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 フォワーディンク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.r*p 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