

アドレスとポートのマッピング（MAP）

アドレスとポートのマッピング（MAP）は、IPv4 アドレスを IPv6 に変換するためのキャリアグレードの機能であるため、サービスプロバイダーエッジで IPv4 に変換される前にサービスプロバイダーの IPv6 ネットワーク経由でトラフィックを送信できます。

- アドレスとポートのマッピング（MAP）について （1 ページ）
- アドレスとポートのマッピング（MAP）に関するガイドライン （3 ページ）
- MAP-T ドメインの設定 （4 ページ）
- MAP のモニタリング （6 ページ）
- MAP の履歴 （7 ページ）

アドレスとポートのマッピング（MAP）について

アドレスとポートのマッピング (MAP) は、主にサービスプロバイダー (SP) ネットワークで使用する機能です。サービス プロバイダーは、IPv6 専用ネットワーク、MAP ドメインを稼働でき、同時に、IPv4 専用のサブスクライバをサポートし、パブリック インターネット上の IPv4 専用サイトとの通信ニーズに対応します。MAP は、RFC7597、RFC7598、および RFC7599 で定義されています。

MAP ドメイン内のサービスプロバイダーの場合、NAT46 を介した MAP の利点は、サブスクライバの IPv4 アドレスに対する IPv6 アドレスの代替（および SP ネットワークエッジでの IPv4 への変換）がステートレスであることです。これにより、NAT46 と比較して SP ネットワーク内の効率が向上します。

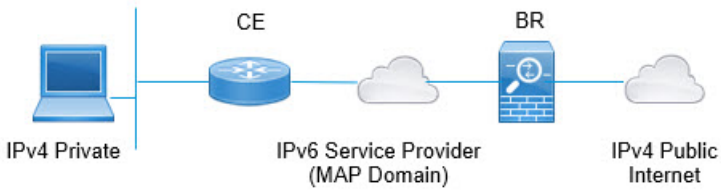
MAP 変換（MAP-T）と MAP カプセル化（MAP-E）という 2 つのマップ技術があります。ASA は MAP-T をサポートしています。MAP-E はサポートされていません。

変換によるアドレスとポートのマッピング（MAP-T）について

MAP-T では、まず、サブスクライバの IPv4 アドレスがサーバープロバイダー（SP）のパブリック IPv4 アドレスに変換されます。これは、1 対 1 のアドレスマッピングである場合も、プレフィックスまたは共有アドレスへのマッピングである場合もあります。次に、その IPv4 アドレスが MAP ドメイン内の IPv6 アドレスに変換され、パケットが SP IPv6 ネットワークを介して送信されます。ネットワークエッジで、SP の境界リレーが、パケットをパブリック IPv4

ネットワークにルーティングする前にIPv6アドレスをSPのIPv4アドレスに変換し直します。パブリック IPv4 ネットワークからサブスクライバに着信するトラフィックに対しては、まったく逆の処理が実行されます。

図 *1: MAP-T* ネットワーク



MAP-T を使用すると、SP ネットワークを IPv6 専用アーキテクチャに移行しながら、サブスクライバは IPv4 を引き続き使用して IPv4 専用インターネットまたは SP ネットワーク外の他のサイトと通信できます。

MAP-T は NAT64 変換と同様に動作しますが、IPv4 アドレスが埋め込まれた IPv6 アドレスを使用する代わりに、ポート番号も埋め込むエンコーディングスキームを使用します。したがって、MAP-T では、デバイスが使用するポート範囲を制限できます。

MAP-T システムには、以下が含まれます。

- **カスタマーエッジ（CE）デバイス**：CE は、ホームゲートウェイ（ワイヤレスルータ、ルータ付きケーブルモデムなど）です。CE は IPv4/IPv6 変換およびネイティブ IPv6 転送を提供します。これには、WAN 側のプロバイダー向け IPv6 アドレス指定インターフェイス、およびプライベート IPv4 アドレッシングを使用してアドレス指定される 1 つ以上の LAN 側インターフェイスがあります。IPv4 から IPv6 へのパケットの変換およびその逆の変換を行うために CE で使用する 1 つ以上の MAP ドメインを設定します。
- **境界リレー（BR）デバイス**：ASA を境界リレーとしてインストールします。BR は、IPv4/IPv6 変換をサポートする、MAP ドメインのエッジにあるプロバイダー側コンポーネントです。BR には、IPv6 対応インターフェイスが少なくとも 1 つ、および IPv4 ネットワークに接続された IPv4 インターフェイスが 1 つあります。IPv4 から IPv6 へのパケットの変換およびその逆の変換を行うために BR で使用する 1 つ以上の MAP ドメインを設定します。同じ MAP ドメインルールを使用して CE と BR を設定する必要があります。
- **MAP ドメイン**：MAP ドメインは、MAP-T CE デバイスのセットと MAP-T BR デバイスのセットをグループ化するメカニズムです。ドメインは、そのドメインに割り当てられた BR デバイスと CE デバイスの間で共有されるパラメータのセットです。BR デバイスと CE デバイスのそれぞれに対して、同じパラメータを含む同じドメインを設定します。

アドレスとポートのマッピング（MAP）に関するガイドライン

ファイアウォール モードのガイドライン

MAP はルーテッドモードでのみ設定できます。トランスペアレント モードはサポートされていません。

その他のガイドライン

- ASA はメッシュモードでのパケット転送には関与しません。したがって、MAP ドメインで転送マッピングルール（FMR）を設定することはできません。
- MAP は、トンネル化された VPN トラフィック、マルチキャストトラフィック、エニーキャストトラフィックをサポートしません。
- 特定の接続で NAT と MAP の両方を使用することはできません。NAT ルールと MAP ルールが重複していないことを確認してください。ルールが重複している場合は、予期しない結果になります。
- 次のインスペクションは、MAP 変換をサポートしていません。これらのインスペクションの対象となるパケットは変換されません。
  - CTIQBE
  - DCERPC
  - [Diameter]
  - WINS 経由の名前解決
  - GTP
  - H.323、H.225、H.245、RAS
  - ILS（LDAP）
  - インスタント メッセージ
  - IP オプション（RFC 791、2113）
  - IPSec Pass Through
  - LISP
  - M3UA
  - MGCP
  - MMP
  - NetBIOS

- PPTP
- RADIUS アカウンティング
- RSH
- RTSP
- SIP
- SKINNY
- SMTP および ESMTP
- SNMP
- SQL*Net
- STUN
- Sun RPC
- TFTP
- WAAS
- XDMCP
- アクティブ FTP

MAP-T ドメインの設定

MAP-T を設定するには、1 つまたは複数のドメインを作成します。カスタマーエッジ（CE）およびボーダーリレー（BR）デバイスで MAP-T を設定する場合は、各ドメインに参加するデバイスごとに同じパラメータを使用するようにしてください。

最大 25 個の MAP-T ドメインを設定できます。マルチコンテキストモードでは、コンテキストごとに最大 25 のドメインを設定できます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[CGNAT Map]** の順に選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しい MAP ドメインを作成します。
- MAP ドメインを選択し、[Edit] をクリックしてドメインを変更します。

ドメインが不要になった場合は、そのドメインを選択し、[Delete] をクリックします。

ステップ 3 [MAP Domain Name] に、ドメインの名前を入力します。名前は 48 文字以下の英数字文字列です。また、名前には、ピリオド（.）、スラッシュ（/）、およびコロン（:）の特殊文字を含めることもできます。

ステップ 4 [Default Mapping Rule] タブをクリックし、ルールの [Rule IPV6 Prefix] と [Rule IPv6 Prefix Length] を設定します。

RFC 6052 に従って IPv4 宛先アドレスを埋め込むために使用する IPv6 プレフィックスを指定します。通常のプレフィックスの長さは 64 ですが、使用可能な値は 32、40、48、56、64、または 96 です。埋め込み IPv4 アドレスの後の任意の末尾ビットは 0 に設定されます。たとえば、2001:DB8:CAFE:CAFE::/64 のように指定します。

ボーダーリレー（BR）デバイスはこのルールを使用し、MAP ドメイン外のすべての IPv4 アドレスを、MAP ドメイン内で動作する IPv6 アドレスに変換します。

ステップ 5 [Basic Mapping Rule] タブをクリックし、基本マッピングルールの IP アドレスプレフィックスとポートパラメータを設定します。

カスタマーエッジ（CE）デバイスは、基本マッピングルールを使用して、専用 IPv4 アドレッシングまたは共有アドレスとポート セットの割り当てを決定します。CE デバイスは最初に、システムの IPv4 アドレスをプールのプレフィックスおよびポート範囲内の IPv4 アドレスおよびポート（NAT44 を使用）に変換し、次にルールの IPv6 プレフィックスによって定義されたプール内の IPv6 アドレスに、新しい IPv4 アドレスを変換します。その後、パケットはサービスプロバイダーの IPv6 専用ネットワークを介してボーダーリレー（BR）デバイスに送信されるようになります。

次のオプションを設定します。

- [Rule IPV4 Prefix]、[Rule IPv4 Subnet Mask]：IPv4 プレフィックスは、カスタマーエッジ（CE）デバイスの IPv4 アドレスプールを定義します。CE デバイスは、最初に IPv4 アドレスを、IPv4 プレフィックスによって定義されたプール内のアドレス（およびポート番号）に変換します。次に、MAP は、デフォルトのマッピング ルールのプレフィックスを使用して、この新しいアドレスを IPv6 アドレスに変換します。

  ネットワーク アドレスとサブネット マスク（たとえば、192.168.3.0 255.255.255.0）を指定します。異なる MAP ドメインで同じ IPv4 プレフィックスを使用することはできません。

- [Rule IPV6 Prefix]、[Rule IPv6 Prefix Length]：IPv6 プレフィックスは、CE デバイスの IPv6 アドレスのアドレスプールを定義します。MAP は、このプレフィックスを持つ宛先アドレスと、デフォルトのマッピングルールで定義されている IPv6 プレフィックスを持つ送信元アドレスを持つパケットが、適切なポート範囲内にある場合にのみ、IPv6 パケットを IPv4 に戻します。他のアドレスから CE デバイスに送信されるすべての IPv6 パケットは、MAP を変換せずに IPv6 トラフィックとして処理されるだけです。MAP の送信元/宛先プールからのパケットは、範囲外のポートでは単にドロップされます。

  IPv6 プレフィックスおよびプレフィックス長（通常は 64）を指定しますが、8 未満を指定することはできません。異なる MAP ドメインで同じ IPv6 プレフィックスを使用することはできません。たとえば、2001:DB8:FFFF:F000::/64 のように指定します。

- [Share Ratio]：プール内に存在する必要があるポートの数を指定します。ポート数は 1～65536 の範囲内とし、2 の累乗にする必要があります（1、2、4、8 など）。

- [Start Port]：変換されたアドレスのポートプールに表示される最初のポート。指定するポートは 1 ～ 32768 の範囲内とし、2 の累乗にする必要があります（1、2、4、8 など）。既知のポートを除外する場合は、1024 以降から開始します。

ステップ 6 [OK] をクリックします。

MAP のモニタリング

次のトピックでは、MAP の構成およびアクティビティをモニタリングする方法について説明します。

MAP ドメイン構成の確認

マップドメインとそのステータスを表示して、構成が正しいことを確認できます。

[Monitoring] > **[Properties]** を選択し、目次から [MAP Domains] を選択します。この情報には MAP 構成が含まれており、**show map-domain** コマンドの出力が表示されます。ドメインの構成がまだ完了していない場合は、そのことが示されます。設定が不完全なドメインはアクティブになりません。マップ名を入力し、[Filter] をクリックして、単一ドメインの情報を表示できます。

```
MAP Domain 1
  Default Mapping Rule
    IPv6 prefix 2001:db8:cafe:cafe::/64
  Basic Mapping Rule
    IPv6 prefix 2001:cafe:cafe:1::/64
    IPv4 prefix 192.168.3.0 255.255.255.0
    share ratio 16
    start port 1024
    PSID length 4
    PSID offset 6
    Rule EA-bit length 12

MAP Domain 2
  Default Mapping Rule
    IPv6 prefix 2001:db8:1234:1234::/64

Warning: map-domain 2 configuration is incomplete and not in effect.
```

MAP syslog メッセージのモニタリング

syslog を有効にすると、次の syslog メッセージで MAP の動作をモニタリングできます。

- 305018: MAP translation from *interface name:source IP address/source port-destination IP address/destination port* to *interface name:translated source IP address/translated source port-translated destination IP address/translated destination port*

  新しい MAP 変換が行われました。このメッセージには、変換前と変換後の送信元および宛先が表示されます。

- 305019: MAP node address *IP address/port* has inconsistent Port Set ID encoding

  パケットのアドレスは MAP の基本的なマッピングルールに一致しますが（つまり、変換されることを意味します)、アドレス内でエンコードされたポートセット ID には（RFC7599 との）一貫性がありません。これは、このパケットの発信元である MAP ノードにソフトウェア障害がある可能性が高いことを意味します。

- 305020: MAP node with address *IP address* is not allowed to use port *port*

  パケットには、MAP の基本的なマッピングルール（つまり、変換されることを意味する）に一致するアドレスがありますが、関連するポートは、そのアドレスに割り当てられた範囲内にありません。これは、このパケットの発信元である MAP ノードの設定に誤りがある可能性が高いことを意味します。

MAP の履歴

機能名	プラットフォームリリース	説明
アドレスとポート変換のマッピング（MAP-T）	9.13(1)	アドレスとポートのマッピング (MAP) は、主にサービスプロバイダー (SP) ネットワークで使用する機能です。サービスプロバイダーは、IPv6 専用ネットワーク、MAP ドメインを稼働でき、同時に、IPv4 専用のサブスクライバをサポートし、パブリックインターネット上の IPv4 専用サイトとの通信ニーズに対応します。MAP は、RFC7597、RFC7598、および RFC7599 で定義されています。 次の画面が変更または導入されました。**[Configuration]** > **[Device Setup]** > **[CGNAT Map]**、**[Monitoring]** > **[Properties]** > **[MAP Domains]**。

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。