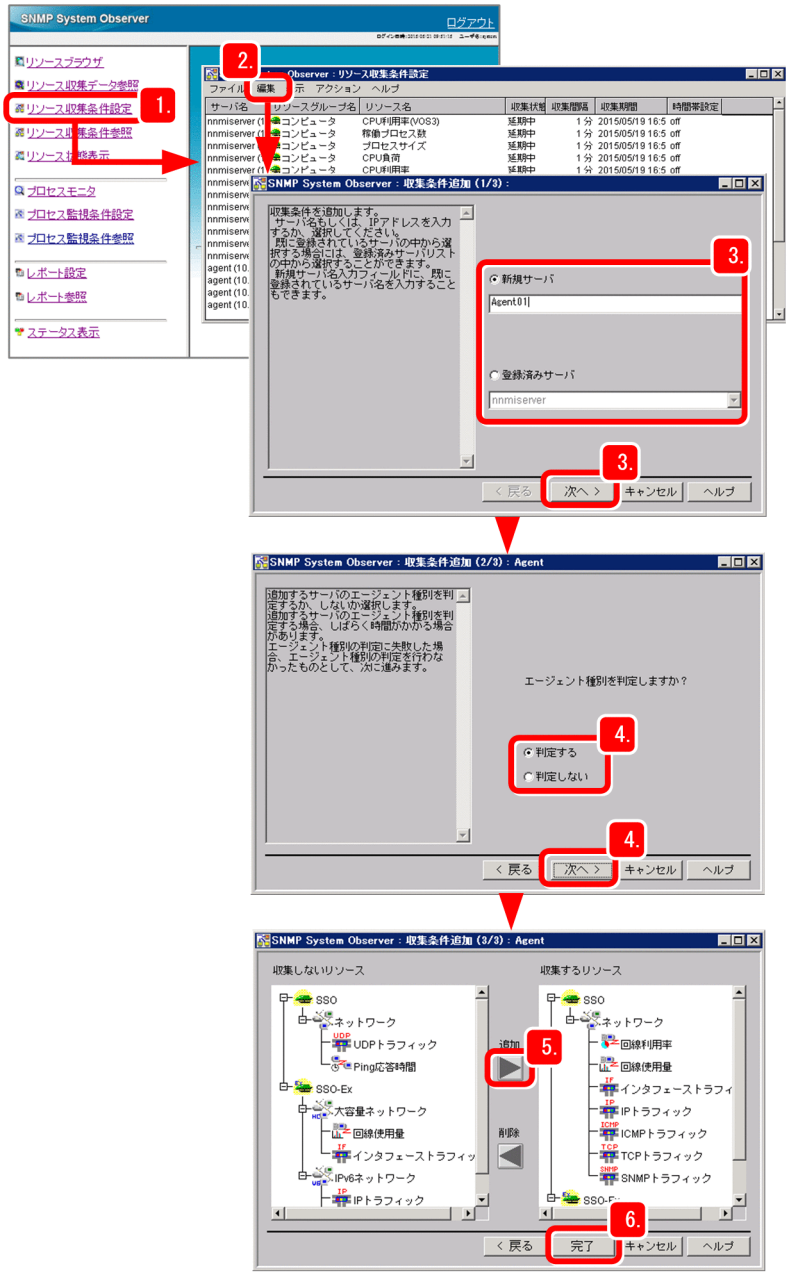
- マニュアル「JP1/SNMP System Observer」の「リソース一覧」のトピック

(2)　リソース収集を開始する

SSO でリソースを収集するための設定をして，リソース収集を開始します。

操作手順

1. SSO コンソールで［リソース収集条件設定］をクリックします。



2. ［編集］－［収集条件追加］を選択します。

3. 監視対象のサーバを選択し，［次へ］をクリックします。

［新規サーバ］で監視対象を直接指定するか，［登録済みサーバ］ですでに登録されている監視対象の中から選択します。

4. 監視対象のサーバのエージェント種別を自動判定するかどうかを選択し［次へ］をクリックします。

収集できるリソースは，エージェント種別によって異なります。［収集条件追加（2/3)］ウィザードで［判定する］を選択すると，［収集条件追加（3/3)］ウィザードでエージェント種別に応じて収集できるリソースだけが表示されます。

5. 収集対象とするリソースを［収集しないリソース］から選択し，［追加］をクリックします。

［収集するリソース］に選択したリソースが追加されます。

6. ［完了］をクリックします。

収集対象とするリソースが設定されます。

7. 収集条件を設定したいリソースを選択し，［編集］－［収集条件変更］を選択し，インスタンス名，サブリソース名，収集モードを選択します。

収集条件を設定しない場合は，すべてのインスタンスが収集の対象となります。収集モードでは，収集したデータを保存するか，およびしきい値を監視するかを設定できます。しきい値を監視する場合は，しきい値としきい値を超えた場合に実行するコマンドも設定します。

8. ［OK］をクリックします。

リソース収集条件が設定されます。

9. ［編集］－［収集時間帯設定］を選択します。

リソースの収集時間帯は，毎日決まった時間帯にリソースを収集したい場合に設定します。

10. 時間帯を指定したい番号のチェックボックスをチェックし，開始時刻および終了時刻を指定します。

例えば，毎日 8：00 から 18：00 の間にリソースを収集したい場合は，開始時刻に「08：00：00」，終了時刻に「18：00：00」を指定します。

11. ［OK］をクリックします。

リソースの収集時間帯が設定されます。

ヒント

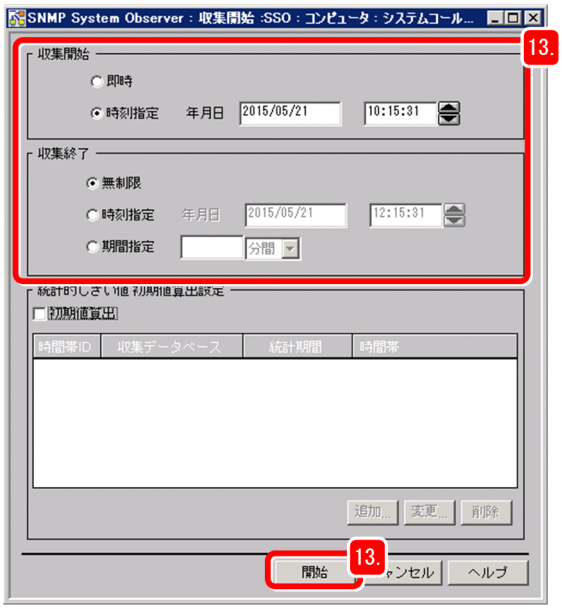
用途に応じて収集間隔を設定することもできます。収集間隔を設定すると，システムの負荷を軽減できます。収集間隔は，［編集］－［収集間隔変更］で設定します。

- リソースの使用量・使用率の急騰を検知したい場合は，収集間隔を短く設定します。
- リソースの使用状況を長期的に監視したい場合は，収集間隔を長く設定します。

12. ［アクション］メニューー［収集開始］を選択します。

13. 収集開始および収集終了で収集する期間を設定し，［開始］をクリックします。

リソース収集が開始されます。



収集時間帯を設定した場合は，［収集開始］ウィンドウの収集開始と収集終了の期間に収集時間帯が含まれるように設定してください。

メモ

- リソースの収集を手動で終了したい場合は，［リソース収集条件設定］ウィンドウから収集を終了したいリソースを選択し，［アクション］メニュー－［収集終了］を選択してください。
- リソースの収集状態を知りたい場合は，［リソース収集条件設定］ウィンドウの収集状態を確認してください。現在の収集状態が［未収集］，［収集中］，［収集完了］などで表示されます。

操作結果

これで，リソースの収集が開始されました。収集したリソースを参照したり，レポートに出力したりして，リソースの監視を始めます。

関連項目

- 3.1.4　リソースを監視する

3 JP1 ネットワーク管理製品での日常運用

JP1 ネットワーク管理製品がネットワークの定期的な監視を開始しました。ネットワーク全体の状況を把握するマップ画面や収集したリソースを表示して，ネットワーク監視を始めましょう。また，ネットワーク管理を継続的に行うために，定期的にメンテナンス作業を行ってください。

3.1　JP1 ネットワーク管理製品でのネットワーク監視

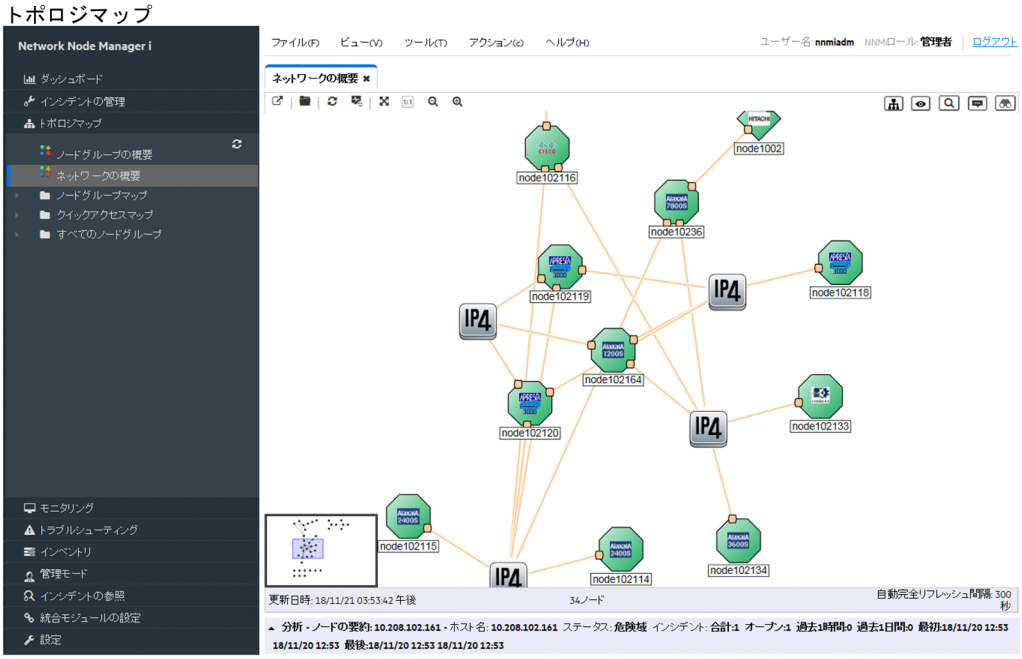
3.1.1　ネットワーク監視の種類

JP1 ネットワーク管理製品でのネットワーク監視の方法は幾つかあります。ここではマップ画面をベースに運用する方法とリソースを確認する方法を紹介します。

(1)　トポロジマップでの監視（NNMi）

NNMi では，検出したネットワーク機器を基に，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



トポロジマップでは，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，アイコンの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。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るので，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。

関連項目

- 3.1.3　ネットワークの監視を始める

(2)　リソース監視（SSO）

SSO では，OS（Windows，Linux）や SNMP をサポートする各種サーバ製品とネットワーク機器のシステムリソース（性能情報，統計情報，稼働情報）やユーザーリソース（ユーザーが独自に定義できるリ

ソース）を収集し，リアルタイムに監視できます。例えば，回線利用率が 90%を超えたらインシデントを発行するなどの監視ができます。

インシデント発行と合わせて，任意のアクションを自動的に実行することもできます。

関連項目

- 3.1.4　リソースを監視する

3.1.2　ポーリングとは

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。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。

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。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るため，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。

メモ

ポーリングには大きく分けて 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，目的や状況によって次のように表記されています。

検出のためのポーリング

- 検出ポーリング
  ［アクション］メニュー－［ポーリング］－［設定のポーリング］で即時ポーリングできます。
- 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（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）
  ［アクション］メニュー－［ポーリング］－［ステータスのポーリング］で即時ポーリングできます。
- 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）

3.1.3　ネットワークの監視を始める

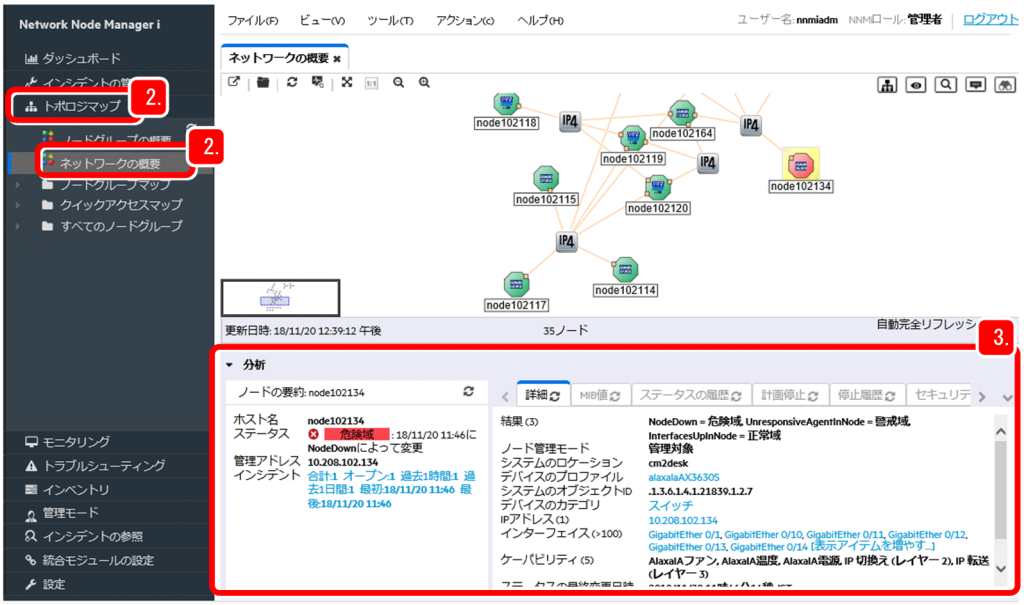
ネットワーク構成のマップ画面（トポロジマップ）を表示してネットワークを監視する方法を紹介します。ネットワークの監視は，NNMi で行います。例えば，運用管理センターなどでは，最も重要なマップを大型ディスプレイに常時表示して監視するなどの運用が行われます。検出の設定をした直後はノードを検出していく過程を参照できます。

前提条件

ネットワークの監視を始める前に，監視業務を行う担当者（オペレーター）をユーザーに登録しておきましょう。

操作手順

1. NNMi コンソールにアクセスします。
2. [トポロジマップ] ワークスペース－ [ネットワークの概要] をクリックします。



3. アイコンの色や詳細から，ノードの状態を確認します。

   マップ上のアイコンを選択すると，画面下の［分析］ペインに詳細が表示されます。［分析］ペインは， ▾ をクリックすると，表示／非表示を切り替えできます。

> **ヒント**
>
> ノードが持つ MIB 情報を確認したい場合は，nnmsnmpwalk.ovpl コマンドを使用して確認できます。

アイコンの色と意味

［設定］ワークスペース－［デバイスのプロファイル］に登録された 6,000 種類以上のデバイス情報によってデバイスの種類が自動判定されます。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）によって，マップ上でのアイコン形状が決められます。マップでのアイコンの色と意味を次に示します。

アイコンの色	意味	アイコンの色	意味
緑	正常域	赤	危険域
水色	注意域	青色	認識不能

アイコンの色	意味	アイコンの色	意味
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

アイコンの詳細については，ヘルプ「使用」の「マップの記号について」のトピックを参照してください。

メモ

メンテナンス中は監視を一時停止したい場合

トポロジマップなどでノードを選択し，［アクション］－［管理モード］－［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。nnmmanagementmode.ovpl コマンドで管理モードをサービス停止中にすると，監視を停止できます。

監視を再開する場合

トポロジマップなどでノードを選択し，［アクション］－［管理モード］－［管理］にすると，監視が再開されます。また，nnmmanagementmode.ovpl コマンドで管理モードを管理対象にすると，監視を再開できます。

非管理対象にしたノードを一覧表示する場合

［管理モード］ワークスペース－［管理対象外ノード］を参照します。

ヒント

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。［設定］ワークスペース－［ユーザーインタフェース］－［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でタイムアウト時間を設定できます。デフォルトは 18 時間です。

なお，URL を指定して開いた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 を指定してください。

- 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※

注※　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

また，トポロジマップとインシデント画面など，複数の画面を開いて監視したい場合は，  （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。また，URL を入力して画面を開いても複数の画面が表示できます。

ヒント

サインインしたときの初期画面を設定したい場合は，［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。インシデントを見たいときは，「重要な未解決インシデント」，マップを見たいときは，「ネットワークの概要」などのように指定します。なお，ユーザーが作成したノードグループマップも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［トポロジマップ順序］を調整してください。詳細は，NNMi ヘルプ「管理」の「NNMi ユーザーインターフェイスの設定」を参照してください。

次の作業

これで，トポロジマップを表示できました。ネットワーク監視を始めましょう。

関連項目

- 2.2.3　ユーザーを登録する

3.1.4　リソースを監視する

監視対象のリソースを参照します。リソースの監視は，SSO で行います。

前提条件

リソース収集条件を設定してください。

操作手順

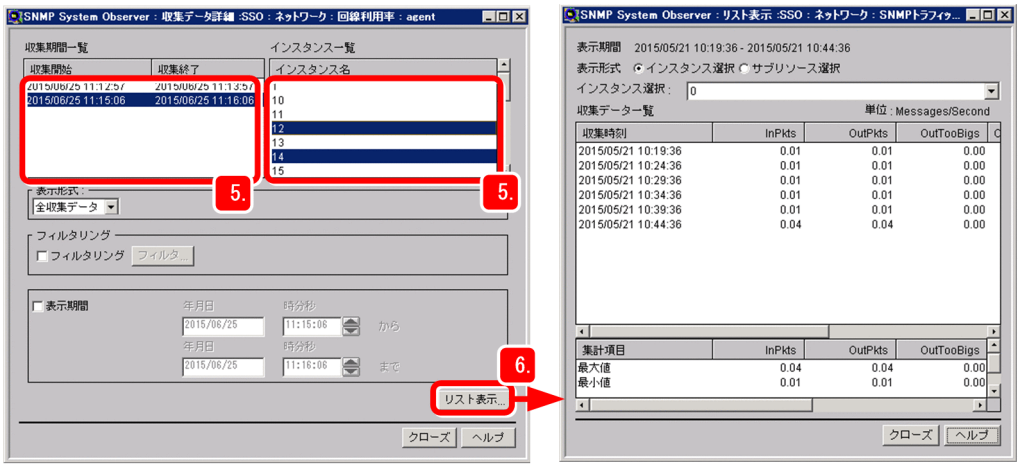
1. NNMi コンソールにアクセスします。
2. ［トポロジマップ］ワークスペース－［ネットワークの概要］をクリックします。
3. リソースを参照したいサーバを選択し，［アクション］メニュー－［SNMP System Observer］－［リソース収集データ参照］をクリックします。

ヒント

 （検索）をクリックすると，参照したいサーバ名を検索できます。

4. 参照したいリソースを選択し，［表示］ − ［収集データ詳細］を選択します。

5. 参照したい期間とインスタンスを「収集期間一覧」と「インスタンス一覧」からそれぞれ選択します。



6. ［リスト表示］をクリックします。

収集データの一覧を参照できます。

> **ヒント**
>
> ［リソース収集データ参照］ウィンドウでは，収集したリソースのデータをコピーおよび削除できます。
>
> 例えば，問題のある期間のリソースだけをコピーして残しておき，それ以外の不要なリソースを削除すれば，データベースの空き容量を確保できます。

次の作業

これで，収集したリソースを参照できました。必要に応じて，収集したリソースをレポートに出力するなどして，サーバの動作傾向を把握し，システム運用の計画を立ててください。

> **メモ**
>
> 収集対象のリソースをレポートに出力できます。レポート出力は，SSO コンソールの［レポート参照］から出力できます。レポートを出力するには，あらかじめレポート設定が必要です。レポート出力の詳細については，マニュアル「JP1/SNMP System Observer」の「レポート設定ウィンドウ」のトピックを参照してください。

関連項目

- 2.3.2　リソースの収集
- マニュアル「JP1/SNMP System Observer」の「収集条件コピーウィンドウ」のトピック

3.2 JP1 ネットワーク管理製品の定期メンテナンス

ネットワーク管理を継続的に行うためには，日頃のメンテナンス作業が大切です。ここでは，JP1 ネットワーク管理製品の運用作業について説明します。

3.2.1 NNMi の稼働状態を確認する

ネットワークを管理するためには，まず NNMi が正常に稼働している必要があります。NNMi が正常に稼働していることを確認しましょう。

操作手順

1. [ヘルプ] メニューー [システム情報] をクリックします。
2. [製品] タブの「ステータス」を確認します。
   ステータスが「正常域」になっていることを確認します。
3. [ヘルス] タブで NNMi の詳細な状態を確認します。
4. [ステートポーラー] タブで稼働状態を確認します。
5. [データベース] タブで検出したオブジェクトの数などを確認します。

操作結果

NNMi が正常に稼働していることを確認できました。

> **ヒント**
>
> NNMi 自体に問題が発生した場合は，NNMi コンソール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，［インシデント］の「カスタム属性」で確認してください。

関連項目

- NNMi ヘルプ「管理」の「NNMi 稼働状態をチェック」のトピック

3.2.2 NNMi 設定をエクスポートまたはインポートする

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，変更管理したりすることは，運用の重要な作業です。NNMi では，システムの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シス

テム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の運用が行えます。

操作手順

1. nnmconfigexport.ovpl コマンドまたは nnmconfigimport.ovpl コマンドを実行します。
   nnmconfigexport.ovpl コマンドと nnmconfigimport.ovpl コマンドの実行例を次に示します。

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

操作結果

NNMi 設定をエクスポートまたはインポートできました。

関連項目

- 1.2.4　各製品のコマンドの格納先
- NNMi ヘルプ「管理」の「構成設定をエクスポートまたはインポートする」のトピック

3.2.3　NNMi をバックアップまたは復元する

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，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。

操作手順

1. nnmbackup.ovpl コマンドまたは nnmrestore.ovpl コマンドを実行します。
   nnmbackup.ovpl コマンドと nnmrestore.ovpl コマンドの実行例を次に示します。

目的	コマンド
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-20150922002454」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-20150922002454

操作結果

NNMi をバックアップまたは復元できました。

関連項目

- 1.2.4　各製品のコマンドの格納先
- NNMi ヘルプ「管理」の「バックアップと復元」のトピック

3.2.4　NNMi のインシデントをアーカイブまたは削除する

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。また，データ件数が増加して性能に影響を与えないように，アーカイブとして保存したり，自動的に古いものを削除（トリム）したりできます。

(1)　SNMP トラップインシデントの件数を確認する

SNMP トラップインシデントの件数を確認します。

操作手順

1. [インシデントの参照] ワークスペース－［SNMP トラップ］を開きます。
   インシデント一覧表示の下の「合計」に件数が表示されます。

操作結果

SNMP トラップインシデントの件数が確認できました。

メモ

SNMP トラップインシデントの件数が上限に近づくと，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

関連項目

- NNMi ヘルプ「管理」の「インシデントをアーカイブまたは削除する」のトピック

(2)　自動トリム機能を有効化する

自動トリム機能を有効化すると，SNMP トラップインシデントの数が指定値を超えると，自動的に古いものを削除（トリム）したり，トリム時にアーカイブを自動作成したりできます。自動トリム機能は，新規インストール環境では，デフォルトで有効になっています。有効にして運用することをお勧めします。

関連項目

- マニュアル「NNMi セットアップガイド」の「古い SNMP トラップインシデントを自動でトリムす る」のトピック

3.2.5 SSO の収集データを定期削除する

SSO の収集データベースは，保存期間がなく単調増加します。そのため，収集を続けるとデータベースが肥大化し，データベースの収集や削除の性能が著しく低下することがあります。収集データベースの性能を保つために，データベースを定期的にバックアップしたり，削除したりすることをお勧めします。収集データの保存期間は，最大で 1 年にする運用にしてください。

操作手順

1. ssodbdel コマンドを実行します。

   保存期間を過ぎた収集データを削除するコマンドの実行例を次に示します。

   ssodbdel -all -stop BMONTH 13

   このコマンドを実行すると，保存期間 1 年を過ぎた収集データベースのデータが削除されます。このコマンドを毎月の初日に実行することで，収集データベースには 1 年間分のデータだけが保存された状態になります。

操作結果

SSO の収集データを削除できました。

関連項目

- 1.2.4 各製品のコマンドの格納先
- マニュアル「JP1/SNMP System Observer」の「ssodbdel」のトピック

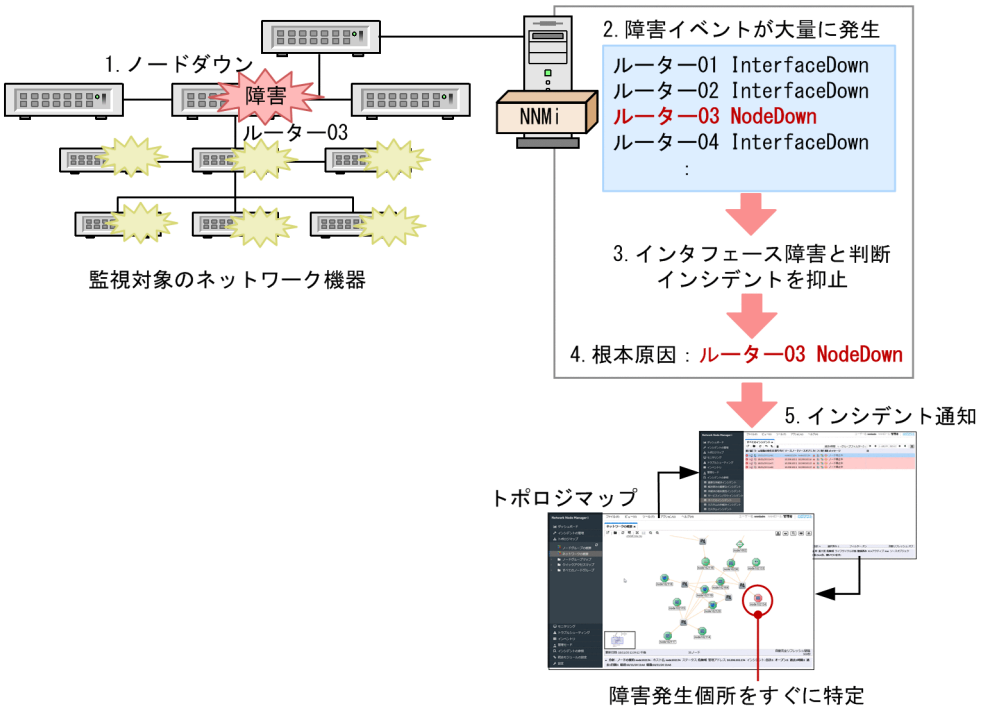
4 JP1 ネットワーク管理製品での障害対応

JP1 ネットワーク管理製品のインシデント管理を利用して，障害を迅速に特定・解決しましょう。

4.1　障害の根本原因の解析

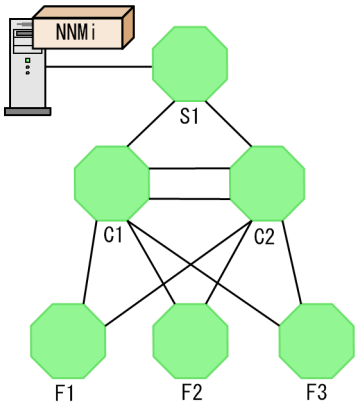
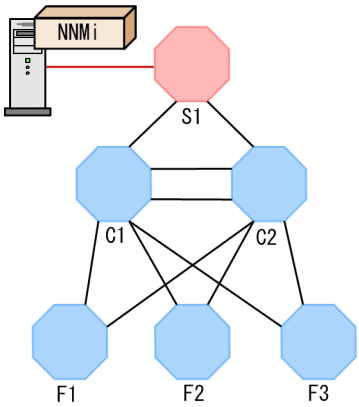
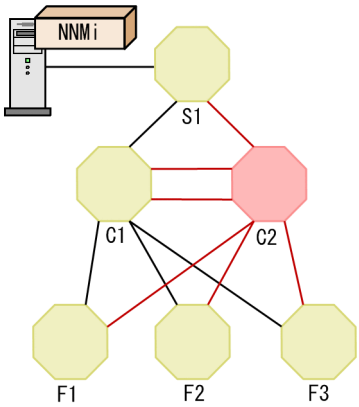
監視マネージャーは障害発生時に，根本原因解析機能によって，大量に発生するイベントの相関関係を調査し，フィルタリングします。レイヤー 2 トポロジおよびレイヤー 3 トポロジに基づいた障害の解析によって，根本原因を特定し，インシデントとして通知します。インシデントの対応の進行状況（ライフサイクル状態）を問題発生から解決まで管理します。

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。



1. ルーター 03 でノードダウンが発生すると，ルーター 03 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。
2. 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。
3. 監視マネージャーは，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します。
4. 近隣ノードでの通信断の状況を基に，ルーター 03 のノードダウンが根本原因と判断します。インタフェース障害はその影響と判断し，ルーター 03 で発生したノードダウンと関連づけます。
5. 根本原因のインシデントとしてルーター 03 のノードダウンが通知されます。

また，監視マネージャー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して，根本原因を解析します。レイヤー 2 トポロジのネットワーク構成を使った根本原因解析の例について次に示します。

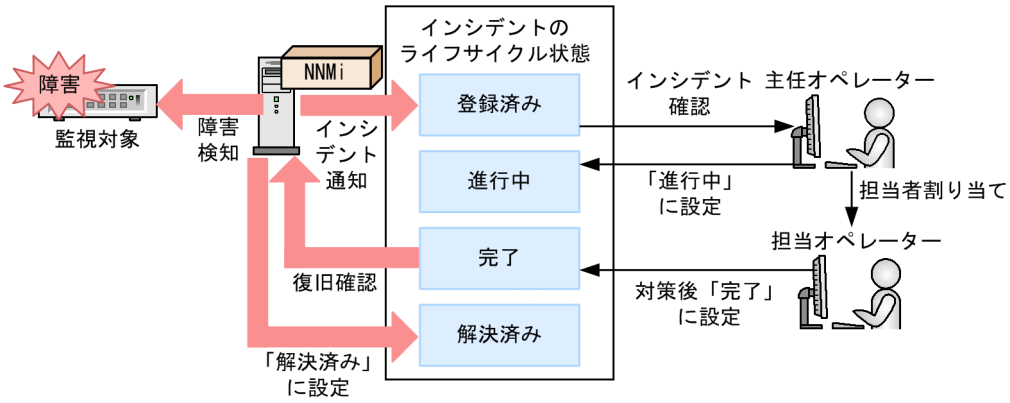
レイヤー 2 トポロジの解析	説明
通常時 	監視マネージャーは最上位のスイッチ「S1」に接続されていて，監視中のネットワークはすべて正常な状態です。
最上位スイッチの障害時 	障害内容：最上位のスイッチ「S1」がダウン 発生イベント： • 「S1」と通信が不可 • 「S1」を経由する他スイッチへの通信が不可 監視マネージャーは，この状況を次のように対応します。 • 「S1」のノード障害を検知します。 • 「S1」の先も通信できないが，「S1」障害の影響と判断し，インシデントを抑止して，状態不明とします。 この結果，「S1」の障害だけを根本原因のインシデントとして通知します。
中間スイッチの障害時 	障害内容：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 監視マネージャーは，この状況を次のように対応します。 • 「C2」のノード障害を検知します。 • 「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します。 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。

監視マネージャーは，ほかにも多くの事象と根本原因の対応を解析できます。

4.2　障害対応の仕組み

監視マネージャーは，インシデント対応の進行状況を［インシデント］ビューでライフサイクル状態として管理しています。複数人で分担して管理する場合，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 上で作業を分担できます。

次のように，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。



監視マネージャーはインシデントを通知したあとも状態監視を続けています。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，インシデントは自動的に「解決済み」になります。

ヒント

操作の練習として擬似障害を発生させて，通知されたインシデントを確認する方法を説明します。

1. 監視対象としているノードで LAN ケーブルを抜いたり，ノードを停止させたりして，障害を発生させます。

   業務に影響が出ないように注意してください。

2. マップ画面でノードを選択して［アクション］メニュー－［ポーリング］－［ステータスのポーリング］を選択します。

   状態ポーリングを行い，障害が検知されます。

4.3　ネットワーク障害に対応する

ネットワーク障害に対応する方法は幾つかありますが，ここでは，ネットワーク機器のノードダウンに対応する方法を説明します。

4.3.1　ネットワーク機器のノードダウンに対応する

ネットワーク機器のノードダウンを知らせるインシデントが発行されたら，問題のある個所を確認し，対策を実施します。

操作手順

1. NNMi コンソールのトポロジマップで障害個所を確認します。

   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。

2. [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] ビューや［すべてのインシデント］ビューを開き，インシデントの内容を参照して，問題個所を確認します。対象のノードを選択して［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，ソースノード，ソースオブジェクト，カスタム属性から確認しましょう。

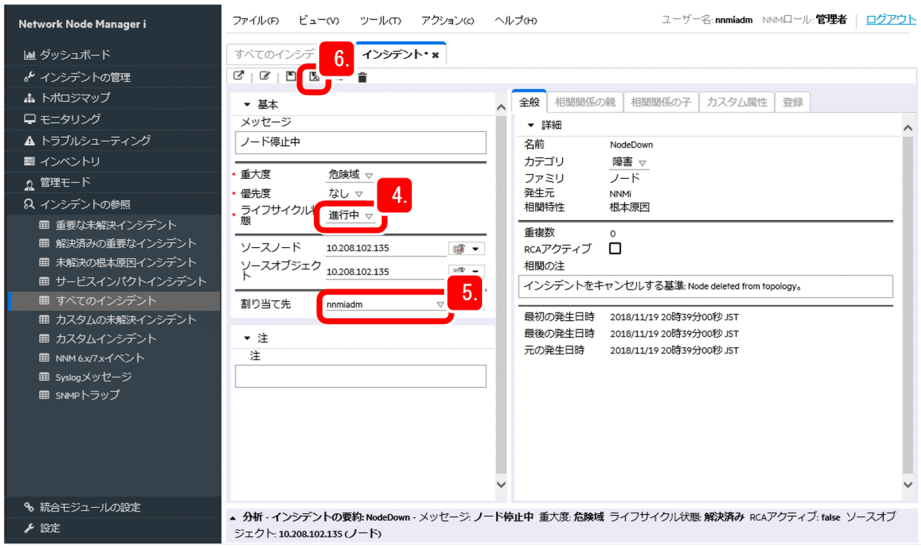
3. インシデントをダブルクリックして，インシデントの詳細情報を確認します。

   [インシデント] ビューが表示されます。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。

   > **メモ**
   >
   > 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 トラップによって通知された情報が表示されるため，SNMP トラップを発行した機器のマニュアルなどを参照して，内容を確認してください。

4. インシデントの［ライフサイクル状態］を［進行中］に設定します。

   問題状況が把握できたら，［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。インシデントの登録直後は［登録済み］になっています。



5. [割り当て先] のプルダウンメニューから自分のアカウントを選択します。

   自分以外のオペレーターを割り当てたい場合は，オペレーターが割り当てるインシデントにアクセスできることを確認してください。

6. （保存して閉じる）をクリックします。

   変更した設定が保存されます。

7. 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，関連部分も確認します。

   - 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，問題部分がないか把握します。

8. 対策を実施します。

   ヒント

   あらかじめ，インシデントに自動アクションを設定しておけば，指定したコマンドを自動的に実行できます。

9. 対策が完了したら，インシデントの [ライフサイクル状態] を [完了] に設定します。

   [解決済み] は，システムが問題ないことを識別したときに自動的に設定します。

10. （保存して閉じる）をクリックします。

    変更した設定が保存されます。

11. 変更したインシデントの状態を確認します。

［インシデントの参照］ビューで，［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ます。

操作結果

これで，ネットワーク機器のノードダウンに対する対策が完了しました。

関連項目

- (4)　インシデントに自動アクションを設定する
- 3.1.3　ネットワークの監視を始める
- 4.2　障害対応の仕組み

付録

付録 A　もっと使いこなすには？

JP1 ネットワーク管理製品をもっと使いこなすための参考情報を紹介します。

NNMi Advanced の紹介

JP1 ネットワーク管理製品では，NNMi の上位製品として，高度なネットワーク技術に対応した監視を実現する NNMi Advanced を提供しています。NNMi Advanced の主な機能を次に示します。

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ーと，それらをまとめるグローバルマネージャーによる集中管理ができます。グローバルマネージャーでは，最大 65,000 ノードまで管理できます。
NNMi IPv6 管理機能	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 ハイパーバイザーベースの仮想ネットワークの検出と監視	ルーター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検出	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。
ルーター冗長グループ	冗長化されたルーターグループの構成を自動認識します。また，ルーター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。

詳細については，マニュアル「NNMi セットアップガイド」を参照してください。

運用方法の紹介

JP1 ネットワーク管理製品を使った運用例を紹介します。詳細は参照先で確認してください。

こんなときは	解説	参照先
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。	次の 3 ステップで始めてみてください。 1. [通信の設定] で SNMP コミュニティ文字列を設定します。 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します。 3. [トポロジマップ] ワークスペース－［ネットワークの概要］を開いて運用を開始します。	2.2.4 2.2.5 3.1.3
ノードがまったく検出されない。	［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］や［インベントリ］で確認します。また検出の処理状況を［ヘルプ］メニュー－［システム情報］－［ステートポーラー］で確認できます。	2.2.5
ルーターやスイッチしか検出されない。	デフォルトの設定では，ルーターやスイッチだけを検出します。 ［検出の設定］－［自動検出ルール］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。	2.2.5

こんなときは	解説	参照先
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。	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［クイックアクセスマップ］フォルダに表示されなくなります。	2.2.6
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。	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」を使用してください。	2.2.6 2.2.8
SNMP マネージャー（NNMi）の IP アドレスは？	SNMP エージェント側の SNMP 設定で，SNMP マネージャーの IP アドレスを指定（接続を許可）する場合，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，NNMi マネージャーの IP アドレスを一とおり設定してください。 IP アドレスを固定したい場合は，ov.conf ファイルの NNM_INTERFACE に IP アドレスを指定してください。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。	リリースノート
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。	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，ノードが検出済み，該当する 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，［インシデントの設定］の［未解決の SNMP トラップおよび Syslog メッセージを破棄する］をオフにします。	ヘルプ「管理」の「未解決の受信トラップを処理する」のトピック
サーバー一覧やインシデント一覧など一覧表を作成したい。	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，CSV 形式でデータをファイルに出力できます。例えば，［インベントリ］ワークスペース－［ノード］を開いて，次の操作を行います。 1. 出力したい行を選択状態にします。 2. マウス右クリックして表示されたメニューから［CSV にエクスポート］を選択します。 3. 表示に従って操作します。 これを表計算ソフトなどに読み込み，一覧表などを作成してください。［ノード］ビューのノード一覧や［管理イベントの設定］ビューのインシデント一覧などを作成できます。	ヘルプ「使用」の「テーブルビューの使用」の「テーブル情報をエクスポートする」のトピック

付録 B　各バージョンの変更内容

付録 B.1　13-00 の変更内容

(1)　資料番号（3021-3-L31）の変更内容

- JP1/Network Element Manager に関する記述を削除した。
- 次の製品に関する記述を変更または削除した。
  - JP1/Extensible SNMP Agent for Windows
  - JP1/Extensible SNMP Agent
  - JP1/SNMP System Observer - Agent for Process
- 監視マネージャーの適用 OS に次の OS を追加した。
  - Linux 9.1
  - Oracle Linux 9.1

  また，次の適用 OS を削除した。
  - Windows Server 2012
  - CentOS
  - Linux 6.1
  - Oracle Linux 6.1
- NNMi が使用する HTTP ポートおよび HTTPS ポートのデフォルト値を変更した。
- Web ブラウザの Internet Explorer のサポート終了に伴い，関連する記述を削除した。
- 監視マネージャーとするサーバに必要なパッケージとライブラリファイルに関する説明を変更した。

付録 B.2　12-60 の変更内容

(1)　資料番号（3021-3-E01-30）の変更内容

- 監視マネージャーおよび監視エージェントとするサーバの適用 OS に，Windows Server 2022 を追加した。
- 監視マネージャーの前提条件の確認項目にシステムアカウントのパスワードを追加した。

- システムアカウントのパスワードを NNMi のインストール中に設定するように変更した。
- 環境変数「LC_ALL」,「LANG」に設定するロケールを変更した。

付録 B.3　12-50 の変更内容

(1)　資料番号（3021-3-E01-20）の変更内容

- NNMi が使用する HTTPS ポートのデフォルト値を追加した。
- 監視マネージャーまたは監視エージェントとするサーバの適用 OS を変更した。
- 使用する Web ブラウザの条件を変更した。
- 監視マネージャーの前提条件であるパッケージおよびライブラリファイルを追加した。
- kernel.shmall に関する説明を追加した。
- NNMi をインストールする際に設定する環境変数として，LANG を追加した。
- 言語環境に関する記載を削除した。
- 自動トリム機能に関する説明を変更した。

付録 B.4　12-10 の変更内容

(1)　資料番号（3021-3-E01-10）の変更内容

- 監視マネージャーとするサーバの適用 OS に Windows Server 2019 を追加した。

付録 B.5　12-00 の変更内容

(1)　資料番号（3021-3-E01）の変更内容

- 適用 OS から Windows 2008 R2 を削除した。
- 監視エージェントとするサーバの適用 OS に次を追加した。
  - SUSE Linux 15

- AIX V7.2

- 監視エージェントとするサーバの適用 OS から次を削除した。
  - AIX V6.1
  - Solaris 10
- Internet Explorer 10 をサポート対象外とした。
- Windows の Firefox のサポートバージョンを変更した。また，Linux では Firefox をサポート対象外とした。
- JP1/SNMP System Observer のセットアップ手順を変更した。これに伴い，Java Plug In の記述を削除した。

付録 B.6　11-10 の変更内容

(1)　資料番号（3021-3-A71-10）の変更内容

- 適用 OS に Windows Server 2016 を追加した。
- 次のブラウザをサポート対象外とした。
  - Internet Explorer 9
- Firefox のサポートバージョンを変更した。

付録 C　このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報を示します。

付録 C.1　関連マニュアル

関連マニュアルを次に示します。必要に応じてお読みください。

- JP1 Version 13 JP1/Network Node Manager i セットアップガイド（3021-3-L32）
- JP1 Version 13 JP1/Network Node Manager i Developer's Toolkit ガイド（3021-3-L33）
- JP1 Version 13 JP1/SNMP System Observer（3021-3-L34）

説明文では，「JP1 Version 13 JP1/Network Node Manager i セットアップガイド」を「NNMi セットアップガイド」，「JP1 Version 13 JP1/SNMP System Observer」を「JP1/SNMP System Observer」と表記します。

付録 C.2　マイクロソフト製品の表記

このマニュアルでは，マイクロソフト製品の名称を次のように表記しています。

表記		製品名
Windows	Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter
		Microsoft(R) Windows Server(R) 2016 Standard
	Windows Server 2019	Microsoft(R) Windows Server(R) 2019 Datacenter
		Microsoft(R) Windows Server(R) 2019 Standard
	Windows Server 2022	Microsoft(R) Windows Server(R) 2022 Datacenter
		Microsoft(R) Windows Server(R) 2022 Standard

付録 C.3　説明文で説明する書式

このマニュアルで使用している記号を次のように定義します。

書式	説明
文字列	可変の値を示します。 （例）日付は YYYYMMDD の形式で指定します。
[　]	ウィンドウ，ダイアログボックス，タブ，メニュー，ボタンなどの画面上の要素名を示します。

書式	説明
[ ] − [ ]	メニューを連続して選択することを示します。 （例）［ファイル］メニュー-［ヘルプ］を選択します。 上記の例では，［ファイル］メニュー内の［ヘルプ］を選択することを示します。

付録 C.4　製品名の表記

このマニュアルでは，製品名を次のように表記します。

このマニュアルでの表記		正 式 名 称
Firefox	Firefox ESR	Mozilla Firefox(R) ESR
JP1/IM		JP1/Integrated Management - Manager
Linux	Linux 7.1	Red Hat Enterprise Linux(R) Server 7（64-bit x86_64）（バージョン 7.1 以降）
	Linux 8.1	Red Hat Enterprise Linux(R) Server 8（64-bit x86_64）（バージョン 8.1 以降）
	Linux 9.1	Red Hat Enterprise Linux(R) Server 9（64-bit x86_64）（バージョン 9.1 以降）
	Oracle Linux 7.1	Oracle Linux(R) Operating System 7（バージョン 7.1 以降）
	Oracle Linux 8.1	Oracle Linux(R) Operating System 8（バージョン 8.1 以降）
	Oracle Linux 9.1	Oracle Linux(R) Operating System 9（バージョン 9.1 以降）
	SUSE Linux 12	SUSE Linux(R) Enterprise Server 12
NNMi		JP1/Network Node Manager i
NNMi Advanced		JP1/Network Node Manager i Advanced
SSO		JP1/SNMP System Observer
VMware		VMware(R)

付録 C.5　英略語

このマニュアルで使用する英略語を次に示します。

英略語	英字での表記
ARP	Address Resolution Protocol
CPU	Central Processing Unit
CSV	Comma Separated Values
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System

英略語	英字での表記
ESC	Enhanced Security Configuration
FQDN	Fully Qualified Domain Name
GIF	Graphics Interchange Format
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over SSL
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
OS	Operating System
PC	Personal Computer
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VPN	Virtual Private Network
WWW	World Wide Web

付録 C.6　KB（キロバイト）などの単位表記

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイト，$1{,}024^4$ バイトです。

用語解説

英字

MIB オブジェクト

MIB にある一つ一つの管理情報です。MIB オブジェクトは階層的なツリー構造で構成されていて，ツリーの階層ごとにユニークな名称とそれを数値で表す識別子を持っています。なお，MIB オブジェクトの特定の値のことをインスタンスと呼びます。

MIB（Management Information Base）

SNMP を利用しているサーバ製品やネットワーク機器が，その機器の状態を外部に知らせるために公開する情報のことです。

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 マネージャーに情報を通知する処理のことです。

ア行

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。

インスタンス

リソースの収集元の実体です。例えば，リソース「CPU 利用率」のインスタンスは各 CPU の CPU 利用率となります。

カ行

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。

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。

タ行

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。

ナ行

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。

ラ行

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。

リソース

SSO が SNMP エージェントから収集した情報の集まりです。例えば，「CPU 利用率」「実行待ちキュー長」などがあります。

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。

索引

V

W

あ

い

か

く

け

こ

さ

し

れ

わ

株式会社 日立製作所
〒 100-8280　東京都千代田区丸の内一丁目 6 番 6 号