APPENDIX D

アドレス、プロトコル、およびポート

この付録では、IP アドレス、プロトコル、およびアプリケーションのクイック リファレンスを提供します。この付録は、次の項で構成されています。

IPv4 アドレスとサブネット マスク

この項では、セキュリティ アプライアンスで IPv4 アドレスを使用する方法について説明します。IPv4 アドレスはドット付き 10 進数表記の 32 ビットの数値であり、バイナリから 10 進数に変換されドットで区切られた 4 つの 8 ビット フィールド（オクテット）で構成されます。IP アドレスの最初の部分はホストが常駐するネットワークを示し、2 番目の部分は所定のネットワーク上の特定のホストを示します。ネットワーク番号フィールドは、ネットワーク プレフィックスと呼ばれます。所定のネットワーク上のホストはすべて、同じネットワーク プレフィックスを共有しますが、固有のホスト番号を持つ必要があります。クラスフル IP では、アドレスのクラスがネットワーク プレフィックスとホスト番号の間の境界を決定します。

この項では、次のトピックについて取り上げます。

クラス

IP ホスト アドレスは、Class A、Class B、および Class C の 3 つの異なるアドレス クラスに分割されます。各クラスは、32 ビット アドレス内の異なるポイントで、ネットワーク プレフィックスとホスト番号の間の境界を修正します。Class D アドレスは、マルチキャスト IP 用に予約されています。

- Class A アドレス（1.xxx.xxx.xxx ～ 126.xxx.xxx.xxx）は、最初のオクテットだけをネットワーク プレフィックスとして使用します。

- Class B アドレス（128.0.xxx.xxx ～ 191.255.xxx.xxx）は、最初の 2 つのオクテットをネットワーク プレフィックスとして使用します。
- Class C アドレス（192.0.0.xxx ～ 223.255.255.xxx）は、最初の 3 つのオクテットをネットワーク プレフィックスとして使用します。

Class A アドレスには 16,777,214 個のホスト アドレス、Class B アドレスには 65,534 個のホストがあるので、サブネット マスクを使用してこれらの膨大なネットワークを小さいサブネットに分割することができます。

プライベート ネットワーク

ネットワーク上に多数のアドレスが必要な場合、それらをインターネットでルーティングする必要がないときは、Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）が推奨するプライベート IP アドレスを使用できます（RFC 1918 を参照）。次のアドレス範囲が、アドバタイズされないプライベート ネットワークとして指定されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

サブネット マスク

サブネット マスクを使用すると、単一の Class A、B、または C ネットワークを複数のネットワークに変換できます。サブネット マスクを使用して、ホスト番号からネットワーク プレフィックスにビットを追加する拡張ネットワーク プレフィックスを作成することができます。たとえば、Class C ネットワーク プレフィックスは常に、IP アドレスの最初の 3 つのオクテットで構成されます。一方、Class C 拡張ネットワーク プレフィックスは、4 番目のオクテットの一部も使用します。

ドット付き 10 進数の代わりにバイナリ表記を使用している場合は、サブネット マスクを容易に理解できます。サブネット マスク内のビットには、インターネット アドレスとの 1 対 1 の対応関係があります。

- IP アドレス内の対応するビットが拡張ネットワーク プレフィックスの一部である場合、ビットは 1 に設定されます。
- ビットがホスト番号の一部である場合、ビットは 0 に設定されます。

例 1 : Class B アドレスが 129.10.0.0 の場合に 3 番目のオクテット全体をホスト番号ではなく拡張ネットワーク プレフィックスとして使用するには、サブネット マスクとして 11111111.11111111.11111111.00000000 を指定する必要があります。このサブネット マスクによって、Class B アドレスは、ホスト番号が最後のオクテットだけで構成される Class C アドレスに相当するものに変換されます。

例 2 : 3 番目のオクテットの一部だけを拡張ネットワーク プレフィックスに使用する場合は、11111111.11111111.11111000.00000000 のようなサブネット マスクを指定する必要があります。ここでは、3 番目のオクテットのうち 5 ビットだけが拡張ネットワーク プレフィックスに使用されます。

サブネット マスクは、ドット付き 10 進数マスクまたは */ ビット*（「スラッシュ *ビット*」）マスクとして記述できます。例 1 では、ドット付き 10 進数マスクに対して、各バイナリ オクテットを 10 進数の 255.255.255.0 に変換します。*/ ビット* マスクの場合は、1s: /24 の数値を追加します。例 2 では、10 進数は 255.255.248.0 で、/ ビットは /21 です。

3 番目のオクテットの一部を拡張ネットワーク プレフィックスに使用して、複数の Class C ネットワークを大規模なネットワークにスーパーネット化することもできます。たとえば、192.168.0.0/20 と入力できます。

この項では、次のトピックについて取り上げます。

- 「サブネット マスクの判別」（P.D-3）
- 「サブネット マスクで使用するアドレスの判別」（P.D-3）

サブネット マスクの判別

必要なホストの数に基づいてサブネット マスクを判別するには、表 D-1 を参照してください。

表 D-1　ホスト、ビット、およびドット付き 10 進数マスク

ホスト[1]	/ビット マスク	ドット付き 10 進数マスク
16,777,216	/8	255.0.0.0 Class A ネットワーク
65,536	/16	255.255.0.0 Class B ネットワーク
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 Class C ネットワーク
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
使用不可	/31	255.255.255.254
1	/32	255.255.255.255 単一ホスト アドレス

1. 単一のホストを示す /32 を除き、サブネットの最初と最後の数は予約されています。

サブネット マスクで使用するアドレスの判別

次の各項では、Class C サイズおよび Class B サイズのネットワークに対してサブネット マスクで使用するネットワーク アドレスを判別する方法について説明します。この項では、次のトピックについて取り上げます。

- 「Class C サイズのネットワーク アドレス」（P.D-3）
- 「Class B サイズのネットワーク アドレス」（P.D-4）

Class C サイズのネットワーク アドレス

2 ～ 254 のホストを持つネットワークの場合、4 番目のオクテットは、0 から始まるホスト アドレスの数の倍数になります。たとえば、8 つのホストを持つサブネット（/29）、192.168.0.x は次のようになります。

マスク /29（255.255.255.248）でのサブネット	アドレス範囲[1]
192.168.0.0	192.168.0.0 ～ 192.168.0.7
192.168.0.8	192.168.0.8 ～ 192.168.0.15
192.168.0.16	192.168.0.16 ～ 192.168.0.31
…	…
192.168.0.248	192.168.0.248 ～ 192.168.0.255

1. サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、192.168.0.0 と 192.168.0.7 は使用できません。

Class B サイズのネットワーク アドレス

254 ～ 65,534 のホストを持つネットワークのサブネット マスクで使用するネットワーク アドレスを判別するには、可能な拡張ネットワーク プレフィックスそれぞれについて 3 番目のオクテットの値を判別する必要があります。たとえば、10.1.*x*.0 のようなアドレスをサブネット化することができます。ここで、最初の 2 つのオクテットは拡張ネットワーク プレフィックスで使用されるため固定されています。4 番目のオクテットは、すべてのビットがホスト番号に使用されるため、0 です。

3 番目のオクテットの値を判別するには、次の手順を実行します。

ステップ 1　65,536（3 番目と 4 番目のオクテットを使用するアドレスの合計）を必要なホスト アドレスの数で割って、ネットワークから作成できるサブネットの数を計算します。

たとえば、65,536 を 4096 のホストで割ると、16 になります。

したがって、Class B サイズのネットワークでは、それぞれ 4096 個のアドレスを持つサブネットが 16 個できます。

ステップ 2　256（3 番目のオクテットの値の数）をサブネットの数で割って、3 番目のオクテット値の倍数を判別します。

この例では、256/16 = 16 です。

3 番目のオクテットは、0 から始まる 16 の倍数になります。

したがって、ネットワーク 10.1 の 16 個のサブネットは次のようになります。

マスク /20（255.255.240.0）でのサブネット	アドレス範囲[1]
10.1.0.0	10.1.0.0 ～ 10.1.15.255
10.1.16.0	10.1.16.0 ～ 10.1.31.255
10.1.32.0	10.1.32.0 ～ 10.1.47.255
…	…
10.1.240.0	10.1.240.0 ～ 10.1.255.255

1. サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、10.1.0.0 と 10.1.15.255 は使用できません。

IPv6 形式のアドレス

IPv6 は、IPv4 後の次世代インターネット プロトコルです。これにより、アドレス空間の拡張、ヘッダー形式の簡略化、拡張子とオプションのサポートの向上、フロー ラベル機能、および認証とプライバシーの機能が提供されます。IPv6 については RFC 2460 で説明されています。IPv6 アドレッシング アーキテクチャについては RFC 3513 で説明されています。

この項では、IPv6 アドレス形式およびアーキテクチャについて説明します。次の項目を取り上げます。

- 「IPv6 アドレス形式」（P.D-5）
- 「IPv6 アドレス タイプ」（P.D-6）
- 「IPv6 アドレス プレフィックス」（P.D-10）

（注）　この項では、IPv6 アドレス形式、タイプ、およびプレフィックスについて説明します。IPv6 を使用するためのセキュリティ アプライアンスの設定については、第 7 章「インターフェイス パラメータの設定」を参照してください。

IPv6 アドレス形式

IPv6 アドレスは、x:x:x:x:x:x:x:x のように、コロン（:）で区切られた 8 つの一連の 16 ビット 16 進数フィールドとして表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

（注）　IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

アドレスの個々のフィールドに先行ゼロを含める必要はありません。ただし、各フィールドに少なくとも 1 桁を含める必要があります。したがって、例のアドレス 2001:0DB8:0000:0000:0008:0800:200C:417A は、左から 3 番目～ 6 番目のフィールドから先行ゼロを削除して、2001:0DB8:0:0:8:800:200C:417A のように短縮することができます。ゼロだけを含むフィールド（左から 3 番目と 4 番目のフィールド）は、単一のゼロに短縮されています。左から 5 番目のフィールドでは、3 つの先行ゼロが削除され、単一の 8 がフィールドに残されています。左から 6 番目のフィールドでは、1 つの先行ゼロが削除され、800 がフィールドに残されています。

IPv6 アドレスには、ゼロの 16 進数フィールドがいくつか連続して含まれていることがよくあります。IPv6 アドレスの先頭、中間、または末尾で 2 つのコロン（::）を使用して、ゼロの連続フィールドを圧縮することができます（コロンは、ゼロの 16 進数フィールドが連続していることを表します）。表 D-2 に、さまざまなタイプの IPv6 アドレスでのアドレス圧縮の例をいくつか示します。

表 D-2　IPv6 アドレスの圧縮例

アドレス タイプ	標準形式	圧縮形式
ユニキャスト	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101

表 D-2　IPv6 アドレスの圧縮例 （続き）

アドレス タイプ	標準形式	圧縮形式
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

（注）　ゼロのフィールドが連続することを表す 2 つのコロン（::）は、IPv6 アドレスの中で一度だけ使用できます。

IPv4 アドレスと IPv6 アドレスの両方を含む環境に対処するため、別の IPv6 形式がよく使用されます。その形式は x:x:x:x:x:x:y.y.y.y です。ここで、x は IPv6 アドレスの 6 つの高次の部分の 16 進数値を表し、y はアドレスの 32 ビット IPv4 部分（IPv6 アドレスの残りの 2 つの 16 ビット部分を占める）の 10 進数値を表します。たとえば、IPv4 アドレス 192.168.1.1 は、IPv6 アドレス 0:0:0:0:0:0:FFFF:192.168.1.1 または ::FFFF:192.168.1.1 として表すことができます。

IPv6 アドレス タイプ

次に、IPv6 アドレスの 3 つの主なタイプを示します。

- **ユニキャスト**：ユニキャスト アドレスは、単一インターフェイスの識別子です。ユニキャスト アドレスに送信されたパケットは、そのアドレスで示されたインターフェイスに送信されます。1 つのインターフェイスに複数のユニキャスト アドレスが割り当てられている場合もあります。
- **マルチキャスト**：マルチキャスト アドレスは、インターフェイスのセットを表す識別子です。マルチキャスト アドレスに送信されたパケットは、そのアドレスで示されたすべてのアドレスに送信されます。
- **エニーキャスト**：エニーキャスト アドレスは、インターフェイスのセットを表す識別子です。マルチキャスト アドレスと違い、エニーキャスト アドレスに送信されたパケットは、ルーティング プロトコルの距離測定によって判別された「最も近い」インターフェイスにだけ送信されます。

（注）　IPv6 にはブロードキャスト アドレスはありません。マルチキャスト アドレスにブロードキャスト機能があります。

この項では、次のトピックについて取り上げます。

- 「ユニキャスト アドレス」（P.D-6）
- 「マルチキャスト アドレス」（P.D-9）
- 「エニーキャスト アドレス」（P.D-10）
- 「必須アドレス」（P.D-10）

ユニキャスト アドレス

この項では、IPv6 ユニキャスト アドレスについて説明します。ユニキャスト アドレスは、ネットワーク ノード上のインターフェイスを識別します。

この項では、次のトピックについて取り上げます。

グローバル アドレス

IPv6 グローバル ユニキャスト アドレスの一般的な形式では、グローバル ルーティング プレフィックス、サブネット ID、インターフェイス ID の順に並んでいます。グローバル ルーティング プレフィックスは、別の IPv6 アドレス タイプによって予約されていない任意のプレフィックスです（IPv6 アドレス タイプ プレフィックスについては、「IPv6 アドレス プレフィックス」（P.D-10）を参照してください）。

バイナリ 000 で始まるものを除くすべてのグローバル ユニキャスト アドレスが、Modified EUI-64 形式で 64 ビットのインターフェイス ID を持っています。インターフェイス識別子用の Modified EUI-64 形式の詳細については、「インターフェイス識別子」（P.D-8）を参照してください。

バイナリ 000 で始まるグローバル ユニキャスト アドレスには、アドレスのインターフェイス ID 部分のサイズまたは構造に対する制約がありません。このタイプのアドレスの一例として、IPv4 アドレスが埋め込まれた IPv6 アドレスがあります（「IPv4 互換 IPv6 アドレス」（P.D-7）を参照）。

サイトローカル アドレス

サイトローカル アドレスは、サイト内のアドレッシングに使用されます。このアドレスを使用すると、グローバルに固有なプレフィックスを使用せずにサイト全体をアドレッシングすることができます。サイトローカル アドレスでは、プレフィックス FEC0::/10、54 ビット サブネット ID、64 ビット インターフェイス ID（Modified EUI-64 形式）の順に並んでいます。

サイトローカル ルータは、サイト外の送信元または宛先にサイトローカル アドレスを持つパケットを転送しません。したがって、サイトローカル アドレスは、プライベート アドレスと見なされます。

リンクローカル アドレス

すべてのインターフェイスに、少なくとも 1 つのリンクローカル アドレスが必要です。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

リンクローカル アドレスは、Modified EUI-64 形式でリンクローカル プレフィックス FE80::/10 とインターフェイス識別子を使用して任意のインターフェイスで自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ネイバー探索プロトコルとステートレス自動設定プロセスで使用されます。リンクローカル アドレスを持つノードは、通信が可能です。これらのノードは通信にサイトローカル アドレスまたはグローバルに固有なアドレスを必要としません。

ルータは、送信元または宛先にリンクローカル アドレスを持つパケットを送信しません。したがって、リンクローカル アドレスは、プライベート アドレスと見なされます。

IPv4 互換 IPv6 アドレス

IPv4 アドレスを組み込むことができる IPv6 アドレスのタイプは 2 つあります。

最初のタイプは、「IPv4 互換 IPv6 アドレス」です。IPv6 移行メカニズムには、ホストとルータが IPv4 ルーティング インフラストラクチャで IPv6 パケットを動的にトンネリングする技術が含まれています。この技術を使用する IPv6 ノードには、低次 32 ビットでグローバル IPv4 アドレスを伝送する特別な IPv6 ユニキャスト アドレスが割り当てられます。このタイプのアドレスは「IPv4 互換 IPv6 アドレス」と呼ばれ、形式は ::y.y.y.y です。この y.y.y.y は IPv4 ユニキャスト アドレスになります。

（注）　「IPv4 互換 IPv6 アドレス」で使用する IPv4 アドレスは、グローバルに固有な IPv4 ユニキャスト アドレスである必要があります。

埋め込み IPv4 アドレスを保持する 2 番目のタイプの IPv6 アドレスは、「IPv4 マッピング IPv6 アドレス」と呼ばれます。このアドレス タイプは、IPv4 ノードのアドレスを IPv6 アドレスとして表すために使用されます。このタイプのアドレス形式は ::FFFF:y.y.y.y です。ここで、y.y.y.y は IPv4 ユニキャスト アドレスです。

未指定アドレス

未指定アドレス 0:0:0:0:0:0:0:0 は、IPv6 アドレスがないことを示しています。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。

（注）　IPv6 未指定アドレスは、インターフェイスに割り当てることができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

ループバック アドレス

ループバック アドレス 0:0:0:0:0:0:0:1 は、ノードが IPv6 パケットをそれ自体に送信するために使用できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレス（127.0.0.1）と同じように機能します。

（注）　IPv6 ループバック アドレスは、物理インターフェイスに割り当てることができません。IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。IPv6 ルータは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

インターフェイス識別子

IPv6 ユニキャスト アドレス内のインターフェイス識別子は、リンク上でインターフェイスを識別するために使用されます。これらの識別子は、サブネット プレフィックス内で固有である必要があります。多くの場合、インターフェイス識別子はインターフェイス リンク層アドレスから導出されます。各インターフェイスが異なるサブネットに接続されていれば、単一ノードの複数のインターフェイスで同一のインターフェイス識別子を使用することもできます。

バイナリ 000 で始まるものを除くすべてのユニキャスト アドレスで、インターフェイス識別子は、64 ビットの長さで Modified EUI-64 形式で構築されている必要があります。Modified EUI-64 形式は、アドレス内のユニバーサル/ローカル ビットを逆にし、MAC アドレスの上の 3 つのバイトと下の 3 つのバイトの間に 16 進数 FFFE を挿入することによって、48 ビット MAC アドレスから作成されます。

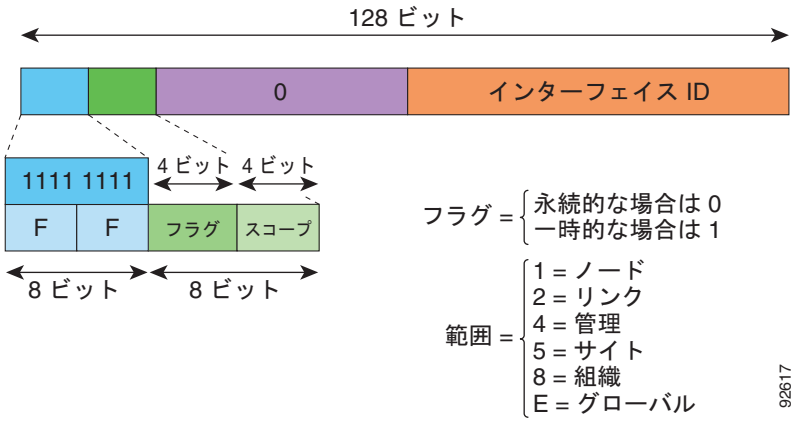
たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビット インターフェイス ID は 02E0:B6FF:FE01:3B7A になります。

マルチキャスト アドレス

IPv6 マルチキャスト アドレスは、通常は異なるノード上にある、インターフェイスのグループの識別子です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。1 つのインターフェイスが任意の数のマルチキャスト グループに属すことができます。

IPv6 マルチキャスト アドレスのプレフィックスは FF00::/8（1111 1111）です。オクテットとそれに続くプレフィックスは、マルチキャスト アドレスのタイプとスコープを定義します。永続的に割り当てられた（「周知の」）マルチキャスト アドレスには、0 に等しいフラグ パラメータがあり、一時的な（「過渡」）マルチキャスト アドレスには 1 に等しいフラグ パラメータがあります。ノード、リンク、サイト、組織のスコープ、またはグローバル スコープを持つマルチキャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、または E です。たとえば、プレフィックスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。図 D-1 に、IPv6 マルチキャスト アドレスの形式を示します。

図 D-1　　IPv6 マルチキャスト アドレス形式



IPv6 ノード（ホストとルータ）は、次のマルチキャスト グループに参加する必要があります。

- All Nodes マルチキャスト アドレス：
  - FF01::（インターフェイスローカル）
  - FF02::（リンクローカル）
- ノード FF02:0:0:0:0:1:FFXX:XXXX/104 上の各 IPv6 ユニキャスト アドレスおよびエニーキャスト アドレスの送信要求ノード アドレス。ここで、XX:XXXX は低次 24 ビットのユニキャスト アドレスまたはエニーキャスト アドレスです。

（注）　送信要求ノード アドレスは、ネイバー送信要求メッセージで使用されます。

IPv6 ルータは、次のマルチキャスト グループに参加する必要があります。

- FF01::2（インターフェイスローカル）
- FF02::2（リンクローカル）
- FF05::2（サイトローカル）

マルチキャスト アドレスは、IPv6 パケットで送信元アドレスとして使用できません。

（注）　IPv6 にはブロードキャスト アドレスはありません。ブロードキャスト アドレスの代わりに IPv6 マルチキャスト アドレスが使用されます。

エニーキャスト アドレス

IPv6 エニーキャスト アドレスは、複数のインターフェイス（通常は異なるノードに属す）に割り当てられたユニキャスト アドレスです。エニーキャスト アドレスにルーティングされたパケットは、そのアドレスを持ち、有効なルーティング プロトコルによって最も近いと判別されたインターフェイスにルーティングされます。

エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられます。エニーキャスト アドレスは、複数のインターフェイスに割り当てられたユニキャスト アドレスにすぎません。インターフェイスは、アドレスをエニーキャスト アドレスとして認識するように設定されている必要があります。

エニーキャスト アドレスには次の制限が適用されます。

- エニーキャスト アドレスは、IPv6 パケットの送信元アドレスとして使用できません。
- エニーキャスト アドレスは、IPv6 ホストに割り当てることはできません。IPv6 ルータにだけ割り当てるこができます。

（注）　エニーキャスト アドレスは、セキュリティ アプライアンスではサポートされていません。

必須アドレス

IPv6 ホストには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 各インターフェイスのリンクローカル アドレス
- ループバック アドレス
- All-Nodes マルチキャスト アドレス
- 各ユニキャスト アドレスまたはエニーキャスト アドレスの送信要求ノード マルチキャスト アドレス

IPv6 ルータには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 必須ホスト アドレス
- ルータとして動作するように設定されているすべてのインターフェイスのサブネットルータ エニーキャスト アドレス
- All-Routers マルチキャスト アドレス

IPv6 アドレス プレフィックス

ipv6-prefix/prefix-length 形式の IPv6 アドレス プレフィックスを使用すると、アドレス空間全体のビット単位の連続ブロックを表現できます。IPv6-prefix は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 プレフィックスは、IPv6 アドレスのタイプを特定します。表 D-3 に、各 IPv6 アドレス タイプのプレフィックスを示します。

表 D-3　IPv6 アドレス タイプのプレフィックス

アドレス タイプ	バイナリ プレフィックス	IPv6 表記
未指定	000...0（128 ビット）	::/128
ループバック	000...1（128 ビット）	::1/128
マルチキャスト	11111111	FF00::/8
リンクローカル（ユニキャスト）	1111111010	FE80::/10
サイトローカル（ユニキャスト）	1111111111	FEC0::/10
グローバル（ユニキャスト）	その他すべてのアドレス。	
エニーキャスト	ユニキャスト アドレス空間から取得。	

プロトコルとアプリケーション

表 D-4 に、プロトコルのリテラル値とポート番号を示します。いずれもセキュリティ アプライアンスのコマンドで入力できます。

表 D-4　プロトコルのリテラル値

リテラル	値	説明
ah	51	IPv6 の認証ヘッダー（RFC 1826）。
eigrp	88	Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）。
esp	50	IPv6 の暗号ペイロード（RFC 1827）。
gre	47	総称ルーティング カプセル化。
icmp	1	インターネット制御メッセージ プロトコル（RPC 792）。
icmp6	58	IPv6 のインターネット制御メッセージ プロトコル（RFC 2463）。
igmp	2	インターネット グループ管理プロトコル（RFC 1112）。
igrp	9	Interior Gateway Routing Protocol。
ip	0	インターネット プロトコル。
ipinip	4	IP-in-IP カプセル化。
ipsec	50	IP セキュリティ。ipsec プロトコル リテラルを入力すると、esp プロトコル リテラルを入力した場合と同じ結果が得られます。

表 D-4　プロトコルのリテラル値 （続き）

リテラル	値	説明
nos	94	ネットワーク オペレーティング システム（Novell の NetWare）。
ospf	89	OSPF ルーティング プロトコル（RFC 1247）。
pcp	108	ペイロード圧縮プロトコル。
pim	103	プロトコル独立型マルチキャスト。
pptp	47	ポイントツーポイント トンネリング プロトコル。pptp プロトコル リテラルを入力すると、gre プロトコル リテラルを入力した場合と同じ結果が得られます。
snp	109	Sitara Networks Protocol。
tcp	6	伝送制御プロトコル（RFC 793）。
udp	17	ユーザ データグラム プロトコル（RFC 768）。

プロトコル番号は、次の IANA Web サイトで確認できます。

http://www.iana.org/assignments/protocol-numbers

TCP ポートと UDP ポート

表 D-5 に、リテラル値とポート番号を示します。いずれもセキュリティ アプライアンスのコマンドで入力できます。次の警告を参照してください。

- セキュリティ アプライアンスは、SQL*Net 用にポート 1521 を使用します。これは、Oracle が SQL*Net に使用するデフォルトのポートです。ただし、この値は IANA ポート割り当てとは一致しません。
- セキュリティ アプライアンスは、ポート 1645 と 1646 で RADIUS をリスンしています。RADIUS サーバが標準ポート 1812 と 1813 を使用している場合は、**authentication-port** コマンドと **accounting-port** コマンドを使用して、それらのポートでリスンするようにセキュリティ アプライアンスを設定できます。
- DNS アクセスにポートを割り当てるには、**dns** ではなく **domain** リテラル値を使用します。**dns** を使用した場合、セキュリティ アプライアンスでは、**dnsix** リテラル値を使用すると見なされます。

ポート番号は、次の URL で IANA の Web サイトにアクセスしてオンラインで参照できます。

http://www.iana.org/assignments/port-numbers

表 D-5　ポートのリテラル値

リテラル	TCP または UDP?	値	説明
aol	TCP	5190	America Online
bgp	TCP	179	ボーダー ゲートウェイ プロトコル（RFC 1163）
biff	UDP	512	新しいメールの受信をユーザに通知するために、メール システムが使用
bootpc	UDP	68	ブートストラップ プロトコル クライアント

表 D-5　ポートのリテラル値 （続き）

リテラル	TCP または UDP?	値	説明
bootps	UDP	67	ブートストラップ プロトコル サーバ
chargen	TCP	19	キャラクタ ジェネレータ
citrix-ica	TCP	1494	Citrix Independent Computing Architecture（ICA）プロトコル
cmd	TCP	514	**cmd** は自動認証機能がある点を除いて、**exec** と同様
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time（日時）（RFC 867）
discard	TCP、UDP	9	廃棄
domain	TCP、UDP	53	DNS
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
echo	TCP、UDP	7	Echo
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	Finger
ftp	TCP	21	ファイル転送プロトコル（コンソール ポート）
ftp-data	TCP	20	ファイル転送プロトコル（データ ポート）
gopher	TCP	70	Gopher
https	TCP	443	HTTP over SSL
h323	TCP	1720	H.323 コール シグナリング
hostname	TCP	101	NIC ホスト ネーム サーバ
ident	TCP	113	ID 認証サービス
imap4	TCP	143	Internet Message Access Protocol バージョン 4
irc	TCP	194	インターネット リレー チャット プロトコル
isakmp	UDP	500	Internet Security Association and Key Management Protocol
kerberos	TCP、UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn シェル
ldap	TCP	389	Lightweight Directory Access Protocol。
ldaps	TCP	636	ライトウェイト ディレクトリ アクセス プロトコル（SSL）
lpd	TCP	515	ライン プリンタ デーモン（プリンタ スプーラー）
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	モバイル IP エージェント
nameserver	UDP	42	ホスト ネーム サーバ
netbios-ns	UDP	137	NetBIOS ネーム サービス

表 D-5　ポートのリテラル値 （続き）

リテラル	TCP または UDP?	値	説明
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	ネットワーク タイム プロトコル
pcanywhere-status	UDP	5632	pcAnywhere ステータス
pcanywhere-data	TCP	5631	pcAnywhere データ
pim-auto-rp	TCP、UDP	496	Protocol Independent Multicast、逆パス フラッド、デンス モード
pop2	TCP	109	Post Office Protocol（POP）Version 2
pop3	TCP	110	Post Office Protocol - Version 3
pptp	TCP	1723	ポイントツーポイント トンネリング プロトコル
radius	UDP	1645	リモート認証ダイヤルイン ユーザ サービス
radius-acct	UDP	1646	リモート認証ダイヤルイン ユーザ サービス（アカウンティング）
rip	UDP	520	ルーティング情報プロトコル
secureid-udp	UDP	5510	SecureID over UDP
smtp	TCP	25	シンプル メール転送プロトコル
snmp	UDP	161	簡易ネットワーク管理プロトコル
snmptrap	UDP	162	簡易ネットワーク管理プロトコル（トラップ）
sqlnet	TCP	1521	構造化照会言語ネットワーク
ssh	TCP	22	セキュア シェル
sunrpc (rpc)	TCP、UDP	111	Sun Remote Procedure Call
syslog	UDP	514	システム ログ
tacacs	TCP、UDP	49	Terminal Access Controller Access Control System Plus
talk	TCP、UDP	517	Talk
telnet	TCP	23	Telnet（RFC 854）
tftp	UDP	69	Trivial File Transfer Protocol
time	UDP	37	Time
uucp	TCP	540	UNIX 間コピー プログラム
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP	80	ワールドワイド ウェブ
xdmcp	UDP	177	X Display Manager Control Protocol

ローカル ポートとプロトコル

表 D-6 に、セキュリティ アプライアンスに向かうトラフィックを処理するためにセキュリティ アプライアンスが開くプロトコル、TCP ポート、および UDP ポートを示します。表 D-6 に記載されている機能とサービスをイネーブルにしない限り、セキュリティ アプライアンスは、TCP または UDP ポートでローカル プロトコルを*開きません*。セキュリティ アプライアンスがデフォルトのリスニング プロトコルまたはポートを開くように機能またはサービスを設定する必要があります。多くの場合、機能またはサービスをイネーブルにすると、デフォルト ポート以外のポートを設定できます。

表 D-6　機能とサービスによって開かれるプロトコルとポート

機能またはサービス	プロトコル	ポート番号	コメント
DHCP	UDP	67、68	—
フェールオーバー制御	108	該当なし	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	該当なし	—
IGMP	2	該当なし	プロトコルは宛先 IP アドレス 224.0.0.1 でだけ開かれます。
ISAKMP/IKE	UDP	500	設定可能。
IPSec (ESP)	50	該当なし	—
IPSec over UDP (NAT-T)	UDP	4500	—
IPSec over UDP（Cisco VPN 3000 シリーズ互換）	UDP	10000	設定可能。
IPSec over TCP (CTCP)	TCP	—	デフォルト ポートは使用されません。IPSec over TCP の設定時にポート番号を指定する必要があります。
NTP	UDP	123	—
OSPF	89	該当なし	プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でだけ開かれます。
PIM	103	該当なし	プロトコルは宛先 IP アドレス 224.0.0.13 でだけ開かれます。
RIP	UDP	520	—
RIPv2	UDP	520	ポートは宛先 IP アドレス 224.0.0.9 でだけ開かれます。
SNMP	UDP	161	設定可能。
SSH	TCP	22	—
ステートフル アップデート	105	該当なし	—
Telnet	TCP	23	—

表 D-6　機能とサービスによって開かれるプロトコルとポート （続き）

機能またはサービス	プロトコル	ポート番号	コメント
VPN ロード バランシング	UDP	9023	設定可能。
VPN 個別ユーザ認証プロキシ	UDP	1645、1646	ポートは VPN トンネルでだけアクセスできます。

ICMP タイプ

表 D-7 に、セキュリティ アプライアンスのコマンドで入力できる ICMP タイプの番号と名前を示します。

表 D-7　ICMP タイプ

ICMP 番号	ICMP 名
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect