

NAT による非標準 FTP ポート番号の使用方法

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定例](#)

[サンプル設定 #1](#)

[サンプル設定 #2](#)

[サンプル設定 #3](#)

[シナリオ例と設定例](#)

[関連情報](#)

概要

Cisco IOS® ソフトウェア バージョン 11.3(3) と 11.2(13) では、非標準 File Transfer Protocol (FTP) ポート番号をサポートするために Network Address Translation (NAT) 対応の機能が導入されました。初期の Cisco IOS ソフトウェア バージョンでは、NAT 対応ルータが NAT 変換する必要のある IP アドレスを持ったパケットを受け取り、標準 TCP ポート番号が FTP 制御接続 (21) 用である場合に、ルータはそのパケットを FTP パケットとして認識し、パケットのペイロード内で必要な変換を実行します。ただし、FTP サーバが非標準 FTP ポート番号を使用している場合には、NAT はパケットのペイロードを無視します。これは、FTP データ接続の確立を妨げることがあります。

標準外の FTP ポート番号の使用をサポートするためには、**ip nat service** コマンドを使用する必要があります。次の表は、このコマンドで使用可能なオプションをまとめたものです。

オプション	定義
<i>list</i>	グローバル アドレスを記述しているアクセス リストを指定する
<i>name</i>	サーバ ローカル アドレスのアクセス リスト名
<i>number</i>	グローバル アドレスのアクセス リスト番号
<i>ftp</i>	FTP プロトコル
<i>tcp</i>	TCP プロトコル
<i>port</i>	特定の非標準ポート
<i>port number</i>	特定の非標準ポートの番号

次に、構文例を示します。

```
router-6(config)#ip nat service list 10 ftp tcp port 2021
```

注意すべき重要事項：

- 上記コマンドのアクセス リスト アドレスは、非標準 FTP 制御ポートを持つ FTP サーバの内部ローカル IP アドレスに合致していなければなりません。
- 非標準 FTP 制御ポートが FTP サーバに設定されている場合、NAT はその FTP サーバ用のポート 21 を使用している FTP 制御接続のチェックを中止します。他のすべての FTP サーバは、引き続き正常に機能します。
- 非標準制御ポートを使用している FTP サーバを持つホストも、標準 FTP 制御ポート (21) を使用している FTP クライアントを保持することができます。
- FTP サーバがポート 21 と非標準ポートの両方を使用している場合は、`ip nat service list <acl> ftp tcp <port>` コマンドを使ってこれらの両方のポートを設定する必要があります。次に、例を示します。

```
ip nat service list 10 ftp tcp port 2021
```

```
ip nat service list 10 ftp tcp port 21
```

ただし、同一のポートと同一のサービスに対して複数のアクセス リストを設定することはできません。次に、例を示します。

```
router-6(config)#ip nat service list 17 ftp tcp port 2021
```

```
router-6(config)#ip nat service list 10 ftp tcp port 2021
```

```
% service "ftp tcp port 2021" is already configured for access-list 17
```

[前提条件](#)

[要件](#)

このドキュメントに関する固有の要件はありません。

[使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 11.2(13) おおおよび 11.3(3) 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

[表記法](#)

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

[設定例](#)

次の各例では、NAT が FTP 制御接続として処理するフローが、設定に続く表の中に記述されています。各表に示されている「任意のローカル アドレス」とは、10.1.1.1 以外の任意のアドレスを指しています。

[サンプル設定 #1](#)

ローカル ネットワークで次の FTP サーバが稼働しているものとします。

- TCP ポート番号 2021 で稼働する IP アドレス 10.1.1.1 の 1 基の FTP サーバ。
- TCP ポート番号 21 での「任意の」IP アドレス (10.1.1.1 以外) の追加 FTP サーバ。


```
ip nat
service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

送信元アドレス	送信元 TCP ポート	送信先アドレス	宛先 TCP ポート
任意のローカル アドレス	任意のポート	10.1.1.1	H33
任意のローカル アドレス	任意のポート	任意のローカル アドレス	21
10.1.1.1	任意のポート	任意のローカル アドレス	21

注: 任意のローカル アドレスは 10.1.1.1 以外です。

上記の表で詳細が指定されている NAT プロセスの説明を、次のリストに示します。

- 1 行目 : 任意の送信元アドレスと任意のポート番号を持ち、宛先 TCP ポート番号 2021 で FTP サーバ (10.1.1.1) を宛先とするパケットでは、ペイロードの NAT 変換が必要です。
- 2 行目 : 任意の送信元アドレスと任意のポート番号を持ち、宛先 TCP ポート番号 21 (通常の FTP コントロール ポート) で任意のローカル アドレス (10.1.1.1 以外) を宛先とするパケットでは、ペイロードの NAT 変換が必要です。このように、通常のポート 21 で稼働するすべての FTP サーバ (10.1.1.1 以外) で、ペイロードの必要な NAT 変換を有効にします。
- 3 行目 : 任意のポート番号を持ち、宛先 TCP ポート 21 で任意のローカル アドレス (10.1.1.1 以外) を宛先として 10.1.1.1 から送信されるパケットでは、ペイロードの NAT 変換が必要です。

サンプル設定 #2

ローカル ネットワークで次の FTP サーバが稼働しているものとします。

- TCP ポート番号 21 と 2021 で稼働する IP アドレス 10.1.1.1 の 1 基の FTP サーバ。
- TCP ポート番号 21 での「任意の」IP アドレス (10.1.1.1 以外) の複数の FTP サーバ。


```
ip nat
service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

送信元アドレス	送信元 TCP ポート	送信先アドレス	宛先 TCP ポート
任意のローカル アドレス	任意のポート	10.1.1.1	H33
任意のローカル アドレス	任意のポート	10.1.1.1	21
任意のローカル アドレス	任意のポート	任意のローカル アドレス	21
任意のローカル アドレス	任意のポート	任意のローカル アドレス	21

上記の表で詳細が指定されている NAT プロセスの説明を、次のリストに示します。

- 1 行目： 任意の送信元アドレスと任意のポート番号を持ち、宛先 TCP ポート番号 2021 で FTP サーバ (10.1.1.1) を宛先とするパケットでは、ペイロードの NAT 変換が必要です。
- 2 行目： 任意の送信元アドレスと任意のポート番号を持ち、宛先 TCP ポート番号 21 で FTP サーバ (10.1.1.1) を宛先とするパケットでは、ペイロードの NAT 変換が必要です。
- 3 行目： 任意の送信元アドレスと任意のポート番号を持ち、宛先 TCP ポート番号 21 (通常の FTP コントロール ポート) で任意のローカル アドレスを宛先とするパケットでは、ペイロードの NAT 変換が必要です。このように、通常のポート 21 で稼働するすべての FTP サーバで、ペイロードの必要な NAT 変換を有効にします。
- 4 行目： 任意のポート番号を持ち、宛先 TCP ポート 21 で任意のローカル アドレスを宛先として 10.1.1.1 から送信されるパケットでは、ペイロードの NAT 変換が必要です。

サンプル設定 #3

ローカル ネットワークで次の FTP サーバが稼働しているものとします。

- TCP ポート番号 21 で稼働する IP アドレス 10.1.1.1 の 1 基の FTP サーバ。
- TCP ポート番号 2021 での IP アドレス 10.1.1.0/24 (10.1.1.1 以外) の複数の FTP サーバ。

```
ip nat service list 10 ftp tcp port 2021
access-list 10 deny 10.1.1.1
access-list 10 permit 10.1.1.0 0.0.0.255
```

送信元アドレス	送信元 TCP ポート	送信先アドレス	宛先 TCP ポート
任意のローカル アドレス	任意のポート	10.1.1.1	21
任意のローカル アドレス	任意のポート	10.1.1.x (注を参照)	H33
10.1.1.x (注を参照)	任意のポート	10.1.1.x 以外の任意のアドレス (注を参照)	21

注: 10.1.1.x は 10.1.1.1 以外です。

上記の表で詳細が指定されている NAT プロセスの説明を、次のリストに示します。

- 1 行目： 任意の送信元アドレスと任意のポート番号を持ち、宛先 TCP ポート番号 21 で FTP サーバ (10.1.1.1) を宛先とするパケットでは、ペイロードの NAT 変換が必要です。注: アクセスリストに deny 10.1.1.1 ステートメントがあるため、ポートが 2021 で 10.1.1.1 を宛先とするパケットは NAT ペイロード変換されません。
- 2 行目： 任意の送信元アドレスと任意のポート番号を持ち、宛先 TCP ポート番号 2021 で任意のローカル アドレス (10.1.1.1 以外) を宛先とするパケットでは、ペイロードの NAT 変換が必要です。
- 3 行目： 任意のポート番号を持ち、宛先 TCP ポート 21 で任意のアドレス (10.1.1.x 以外) を宛先として 10.1.1.x (上記の表の下にある注を参照) (10.1.1.1 以外) から送信されるパケットでは、ペイロードの NAT 変換が必要です。

非標準 FTP 制御ポートが FTP サーバに対して設定されている場合、NAT は、特定のサーバ用のポート 21 を使用している FTP 制御セッションを停止する点に留意する必要があります。FTP サーバが標準ポートと非標準ポートの両方を使用している場合は、`ip nat service` コマンドを使って両方のポートを設定する必要があります。

[シナリオ例と設定例](#)

TCP ポート番号 2021 の FTP サーバ 10.1.1.1 が内部ネットワークで稼働しています。NAT ルータは、ポート 2021 でコントロール接続のために FTP トラフィックに NAT が実行されるように設定されています。

ネットワーク図

設定：

```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip nat inside
!
interface Serial0
 ip address 192.168.10.1 255.255.255.252
 ip nat outside
!
ip nat service list 10 ftp tcp port 2021
ip nat inside source static 10.1.1.1 20.20.20.1
!--- Static NAT translation for inside local address 10.1.1.1 !--- to inside global address
20.20.20.1. ! access-list 10 permit 10.1.1.1
```

[関連情報](#)

- [NAT の機能](#)
- [NAT に関する FAQ](#)
- [ip nat outside source static コマンドを使用した設定例](#)
- [NAT の動作確認と NAT の基本的なトラブルシューティング](#)
- [NAT に関するサポートページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)