

HP Network Node Manager i Software

Windows® オペレーティングシステム用

ソフトウェアバージョン : 9.10

インストール ガイド

製造パート番号 : TB774-99004

ドキュメント リリース日 : 2011 年 3 月

ソフトウェア リリース日 : 2011 年 3 月



ご注意

保証について

HP 製品とサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。HP では、ここに記載されている技術的、または編集上の不正確さや脱漏については責任を負いません。

ここに記載されている情報は、予告なく変更されることがあります。

権利制限について

機密性のあるコンピュータソフトウェアです。これらを所有、使用、または複製するには、HP からの有効なライセンスが必要です。商用コンピュータ ソフトウェア、コンピュータ ソフトウェアに関する文書類、および商用アイテムの技術データは、FAR 12.211 および 12.212 の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

© Copyright 2008–2011 Hewlett-Packard Development Company, L.P.

商標に関する通知

Acrobat® は Adobe Systems Incorporated の登録商標です。

HP 9000 コンピュータ上で動作する HP-UX リリース 10.20 以降、および、HP-UX リリース 11.00 以降 (32 および 64 ビット構成) は、すべて、Open Group UNIX 95 製品です。

Microsoft® および Windows® は、Microsoft Corporation の米国における登録商標です。

Oracle および Java は Oracle およびその関連会社の登録商標です。

UNIX® は The Open Group の登録商標です。

Oracle テクノロジーの制限された権限に関する通知

国防省連邦調達規則補足 (DOD FAR Supplement) に従って提供されるプログラムは、「商用コンピュータ ソフトウェア」であり、ドキュメントを含む同プログラムの使用、複製および開示は、該当する Oracle 社のライセンス契約に規定された制約を受けるものとします。それ以外の場合、連邦調達規則に従って提供されるプログラムは「制限付きコンピュータ ソフトウェア」であり、ドキュメントを含む同プログラムの使用、複製および開示は、FAR 52.227-19 「商業コンピュータ ソフトウェア制限付き権利」(1987 年 6 月) に規定された制約を受けるものとします。Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Oracle ライセンスの全文は、NNMi の製品 DVD 上にある license-agreements のディレクトリを参照してください。

謝辞

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>)

ドキュメントの更新

本書の表紙には、以下の識別情報が記載されています。

- ソフトウェアのバージョンを示すソフトウェア バージョン番号
- ドキュメントの更新ごとに変更されるドキュメント リリース日
- ソフトウェアのこのバージョンがリリースされた日を示すソフトウェア リリース日

最近の更新を確認する場合、または最新のドキュメントを使用しているか確認する場合は、以下をご覧ください。

<http://h20230.www2.hp.com/selfsolve/manuals>

このサイトでは、HP Passport ユーザー ID への登録とサインインが必要です。HP Passport ユーザー ID のご登録は、以下の URL で行ってください。

<http://h20229.www2.hp.com/passport-registration.html>

または、HP Passport ログインページの **[New users - please register]** リンクをクリックします。

製品のサポート サービスに登録すると、最新版を入手できます。詳細は HP 販売員にお尋ねください。

サポート

次の HP ソフトウェア サポート オンライン Web サイトを参照してください。

www.hp.com/go/hpsoftwaresupport

この Web サイトには、製品、サービス、および HP Software が提供するサポートの問い合わせ情報および詳細が記載されています。

HP ソフトウェア オンライン サポートには、お客様の自己解決機能が備わっています。ビジネスを管理するために必要な対話形式のテクニカル サポート ツールにアクセスする迅速で効率的な方法が用意されています。お客様は、サポート Web サイトで以下の機能を利用できます。

- 関心のあるドキュメントの検索
- サポートケースおよび拡張リクエストの送信および追跡
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HP サポートの問合せ先の検索
- 利用可能なサービス情報の確認
- ソフトウェアを利用している他のユーザーとの情報交換
- ソフトウェアトレーニング情報の検索および参加登録

大部分のサポートには、HP Passport へのユーザー登録とサインインが必要です。また、サポート契約が必要な場合もあります。HP Passport ユーザー ID のご登録は、以下の URL で行ってください。

<http://h20229.www2.hp.com/passport-registration.html>

アクセス レベルに関する詳細は、次の URL で確認してください。

http://h20230.www2.hp.com/new_access_levels.jsp

目次

1	HP Network Node Manager i Software の紹介	7
	このガイドについて	7
	このドキュメントで使用する環境変数	8
2	インストール前チェックリスト	9
	対応ハードウェアおよびソフトウェア	9
	NNMi 管理サーバーの準備	11
	データベースのインストール	14
	適格に設定された DNS の確認	16
	NNMi クイックスタート設定ウィザード	18
3	NNMi のインストールおよび有効化	19
	NNMi のインストール	19
	NNMi のサイレント インストール	25
	ovinstallparams.ini サンプル ファイルを使用したサイレント インストール	26
	以前のインストールの ovinstallparams.ini ファイルを使用したサイレント インストール	28
	クイック スタート設定ウィザードの使用	30
	NNMi ライセンスの取得	35
	恒久ライセンス キーのインストール準備	35
	ライセンスの種類および管理対象ノードの数の確認	35
	恒久ライセンス キーの取得およびインストール	36
	Autopass および HP 注文番号の使用 (ファイアウォール使用時は不可)	36
	コマンド行で、シードを追加する	37
	ライセンスキーの追加取得	37
	NNMi の削除	38
	NNMi インストール ログ ファイルへのアクセス	40

4	NNMi 入門	41
	NNMi へのアクセス	41
	NNMi ヘルプ	44
	ネットワーク検出の設定	45
	コミュニティ文字列の設定	46
	自動検出ルールの設定	47
	検出の進行状況の確認	49
A	追加情報	51
	ディスク レベルで互換性のあるセキュリティ レベルの設定	51
	正式な完全修飾ドメイン名の取得または設定	52
	ウイルス対策ソフトウェアの無効化	52
	NNMi コンソール 用の Web ブラウザの有効化	53
	システム アカウントのパスワードのリセット	55
	Windows Server 2008 でよく知られているポートを有効にする	55
B	インストールおよび初期スタートアップのトラブルシューティング	57
	インストールの問題	57
	初期スタートアップの問題	58
	用語集	63

1 HP Network Node Manager i Software の紹介

HP Network Node Manager i Software には、組織内のネットワークを正常に維持するために役立つツールセットが含まれています。NNMi を使用すると、ネットワーク ノード (スイッチやルーターなど) を継続的に検出し、最新のネットワーク トポロジを表現できます。NNMi は、ネットワークの状況を正常に維持するため、**例外管理**、つまりイベント関連処理や根本原因解析 (RCA) を使用してネットワークの問題を特定する機能による問題の処理にも役立ちます。他のネットワーク管理ソフトウェアとは異なり、NNMi では、動的な障害管理をサポートするために、洗練された RCA アルゴリズムが、正確で、絶えず変化するネットワーク トポロジの表示に適用されています。

このガイドについて

本ガイドは、NNMi をインストールし、基本的な NNMi の設定を実行する際に役立ちます。本ガイドには、単一のサーバーへのインストール手順、および NNMi のインストール後すぐに**クイック スタート設定ウィザード**を使用する手順が含まれています。本ガイドでは、スパイラル検出プロセスを使用してネットワーク管理を開始する際に役立つ、簡単な手順についても説明しています。

本ガイドでは、HP が開発した、NNMi の初期配備に役立つ手順について説明しています。基本的な NNMi のプロセス (ネットワーク検出およびポーリングなど) の設定の詳細について理解すると、ネットワーク管理ソリューションを調整および拡張し、総合的な管理方針を立てることができるようになります。

本ガイドは、それらの開始に役立つために HP によって設計されました。NNMi の使用に関する詳細は、NNMi のヘルプに記載されています (44 ページの「[NNMi ヘルプ](#)」を参照)。NNMi 設定のカスタマイズに関する詳細については、『HP Network Node Manager i Software デプロイメント リファレンス』を参照してください。

このドキュメントで使用する環境変数

このドキュメントでは、以下の **NNMi** 環境変数を使用して、ファイルやディレクトリの場所を参照します。デフォルト値は以下のとおりです。実際の値は、**NNMi** のインストール中に行った選択内容によって異なります。

Windows 2008:

- %NmInstallDir%: <drive>%Program Files(x86)%HP%HP BTO Software
- %NmDataDir%: <drive>%ProgramData%HP%HP BTO Software



Windows システムでは、**NNMi** インストール プロセスによってこれらの環境変数が作成されるので、いつでも使用できます。

入手可能なその他の **NNMi** 環境変数については、『**HP Network Node Manager i Software** デプロイメント リファレンス』を参照してください。

2 インストール前チェックリスト

この章では、NNMi のインストールの前に完了させておく必要のあるタスクのチェックリストや、対応するハードウェアおよびソフトウェアのリストの入手場所などを記載しています。

対応ハードウェアおよびソフトウェア

NNMi をインストールする前に、9 ページの表 1 に示す、NNMi でサポートされるハードウェアとソフトウェアに関する情報をお読みください。



表 1 に挙げたドキュメントの最新バージョンについては、以下のアドレスをご覧ください。

<http://h20230.www2.hp.com/selfsolve/manuals>

この Web サイトにアクセスするには、HP Passport ID が必要です。

表 1 ソフトウェアおよびハードウェアのインストール前チェックリスト

チェック 欄 (はい/ いいえ)	確認していただくドキュメント
	『HP Network Node Manager i Software デプロイメント リファレンス』 NNMi の高度な展開および企業向けインストールの設定情報について説明した、Web でのみ提供しているドキュメントは、 http://h20230.www2.hp.com/selfsolve/manuals でご覧いただけます。

表 1 ソフトウェアおよびハードウェアのインストール前チェックリスト

チェック 欄 (はい/ いいえ)	確認していただくドキュメント
	<p>『HP Network Node Manager i Software アップグレードドリファレンス』</p> <p>NNMi の高度な企業向けインストールのアップグレード情報について説明した、Web でのみ提供しているドキュメントは、 http://h20230.www2.hp.com/selfsolve/manuals でご覧いただけます。</p>
	<p>HP Network Node Manager リリースノート</p> <ul style="list-style-type: none"> • ファイル名 = releasenotes_ja.html • 製品メディア = トップレベルまたはルート ディレクトリ • NNMi コンソール = [ヘルプ] > [NNMi ドキュメント ライブラリ] > [リリース ノート]
	<p>HP Network Node Manager i Software システムとデバイス対応マトリックス</p> <ul style="list-style-type: none"> • ファイル名 = supportmatrix_ja.html • 製品メディア = トップレベルまたはルート ディレクトリ • NNMi コンソール = リリース ノートからリンクしている



新しい情報が入手可能になった時点で、HP は「HP Network Node Manager i Software システムおよびデバイスの対応マトリックス」を更新しています。NNMi の展開を開始する前に、以下の Web サイトで、お持ちのソフトウェアのバージョンに関する最新の「HP Network Node Manager i Software システムおよびデバイスの対応マトリックス」をチェックしてください。

<http://h20230.www2.hp.com/selfsolve/manuals>

この Web サイトにアクセスするには、HP Passport のユーザー ID が必要です。

NNMi 管理サーバーの準備

NNMi 管理サーバー とは、NNMi ソフトウェアがインストールされているサーバーのことです。各 NNMi 管理サーバーは、64 ビット マシンである必要があります。ハードウェア要件の詳細については、9 ページの「[対応ハードウェアおよびソフトウェア](#)」を参照してください。

NNMi では、組み込み Java 仮想マシンおよび JDK バージョン 1.6 が出荷されます。Java が適切に機能するためには、特定のオペレーティングシステムのパッチが必要です。

HP-UX 以外でサポートされているオペレーティングシステムを実行しているサーバーに NNMi をインストールする場合は、そのオペレーティングシステムのリリースノートを参照してください。

NNMi 管理サーバー に NNMi をインストールする前に、表 2 のチェックリストを完了させてください。NNMi データを保存するために Oracle データベースのインスタンスを使用する場合は、14 ページの「[データベースのインストール](#)」を参照してください。

表 2 NNMi 管理サーバー インストール前チェックリスト

チェック 欄 (はい / いいえ)	NNMi 管理サーバーの準備
	<p>NNMi 管理サーバー の正式な完全修飾ドメイン名 (FQDN) を判別します。インストール中にこの情報が必要です。正式な FQDN は以下の要件を満たす必要があります。</p> <ul style="list-style-type: none">• NNMi 管理サーバーに対して DNS を解決できる必要があります。• ネットワーク上の他のコンピュータから NNMi 管理サーバーにアクセスできる必要があります。 <p>詳細については、52 ページの「正式な完全修飾ドメイン名の取得または設定」を参照してください。</p>

表 2 NNMi 管理サーバー インストール前チェックリスト

チェック 欄 (はい/ いいえ)	NNMi 管理サーバーの準備
	制限付きのセキュリティ設定がある場合、NNMi インストールとデータディレクトリを配置するドライブ (複数可) のアクセス許可を調整する必要がある場合があります。51 ページの「ディスク レベルで互換性のあるセキュリティ レベルの設定」を参照してください。
	SNMP サービスをチェックしてください。インストールされされた場合、SNMP トラップサービスをこのサーバーから無効にする必要があります。
	NNMi のインストール中にパッチのインストールする場合は、圧縮されているパッチファイルを解凍してください。解凍したファイルをターゲットサーバーのフォルダに配置します。
	対応 Web ブラウザをインストールして有効にします。9 ページの「対応ハードウェアおよびソフトウェア」および 53 ページの「NNMi コンソール 用の Web ブラウザの有効化」を参照してください。
	Dynamic Host Configuration Protocol (DHCP) ユーザー : NNMi 管理サーバーに対して常に同じ IP アドレスが割り当てられることを確認してください。
	ウイルス対策ソフトウェアを無効にします。52 ページの「ウイルス対策ソフトウェアの無効化」を参照してください。

表 2 NNMi 管理サーバー インストール前チェックリスト

チェック 欄 (はい/ いいえ)	NNMi 管理サーバーの準備
	<p>NNMi は、数個のよく知られているポートを使用しますが、それらのポートはNNMiのインストール前にNNMi 管理サーバーで使用可能になっている必要があります。NNMi のインストール前に、以下のポートがすべて使用可能になっていることを確認してください。</p> <ul style="list-style-type: none"> • TCP ポート 80、443、1098、1099、3873、4444 ～ 4446、4457 ～ 4460、5432、7800 ～ 7810、8083、8886、および 8887 • UDP ポート 162 <p>NNMi のインストール前に、上のポートのどれも、NNMi 管理サーバーのファイアウォールおよび他のウィルス対策ソフトウェアによってブロックされないことを確認してください。ポート競合の解決の詳細については、『HP Network Node Manager i Software デプロイメント リファレンス』を参照してください。</p>
	<p>US-English 以外のロケールが必要な場合は、必要とする (Japanese などの) ロケールをサポートするように NNMi 管理サーバーを設定してください。NNMi がサポートするロケールの詳細については、『HP Network Node Manager i Software システムとデバイス対応マトリックス』を参照してください。</p>
	<p>グローバルネットワーク管理機能またはアプリケーションフェイルオーバー機能の設定に関する詳細については、『HP Network Node Manager i Software デプロイメント リファレンス』を参照してください。</p>

データベースのインストール

NNMi では、以下のデータベースをサポートしています。

組み込みデータベース NNMi 製品に付属しています。このデータベースのインストール前提条件はありません。

NNMi 用の Oracle データベースの管理者によって作成されます。
データベースのインスタンス NNMi 用の Oracle データベースのインスタンスをインストールする際には、表 3 のチェックリストを完了させてください。

表 3 Oracle データベースのインストール前チェックリスト

チェック欄 (はい/いいえ)	Oracle データベースの事前準備
	パフォーマンスを向上させ、NNMi ソフトウェアとのポートの競合を回避するため、Oracle は NNMi 管理サーバー とは異なるサーバーにインストールする必要があります。 詳細については、59 ページの「問題 : jboss ポートの競合」を参照してください。
	Oracle データベースの管理者と共に、Oracle の提供する説明書に従って、Oracle データベースをインストールしてください。

表 3 Oracle データベースのインストール前チェックリスト（続き）

チェック 欄（はい/ いいえ）	Oracle データベースの事前準備
	<p>NNMi 用のデータベースのインスタンスを作成します。Oracle サーバーのホスト名とデータベースのインスタンス名は、大切に保管してください。NNMi のインストール時に必要となります。</p>
	<p>インストールするノードの数に基づいたテーブル空間を割り当てます。たとえば、18,000 ノードのネットワークの場合は、開始テーブル空間サイズを 12 ギガバイト (GB) に設定します。12 GB の増分で無制限のテーブル空間拡張を行うオプションを設定します。</p> <p>データベースの必要サイズは NNMi が追加ノードを検出するにつれて大きくなるため、その拡張状況に注意し、必要な場合は設定したテーブル空間サイズを増やしてください。</p>
	<p>以下のアクセス権限を持つ Oracle ユーザーを作成します。</p> <ul style="list-style-type: none"> • シーケンスの作成 • セッションの作成 • 表の作成 • ビューの作成 • FLASHBACK ANY TABLE <p>HP では、FLASHBACK ANY TABLE 許可を推奨します。これにより NNMi で、移行時に復元ポイントを作成できます。</p> <p>Oracle ユーザー名とパスワードを記録して保管します。これらは NNMi のインストール時に必要となります。</p> <p>十分に大きいテーブル空間をユーザーに割り当てることが重要です。テーブル空間が十分な大きさでなくても、NNMi はインストールされますが、テーブルは作成されません。これはインストール後に発生する問題の原因となります。これを防止するには、割り当てを unlimited に設定しますが、1MB 以上にしてから NNMi をインストールします。</p>

適格に設定された DNS の確認

NNMi は、ドメイン名システム (**DNS**) を使用してホスト名と IP アドレスの関係を判断します。これにより、自動検出が有効になっている場合は、大量のネームサービスクエリーが行われる可能性があります。

DNS サーバーが、ネームサービスクエリーを解決する際に長時間にわたる遅延を防ぐよう的確に設定されていることを確認します。つまり、NNMi ネームサービスクエリーに応答する DNS サーバーに以下の特性があることを確認します。

- DNS サーバーは、権限サーバーであり、DNS 要求を転送しません。
- DNS サーバーには、ホスト名から IP アドレスと、IP アドレスからホスト名への一貫したマッピング情報があります。

ネットワークで複数の DNS サーバーを使用している場合は、すべての DNS サーバーがすべてのネームサービスクエリーに一貫して応答する必要があります。



ラウンドロビン DNS (Web アプリケーション サーバーの負荷分散に使用される) では、任意のホスト名が時間の経過に伴って異なる IP アドレスにマップされる可能性があるため、適切ではありません。



nslookup の応答時間を改善するには、セカンダリ DNS サービスを NNMi 管理サーバー または NNMi 管理サーバー と同一のサブセット内の別のシステムに配置します。そして、プライマリ DNS サービスの情報をミラーリングするように、このセカンダリ DNS サービスを設定してください。別のオプションとして、小規模な環境では、DNS の代わりに

`%SystemRoot%\system32\drivers\etc\hosts` ファイルを使用することもできます。

NNMi 管理サーバー 上で、使用している環境に対して以下が適切に設定されているかを確認します。

- nslookup コマンドが失敗すると、
`%SystemRoot%\system32\drivers\etc\hosts` ファイルが優先されます。hosts ファイルに最低限以下の 2 つのエントリが含まれていることを確認します。

127.0.0.1 (ループバックのログホスト)

<NNMi 管理サーバー IP アドレス> <NNMi 管理サーバー 名前>

前の項で示した **NNMi** 管理サーバー名は、インストール時に設定された **NNMi** 管理サーバーの正式な完全修飾ドメイン名 (**FQDN**) です。前の項で示した **NNMi** 管理サーバーの **IP** アドレスは、**NNMi** 管理サーバーの **FQDN** の **IP** アドレスです。

- **NNMi** 管理サーバーが使用するすべての **DNS** サーバーに、ホスト名から **IP** アドレスと、**IP** アドレスからホスト名への一貫したマッピング情報があることを確認してください。

ネットワーク ドメイン内の **DNS** の設定に問題がある（適切に解決されないホスト名やアドレス）ことが分かっている場合は、重要ではないデバイスが対象の **nslookup** 要求を避けるよう、**NNMi** を設定してください。これを行う利点は、以下の通りです。

- スパイラル検出の速度向上。
- **NNMi** が引き起こすネットワーク トラフィックの最小化。

NNMi が問題のあるデバイスを識別するには、**NNMi** の検出を設定する前に以下の 2 つのファイルを作成します。**NNMi** は、これらのファイルで識別されたホスト名または **IP** アドレスの **DNS** 要求を発行しません。

- **hostnlookup.conf** (完全修飾ドメイン名またはホスト名のグループを識別するワイルドカードを入力)
- **ipnlookup.conf** (**IP** アドレスまたは **IP** アドレスのグループを識別するワイルドカードを入力)

ファイルを作成するには、**ASCII** エディタを使用します。ファイルを **NNMi** 管理サーバー 上の以下の場所に配置します：

```
%NmDataDir%\shared\%nnm%\conf\
```

NNMi クイックスタート設定ウィザード

インストール後に**クイック スタート設定ウィザード**を起動すると、制限のある環境（またはテスト環境）で NNMi を設定することができます。このウィザードを使用する場合は、[表 4](#) のチェックリストを完了させてください。

表 4 NNMi クイック スタート設定ウィザードのインストール前チェックリスト

チェック 欄（はい/ いいえ）	初期環境設定の事前準備
	自動検出における IP 設定範囲を決定します。ライセンス制限に基づいてインストールできるデバイス数を決定するには、 35 ページの「NNMi ライセンスの取得」 を参照してください。
	検出シードの IP アドレスを決定します。シードの詳細については、 30 ページの「検出シードおよび自動検出ルールについて」 を参照してください。
	検出領域内のノードの読み取り専用 SNMP コミュニティ文字列を、ネットワーク管理者から取得します。
	NNMi 管理者アカウントのユーザー名とパスワードを決定します。

3 NNMi のインストールおよび有効化

この章では、NNMi のインストールのプロセスについて説明します。NNMi の初回インストール時には、インストールに関する質問応答内容を保存したファイルが、インストールプログラムにより作成されます。このファイルは、以後、他のサーバーでインストールを行う際に、サイレント インストールの入力として利用することができます。詳細については、25 ページの「[NNMi のサイレント インストール](#)」を参照してください。

NNMi を初めてインストールする場合は、インストール プロセスのデフォルトの環境設定パラメータを使用することをお勧めします。このようにすれば、デフォルトの環境設定を使用しながら、後から管理対象のネットワークが増えた場合には、その部分だけをカスタマイズして対応することができます。

- ▶ **Linux および Windows:** この章で説明するインストール手順を使用し、VMWare を実行しているサーバーなどの仮想マシンに NNMi をインストールできます。仮想マシンとそのソフトウェアおよびハードウェアの要件については、『**HP Network Node Manager i-series Software** システムおよびデバイス対応マトリックス』を参照してください。

NNMi のインストール

ウィルス対策ソフトウェアを無効にするなど、インストール前の要件を確認してください（第 2 章、[インストール前チェックリスト](#)を参照）。

- ▶ **Oracle データベースに、NNMi データを保存する場合は、Oracle データベースの管理者と作業を行う必要があります。**14 ページの「[データベースのインストール](#)」を参照してください。

NNMi のサポート対象のバージョンからアップグレードしない場合は、以前の NNMi のインストールをすべて削除します。NNMi を削除する方法については、38 ページの「[NNMi の削除](#)」を参照してください。サポート対象のアップグレードパスを確認するには、『*HP Network Node Manager i Software デプロイメント リファレンス*』の「*NNMi 9.0x からのアップグレード*」を参照してください。

NNMi をインストールするには、以下の手順に従います。

- 1 NNMi をインストールするシステムに、管理者権限を持つユーザーとしてログオンします。
- 2 DVD ドライブに、NNMi インストール メディアを挿入します。
- 3 インストールメディアのルートディレクトリにある、`setup.exe` ファイルをダブルクリックします。

インストールの初期化プロセスで、使用する言語を選択するように求められます。この言語は、システムでサポートするように構成した言語から選択できます。次に、インストールする準備ができているかどうかのチェックが行われます。
- 4 **[アプリケーションの要件チェックの警告]** ダイアログ ボックスが表示された場合、各警告をクリックして、内容を理解した上で対処法を決定します。**[アプリケーションの要件チェックの警告]** ダイアログボックスで警告に対処した後、**[続行]** をクリックします。
- 5 **[インストーラの設定]** ダイアログ ボックスが表示された場合、以前のインストール時に保存した値を使用してインストールするか、インストール オプションを変更してインストールするのを選択します。保存した値のまま使用の場合は、**[はい]** をクリックします。新しくインストールオプションを自分で選択する場合は、**[いいえ]** をクリックします。
- 6 **[はじめに]** ページでインストールの概要を確認し、**[次へ]** をクリックします。
- 7 **[ライセンス契約]** ページで、NNMi のライセンス条項を確認します。ライセンス契約条項に同意する場合は、**[ライセンス契約の条項に同意します]** を選択し、**[次へ]** をクリックします。
- 8 **[セットアップタイプ]** ページで **[標準]** を選択し、**[次へ]** をクリックします。

- 9 **【アプリケーション及びデータ フォルダの選択】** ページで、アプリケーションフォルダとデータフォルダのデフォルトの場所を受け入れるか別の場所を参照し、**【次へ】** をクリックします。



アプリケーションフォルダのデフォルトの場所をデータフォルダの場所にコピーして、2 つのインストール場所を組み合わせないようにしてください。デフォルトのアプリケーションフォルダには、Program Files (x86) のように括弧が含まれます。括弧を含むデータフォルダの場所を使用すると、NNMi のアプリケーションフェイルオーバー機能が誤動作します。



NNMi は 32 ビットとの互換性がないため、64 ビット システム上の < ドライブ名 >:\Program Files¥ 以外のフォルダ にインストールする必要があります。お勧めするフォルダは、< ドライブ名 >:\Program files(x86)¥ です。

サーバー メッセージ ブロック (SMB) / Common Internet File System (CIFS) ネットワーキング プロトコル (Samba) を使用して、NNMi をインストールするのが認定されません。マップされたネットワーク ドライブに NNMi をインストールしないでください。



ほかの HP Software アプリケーションがこのサーバーにインストールされている場合、このダイアログ ボックスは表示されません。

- 10 NNMi の以前のバージョンからアップグレードし、既存の Oracle データベース インスタンスを使用する場合は、**手順 15** に進みます。
- 11 NNMi の以前のバージョンからのアップグレードではなく、新規インストールを実行している場合は、**【データベース タイプの選択】** ページが表示されます。このページで以下のいずれかのオプションを選択し、**【次へ】** をクリックします。
- NNMi に付属しているデータベース ソリューションを使用する場合は、**【HP Software の組み込みのデータベース】** を選択し、**【次へ】** をクリックしてから、**手順 15** にお進みください。
 - 以下のいずれかの設定で既存の Oracle データベース インスタンスを使用する場合は、**【Oracle】** を選択してから **手順 12** に進みます。
 - スタンドアロン
 - アプリケーションフェイルオーバーを使用するグローバルネットワーク管理設定のグローバルマネージャ

— アプリケーションフェイルオーバーまたは HA 設定



グローバルマネージャおよびグローバルネットワーク管理機能に関する詳細については、『HP Network Node Manager i Software デプロイメント リファレンス』を参照してください。

12 **[データベース初期化設定の選択]** ページで、以下のいずれかを実行します。

- 以前に定義したデータベース アカウントで **Oracle** データベースを初期化する場合は、**[プライマリ サーバーのインストール]** を選択して **[次へ]** をクリックします。
- 別のプライマリインストールで初期化済みの既存のデータベースに接続し、このインストールをアプリケーション フェイルオーバーまたは HA 構成で使用する場合は、**[セカンダリ サーバーのインストール]** を選択して **[次へ]** をクリックします。

13 **[データベース サーバー情報の入力]** のページで、Oracle データベース システムのホスト名を入力します。NNMi データベースのインスタンス名を入力し、**[次へ]** をクリックします。

14 **[データベース ユーザー アカウント情報の入力]** のページで、Oracle データベース ユーザーのユーザー名とパスワードを入力します。

インストール プロセスでエラーが報告された場合は、57 ページの「**問題 : NNMi のインストール プロセスが、Oracle ユーザー名とパスワードを受け付けない**」を参照してください。

15 インストール ソフトウェアが追加の NNMi インストール要件をチェックする間、**[インストールのチェック]** のページには進行状況が表示されます。チェック完了後、**[次へ]** をクリックします。

16 **[プレインストールの概要]** のページで、インストールの設定内容を確認し、以下のいずれかの操作を実行します。

- 設定の変更を行う場合は、**[前へ]** をクリックします。
- インストールプロセスを開始する場合は、**[インストール]** をクリックします。

インストールプロセスによって NNMi がインストールされ、一部の初期設定が実行されます。このプロセスの完了には、一般的に 10 ～ 30 分かかります。

- 17 NNMi の以前のバージョンからのアップグレードではなく、新規インストールを実行している場合は、[**システムアカウントのパスワード**] ダイアログボックスが表示されます。画面の指示に従ってシステム アカウントのパスワードを作成し、[**OK**] をクリックします。

▶ **システムアカウント**は、インストール中に NNMi により作成される特別な管理者アカウントです。システム アカウントは、インストール終了後も有効ですが、コマンドラインのセキュリティや復旧目的にのみ使用されます。システム パスワードを確認または変更する方法の説明は、55 ページの「**システム アカウントのパスワードのリセット**」を参照してください。

- 18 NNMi へアクセスするには、[**NNMi Web サーバーポート**] ダイアログボックスにあるポート番号が必要になりますので、このポートを記録しておきます。[**OK**] をクリックしてデフォルトのポートを適用するか、ポート番号を変更してから、[**OK**] をクリックします。

- 19 [**NNMi HTTPS Web サーバー ポート**] ダイアログ ボックスで、NNMi が NNMi Web サーバーに使用するポート番号を適用または変更できます。[**OK**] をクリックして、デフォルトのポートまたは変更したポートを適用します。NNMi のアップグレードの場合は、24 ページの**手順 21**に進みます。

- 20 インストール プロセスでは、NNMi 管理サーバー に対する正式な完全修飾ドメイン名 (FQDN) を検索します。ダイアログ ボックスに不完全または解決できない FQDN がある場合、名前を変更して [**OK**] をクリックします。

▶ このエントリは、NNMi 管理サーバー へのアクセスで、正式な FQDN として使用されます。シングルサインオン (SSO) を NNM iSPI に対して有効にするためにも使用されます。SSO を機能させるため、URL は NNMi にアクセスし、NNM iSPI は共通のドメインを共有する必要があります。NNMi 管理サーバー が使用する FQDN がない場合、NNMi 管理サーバー の IP アドレスを置き換えることができますが、置き換えた場合、NNM iSPI のシングルサインオンが使用できなくなります。

以下のインストールでは、正しくない、または解決できない FQDN のために、NNMi をアクセスするうえで問題がある場合は、52 ページの「**正式な完全修飾ドメイン名の取得または設定**」を参照してください。

- 21 インストールプロセスでは、NNMi を起動する前に、インストールする NNMi パッチの場所を指定するように要求されます。**[パッチのインストール]** または **[パッチのスキップ]** を選択して続行します。
- ▶ パッチのインストール前に、圧縮されているパッチファイルを解凍し、解凍したファイルをターゲットサーバーのフォルダに配置してから **手順 21** を実行してください。NNMi のインストールでは、*patchfilename.msi* (Windows)、*patchfilename.tar* (Solaris)、*patchfilename* (shar ファイル) または *patchfilename.depot* (HP-UX)、*patchfilename.rpm* (Linux) という形式になっているパッチファイルがサポートされます。このファイルの元の形式を変更しないでください。
 - ▶ パッチの入手方法などのサポート情報については、4 ページの「**サポート**」を参照してください。
- 22 インストールおよび構成が完了すると、NNMi サービスが起動します。このプロセスには数分かかります。
- ▶ jboss とは、NNMi サービスを含むアプリケーション サーバーです。このインストール ルーチンの段階では、jboss ポートの競合が発生する場合があります。その場合は、59 ページの「**問題 : jboss ポートの競合**」を参照してください。
- 23 NNMi の以前のバージョンからのアップグレードを実行した場合、この時点でデータベース移行が行われるため、構成にかかる時間が長くなります。終了すると、移行が正常に行われたことを示すダイアログ ボックスが表示されます。データベース移行中にエラーが発生した場合は、HP サポートにお問い合わせください。
- 24 **[終了]** をクリックします。
- 25 ソフトウェアのインストールによって NNMi の設定が完了すると、**[クイックスタート設定ウィザードを起動]** ダイアログボックスが表示されます。
- このダイアログの情報をよく読んでください。NNMi をインストールして、アプリケーション フェイルオーバーまたは HA 構成で既存の Oracle データベース インスタンスを使用する場合は、このウィザードを実行する必要がないため、**[いいえ]** をクリックします。

このウィザードの詳細については、30 ページの「[クイック スタート設定ウィザードの使用](#)」を参照してください。

- ▶ インストール中、NNMi のインストール ルーチンは [ローカル サービス] アカウントを有効にし、組み込み DB サービス (nmsdbmgr) を実行します。
- ▶ NNMi をインストールして、アプリケーション フェイルオーバーまたは HA 構成で既存の Oracle データベース インスタンスを使用する場合は、『[HP Network Node Manager i Software デプロイメントリファレンス](#)』の手順を参照してください。

26 **【完了】** をクリックして、インストールを終了します。

NNMi のサイレント インストール

このセクションでは、システムへの入力が必要としない NNMi のサイレント インストールの 2 つの実行方法について説明します。

- 26 ページの「[ovinstallparams.ini サンプル ファイルを使用したサイレント インストール](#)」に、サンプルファイルとして、ovinstallparams.ini ファイルを使用した、NNMi のサイレント インストール手順が記載されています。
- 28 ページの「[以前のインストールの ovinstallparams.ini ファイルを使用したサイレント インストール](#)」に、以前のインストールでインストールされた ovinstallparams<time_stamp>.ini ファイルを使用した、NNMi のサイレント インストール手順が記載されています。

誤解を避けるために、このセクションでは以下の用語を使用します。

- **ソース** - NNMi のインストール ウィザードを使用して初期インストールを行うサーバーです。このサーバーに指定するインストール オプションは、以降のサイレント インストールで使用するために保存されます。
- **ターゲット** - サイレントインストールを行うサーバーです。

ovinstallparams.ini サンプル ファイルを使用したサイレント インストール

NNMi インストール メディアには、ovinstallparams.ini ファイルの例が含まれています。NNMi インストール メディアのサポート ディレクトリを参照し、ファイルの中身を表示するか、このサンプルの ovinstallparams.ini ファイルのコピーを入手します。

▶ NNMi のサポート対象のバージョンからアップグレードを行わない限り、以前の NNMi のインストールがすべて削除されていることを確認します。詳細については、『HP Network Node Manager i Software デプロイメント リファレンス』の「**NNMi 9.0x** からのアップグレード」および 38 ページの「**NNMi の削除**」を参照してください。

- 1 管理者権限を持つユーザーとして、ターゲット サーバー (NNMi をインストールするサーバー) にログオンします。
- 2 NNMi インストールメディアの **support** ディレクトリから以下のディレクトリに、ovinstallparams.ini ファイルをコピーします。
%TEMP%
- 3 以下に示すように、ovinstallparams.ini ファイルを変更します。
 - a 以下のエントリは、組み込みデータベースで使用するようサイレントインストール スクリプトを設定します。これらの設定を以下のように設定します。

```
[obs.install]  
db.embedded=Solid
```

▶ Oracle データベースを使用しており、HA またはアプリケーション フェイルオーバーを使用していない場合は、db.instance パラメータに一意の値を使用する必要があります。

▶ Oracle データベースを使用しており、HA またはアプリケーション フェイルオーバーを使用する場合は、サイレント インストールを開始する前に、ソース システムで **ovstop -c** コマンドを実行します。

- b 以下のエントリは、NNMi にアクセスする HTTP ポート番号を設定します。一般的に、**Windows** オペレーティング システムに **NNMi** をインストールする場合はポート 8004 (既存のポート番号)、**UNIX** オペレーティング システムに **NNMi** をインストールする場合はポート 80 を使用します。

```
[nonOV.jboss]
```

```
httpport=8004
```

- 4 ターゲット サーバーで、DVD ドライブに **NNMi** インストール メディアを挿入します。
- 5 コマンド プロンプトで、以下のコマンドを入力します。

```
<DVD_drive>%setup.exe -i silent
```

サイレントインストールは、バックグラウンドプロセスとして実行され、しばらく時間がかかります。進行状況は表示されません。

サイレント インストールが完了すると、**NNMi** がターゲット サーバーにインストールされ、使用できるようになります。

- 6 **NNMi** サービスが実行されていることを確認するには、コマンドラインに以下を入力します。

```
ovstatus -c
```

- 7 **ovstop -c** コマンドを使用して **NNMi** プロセスを停止します。
- 8 ルートまたは管理者として **nnmchangesyspw.ovpl** スクリプトを実行し、システム パスワードを設定します。[手順 10](#) を実行するには、この新しいシステム パスワードが必要です。
- 9 **ovstart -c** コマンドを使用して **NNMi** プロセスを開始します。
- 10 **NNMi** の設定については、30 ページの「[クイック スタート設定ウィザードの使用](#)」を参照してください。

以前のインストールの ovinstallparams.ini ファイルを使用したサイレント インストール

対話形式によるインストール ウィザードを使用して **NNMi** を初回インストールしたときの質問に対する応答は、ovinstallparams<time_stamp>.ini ファイルに保存されます。このファイルは、システムへの入力を必要としない **NNMi** のサイレントインストールを実行する場合に、入力ファイルとして使用されます。

インストールの質問ファイルは、以下の場所に保存されます。

```
%TEMP%\¥HPOvInstaller¥NNM_<version_number>¥
```

NNMi のサイレント インストールを実行するには、以下の手順に従います。

- 1 管理者権限を持つユーザーとして、ターゲット サーバー (**NNMi** をインストールするサーバー) にログオンします。
- 2 %TEMP%\¥HPOvInstaller¥ フォルダが存在する場合は削除します。
- 3 ソース サーバーでは、**NNMi** のインストール ウィザードを使用して、**NNMi** のインストールを完了します。19 ページの「**NNMi のインストール**」を参照してください。



サイレント インストールを完了するには、ターゲット サーバーと同じオペレーティング システムをソース サーバーで実行している必要があります。たとえば、**Windows** ターゲットサーバーに **NNMi** をサイレントインストールするには、ソースサーバーも **Windows** サーバーである必要があります。

- 4 ソース サーバーにおける以下のファイルのバックアップ コピーを作成し、安全な場所に保管してください。

```
%TEMP%\¥HPOvInstaller¥NNM_<version_number>¥  
ovinstallparams<time_stamp>.ini
```

- 5 ovinstallparams<time_stamp>.ini ファイルを、ソース サーバーからターゲット サーバーに以下の手順でコピーします。
 - a ターゲット サーバーの %TEMP%\¥ フォルダに ovinstallparams<time_stamp>.ini ファイルを配置します。
 - b コピーしたファイルの名前を以下のように変更します。
ovinstallparams.ini

- 6 ovinstallparams.ini ファイルに、以下の 2 行を追加します。

```
[nonOV.jboss]
httpport=<port_number>
```

この例では、<port_number> は、対話形式によるインストールにおいて 23 ページの[手順 18](#) で特定されたポートです。

例：

```
[nonOV.jboss]
httpport=80
```



以前のインストールで Oracle データベースを使用しており、HA またはアプリケーション フェイルオーバーを使用していなかった場合は、db.instance パラメータに一意の値を使用する必要があります。

- 7 ターゲット サーバーで、DVD ドライブに NNMi インストール メディアを挿入します。
- 8 コマンド プロンプトで、以下のコマンドを入力します。

```
<DVD_drive>¥setup.exe -i silent
```

サイレントインストールは、バックグラウンドプロセスとして実行され、しばらく時間がかかります。進行状況は表示されません。

サイレント インストールが完了すると、NNMi がターゲット サーバーにインストールされ、使用できるようになります。

- 9 NNMi サービスが実行されていることを確認するには、コマンドラインに以下を入力します。

```
ovstatus -c
```

- 10 **ovstop -c** コマンドを使用して NNMi プロセスを停止します。
- 11 管理者として **nnmchangesyspw.ovpl** スクリプトを実行し、システム パスワードを設定します。[手順 13](#) を実行するには、この新しいシステム パスワードが必要です。
- 12 **ovstart -c** コマンドを使用して NNMi プロセスを開始します。
- 13 NNMi の設定については、30 ページの「[クイック スタート設定ウィザードの使用](#)」を参照してください。

クイック スタート設定ウィザードの使用

このセクションでは、NNMi のいくつかの基本的な設定タスクについて説明します。このタスクは、NNMi のインストール後に完了する必要があります。

以下のような初期設定（たとえばテスト環境）では、**クイック スタート設定ウィザード**を使用することを推奨します。

- SNMP コミュニティ文字列の設定
- ネットワークノードの制限範囲の検出
- 初期管理者アカウントの設定



クイック スタート設定ウィザードを使用して、SNMP バージョン 3 (SNMPv3) 設定を完了させることはできません。SNMPv3 を使用して監視するデバイスがある場合は、以下を実行します。

- 1 NNMi コンソールを開きます。
- 2 **【設定】** ワークスペースの **【通信の設定】** を選択します。
- 3 SNMPv3 設定を完了します。

初期環境設定の完了後は、NNMi コンソールを使って、ネットワーク トポロジへのノードの追加やモニタリングの設定のような、追加の環境設定作業を行うことができます。詳細については、NNMi ヘルプを参照してください。

検出シードおよび自動検出ルールについて

検出シードとは、NNMi によるネットワーク トポロジの検出を助けるためのノードです。たとえば、管理環境内のコア ルーターなどがシードになることができます。各シードは、IP アドレスまたはホスト名により識別されます。NNMi ヘルプの「*自動検出ルールを設定する*」を参照してください。

- シードとして指定したデバイスのみが検出されるように検出を設定するには、自動検出を無効にします。NNMi ヘルプの「*自動検出ルールを使用しない*」を参照してください。
- シードとして指定したデバイスが、追加検出の開始ポイントとなるように検出を設定するには、自動検出ルールを作成して設定してください。NNMi ヘルプの「*検出ノードを指定する*」を参照してください。

検出プロセスの概要については、NNMi ヘルプの「*スパイラル検出の動作原理*」を参照してください。

- 1 インストールプロセスが完了すると、[**クイックスタート設定ウィザードを起動**] ダイアログ ボックスが表示されます。[**はい**] をクリックします。

▶ **クイックスタート設定ウィザード**は、インストール後すぐに実行する必要があります。**クイックスタート設定ウィザード**を手動で起動するには、以下の URL にアクセスします。

`http://<fully_qualified_domain_name>:<port_number>/quickstart/`

<fully_qualified_domain_name> は NNMi 管理サーバーの完全修飾ドメイン名で、**<port_number>** は 23 ページの**手順 18**に説明されているポート番号です。

使用している NNMi 管理サーバー に複数のドメイン名がある場合は、NNMi では、インストール時にその中から 1 つを選択します。NNMi が使用している完全修飾ドメイン名を判断するには、**nnmofficialfqdn.ovpl** スクリプトを実行します。詳細については、**nnmofficialfqdn.ovpl** リファレンス ページまたは UNIX のマンページを参照してください。

NNM クイック スタート設定ウィザードが、Web ブラウザのウィンドウで開きます。

- 2 以下のようにログオンします。

ユーザー名 : **system**

パスワード : インストール プロセスの最後 (23 ページの**手順 17**) またはサイレント インストール中 (29 ページの**手順 11**) に作成したパスワード。

- 3 [**コミュニティ文字列の設定**] ページで、検出範囲内にあるノードのいずれかのコミュニティ文字列を入力し、[**追加**] をクリックします。

▶ NNMi は、コミュニティ文字列を、既知のデバイスと自動的に照合します。特定のデバイスと各コミュニティ文字列の関連付けを、手動に行う必要はありません。

- 4 **[SNMP コミュニティ文字列]** のリストに、検出範囲内のすべてのノードのコミュニティ文字列が含まれるまで **手順 3** を繰り返し、**[次へ]** をクリックします。

➤ ここで追加した **SNMP コミュニティ文字列** が、NNMi データベースに保存されます。NNMi コンソールでは、**SNMP コミュニティ文字列** は、**[通信の設定]** フォームの **[デフォルトの SNMPv1/v2 コミュニティ文字列]** タブに表示されます。

- 5 **[自動検出ルールの設定]** ページにて、既存のルール名と **[含まれる IP アドレス範囲]** との関連付けを行います。検出規則のための IP アドレス範囲を入力し、**[次へ]** をクリックします。

以下は、有効な IP アドレス範囲の例です。

- 10.1.1.*
- 10.1.1.1-99
- 10.10.50-55.*
- 10.1-7.1-9.1-9

コミュニティ文字列の追加
自動検出の設定
検出シードの追加
シードのテスト
管理者アカウントの作成
要約

自動検出ルールの設定

ルール名と含まれる IP アドレス範囲を設定している場合には、NNMi はその IP アドレス範囲に含まれるネットワーク デバイスを自動的に検出します。[含まれる IP アドレス範囲] フィールドに自動検出ルール名とアドレスの範囲を入力してください。

ルール名:
含まれる IP アドレス範囲:

- 6 **[シードの設定]** ページで、ネットワークに検出シードの情報を追加します。その後、**[次へ]** をクリックします。

検出シードを、IP アドレスまたは完全修飾ドメイン名の形式で入力します。これらシードで示されたネットワーク デバイスにより、NNMi のスパイラル検出プロセスがネットワークを検出できるようになります。

➤ コマンドラインから、`nnmloadseeds.ovpl` コマンドを使用してシードをロードできます。詳細については、*nnmloadseeds.ovpl* のリファレンス ページまたは UNIX のマンページを参照してください。

- 7 **[シードのテスト]** ページで、通信テストの結果を確認します。手順 3 で特定したコミュニティ文字列では、どのシード ノードにも到達できない場合には、**[前へ]** をクリックし、**[コミュニティ文字列の設定]** ページまで戻ってください。コミュニティ文字列を修正してから、**[次へ]** をクリックします。
- 8 すべてのノードに到達できるまで、手順 7 を繰り返したら、**[次へ]** をクリックします。
- 9 **[管理者アカウントの設定]** ページで、NNMi ソフトウェアを管理している新規アカウントのユーザー名を入力し、パスワードを設定して **[次へ]** をクリックします。
- 10 **[要約]** ページで、指定した情報を確認し、以下のいずれかを実行します。
 - 設定の変更を行う場合は、**[前へ]** をクリックします。
 - 現在の設定を使用する場合、**[コミット]** をクリックします。

<p>コミュニティ文字列の追加</p> <p>自動検出の設定</p> <p>検出シードの追加</p> <p>シードのテスト</p> <p>管理者アカウントの作成</p> <p>要約</p>	<p>要約</p> <div> <p>表示された情報をレビューし、ナビゲーションボタンを使って修正します。コミットを使って、設定変更を適用して保存します。</p> </div> <div> <p>デフォルトのコミュニティ文字列: [ntcpublish]</p> <p>自動検出ルール: quickstart ルール</p> <p>含める IP 範囲: 10.97.*.*</p> <p>シード: [10.97.246.162, 10.97.246.196]</p> <p>管理者ユーザー名: system</p> </div>
--	---

- 11 **[ウィザードは終了しました]** ページでは、ネットワークの一部を検出するために NNMi を正常に設定したことが表示されます。**[前へ]** をクリックして変更をするか、**[UI を起動]** をクリックします。

NNMi コンソール ユーザー インタフェースが表示されます。NNMi の使用を開始するには、[第 4 章、NNMi 入門](#)を参照してください。

▶ インストール後、ウイルス対策ソフトウェアを再起動します。[52 ページ](#)の「[ウイルス対策ソフトウェアの無効化](#)」を参照してください。

NNMi ライセンスの取得

恒久ライセンス キーをインストールしていない場合は、NNMi 製品には、NNMi のインストール後 60 日間有効な一時試用ライセンス キーが含まれています。この一時試用ライセンス キーを使用すると、NNMi Advanced 機能を使用できるようになります。できるだけ早く、恒久ライセンス キーを入手し、インストールしてください。

NNMi Advanced のライセンスに含まれる機能のリストを表示するには、『HP NNMi Software リリースノート』の「ライセンス」のセクションを参照してください。

恒久ライセンス キーのインストール準備

試用ライセンスでは、250 ノードまでの制限が付けられています。試用ライセンス キーで NNMi を実行している場合、恒久ライセンスでサポートできる数以上のノードを管理できる場合があります。ただし、恒久ライセンスが有効になると、ライセンス制限を超えた分のノードは NNMi により自動的に管理対象外になります。

恒久ライセンスでは管理対象から除外するノードをご自身で決定する場合は、新規ライセンス キーをインストールする前に、あまり重要でないノードを NNMi コンソール を使用して削除してください。

ライセンスの種類および管理対象ノードの数の確認

現在、NNMi が使用しているライセンスの種類を確認するには、以下の手順に従います。


- 1 NNMi コンソール で、[ヘルプ] > [HP Network Node Manager i Software について] の順にクリックします。
- 2 [HP Network Node Manager i Software について] ウィンドウで、[ライセンス情報] をクリックします。

([ライセンス情報] は、NNMi コンソールのサインインのページからでも使用可能です。)

- 3 **【消費】**フィールドに表示されている値を探します。この値が、現在 NNMi が管理しているノードの数です。
- 4 恒久ライセンスがサポートできるノード数が、現在 NNMi が管理しているノード数より少ない場合は、NNMi コンソールを使用して、あまり重要でないノードを削除します。詳細については、NNMi ヘルプの「**ノードの削除**」を参照してください。

恒久ライセンス キーの取得およびインストール

恒久ライセンス キーを申請するには、以下の情報が必要です。

- HP 製品番号や製造番号が明記されたエンタイトルメント証明書
 - NNMi 管理サーバーの IP アドレス
 - HA で動作する NNMi のライセンスの場合は、クラスタの仮想 IP アドレス
-  NNMi を HA で実行する場合は、NNMi の商用ライセンスはクラスタの仮想 IP アドレスが対象になります。さらに、HA クラスタのいずれかのノードでは、NNMi の非商用ライセンスが必要です。
- お客様の企業情報もしくは団体情報

Autopass および HP 注文番号の使用 (ファイアウォール使用時は不可)

恒久ライセンス キーを入手してインストールするには、以下の手順に従ってください。

- 1 コマンドプロンプトで、以下のコマンドを入力し、Autopass ユーザーインターフェースを開きます。
nnmlicense.ovpl NNM -gui
- 2 Autopass ウィンドウの左側で、**【ライセンス管理】**をクリックします。
- 3 **【ライセンス キーのインストール】**をクリックします。
- 4 **【ライセンス キーの取得 / インストール】**をクリックします。
- 5 HP 注文番号を入力し、Autopass プロンプトに従ってライセンスキーの取得プロセスを完了します。
- 6 NNMi のインストールは自動的に完了します。

コマンド行で、シードを追加する

自動プロセスを実行しても完了しない場合は（たとえば NNMi 管理サーバーがファイアウォールの背後にあるなど）、以下の手順を実行します。

- 1 ライセンスキーを取得するには、以下の HP パスワード配信サービスサイトを表示します。

<https://webware.hp.com/welcome.asp>

- 2 NNMi 管理サーバーのコマンドプロンプトで以下のコマンドを入力し、システムをアップデートして、ライセンスデータファイルを格納します。

`nnmlicense.ovpl NNM -f license_file`

（製品ライセンス ID (NNM) では大文字と小文字が区別されます。）

詳細については、*nnmlicense.ovpl* のリファレンス ページまたは UNIX のマニページを参照してください。

- 3 NNMi のインストールは自動的に完了します。

ライセンスキーの追加取得

NNMiライセンス構造に関する詳細についてHP営業担当またはHewlett-Packard正規販売店に問い合わせ、企業向けインストールにライセンス層を追加する方法について調べます。

追加のライセンス キーを取得するには、HP ライセンス キー配信サービスに移動します。

<https://webware.hp.com/welcome.asp>

詳細については、NNMi ヘルプの「*ライセンス機能の拡張*」を参照してください。

開発者の方へ： NNMi 開発者ツールキットを使用すると、カスタム Web サービスクライアントを統合して NNMi の機能を拡張できます。NNMi 開発者ライセンスをインストールすると、NNMi により doc フォルダに sdk-dev-kit.jar ファイルが作成されます。sdk-dev-kit.jar ファイルを解凍すると、NNMi 開発者ツールキット ドキュメントやサンプル集を表示できます。

NNMi の削除

ローカルシステムから NNMi を削除するには、以下の手順に従います。

- 1 NNMi を削除するシステムに、管理者権限を持つユーザーとしてログオンします。
- 2 システムにあるいくつかのウイルス対策ソフトウェアを無効にします。
52 ページの「[ウイルス対策ソフトウェアの無効化](#)」を参照してください。
- 3 アプリケーションフェイルオーバー、グローバルネットワーク管理、HA を使用するよう NNMi を設定した場合は、『NNMi デプロイメントリファレンス』の指示に従って、NNMi からこのような機能を設定解除します。
- 4 **nnmversion.ovpl** スクリプトを実行し、NNMi 管理サーバーにインストールされている NNMi パッチのリストを取得します。
- 5 NNMi 管理サーバーにインストールされているすべての NNMi パッチを削除します。パッチの削除方法については、パッチごとにパッチインストールのテキストを参照してください。

▶ パッチをアンインストールするには、[スタート] > [すべてのプログラム] > [HP] > [Network Node Manager] > [Uninstall Patch] を使用します。

- 6 NNMi のアンインストールを開始するには、以下のいずれかを実行します。
 - コマンドプロンプトで、以下のコマンドを入力します。
%NnmInstallDir%\Uninstall\NNMi\setup.exe
 - **setup.exe** コマンドを実行する代わりに、[スタート] > [すべてのプログラム] > [HP] > [Network Node Manager] > [Uninstall NNM] メニュー アイテムの順に選択してアンインストールを実行することができます。

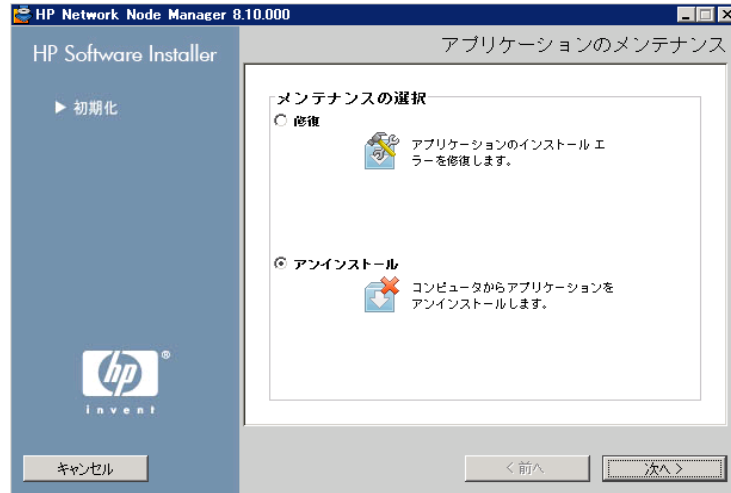
▶ このコマンドは大文字と小文字を区別します。

▶ **setup.exe** コマンドで **-i silent** オプションを使用すると、NNMi のサイレントアンインストールを実行できます。

インストールの初期化プロセスで、使用する言語の選択が要求されます。この言語はシステムがサポートする言語から選択できます。その後、このプロセスでは、ソフトウェアの削除準備ができているかどうかシステムがチェックされます。

[アプリケーションの要件チェックの警告] ダイアログ ボックスが表示された場合、各警告をクリックして、内容を理解した上で対処法を決定します。

- 7 **[アプリケーションの要件チェックの警告]** ダイアログボックスで警告に対処した後、**[続行]** をクリックします。
- 8 インストール プロセスは、システムのインベントリを終了すると、メンテナンス タスクを選択するように要求します。**[アンインストール]** を選択し、**[次へ]** をクリックします。



- 9 **[プレアンインストールの概要]** ページで、システムから削除するファイルのリストを確認し、以下のいずれかを実行します。
 - アンインストールを中止する場合は、**[キャンセル]** をクリックします。
 - 戻るには、**[前へ]** をクリックします。
 - システムからファイルを削除する場合は、**[アンインストール]** をクリックします。
- 10 **[アンインストールの完了]** ページで、**[完了]** をクリックします。

NNMi インストール ログ ファイルへのアクセス

NNMi は、インストールおよび削除プロセスについての情報を記録します。その情報については、以下の場所で確認することができます。

`%NnmDataDir%\log\%nnm%`

最も重要なログ ファイルは以下のとおりです。

- `nnm-install-config.log`: 初期化されたプロセスを含む、最新のインストール情報が記録されます (`nnm-install-config.log` ファイルの最後を参照)。
- `%TEMP%\nnm-install-config_vbs.log`: インストール前後のアクティビティが記録されます。
- `%TEMP%\HPOvInstallerLog.txt`: NNMi をインストールした後に疑わしい問題がある場合は、このログファイルを確認します。

さらに、下記のログ ファイルも役立つ可能性があります。

- `%TEMP%\nnm-preinstallcheck.log`: プレインストールのチェックに未解決の警告またはエラーが含まれる場合、このログファイルを問題の診断材料に使用します。
- `%TEMP%\NNMUninstall.log`: NNMi をアンインストールした後に疑わしい問題がある場合は、このログファイルを確認します。

4 NNMi 入門

この章では、検出プロセスについての詳細など、NNMi でネットワーク管理を始めるにあたり必要な情報を記載しています。オペレータおよび管理者用の詳細情報は、NNMi ヘルプに記載されています (44 ページの「[NNMi ヘルプ](#)」を参照)。

NNMi へのアクセス

NNMi をインストールし、インストール後の設定作業を完了し、**クイック スタート設定ウィザード**を使用して検出の設定を行ったので、ネットワークの管理を開始できます。ネットワークのモニタリングやイベント処理のタスクについては、Web ブラウザのウィンドウで開く **NNMi コンソール** からアクセスすることができます。



日本語または中国語 (簡体字) で NNMi コンソールを表示するには、ブラウザで言語を設定してください。

NNMi コンソール にアクセスするには、以下の手順に従います。

- 1 対応 Web ブラウザを使用していることを確認してください (9 ページの「[対応ハードウェアおよびソフトウェア](#)」を参照)。
- 2 Web ブラウザで JavaScript、NNMi 管理サーバーからのポップアップ ウィンドウを有効にし、ブラウザが NNMi 管理サーバーからの cookie を受け入れるようにします (53 ページの「[NNMi コンソール 用の Web ブラウザの有効化](#)」を参照)。

- 3 以下の URL を Web ブラウザのアドレス入力用のウィンドウに入力します。

`http://<fully_qualified_domain_name>:<port>/nnmi/`

<fully_qualified_domain_name> は、NNMi 管理サーバーの完全修飾ドメイン名を表し、**<port>** は、jboss アプリケーション サーバーが NNMi コンソールとの通信で使用するポートを表します。

▶ 使用している NNMi 管理サーバー に複数のドメイン名がある場合は、NNMi では、インストール時にその中から 1 つを選択します。NNMi が使用している完全修飾ドメイン名を判断するには、**`nnmofficialfqdn.ovpl`** スクリプトを実行します。詳細については、**`nnmofficialfqdn.ovpl`** リファレンス ページまたは UNIX のマンページを参照してください。

どのポートを使用するかが不明な場合は、58 ページの「[問題 : NNMi コンソールのページが見つからない](#)」を参照してください。

▶ ブラウザで Windows オペレーティングシステムにインストールされている NNMi 管理サーバーを指しても NNMi コンソールを起動できない場合、NNMi 管理サーバーで Windows ファイアウォールが http ポートをブロックしている可能性があります。62 ページの「[問題 : Windows NNMi 管理サーバーにアクセスしていると、NNMi コンソールを起動できない](#)」を参照してください。

新規 Web ブラウザのウィンドウから NNMi コンソール を起動するか、または現在の Web ブラウザのウィンドウを使用するのかを、NNMi コンソール 製品のウィンドウでリンクを選択します。

NNMi サインイン用ウィンドウで、ユーザーのアカウント名とパスワードを入力したあと **[サインイン]** をクリックします。詳細については、43 ページの「[ユーザーのアカウントとロール](#)」を参照してください。

ユーザーのアカウントとロール

インストール中の **NNMi** への初回アクセスのために、**NNMi** は特別のシステムアカウントを提供します。インストール後は、このシステムアカウントは使用しないでください。

通常のご使用のために、**NNMi** 管理者は各ユーザー（またはユーザーグループ）のアカウントを設定し、各アカウントに対し定義済みのユーザーロールを割り当てます。ユーザーロールによって、**NNMi** コンソールにアクセスできるユーザーと、各ユーザーが使用できるワークスペースとアクションが決まります。**NNMi** では、**NNMi** コンソールへのアクセスに対して以下のユーザーロールが用意されています。これらのロールは、プログラムによってあらかじめ定義されており修正はできません。

- 管理者
- オペレータ レベル 2
- オペレータ レベル 1
- ゲスト

チームのために **NNMi** サインインのアクセス設定を行う前に、各チームのメンバに、どの定義済みの **NNMi** ロールを割り当てるのがふさわしいかを判断します。ロールは階層的です。すなわち、階層内で高位のロールは下位のロールの特権をすべて含みます（管理者が最高位で、ゲストが最低位です）。

コマンドラインへのアクセスと同様、ユーザーのアカウントとロールは、**NNMi** コンソールで設定します。詳細については、**NNMi** ヘルプの「*NNMi* へのアクセスの制御」を参照してください。



NNMi には、インストール時に作成された自己署名証明書を使用してそのまま使用できる **https** 設定があります。自己署名証明書の代わりに認証機関による署名入り証明書を使用する場合の詳細については、『**HP Network Node Manager i Software** デプロイメント リファレンス』を参照してください。

NNMi ヘルプ

NNMi ヘルプには、NNMi コンソール の使用方法が記載されています。NNMi ヘルプの詳細情報は、下記のセクションに分類されています。

- NNMi コンソールの使用法
- オペレータ用のヘルプ
- 管理者用のヘルプ

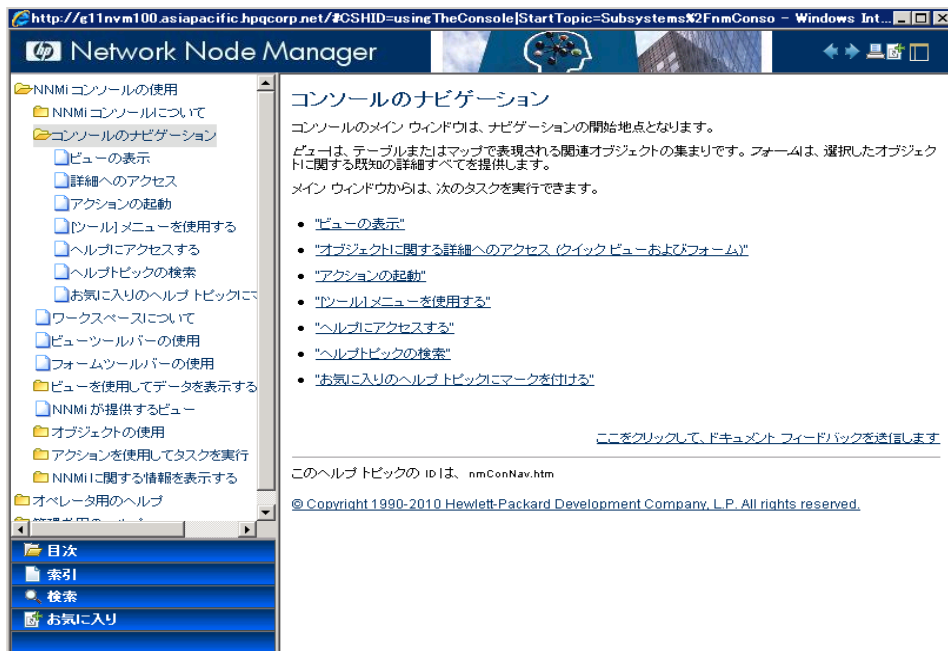
NNMi のヘルプにアクセスするには、NNMi コンソール メニュー バーの **[ヘルプ]** をクリックし、メニューにある最初の区切りラインの上のオプションの 1 つをクリックしてください。



NNMi コンソール には、情報入力フォームが含まれています。フォーム名は、ウィンドウの右上のコーナーに表示されています。どの NNMi フォームからでも、フォームのヘルプ情報にアクセスすることができます。**[ヘルプ]** メニューで、**[<xyz> フォームの使用法]** (<xyz> は現在のフォームのタイトル) をクリックしてください。

図 1 は、NNMi ヘルプ ウィンドウを示しています。

図 1 NNMi ヘルプ



ネットワーク検出の設定

NNMi を使ってネットワークの検出や管理を開始するときは、テスト用ネットワークから始め、ごくわずかのインタフェースしか持たない少数のノードを検出、管理するように NNMi を設定することをお勧めします。**クイック スタート設定ウィザード** (30 ページを参照) を使用すると、このような小さな構成が簡単に設定できます。NNMi のインストール直後は、**クイック スタート設定ウィザード** を使用することを推奨します。

NNMi の操作に慣れると、どのようにその豊富な機能がネットワークの管理に使われているのかを理解できるようになります。NNMi で管理するネットワークポロジは、検出規則や管理領域を系統的に追加していくことにより、次第に拡張していくことができます。

ここでは検出プロセスを開始する前に必要となる定作業について、簡単に概要を説明します。表 5 のチェックリストでは、これらの作業についてまとめてあります。

表 5 検出設定チェックリスト

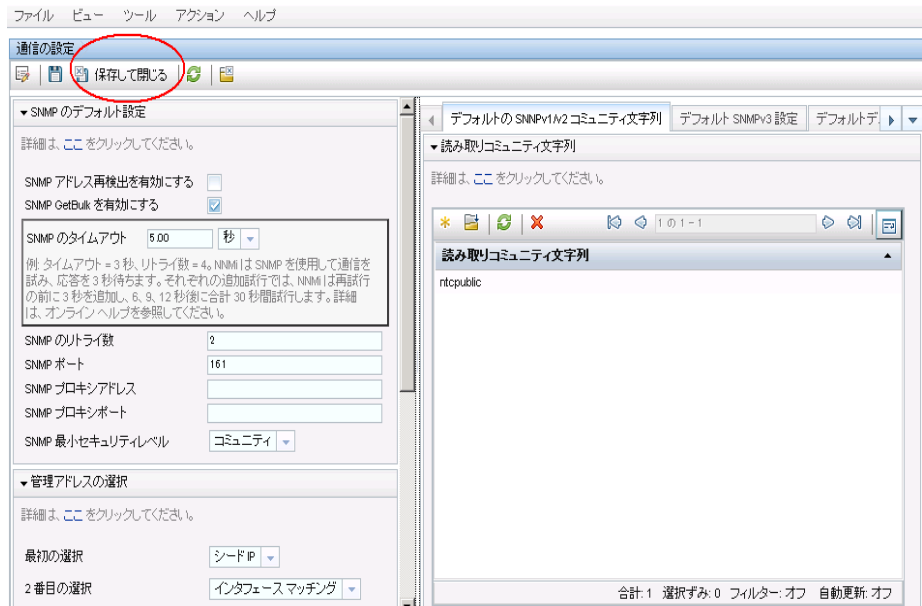
チェック 欄 (はい/ いいえ)	タスク
	検出するノードのすべてがネットワークに接続され、それに対応している SNMP のバージョン (SNMPv1、SNMPv2c、または SNMPv3) で設定されているかを検証します。
	ネットワーク管理者より、管理するノードの読み取り専用コミュニティ文字列を入手します。
	NNMi コンソールを使用して、46 ページの「コミュニティ文字列の設定」に記載されている手順でコミュニティ文字列を設定します。
	NNMi コンソールを使用して、47 ページの「自動検出ルールの設定」に記載されている手順でスパイラル検出プロセスを設定します。
	NNMi コンソールを使用して、49 ページの「検出の進行状況の確認」に記載されている手順でスパイラル検出プロセスをチェックします。

検出プロセスの詳細については、NNMi ヘルプの「ネットワークの検出」を参照してください。

コミュニティ文字列の設定

コミュニティ文字列を使用して NNMi を設定するには、以下の手順に従います。

- 1 ワークスペースのナビゲーションパネルで **[設定]** ワークスペースを選択します。
- 2 以下のように、**[通信の設定]** フォームを開きます。



- 3 **[デフォルトの SNMPv1/v2 コミュニティ文字列]** タブで、**[新規作成]** アイコンをクリックします。
- 4 **[デフォルトの読み取りコミュニティ文字列]** フォーム上の **[読み取りコミュニティ文字列]** のボックスに、検出範囲内の特定のノードのコミュニティ文字列を入力して、**[保存して新規作成]** アイコンをクリックします。
- 5 手順 4 を繰り返し実行し、検出範囲内のノードのコミュニティ文字列をすべて入力してから、**[保存して閉じる]** アイコンをクリックします。
- 6 **[通信の設定]** フォームで、**[保存して閉じる]** アイコンをクリックします。

デバイスのコミュニティ文字列の設定やファイルからのコミュニティ文字列のロードの詳細については、NNMi ヘルプの「**通信プロトコルを設定する**」を参照してください。

自動検出ルールの設定

ネットワーク管理で最も重要な作業の一つは、常に最新のネットワーク トポロジを把握しておくことです。NNMi は、ネットワーク ノードの継続検出によってこのトポロジを維持します。NNMi の検出プロセスは、根本原因解析やトラブルシューティングのツールが、インシデント解決のための正確な情報を提供することを保証します (48 ページの「ネットワーク検出」を参照)。

自動検出ルールを設定するには、以下の手順に従います。

- 1 ワークスペースのナビゲーションパネルで **[設定]** ワークスペースを選択します。
- 2 **[検出の設定]** フォームを開きます。
- 3 **[自動検出ルール]** タブをクリックし、次に **[新規作成]** アイコンをクリックします。
- 4 **[自動検出ルール]** フォームの **[基本]** のところに、ルールの **名前** および **順序** の情報を入力します。
この順序は、他の自動検出ルールに対するこのルールの優先度を示す数値です。詳細については、**[ヘルプ]** > **[自動検出ルールフォームの使用方法]** の順にクリックしてください。
- 5 **[このルールの自動検出開始ポイント]** で、この規則に対する適切な自動検出アクションを選択します。
- 6 **[IP の範囲]** タブで、**[新規作成]** アイコンをクリックします。
- 7 **[IP の自動検出範囲]** フォームで、**[IP の範囲]** を入力し、**[範囲のタイプ]** は **[ルールに含める]** という設定のままにして、**[保存して閉じる]** アイコンをクリックします。
- 8 **[自動検出ルール]** フォームで、**[保存して閉じる]** アイコンをクリックします。
- 9 **手順 3** から **手順 8** までを繰り返し実行し、使用するすべてのルールを追加します。
- 10 **[検出の設定]** フォームで、**[保存して閉じる]** アイコンをクリックし、すべての新しい自動検出ルールを NNMi データベースに保存します。
- 11 **[設定]** ワークスペースから **[検出]** を開き、**[シード]** をクリックします。
- 12 **[新規作成]** アイコンをクリックします。

13 **【 検出シード 】**のフォームで、ホスト名または IP アドレスを入力し、**【 保存して閉じる 】**アイコンをクリックします。

14 **手順 12**および**手順 13**を繰り返して、検出シード用のすべてのホスト名または IP アドレスを追加します。

検出の進行状況をモニタリングする方法は、49 ページの「**検出の進行状況の確認**」を参照してください。



検出の設定の詳細については、NNMi ヘルプの「**検出の設定**」を参照してください。

ネットワーク検出

NNMi は、ネットワークにあるデバイス（スイッチやルータなど）に関する情報を収集したり、ユーザーやチームにとって重要なデバイスの管理を積極的に行ったりします。検出モードは、以下の 2 つから選ぶことができます。

- **検出シード**：ユーザーが、デバイスのリストを提供して、NNMi の検出やモニタリングの対象となるデバイスを包括的に管理します。
- **自動検出ルール**：ユーザーが検出シードとなるアドレスやホスト名のリストを提供し、NNMi はこの情報を包括的な自動検出用の開始ポイントとして使用します。さらに、ユーザーは、IPv4 アドレス範囲や MIB II sysObjectIDs を提供することにより、NNMi の検出プロセスに制限をかけます。

検出モードの選択が済むと、**NNMi スパイラル検出**を行います。NNMi は、さまざまなプロトコルや技術を利用して、ネットワーク インベントリについての豊富な情報を収集し、デバイス（サブネットや VLAN）間の関係を確認し、デバイス間の接続関係を正確に描き出します。NNMi Causal Engine は、各デバイス（および、デバイスに関連する各インタフェースやアドレス）の現在のステータスを判定し、発生した問題や潜在的な問題を検出した場合には、積極的に通知を行います。

ダイナミック検出プロセスは、長期的に継続されます。ネットワーク管理ドメインの中でなんらかの変化が起こった際には、NNMi スパイラル検出が自動的に情報を更新します。

ネットワーク検出の詳細については、NNMi ヘルプの「**ネットワークの検出**」を参照してください。

検出の進行状況の確認

スパイラル検出プロセスの起動後、そのプロセスが正しく実行されているか検証します。



スパイラル検出は動的であるため、NNMi は継続的にネットワーク ノードを検出します。NNMi は、検出規定に新しいノードが追加されるたびに、そのノードを検出し、ノードに関するトポロジ情報を収集し、ノードのモニタリングを開始します。

検出の進行状況の測定にはいくつかの方法があります。検出の進行状況を調べるには、以下のいずれかの処理を実行します。

- 検出中に、**[設定] > [検出] > [シード]**の順に操作し、シードのステータスをチェックします。**[検出シードの結果]**列のステータス情報を確認します。検出が終わりに近づくと、ノードの大半が「**ノードが作成されました**」のステータスになります。
- 検出中に、**[ヘルプ] > [システム情報]**から**[データベース]**をクリックして、検出の進行状況を確認します。**[データベースのオブジェクト数]**を 1 時間に数回確認します。**ノード、SNMP エージェント、インタフェース、IP アドレス、L2 接続**のフィールドの数は、必ず一定になります。サンプリング周期を通して、この数字の増加がなければ、検出は完了です。
- 検出中に、NNMi コンソールで、**[インベントリ]**ワークスペースから**[ノード]**を選択します。**[合計]**フィールドの値を 1 時間に数回確認します。サンプリング周期を通して、この値の増加していなければ検出は完了です。
- 検出中に、NNMi コンソールで **[ツール] > [NNMi セルフモニタリングのグラフ] > [検出の進行状況]**をクリックして、検出の進行状況を確認します。
- 検出中に、NNMi コンソールで **[ツール] > [ステータス分布グラフ] > [ノードステータス]**をクリックして、検出の進行状況を確認します。
- 検出中にNNMi コンソールの**[トポロジマップ]**ワークスペースの**[ネットワークの概要]**をクリックします。マップの複雑性の成長を 1 時間監視します。マップの成長が鈍化し、サンプリング周期を通してこの成長が止まれば、検出は完了です。



検出で問題が発生する場合は、61 ページの「**問題 : NNMi がノードを検出しない**」を参照してください。

A 追加情報

以下のセクションでは、NNMi のインストールと、NNMi の使用開始時の問題のトラブルシューティングについて説明します。また、本ガイドの他のセクションでも、必要に応じてこのセクションを参照しています。

ディスク レベルで互換性のあるセキュリティ レベルの設定

NNMi をインストールする前にディスク ドライブに互換性のあるセキュリティ レベルを設定するには、以下の手順に従ってください。

- 1 **【マイ コンピュータ】**を開いて、ディスク ドライブを表示します。
- 2 NNMi のインストールで使用するドライブの **【プロパティ】->【セキュリティ】** タブを開きます。
- 3 管理者権限のユーザーとしてログオンし、**【完全な制御を許可】** 設定が選択されていることを確認します (直接またはグループ メンバーシップを介して)。
- 4 組み込まれた **【ローカル サービス】** ユーザーが **【完全な制御を許可】** 設定を選択していることを確認します (直接またはローカル ユーザー グループを介して)。
- 5 変更を適用します。
- 6 NNMi のインストールを続行します。

正式な完全修飾ドメイン名の取得または設定

NNMi ユーザは、正式な完全修飾ドメイン名 (FQDN) を使用して NNMi にアクセスします。FQDN は、NNM iSPI への SSO (シングルサインオン) を有効にするときにも使用されます。


- 1 NNMi 管理サーバー の正式な FQDN を判別するには、以下のいずれかの方法を使用します。
 - **nnmofficialfqdn.ovpl** コマンドを使用して、インストール中に FQDN 設定の値を表示します。詳細については、*nnmofficialfqdn.ovpl* リファレンス ページまたは UNIX のマンページを参照してください。
 - NNMi コンソールで、[ヘルプ] > [システム情報] の順にクリックします。[サーバー] タブをクリックして、完全修飾ドメイン名の値を見つけます。
- 2 インストール時に設定した FQDN を変更する必要がある場合は、**nnmsetofficialfqdn.ovpl** コマンドを使用します。詳細については、*nnmsetofficialfqdn.ovpl* リファレンス ページまたは UNIX のマンページを参照してください。
- 3 NNM iSPI へのシングルサインオンでは、FQDN を含む URL を介してユーザーが NNMi コンソールにアクセスする必要があります。ユーザーがこの要件を容易に満たせるように、NNMi URL を FQDN にリダイレクトするように NNMi を設定できます。この設定を行う場合は、正式な FQDN を設定しておく必要があります。詳細については、NNMi ヘルプを参照してください。

ウイルス対策ソフトウェアの無効化

インストールパフォーマンスの向上のために、以下の手順にてターゲットシステムのウイルス対策ソフトウェアを無効にします。

- 1 Windows のデスクトップから、[スタート] > [設定] > [コントロール パネル] の順にクリックします。
- 2 [管理ツール] をダブルクリックします。
- 3 [コンポーネント サービス] をダブルクリックします。
- 4 [サービス] を選択します。


- 5 Symantec や McAfee などの企業が提供しているウィルス対策サービスの状態を確認します。
- 6 各ウィルス対策サービスを右クリックして、**[停止]** をクリックします。

 NNMi のインストールが完了したら、各ウィルス対策サービスを再起動します。

NNMi コンソール 用の Web ブラウザの有効化

NNMi にサインオンする前に、NNMi コンソールと相互動作するように Web ブラウザが設定されていることを確認してください。NNMi 管理サーバーにアクセスする各クライアントマシンの Web ブラウザで、以下の項目を有効にする必要があります。

- JavaScript
- NNMi 管理サーバーからのポップアップ ウィンドウ
- NNMi 管理サーバーからの Cookie

 以下の手順を完了するには、NNMi 管理サーバー の完全修飾ドメイン名が必要になります。

使用している NNMi 管理サーバー に複数のドメイン名がある場合は、NNMi では、インストール時にその中から 1 つを選択します。NNMi が使用している完全修飾ドメイン名を判断するには、`nnmofficialfqdn.ovpl` スクリプトを実行します。詳細については、`nnmofficialfqdn.ovpl` リファレンス ページまたは UNIX のマンページを参照してください。


Web ブラウザの準備方法は、下記の手順のとおりです。

Mozilla Firefox

- 1 Mozilla Firefox で、**[ツール] > [オプション]** または **[編集] > [設定]** をクリックします。
- 2 **[コンテンツ]** タブで、**[JavaScript を有効にする]** チェック ボックスをオンにします。

- 3 **[JavaScript を有効にする]** チェック ボックスの横にある **[詳細設定]** をクリックします。
- 4 **[ウィンドウのフォーカス (前面か背面か) を切り替える]** チェック ボックスをオンにして、**[OK]** をクリックします。
- 5 **[コンテンツ]** タブをクリックして、**[ポップアップウィンドウをブロックする]** チェック ボックスをオンにします。
- 6 **[許可サイト]** をクリックして、NNMi 管理サーバーの完全修飾ドメイン名を許可サイトのリストに追加します。
- 7 **[プライバシー]** タブをクリックし、**[記憶させる履歴を詳細設定する]** のプルダウン リストを表示します。
- 8 **[サイトから送られてきた Cookie を保存する]** チェック ボックスをオンにし、**[例外サイト]** をクリックします。
- 9 NNMi 管理サーバーの完全修飾ドメイン名を、許可されたサイトのリストに追加します。
- 10 **[OK]** をクリックします。
- 11 Web ブラウザを再起動します。

Microsoft Internet Explorer

- 1 Internet Explorer にて、**[ツール] > [インターネット オプション]** の順にクリックします。
- 2 **[セキュリティ]** タブで、NNMi 管理サーバーを含むゾーンを選択した後、**[レベルのカスタマイズ]** をクリックします。
- 3 **[スクリプト]** にある **[アクティブ スクリプト]** のオプションを**有効にする**に選択します。
- 4 **[プライバシー]** タブの **[設定]** 領域で、**[すべての Cookie を受け入れる]** から **[中 - 高]** までのオプションの 1 つを選択します。
 この設定は、インターネットゾーンでのみ有効です。イントラネット上の NNMi 管理サーバーに接続する場合は、この設定による影響はありません。
- 5 **[プライバシー]** タブで、**[ポップアップ ブロックを有効にする]** のチェック ボックスをオンにした後、**[設定]** をクリックします。

- 6 NNMi 管理サーバーの完全修飾ドメイン名を、許可されたサイトのリストに追加します。
- 7 Web ブラウザを再起動します。

システム アカウントのパスワードのリセット

NNMi のインストール中に、システム アカウントの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を忘れた場合は、`nnmchangesyspw.ovpl` スクリプトを使用して変更できます。以下の手順に従います。

- 1 **ovstop -c** コマンドを使用して NNMi プロセスを停止します。
- 2 管理者として **nnmchangesyspw.ovpl** スクリプトを実行し、システム パスワードを設定します。
- 3 **ovstart -c** コマンドを使用して NNMi プロセスを開始します。

詳細については、`nnmchangesyspw.ovpl` のリファレンスページまたは UNIX のマンページを参照してください。

Windows Server 2008 でよく知られているポートを有効にする

Windows Server 2008 を設定して、NNMi で必要とされるポートへのアクセスが有効にならないようにします。NNMi をインストールする前に、Windows Server 2008 で以下のポートへのアクセスが有効になっていることを確認してください。

- TCP ポート 80、443、1098、1099、3873、4444、4445、4446、4447、4457、4458、8083、8086、および 8087
- UDP ポート 162 および 696

Windows Server 2008 で正しいポートを有効にするには、以下の手順に従います。詳細については、Windows Server 2008 のマニュアルを必要に応じて参照してください。

- 1 [セキュリティが強化された Windows ファイアウォール] コンソールを開きます。開くには、[スタート]->[管理ツール]->[セキュリティが強化された Windows ファイアウォール] メニューを選択します。
- 2 受信規則を作成し、NNMi が必要とするポートごとに有効にします。

Windows Server 2008 では、ウィルス対策保護が有効になっている場合があります。ウィルス対策保護を設定し、Windows Server 2008 で上記のポートへのアクセスが許可されることを確認してください。

B インストールおよび初期スタートアップのトラブルシューティング

インストールの問題

問題: NNMi のインストール プロセスが、Oracle ユーザー名とパスワードを受け付けない

解決方法:

- 1 Oracle ユーザー名とパスワードを Oracle データベース管理者に確認してから、インストールを続行してください。
- 2 手順 1 で問題が解決できない場合、Oracle データベース管理者から正しいポート番号を入手してから、インストールを続行してください。

初期スタートアップの問題

問題 : NNMi コンソールのページが見つからない

解決方法 : NNMi コンソールにアクセスするための URL アドレスには、jboss アプリケーション サーバーが NNMi コンソールとの通信に使用するポートが含まれています。NNMi コンソールにアクセスするには、以下の URL を Web ブラウザのアドレス バーに入力します。

`http://<fully_qualified_domain_name>:<port>/nnm/`

<fully_qualified_domain_name> は、NNMi 管理サーバーの完全修飾ドメイン名を表し、**<port>** は、jboss アプリケーション サーバーが NNMi コンソールとの通信で使用するポートを表します。



使用している NNMi 管理サーバー に複数のドメイン名がある場合は、NNMi では、インストール時にその中から 1 つを選択します。NNMi が使用している完全修飾ドメイン名を判断するには、**nnmofficialfqdn.ovpl** スクリプトを実行します。詳細については、**nnmofficialfqdn.ovpl** リファレンス ページまたは UNIX のマンページを参照してください。

NNMi インストーラは、使用可能なポートを使用するように jboss アプリケーション サーバーを設定します。この設定はインストーラが自動的に行うため、ユーザーの操作は必要ありません。選択されたポート番号は、NNMi のインストール プロセス中に現れる **[jboss アプリケーション サーバー ポート]** のダイアログ ボックスに表示されます。

NNMi のインストールに使うポートを求めるには、以下のファイルを参照してください。

```
%NnmDataDir%¥conf¥nnm¥props¥nms-local.properties
```

このファイルから、以下のような行を探してください。

```
jboss.http.port=8004
```

jboss.http.port に割り当てられたポートが、URL に指定するポートです。詳細については、**nnm.ports** リファレンス ページ、または UNIX マンページを参照してください。

問題 : jboss ポートの競合

解決方法 : デフォルトでは、jboss アプリケーション サーバーは、NNMi との通信に複数のポートを使用します。通常これらのポートは、Oracle や他のアプリケーションにも使用されます。jboss アプリケーション サーバーのポートが、すでに Oracle データベース サーバーなど他のアプリケーションによって使用されていると判明した場合、NNMi インストーラはポートの競合に関するエラー メッセージを表示します。NNMi のプログラムでポートの競合が問題になっているかを調べるには、以下のログファイルを確認します。

```
%NnmDataDir%\log\%nnm%\jbossServer.log
```

ポートの競合を解決するには、以下の手順を実行します。

- 1 管理者権限のあるユーザーとして、テキスト エディタで以下のファイルを開いてください。

```
%NnmDataDir%\conf\%nnm%\props\%nms%-local.properties
```

- 2 既存のエントリーを修正し、競合しているポート番号を使用可能なポート番号に変更します。
- 3 ファイルを保存してから、NNMi サービスを再起動します。

```
ovstop -c  
ovstart -c
```



ovstop コマンドと ovstart コマンドは、[スタート] メニューからも実行できます。

詳細については、*nnm.ports* リファレンス ページ、または UNIX マニュアルを参照してください。

問題 : 一部正常に動作しない NNMi プログラム コンポーネントがある

解決方法 : NNMi サービスがすべてインストールされ、起動していることを確認します。

- 1 コマンドプロンプトで、以下のコマンドを入力します。

```
ovstatus -c
```

コマンド出力の内容が、表 6 に示すような出力になっているか確認します。

- 必要に応じて、NNMi サービスを停止または開始させます。コマンドプロンプトにて、適切なコマンドを入力します。

```
ovstop -c <service name>
```

```
ovstart -c <service name>
```

表 6 ovstatus -c コマンドからの出力

名前	PID	状態	最後のメッセージ
OVsPMD	3262	実行中	-
pmd	3327	実行中	初期化が終了しました。
ovjboss	3292	実行中	初期化が終了しました。
nmsdbmgr	3263	実行中	データベースが利用可能です。

問題 : NNMi が SNMP トラップを受信できないが、MKS Toolkit はインストールされている

解決方法: MKS Toolkit で専有の SNMP サービスをインストールします。専有の *SNMPTrapd* サービスおよび *Windows SNMP* トラップサービスの両方を無効にします。

- Windows のデスクトップから、[スタート]>[設定]>[コントロールパネル]の順にクリックします。
- [管理ツール] をダブルクリックします。
- [コンポーネント サービス] をダブルクリックしてから、[サービス] をダブルクリックします。
- サービスのリストの中から、[SNMPTrapd Service] を探します。
- [SNMPTrapd service] を右クリックし、[停止] をクリックします。
- [SNMPTrapd service] をダブルクリックし、[スタートアップの種類] リストで [無効] をクリックします。
- サービスのリストの中から、[SNMP Trap Service] を探します。
- [SNMP Trap Service] を右クリックし、[停止] をクリックします。
- [SNMP Trap Service] の [スタートアップの種類] が [無効] に設定されているか確認します。

[スタートアップの種類] が正しく設定されていない場合は、サービス名をダブルクリックしたあと、[スタートアップの種類] のリストで [無効] をクリックします。

- 10 以下のように、NNMi NnmTrapService サービスを再起動します。

```
ovstop -c ovjboss
ovstart -c ovjboss
```

問題 : NNMi がノードを検出しない

解決方法 :

- 1 ワークスペースのナビゲーションパネルで [設定] ワークスペースを選択します。
- 2 [シード] フォームを開きます。
- 3 [検出シードの結果] 列の値を調べます。

検出されたノードの大部分のステータスが、[ノードが作成されました] 以外の場合は、NNMi 検出プロセスが正常に動作していなかったということです。

ステータスが [SNMP 応答がない] の場合は、ノードに対して ping が可能であるか、また、`nnmsnmpwalk.ovpl -c communitystring nodename` を実行してノードから情報を取得できるかを確認します。これらのツールが実行できない場合は、以下の事項を確認してください。

- a ノードに ping し、応答するか確認してください。
- b ノードで SNMP が有効になっているか確認してください。
- c ノードの SNMP エージェント アクセス リストに、ローカル管理サーバーが含まれていることを確認してください。
- d NNMi がノードを適切に検出できるよう、ノードの正しいコミュニティ文字列を設定していることを確認してください。この情報は、[通信の設定] フォームの [デフォルトの SNMPv1/v2 コミュニティ文字列] タブに表示されています。
- e ルーター、スイッチ、またはファイアウォールについて、検出を制限する可能性のあるアクセス制御リストが設定されていないことを確認します。

詳細については、NNMi ヘルプにある「検出の設定」を参照してください。

問題 : Windows NNMi 管理サーバーにアクセスしていると、NNMi コンソールを起動できない

ブラウザで Windows NNMi 管理サーバーをポイントしているときに、NNMi コンソールを起動できない場合、ファイアウォールが HTTP ポートをブロックしている可能性があります。この問題のトラブルシューティングを行うには、NNMi 管理サーバーでブラウザを実行します。このブラウザからは NNMi コンソールにアクセスでき、リモートのブラウザからはアクセスできない場合、ポートをチェックする必要があります。

この問題を解決するには、許可ポート リストに `%NnmDataDir%\conf\%nnm%\props\%nms-local.properties` ファイルに示されている `jboss.http.port` 値を追加します。詳細については、*nnm.ports* リファレンス ページ、または UNIX マニュアルを参照してください。

用語集

H

HP Network Node Manager i Software

ネットワーク管理の支援や統合のために設計された HP のソフトウェア商品です。ネットワーク ノードの継続検出、イベントの監視、およびネットワーク障害管理といった機能を備えています。「[NNMi コンソール](#)」も参照。

J

jboss アプリケーション サーバー

Java 2 プラットフォーム、Java 2 Enterprise Edition (J2EE)、Enterprise Java Beans (EJB) と組み合わせて使用するアプリケーションサーバー プログラムです。

N

NNMi

[HP Network Node Manager i Software](#) を参照してください。

NNMi 管理サーバー

NNMi ソフトウェアがインストールされ、NNMi プロセスやサービスが実

行されるコンピュータ システムのことです。

NNMi コンソール

NNMi ソフトウェアのユーザー インタフェースです。オペレータや管理者は、NNMi コンソール を使用することで、大部分の NNMi ネットワーク管理タスクを実行できます。

O

ovstart コマンド

NNMi の管理プロセスを起動するためのコマンドです。詳細については、[\[ヘルプ\]>\[ドキュメントライブラリ\]>\[リファレンスページ\]](#) (NNMi ヘルプ) を参照してください。

ovstatus コマンド

NNMi が管理するプロセスの現在のステータスを報告するコマンドです。詳細については、[\[ヘルプ\]>\[ドキュメントライブラリ\]>\[リファレンスページ\]](#) (NNMi ヘルプ) を参照してください。

ovstop コマンド

NNMi の管理プロセスを停止するためのコマンドです。詳細については、[\[ヘルプ\]>\[ドキュメントライブラリ\]>](#)

[リファレンスページ] (NNMi ヘルプ) を参照してください。

S

SID

システム識別子のことです。

SNMP

簡易ネットワーク管理プロトコル (SNMP) を参照してください。

SNMP トラップ

内部の状態の変化や障害を検知すると、SNMP エージェントにより生成される未確認イベントで、RFC-1155 で指定されるプロトコルに準拠しています。

あ

アカウント

ユーザー アカウントを参照してください。

アプリケーション フェイルオーバー

NNMi で、現在アクティブなサーバーが停止した場合に、NNMi のプロセスの制御をスタンバイ サーバーに移行するオプション機能 (ユーザーが設定し、jboss クラスタリング サポートを利用)。

い

インシデント

ネットワークに関する重要なイベントの通知 イベントは、ネットワークマップ内のノードの背景色に反映されると同時に、インシデント ビューに

も表示されます。すべてのインシデントでノードの色が変わるわけではありません。

か

簡易ネットワーク管理プロトコル (SNMP)

マネージャプロセスとエージェントプロセス間のネットワーク管理情報の通信に使用される TCP/IP 上の ARPA ネットワーク管理プロトコルです。

く

クイック スタート設定ウィザード

クイック スタート設定ウィザードは、NNMi のインストールが完了した直後に自動的に実行されます。クイック スタート設定ウィザードを使用して、SNMPv1 または SNMPv3 環境の読み取りコミュニティ文字列を準備したり、検出されるノードの範囲に制限を設定したり、管理者アカウントを設定したりできます。

組み込みデータベース

NNMi ソフトウェアに付属しているデータベースです。Oracle データベースを使用するように NNMi を設定することもできます。

グローバル ネットワーク管理

地理的に分散している 1 つ以上のリージョナル マネージャからのデータを統合する 1 つ以上のグローバル マネージャを持つ、NNMi の分散型の配備です。

グローバル マネージャ

分散 NNMi リージョン マネージャ サーバーからのデータを統合する、グローバル ネットワーク管理配備内の NNMi 管理サーバーです。グローバル マネージャは、環境全体のトポロジおよびインシデントの統合ビューを提供します。グローバル マネージャには、NNMi Advanced ライセンスが必要です。

け

検出プロセス

NNMi が、ノードを管理下におくために、ネットワーク ノードの情報を収集するプロセスです。初期検出は、まずデバイス インベントリの情報を収集し、次にネットワーク接続情報を収集するという 2 つのフェーズのプロセスで実行されます。この検出プロセスは、初期検出の後には継続的に、または要求に応じて起動します。「[スパイラル検出](#)」、「[自動検出](#)」、および「[シード済み検出](#)」も参照してください。

検出ルール

自動検出プロセスを制限するために使用する、ユーザ定義の IP アドレス範囲です。検出規定は、[自動検出](#)の設定の一部として、NNMi コンソールで設定されます。「[自動検出](#)」も参照。

こ

高可用性

このガイドでは、設定の一部に障害があっても中断されないサービスを提供するハードウェアおよびソフトウェア

の設定のことです。高可用性 (HA) とは、コンポーネントに障害があった場合でもアプリケーションを実行し続けるよう冗長コンポーネントを備えた構成を意味します。NNMi は、市販されているいくつかの HA ソリューションの 1 つをサポートするように設定できます。[アプリケーション フェイルオーバー](#)と比べてください。

コミュニティ文字列

SNMP エージェントに送信する SNMP クエリーを認証するために使用されるテキストパスワードです。

コンソール

[NNMi コンソール](#)を参照してください。

根本原因解析 (RCA)

ネットワーク インシデントの根本原因の特定を目指した、問題解決方法のクラス。NNMi は、NNMi 根本原因解析 (RCA) エンジンが、インシデントから通知された問題をアクティブに評価している場合に、そのインシデントをアクティブであるとみなします。

し

シード

ネットワーク検出プロセスの開始点として機能することによって、NNMi のネットワーク検出を助ける SNMP ノードのことです。たとえば、管理環境内のコア ルーターなどがシードになることができます。各シードは、IP アドレスやホスト名によって識別されます。自動検出を無効にすると、検出

プロセスはシード検出に限定されません。この場合、指定したノードのみが検出され、NNMi データベースに追加されます。「自動検出」と「シード済み検出」も参照。

シード済み検出

シード、またはシード ファイルを元にしたプロセスで、シードとして指定したノードのみについてのレイヤ 2 の接続情報を検出します。シード検出は、特定したクエリーとタスクのネットワークインベントリのみを保守します。自動検出と比べてください。「スパイラル検出」も参照。

システムアカウント

NNMi のインストール時に使用するために提供される特別なアカウントです。システムアカウントは、インストール終了後は、コマンドラインのセキュリティや復旧目的のみに使用されます。「ユーザー アカウント」も参照。

自動検出

1 つ以上の検出規定に該当するすべての SNMP ノードを自動的に検出し管理下とする、スパイラル検出プロセスです。シード済み検出と比べてください。「スパイラル検出」と「検出ルール」も参照。

す

スパイラル検出

NNMi の管理するネットワークのインベントリ、コンテインメント、リレーションシップ、接続についての情報を含む、ネットワーク トポロジ情報を常

時更新する処理のことです。検出プロセスを参照してください。「自動検出」と「シード済み検出」も参照。

と

トポロジ (ネットワーク)

ネットワークのノードや接続などが、通信ネットワーク上でどのように配置されているのかを示す図のことです。

トラップ

SNMP トラップを参照してください。

の

ノード

ネットワーク関係で、ネットワークに接続されているコンピュータ システムやデバイス (プリンター、ルーター、ブリッジなど) のことです。NNMi で十分に管理するには、ノードを SNMP で設定する必要があります。

ほ

ポート

ハードウェアコンテキストにて、ネットワークデバイスを経由して情報の受け渡しを行う場所です。

ゆ

ユーザー アカウント

ユーザーやユーザー グループが、NNMi にアクセスするための方法です。ユーザー アカウントは、NNMi コンソールで設定されます。それに定義済みのユーザー ロールが割り当てられます。シス

テムアカウントおよびユーザーロールを参照してください。

ユーザーロール

NNMi 管理者は、ユーザー アクセス設定の一環として、各ユーザー アカウントに定義済みのユーザー ロールを割り当てます。ユーザー ロールにより、NNMi コンソールにアクセス可能なユーザー アカウント、および各ユーザー アカウントで使用可能なワークスペースとアクションが決まります。NNMi には、プログラムによってあらかじめ定義され変更することのできない以下の階層型ユーザー ロールがあります：管理者、Web サービス クライアント、オペレータ レベル 2、オペレータ レベル 1、ゲスト。「ユーザー アカウント」も参照。

る

ルール

検出ルールを参照してください。

れ

レイヤ 2 (L2)

階層化通信モデルである Open Systems Interconnection (OSI) のデータ リンク層です。データ リンク層では、ネットワークの物理リンクを介してデータの伝送を行います。スイッチは、レイヤ 2 のデータを転送するデバイスで、メディアアクセス制御 (MAC) アドレスからメッセージの転送先を決定します。

レイヤ 3 (L3)

階層化通信モデルである Open Systems Interconnection (OSI) のネットワーク層です。ネットワーク層は、ネットワーク上の隣接するノードのアドレスの取得、データ伝送経路の選択、サービス品質などに関与します。また、ローカルホストドメインへの受信メッセージの認識・転送なども行っています。サブネットの接続はすべてレイヤー 3 (IP) レベルで行われます。

