アドレス、プロトコル、およびポート

この章では、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。

IPv4 アドレスとサブネット マスク

この項では、ASA 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。

クラス

IP ホスト アドレスは、Class A、Class B、Class C の 3 つの異なるアドレス クラスに分かれています。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決定します。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、最初のオクテットのみをネットワーク 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、インターネット割り当て番号局（IANA）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 プレフィックスの一部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 です。

サブネットマスクの決定

必要なホストの数に基づいてサブネットマスクを決定するには、次の表を参照してください。

（注） 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。

表 *1*：ホスト、ビット、ドット区切りの *10* 進数マスク

ホスト	/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

ホスト	/ビットマスク	ドット付き 10 進数マスク
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

サブネットマスクに使用するアドレスの決定

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。

クラス C 規模ネットワーク 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。例として、次の表に 8 個のホストを持つサブネット（/29）、192.168.0.x を示します。

（注） 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。

表 *2:* クラス *C* 規模ネットワーク アドレス

マスク /29（255.255.255.248）でのサブネット	アドレス範囲
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

クラス B 規模ネットワーク 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。

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。

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。

次の表に、ネットワーク 10.1 の 16 個のサブネットを示します。

（注） 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。

表 *3:* ネットワークのサブネット

マスク /20（255.255.240.0）でのサブネット	アドレス範囲
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

IPv6 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 のアドレス形式とアーキテクチャについて説明します。

IPv6 アドレスの形式

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入れる必要はありませんが、各フィールドに 1 個以上の桁が含まれている必要があります。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）。次の表に、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 *4: 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） 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。

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。

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。

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。

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。

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、グローバルで一意の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、IPv4 ルーティング インフラストラクチャ上で IPv6 パケットを動的にトンネリングさせるためのホストおよびルータの技術が実装されています。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。

2 つ目のタイプの IPv6 アドレスは、IPv4 アドレスが埋め込まれたもので、「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。

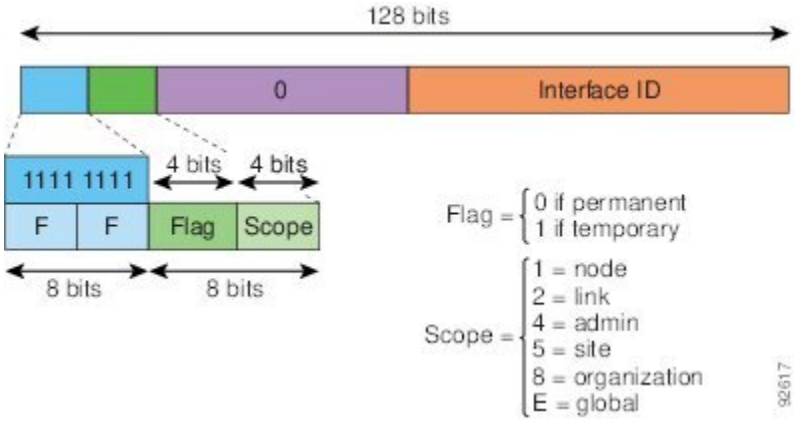
マルチキャスト アドレス

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。次の図に、IPv6 マルチキャスト アドレスの形式を示します。

図 *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） ASA では、エニーキャスト アドレスを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
- このルータが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 アドレス プレフィックスは、ipv6-prefix/prefix-length の形式で、アドレス空間全体のビット連続ブロックを表すために使用できます。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。次の表に、各 IPv6 アドレス タイプのプレフィックスを示します。

表 *5 : 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

次の表に、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 ASA のコマンドで入力できます。

表 *6 :* 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。

リテラル	値	説明
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。
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	ユーザー データグラム プロトコル（RFC 768）。

IANA の Web サイトでオンラインでプロトコル番号を確認できます。

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

TCP ポートおよび UDP ポート

次の表に、リテラル値とポート番号を示します。いずれも ASA 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。

- ASA 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。
- ASA は、ポート 1645 と 1646 で RADIUS をリッスンしています。RADIUS サーバーが標準ポート 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ッスンするように ASA 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、ASA では、**dnsix** リテラル値を使用すると見なされます。

IANA の Web サイトでオンラインでポート番号を確認できます。

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

表 7: 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ーに通知するために、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
bootps	UDP	67	ブートストラップ プロトコル サーバー
chargen	TCP	19	キャラクタ ジェネレータ
cifs	TCP、UDP	3020	Common Internet File System
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
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
domain	TCP、UDP	53	DNS
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）

リテラル	TCP または UDP	値	説明
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
h323	TCP	1720	H.323 発呼信号
hostname	TCP	101	NIC ホスト ネーム サーバー
http	TCP、UDP	80	World Wide Web HTTP
https	TCP	443	HTTP over SSL
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
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）
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
lpd	TCP	515	ライン プリンタ デーモン（プリンタ スプーラー）
mobile-ip	UDP	434	モバイル IP-Agent
nameserver	UDP	42	ホスト ネーム サーバー
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス
nfs	TCP、UDP	2049	ネットワーク ファイル システム（Sun Microsystems）

リテラル	TCP または UDP	値	説明
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-data	TCP	5631	pcAnywhere データ
pcanywhere-status	UDP	5632	pcAnywhere ステータス
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 ユーザー サービス
radius-acct	UDP	1646	リモート認証ダイヤルイン ユーザー 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
rsh	TCP	514	リモート シェル
rtsp	TCP	554	Real Time Streaming Protocol
secureid-udp	UDP	5510	SecureID over UDP
sip	TCP、UDP	5060	Session Initiation Protocol
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	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

リテラル	TCP または UDP	値	説明
talk	TCP、UDP	517	Talk
Telnet	TCP	23	Telnet（RFC 854）
tftp	UDP	69	『Trivial File Transfer Protocol』
time	UDP	37	時刻
uucp	TCP	540	UNIX 間コピー プログラム
vxlan	UDP	4789	Virtual eXtensible Local Area Network（VXLAN）
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP、UDP	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

次の表に、ASA に向かうトラフィックを処理するために ASA が開くプロトコル、TCP ポート、および UDP ポートを示します。この表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、ASA 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。ASA 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 *8*：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	注
DHCP	UDP	67、68	—
フェールオーバー制御	105	なし	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	なし	—

機能またはサービス	プロトコル	ポート番号	注
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 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	8（ノンセキュア）9（セキュア）	なし	—
Telnet	TCP	23	—
VPN ロードバランシング	UDP	9023	設定可能。
VPN 個別ユーザー認証プロキシ	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

次の表に、ASA 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 *9 : ICMP* タイプ

ICMP 番号	ICMP 名
0	echo-reply
3	unreachable
4	ソース クエンチ（始点抑制要求）
5	redirect
6	代替アドレス
8	echo
9	ルータ アドバタイズメント
10	ルータ要求
11	time-exceeded
12	パラメータ問題
13	timestamp-request
14	タイムスタンプ応答
15	情報要求
16	情報応答
17	マスク要求
18	mask-reply
30	traceroute
31	変換エラー
32	mobile-redirect

翻訳について
このドキュメントは、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。