アドレス、プロトコル、およびポート

この付録は、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 リファレンスです。ここで説明する内容は次のとおりです。

IPv4 アドレスおよびサブネット マスク

ここでは、FWSM で IPv4 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 進数で表記される 32 ビットの数値です。バイナリから 10 進数に変換された 4 つの 8 ビット フィールド（オクテット）が、ドットで区切られて表記されます。IP アドレスの最初のパートはホストが存在するネットワークを識別し、2 つめのパートは特定ネットワーク上の特定ホストを識別します。ネットワーク番号フィールドは、ネットワーク プレフィクスと呼ばれます。特定ネットワーク上のホストはすべて同じネットワーク プレフィクスを共有しますが、ホスト番号は固有でなければなりません。クラスフル IP では、アドレスのクラスによって、ネットワーク プレフィクスとホスト番号を区切る位置が異なります。

次の内容について説明します。

クラス

IP ホスト アドレスは 3 つの異なるアドレス クラスに分けられています。クラス A、クラス B、およびクラス C です。各クラスは、32 ビット アドレス内のネットワーク プレフィクスとホスト番号の区切り箇所がそれぞれ異なります。クラス D アドレスは、マルチキャスト IP 専用です。

- クラス 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 プレフィクスとして使用します。
- クラス 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 プレフィクスとして使用します。
- クラス 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 プレフィクスとして使用します。

クラス A アドレスには 16,777,214 のホスト アドレス、クラス B には 65,534 のホスト アドレスが存在するので、サブネット マスクを使用して、これらの巨大なネットワークを、より小さなサブネットに分割できます。

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で、これらをインターネット上にルーティングする必要がない場合には、Internet Assigned Numbers Authority（IANA）が推奨しているプライベート IP アドレスを使用できます（RFC 1918 を参照）。プライベート ネットワークに使用できるアドレス範囲は、次のとおりです。これらのアドレスはアドバタイズすべきではありません。

- 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、単一のクラス A、クラス B、またはクラス 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 マスクでは、ホスト番号のビットをネットワーク プレフィクスに追加して、拡張ネットワーク プレフィクスを作成できます。たとえば、クラス C のネットワーク プレフィクスには、常に IP アドレスの最初の 3 オクテットが使用されます。クラス C 拡張ネットワーク プレフィクスの場合には、さらに 4 つめのオクテットの一部が使用されます。

サブネット マスクは、ドット付き 10 進数ではなくバイナリ表記を使用するほうが簡単に理解できます。サブネット マスク内のビットは、インターネット アドレスと 1 対 1 で対応しています。

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

例 1 : クラス B アドレス 129.10.0.0 について、3 つめのオクテット全部をホスト番号ではなく拡張ネットワーク プレフィクスに使用したい場合、サブネット マスク 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、クラス B アドレスは、最後のオクテットだけをホスト番号に使用するクラス C アドレスと同等になります。

例 2 : 3 つめのオクテットの一部だけを拡張ネットワーク プレフィクスに使用したい場合には、サブネット マスクを 11111111.11111111.11111000.00000000 などのように指定します。この場合、3 つめ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*）マスクで記述できます。例 1 の場合、ドット付き 10 進数マスクにすると、各バイナリ オクテットを 10 進数に変換した 255.255.255.0 になります。*/ ビット* マスクの場合、1 の数を指定するため、/24 になります。例 2 の場合、ドット付き 10 進数は 255.255.248.0、/ ビットは /21 です。

また、3 つめ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することによって、複数のクラス C ネットワークを、より大規模なネットワークに統合することもできます（たとえば、192.168.0.0/20）。

次の内容について説明します。

- 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-4）

サブネット マスクの判別

使用したいホスト数に適したサブネット 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

ホスト数[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 クラス A ネットワーク
65,536	/16	255.255.0.0 クラス 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

表 D-1　ホスト、ビット、およびドット付き 10 進数マスク（続き）

ホスト数[1]	/ ビット マスク	ドット付き 10 進数マスク
512	/23	255.255.254.0
256	/24	255.255.255.0 クラス 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
未使用	/31	255.255.255.254
1	/32	255.255.255.255 単一ホスト アドレス

1. 単一ホストである /32 を除き、サブネットの最初と最後の番号は予約済みです。

サブネット マスクで使用するアドレスの判別

ここでは、クラス C およびクラス B 規模のネットワークにサブネット マスクを適用する場合、使用できるネットワーク アドレスを判別する方法を示します。次の内容について説明します。

- クラス C 規模のネットワーク アドレス（p.D-4）
- クラス B 規模のネットワーク アドレス（p.D-5）

クラス C 規模のネットワーク アドレス

2 ～ 254 のホスト数のネットワークでは、4 つめのオクテットが 0 から始まり、ホスト アドレス数の倍数になります。次に、192.168.0.x の 8 ホストのサブネット（/29）の例を示します。

マスク /29（255.255.255.248）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済みです。最初のサブネットの例では、192.168.0.0 または 192.168.0.7 は使用できません。

クラス B 規模のネットワーク アドレス

ホスト数が 254 ～ 65,534 のネットワークにサブネット マスクを適用する場合、使用するネットワーク アドレスを判別するには、使用できる各拡張ネットワーク プレフィクスについて、3 つめのオクテットの値を決定する必要があります。たとえば、10.1.*x*.0 のようなアドレスのサブネットを作成する場合、最初の 2 つのオクテットは拡張ネットワーク プレフィクスに使用されるので固定され、4 つめのオクテットの全ビットがホスト番号に使用されます。

3 つめのオクテットの値を決定する手順は、次のとおりです。

ステップ 1　65,536（3 つめと 4 つめのオクテットで使用できるアドレスの総数）を使用したいホスト アドレス数で割って、ネットワークに作成できるサブネット数を計算します。

たとえば、65,536 を 4096 で割った値は 16 です。

したがって、クラス B ネットワークに、それぞれ 4096 のアドレスを持つ 16 のサブネットを作成できます。

ステップ 2　256（3 つめのオクテットの値の数）をサブネット数で割って、3 つめのオクテット値の倍数を算出します。

この例では、256/16 = 16 です。

3 つめのオクテットは、0 から開始され、16 の倍数になります。

次に、ネットワーク 10.1 の 16 のサブネットを示します。

マスク /20（255.255.240.0）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済みです。最初のサブネットの例では、10.1.0.0 または 10.1.15.255 は使用できません。

IPv6 アドレス

IPv6 は IPv4 の次世代のインターネット プロトコルです。アドレス スペースが拡張され、ヘッダー フォーマットが簡素化され、拡張やオプション、フロー ラベリング機能、認証やプライバシー機能のサポートが向上しています。IPv6 は RFC 2460 で規定されています。IPv6 のアドレス指定アーキテクチャは RFC 3513 で規定されています。

ここでは、IPv6 アドレス フォーマットとアーキテクチャについて説明します。内容は次のとおりです。

（注）　ここでは、IPv6 のアドレス フォーマット、タイプ、プレフィクスについて説明します。FWSM で IPv6 を使用するよう設定する方法については、第 9 章「IPv6 の設定」を参照してください。

IPv6 アドレス フォーマット

IPv6 アドレスは、コロン（:）で区切った 8 個の 16 ビット 16 進数フィールドで表現されます。x:x:x:x:x:x:x:x というフォーマットになります。IPv6 アドレスの例を 2 つ挙げます。

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

（注）　IPv6 アドレスの 16 進数の文字では、大文字と小文字は区別されません。

アドレスの個々のフィールドで、先行 0 は記述する必要がありません。しかし、各フィールドに 1 桁以上の値を入力する必要があります。そのため、アドレスの例 2001:0DB8:0000:0000:0008:0800:200C:417A の場合、左から 3 番めから 6 番めのフィールドの先行 0 を省略して、2001:0DB8:0:0:8:800:200C:417A とすることができます。すべてが 0 のフィールド（左から 3 番めと 4 番め）は、1 個の 0 として表現できます。左から 5 番めのフィールドは 3 個の先行 0 を省略して 8 だけを残し、左から 6 番めのフィールドは 1 個の先行 0 を省略して 800 だけを残しています。

いくつかの連続する 16 進数の 0 のフィールドを持つことは、IPv6 のアドレスに一般的に見られることです。2 個のコロン（::）を使用して、IPv6 アドレスの最初、中間、最後の連続する 0 のフィールドを圧縮することができます（コロンは連続する 16 進数の 0 のフィールドを示します）。表 D-2 に、各種 IPv6 アドレスのアドレス圧縮の例を示します。

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
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）　連続した 0 のフィールドを示すために IPv6 アドレスで 2 つのコロン（::）を使用できるのは 1 回のみです。

IPv4 と IPv6 が混在する環境では、別の IPv6 フォーマットも使用されます。そのフォーマットは x:x:x:x:x:x:y.y.y.y です。ここで、x は IPv6 の上位 6 個の部分を示す 16 進数の値で、y は 32 ビットの IPv4 アドレス部分を示す 10 進数の値（IPv6 アドレスの残りの 2 つの 16 ビット部分を利用）です。たとえば、192.168.1.1 という IPv4 アドレスは、IPv6 アドレスで 0:0:0:0:0:0:FFFF:192.168.1.1 または ::FFFF:192.168.1.1 と表現できます。

IPv6 アドレス タイプ

IPv6 アドレスの主要タイプは、次の 3 つです。

- **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るパケットは、このアドレスで識別されるインターフェイスに伝送されます。1 つのインターフェイスには、複数のユニキャスト アドレスを割り当てることができます。
- **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るパケットは、このアドレスで識別されるすべてのアドレスに伝送されます。
- **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 アドレスと異なり、エニーキャスト アドレスに送信されるパケットは、ルーティング プロトコルの距離測定に従って、「直近の」インターフェイスにのみ伝送されます。

（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 アドレスがブロードキャスト機能を提供します。

次の内容について説明します。

ユニキャスト アドレス

ここでは、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示します。

次の内容について説明します。

グローバル アドレス

IPv6 グローバル ユニキャスト アドレスの一般フォーマットは、グローバル ルーティング プレフィクス、サブネット ID、インターフェイス ID を順に並べた形になります。グローバル ルーティング プレフィクスには、IPv6 アドレス タイプで予約されているものを除いて、任意のプレフィクスを使用できます（IPv6 アドレス タイプのプレフィクスの詳細については、「IPv6 アドレス プレフィクス」[p.D-12] を参照）。

グローバル ユニキャスト アドレス（バイナリ 000 で始まるものを除く）は、Modified EUI-64 フォーマットの 64 ビット インターフェイス ID を持ちます。インターフェイス識別子の Modified EUI-64 フォーマットの詳細については、「インターフェイス識別子」（p.D-9）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 アドレスは、アドレスのインターフェイス ID 部分のサイズや構成について、制約はありません。このタイプのアドレスの一例は、IPv4 アドレスが組み込まれた IPv6 アドレスです（「IPv4 互換 IPv6 アドレス」[p.D-8] 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、サイト内のアドレス指定に使用されます。グローバルに一意なプレフィクスを使用しなくても、サイト全体のアドレス指定が行えます。サイトローカル アドレスは、プレフィクス FEC0::/10 のあとに、54 ビットのサブネット ID、Modified EUI-64 フォーマットの 64 ビットのインターフェイス ID が続きます。

サイトローカル ルータは、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サイト外部に転送しません。そのため、サイトローカル アドレスはプライベート アドレスと考えられます。

リンクローカル アドレス

インターフェイスには、少なくとも 1 つのリンクローカル アドレスが必要です。各インターフェイスに複数の 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、リンクローカル プレフィクス FE80::/10 と Modified EUI-64 フォーマットのインターフェイス識別子によって任意のインターフェイス上で自動的に設定される 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、Neighbor Discovery Protocol およびステートレス自動コンフィギュレーション 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、通信用のサイトローカル アドレスまたはグローバルに一意なアドレスがなくても、通信が可能です。

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転送しません。そのため、リンクローカル アドレスはプライベート アドレスと考えられます。

IPv4 互換 IPv6 アドレス

IPv4 アドレスの組み込みが可能な IPv6 アドレスは、2 種類あります。

1 つめのタイプは、「IPv4 互換 IPv6 アドレス」です。IPv6 移行メカニズムでは、ホストとルータで IPv4 ルーティング インフラストラクチャ上を IPv6 パケットをダイナミックにトンネリングさせる技法が取られています。この技法を使用した IPv6 ノードには、下位 32 ビットにグローバル IPv4 アドレスを組み込んだ特別な 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、フォーマットは ::y.y.y.y です。y.y.y.y が IPv4 ユニキャスト アドレスです。

（注）「IPv4 互換 IPv6 アドレス」で使用される IPv4 アドレスは、グローバルに一意な IPv4 ユニキャスト アドレスでなければなりません。

2 つめのタイプの IPv6 アドレスは、Ipv4 アドレスが組み込まれており、「IPv4 マップ 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 アドレスとして表現するために使用します。このタイプのアドレス フォーマットは、::FFFF:y.y.y.y です。y.y.y.y が 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ます。たとえば、IPv6 ネットワークで新しく初期化したノードは、IPv6 アドレスを受信するまで、パケットの送信元アドレスとして未指定アドレスを使用することができます。

（注）IPv6 未指定アドレスは、インターフェイスには割り当てることができません。未指定 IPv6 アドレスは、IPv6 パケットまたは IPv6 ルーティング ヘッダーの宛先アドレスとして使用しないでください。

ループバック アドレス

ノードで IPv6 パケットを自分宛に送信するため、ループバック アドレス 0:0:0:0:0:0:0:1 を使用することができます。IPv6 のループバック アドレスの機能は、IPv4 のループバック アドレス（127.0.0.1）と同じです。

（注）IPv6 ループバック アドレスは、物理インターフェイスには割り当てることができません。送信元アドレスまたは宛先アドレスとして IPv6 ループバック アドレスを持つパケットは、パケットを作成したノードの外部に転送されないようにする必要があります。IPv6 ルータは、送信元アドレスまたは宛先アドレスに IPv6 ループバック アドレスを持つ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 アドレスのインターフェイス識別子は、リンク上でのインターフェイスの識別に使用されます。これは、サブネット プレフィクス内で一意でなければなりません。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のリンク層アドレスに基づいて作成されます。インターフェイスが異なるサブネットに属していれば、同じインターフェイス識別子をシングル ノードの複数のインターフェイスで使用することができます。

ユニキャスト アドレス（バイナリ 000 で始まるものを除く）の場合、インターフェイス識別子は 64 ビットの Modified EUI-64 フォーマットで構成する必要があります。Modified EUI-64 フォーマットは、アドレスのユニバーサル / ローカル ビットを反転し、MAC アドレスの上位 3 バイトと下位 3 バイトの間に 16 進数の FFFE を挿入することにより、48 ビット MAC アドレスから生成されます。

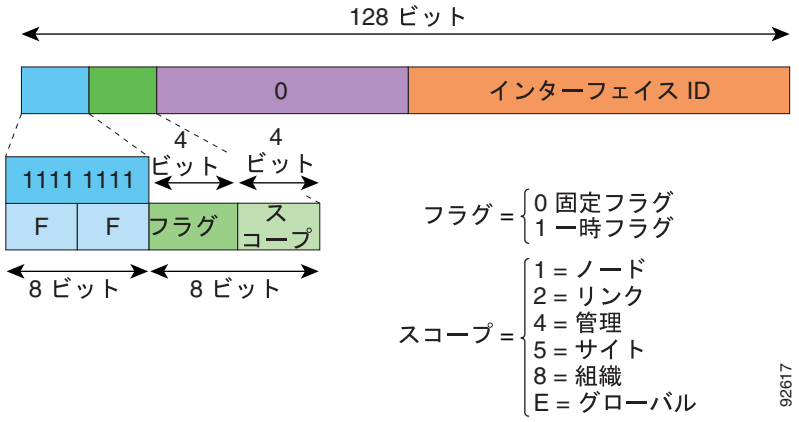
たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビットのインターフェイス ID は 02E0:B6FF:FE01:3B7A となります。

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るパケットは、このマルチキャスト アドレスで示されるすべてのアドレスに伝送されます。1 つのインターフェイスは、任意の数のマルチキャスト グループに属することができます。

IPv6 マルチキャスト アドレスのプレフィクスは FF00::/8（1111 1111）です。プレフィクスに続くオクテットは、マルチキャスト アドレスのタイプとスコープを定義するためのものです。永久に割り当てられる（「既知」）マルチキャスト アドレスにはフラグ パラメータ 0 が割り当てられ、一時（「一時的」）マルチキャスト アドレスにはフラグ パラメータ 1 が割り当てられます。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 アドレスは、それぞれ 1、2、5、8、E のスコープ パラメータを持ちます。たとえば、プレフィクスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永久マルチキャスト アドレスです。図 D-1 に、IPv6 マルチキャスト アドレスのフォーマットを示します。

図 D-1　　IPv6 マルチキャスト アドレス フォーマット



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

- 全ノードのマルチキャスト 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）
- ノード上の各 IPv6 ユニキャスト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 FF02:0:0:0:0:1:FFXX:XXXX/104。XX:XXXX はユニキャストまたはエニーキャスト アドレスの下位 24 ビット

（注）　送信要求ノード アドレスは、ネイバの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 グループに加入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 パケットの送信元アドレスとして使用することはできません。

（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、異なるノードに属する）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るパケットは、そのアドレスを持つ直近のインターフェイスにルーティングされます。直近インターフェイスは、有効なルーティング プロトコルに基づいて判断されます。

エニーキャスト アドレスはユニキャスト アドレス スペース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 アドレスで、その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インターフェイスを設定する必要があります。

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することはできません。
- 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 ルータへの割り当てだけが可能です。

（注）　FWSM では、エニーキャスト アドレス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、次のアドレスを設定する必要があります（自動または手動で）。

- 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
- 全ノードのマルチキャスト アドレス
- 各ユニキャスト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、次のアドレスを設定する必要があります（自動または手動で）。

- 必須ホスト アドレス
- 全インターフェイスのルータとして動作するよう設定したサブネットルータのエニーキャスト アドレス
- 全ルータのマルチキャスト アドレス

IPv6 アドレス プレフィクス

アドレス スペース全体の連続するビット ブロックを示すため、ipv6-prefix/prefix-length というフォーマットの IPv6 アドレス プレフィックスを使用することができます。IPv6 のプレフィックスは、RFC 2373 に規定された形式でなければなりません。RFC 2373 では、アドレスは 16 ビットの値をコロンで区切った 16 進数で指定されています。プレフィクス長は、プレフィクスを構成するアドレスの上位の連続ビット（アドレスのネットワーク部分）の桁数を示す 10 進数の値です。たとえば、2001:0DB8:8086:6502::/32 は IPv6 プレフィクスとして有効です。

IPv6 プレフィクスは IPv6 アドレスのタイプを識別するためのものです。表 D-3 に、IPv6 の各アドレス タイプのプレフィクスを示します。

表 D-3　IPv6 アドレス タイプのプレフィクス

アドレス タイプ	バイナリ プレフィクス	IPv6 の表記
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）	その他のアドレス	
エニーキャスト	ユニキャスト アドレス スペースから取得	

プロトコルおよびアプリケーション

表 D-4 に、プロトコルの文字名およびポート番号を示します。どちらも、FWSM のコマンドに入力できます。

表 D-4　プロトコルの文字名

文字名	番号	説明
ah	51	IPv6 の認証ヘッダー、RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	IPv6 の Encapsulated Security Payload（カプセル化セキュリティ ペイロード）、RFC 1827
gre	47	Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）
icmp	1	Internet Control Message Protocol、RFC 792
icmp6	58	IPv6 の Internet Control Message Protocol、RFC 2463
igmp	2	Internet Group Management Protocol、RFC 1112
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol
ipinip	4	IP-in-IP カプセル化
ipsec	50	IP セキュリティ。ipsec プロトコルの文字の入力は、esp プロトコルの文字の入力と同じです。
nos	94	Network Operating System（Novell NetWare）
ospf	89	Open Shortest Path First（OSPF）ルーティング プロトコル、RFC 1247
pcp	108	Payload Compression Protocol
pim	103	Protocol Independent Multicast
pptp	47	Point-to-Point Tunneling Protocol（ポイントツーポイント トンネリング プロトコル）。pptp プロトコルの文字の入力は、gre プロトコルの文字の入力と同じです。
snp	109	Sitara Networks Protocol
tcp	6	TCP、RFC 793
udp	17	UDP、RFC 768

プロトコル番号は、IANA の Web サイトからオンラインで表示できます。

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

TCP ポートおよび UDP ポート

表 D-5 に、文字名およびポート番号を示します。どちらも、FWSM のコマンドに入力できます。次の事項に注意してください。

- FWSM は、SQL*Net 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 のポート割り当てと一致していません。
- FWSM は、ポート 1645 および 1646 で RADIUS を待ち受けます。RADIUS サーバが標準ポート 1812 および 1813 を使用している場合、**authentication-port** および **accounting-port** コマンドを使用して、これらのポートを待ち受けるよう FWSM を設定することができます。
- ポートに DNS アクセスを割り当てる場合には、**dns** ではなく、**domain** 文字名を使用してください。**dns** を使用した場合、FWSM では **dnsix** 文字名が使用されたとみなされます。

ポート番号は、IANA の Web サイトからオンラインで表示できます。

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

表 D-5　ポートの文字名

文字名	TCP/UDP	番号	説明
aol	TCP	5190	America Online
bgp	TCP	179	Border Gateway Protocol（BGP）、RFC 1163
biff	UDP	512	新着メールをユーザに通知するメール システムで使用
bootpc	UDP	68	ブートストラップ プロトコル クライアント
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	**exec** と同様だが、**cmd** は自動認証をサポート
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	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	エコー
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	フィンガ
ftp	TCP	21	FTP（ファイル転送プロトコル）（制御ポート）
ftp-data	TCP	20	FTP（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	Ident 認証サービス
imap4	TCP	143	Internet Message Access Protocol（IMAP）Version 4
irc	TCP	194	Internet Relay Chat Protocol
isakmp	UDP	500	Internet Security Association and Key Management Protocol（ISAKMP）

表 D-5　ポートの文字名（続き）

文字名	TCP/UDP	番号	説明
kerberos	TCP、UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	Lightweight Directory Access Protocol
ldaps	TCP	636	Lightweight Directory Access Protocol（SSL）
lpd	TCP	515	Line Printer Deamon ― プリンタ スプーラ
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	Mobile 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
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（NNTP）
ntp	UDP	123	Network Time Protocol（NTP）
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、リバース パス フラッディング、dense（密）モード
pop2	TCP	109	POP Version 2
pop3	TCP	110	POP Version 3
pptp	TCP	1723	Point-to-Point Tunneling Protocol（PPTP）
radius	UDP	1645	Remote Authentication Dial-In User Service（RADIUS）
radius-acct	UDP	1646	RADIUS（アカウンティング）
rip	UDP	520	Routing Information Protocol（RIP）
secureid-udp	UDP	5510	SecureID over UDP
smtp	TCP	25	Simple Mail Transport Protocol（SMTP）
snmp	UDP	161	SNMP（簡易ネットワーク管理プロトコル）
snmptrap	UDP	162	SNMP ― トラップ
sqlnet	TCP	1521	Structured Query Language（SQL）ネットワーク
ssh	TCP	22	Secure Shell
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（TACACS+）
talk	TCP、UDP	517	Talk
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	TFTP（簡易ファイル転送プロトコル）
time	UDP	37	Time
uucp	TCP	540	UNIX-to-UNIX Copy Program（UUCP）
who	UDP	513	Who

表 D-5　ポートの文字名（続き）

文字名	TCP/UDP	番号	説明
whois	TCP	43	Who Is
www	TCP	80	WWW
xdmcp	UDP	177	X Display Manager Control Protocol

ローカル ポートおよびプロトコル

表 D-6 に、FWSM 宛に送信されたトラフィックを処理するために FWSM がオープンするプロトコル、TCP ポート、UDP ポートの一覧を示します。表 D-6 に示した機能とサービスをイネーブルにしないと、FWSM はローカル プロトコル、TCP ポート、UDP ポートをオープンしません。FWSM でデフォルトのリスニング プロトコルまたはポートをオープンするには、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場合、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りオープンされるプロトコルおよびポート

機能またはサービス	プロトコル	ポート番号	説明
DHCP	UDP	67、68	—
フェールオーバー制御	108	適用外	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	適用外	—
IGMP	2	適用外	プロトコルは宛先 IP アドレス 224.0.0.1 でのみオープン
ISAKMP/IKE	UDP	500	設定可能
IPSec（ESP）	50	適用外	—
NTP	UDP	123	—
OSPF	89	適用外	プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でのみオープン
PIM	103	適用外	プロトコルは宛先 IP アドレス 224.0.0.13 でのみオープン
RIP	UDP	520	—
RIPv2	UDP	520	プロトコルは宛先 IP アドレス 224.0.0.9 でのみオープン
SNMP	UDP	161	設定可能
SSH	TCP	22	—
ステートフル アップデート	105	適用外	—
Telnet	TCP	23	—

ICMP のタイプ

表 D-7 に、FWSM のコマンドに入力できる ICMP のタイプ番号および名前を示します。

表 D-7　ICMP のタイプ

ICMP 番号	ICMP 名
0	echo-reply（エコー応答）
3	unreachable（到達不能）
4	source-quench
5	redirect（リダイレクト）
6	alternate-address（代替アドレス）
8	echo（エコー）
9	router-advertisement（ルータ アドバタイズ）
10	router-solicitation（ルータ送信要求）
11	time-exceeded（時間超過）
12	parameter-problem（パラメータの問題）
13	timestamp-request（タイムスタンプ要求）
14	timestamp-reply（タイムスタンプ応答）
15	information-request（情報要求）
16	information-reply（情報応答）
17	mask-request（マスク要求）
18	mask-reply（マスク応答）
31	conversion-error（変換エラー）
32	mobile-redirect（モバイル リダイレクト）