CiscoWorks Network Compliance Manager 1.8
サテライト ユーザ ガイド

Text Part Number: OL-27503-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CiscoWorks Network Compliance Manager 1.8 サテライト ユーザ ガイド

Contents

1　スタートアップ ガイド

このマニュアルには、CiscoWorks Network Compliance Manager ソフトウェア（NCM）サテライト機能の設定に関する情報が含まれています。

サテライトのインストールは、英語で実行されるサポート対象オペレーティング システム上でのみサポートされます。

用語

このガイドでは次の用語が使用されています。

- **レルム**：重複する IP アドレスを含まない到達可能なネットワークの集合。
- **IP スペース**：重複する IP アドレスを持たない 1 つ以上のレルム。
- **NCM コア**：単一の NCM Management Engine、関連サービス（Syslog と TFTP）、および単一のデータベース。NCM コアにより複数のパーティションを管理できます。
- **NCM ゲートウェイ**：管理対象デバイスとの間でトラフィックをトンネルするサービス。NCM ゲートウェイは、IP トラフィックを他のゲートウェイへとルーティングします。ゲートウェイを使用すると、NAT されたデバイスやファイアウォールの向こうにあるサーバを管理できます。さらに、ゲートウェイはレルム間のトンネルに対する帯域幅スロットルをサポートしており、SSL プロキシまたは TCP ポート フォワーディングが使用されている場所ならばどこでも使用可能です。トンネルは、SSL を使用して認証および暗号化が可能です。
- **コア ゲートウェイ**：コアと同じレルム内で実行される NCM ゲートウェイ。コア ゲートウェイは、サテライト ゲートウェイと同じソフトウェアです。サテライト ゲートウェイの場合とは異なり、コア ゲートウェイは、NCM コアに対して簡単に設定できます。NCM コアが 1 つしかない場合には、コア ゲートウェイ レルムの名前を「Default Realm」にする必要があります。

  NCM 管理設定を使用する場合は、ローカル ゲートウェイ ホストが使用されます。このオプションはコア ゲートウェイと関連することに留意してください。

- **サテライト ゲートウェイ**：NCM コアを含まないレルムで実行されるゲートウェイ。サテライト ゲートウェイには、NCM ゲートウェイ サービスと NCM リモート エージェントが含まれます。
- **NCM リモート エージェント**：NCM リモート エージェントには以下が含まれます。
  - SNMP の処理を行い、NCM コア上の NCM Management Engine と連係するプロセス。
  - ローカル デバイスからの Syslog 通知の処理を行う Syslog プロセス。
  - ローカル デバイスへの TFTP アクセスを可能にする TFTP プロセス。
- **トンネル**：2 つのゲートウェイ間の通信を可能にする、ゲートウェイ間の TCP/IP 接続。

- **ゲートウェイ メッシュ**：2 つ以上のゲートウェイの集合で、それらのゲートウェイの間でトラフィックがルーティングされます。少なくとも、ゲートウェイ メッシュは 1 つのコア ゲートウェイと 1 つのサテライト ゲートウェイから構成されます。
- **ゲートウェイ暗号データ ファイル**：SSL ゲートウェイ通信用の秘密キーと公開キーが含まれます。

サテライト機能により何が行われますか？

今日の企業ネットワークは複雑で、企業の本社とリモート オフィスを接続するさまざまなタイプの回線を含んでいます。しばしば、そのようなオフィスの間のリンクは、パブリック ネットワーク上の VPN 接続や帯域幅が制限された回線（またはその両方）を横断しています。これらの不確定要素のために、多くの場合、セキュリティと効率が最上位の懸案事項になっています。

サテライト機能は、NCM コアとリモート ネットワークの間に暗号化されたトンネルを作成することにより、NCM コアからリモート ネットワークへのパケットをルーティングするための安全な手段を提供します。1 つ以上のサテライト ゲートウェイが存在する場合は、NCM Management Engine によりトンネルのネットワーク内に NCM メッシュが作成され、NCM コアは NCM メッシュを介して任意のサテライト ゲートウェイに安全に到達することができます。

以下の理由のため、コア ゲートウェイを NCM コアと同じホスト上で実行することが推奨されます。

- パフォーマンス：TCP/IP ソケットのオーバーヘッドを回避することができます。
- セキュリティ：パケットは内部で送信されるため、ネットワーク上の他のホストはスヌープすることができません。NCM コアとコア ゲートウェイの間の接続は暗号化されません。したがって、同じホスト上でローカル接続を使用するとさらに安全になります。

NCM ゲートウェイは Windows オペレーティング システム上では実行されません。NCM アプリケーション サーバで Windows オペレーティング システムが使用される場合、コア ゲートウェイは NCM コアとは異なるホスト上になければなりません。

サテライト機能は、パケットを暗号化し、開く必要のあるファイアウォール ポートの数を制限することにより、NCM コアとリモート ネットワークの間の通信を簡素化することができます。このため、ファイアウォールにより通信が制限されている場合、またはネットワーク間の通信を保護しなければならない場合の初期セットアップを簡素化することができます。

NCM リモート エージェントのインストール時に、NCM によってサテライト ホストとの SSH 接続が作成されます。この接続は、ゲートウェイ メッシュを介して作成されます。したがって、SSH 用ポート 22 へのアクセスをファイアウォールが許可する必要はありません。ポート 2001（ゲートウェイ トンネル ポート）のみを開かなければなりません。

現在、Detect Network Devices タスクと OS Analysis タスクは、NCM サテライトにより管理されるデバイスに対しては機能しません。

サテライト機能は、自分に適していますか？

以下を管理している場合にサテライト構成を使用できます。

- NCM コア間で厳格なファイアウォール ルールを適用している高速な LAN 上のデバイス。NCM サテライトにより、NCM コアとデバイスの間の接続の管理が容易になります。
- 重複する IP アドレスを持つデバイス。NCM コアは、同じ IP アドレスを持つ 2 つのデバイスを直接に管理することはできません。サテライト機能を使用すると、ネットワークを複数のレルムへと分割し、すべてのデバイスに直接にアクセスすることができます。
- 速度のために、ただし第一にはセキュリティのために TFTP をローカル サーバのみに制限しているデバイス。ローカル ネットワークを経由するトラフィックは、ファイアウォールを横断してインターネットに入るトラフィックよりも安全です。
- 低速な WAN リンクを使用し、ソフトウェアアップグレード中にネットワーク中断の影響を受けるデバイス。リモート デバイスと同じ LAN 上にあるサテライトにはソフトウェア イメージがキャッシュされるため、ネットワークを通じた NCM コアからサテライトへのコピーが 1 回だけで済みます。

ゲートウェイ メッシュを実行するためのサーバが必要になることに留意してください。ゲートウェイ メッシュを適切に作成するためには各ゲートウェイをインストールする必要があります。

インストールの前提条件

サテライト機能をインストールする前に、以下の点に留意してください。

- サテライトのインストールは、英語で実行されるサポート対象オペレーティング システム上でのみサポートされます。
- ゲートウェイ メッシュを実行するためのサーバが必要になります。ゲートウェイ メッシュを適切に作成するためには各ゲートウェイをインストールしなければなりません。
- レルム内では、IP アドレス スペースは一意でなければなりません。
- ゲートウェイ メッシュを使用すると、Telnet により管理されるデバイスに対して暗号化を追加できます。しかし、Telnet 接続の暗号化は、コア ゲートウェイとリモート ゲートウェイの間のみでの暗号化であることに留意してください。パケットがゲートウェイを離れた後では、クリア テキストになります。
- ゲートウェイ間のすべてのトラフィックは、ゲートウェイ メッシュごとに作成される秘密キー（ゲートウェイ暗号データ ファイル内に保存されます）を使用した SSL によって暗号化されます。
- ゲートウェイは、レルム間のトラフィックをスロットリングすることができます。これは、NCM が低速リンクを使用してリモート デバイスを管理している場合、デバイスの設定をキャプチャするときにリンクが飽和しないことを保証するために便利です。
- 冗長性のために、複数のゲートウェイを同じレルム内にインストールすることができます。したがって、サテライト ゲートウェイにはレルム名とゲートウェイ名の両方があります。
- サテライト ゲートウェイのインストール前にコア ゲートウェイをインストールします。
- サテライト ゲートウェイからコア ゲートウェイへの TCP ポート 2001 を開かなければなりません。

- サテライト ゲートウェイのインストール中には、サテライト ゲートウェイからコア ゲートウェイへのポート 9090 も開かなければなりません。サテライト ゲートウェイのインストール後に、ポート 9090 は必要なくなります。

ファイアウォールでポート 3333 を開く必要はありません。NCM ゲートウェイ インストーラでは、コア ゲートウェイと同じホストにサテライト ゲートウェイがインストールされないことを保証するために、ポート 3333 が使用されます。NCM ゲートウェイ インストーラは、ポート 3333 上でリッスンして、ポート 3333 上でコア ゲートウェイと接続しようと試みます。ポート 3333 との接続は失敗するはずです。接続が成功した場合、NCM ゲートウェイ インストーラはエラーで終了します。

インストール例については、付録 A を参照してください。

ゲートウェイによりサポートされるプラットフォーム

- このサテライト機能では、以下のプラットフォーム上の CiscoWorks Network Compliance Manager（NCM）バージョン 1.2 以降がサポートされます。
- Red Hat-Linux-3AS
- Red Hat-Linux-4AS
- Red Hat-Linux-5SERVER-X86-64
- SuSE-Linux-9ES, 10.x
- SunOS-5.9
- SunOS-5.10

RH EL 5 にゲートウェイをインストールするためには追加手順が必要なことに注意してください。

1. <*gateway directory*>*/lib/* に移動します。
2. *rpm -ivh OPSWgw-ism-37.0.0.0.12.7-1.x86_64.rp*m を実行します。
3. tar xvzf saOPSWgw-ncm-37.0.0.0.12.7-installer-RedHat-Linux-5SERVER-X86_64.tgz
4. mv saOPSWgw-37.0.0.0.12.7-installer-RedHat-Linux-5SERVER-X86_64/ saOPSWgw-ncm-37.0.0.0.12.7-installer-RedHat-Linux-5SERVER-X86_64
5. tar -cvzf saOPSWgw-ncm-37.0.0.0.12.7-installer-RedHat-Linux-5SERVER-X86_64.tgz saOPSWgw-ncm-37.0.0.0.12.7-installer-RedHat-Linux-5SERVER-X86_64/

リモート エージェント プラットフォーム

表 1 には、サポートされるリモート エージェント プラットフォームに関する情報を記載しています。

表 1　　NCM サテライトによりポートされるプラットフォーム

	OS	バージョン	アーキテクチャ
Red Hat	RH AS RH EL	3（32 ビット）、4（32 ビット） 5（64 ビット）	i386 i386
Oracle	Solaris	9、10	Oracle SPARC
Novell	SuSE Enterprise Linux Server	9ES、10.x	i386

HP Server Automation（SA）と NCM の間でのサテライト共有は、SA 7.50 と NCM 1.8 でサポートされます。VMWare 上でのサテライトの実行は、SA 7.50 と NCM 1.8 でサポートされます。

ハードウェアの要件

表 2 に、サテライト機能の最小ハードウェアをリストします。

表 2　　NCM サテライトの最小ハードウェア

カテゴリ	最小ハードウェア
CPU	各サテライト コアの 1,500 台の管理対象サーバ、および 5,000 ネットワーク ノードごとに 2 個の CPU。
メモリ	各サテライト コアの 1,500 台の管理対象サーバ、および 5,000 ネットワーク ノードごとに 4 GB の RAM。
ディスク	128 GB

2 インストール

サテライトのインストールは以下のプロセスから構成されます。

- 「コア ゲートウェイのインストール」（P.12）の記載に従って各 NCM コアにコア ゲートウェイをインストールする。最初のコア ゲートウェイをインストールするとゲートウェイ暗号データ ファイルが作成されますが、該当する場合、これは他のコア ゲートウェイをインストールするために必要になります。
- 「サテライト ゲートウェイのインストール」（P.14）の記載に従って各リモート レルムにサテライト ゲートウェイをインストールする。
- 「コア ゲートウェイと通信するための NCM の設定」（P.14）の記載に従って NCM を設定する。コア ゲートウェイ ホスト（ローカル ゲートウェイ ホストと呼ばれます）の場合は、コア ゲートウェイの DNS ホスト名または IP アドレスを知る必要があります。
- 「サテライト ゲートウェイ ホストへのリモート エージェントの追加」（P.17）に記載の方法で各リモート Stellite ゲートウェイ ホストにリモート エージェントを導入する。インストールした各サテライト ゲートウェイについて Deploy Remote Agent タスクを使用しなければなりません。

推奨事項

サテライト機能が適切にインストールおよび実行されることを保証するためには、以下の推奨事項に従う必要があります。

- NCM コアごとにコア ゲートウェイを 1 つずつインストールすること。
- NCM コアが Solaris または Linux プラットフォーム上で実行されている場合は、NCM コアと同じホストにコア ゲートウェイをインストールすること。サテライト ゲートウェイの前にコア ゲートウェイをインストールしなければならないことに留意してください。
- 複数のコア ゲートウェイがある場合は、各サテライト ゲートウェイは各コア ゲートウェイへのトンネルを持つ必要があります。

セキュリティ

Solaris または Linux プラットフォーム上に NCM コアをインストールした後で、同じホスト上にコア ゲートウェイをインストールすること。これにより、NCM コアとコア ゲートウェイの間の通信がプライベートになることが保証されます。

ゲートウェイ暗号データ ファイル（コア ゲートウェイのインストール時にゲートウェイ インストーラによってゲートウェイ暗号データ ファイルが作成されます）を安全な場所に保管してください。このファイルに含まれる秘密キーにより、誰がゲートウェイ メッシュと接続できるのかが制御されます。ゲートウェイ メッシュ内の各ゲートウェイには独自の暗号キーがあり、コア ゲートウェイがゲートウェイ メッシュに参加するためには、公開キーを知らなければなりません。

冗長性

冗長性のために、同じレルムに複数のサテライト ゲートウェイをインストールすることができます。

コア ゲートウェイのインストール

NCM コアと同じレルムにコア ゲートウェイをインストールするには、次の手順を実行します。

xterm で次を実行します（$DISPLAY は必要ありません）

1. `cisco_gw-37.0.0.0.12.7-2.zip` を解凍します。
2. **`perl install.pl`** と入力してから Enter を押します。
3. プラットフォームの番号を入力してから Enter を押します。
4. 新しいコア メッシュを設定するのか、新しいコア ゲートウェイを追加するのか、新しいゲートウェイを既存のメッシュに追加するのかがインストーラにより尋ねられます。
   a. これが最初のコア ゲートウェイである場合は、**1** を入力します。
   b. これがコア ゲートウェイであるものの、最初のコア ゲートウェイではない場合は、**2** を入力します。
   c. Enter を押します。
5. ゲートウェイ暗号データ ファイルの新しいパスワードを入力するように求められた場合は、ゲートウェイ メッシュを保護するためのパスワードを入力してから Enter を押します。求められる場合は、ゲートウェイ暗号データ ファイルの新しいパスワードを再入力してから Enter を押します。
6. このゲートウェイと接続するその他のゲートウェイの IP アドレスまたはホスト名を入力してから Enter を押します。
7. コア NCM サーバの IP アドレスまたはホスト名を入力してから Enter を押します。
8. ゲートウェイ名を求められた場合は、インストールしているゲートウェイの名前を入力してから Enter を押します。ゲートウェイ名にスペースを含めることはできません。
9. レルム名を求められた場合は、ゲートウェイのインストール先であるレルムの名前を入力してから Enter を押します。注記：これがコア ゲートウェイの場合は、**`Default Realm`** と入力します。

10 ゲートウェイ設定オプションを見直します。正しい場合は **y** と入力してから Enter を押します。

ゲートウェイ暗号データ ファイルは、サテライト ゲートウェイのインストールに必要となります。ゲートウェイ間の IP トラフィックを保護するために、このデータ ファイルを安全な場所に保管してください。さらに、NCM にはコア ゲートウェイの管理ポート用の秘密キーが必要です。コア ゲートウェイが NCM コアと同じホスト上にない場合は、後で使用するために `saOPSWgw*/certificates/opswgw-mngt-server.pkcs8` ファイルをコピーします。

NCM コアと同じサーバ上に最初のコア ゲートウェイをインストールするには、次の手順を実行します。

xterm で次を実行します（$DISPLAY は必要ありません）

1 `cisco_gw-37.0.0.0.12.7-2.zip` を解凍します。

2 **`perl install.pl`** と入力してから Enter を押します。

3 プラットフォームの番号を入力してから Enter を押します。

4 新しいコア メッシュを設定するのか、新しいコア ゲートウェイを追加するのか、新しいゲートウェイを既存のメッシュに追加するのかがインストーラにより尋ねられます。

   a これが最初のコア ゲートウェイである場合は、**1** を入力します。

   b これがコア ゲートウェイであるものの、最初のコア ゲートウェイではない場合は、**2** を入力します。

   c Enter を押します。

5 ゲートウェイ暗号データ ファイルの新しいパスワードを入力するように求められた場合は、ゲートウェイ メッシュを保護するためのパスワードを入力してから Enter を押します。求められる場合は、ゲートウェイ暗号データ ファイルの新しいパスワードを再入力してから Enter を押します。

6 これがコア ゲートウェイであるかどうかを尋ねられた場合は、**y** を入力してから Enter を押します。

7 このゲートウェイと接続するその他のゲートウェイの IP アドレスを入力してから Enter を押します。

8 コア NCM サーバの IP アドレスまたはホスト名（通常は 127.0.0.1）を入力してから Enter を押します。

9 コア アプリケーション サーバもこのホストにインストールするかどうかを尋ねられた場合は、**y** を入力してから Enter を押します。

10 コア アプリケーション サーバのインストール場所を尋ねられた場合は、NCM のインストール ディレクトリを入力してから Enter を押します。

11 ゲートウェイ名を求められた場合は、インストールしているゲートウェイの名前を入力してから Enter を押します。

12 レルム名を求められた場合は、ゲートウェイのインストール先であるレルムの名前を入力してから Enter を押します。注記：これがコア ゲートウェイの場合は、**`Default Realm`** と入力します。

13 ゲートウェイ設定オプションを見直します。正しい場合は **y** と入力してから Enter を押します。

サテライト ゲートウェイのインストール

NCM コアを持たないすべてのレルムにサテライト ゲートウェイをインストールします。

xterm で次を実行します（$DISPLAY は必要ありません）

1. `cisco_gw-37.0.0.0.12.7-2.zip` を解凍します。
2. **`perl install.pl`** と入力してから Enter を押します。
3. プラットフォームの番号を入力してから Enter を押します。
4. 新しいコア メッシュを設定するのか、新しいコア ゲートウェイを追加するのか、新しいゲートウェイを既存のメッシュに追加するのかがインストーラにより尋ねられます。**3** を入力してから Enter を押します。
5. サテライト ゲートウェイをインストールするためには、コア ゲートウェイのインストール中に作成されたゲートウェイ暗号データ ファイルのファイル名が必要です。ファイル名にコロン（:）が含まれる場合は、ファイルをコピーするために SCP が使用されます。ゲートウェイ暗号データ ファイルを含むディレクトリへのパスを入力してから Enter を押します。たとえば、コア ゲートウェイをホスト 'foo' にインストールし、ゲートウェイ暗号データ ファイルを `/tmp/gw` に保存した場合は、次のように入力します：`LOGINNAME@foo:/tmp/gw`
6. ゲートウェイ暗号データ ファイルのパスワードを求められた場合は、コア ゲートウェイのインストール時に使用したパスワードを入力してから Enter を押します。求められる場合は、ゲートウェイ暗号データ ファイルの新しいパスワードを再入力してから Enter を押します。
7. コア ゲートウェイと接続するための IP アドレスまたは DNS ホスト名を求められた場合は、このサテライト ゲートウェイと接続するコア ゲートウェイの IP または DNS ホスト名を入力してから Enter を押します。
8. コア NCM サーバの IP アドレスまたはホスト名（通常は 127.0.0.1）を入力してから Enter を押します。
9. ゲートウェイのゲートウェイ名を求められた場合は、インストールしているゲートウェイの名前を入力してから Enter を押します。
10. ゲートウェイのレルム名を求められた場合は、ゲートウェイのインストール先であるレルム名を入力してから Enter を押します。注記：これがコア ゲートウェイの場合は、Default Realm と入力します。
11. ゲートウェイ設定オプションを見直します。正しい場合は **`y`** と入力してから Enter を押します。

コア ゲートウェイと通信するための NCM の設定

コア ゲートウェイと通信するための NCM を設定するには、次の手順を実行します。

1. NCM がインストールされているホストにログインします。
2. コア ゲートウェイが NCM コアと同じホスト上にない場合は、コア ゲートウェイから NCM のインストール先のルートに `opswgw-mngt-server.pkcs8` ファイルをコピーします。一般には、`C:\NCM` または `/opt/NCM` です。
3. 管理者として NCM にログインします。

4 メイン メニューで、[Admin] > [Administrative Settings] > [Device Access] の順にクリックします。[Administrative Settings - Device Access] ページが開きます。

5 [Gateway Mesh] セクションまで下にスクロールします。

6 コア ゲートウェイ ホストの場合（ローカル ゲートウェイ ホストと呼ばれます）には、コア ゲートウェイの DNS ホスト名または IP アドレスを入力します。一般に、同じシステムにインストールする場合は `localhost` となります。

7 [Save] をクリックします。

[Gateways] ページ

NCM がコア ゲートウェイと通信できるかどうかをテストするには、メイン メニューバーで、[Admin] > [Gateways] の順にクリックします。[Gateway List] ページが開きます。[Gateway List] ページには、現在設定されているゲートウェイが表示されるため、ゲートウェイ情報を編集することができます。詳細については、「[Edit Gateway] ページ」（P.17）を参照してください。

表 3 に、[Gateway List] ページの説明を示します。

表 3　　[Gateway List] ページのフィールド

フィールド	説明 / 処理
Deploy Remote Agent link	[Deploy Remote Agent] ページが開くので、NCM リモート エージェントを導入できます。
IP Space	IP スペース名が表示されます。IP スペースは、重複する IP アドレスを持たない 1 つ以上のレルムです。
Realm	レルム名が表示されます。ゲートウェイからレルム名が返されます。レルム名は、ゲートウェイのインストール時に設定されるため、NCM で変更することはできません。レルム名を変更するには、ゲートウェイを再インストールする必要があります。
Gateway	ゲートウェイ名が表示されます。ゲートウェイ名は、ゲートウェイのインストール時に設定されるため、NCM で変更することはできません。
Host	ゲートウェイのインストール先であるシステムのホスト名または IP アドレスが表示されます。ゲートウェイ ホストに複数の IP アドレスがある場合、これはそのゲートウェイ ホストから使用されることになる IP アドレスです。ホスト IP アドレスが重要になるのは、同じレルム内に 1 つ以上のゲートウェイをインストールしてある場合に限られます。 **注記**：冗長性のために、同じレルムに複数のサテライト ゲートウェイをインストールできます。
Partition	該当する場合は、レルム名と関連付けられた NCM パーティション名が表示されます。
Core	マルチマスター分散システム環境では、コア名は [Edit Core] ページで設定されます。[Edit Core] ページのレルム名が、ゲートウェイのレルム名と一致する場合は、[Gateway List] ページにそのコアのコア名が表示されます。
Agent	サテライト ゲートウェイの NCM リモート エージェントの名前が表示されます。 NCM リモート エージェント名を [Edit Gateway] ページで変更することができます。ゲートウェイ メッシュをインストールした後で、各サテライト ゲートウェイ ホスト上に NCM リモート エージェントをインストールしなければなりません。NCM リモート エージェントがインストールされていない場合、[Agent] カラムは空になります。
Actions	オプションが 1 つあります。 • [Edit]：[Edit Gateway] ページが開きます。

[Edit Gateway] ページ

IP スペース名は、レルム名に基づいて NCM により自動的に設定されます。しかし、同じ IP スペース内に 2 つのレルムがあり、L3 ダイアグラム内にそれらを正確に図示したい場合は、ゲートウェイを編集して IP スペース名を設定することができます。

[Edit Gateway] ページを開くには、[Gateway List] ページで、[Actions] カラム内の [Edit] オプションをクリックします。表 4 に、[Edit Gateway] ページの説明を示します。

表 4　　[Edit Gateway] ページのフィールド

フィールド	説明 / 処理
Gateway	ゲートウェイ名が表示されます。ゲートウェイ名は、ゲートウェイのインストール時に設定されるため、NCM で変更することはできません。
Realm	レルム名が表示されます。ゲートウェイからレルム名が返されます。レルム名は、ゲートウェイのインストール時に設定されるため、NCM で変更することはできません。
IP Space	IP スペース名が表示されます。IP スペースは、重複する IP アドレスを持たない 1 つ以上のレルムです。新しい IP スペース名を入力します。
Host	ゲートウェイのインストール先であるシステムのホスト名または IP アドレスが表示されます。新しいホスト名または IP アドレスを入力します。
Satellite	NCM コアを持たないレルムで実行されているサテライト ゲートウェイが表示されます。該当する場合は、サテライト ゲートウェイの名前を入力します。

サテライト ゲートウェイ ホストへのリモート エージェントの追加

リモート エージェントをサテライト ゲートウェイ ホストに追加するには、NCM で Deploy Remote Agent タスクを作成しなければなりません。Deploy Remote Agent タスクを使用すると、各ゲートウェイ ホスト上に NCM リモート ホストを導入できます。NCM リモート エージェントを、管理されるデバイスと同じ LAN 上にインストールすることにより、WAN トラフィックを最小化して、Syslog と TFTP を使用して各デバイスをローカルに管理することができます。

Deploy Remote Agent タスクを開くには、次の手順を実行します。

1. NCM にログインします。
2. メニューバーで、[Tasks] > [New Task] > [Deploy Remote Agent] の順にクリックします。[Deploy Remote Agent] ページが開きます。終了したら忘れずに、[Save Task] をクリックします。タスクがただちに実行されるようにスケジュールされている場合には、[Task Information] ページが開きます。[Task Information] ページには、タスクの詳細、たとえばタスクの開始日付、期間、ステータスが表示されます。

表 5 に、[Deploy Remote Agent] ページの説明を示します。

表 5　[Deploy Remote Agent] ページのフィールド

フィールド	説明 / 処理
Task Name	Deploy Remote Agent が表示されます。該当する場合は、別のタスク名を入力できます。
Save Options	次のオプションのいずれかを選択します。 • [Save as task] : デフォルトではこのオプションが選択されます。 • [Save as task template] : これを選択した場合、タスクはタスク テンプレートとして保存され、[Tasks Templates] ページに表示されます。
Start Date	次のオプションのいずれかを選択します。 • Start As Soon As Possible（デフォルト） • [Start At] : タスクの開始日時を入力します。日付ボックスの横にあるカレンダー アイコンをクリックするとカレンダーが開くので、日時を選択します。
Task Priority	タスクの優先順位を設定できます。下向きの矢印をクリックして、1 ～ 5 までのタスク優先順位を選択します。ここで、1 が最も高い優先順位になります。デフォルト値は 3 です。高い優先順位のタスクは低い優先順位のタスクより先に実行されます。
Comments	タスクに関するコメントを入力します。
タスクのオプション	
Action	次のオプションのいずれかを選択します。 • [Install]（または [Reinstall]）: NCM リモート エージェントをインストールします。すでに NCM リモート エージェントがインストールされている場合は、既存の NCM リモート エージェントが削除され、新しい NCM リモート エージェントがインストールされます。 • [Uninstall] : NCM リモート エージェントをアンインストールします。
Deploy Agent to Gateway	NCM リモート エージェントの導入先とするゲートウェイ名をドロップダウン メニューから選択します。
Login	リモート エージェントを導入するためには、サテライト ゲートウェイ ホスト上でルート権限が必要です。次のオプションのいずれかを選択します。 • [As Root] : ユーザ名 root として SSH して root のパスワードを入力します。 • [As Non-root] : ルート以外のユーザとして SSH します。このオプションを選択した場合は、su パスワード（root のパスワード）または sudo パスワード（sudo のパスワード、一般にはユーザ名のパスワードと同じですが、sudo の設定方法しだいでは異なっていてもかまいません）を選択します。

表 5　　[Deploy Remote Agent] ページのフィールド

フィールド	説明 / 処理
Managing Core	コア ゲートウェイを NCM コアと同じホスト上にインストールする場合は、[Managing Core] を「localhost」とする必要があります（デフォルト）。コア ゲートウェイが NCM コアとは異なるホスト上にある場合は、[Managing Core] を NCM コアのホスト名または IP アドレスとする必要があります。 （**注記**：NCM コア ホストが別の IP アドレスを持っている場合は、コア ゲートウェイ ホストから NCM コアに接続する際に適している IP アドレスを使用します）
In Realm	コア ゲートウェイのレルム名をドロップダウン メニューから選択します。
承認オプション 承認オプションが表示されるのは、タスクが Workflow Approval Rule の一部である場合に限られます。	
Request Approval	タスクの実行前に承認が必要な場合は、デフォルトでチェックされます。どの日付までにタスクを承認しなければならないのかを変更するには、日付の横にあるカレンダー アイコンをクリックするとカレンダーが開くので日時を選択します。タスクの優先順位を選択することもできます。ワークフローの設定時には、緊急や通常などの異なる優先順位の値を追加できることに留意してください。NCM スケジューラでは、この値は参照されません。これは基本的に、どのタスクが承認を必要とするのかを時宜を得た方法で判断するためにユーザに示されるキューです。
Override Approval	タスクにより無効化が許可される場合は、このオプションを選択して承認プロセスを無効化します。
Save as Draft	チェックした場合は、タスクをドラフトとして保存し、後でそこに戻ることができます。ドラフト モードではタスクは実行されません。
スケジューリング オプション	
Retry Count	タスクが失敗した場合、NCM は再試行間隔を考慮して、この回数だけタスクを再実行しようと試みます。次のオプションのいずれかを選択します。 • No Retry（デフォルト） • Once • Twice • Three Times
Retry Interval	再試行するまで何分間待機するのかを入力します。デフォルトは 5 分です。
Recurring Options	Not available

表 5　[Deploy Remote Agent] ページのフィールド

フィールド	説明 / 処理
タスク完了通知	
Task Completed Notification	タスク完了時に、NCM から電子メール メッセージが送信されるようにしたい場合は、[Email Notification] チェックボックスを選択します。 **ヒント**：電子メールの内容の形式は、どのタスクについても同じです。電子メールの内容の変更については、*NCM アドミニストレーション ガイド*を参照してください。
Email Recipients	メッセージを受信する電子メール アドレスのカンマ区切のリストを入力します。デフォルト値は、タスク発信者の電子メール アドレスです。
タスクのロギング	
Task Logging	使用可能な場合は、1 回実行されるようにスケジュールされた特定タスクのロギングを有効化することができます。[Store log output generated by this task] チェックボックスを選択し、Shift キーを使用して 1 つ以上のログを選択します。選択したログは強調表示されます。ロギングありで実行されるようにタスクがセットアップされていても、ログを開始できない場合は、タスクがただちに失敗して追加処理は行われないことに留意してください。

サテライト ホスト上での複数 NIC の取り扱い

サテライト ゲートウェイ ホストに複数のネットワーク インターフェイス カード（NIC）がある場合は、特定の NIC を使用するようにサテライトを設定できます。リモート エージェントをインストールした後に、`/opt/opsware/nassat/jre/nassat.rcx` ファイルを編集して、`tftp/server` の値を、各デバイスがその設定をサテライトへと TFTP するために使用する必要があるゲートウェイ NIC IP アドレスに変更します。

`nassat.rcx` ファイル内の `syslog/server` の値も変更する必要があります。これは、NCM 内で Configure Syslog タスクを実行する際にデバイス上で設定されるロギング アドレスです。

サテライト エージェントを再導入する際には、`nassat.rcx` ファイルを再度変更する必要があります。

サテライトからの SCP 転送の有効化

デフォルトでは、バックアップ デバイス ソフトウェアについて、およびサテライト ゲートウェイを介した設定についてのみ、NCM によって TFTP がサポートされます。リモートから管理されるデバイスからサテライトへの SCP 転送を有効化するには、次の手順を実行します。

1 使用する SCP アカウントを確認します。[Administrative Settings - Device Access page] ページの [FTP and SSH Device Access] セクションに移動します（[Admin] > [Administrative Settings] > [Device Access]）。

- [FTP/SSH User] フィールドと [FTP/SSH Password] フィールドの値を指定した場合は、その情報を SCP アカウントについて使用しなければなりません。
- [FTP/SSH User] フィールドと [FTP/SSH Password] フィールドの値を指定しない場合は、SCP アカウントについて使用するユーザ名とパスワードを決定してください。そのアカウントを設定します。

FTP/SSH ユーザ名は、NCM コンソールにアクセスするための NCM ユーザ名とは異なっていなければなりません。

2 サテライト システムで、確認した SCP アカウントを設定します。たとえば、ユーザ名が `nascp` でパスワードが `napass` のアカウントを設定するには、次のコマンドを使用します。

```
chmod -R o+rx /opt/opsware/nassat/server/ext/tftp
useradd -d /opt/opsware/nassat/server/ext/tftp/tftpdroot nascp
passwd napass
```

このユーザのホーム ディレクトリは `/opt/opsware/nassat/server/ext/tftp/tftpdroot` でなければなりません。

3 NCM アプリケーション サーバ上で、`adjustable_options.rcx` ファイルに `DeviceAccess/scp/allow_satellite` オプションを追加します。

a `adjustable_options.rcx` ファイルのバックアップを、`<NCM_HOME>` ディレクトリ以外の場所に作成します。

b `adjustable_options.rcx` ファイルに、次の行を追加します。

```
<option name="DeviceAccess/scp/allow_satellite">true</option>
```

c `adjustable_options.rcx` ファイルを保存します。

d 次のいずれかを実行して .rcx 設定をリロードします。

— NCM プロキシから `reload server options` コマンドを実行します。

— NCM サービスを再起動します

サテライト ゲートウェイホストからのリモート エージェントの削除

サテライト ゲートウェイをアンインストールする前にリモート エージェントを削除しなければなりません。ゲートウェイからリモート エージェントを削除するには、次の手順を実行します。

1. NCM にログインします。
2. メニューバーで、[Tasks] > [New Task] > [Deploy Remote Agent] の順にクリックします。[Deploy Remote Agent] ページが開きます。([Gateway List] ページの [Deploy Remote Agent link] をクリックしてこのページに移動することもできます)
3. [Actions] フィールドの [Task Options] の下で、[Uninstall] をクリックします。
4. [Save Task] をクリックします。

ゲートウェイのアンインストール

ゲートウェイをアンインストールするには、次の手順を実行します。

1. ゲートウェイをインストールするために `gateway.zip` ファイルを解凍したディレクトリに変更します。
2. 次のコマンドを入力します。

```
./saOPSWgw*/uninstall --removeall
```

`--removeall` オプションを指定しない場合、一部の設定とログファイルは削除されません。

NCM サテライトの削除

NCM サテライトを削除するには、次の手順を実行します。

1. 「サテライト ゲートウェイホストからのリモート エージェントの削除」(P.22) の記載に従ってサテライト ゲートウェイ ホストからリモート エージェントを削除します。
2. 「ゲートウェイのアンインストール」(P.22) の記載に従ってゲートウェイをアンインストールします。

サテライトのアップグレード

サテライトを NCM 1.4x から NCM 1.8 にアップグレードするには、次の手順を実行します。

1. 「サテライト ゲートウェイホストからのリモート エージェントの削除」（P.22）の記載に従ってゲートウェイ メッシュ内の古いゲートウェイをすべてアンインストールします。
2. 「コア ゲートウェイのインストール」（P.12）の記載に従って NCM 1.4 ゲートウェイ インストーラを使用して新しいゲートウェイを再インストールします。これにより、NCM 1.4 についてゲートウェイのセキュリティが正しくセットアップされることが保証されます。
3. 「サテライト ゲートウェイ ホストへのリモート エージェントの追加」（P.17）の記載に従って各サテライト ゲートウェイ用の Deploy Remote Agent タスクを実行します。

NCM 1.5x、NCM 1.6x、または NCM 1.7x から NCM 1.8 へとアップグレードするには、次の手順を実行します。

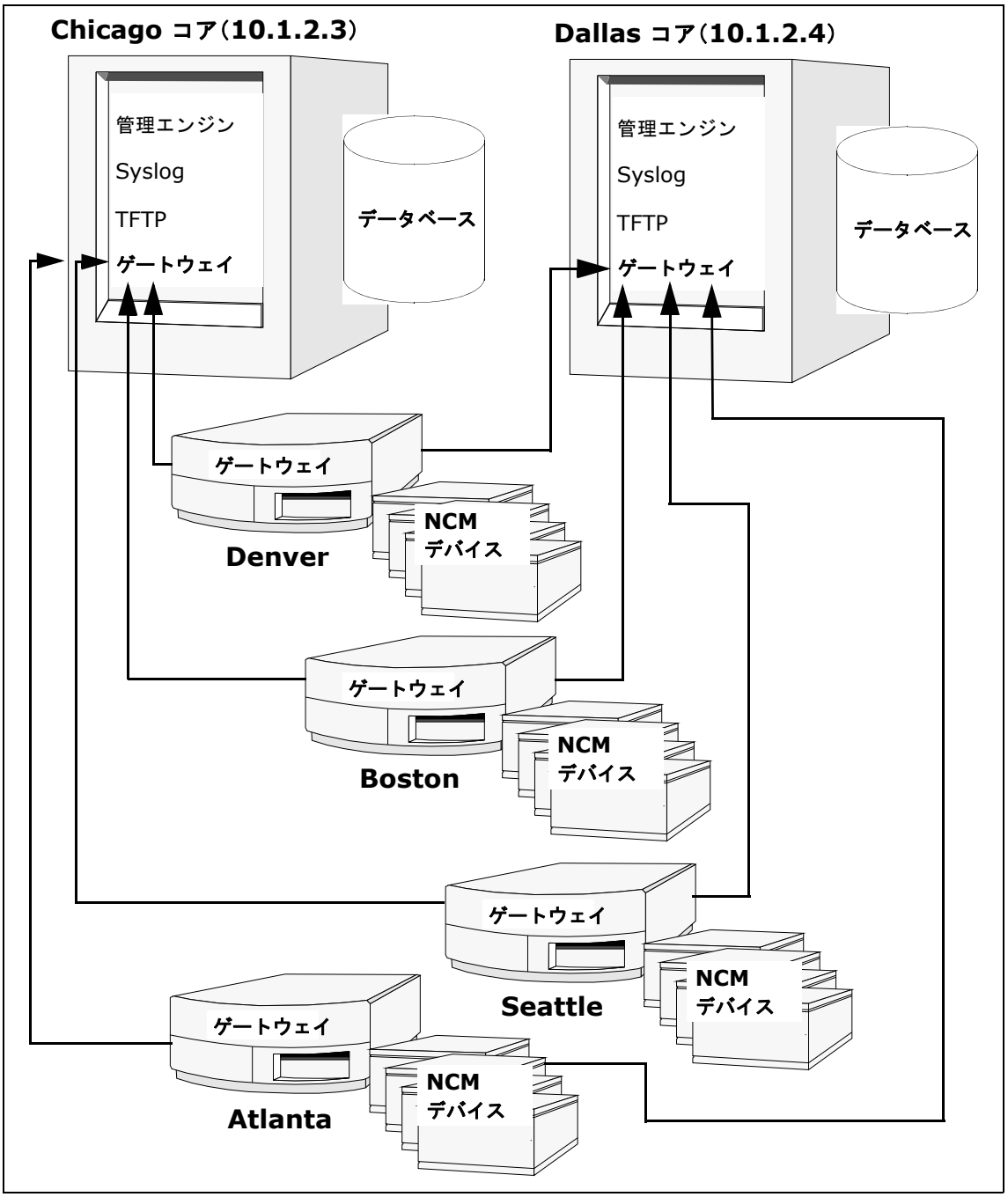
1. ゲートウェイを使用している場所で、NCM アプリケーション サーバ上の NCM をアップグレードした後で、「Deploy Remote Agent」タスクを実行して、すべてのリモート ゲートウェイ上でアップグレードしたサテライト エージェントを再インストールします。「サテライト ゲートウェイ ホストへのリモート エージェントの追加」（P.17）を参照してください。
2. [Deploy Remote Agent] ページで、[Task Options] セクションまで下にスクロールします。
3. [Action] フィールドで、[Install]（または [Reinstall]）オプションを選択します。
4. [Save Task] をクリックします。

A インストール例

以下の例では、大きな 2 つのオフィス（NCM コア）が、Chicago と Dallas に 1 つずつあります。それより小さなオフィスが Boston、Atlanta、Seattle、Denver にあります（レルム）。サテライト構成をセットアップする 1 つの方法を次に示します。

- 都市ごとにレルムを 1 つ置く。
- NCM コアを Chicago と Dallas に置く。
- サテライト ゲートウェイを Boston、Atlanta、Seattle、Denver に置く。

以下の図に例を示します。NCM コアには NCM アプリケーション サーバとデータベース サーバの両方が含まれますが、一般には別々のホスト上に置かれることに留意してください。コア レルムは NCM アプリケーション サーバと同じホスト上のコア ゲートウェイを表します。リモート レルムは、独立したホスト上のサテライト ゲートウェイを表します。各サテライト ゲートウェイには、コア ゲートウェイとつながるトンネルが 1 つずつ、合計 2 つあります。



Solaris プラットフォーム上に 2 つの NCM コアがインストールされているものとします。

1 まず Chicago ゲートウェイをインストールします。

   a 第一ゲートウェイ：**y**

   b コア ゲートウェイ：**y**

   c ゲートウェイ名：**Chicago1**

   d レルム名：**Chicago**

e NCM コアの IP アドレス：**127.0.0.1**

ループバック インターフェイスを使用して NCM コア間のトラフィックがイーサネット セグメントへと出ないようにしています。したがって、接続はさらに安全となります。

f 接続するもう一方のゲートウェイの IP アドレス：**10.1.2.3**

これは、もう一方のゲートウェイがこのゲートウェイと接続できるようにするための外部 IP アドレスでなければなりません。10.1.2.3 は一例です。ホストの正確な IP アドレスを使用してください。

2 Dallas コアをインストールします。

a 第一ゲートウェイ：**n**

b コア ゲートウェイ：**y**

c ゲートウェイ名：**Dallas1**

d レルム名：**Dallas**

e NCM コアの IP アドレス：**127.0.0.1**

f 接続するもう一方のゲートウェイの IP アドレス：**10.1.2.4**

第二コア ゲートウェイが機能するようにするために、ゲートウェイ プロパティ ファイル / etc/opt/opsware/opswgw-<gateway name>/opswgw-properties を修正し、opswgw.EgressFilter の値を次のように変更します。

```
opswgw.EgressFilter=tcp:*:443:127.0.0.1:*,tcp:*:22:NAS:,tcp:*:23:NAS:,tcp:*:
513:NAS:,tcp:*:443:NAS:,tcp:*:80:NAS:
```

3 サテライト ゲートウェイをインストールします。Boston の場合。

a 第一ゲートウェイ：**n**

b コア ゲートウェイ：**n**

c ゲートウェイ名：**Boston1**

d レルム名：**Boston**

e コア ゲートウェイの IP アドレス：**10.1.2.3**

4 Boston1 で opswgw.properties ファイルを編集します。opswgw.properties ファイルを次のようにする必要があります。

```
opswgw.TunnelSrc=10.1.2.3:2001:100:0:/var/opt/opsware/crypto/opswgw-Boston1/
opswgw.pem
opswgw.TunnelSrc=10.1.2.4:2001:200:0:/var/opt/opsware/crypto/opswgw-Boston1/
opswgw.pem
```

5 同様にして他のサテライト ゲートウェイをインストールします。

6 冗長化のために、Boston に第二ゲートウェイをインストールします。

a 第一ゲートウェイ：**n**

b コア ゲートウェイ：**n**

c ゲートウェイ名：**Boston2**

d レルム名：**Boston**

e コア ゲートウェイの IP アドレス：**10.1.2.3**

7 Boston のオフィスとの間には T1 リンクしかなく、NCM によりそのリンクが独占されるのが望ましくないとします。T1 リンクは約 1.5Mbit/s であるため、NCM をその半分（つまり 750Kbit/s）に制限します。opswgw.properties ファイルを編集して帯域幅スロットルを 750 に設定します。opswgw.properties ファイルは次のようになるはずです。

```
opswgw.TunnelSrc=10.1.2.3:2001:100:750:/var/opt/opsware/crypto/opswgw-Boston1/
opswgw.pem
opswgw.TunnelSrc=10.1.2.4:2001:200:750:/var/opt/opsware/crypto/opswgw-Boston1/
opswgw.pem
```

両方のトンネルの帯域幅スロットルを設定し、Dallas（10.1.2.4）にフェールオーバーする場合でも帯域幅がスロットルされるようにします。

B トラブルシューティング

NCM サテライトには、不正なプロセスがサテライトにアクセスできないようにするために 2 つのレベルのセキュリティがあります。通常は、それらのセキュリティ チェックによる接続拒否を引き起こした設定エラーの結果として NCM サテライトの障害が発生します。以下のセクションでは、NCM サテライトの稼働が失敗した場合にセキュリティのレベルをチェックする方法について説明します。

ゲートウェイ メッシュのセキュリティ

最初のセキュリティ レベルは、ゲートウェイ メッシュでのセキュリティ レベルです。NCM コア ホストのみが、コア ゲートウェイとの接続を許可されます。コア ゲートウェイのインストール時に正しくない NCM コアの IP アドレスが使用された場合、接続は失敗します。

ゲートウェイ メッシュのセキュリティによって接続が拒否されているかどうかをチェックするには、コア ゲートウェイ ホストのシェル プロンプトで以下のコマンドを実行して、コア ゲートウェイ ログ ファイルの中で「disallow」という単語を探します。

```
grep disallow /var/log/opsware/opswgw-*/opswgw.log
```

特定 IP アドレスからの接続を禁止することを記述した行がある場合は、コア ゲートウェイでのセキュリティが問題です。解決策は、ローカル ゲートウェイの NCM 管理設定とゲートウェイ IngressMap が同期していることを確認することです。

コア ゲートウェイが NCM コアと同じホスト上にある場合、IngressMap 内の IP アドレスは 127.0.0.1 である必要があります。ローカル ゲートウェイ管理設定は、ローカル ホストまたは 127.0.0.1 である必要があります。

コア ゲートウェイが別個のホスト上にある場合は、ローカル ゲートウェイ管理設定にコア ゲートウェイの正しい IP アドレスがなければなりません。IngressMap には NCM コア ホストの正しい IP アドレスがなければなりません。

`properties` ファイルで IngressMap の行を変更するには、`/etc/opt/opswgw-*/opswgw.properties` ファイルを編集します。複数のゲートウェイがインストールされている場合は、アスタリスク（*）をゲートウェイの名前と置き換えます。次のような IngressMap の行を探します。

```
opswgw.IngressMap=127.0.0.1:NCM
```

NCM コアおよびサテライトでのセキュリティ

2 番目のセキュリティ レベルは、NCM コアと NCM サテライトでのセキュリティ レベルです。これらは、既知のホストからの接続のみを受け入れます。

NCM コアでは、既知のホストはローカル ゲートウェイ管理設定に含まれています。サテライトでは、既知のホストは常にローカル ホストです。これをチェックするには、NCM コア jboss wrapper ログで、「Rejected」を探します。次のように入力します。

```
grep Rejected $NCM/server/log/jboss_wrapper.log
```

（ここで $NCM は NCM コアのインストール先のルートです）。

誤った NCM コア ホストのホスト名を使用して Deploy Remote Agent タスクが実行された場合、サテライトは NCM コアに再接続することができなくなります。これをチェックするには、上記の「grep」コマンドを NCM サテライト ホストに入力します。詳細については、「サテライト ゲートウェイホストからのリモート エージェントの削除」（P.22）を参照してください。

さらに、コア ゲートウェイ上の EgressFilter で NCM サテライトの IP アドレスが正しいかどうかをチェックします。そのために、サテライト ホスト上でゲートウェイの *properties* ファイルを編集します。次のような行を探します。

```
opswgw.EgressFilter=tcp:*:443:XXX.XXX.XXX.XXX:*,tcp:*:22:NCM:,tcp:*:23:NCM:,tcp:
*:513:NCM:
```

（ここで XXX.XXX.XXX.XXX は 127.0.0.1）。

ゲートウェイ インストーラでは、冗長コア ゲートウェイはサポートされません。しかし、冗長コア ゲートウェイを使用したい場合（推奨されません）には、adjustable_options.rcx ファイルを編集し、以下の行をファイルに追加することにより、他のコア ゲートウェイ IP アドレスを追加します。

```
<array name="rpc/allowed_ips">
<value>10.255.52.10</value>
<value>10.255.54.22</value>
</array>
```

上記の IP アドレスを、NCM コア ゲートウェイの正しい IP アドレスと置き換える必要があります。

C　ゲートウェイ メッシュの共有

この付録には、CiscoWorks Network Compliance Manager Network Automation（NCM）と HP Server Automation（SA）が同じゲートウェイ メッシュを共有するようにセットアップする方法に関する情報が含まれています。

概要

ゲートウェイ メッシュを共有する際には、以下のことに留意してください。

- NCM は SA によりインストールされたゲートウェイ メッシュのみを使用できます。
- NCM コアが NCM ホストを識別するために使用する SA コア ゲートウェイを、ゲートウェイ メッシュに変更できます。
- SA サテライトを変更して、NCM がデバイスを管理するために使用するポートへの出力を有効化できます。

インストールの手順

各 NCM コアについて、その NCM コアにより使用される SA コア ゲートウェイを識別します。

1. SA ホスト上で、`/etc/opt/opsware/opswgw-cgws`*N*-*core*`/opswgw.custom` ファイルを編集（または作成）します。*N* はコア番号、*core* はコア名です（例：`/etc/opt/opsware/opswgw-cgws1-VMCORE1/opswgw.custom`）。
2. ファイルの末尾に次の行を追加します。
   ```
   opswgw.EgressFilter=tcp:*:443:127.0.0.1:*
   opswgw.IngressMap=192.168.99.1:NCM
   ```
3. `192.168.99.1` を、NCM コアの正しい IP アドレスに変更します。`cgw` がコア ゲートウェイの略であることに注意してください。複数の cgw スライスがある場合は、それらすべてに NCM の IngressMap を追加します。NCM は cgw を 1 つのみ使用できますが、将来のバージョンでは他のスライスにフェールオーバーできるようになる可能性があります。
4. コア ゲートウェイを再起動します。
   ```
   /etc/init.d/opswgw-sas restart opswgw-cgws
   ```

   同じ SA コア ゲートウェイを使用している NCM が 1 つ以上ある場合には、NCM コアの IP アドレスごとに 1 行ずつ、複数の行を各ファイルに追加します。

NCM により使用される各サテライト ゲートウェイの場合。

1. `/etc/opt/opsware/opswgw-`*gateway*`/opswgw.properties` ファイルを編集します（*gateway* は SA サテライトのインストール時に指定したゲートウェイの名前）。

2 次の行を追加します。

```
opswgw.EgressFilter=tcp:*:22:NCM:,tcp:*:23:NCM:,tcp:*:513:NCM:,tcp:*:80:
NCM:,tcp:*:443:NCM:
opswgw.EgressFilter=tcp:127.0.0.1:8443:NCM:
opswgw.ProxyPort=3002
```

最初の行により、各種のデバイスを管理するために必要なすべてのポート（SSH、Telnet、rlogin、http、https）を NCM が使用できるようになることに注意してください。2 行目により、NCM コアはポート 8443 上で RPC コールをリッスンする NCM リモート エージェントと通信できるようになります。3 行目により、NCM が予期する ProxyPort と一致する 2 番目の ProxyPort が追加されます（3002）。

3 サテライト ゲートウェイを再起動します。

```
/etc/init.d/opswgw-sas restart opswgw
```

4 SA ホスト上の `/var/opt/opsware/crypto/twist/spog.pkcs8` から NCM ホスト上の *`NCMRoot`*`/spog.pkcs8` に `spog.pkcs8` ファイルをコピーします（*`NCMRoot`* は NCM をインストールしたディレクトリ）。

5 [Gateway Mesh] セクションの [Device Access] タブを使用して、NCM の [Admin Settings] ページにある SA コア ゲートウェイが NCM により使用されるように設定します。詳細については、『*User Guide for CiscoWorks Network Compliance Manager 1.8*』を参照してください。

ローカル ゲートウェイ ホスト：SAS（コア ゲートウェイ）ホストの IP アドレス
ローカル ゲートウェイ プロキシ ポート：3002
ローカル ゲートウェイ管理ポート：8085
ゲートウェイ管理秘密キー ファイル名：spog.pkcs8

6 NCM で各サテライト ゲートウェイ ホストについて Deploy Remote Agent タスクを実行します。SA サテライトにより OS Provisioning Media Server が実行されている場合は、OS Provisioning Media Server により使用される TFTP サーバを使用するように、そのホスト上の NCM リモート エージェントを再設定しなければなりません。

7 `/opt/opsware/nassat/nassat.rcx` ファイルを編集し、`TFTP/Server` の値を `/opt/opsware/boot/tftpboot`（OS Provisioning Media Server により使用される TFTP ルート ディレクトリへのパス）に変更します。

8 `/etc/xinetd.d/tftp` ファイルを編集して、`server_args = -s /tftpboot`
を、`server_args = -c -s /tftpboot`
と変更します。
`-c` フラグを使用すると、NCM はネットワーク デバイス設定をキャプチャするために必要な TFTP ルート ディレクトリ内にファイルを作成できるようになります。SA は TFTP を使用してファイルをサーバにエクスポートします。したがって、SA には作成能力が必要ありません。

9 `/opt/opsware/boot/tftpboot` ディレクトリが、`/etc/xinetd.d/tftp` ファイルで指定されているのと同じユーザにより所有されていることを確認してください。

10 xinetd プロセスに HANGUP 信号を送信することにより、TFTP デーモン（in.tftpd）を再起動します。

```
kill -1 `ps ax | grep xinetd | grep -v grep | awk '{print $1}'`
```

11 `/etc/init.d/nassat` ファイルを編集し、StartTFTP の行をコメント アウトするために、行の前にポンド記号（#）を挿入します。例を次に示します。

```
#  StartTFTP
```

12 NCM エージェントを再起動します。

```
/etc/init.d/nassat restart
```

ゲートウェイ メッシュのアンインストール

ゲートウェイ メッシュをアンインストールするには、次の手順を実行します。

1 NCM で「uninstall」オプション ボタンを選択した状態で、Deploy Remote Agent タスクを実行します。サテライト ゲートウェイ ホストごとに、このタスクを 1 回ずつ実行します。

2 NCM により使用される各サテライト ゲートウェイの場合。

   a /etc/opt/opsware/opswgw-*gateway*/opswgw.properties ファイルを編集します（*gateway* は SA サテライトのインストール時に指定したゲートウェイの名前）。

   b ファイルから次の行を削除します。

```
opswgw.EgressFilter=tcp:*:22:NCM:,tcp:*:23:NCM:,tcp:*:513:NCM:,tcp:*:80:N
CM:,tcp:*:443:NCM:
opswgw.EgressFilter=tcp:127.0.0.1:8443:NCM:
```

3 サテライト ゲートウェイを再起動します。

```
/etc/init.d/opswgw-sas restart opswgw
```

4 [Gateway Mesh] セクションの [Device Access] タブで、NCM の [Admin Settings] ページ内のゲートウェイが NCM により使用されないように設定します。詳細については、『*User Guide for CiscoWorks Network Compliance Manager 1.8*』を参照してください。

5 [Local Gateway Host] オプションに空の文字列を設定します。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/