Oracle® Solaris 11.2 でのネットワーク配備の計画

Part No: E53781
2014 年 7 月

ORACLE

Copyright © 2011, 2014, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション（人的傷害を発生させる可能性があるアプリケーションを含む）への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性（redundancy）、その他の対策を講じることは使用者の責任となります。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、オラクル社およびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはOracle Corporationおよびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

目次

このドキュメントの使用

- **概要** – IPv4 および IPv6 ネットワークの配備計画を支援するための基本的なトピックとタスクについて記述しています。
- **対象読者** – システム管理者。
- **前提知識** – ネットワーク管理の概念と実践に関する基本的な理解。

製品ドキュメントライブラリ

この製品の最新情報や既知の問題は、ドキュメントライブラリ (http://www.oracle.com/pls/topic/lookup?ctx=E56342) に含まれています。

Oracle サポートへのアクセス

Oracle のお客様は、My Oracle Support を通じて電子的なサポートを利用することができます。詳細は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info を参照してください。聴覚に障害をお持ちの場合は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs を参照してください。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお聞かせください。

♦ ♦ ♦ 第 1 章

1 ネットワーク配備の計画

この章では、TCP/IP ネットワークの配備を計画するときのさまざまな考慮点について説明します。説明する計画タスクは、系統的なコスト効率の高い方法でネットワークを配備することを支援します。ネットワーク計画の詳細はこのドキュメントの範囲外です。一般的な指示のみが提供されます。このドキュメントでは、ネットワークの基本的な概念と用語について習熟していることを前提にしています。

Oracle Solaris での TCP/IP の実装方法の説明およびこのリリースでのネットワーク管理の概要については、『Oracle Solaris 11.2 でのネットワークコンポーネントの構成と管理 』の第 1 章「Oracle Solaris でのネットワーク管理について」を参照してください。

サイト全体のネットワークスキームの計画については、『Oracle Solaris 11.2 でのネットワーク管理の計画 』の第 1 章「Oracle Solaris ネットワーク管理のサマリー」で説明しているネットワーク構築戦略を参照してください。

この章の内容は、次のとおりです。

ネットワークハードウェアの決定

サポートする予定のシステムの数は、ネットワークの構成方法に影響を与えます。組織によっては、1 つの階または 1 つのビルの中にある数十台のスタンドアロンシステムから成る小さい

ネットワークが必要な場合もあります。また、複数のビルに散在する 1000 以上のシステムを持つネットワークの設定が必要な場合もあります。このような大きい設定の場合は、ネットワークを「*サブネット*」と呼ばれる小区分に分割することが必要になる場合もあります。

ハードウェアに関して下す必要のある計画上の決定のいくつかを、次に示します。

- ネットワークトポロジ、ネットワークハードウェアのレイアウトと接続
- ネットワークでサポート可能なホストシステムのタイプと数 (サーバーで必要になる可能性のある仮想システムも含む)
- それらのシステムに装着するネットワークデバイス
- Ethernet など、使用するネットワークメディアのタイプ
- ネットワークメディアの拡張またはローカルネットワークの外部ネットワークへの接続におけるブリッジ、ルーター、およびファイアウォールの使用

  ブリッジの動作の詳細は、『Oracle Solaris 11.2 でのネットワークデータリンクの管理 』の「ブリッジネットワークの概要」を参照してください。

  ルーターがどのように機能するかについては、13 ページの「ネットワーク上でのルーターの計画」を参照してください。

  ファイアウォールの詳細については、『Oracle Solaris 11.2 でのネットワークのセキュリティー保護 』の第 4 章「Oracle Solaris の IP フィルタについて」を参照してください。

ネットワークトポロジの概要

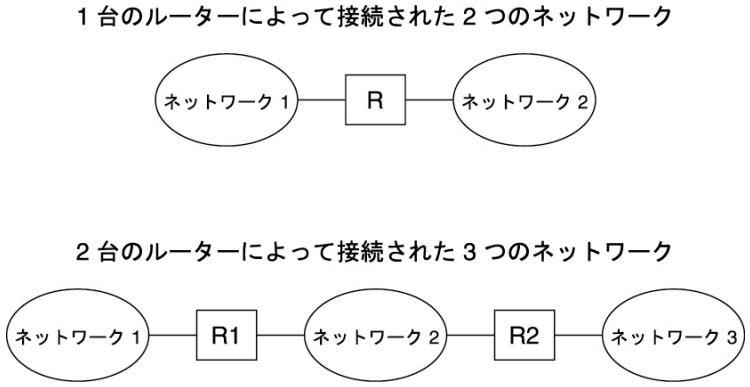
ネットワークトポロジは、ネットワークの組み合わせ方を定義します。ルーターは、ネットワークを相互に接続するエンティティーです。ルーターは、複数のネットワークインタフェースを持ち、IP 転送を実行するマシンです。しかし、適切に構成しないとシステムはルーターとして機能できません (『ルーターまたはロードバランサとしての Oracle Solaris 11.2 システムの構成 』の第 2 章「ルーターとしてのシステムの構成」を参照)。

ルーターは、複数のネットワークを接続して、より大きなインターネットワークを形成します。ルーターは、隣接する 2 つのネットワーク間でパケットの受け渡しをするように構成する必要があります。さらに、隣接するネットワークに接続されたルーターにパケットを転送することで、隣接するネットワークを越えた位置にあるネットワークに、パケットを渡す機能も備えている必要があります。

次の図に、ネットワークトポロジの基本部分を示します。図の上部は、2 つのネットワークを 1 台のルーターで接続した単純な構成を示しています。図の下部は、3 つのネットワークを 2 台のルーターで相互接続した構成を示しています。最初の例では、ルーター R がネットワーク 1 と

ネットワーク 2 を連結して、より大きなインターネットワークを作っています。2 番目の例では、ルーター R1 はネットワーク 1 と 2 に接続し、ルーター R2 は、ネットワーク 2 と 3 に接続しています。この接続で、ネットワーク 1、2、3 を含むネットワークが形成されます。

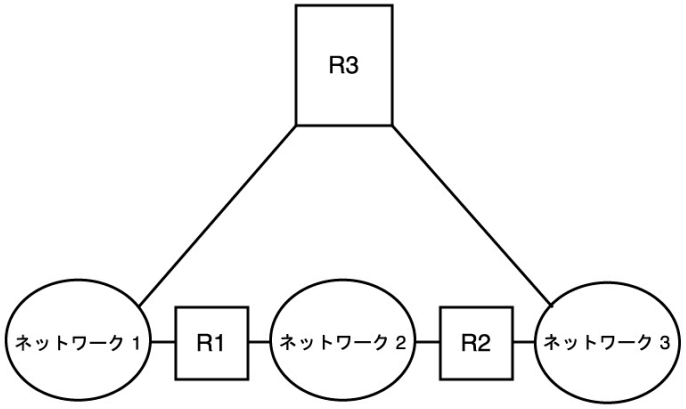
図 1-1 基本的なネットワークトポロジ



ネットワークをインターネットワークに結合したあと、ルーターは、宛先ネットワークのアドレスを基にネットワーク間でパケットの経路制御を行います。インターネットワークがより複雑になるにつれて、ルーターがパケットの宛先を決定する回数は増加します。

次の図に、より複雑な例を示します。ルーター R3 は、ネットワーク 1 と 3 に直接接続されており、この冗長性によって信頼性が向上します。ネットワーク 2 が停止しても、ルーター R3 は、ネットワーク 1 と 3 の間にルートを提供できます。 多くのネットワークを相互接続することが可能です。ただし、相互接続するネットワークは、同じネットワークプロトコルを使う必要があります。

図 1-2 ネットワーク間に追加パスを提供するネットワークトポロジ



ルーターについては、13 ページの「ネットワーク上でのルーターの計画」で詳細に説明しています。

ネットワーク上のサブネットの使用

サブネットの使用は、サイズや制御の問題を解決するための管理区分の必要性と関係しています。ネットワーク上のホストとサーバーの数が増えるに従って、管理タスクはますます複雑になります。管理区分を作成しサブネットを使用することで、複雑なネットワークを容易に管理できるようになります。

ネットワーク管理の作業を分化するかどうかは、次の要因によって判断します。

- **ネットワークのサイズ**

  サブネットは、区分の場所が地理的に広範囲に分散している比較的小規模なネットワークでも役立ちます。

- **ユーザーのグループが共有する共通のニーズ**

  たとえば、単一の建物内のみに制限された、比較的少数のマシンをサポートするネットワークがあるとします。これらのマシンはいくつかのサブネットワークに分割されています。各サ

ブネットワークは、異なるニーズを持つユーザーのグループをサポートします。このような場合は、サブネットごとに管理部門を設立するとよいでしょう。

- **セキュリティー**

  ミッションクリティカルなサーバー、デスクトップシステム、インターネットに直接接続された Web サーバーを個別のサブネットに分割し、各サブネット間にファイアウォールを設置したほうがよい場合があります。

IPv4 自律システムのトポロジ

複数のルーターとネットワークを持つサイトでは、通常そのネットワークトポロジは単一のルーティングドメイン、つまり*自律システム* (AS) として管理されます。図1-3「複数の IPv4 ルーターを備えた自律システム」は、3 つのローカルネットワーク `10.0.5.0`、`172.20.1.0`、および `192.168.5.0` に分割された AS を示しています。

ネットワークは次の種類のシステムで構成されています。

- ルーター

  ルーターはルーティングプロトコルを使用して、ローカルネットワーク内で、または外部ネットワークに対して、ネットワークパケットを発信元から着信先に伝送またはルーティングする方法を管理します。Oracle Solaris でサポートされているルーティングプロトコル、およびシステムをルーターとして構成する方法の詳細については、『ルーターまたはロードバランサとしての Oracle Solaris 11.2 システムの構成 』の「ルーティングプロトコル」を参照してください。

  ルーターのタイプには次のものがあります。

  - ボーダールーターは、`10.0.5.0` などのローカルネットワークを外部のサービスプロバイダに接続します。
  - デフォルトルーターは、ローカルネットワーク内のパケットルーティングを管理し、それ自体にいくつかのローカルネットワークを含めることができます。たとえば、図1-3「複数の IPv4 ルーターを備えた自律システム」では、ルーター 1 は `192.168.5` のデフォルトルーターとして機能します。同時に、ルーター 1 は `10.0.5.0` の内部ネットワークにも接続されています。ルーター 2 のインタフェースは `10.0.5.0` および `172.20.1.0` の内部ネットワークに接続しています。
  - パケット転送ルーターは、内部ネットワーク間でパケットを転送しますが、ルーティングプロトコルは実行しません。図1-3「複数の IPv4 ルーターを備えた自律システム」で、ルー

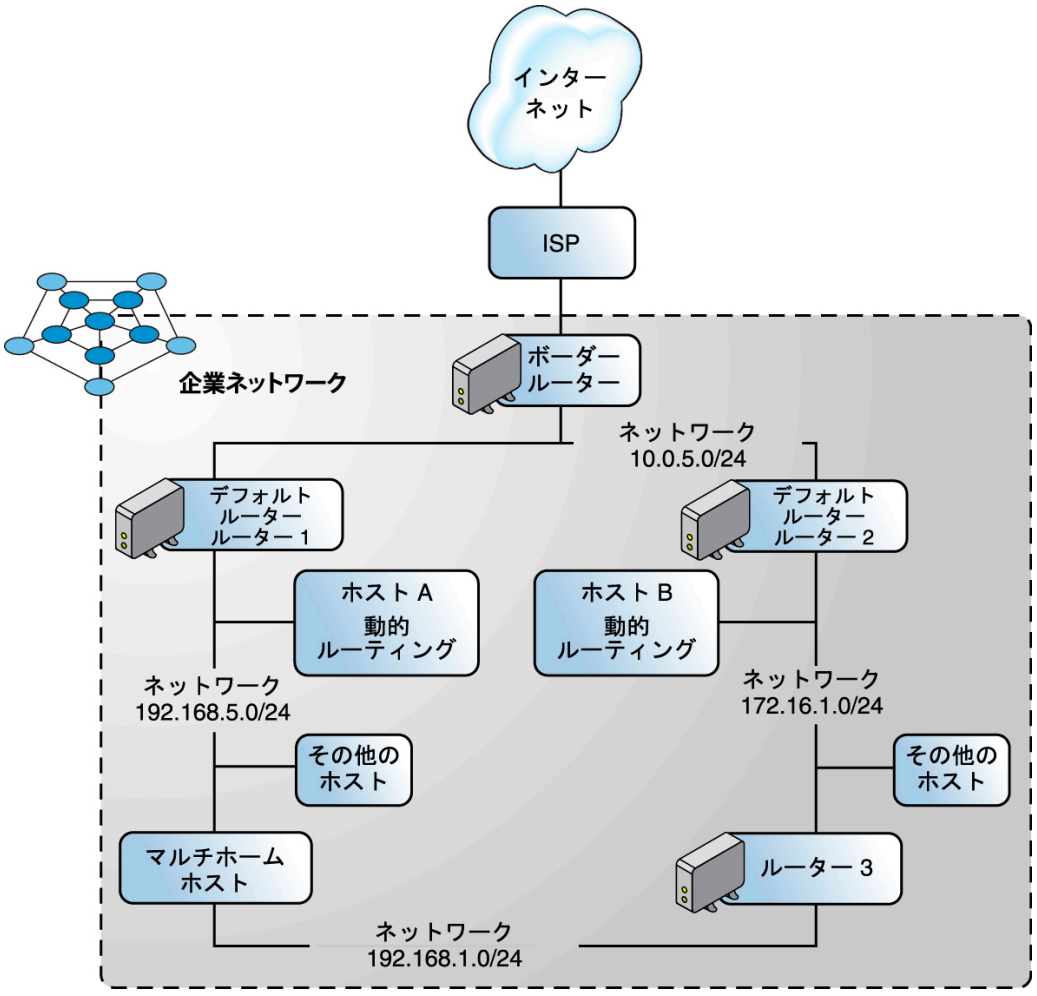
ター 3 はパケット転送ルーターで、172.20.1 および 192.168.5 ネットワークに接続されています。

- クライアントシステム
  - マルチホームシステム、つまり複数の NIC を持つシステム。Oracle Solaris では、これらのシステムは、デフォルトで、同じネットワークセグメント内の別のシステムに対してパケットを転送できます。
  - 単一インタフェースシステムでは、パケットの転送と受信の両方の構成情報をローカルルーターに依存しています。

タスク関連の詳細については、『Oracle Solaris 11.2 でのネットワークコンポーネントの構成と管理 』の第 3 章「Oracle Solaris での IP インタフェースとアドレスの構成および管理」を参照してください。

追加のネットワークコンポーネントを構成する場合は次の図を参照として使用してください。

図 1-3 複数の IPv4 ルーターを備えた自律システム



ネットワーク上でのルーターの計画

TCP/IP では、ネットワークに 2 種類のエンティティーがあります。つまりホストとルーターです。ホストはすべてのネットワークに必要ですが、ルーターはすべてのネットワークに必要なわけではありません。ネットワークの物理的なトポロジによってルーターを使用する必要があるかどうかが

決まります。このセクションでは、ネットワークトポロジとルーティングの概念を紹介します。これらの概念は、既存のネットワーク環境に別のネットワークを追加すると決めた場合に重要になります。

注記 - IPv4 および IPv6 ネットワークでのルーター構成における詳細とタスクについては、『ルーターまたはロードバランサとしての Oracle Solaris 11.2 システムの構成 』の第 2 章「ルーターとしてのシステムの構成」を参照してください。

ルーターがどのようにパケットを転送するか

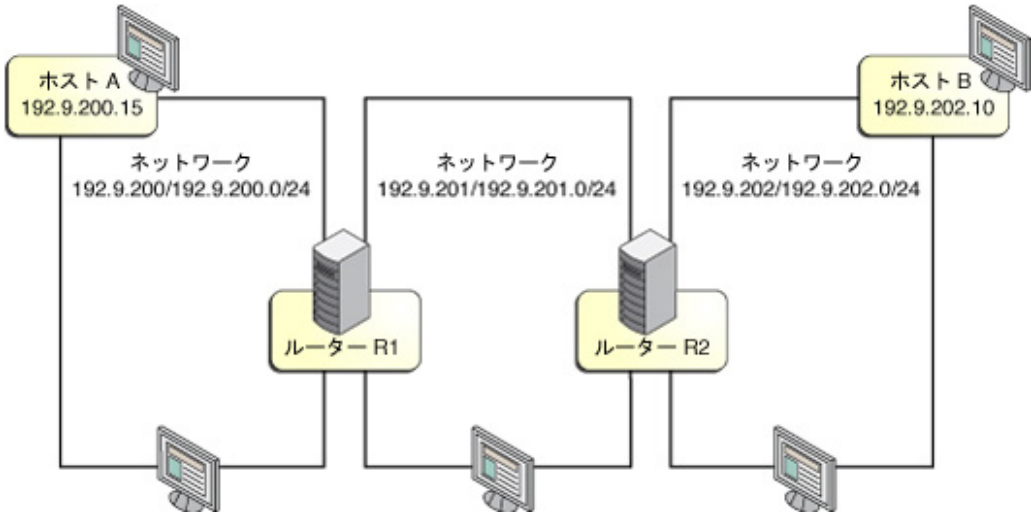
ルーターは次のようにしてパケットを転送します。

- IP ネットワーク上のすべてのノードはルーティングテーブル内にルーティング情報を保持しています。これらのテーブルには、ローカルネットワークとリモートネットワークの両方に接続されているシステムに到達する方法についての情報が格納されています。ルーティングテーブルは、ローカルの構成情報および隣接するシステムと交換されるルーティングプロトコルメッセージから生成されます。
- ホストシステムは最初にパケットを送信するとき、ルーティングテーブル内のパケットの宛先アドレスを参照して、その宛先がローカルネットワーク上に存在するかどうかを決定します。ローカルネットワーク上に存在する場合、パケットは、その IP アドレスを持つホストに直接送信されます。ローカルネットワーク上に存在しない場合、パケットは、ローカルネットワーク上のルーターに送信されます。
- ルーターは、パケットを受信すると、自分のルーティングテーブルをチェックして、宛先アドレスが自分に接続されているいずれかのネットワーク上のシステムのものか、あるいは別のルーターを介してメッセージを転送する必要があるのかを判断します。次に、メッセージを宛先までのパス上にある次のシステムに送信します。
- このプロセスは、メッセージが宛先システムに到達するまで、メッセージを受信する各ルーターで繰り返されます。

『ルーターまたはロードバランサとしての Oracle Solaris 11.2 システムの構成 』の第 2 章「ルーターとしてのシステムの構成」を参照してください。

次の図は、2 つのルーターにより接続された 3 つのネットワークのネットワークトポロジを示します。

図 1-4 3 つの相互接続ネットワークを持つネットワークトポロジ



ルーター R1 は、ネットワーク 192.9.200.0/24 とネットワーク 192.9.201.0/24 を接続しています。ルーター R2 は、ネットワーク 192.9.201.0/24 とネットワーク 192.9.202.0/24 を接続しています。

ネットワーク 192.9.200.0/24 のホスト A がネットワーク 192.9.202 のホスト B にメッセージを送る場合、次のイベントが発生します。

1. ホスト A は自分のルーティングテーブルを調べて、192.9.202.10 へのパスが存在するかどうかチェックします。ローカルネットワークアドレスの範囲にこのアドレスは含まれませんが、ルーター R1 経由で以前に学習したデフォルト経路にこのアドレスが含まれています。したがって、ホスト A はルーター R1 にパケットを送信します。
2. ルーター R1 は自己のルーティングテーブルを調べます。ローカルネットワークアドレスの範囲にこの宛先アドレスは含まれませんが、ルーター R2 経由のネットワーク 192.9.202.0/24 への既知の経路にはこのアドレスが含まれているため、ルーター R1 はルーター R2 にパケットを送信します。
3. ルーター R2 はネットワーク 192.9.202.0/24 に直接接続されています。ルーティングテーブルを検索すると、接続されているネットワーク上に 192.9.202.10 が存在することが判明します。ルーター R2 は、ホスト B に直接パケットを送信します。

ネットワークの IP アドレス指定形式の決定

ネットワークのアドレス指定スキームを計画するときには、次の要因を考慮してください。

- 使用する IP アドレスの種類 (IPv4 または IPv6)
- ネットワーク上の潜在的なシステムの数
- それぞれ個別の IP アドレスを持つ複数のネットワークインタフェースカード (NIC) を必要とする、マルチホームシステムまたはルーターの数
- ネットワークでプライベートアドレスを使用するかどうか
- IP アドレスのプールを管理する DHCP サーバーを使用するかどうか

IPv4 アドレス

これは、TCP/IP ネットワークで使用される元の IP アドレス形式です。IPv4 のアドレス長は 32 ビットです。IPv4 アドレスは当初、16777216 個 (クラス A)、65536 個 (クラス B)、256 個 (クラス C) の連続するアドレスのブロックとして、さまざまな組織に割り当てられました。アドレスブロックを要求した各組織は、固定のアドレス接頭辞と暗黙の接頭辞マスク (どちらも 10 進ドット表記で指定) を受け取ります。たとえば、Internet Assigned Numbers Authority (IANA) は、クラス A アドレスブロック `156.0.0.0` とネットマスク `255.0.0.0` を American Registry for Internet Numbers (ARIN) に割り当てました。先頭バイトが 156 のすべてのアドレスが、このアドレスブロックに含まれます。ARIN は、自分のクラス A ブロックからクラス B アドレスブロック `156.151.0.0` ネットマスク `255.255.0.0` を Sun Microsystems (現在の Oracle) に分割して割り当てました。

その後、Internet Engineering Task Force (IETF) は、IPv4 アドレスの不足や世界的なインターネットルーティングテーブルの容量不足に対する臨時的な対応策として、*クラスレスドメイン間ルーティング (CIDR)* アドレスを開発しました。CIDR では、組織の要件にもっとも適合する任意のビット境界で、アドレス割り当てが分割されます。アドレスブロックは、10 進ドット IPv4 アドレスの後に続くスラッシュとアドレス接頭辞のビット長として指定されます。

詳細は、次のリソースを参照してください。

- インターネットプロトコル DARPA インターネットプログラムのプロトコル仕様 (http://tools.ietf.org/html/rfc791)
- ドメイン間のクラスレスルーティング (CIDR): インターネットアドレスの割り当ておよびアグリゲーションの計画 (http://tools.ietf.org/html/rfc4632)

次の表に、サブネット長指定の例 (CIDR 表記と 10 進ドット形式の両方)、および各接頭辞長を持つネットワークに収容可能なホストの合計台数を示します。

表 1-1 CIDR 接頭辞と 10 進数での表現

CIDR ネットワーク接頭辞長	対応する 10 進ドットサブネットマスク	割り当て可能な IP アドレス
/19	255.255.224.0	8,192
/20	255.255.240.0	4,096
/21	255.255.248.0	2,048
/22	255.255.252.0	1,024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32

プライベートアドレス

IANA は IPv4 アドレスのブロックを予約しています。これらのプライベートアドレスは、プライベートネットワーク内のネットワークトラフィックに対して使用されます。インターネットサービスプロバイダから IPv4 アドレスのブロックを要求する組織が、組織内の各システムに一意のアドレスを付与できる十分な割り当てを受けることはまずありません。組織は通常、内部ネットワーク上のシステムにプライベートアドレスを割り当てます。各システムは、ネットワークアドレス変換 (NAT) とアプリケーションプロキシサーバーを使用してインターネット上のほかのサイトと通信することによって、インターネットサービスプロバイダ (ISP) から与えられた数に限りのあるアドレスを効果的に共有できます。

次の表に、プライベート IPv4 アドレスの範囲と、各範囲に対応するネットマスクの一覧を示します。

ネットワーク接頭辞/ネットワーク長	IPv4 アドレス範囲
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/125	172.16.0.0 - 172.31.255.25
192.168.0.0/16	192.168.0.0 - 192.168.255.255

DHCP アドレス

動的ホスト構成プロトコル (DHCP) を使用すると、システムは、ブートプロセスの一環として、IP アドレスなどの構成情報を DHCP サーバーから受け取ることができます。DHCP サー

バーは IP アドレスのプールを保持しており、その中から DHCP クライアントにアドレスを割り当てます。DHCP を使用するサイトでは、クライアントが継続的に接続されることはないものとして、すべてのクライアントに永続的な IP アドレスを割り当てた場合に必要となる IP アドレス数よりも少ない数の IP アドレスのプールを使用します。この場合、クライアント間でアドレスを共有することによって、必要な IP アドレスの総数を減らすことができます。しかし、各クライアントが十分な頻度で IP アドレスの取得と返却を繰り返さないと、最終的には、クライアントと同数の IP アドレスが必要になります。DHCP アドレスを使用することのより全般的な利点は、DHCP サーバーで構成の詳細を設定できるので、個々のホストの構成作業が軽減される点です。これにより、ホストでの手動による構成が最小限または不要になります。サイトの IP アドレスまたはその一部を管理するように DHCP サービスを設定できます。詳細は、『Oracle Solaris 11.2 での DHCP の作業 』を参照してください。

IPv6 アドレス

128 ビットの IPv6 アドレスは、IPv4 で使用可能なアドレス空間よりも広大なアドレス空間を提供します。IPv6 アドレスは、4 桁の 16 進数のグループを 8 個、コロンで区切ったものとして表現されます。各グループの先頭のゼロは非表示にできます。次の例に示すように、すべてゼロのグループが 1 つ以上連続する場合は、二重コロンで置換できます。

```
2001:db8:2f32:27:214:4fff:fe4a:9926
```

CIDR 形式の IPv4 アドレスと同様、IPv6 アドレスはクラスレスであり、サイトのネットワークを定義するアドレスの一部を指定するのに接頭辞を使用します (次の例を参照)。

```
2001:db8:2f32::/48
```

IPv6 アドレス指定の詳細については、IP Version 6 Addressing Architecture (http://tools.ietf.org/html/rfc4291) を参照してください。

ドキュメント接頭辞

IPv6 アドレスの場合、`2001:db8::/32` という接頭辞は、このドキュメントの例だけで使用される特別な IPv6 接頭辞です。このドキュメントの例では、プライベート IPv4 アドレスと予約 IPv6 文書接頭辞を使用します。

ネットワークの IP 番号の取得

IPv4 ネットワークは、IPv4 ネットワーク番号とネットワークマスク、つまり「*ネットマスク*」を組み合わせて定義されます。IPv6 ネットワークは、「*サイト接頭辞*」、およびサブネット化されている場合は、「*サブネット接頭辞*」で定義されます。

プライベートネットワークがインターネット上の外部ネットワークと通信できるようにするには、ネットワーク用の登録済み IP 番号を適切な組織から取得する必要があります。取得したアドレスが、IPv4 アドレス指定スキームのネットワーク番号または IPv6 アドレス指定スキームのサイト接頭辞となります。

ISP は、複数のサービスレベルを基準にした課金体系によって、ネットワークの IP アドレスを提供します。各 ISP を調査して、どこが自分のネットワークに最も合ったサービスを提供しているのかを決定します。一般的に ISP は、企業に対して、動的に割り当てられるアドレスまたは静的 IP アドレスを提供します。IPv4 アドレスと IPv6 アドレスの両方を提供する ISP もあります。

自分が ISP の場合は、自分のロケールのインターネットレジストリ (IR) から、顧客用の IP アドレスを取得します。IANA は、世界中の登録 IP アドレスの IR への委託に対して最終的な責任を負います。各 IR には、IR がサービスを提供するロケールの登録情報とテンプレートが含まれています。IANA とその IR については、IANA の IP Address Service のページ (http://www.iana.org/ipaddress/ip-addresses.htm)を参照してください。

ネットワーク上の名前付けエンティティーの使用

TCP/IP は、ネットワーク上の特定のシステムを見つけるときに、そのシステムの IP アドレスを使用します。ただし、ホスト名を使用すれば、IP アドレスの場合よりも容易にシステムを識別できます。

TCP/IP の視点から見れば、ネットワークは名前が付けられたエンティティーの集合です。ホストは名前が付けられた 1 個のエンティティーです。ルーターも名前が付けられた 1 個のエンティティーです。さらに、ネットワークも名前が付けられた 1 個のエンティティーです。ネットワークがインストールされているグループや部門にも、名前を付けることができます。部課、地区、会社も同様です。理論的には、ネットワークを識別するために使用できる名前の階層については、事実上まったく制限はありません。

ドメイン名

多くのネットワークでは、そのホストとルーターが管理ドメインの階層に編成されます。ネットワーク情報サービス (NIS) またはドメインネームシステム (DNS) のネームサービスを使用する場合は、所属組織のドメイン名として、全世界で一意な名前を選択する必要があります。ドメイン名が一意であることを保証するには、そのドメイン名を *InterNIC* に登録する必要があります。自分のシステムをインターネット上のほかのサイトが DNS を介して検索できるようにする場合は、一意のドメイン名が必要です。

別のドメインの下に配置されるドメイン名は、よくサブドメインと呼ばれます。ドメイン名は階層構造になっています。一般に、新規のドメインは、既存の関連するドメインの下に配置されます。たとえば、子会社のドメイン名はその親会社のドメイン名の下に配置されます。ドメイン名がほかの関係を持たない場合、組織はそのドメイン名を、`.com`、`.org`、`.edu`、`.gov` など、既存の最上位ドメインのいずれかの下に直接配置できます。

ネームサービスとディレクトリサービスの選択

Oracle Solaris では、ローカルファイル、NIS、および DNS の 3 種類のネームサービスから選択できます。ネームサービスは、ホスト名や IP アドレスなど、ネットワーク上のマシンに関する重要な情報を維持します。また、ネームサービスに加えて、あるいはネームサービスの代わりに、LDAP ディレクトリサービスも使用できます。LDAP は、ディレクトリサーバーにアクセスして分散型ネームサービスやその他のディレクトリサービスを利用するために使用される、セキュアなネットワークプロトコルです。この標準ベースのプロトコルは、階層的なデータベース構造をサポートしています。同じプロトコルを使用して、UNIX とマルチプラットフォームの両方の環境でネームサービスを提供できます。Oracle Solaris のネームサービスの概要については、『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS 』の第 1 章「ネームサービスとディレクトリサービスについて」を参照してください。

ネットワークデータベースの構成は重要です。したがって、ネットワーク計画工程の一環として、どのネームサービスまたはディレクトリサービスを使用するかを決定する必要があります。ネームサービスの使用の決定は、ネットワークを管理ドメインとして編成するかどうかにも影響を与えます。

ネームサービスまたはディレクトリサービスは、次の中から選択できます。

- NIS または DNS – NIS および DNS ネームサービスは、ネットワーク上の複数のサーバー上でネットワークデータベースを維持します。『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS 』では、これらのネームサービスについて説明し、

データベースの構成方法について解説しています。このガイドでは、*名前空間*と*管理ドメイン*の概念についても詳しく説明しています。

- LDAP - ネームサービスに加えて、あるいはネームサービスの代わりに、LDAP ディレクトリサービスも使用できます。LDAP は、ディレクトリサーバーにアクセスして分散型ネームサービスやその他のディレクトリサービスを利用するために使用される、セキュアなネットワークプロトコルです。
- ローカルファイル – NIS、DNS、または LDAP を実装しない場合、ネットワークは*ローカルファイル*を使用してネームサービスを提供します。「ローカルファイル」とは、ネットワークデータベースが使用するためのものとして `/etc` ディレクトリに入っている一連のファイルのことです。このドキュメントに示す手順では、特に断らないかぎり、ネームサービスとしてローカルファイルを使用しているものとします。

注記 - ネットワーク用のネームサービスとしてローカルファイルを使用することに決めた場合でも、後日、別のネームサービスを設定できます。

ホスト名の管理

ネットワークを構成するシステムの命名スキームを計画します。ネットワーク上の各マシンは、プライマリネットワークインタフェースの IP アドレスに対応する TCP/IP ホスト名を持つ必要があります。ホスト名は、システムのサブドメイン内で一意である必要があります。物理マシンと同様に、仮想システムにも一意の IP アドレスとホスト名を与える必要があります。

システムには次のものを持つことができます。

- システムの IP アドレスにマップされる複数のホスト名。たとえば、`systema.mycompany.com` を、`www.mycompany.com` として認識されるようにすることもできます。
- IPv4 アドレスと IPv6 アドレスの両方に対する同一のホスト名。
- ネットワークのリナンバリングに対応するため、一定期間、同一のホスト名に対して構成される新しい IP アドレスと古い非推奨の IP アドレス。
- それぞれ一意の IP アドレスとホスト名を持つ、異なるサブネット上の複数のネットワークインタフェース。

ネットワークの計画を立てるときは、IP アドレスとそれぞれのホスト名のリストを作って、設定工程中に各マシンに簡単にアクセスできるようにしてください。このリストは、すべてのホスト名が一意かどうかを検査するために役立ちます。

注記 - プライマリインタフェースの TCP/IP ホスト名は、`hostname` コマンドで設定した*システムのホスト名*とは別個のエンティティーです。Oracle Solaris では必須ではありませんが、両者には通常、同じ名前が使用されます。一部のネットワークアプリケーションは、この慣習に依存しています。詳細は、`hostname`(1)のマニュアルページを参照してください。

♦ ♦ ♦ 第 2 章

2 IPv6 アドレスの使用の計画

この章では、第1章「ネットワーク配備の計画」に対する補足情報として、ネットワーク上で IPv6 アドレスを使用することにした場合の追加の考慮点について説明します。

IPv4 アドレスのほかに IPv6 アドレスを使用することを計画している場合、現在の ISP が両方のアドレスタイプをサポートしていることを確認してください。

IPv6 の概念の概要については、Internet Protocol, Version 6 (IPv6) Specification (http://www.ietf.org/rfc/rfc2460.txt) を参照してください。

IPv6 の構成タスクについては、『Oracle Solaris 11.2 でのネットワークコンポーネントの構成と管理 』の「IPv6 インタフェースの構成」を参照してください。

IPv6 ネットワークのトラブルシューティングに関する詳細については、『Oracle Solaris 11.2 でのネットワーク管理のトラブルシューティング 』の「IPv6 配備に関する問題のトラブルシューティング」を参照してください。

この章の内容は、次のとおりです。

IPv6 計画タスク

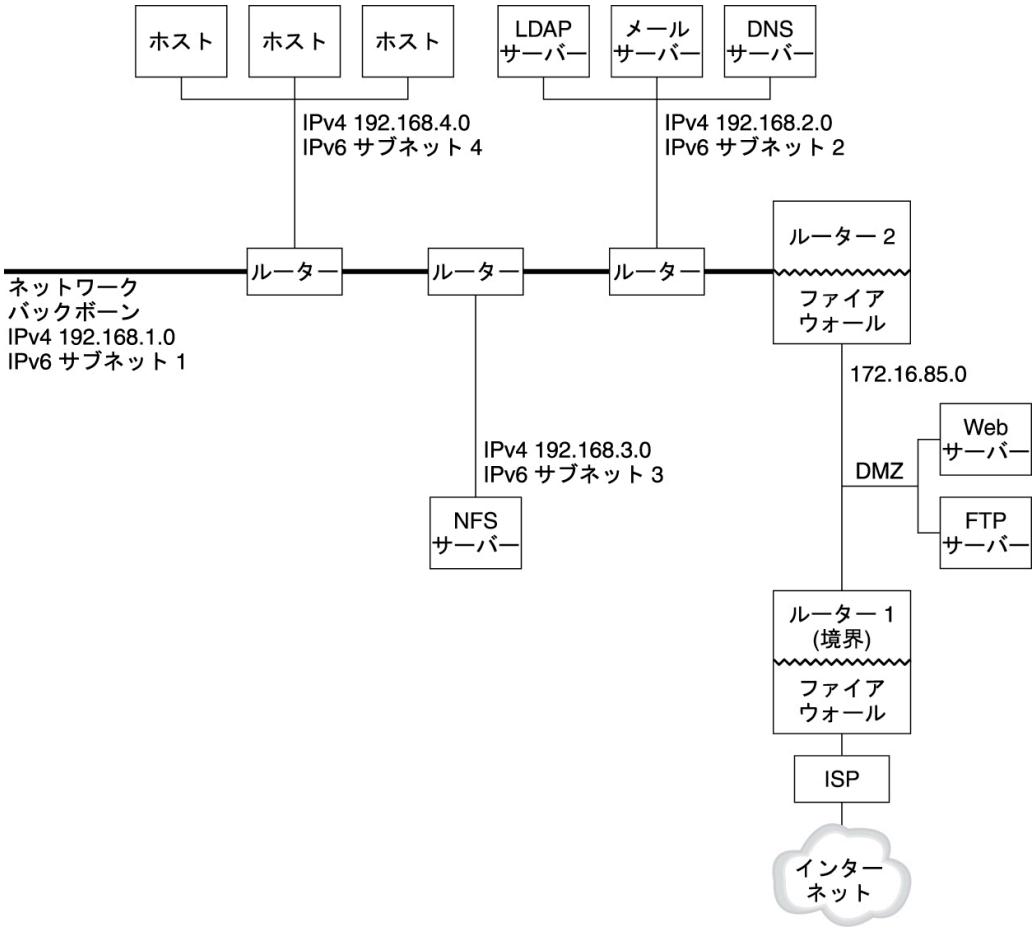
次の表に、ネットワーク上での IPv6 の実装を計画する場合のさまざまな考慮点を示します。既存の IPv4 ネットワークを IPv6 ネットワークに移行する場合の追加の手順については、『Oracle Solaris 11.2 でのネットワークコンポーネントの構成と管理 』の「IPv4 ネットワークから IPv6 ネットワークへの移行」を参照してください。

タスク	説明	参照先
IPv6 をサポートするようにハードウェアを準備します。	IPv6 をサポートできるようにハードウェアをアップグレードします。	26 ページの「IPv6 のハードウェアサポートの確認」
アプリケーションが IPv6 をサポートすることを確認します。	使用するアプリケーションが IPv6 環境で動作できることを確認します。	29 ページの「IPv6 をサポートするようにネットワークサービスを構成する」
トンネルの使用について計画します。	ほかのサブネットまたは外部ネットワークへのトンネルを実行するルーターを判断します。	31 ページの「ネットワークでのトンネル使用の計画」
ネットワークのセキュリティー保護を行う方法を計画し、IPv6 セキュリティーポリシーを開発します。	IPv6 を構成する前に、セキュリティーのため、DMZ およびそのエンティティーへのアドレス指定を計画する必要があります。 IP フィルタ、IP セキュリティーアーキテクチャー (IPsec)、インターネット鍵交換 (IKE)、およびこのリリースのその他のセキュリティー機能を使用するなど、セキュリティーの実装方法を決定します。	32 ページの「IPv6 実装のセキュリティーについて」 『Oracle Solaris 11.2 でのネットワークのセキュリティー保護 』
ネットワーク上のシステムへのアドレス指定を計画します。	IPv6 を構成する前に、サーバー、ルーター、およびホストへのアドレス指定スキームを計画する必要があります。この手順には必要に応じて、ネットワークのサイト接頭辞の取得や IPv6 サブネットの計画も含まれます。	27 ページの「ノードの IPv6 アドレス指定計画の立案」

IPv6 ネットワークトポロジの概要

IPv6 は通常、次の図に示すような IPv4 も使用されている混在ネットワークトポロジで使用されます。次の図は、この章で IPv6 構成タスクを説明する際に参照用に使用されます。

図 2-1 IPv6 ネットワークトポロジのシナリオ



図に示した企業ネットワークシナリオでは、既存の IPv4 アドレスを持つサブネットが 5 つあります。ネットワークのリンクは管理サブネットに直接対応します。4 つの内部ネットワークは、RFC 1918 スタイルの IPv4 専用アドレスで表されています。このアドレスは、IPv4 アドレスの不足に対応するための一般的な解決方法です。

これらの内部ネットワークでは、次のアドレススキームを使用します。

- Subnet 1 は内部ネットワークバックボーン `192.168.1` です。
- Subnet 2 は内部ネットワーク `192.168.2` であり、LDAP、`sendmail`、および DNS サーバーが含まれます。

- Subnet 3 は内部ネットワーク 192.168.3 であり、企業の NFS サーバーが含まれます。
- Subnet 4 は内部ネットワーク 192.168.4 であり、企業の従業員用のホストが含まれます。

外部の公開ネットワーク 172.16.85 は、企業の DMZ として機能します。このネットワークには、Web サーバーや匿名 FTP サーバーなど、企業が外部に提供するリソースが含まれます。Router 2 はファイアウォールを実行して、公開ネットワーク 172.16.85 を内部バックボーンから分離します。非武装ゾーン (DMZ) のもう一方の終端では、Router 1 がファイアウォールを実行して、企業の境界サーバーとして機能します。

図2-1「IPv6 ネットワークトポロジのシナリオ」では、公開 DMZ は RFC 1918 専用アドレス 172.16.85 を持っています。実際には、公開 DMZ は登録済み IPv4 アドレスを持っている必要があります。ほとんどの IPv4 サイトは、公開アドレスと RFC 1918 専用アドレスの組み合わせを使用します。しかし、IPv6 を導入すると、公開アドレスと専用アドレスの概念が変わります。IPv6 は巨大なアドレス空間を持つため、専用ネットワークにも、公開ネットワークにも、IPv6 公開アドレスを使用します。

Oracle Solaris デュアルプロトコルスタックは、IPv4 と IPv6 の並行動作をサポートします。ネットワークに IPv6 を配備している最中および配備したあとも、IPv4 関連の操作を問題なく実行できます。IPv4 をすでに使用している動作中のネットワーク上で IPv6 を配備するときは、進行中の処理の邪魔にならないようにしてください。

IPv6 のハードウェアサポートの確認

次のクラスのハードウェアについては、メーカーのドキュメントで IPv6 の対応状況を調べてください。

- ルーター
- ファイアウォール
- サーバー
- スイッチ

注記 - このドキュメントで説明するすべての手順では、装置 (特に、ルーター) が IPv6 向けにアップグレードできると仮定します。ただし、IPv6 向けにアップグレードできないルーターモデルもあります。詳細な情報と回避策については、『Oracle Solaris 11.2 でのネットワーク管理のトラブルシューティング 』の「IPv4 ルーターを IPv6 にアップグレードできない」を参照してください。

IPv6 アドレス指定計画の準備

IPv4 から IPv6 への移行の主要な作業として、アドレス指定計画の策定があり、これには次の準備が必要です。

- 27 ページの「サイト接頭辞の取得」
- 27 ページの「IPv6 番号付けスキームの作成」

実際の移行タスクについては、『Oracle Solaris 11.2 でのネットワークコンポーネントの構成と管理 』の「IPv4 ネットワークから IPv6 ネットワークへの移行」を参照してください。

サイト接頭辞の取得

IPv6 を構成する前に、サイト接頭辞を取得する必要があります。サイト接頭辞は、自分の IPv6 実装におけるすべてのノードの IPv6 アドレスを抽出するときに使用します。

IPv6 をサポートする ISP は、48 ビットの IPv6 サイト接頭辞を提供できます。現在の ISP が IPv4 しかサポートしない場合、現在の ISP を IPv4 サポート用に残したまま、別の ISP を IPv6 サポート用に使用できます。このような場合の回避方法は複数あります。詳細は、『Oracle Solaris 11.2 でのネットワーク管理のトラブルシューティング 』の「現在の ISP が IPv6 をサポートしない」を参照してください。

企業自身が ISP である場合、顧客のサイト接頭辞は適切なインターネットレジストリから取得します。詳細については、Internet Assigned Numbers Authority (IANA) (http://www.iana.org) を参照してください。

IPv6 番号付けスキームの作成

IPv6 ネットワークがまったく新しいものでない限り、既存の IPv4 トポロジを IPv6 番号付けスキームとして使用します。

ノードの IPv6 アドレス指定計画の立案

ほとんどのホストにおいて、インタフェースに IPv6 アドレスを構成するのに適切で時間がかからない戦略は、ステートレス自動構成です。ホストが最も近いルーターからサイト接頭辞を受信

したとき、近傍検索プロトコルは自動的に、ホストの各インタフェースに IPv6 アドレスを生成します。

サーバーは安定した IPv6 アドレスを持つ必要があります。サーバーの IPv6 アドレスを手動で構成しない場合、サーバーの NIC カードを交換したときには、新しい IPv6 アドレスが自動構成されます。

サーバーのアドレスを作成するときには、次のことを覚えておいてください。

- サーバーには意味のある安定したインタフェース ID を指定してください。インタフェース ID の番号付けスキームを使用するときには、1 つの戦略だけを使用します。たとえば、図 2-1「IPv6 ネットワークトポロジのシナリオ」の LDAP サーバーの内部インタフェースは `2001:db8:3c4d:2::2` になります。
- あるいは、IPv4 ネットワークの番号を定期的に変更しない場合、ルーターおよびサーバーの既存の IPv4 アドレスをそのインタフェース ID として使用することを考えてください。図 2-1「IPv6 ネットワークトポロジのシナリオ」では、Router 1 の DMZ へのインタフェースは IPv4 アドレス `192.168/16` を持っていると仮定します。この IPv4 アドレスを 16 進数に変換すると、その結果をインタフェース ID として使用できます。つまり、新しいインタフェース ID は `::7bc8:156F` になります。

  この方法は、ISP から IPv4 アドレスを取得したのではなく、登録済み IPv4 アドレスを所有しているときだけに使用するようにしてください。ISP から取得した IPv4 アドレスを使用している場合、依存関係が発生し、ISP を変更する場合に問題が発生します。

使用可能な IPv4 アドレスの数には制限があるため、ネットワーク設計者は、すでに登録済みのグローバルアドレスや RFC 1918 のプライベートアドレスをどのように使用するかを考える必要がありました。しかし、IPv4 のグローバルアドレスや専用アドレスの表記は IPv6 アドレスには適用されません。サイト接頭辞を含む*グローバルユニキャストアドレス*は、ネットワークのすべてのリンクで使用できます (公開 DMZ を含む)。

サブネット用の番号付けスキームの作成

番号付けスキームを開始するには、まず、既存の IPv4 サブネットを等価な IPv6 サブネットにマッピングします。たとえば、図2-1「IPv6 ネットワークトポロジのシナリオ」に示したサブネットを考えてください。サブネット 1 からサブネット 4 までは、RFC 1918 の IPv4 専用アドレス指定を使用して、アドレスの最初の 16 ビットを指定し、さらに、1 から 4 までの数字を使用して、サブネットを指定しています。この例では、IPv6 接頭辞 `2001:db8:3c4d/48` がサイトに割り当てられていると仮定します。

次の表に、専用アドレスの IPv4 接頭辞から IPv6 接頭辞にマッピングする方法を示します。

IPv4 サブネット接頭辞	等価な IPv6 サブネット接頭辞
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

IPv6 をサポートするようにネットワークサービスを構成する

次に示す典型的な IPv4 ネットワークサービスは、IPv6 にも対応しています。

- DNS
- HTTP (Apache 2 リリースまたは Orion)
- LDAP
- NFS
- `sendmail`

IMAP メールサービスは IPv4 専用です。

IPv6 向けに構成されたノードでも IPv4 サービスは実行できます。IPv6 を有効にしても、必ずしもすべてのサービスが IPv6 接続を受け入れるわけではありません。IPv6 向けに移植されたサービスだけが IPv6 接続を受け入れます。IPv6 向けに移植されていないサービスは、プロトコルスタックの IPv4 部分を使用して機能し続けることができます。

IPv6 向けにアップグレードしたあとで、いくつかの問題が発生する可能性があります。詳細は、『Oracle Solaris 11.2 でのネットワーク管理のトラブルシューティング 』の「サービスを IPv6 サポート用にアップグレードしているときに問題が発生する」を参照してください。

▼ IPv6 をサポートするためにネットワークサービスを準備する方法

1. **IPv6 をサポートするには、次のネットワークサービスを更新します。**

   - メールサーバー

- NIS サーバー
- NFS

注記 - LDAP は IPv6 をサポートします。IPv6 固有な構成タスクは必要ありません。

---

2. **ファイアウォールハードウェアが IPv6 をサポートできるかどうかを確認します。**

   この手順については、ファイアウォール関連の適切なドキュメントを参照してください。

3. **ネットワーク上のほかのサービスが IPv6 向けに移植されているかどうかを確認します。**

   詳細については、ソフトウェアに付属するドキュメントや関連するドキュメントを参照してください。

4. **次のサービスを配備しているサイトでは、これらのサービスを適切に評価しているかどうかを確認します。**

   - **ファイアウォール** – IPv6 をサポートするため、IPv4 向けに策定されているポリシーの強化を検討します。セキュリティーの詳しい考慮事項については、32 ページの「IPv6 実装のセキュリティーについて」を参照してください。
   - **メール**– DNS の Mail Exchange レコード (MX レコード) に、メールサーバーの IPv6 アドレスを追加することを検討します。
   - **DNS**– DNS 固有の考慮事項については、30 ページの「IPv6 をサポートするために DNS を準備する方法」を参照してください。
   - **IPQoS** – ホストで IPv4 向けに使用していたのと同じ *Diffserv* ポリシーを使用します。

5. **ノードを IPv6 向けに変更する前に、そのノードが提供するネットワークサービスを評価します。**

▼ IPv6 をサポートするために DNS を準備する方法

Oracle Solaris は、クライアント側とサーバー側の両方において、DNS による名前解決をサポートします。IPv6 をサポートするために DNS サービスを準備するには、次の手順を実行します。

IPv6 用の DNS サポートに関係する詳細情報については、『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS 』を参照してください。

1. **再帰的な名前解決を実行する DNS サーバーがデュアルスタックであるか (つまり、IPv4 と IPv6 両用であるか)、あるいは、IPv4 専用であるかを判断します。**

2. **DNS サーバーでは、関連する IPv6 データベース AAAA レコードを前進ゾーンで使用して、DNS データベースを作成します。**

   注記 - 複数の基幹系のサービスを実行しているサーバーには、特に注意する必要があります。ネットワークが適切に機能していることを確認します。また、すべての基幹系のサービスが IPv6 向けに移植されていることを確認します。次に、そのサーバーの IPv6 アドレスを DNS データベースに追加します。

3. **AAAA レコードの関連する PTR レコードを逆進ゾーンに追加します。**

4. **IPv4 専用データまたは IPv6 と IPv4 両用データを、ゾーンを記述する NS レコードに追加します。**

ネットワークでのトンネル使用の計画

IPv6 実装は、IPv4 と IPv6 が混在するネットワークへの移行メカニズムとして、多数のトンネル構成をサポートします。トンネルを使用すると、孤立した IPv6 ネットワークどうしが通信できるようになります。ほとんどのインターネットは IPv4 で動作しているため、自分のサイト (IPv6 ネットワーク) から宛先のサイト (IPv6 ネットワーク) に IPv6 パケットを送信するためには、インターネットにトンネルを開けて、そこを通す必要があります。

次に、IPv6 ネットワークトポロジにおいてトンネルを使用するいくつかのシナリオを示します。

- ISP から IPv6 サービスを購入すると、自分のサイトの境界ルーターから ISP ネットワークにトンネルを作成できます。図2-1「IPv6 ネットワークトポロジのシナリオ」に、このようなトンネルを示します。このようなシナリオの場合は、手動の IPv6 over IPv4 トンネルを実行します。
- 大規模な分散ネットワークを IPv4 接続で管理している場合。IPv6 を使用する分散サイトに接続するには、各サブネットの境界ルーターから自動 6to4 トンネルを実行します。
- 自分のインフラストラクチャー内のルーターを IPv6 向けにアップグレードできないこともあります。このような場合には、2 つの IPv6 ルーターをエンドポイントとして、IPv4 ルーターに手動トンネルを作成できます。

トンネルを構成する手順については、『Oracle Solaris 11.2 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理 』の第 5 章「IP トンネルの管理」を参照してください。ト

ンネルの概念については、『Oracle Solaris 11.2 での TCP/IP ネットワーク、IPMP、および IP トンネルの管理 』の「IP トンネルの機能のサマリー」を参照してください。

IPv6 実装のセキュリティーについて

IPv6 を既存のネットワークに導入するとき、サイトのセキュリティーを損なわないように注意する必要があります。

IPv6 を導入するときには、次のセキュリティーの問題点に注意してください。

- IPv6 パケットと IPv4 パケットには、両方とも、同じ量のフィルタリンクが必要です。
- IPv6 パケットは頻繁にファイアウォールにトンネルを開けます。

  したがって、次のシナリオのどちらかを実装する必要があります。

  - ファイアウォールでトンネル内部のコンテンツを検査すること。
  - トンネルの反対側にあるエンドポイントでも、同じような規則の IPv6 ファイアウォールを設置すること。
- IPv6 over User Datagram Protocol (UDP) over IPv4 トンネルを使用するような移行メカニズムもあります。しかし、このようなメカニズムはファイアウォールを通らないため、危険であることが証明されています。
- IPv6 ノードは企業ネットワークの外からグローバルに到達できます。セキュリティーポリシーで公開アクセスを禁止する場合、ファイアウォールに対して、より厳しい規則を確立する必要があります。たとえば、*ステートフルなファイアウォール*の構成を考えてください。

このマニュアルには、IPv6 実装内で使用可能な次のセキュリティー機能に関する情報が含まれています。

- IP セキュリティーアーキテクチャー (IPsec) 機能を使用すると、IPv6 パケットを暗号化で保護できます。詳細は、『Oracle Solaris 11.2 でのネットワークのセキュリティー保護 』の第 6 章「IP セキュリティーアーキテクチャーについて」を参照してください。
- インターネットキー交換 (Internet Key Exchange、IKE) は、IPsec の鍵管理を自動化します。詳細は、『Oracle Solaris 11.2 でのネットワークのセキュリティー保護 』の第 8 章「インターネット鍵交換について」を参照してください。

索引

ら

C

D

I

N