# HP Automated Network Management

ソリューションバージョン : 9.20

## コンセプトガイド

ドキュメントリリース日 : 2012 年 7 月
ソフトウェアリリース日 : 2012 年 7 月

# ご注意

## 保証

HP 製品、またはサービスの保証は、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。ここに含まれる技術的、編集上の誤り、または欠如について、HP はいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

## 権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HP からの有効な使用許諾が必要です。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



## 商標について

Adobe は、Adobe Systems Incorporated の商標です。

AMD は、Advanced Micro Devices, Inc の商標です。

HP 9000 コンピューター上の HP-UX リリース 10.20 以降および HP-UX リリース 11.00 以降 (32 ビットおよび 64 ビット両方の環境 ) は、すべて Open Group UNIX 95 製品です。

Intel、Itanium、および Intel Xeon は、Intel Coporation の米国およびその他の国の登録商標です。

Microsoft および Windows は、Microsoft Corporation の米国登録商標です。

Oracle は、Oracle Corporation 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。

## ドキュメントの更新情報

このマニュアルの表紙には、以下の識別番号が記載されています。

- ソフトウェアのバージョン番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

最新の更新のチェック、またはご使用のドキュメントが最新版かどうかのご確認には、次のサイトをご利用ください。

**http://support.openview.hp.com/selfsolve/manuals**

このサイトを利用するには、HP Passport への登録とサインインが必要です。HP Passport ID の取得登録は、次の Web サイトから行なうことができます。

**http://h20229.www2.hp.com/passport-registration.html ( 英語サイト )**

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

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HP の営業担当にお問い合わせください。

## 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。

**http://support.openview.hp.com**

HP ソフトウェアが提供する製品、サービス、サポートに関する詳細情報をご覧いただけます。

HP ソフトウェアオンラインではセルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに素早く効率的にアクセスいただけます。HP ソフトウェアサポート Web サイトのサポート範囲は次のとおりです。

- 関心のある技術情報の検索
- サポートケースとエンハンスメント要求の登録とトラッキング
- 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 サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部を除き、サポートのご利用には、HP Passport ユーザーとしてご登録の上、ログインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport ID を登録するには、以下の Web サイトにアクセスしてください。

**http://h20229.www2.hp.com/passport-registration.html ( 英語サイト )**

アクセスレベルに関する詳細は、以下の Web サイトにアクセスしてください。

**http://support.openview.hp.com/access_level.jsp**

# 目次

# 1 ANM の概要

Automated Network Management (ANM) は、ネットワークの障害検出、パフォーマンス監視、設定管理と適合、および診断と自動化のためのツールを統合したソリューションです。ANM を使用することにより、ネットワークドメインにおける ITILv3 のベストプラクティス、つまりイベント、インシデント、および問題の管理、変更設定、およびリリースと配備の管理を実現できます。

ANM を使用することにより、IT 組織は次の課題に取り組むことができます。

- 平均修復時間 (MTTR) を短縮する。
- 平均故障間隔 (MTBF) を長くする。
- ポリシーに準拠する。
- ネットワーク設定の変更までの平均時間を短縮する。
- 投資回収率 (ROI) を高めることによりサービスレベル契約 (SLA) を強化する。

ANM は、次の 6 つの個別製品で構成されており、HP Automated Network Management (ANM) Suite として統合されています。

- HP Network Node Manager i Software (NNMi)
- HP Network Automation Software (NA)
- HP Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics)
- HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA)
- HP Network Node Manager iSPI Performance for Traffic Software (NNM iSPI Performance for Traffic)
- NNM iSPI Network Engineering Toolset Software (NNM iSPI NET)

ANM Advanced には、追加の iSPI ポイントライセンスキーが組み込まれており、高度なサービスを提供する NNM iSPI で使用する iSPI ポイントの機能が追加されています。

- HP Network Node Manager iSPI for MPLS Software (NNM iSPI for MPLS)
- HP Network Node Manager iSPI for IP Multicast Software (NNM iSPI for IP Multicast)
- HP Network Node Manager iSPI for IP Telephony Software (NNM iSPI for IP Telephony)

ANM は、ネットワークを有効に管理するために、次の機能を備えています。

- ネットワークの変更と設定の管理
- ネットワークのパフォーマンス管理
- ネットワークの障害管理
- ネットワークランブックの自動化
- ネットワークの診断

これらの機能により、次の操作が可能になります。

- ネットワークの診断
- 自動化イベントの強化
- ネットワークのパフォーマンスとメトリックスの管理 ( トラフィック管理を含む )
- 検出、インベントリ、およびトポロジの管理
- ネットワークの障害管理
- 適合性と設定の監視
- ネットワークの変更、設定、および配備の管理
- ネットワークのイベントとインシデントの管理
- ネットワーク障害の発生による変更の自動処理

HP Network Node Manager Smart Plug-ins (NNM iSPIs) により、ネットワークの現在の稼動状態と継続的傾向について貴重な洞察を得ることができます。これらのプラグインは、関連するサポートコストを抑え、キャパシティ管理と計画を改善しながら、可用性とパフォーマンス管理機能を向上させるためのプロセスで役立ちます。

# ネットワーク管理のコンセプト

ネットワークが拡張されるにつれ、ネットワークサービスとトポロジはより複雑になります。また、現在の多くのネットワークには規制やセキュリティに関するベストプラクティスに準拠する必要性があり、そのためインフラストラクチャーは、サポートする複数のプロトコル、テクノロジ、およびベンダーで構成されて複雑化しています。ネットワークのパフォーマンスを維持するために、また責務の増大、収益の損失、生産性の損失につながる余分なセキュリティの脆弱性および完全な機能停止状態を回避するために、セキュアーで自動化された有効な方法でネットワークインフラストラクチャーを一元管理することの重要性は高まっています。

こうした複雑な状況において、管理と監視の必要項目は次の 3 つの主要な分野に分けられます。

- **可用性とインシデント管理** : ネットワーク管理の基本要件は、ネットワークの機能停止状態が現在発生しているかどうかを知り、発生している場合にはその根本原因を特定することです。ネットワーク管理者は、ハードウェアの障害やその他の環境由来の原因など、根本原因の発生元を迅速かつ視覚的に把握する必要があります。

  またネットワーク管理者には、ネットワークに存在するデバイスやその接続状態など、実際のネットワークを反映したネットワーク図を見る必要があります。

- **パフォーマンス分析** : ネットワーク管理の問題のほとんどは、機能停止に陥らないまでも、ネットワークのサービスレベルが低いことに顧客が不満を募らせる形で顕在化し、ビジネスのサービス品質 (QoS) に影響します。このような場合、ネットワーク管理者には、そのような状況の根本原因を理解するための高度なトラブルシューティングツールが必要です。それらのツールでは、使用率およびエラーなどの基本的なパフォーマンスのリアルタイムデータと履歴データ ( 比較目的 )、およびネットワークに過負荷を与えたアプリケーションが問題の発生元なのかどうかを調べる IP トラフィック分析の結果を表示することができます。また、ネットワーク応答が適切であるかどうかを示したり、VoIPやビデオなどのサービスを提供する重要なリンクに対してQoSポリシーが正しく設定されているかどうかを判断するプロトコル サービスレベルの応答情報も提供されます。

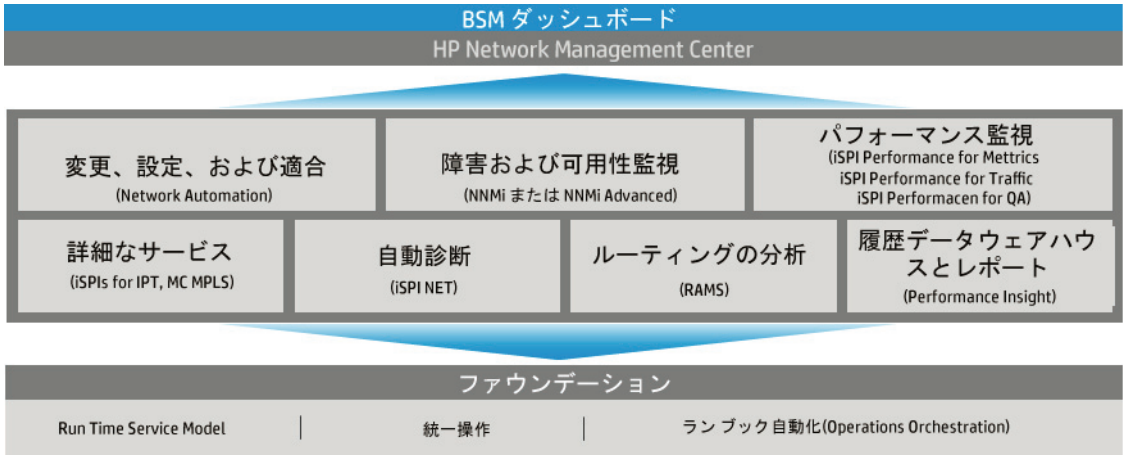
- **変更と設定の管理と適合:** デバイスの設定変更 (問題の発生やインフラストラクチャーの変更の結果 ) やネットワークへの新規デバイスの追加などの毎日のタスクには、長時間を要する可能性があります。そのようなタスクを大量の数のデバイスで手動で実行する場合には、設定を間違い、ネットワークのパフォーマンスが低下したり、最悪のシナリオではネットワークが機能停止に陥ったりする可能性があります。

  ネットワーク設定を適正に管理するには、必須の適合ポリシーに従ってすべての設定を行い、設定変更のアーカイブを保持することが求められます。

「ANM 製品」(10 ページ ) では、日々の業務を容易にし、効率を高める、操作性に優れた製品と連携して、ANM がそれらのネットワーク管理上の必要性を満たす仕組みについて説明します。

図 1 に、本章で説明する必要性を満たすことができる HP Network Management Center 製品を示します。第 2 章、ソリューションの利点では、このセンターを構成する ANM ソリューション製品によってそれらの必要性を満たす仕組みについて詳しく説明します。

**図 1　HP Network Management Center の製品**



# ANM 製品

HP Automated Network Management を使用すると、お客様は、すべてのネットワーク操作についてプロセスを自動化することにより、コストを削減し、機敏性を向上させることができます。製品を部分的に適用する手法とは異なり、ANM は、イベント、パフォーマンス、変更と設定の管理、およびその他の IT プロセスを自動化する統合ソリューションポートフォリオです。

図 2 に、主要なネットワーク管理の必要事項と関連する ANM 製品を示します。次の項では、これらの各製品について説明します。

**図 2　ANM 製品間の関係**

## HP Network Node Manager i Software

NNMi は、SNMP や ICMP などの一般的なネットワークプロトコルを使用して高度なネットワークの障害および可用性監視機能を提供し、組織全体でネットワークの稼動状態を維持するのに役立ちます。NNMi は、自動的かつ継続的にネットワークのノード ( スイッチやルーターなど ) を検出し、ネットワークトポロジ ( レイヤー 2 および 3) を最新の状態で表示できます。

NNMi は、トポロジベースの根本原因分析 (RCA) 機能を使用することにより、ネットワークの状態を正確に把握してネットワークの問題を特定します。RCA、高度な相関機能、および例外別の管理インシデント管理モデルと連携することにより、刻々と変化するネットワーク環境のための動的障害管理ソリューションとして機能します。

また NNMi は、使用率とインタフェースエラーなどのインタフェースのパフォーマンスメトリックスとともに、CPU やメモリの使用率などのデバイスのヘルスインジケーターを監視します。リアルタイムのパフォーマンスインジケーターは、ライブパフォーマンスグラフにより、1 秒間隔の細分度で監視することができます。

動作の観点からすると、NNMi は ANM の中心的な機能を提供します。このソリューションのその他の各ツールには、ANM の単一ペインである NNMi コンソールを介してアクセスできます。

**図 3　NNMi**

## HP Network Automation Software

NA は、エンタープライズクラスのネットワークデバイス変更および設定管理ツールです。ポリシーベースの変更管理モデルによって標準への適合状態を維持しつつ、デバイスの設定変更時における人的誤りを解消します。NA は、NA telnet プロキシを介して行われたコマンドライン変更のキーストロークログを含め、すべてのデバイス変更の完全な監査証跡を保持します。

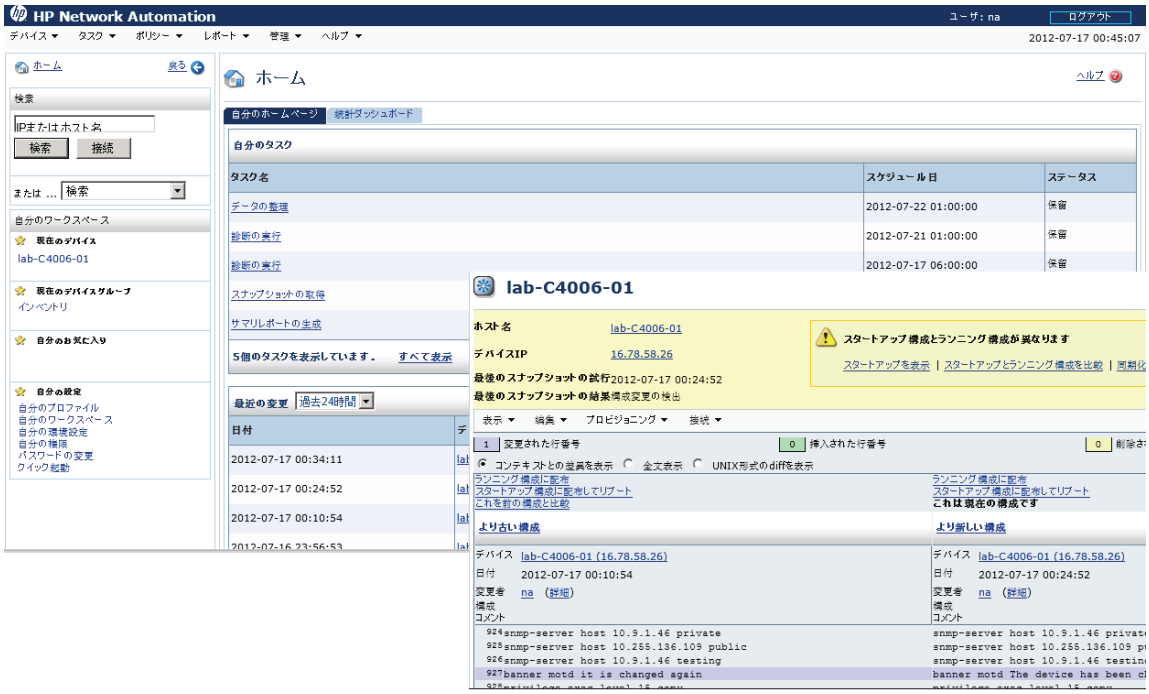
NA は、次のベンダーを含む主要なベンダーが提供するネットワークデバイスモデルとオペレーティングシステムの数千におよぶ組み合わせをサポートしています。

- HP Networking (ProCurve、3Com、H3C、TippingPoint)
- HP Virtual Connect
- Acme Packet
- Alcatel–Lucent
- Avaya
- Brocade (Foundry)
- Check Point
- Cisco
- Citrix
- Crossbeam
- Extreme
- Force 10 (Dell)
- F5
- Gigamon
- Huawei
- Juniper
- Nortel
- VMware

NA は、設定アーカイブと配備を使用して MTTR を最小限に短縮し、次の情報を追跡します。

- ネットワークデバイスに加えられた変更。
- 各変更の実行者。
- 現在のデバイスの設定。
- 組織的な標準に対するデバイスの設定の適合性

## 図 4　NA


HP Network Automation
ユーザ: na
ログアウト
デバイス
タスク
ポリシー
レポート
管理
ヘルプ
2012-07-17 00:45:07
ホーム
戻る
検索
IPまたはホスト名
検索
接続
または ...
検索
自分のワークスペース
現在のデバイス
lab-C4006-01
現在のデバイスグループ
インベントリ
自分のお気に入り
自分の設定
自分のプロファイル
自分のワークスペース
自分の環境設定
自分の権限
パスワードの変更
クイック起動
ホーム
ヘルプ
自分のホームページ
統計ダッシュボード
自分のタスク
タスク名
スケジュール日
ステータス
データの整理
2012-07-22 01:00:00
保留
診断の実行
2012-07-21 01:00:00
保留
診断の実行
2012-07-17 06:00:00
保留
スナップショットの取得
サマリレポートの生成
5個のタスクを表示しています。
すべて表示
最近の変更
過去24時間
日付
2012-07-17 00:34:11
2012-07-17 00:24:52
2012-07-17 00:10:54
lab-C4006-01
ホスト名
lab-C4006-01
デバイスIP
16.78.58.26
最後のスナップショットの試行2012-07-17 00:24:52
最後のスナップショットの結果構成変更の検出
スタートアップ構成とランニング構成が異なります
スタートアップを表示 | スタートアップとランニング構成を比較
表示
編集
プロビジョニング
接続
変更された行番号
挿入された行番号
コンテキストとの差異を表示
全文表示
UNIX形式のdiffを表示
ランニング構成に配布
スタートアップ構成に配布してリブート
これを前の構成と比較
より古い構成
デバイス lab-C4006-01 (16.78.58.26)
日付 2012-07-17 00:10:54
変更者 na (詳細)
構成コメント
924 snmp-server host 10.9.1.46 private
925 snmp-server host 10.255.136.109 public
926 snmp-server host 10.9.1.46 testing
927 banner motd it is changed again
ランニング構成に配布
スタートアップ構成に配布してリブート
これは現在の構成です
より新しい構成
デバイス lab-C4006-01 (16.78.58.26)
日付 2012-07-17 00:24:52
変更者 na (詳細)
構成コメント
snmp-server host 10.9.1.46 private
snmp-server host 10.255.136.109
snmp-server host 10.9.1.46 testing
banner motd The device has been

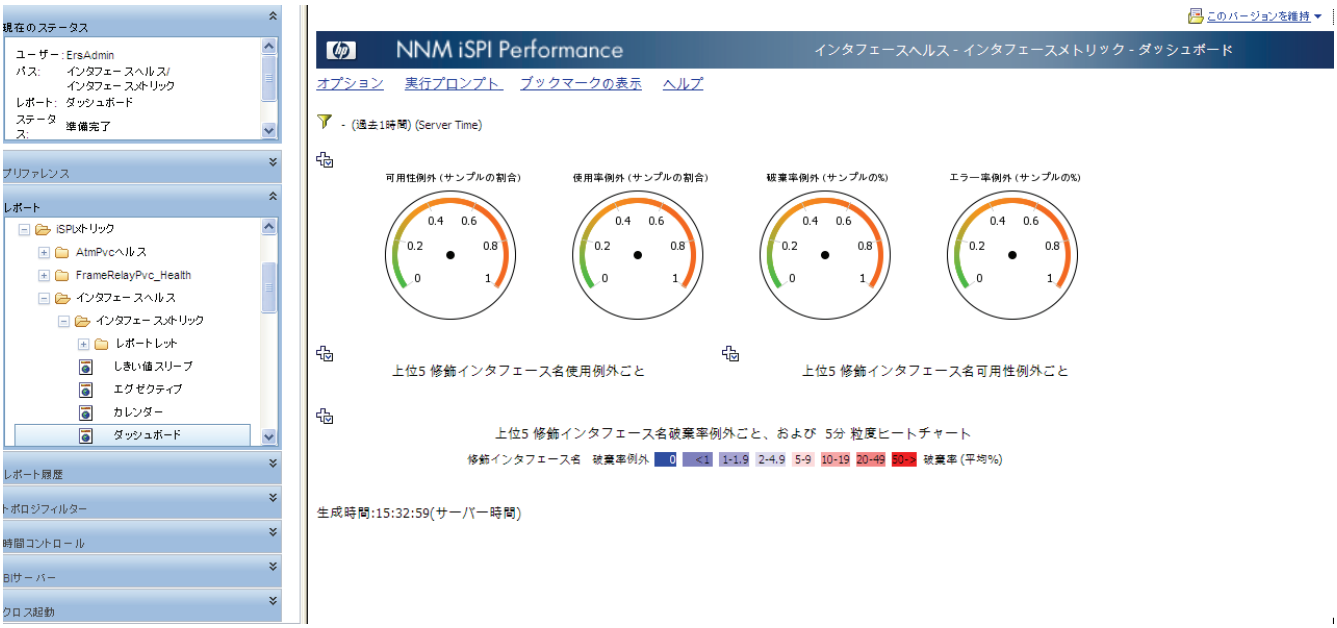
## HP Network Node Manager iSPI Performance for Metrics Software

NNM iSPI Performance for Metrics は、ANM のパフォーマンスレポートの生成基盤 (Network Performance Server または NPS) を提供します。NNMi は、障害およびパフォーマンス両方のポーリングエンジンです。NNM iSPI Performance for Metrics は、データ保持期間が最長 13 か月のパフォーマンスデータベースであり、定義済みレポートとカスタムレポート両方のレポートツールとして使用できます。

NNM iSPI Performance for Metrics の主要な機能は次のとおりです。

- パフォーマンスデータの履歴グラフ。
- パフォーマンスメトリックスとベースラインしきい値の監視。
- パフォーマンスベースラインレポート。
- パフォーマンス予測レポート。

**図 5　NNM iSPI Performance for Metrics**



## HP Network Node Manager iSPI Performance for Quality Assurance Software

NNM iSPI Performance for QA は NNMi の機能を強化し、各種応答時間のプローブで設定されたデバイスおよびクラスベースのサービス品質用に設定されたインタフェースから (SNMP を使用して ) データを収集することによって、サービス品質を監視します。また、NNM iSPI Performance for QA には、サーバー上で分散されたプローブを監視する機能もあります。

NNM iSPI Performance for QA はサーバーベースのプローブを備えており、プローブのステータスを報告し、しきい値を超えた場合にオペレーターに対してアラートを生成します。OS ベースの HP Intelligent Response Agent (HP iRA) は選択されたサーバー (Windows または Linux) に存在し、ルーターレベルではなくホストレベルで IP SLA に同様の機能を提供します。HP iRA に必要なシステムリソースは非常に少ないため、パフォーマンスに顕著な悪影響を与えることなく iRA をワークステーションにインストールできます。サーバーベースのプローブは、サーバーからホストされるテストに対して柔軟性があります。以下に例を挙げます。

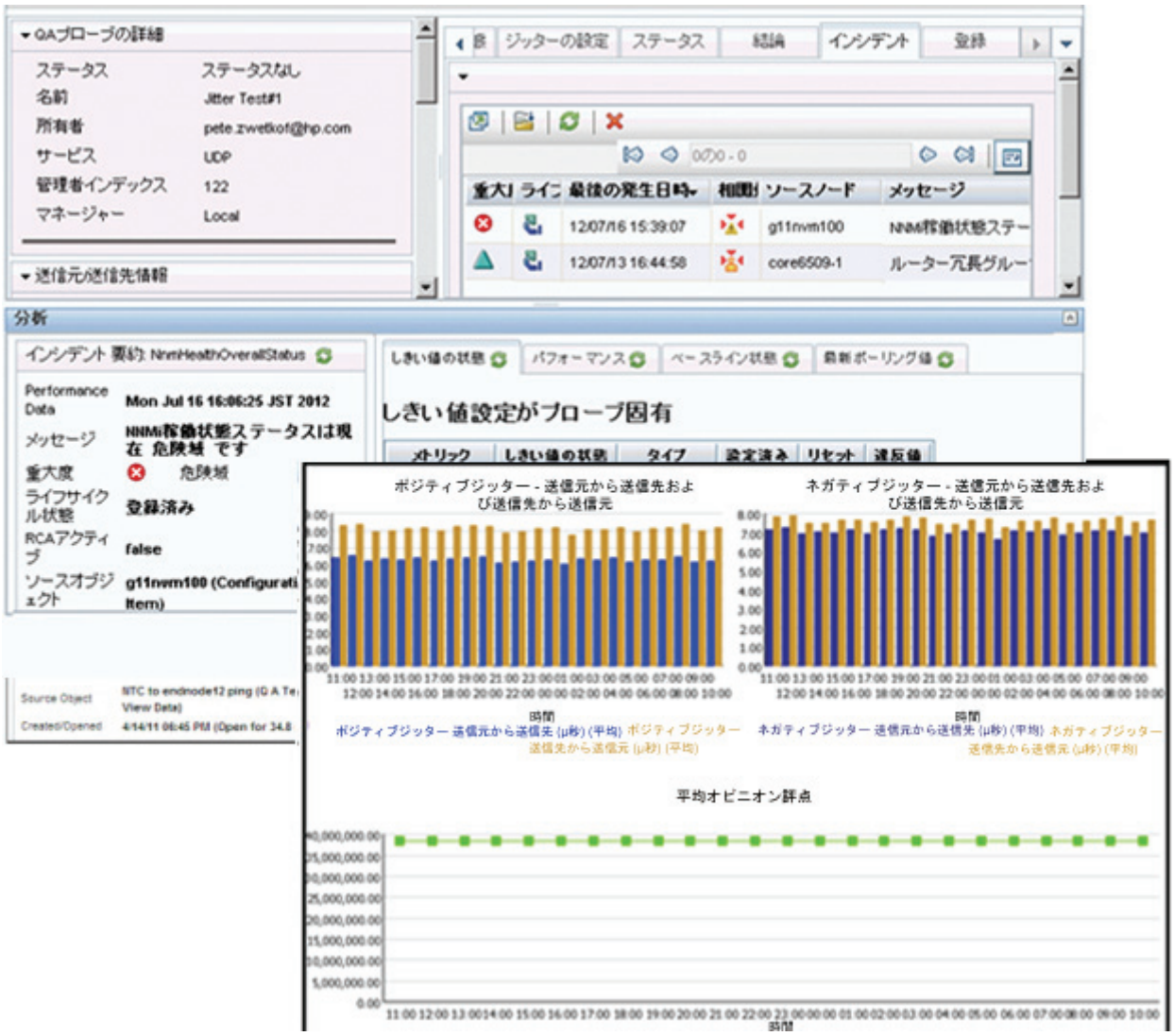
- SQL Server は、特定のサイトに到達できない。
- Webcast の表示中に、加入者によっては、ビデオ品質に関して問題が生じることがある。
- 特定のサイトからのダウンロードに余分な時間がかかる。
- 仮想サーバーを新しい場所に移動した後、SLA への準拠が確認される。

NNM iSPI Performance for QA によって収集されたデータは、VoIP やビデオなどのサービスを提供する重要なインタフェースの監視、報告、しきい値チェックに使用されます。

NNM iSPI Performance for QA は、NNMi と連携動作して、次のタスクを実行します。

- さまざまなネットワーク要素を対象に事前設定された QA プローブを検出する。
- QA プローブの設定を追加する。
- QA プローブのステータスとテスト結果を監視し、設定されたしきい値を超えた場合にアラートを生成する。
- CBQoS 対応の事前設定されたインタフェースを検出する。
- CBQoS 対応のインタフェースのステータスとしきい値を監視し、設定されたしきい値を超えた場合にアラートを生成する。
- 応答テストおよび CBQo 対応のインタフェースに対して、履歴およびリアルタイムのグラフとレポートを提供する。

**図 6　NNM iSPI Performance for QA**



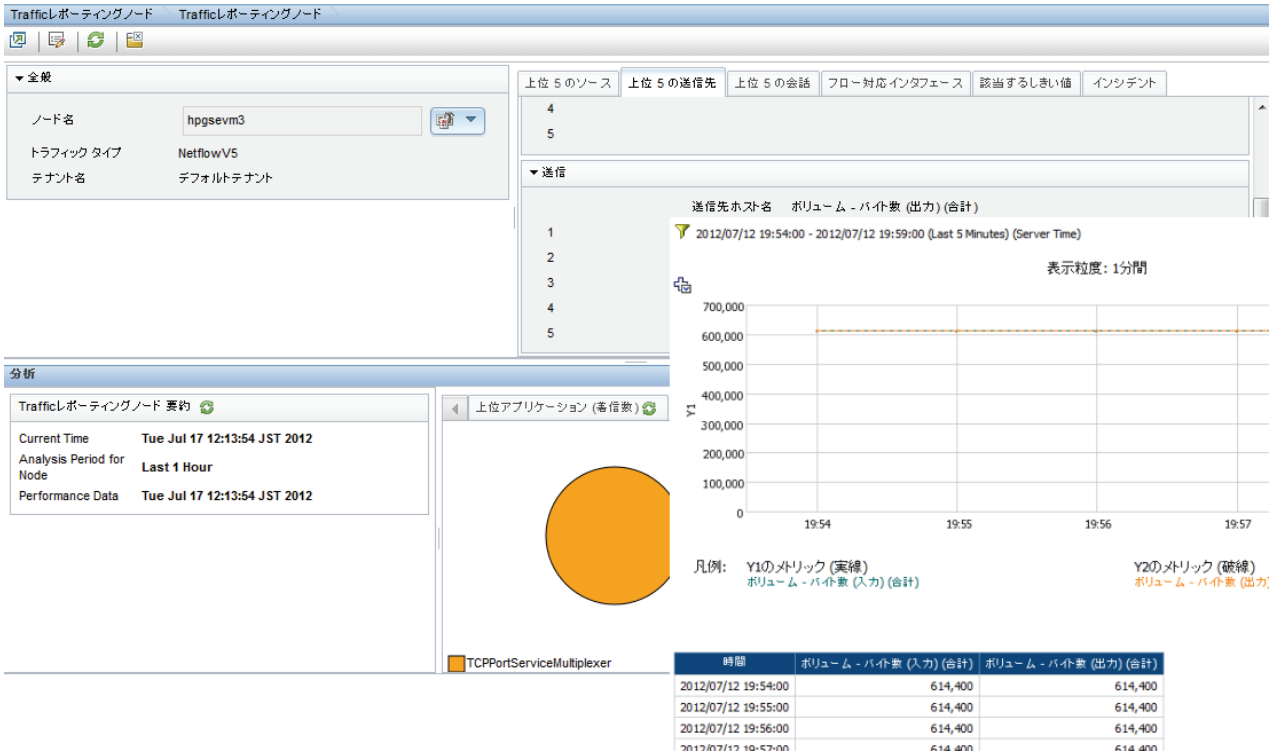
## HP Network Node Manager iSPI Performance for Traffic Software

NNM iSPI Performance for Traffic は、ルーターからエクスポートされる NetFlow、sFlow、J-Flow、および IPFIX IP フローレコードを収集することにより、NNMi パフォーマンス監視機能を強化します。これらのデータは、収集可能なネットワークパフォーマンス情報を補足します。たとえば、NNM iSPI Performance for Traffic のデータに基づき、ネットワーク接続の使用率が高い理由を理解できます。

NNM iSPI Performance for Traffic は、次のタスクを実行します。

- IP フローレコードを集約する。
- コンテキストベース分析で、収集した IP フローレコードと NNMi を相関させる。
- マップを生成してネットワークのトラフィックフロー情報を表示する。
- NPS にデータをエクスポートすることによってパフォーマンスレポートを生成する。

**図 7　NNM iSPI Performance for Traffic**



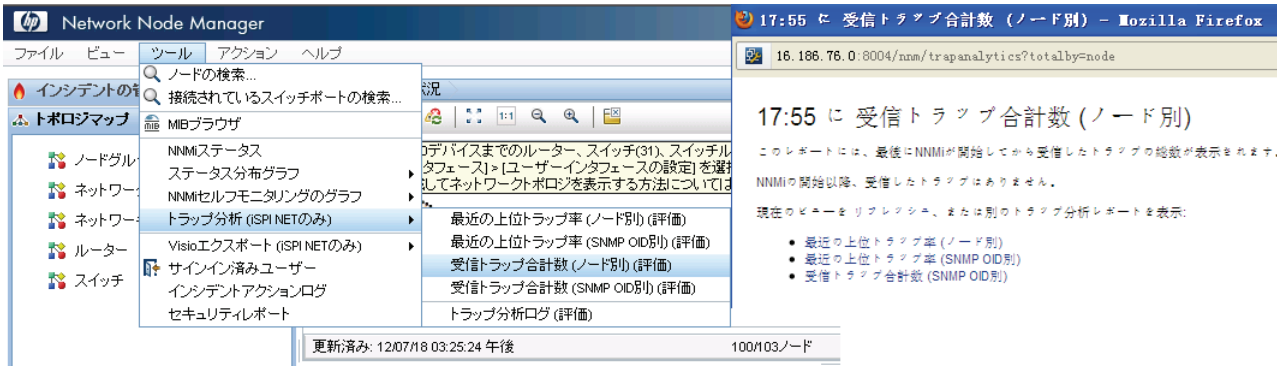
## NNM iSPI Network Engineering Toolset Software

NNM iSPI NET は、追加のトラブルシューティングツールと診断ツールを提供することにより、NNMi の強力なネットワーク管理機能をさらに強化します。

NNM iSPI NET には以下の機能があります。

- ネットワークの SNMP トラップトラフィックの概要と詳細情報を提供する SNMP トラップ分析。
- Visio エクスポート機能により、NNMi トポロジマップデータを Microsoft Visio のファイルに保存。
- SSH または telnet を介してデバイスで実行されるコマンドを使用して、ネットワークデバイスからの情報を自動的に収集および分析する診断フロー。ネットワークの機能停止時に診断フローを実行すれば、根本原因の調査に役立ちます。

**図 8　NNM iSPI NET**



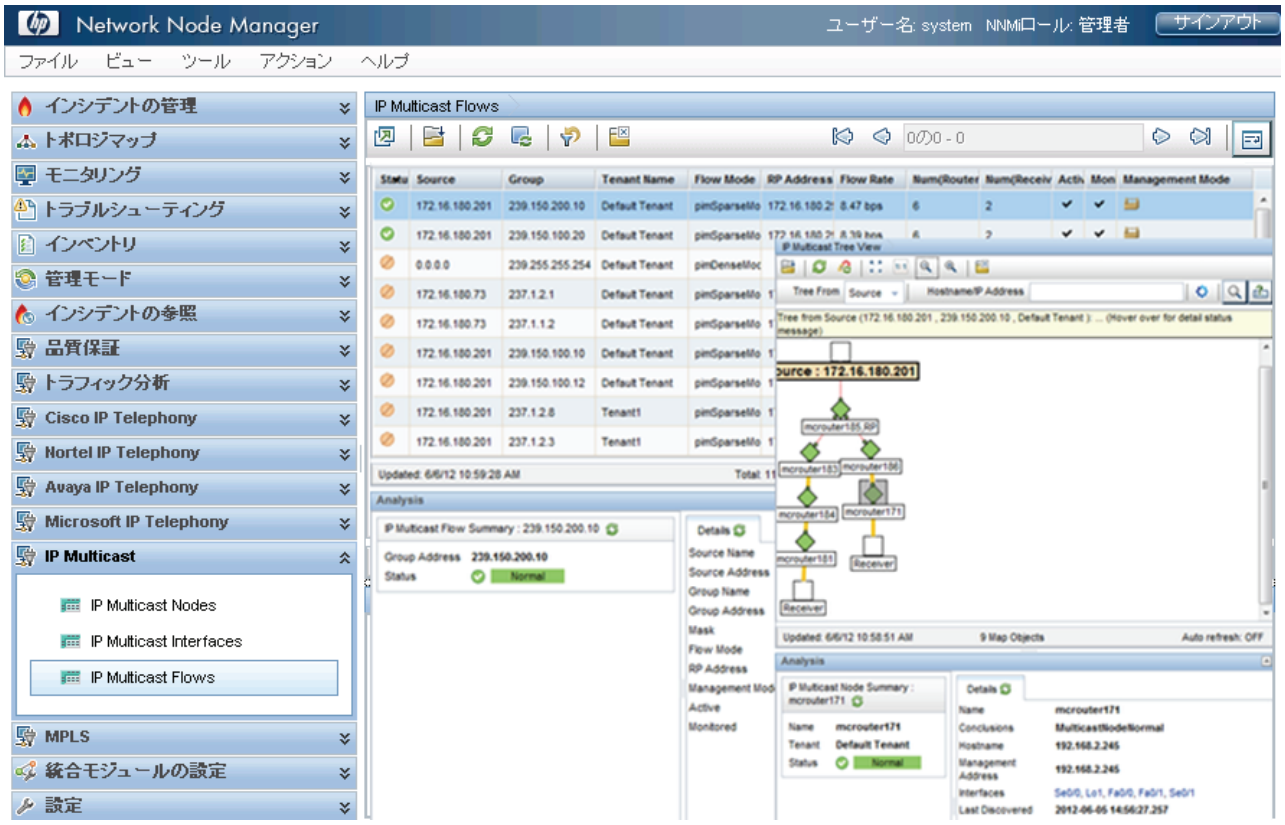
## HP Network Node Manager iSPI for IP Multicast Software (NNM iSPI for IP Multicast)

NNM iSPI for IP Multicast は NNMi の機能を強化し、マルチキャストテクノロジサービスを NNMi で管理できるようにします。NNM iSPI for IP Multicast は、マルチキャスト対応のノード、インタフェース、および関連する近隣接続を自動的に検出し、監視します。監視対象のネットワークで発生するマルチキャストフローは、グラフィカルに表現されます。NNM iSPI for IP Multicast は、最先端のインテリジェンスを使用して、このグラフィカル表現を補足します。つまり、ネットワークでアクティブなマルチキャストフローを監視し、逸脱が生じたりノードの追加や削除が行われた場合にインシデントを作成して、問題があることをオペレーターに知らせます。

NNM iSPI for IP Multicast は、NNMi と連携動作して、次のタスクを実行します。

- 管理環境で IP マルチキャストルーティングトポロジを監視する。
- マルチキャスト対応のノードの稼動状態、Protocol Independent Multicast (PIM) インタフェース、および近隣接続を検出し、監視する。
- ベースラインススナップショットに突き合わせてマルチキャストフローを監視する。
- ルーターの特定のグループアドレスの受信者の詳細を表示する。
- ネットワークのトラブルシューティングに使用するIPマルチキャストマップビューを提供する。
- ネットワークの IP マルチキャストトラフィックフローの監視に使用するマップビューを提供する。
- グローバルマネージャーおよびリージョナルマネージャーからIPマルチキャストインベントリを監視する機能を提供する。
- IP マルチキャストアクティビティに基づいてインシデントを監視する機能を提供して、ネットワーク上の障害をすばやく特定できるようにする。
- NNM iSPI for IP Multicast を NNM iSPI for MPLS に統合することにより、IP マルチキャスト - VPN ネットワークのトラブルシューティング機能を提供する。
- NNM iSPI Performance for Metricsによって収集されたパフォーマンスデータを使用してIPマルチキャストレポートを生成する。

**図 9　NNM iSPI for IP Multicast**



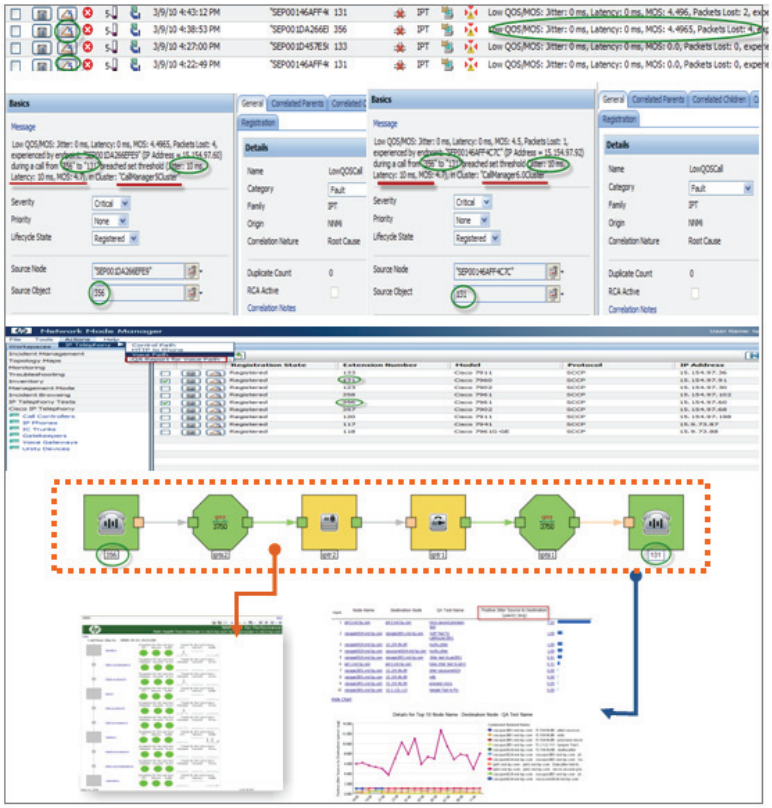
## HP Network Node Manager iSPI for IP Telephony Software (NNM iSPI for IP Telephony)

NNM iSPI for IP Telephony は NNMi の機能を強化し、企業における IP Telephony のマルチベンダー配備および統合通信を NNMi で管理できるようにします。NNM iSPI for IP Telephony を ANM ソリューションに追加すると、オペレーターと管理者は 1 つのツールを使用して、マルチベンダーのエンタープライズ IP Telephony に対してエンタープライズ NOC のさまざまなニーズを管理できます。

NNM iSPI for IP Telephony は、NNMi と連携動作して、次のタスクを実行します。

- インフラストラクチャーの稼動状態、可用性、使用状況、使用率と、エンタープライズ IP Telephony および通信のエンドポイントを監視する。
- 運用上のトラブルシューティングや容量計画を行うために、主要 IP Telephony インフラストラクチャーに関する使用状況、使用率、稼動状態、可用性を報告する。
- 運用上のトラブルシューティングや容量計画を行うために、Call Detail Record (CDR) に基づいて報告する。
- Quality of Experience (QoE) に関するリアルタイムレポートおよび履歴レポートを提供して、QoE を監視する。ANM ユーザーはこれらのメトリックスを使用して、エンドユーザーの呼び出しの QoE に関するトラブルシューティングを行うことができます。
- 管理対象サービスプロバイダー (MSP) または大規模なエンタープライズ配備用の組み込みマルチテナント、分散、拡張性。

**図 10 NNM iSPI for IP Telephony**



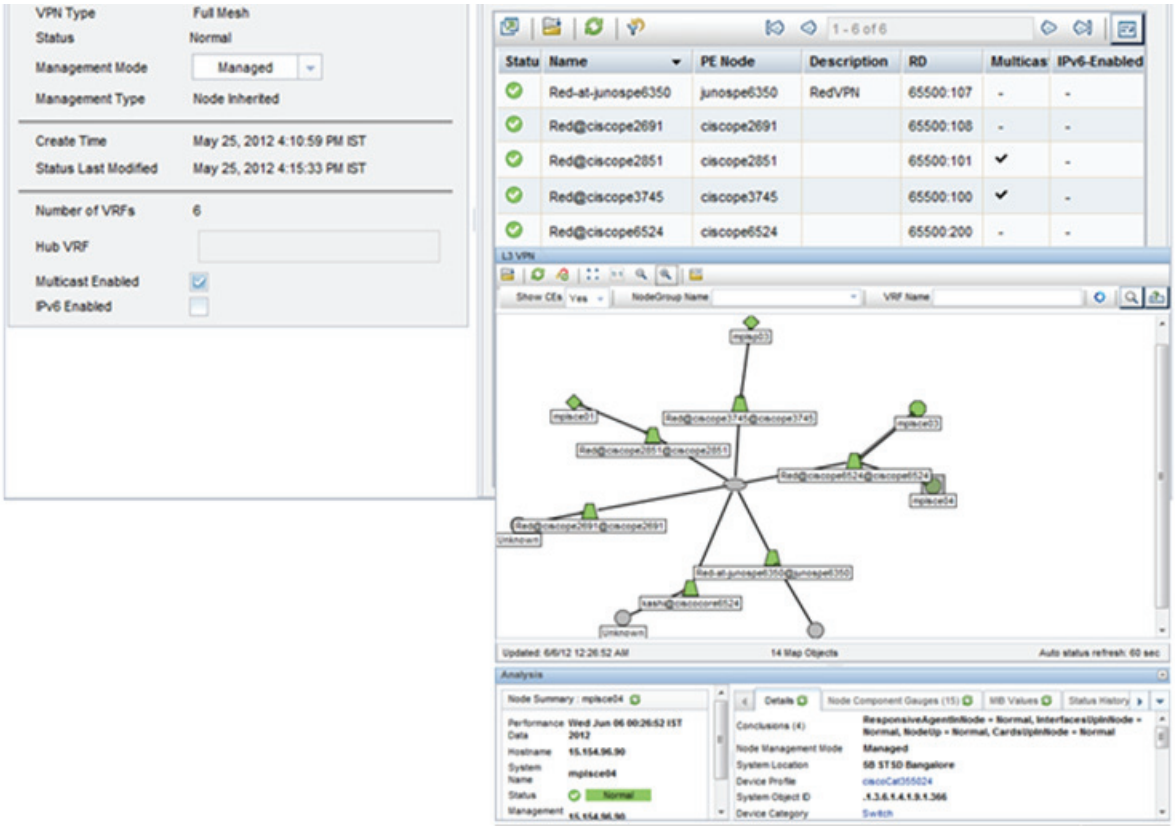
## HP Network Node Manager iSPI for MPLS Software (NNM iSPI for MPLS)

NNM iSPI for MPLS は、レイヤー 3 仮想プライベートネットワーク (VPN)、レイヤー 2 VPN、マルチキャスト VPN (MVPN)、トラフィックエンジニアリングトンネル (TE トンネル ) の検出と監視を自動的に行うことにより、マルチプロトコルラベルスイッチング (MPLS) テクノロジサービスの管理において NNMi の機能を強化します。NNM iSPI for MPLS は、検出されたサービスごとにグラフィカルに表現し、MPLS オブジェクトの最新ステータスをオーバーレイします。NNM iSPI for MPLS グラフと、NNM iSPI for MPLS で生成されたオブジェクトインシデントおよびサービスインシデントを一緒に表示することで、オペレーターは障害をすばやく検出できます。

NNM iSPI for MPLS は、NNMi と連携動作して、次のタスクを実行します。

- ネットワークプロバイダーのエッジデバイスで設定されたレイヤー3 VPN を検出し、監視する。
- ネットワークで仮想プライベート LAN サービス VPN (VPLS VPN)、仮想プライベートワイヤーサービス VPN (VPWS VPN)、TE トンネル、PseudoWire バーチャルサーキット (VC)、サービス指向のラベルスイッチパス (LSP)、マルチキャスト VPN (MVPN) を検出し、監視する。
- レイヤー 3 VPN、レイヤー 2 VPN、MVPN、TE トンネル、サービス指向の LSP をグラフィカルに表現する。
- ネットワークでプロバイダーエッジ (PE10) とカスタマーエッジ (CE11) の関係を検出し、監視する。カスタマーエッジノードを監視し、サービス関連の影響を分析する。
- グローバルマネージャーおよびリージョナルマネージャーから MPLS インベントリを監視する。
- インシデントおよびサービスインパクトインシデントを表示して、ネットワークに関する問題を調査する。

**図 11 NNM iSPI for MPLS**



# 2 ソリューションの利点

ANM により、HP ソフトウェアネットワーク管理製品を使用して、完全なネットワーク管理を実行できます。可能な場合にはいつもでこれらの製品によってネットワーク管理タスクを自動化し、ネットワークエンジニアがネットワークのメンテナンスに要する時間を短縮することができます。

ANM 製品は、ネットワーク監視 (NNMi) システムとネットワーク設定 (NA) システムの間でネットワークデバイスのトポロジおよびインベントリデータを自動的に同期します。この共有情報により、現行オブジェクトのコンテキストで、NNMi コンソールからの NA ビューの起動をサポートします。デバイスインベントリの同期処理には、次の利点があります。

- 最新の適合資産管理情報が得られる。
- デバイスおよびサービスを短時間で本稼働環境に導入できる。
- 1 つのツールでインベントリを検出し、この情報を他のすべてのツールとの間で自動的に同期できる。
- さまざまな ANM ユーザーインタフェースでコンテキストに応じてクロス起動し、時間を節約して MTTR を短縮できる。
- ソリューションのすべての操作において、ネットワークインベントリとネットワークトポロジに関する共通の理解を得ることができる。

ANM 製品間でのシングルサインオンにより、ANM の各コンソール間を移動するときに各製品へのログオンが不要になり、ユーザーは当面のタスクに注意を集中することができます。

多くのネットワーク管理シナリオにおいて、エンドツーエンドのネットワーク管理のために ANM を活用できます。本章では、ANM の能力を示す次のシナリオ例について説明します。


- 「例 1: 非適合デバイス変更を識別して修正する」(24 ページ )
- 「例 2: ネットワーク障害問題をトラブルシューティングする」(26 ページ )
- 「例 3: デバイス設定の変更後にネットワークを通過するトラフィックフローを検証する」(28 ページ )
- 「例 4: IPv4 アドレスを対応する IPv6 アドレスに再割り当てする」(30 ページ )
- 「例 5: ネットワークのコンテキストからアプリケーションのパフォーマンス問題をトラブルシューティングする」(32 ページ )
- 「例 6: エッジルーターで期待されるサービスレベルを確保する」(34 ページ )
- 「例 7: ベースラインデータを使用してシステム使用率の異常を識別する」(35 ページ )
- 「例 8: エラーレートと使用率の問題を識別して修正する」(37 ページ )

# 例 1: 非適合デバイス変更を識別して修正する

不適切なデバイス設定は、ネットワーク問題の一般的な原因です。ANM は、非適合設定のデバイスが存在しないかどうかネットワークを監視し、デバイス設定が期待される以外の設定になっている場合に通知を生成することができます。ANM は、現在のデバイス設定と前のデバイス設定を比較したり、前の設定を使用するようにデバイスをリセットしたりするためのツールを用意しています。

## ANM なしのプロセス

この例では、デバイスに対して無権限での設定変更が行われます。デバイス設定変更について知らせる自動通知機能がない場合は、ネットワークオペレーターがデバイスの設定に誤りがあることを識別する必要があります。通常、変更に気付くのは、問題が発生したときか、手動での設定監査が実行されたときのみです。この時点で、ネットワークオペレーターは次の手順を実行します。

1. デバイスを特定し、設定管理システムにおける変更点を調べます。
2. マニュアルで指定されている設定とそのデバイスの設定を比較して調べ、その設定の変更が適合範囲外にあることを確認します。
3. 正しい設定を再作成するか、それをデバイスに復元します。
4. デバイスが正しく設定されたことを検証します。

## ANM によるプロセス

この例では、次の ANM 製品の機能を使用します。

- NNMi
- NA

ANM は、次のプロセスが有効になるように設定できます。

1. NA は、syslog イベント ( または別の変更トリガー ) を受信し、新しい設定を収集し、新しい設定で適合チェックを自動的に実行します。
2. NA は、非適合について記述した SNMP トラップを NNMi に送信します。NNMi は、このトラップを [ 重要な未解決インシデント ] ビューに表示します。
3. NNMi インシデントの分析ペインで [ **ノード設定の履歴** ] タブを開き、次に最新行の [ **前と比較** ] をクリックして、現在のデバイス設定と前のデバイス設定の比較を表示します。
4. NA コンソールで、実行設定への配備タスクを実行してデバイス設定をロールバックします。
5. NA がデバイスに適切な設定を復元し、新しい設定を収集します。次に NA は、自動的に新しい設定の適合性をチェックします。

## 利点

この例の場合、ANM を使用することには次の利点があります。

- 操作の効率が高まる。
- 変更が自動検出される。
- 適合性が自動的にチェックされる。
- 設定と適合性を 1 つのインシデントビューで確認することができ、それにより MTTR が短縮される。
- セキュリティとサービス可用性が向上し、それにより ROI が向上する。

# 例 2: ネットワーク障害問題をトラブルシューティングする

デバイス障害が発生した場合は、障害発生時のデバイスに関する情報を収集することが役立ちます。ANM は、デバイスについてクエリーを自動的に実行することができ、デバイスの障害インシデントに対応するためのツールを提供します。

## ANM なしのプロセス

この例では、ルーターでの ACL 設定によって、デスティネーションアドレスが 224.0.0.5 のトラフィックをブロックします。OSPF はこのアドレスに依存して hello パケットをブロードキャストするため、ルーターは近隣接続ルーターとの近隣接続を確立できません。自動処理なしの場合は、ルーターに直接接続して設定の調査と更新を行うことを含め、ネットワークオペレーターが徹底的な診断手順を実行することによってネットワーク障害インシデントに対応します。そのプロセスは、次のような手順になります。

1 ネットワーク障害インシデントを分類します。

2 ルーターにログオンして、インシデントの原因を特定する診断機能を実行します。

3 ルーターで、設定を更新します。

4 ルーターで、設定を目視で検査して正しいことを確認します。

## ANM によるプロセス

この例では、次の ANM 製品の機能を使用します。

- NNMi
- NA

ANM は、次のプロセスが有効になるように設定できます。

1 NNMi は、OSPF 近隣接続ノードの状態が変化したことを判別し、そのルーターの OSPFNbrStateChange インシデントを生成します。このインシデントによって NA が起動し、そのルーターに関する情報を収集します。

2 NA は、隣接デバイスの表示診断を実行してルーターの OSPF 近隣接続ノードを判別し、その診断のタスク ID を NNMi OSPFNbrStateChange インシデントの属性として保存します。

3 NNMi インシデントから、診断レポートを開き、OSPF 近隣接続が INIT 状態のまま留まっているかどうか判断します。

4 NA コンソールで、OSPF 近隣接続ルーターの診断レポートを表示し、ACL 設定エラーを確認します。

5 NA コンソールで、hello パケットを許可するように OSPF 近隣接続ルーターの ACL を変更します。

6 この問題の再発を防止するため、このデバイスまたはその他の関連デバイスで問題のある ACL が許可されないようにする NA デバイスポリシーを作成します。このポリシーに対する違反は、「例 1: 非適合デバイス変更を識別して修正する」で処理します。

## 利点

この例の場合、ANM を使用することには次の利点があります。

- 必要な時点で設定データを利用できる。
- 操作の効率が高まる。
- ネットワークの停止時間が短縮される。
- ネットワークのパフォーマンス問題が減少する。
- セキュリティとサービス可用性が向上し、それにより ROI が向上する。

# 例 3: デバイス設定の変更後にネットワークを通過するトラフィックフローを検証する

承認されたデバイス設定変更を完了する業務の一部として、ネットワークエンジニアは、変更によりアプリケーションのトラフィックが改善されたことの証拠を必要とします。ANM は、2 つのネットワークデバイス間のトラフィックのグラフを表示します。ネットワークエンジニアは、デバイス設定を変更する前後のグラフを表示し、変更の有効性を検証することができます。

## ANM なしのプロセス

この例の場合、ネットワークエンジニアは、その領域のネットワークの効率を改善することが期待されるデバイスで利用可能なルーティングプロトコルなどを変更して、デバイスの設定を更新することを計画します。ネットワークの自動化なしの場合、ネットワークエンジニアは、時間経過に伴うネットワークトラフィックフローの統計データを収集します。トラフィックフローに影響を与えるような方法でネットワークに変更を加えた後、ネットワークエンジニアは、再びトラフィックフロー情報を収集して、変更によってネットワークトラフィックに悪影響が出ていないことを検証します。そのプロセスは、次のような手順になります。

1. 一定期間、可能であれば一定間隔で、トラフィックフローデータを収集します。
   a. NetFlow エクスポーターにログオンします。
   b. NetFlow エクスポーターで、コマンド ( 例えば、show) を実行して、変更するデバイスの NetFlow 統計データを観察します。
   c. トラフィック統計情報を記録します。
   d. 一定期間、この手順を繰り返します。
2. トラフィックのルーティングに影響を与えるようにネットワーク設定を変更します。
3. データ収集プロセスを繰り返し行います。
4. ネットワークの変更後にトラフィックが再集中したことを検証するには、ネットワークの変更前後のトラフィックフローデータを比較します。

## ANM によるプロセス

この例では、次の ANM 製品の機能を使用します。

- NNMi
- NA
- NNM iSPI Performance for Traffic

ANM は、次のプロセスが有効になるように設定できます。

1. NNMi コンソールで、再構築するネットワーク領域でのトラフィックフローのソースノードとデスティネーションノードを表すトラフィック経路ビューを開きます ([ **アクション** ] > [ **トラフィックマップ** ] > [**Traffic パスビュー** ])。
2. NetFlow 対応のインタフェースを選択し、次に分析ペインで [ **パフォーマンス** ] タブを開きます。

   比較を行うため、トラフィックグラフの画面キャプチャを取得します。

3 トラフィックのルーティングに影響を与えるようにネットワーク設定を変更します。

4 ネットワークの変更後にトラフィックが再集中したことを確認するには、10 分待機してから [**パフォーマンス**] タブを更新して、更新されたトラフィックのグラフを表示します。

## 利点

この例の場合、ANM を使用することには次の利点があります。

- トラフィックフローデータの収集プロセスが簡素化される。
- 転記エラーのリスクがない。
- トラフィックフローを視覚化できる。

# 例4: IPv4アドレスを対応するIPv6アドレスに再割り当てする

IPv4 ネットワークのアドレスを再割り当てして IPv6 アドレスを使用するプロセスを手動で行うと、時間がかかり、誤りが入り込みやすくなります。ANM は、現在使用中の IPv4 アドレスの収集と管理対象デバイスの IPv6 アドレスの設定の両方を自動的に処理できます。

## ANM なしのプロセス

この例の場合、ネットワークエンジニアは、各デバイスから IPv4 情報を手動で収集し、次に IPv6 アドレスを使用して各インタフェースを手動で設定します。そのプロセスは、次のような手順になります。

1. 各デバイスの現在の IPv4 アドレスを確認します。
   a. デバイスにログオンします。
   b. 各インタフェースの IP アドレスを確認し、スプレッドシートファイルに記録します。
2. スプレッドシートファイルで、各 IPv4 アドレスを IPv6 アドレスにマップします。
3. IPv6 アドレスで各デバイスを設定します。
   a. デバイスにログオンします。
   b. スプレッドシートファイルを参照しながら、各インタフェースで正しい IPv6 アドレスを設定します。
   c. 設定を目視で検査して正しいことを確認します。

## ANM によるプロセス

この例では、次の ANM 製品の機能を使用します。

- NNMi
- NA

ANM は、次のプロセスが有効になるように設定できます。

1. NNMi コンソールで [IP アドレス ] インベントリビューをフィルターして、アドレスを再割り当てするネットワークの領域のみを表示し、そのリストをカンマ区切り値 (CSV) 形式でエクスポートします。
2. その CSV ファイルをスプレッドシートアプリケーションで開いた状態で、各 IPv4 アドレスを 1 つの IPv6 アドレスにマップし、そのスプレッドシートファイルを CSV 形式で保存します。
3. 新しい IPv6 アドレスを設定するスクリプトを作成します。
4. NA コンソールで、適切な時刻に適切なデバイスに対してそのスクリプトを実行する、スケジュールされたタスクを割り当てます。
5. NNMi コンソールで、[IP アドレス ] インベントリビューを CSV 形式ファイルにエクスポートします。
6. 設定した IPv6 アドレスと予定されている IPv6 アドレスを比較します。

## 利点

この例の場合、ANM を使用することには次の利点があります。

- データ収集と設定のプロセスが自動化される。
- アドレスの再割り当てでの誤りのリスクが抑えられる。

# 例 5: ネットワークのコンテキストからアプリケーションのパフォーマンス問題をトラブルシューティングする

重要なネットワークインタフェース間の予期せぬネットワークトラフィックは、アプリケーションのパフォーマンス問題の一般的な原因です。ANM は、重要なインタフェースの使用率を監視し、使用率が許容レベルを超えた場合には通知を生成することができます。ANM は、デバイス設定を更新して重要なインタフェースで許可されていないトラフィックをブロックするツールを提供します。

## ANM なしのプロセス

この例では、許可されていないトラフィックがネットワークインタフェースの帯域幅のかなりの部分を消費し、そのインタフェースを使用しているアプリケーションの応答時間が遅くなります。トラフィックの増加を知らせる自動通知機能なしの場合、ネットワークオペレーターは、アプリケーションユーザーがアプリケーションに対する不満を訴えるまで、トラフィックの増加に気付かないのが普通です。この時点で、ネットワークオペレーターは次の手順を実行します。

1. アプリケーションが使用する通信経路とサーバーを特定します。
2. traceroute を実行して、アプリケーショントラフィックの経路指定インフラストラクチャーを特定します。
3. 経路指定インフラストラクチャー内の各ルーターを調べます。
   a. ルーターにログオンします。
   b. ルーティングテーブルを調べ、アプリケーション経路に関連付けられているインタフェースを特定します。
   c. そのルーターについて全体として、およびアプリケーション経路に関係する個々のインタフェースについて、パフォーマンスメトリックスを収集します。
4. アプリケーション経路に配備されている sniffer またはプローブツールからトラフィックメトリックスを収集します。このデータを調べて、使用率が高いルーター全体にわたってターゲットのアプリケーショントラフィックを妨害している異常または許可されていないトラフィックを識別します。
5. 適切なネットワークデバイスにログオンして、許可されていないトラフィックをブロックするか、代替の、使用率の低いルーターを通過するようにアプリケーショントラフィックの経路指定を再度行います。

## ANM によるプロセス

この例では、次の ANM 製品の機能を使用します。

- NNMi
- NA
- NNM iSPI Performance for Metrics
- NNM iSPI Performance for Traffic

ANM は、次のプロセスが有効になるように設定できます。

1. NNMi は、重要なネットワークインタフェースについて、インタフェースの使用率が許容境界を超えたことを示す管理イベントインシデントを生成します。
2. トラフィックインベントリで NNMi インシデントのソースインタフェースを見つけ、分析ペインで [ **上位アプリケーション - 受信** ] タブを表示します。

   このタブには、トラフィックの大半を生成しているアプリケーションを示す円グラフが表示されます。このグラフにより、権限のないアプリケーションからの競合トラフィックが判明します。
3. NA コンソールで、ACL 行のバッチ挿入タスクを実行して複数の ACL を複数のデバイスに変更し、許可されていないトラフィックをブロックします。
4. そのインタフェース全体のネットワークトラフィックが許容レベルに戻り、NNMi コンソールでインタフェース使用率インシデントが自動的に終了します。

## 利点

この例の場合、ANM を使用することには次の利点があります。

- ネットワーク使用率の問題を見越した管理により、ミッションクリティカルなアプリケーションでのサービスレベルが高められる。
- ネットワーク使用率問題の検出、トラブルシューティング、および原因の修正を一式のツールで実行することができ、これらにより MTTR が短縮される。
- ネットワーク全体にわたり、重要なサービスに影響するネットワーク設定問題を事前に修正できる。
- パフォーマンスおよびトラフィックデータが自動的に収集される。
- 許可されていないトラフィックを検出してブロックする。

# 例 6: エッジルーターで期待されるサービスレベルを確保する

ネットワーク管理の観点からは、サーバーをすべてのユーザーが利用可能な状態で維持することが重要です。ビジネス管理の観点からは、インターネットサービスプロバイダー (ISP) から購入した一定レベルのサービスの提供を受けることが重要です。ANM は、企業のネットワークの外部にあるデバイスの応答性を監視し、応答性が許容レベルを下回った場合には通知を生成することができます。

## ANM なしのプロセス

この例では、ISP のネットワーク内の何らかの状態により、アプリケーショントラフィックをインターネットに搬送するエッジルーターの有効性が低下します。エッジルーターのパフォーマンスの低下を知らせる自動通知機能なしの場合、ネットワークオペレーターは、アプリケーションユーザーがアプリケーションに対する不満を訴えるまで、その問題に気付かないのが普通です。この時点で、ネットワークオペレーターは次の手順を実行します。

1 アプリケーションが使用する通信経路とサーバーを特定します。

2 通信とアプリケーションの経路のトラブルシューティングを行って、問題の原因がエッジルーターにあることを識別します。

3 ISP に問題を通知します。

## ANM によるプロセス

この例では、次の ANM 製品の機能を使用します。

- NNMi
- NNM iSPI Performance for QA

ANM は、次のプロセスが有効になるように設定できます。

1 NNMi は、エッジルーターからの IP SLA テストの特定のメトリックスが許容境界を超えたことを示す管理イベントインシデントを生成します。

2 NNMi インシデントの分析ペインで、IP SLA テストの最近の値を示す QA グラフを表示した [ **パフォーマンス** ] タブを開きます。

3 ISP に問題を通知します。

## 利点

この例の場合、ANM を使用することには次の利点があります。

- ネットワークが、重要なアプリケーションをサポートするために必要なすべての SLA に準拠していることを保証する。
- ISP を効果的に監視して、確実に契約したサービスの提供を受ける。

# 例 7: ベースラインデータを使用してシステム使用率の異常を識別する

不規則なトラフィックパターンは、ネットワークの使用状態が不適切であることを示す可能性があります。ANM は、通常のトラフィックパターンを判別し、トラフィックパターンが通常の範囲外になった場合には通知を生成することができます。

## ANM なしのプロセス

この例の場合、会社のお客様は、会社のメイン Web サイトにインターネットからアクセスするときの遅さについて不満を訴えます。この時点で、ネットワークオペレーターは次の手順を実行します。

1. Web サーバーと外部ルーターのネットワーク使用率を調べ、使用率が高いことを確認します。
2. sniffer を使用し、パフォーマンスツールを実行し、ファイアウォールのログを調べて遅さの原因を特定します。
3. その Web サイトの URL が多くの HTTP 要求とともにロードされていることを確認します。要求は Web サイトでの攻撃のように見えます。
4. Web サイトへのすべての接続を終了し、その Web サイトを完全に停止させます。
5. その状況での支援を得るため、セキュリティのスペシャリストに連絡します。

## ANM によるプロセス

この例では、次の ANM 製品の機能を使用します。

- NNMi
- NA
- NNM iSPI Performance for Metrics
- NNM iSPI Performance for Traffic

ANM は、次のプロセスが有効になるように設定できます。

1. NNMi は、Web サイトへのパスに含まれるインタフェースでの使用率に関して、通常の状態からの逸脱を示す管理イベントインシデントを生成します。
2. NNM iSPI Performance for Traffic は、Web サイトの場所を表す NNM iSPI Performance for Traffic サイトに向かう HTTP トラフィックに関して、高ボリュームのデータを示す管理イベントインシデントを生成します。
3. NNM iSPI Performance for Traffic インシデントから、分析ペインの [ **上位アプリケーション - 受信** ] タブを開いてインシデントで特定されるインタフェースを表示します。

   このタブには、トラフィックの大半を生成しているアプリケーションを示す円グラフが表示されます。
4. [ トラフィック分析 ] ワークスペースのトラフィックレポートインタフェーステーブルから、NNM iSPI Performance for Traffic インシデントで示されるインタフェースを開きます。

   [ **上位 5 のソース** ] および [ **上位 5 のデスティネーション** ] タブに、限られたホストにおけるインタフェースの高い使用率が表示されます。

5 その Web サイトの URL が多くの HTTP 要求とともにロードされていることを確認します。要求は Web サイトでの攻撃のように見えます。

6 NA コンソールで、Web サーバーをホストしているデバイスの ACL を変更して、攻撃元からのトラフィックを拒否します。

7 そのインタフェース全体のネットワークトラフィックが許容レベルに戻り、NNMi コンソールでインタフェース使用率インシデントが自動的に終了します。

## 利点

この例の場合、ANM を使用することには次の利点があります。

- ネットワーク使用率の問題を見越した管理により、お客様の満足度を高めることができる。
- ネットワーク使用率問題の検出、トラブルシューティング、および原因の修正を一式のツールで実行することができ、これらにより MTTR が短縮される。
- 許可されていないトラフィックを検出してブロックする。
- 高品質なサービスを提供する。

# 例 8: エラーレートと使用率の問題を識別して修正する

インタフェースでのエラーレートが高いと、通常、そのインタフェースに接続されているワークステーション、サーバー、またはその他のデバイスの動作が著しく遅くなります。ANM は、インタフェースを監視し、エラーレート、使用率、またはその両方が定義済みのしきい値を超えた場合には通知を生成することができます。

## ANM なしのプロセス

この例の場合、重要なアプリケーションの応答が遅くなり、最終的にタイムアウトしますが、問題は自然に解消されます。この障害はピーク使用期間中に断続的に発生するため、アプリケーションをより処理能力の高いサーバーに移動します。この変更を行っても、アプリケーションのタイムアウトは回避されません。最終的に、全二重の不一致が発見されます。全二重設定を修正すると、タイムアウト問題が解決します。

## ANM によるプロセス

この例では、次の ANM 製品の機能を使用します。

- NNMi
- NA
- NNM iSPI Performance for Metrics

ANM は、次のプロセスが有効になるように設定できます。

1. NNMi は、インタフェースでのエラーレートが高いことを示す管理イベントインシデントを生成します。インシデントの詳細タブの接続テーブルは、全二重の不一致を示します。
2. NNMi コンソールで、接続の両端それぞれにあるルーターの [ デバイス設定の違い ] ページを開き、このインタフェースで設定されている全二重を確認し、デバイス設定が最近変更されたかどうかを調べます。
3. 修飾インタフェース名によってグループ化された LAN 衝突率メトリックスおよび LAN 衝突カウントメトリックスについての、NNM iSPI Performance for Metrics インタフェースヘルスレポートを開きます。また、修飾インタフェース名によってグループ化されたLAN FCSエラーレートメトリックスおよび LAN FCS エラーカウントメトリックスについての NNM iSPI Performance for Metrics インタフェースヘルスレポートも開きます。

   この組み合わせレポートには、接続の一方の側にエラーが多いが、他方の側には衝突数が多いことが示されます。この情報は、全二重の不一致を示すものです。
4. NA コンソールから、スイッチ設定を更新します。
5. NNM iSPI Performance for Metrics のレポートでインタフェースのパフォーマンス履歴を調べ、エラー問題が発生しなくなったことを検証します。

## 利点

この例の場合、ANM を使用することには次の利点があります。

- アプリケーションのパフォーマンスに影響が出る前に、ネットワークの設定誤りを事前に検出できる。
- ネットワーク使用率問題の検出、トラブルシューティング、および原因の修正を一式のツールで実行することができ、これらにより MTTR が短縮される。

# フィードバックをお待ちしております。

ご使用のシステムに電子メールクライアントが設定されている場合は、デフォルトで、ここをクリックすると電子メールウィンドウが開きます。

使用可能な電子メールクライアントがない場合は、Web メールクライアントの新規メッセージに以下の情報をコピーして、**ovdoc-nsm@hp.com** にこのメッセージを送信してください。

**製品名およびバージョン :** ANM 9.20

**ドキュメントタイトル :** ANM コンセプトガイド

**フィードバック :**