

Cisco Start Router

設定マニュアル 管理 IP アドレスとサブネットの変更 Cisco 841M J

2016年3月7日
第1.0版



www.networld.co.jp

株式会社ネットワーク



Networld



Cisco Start Router

設定マニュアル 管理 IP アドレスとサブネットの変更 Cisco 841M J



改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016年3月7日	ネットワーク	● 新規



免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワーク（以下 弊社）が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではありません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃止する場合がございます。なお、弊社が本書を更新することをお約束するものではありません。



表記規則

表記	表記の意味
「」 (括弧記号)	キー、テキストボックス、ラジオボタンなどのオブジェクト
bold (ボールド文字)	入力または選択するシステム定義値
<i><italic></i> (イタリック文字)	入力または選択するユーザー定義値
□ (囲み線)	入力または選択するオブジェクト
"" (二重引用符記号)	表示されるメッセージ
[] (蛍光マーカー)	確認するメッセージ

表記の例)

(1) 「Exec」ラジオボタンを選択します。

(2) テキストボックスに以下のコマンドを入力します。

copy running-config <file name>

(3) 「コマンドを実行」ボタンをクリックします。正常に実行されれば、画面に"[OK]"が表示されます。

Destination filename [startup-config]?

Building configuration...

[OK]

CLIによる設定

CLI機能はルータのコマンドプロンプトで実行可能な設定や、全てのIOS CLIコマンドを入力できます

1 Exec
 Configure

2

3

Destination filename [startup-config]?
 Building configuration...

[OK]



目次

1. はじめに.....	1
1.1 対象製品.....	1
1.2 CCP Express のシステム要件.....	1
1.3 クイックリンク.....	2
2. システム構成.....	3
2.1 使用した機材.....	3
3. 設定手順.....	5
3.1 新しいアクセス制御エントリーの作成.....	5
3.2 新しいネットワークオブジェクトグループエントリーの作成.....	6
3.3 管理 IP アドレスの変更.....	8
3.4 古いネットワークオブジェクトグループエントリーの削除.....	12
3.5 古いアクセス制御エントリーの削除.....	14
3.6 セキュリティ ACL の設定.....	16
3.7 新しい DHCP プールの作成.....	19
3.8 古い DHCP プールの削除.....	22
4. 設定ファイル.....	25



1. はじめに

本書は、Cisco Configuration Professional Express（以下 CCP Express）のアドバンスドセットアップを使用してCisco 841M Jシリーズの管理IPアドレスとサブネットの変更を実行する手順を説明した資料です。CCP Expressは、Web UIを備えた組み込みのデバイス管理ツールです。CCP Expressのアドバンスドセットアップを使用すると、WAN、LAN、およびセキュリティなど、製品の詳細設定を簡単に実行できます。



図 1 本書で実行する設定

1.1 対象製品

本書を使用して管理 IP アドレスとサブネットの変更を実行できる製品は、以下のとおりです。

表 1 本書の対象製品

C841M-4X-JSEC/K9	C841M-4X-JAIS/K9	C841M-8X-JAIS/K9
☑	☑	☑

1.2 CCP Express のシステム要件

CCP Express を使用できる Cisco IOS および Web ブラウザーは、次のとおりです。

- Cisco IOS 15.2(4)M2～、または 15.3(1)T～、セキュリティ機能は 15.5(1)T～
- Microsoft Internet Explorer 10
- Google Chrome 17～
- Mozilla Firefox 10～



1.3 クイックリンク

Cisco 841M J シリーズの公式の情報は、以下の URL から入手できます。

- Cisco Start Router ホーム:
<http://www.cisco.com/web/JP/smb/c800m/index.html>
- 製品カタログ:
http://www.cisco.com/web/JP/product/catalog/pdf/1082_en_start_catalog.pdf
- データシート:
http://www.cisco.com/web/JP/smb/c800m/docs/c800mj_data_sheet_c78-732678.pdf
- サポートコミュニティ:
<https://supportforums.cisco.com/ja/start>
- よくある質問:
<http://www.cisco.com/web/JP/smb/c800m/c800m-faq.html>
- サポート窓口:
<http://www.cisco.com/web/JP/smb/c800m/c800m-support.html>



2. システム構成

既定の管理 IP アドレスは、VLAN1 の SVI に設定された 10.10.10.1/25 です。すべての LAN ポートは既定で VLAN1 に所属しており、LAN ポートでは 10.10.10.0/25 のサブネットを含む DHCP プールをホストする DHCP サーバー機能が有効化されています。また、このサブネットに所属するホストが CCP Express、SSH または TELNET を使用して製品にリモートアクセスするためのアクセス制御リスト（以下セキュリティ ACL）が既定で設定されています。CCP Express のクイックセットアップウィザードを使用してインターネット接続の設定が完了している場合、IP マスカレードを使用するためのセキュリティ ACL が作成され、このサブネットを含むネットワークオブジェクトグループに関連付きます。纏めると、10.10.10.0/25 のサブネットは、VLAN1 の SVI、DHCP プール、リモートアクセス用のセキュリティ ACL、および IP マスカレード用のセキュリティ ACL に紐づくネットワークオブジェクトグループと関係しています。つまり、VLAN1 の SVI のサブネットを変更した場合、CCP Express、SSH、または TELNET を使用した製品へのリモートアクセスや、インターネット接続に失敗します。したがって、管理 IP アドレスとそのサブネットを変更する場合、それに関係する設定も併せて変更する必要があります。なお、10.10.10.0/25 のサブネットのまま、管理 IP アドレスだけを変更する場合は、それに関係する設定を変更する必要はありません。

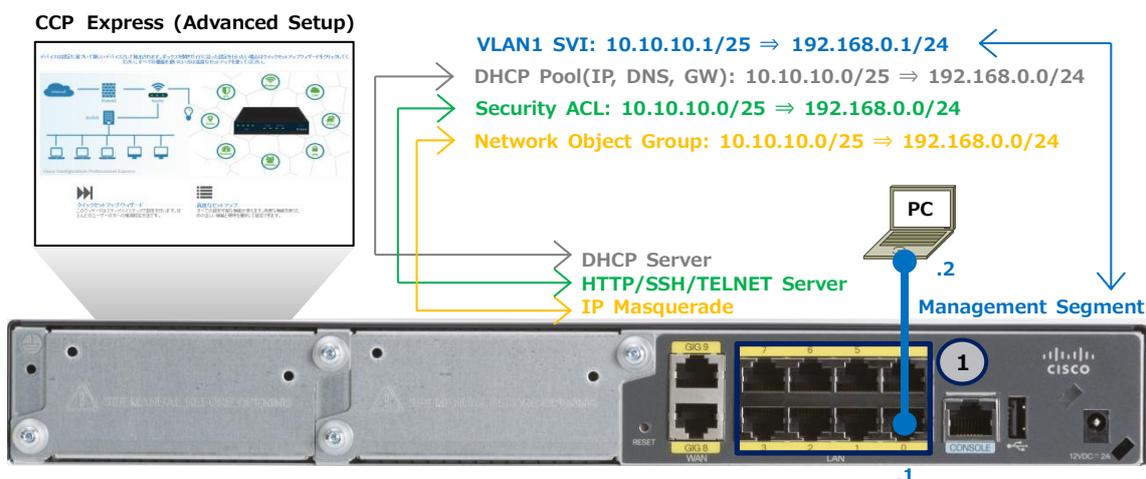


図 2 管理 IP アドレスとサブネットの変更で使用する構成 (C841M-8X-JAIS/K9 の場合)

本書では、CCP Express への接続やログインの手順を省略しています。これらの手順については、クイックスタートガイドをご参照ください。

- Cisco Start Router 設定マニュアル クイックスタートガイド Cisco 841M J:
http://www.networkworld.co.jp/download_file/4574/7266/

2.1 使用した機材



本書で使用した機材は、以下のとおりです。

表 2 本書で使用した機材

機材	製品型番または名称	備考
Cisco 841M J シリーズ	C841M-4X-JAIS/K9 15.5(3)M	
デバイス管理ツール	CCP Express 3.1.2	
PC	Windows 7 x64 Professional SP1	
Web ブラウザー	Internet Explorer x64 11.0.9600.18163	



3. 設定手順

Cisco 841M Jシリーズの管理 IP アドレスとサブネットの変更を実行します。なお、DHCPを使用しない場合は、DHCP プールの変更は不要です。また、IP アドレスは変更するがサブネットは変更しない場合は、アクセス制御エントリー、ネットワークオブジェクトグループエントリー、およびDHCPプールの変更は不要です。

3.1 新しいアクセス制御エントリーの作成

リモートアクセス用の既定のセキュリティ ACL に、新しいアドレス体系で使用するアクセス制御エントリーを作成します。

(1) CLI コマンドの実行画面に移動します。「任意のコマンド」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「CLI の設定」ボタンをクリックしてください。



図 3 CCP Express のホーム (任意のコマンド)



図 4 CCP Express のショートカット（ホームと CLI の設定）

(2) 新しいアクセス制御エントリを作成します。「Configure」ラジオボタンをクリックします。「Configure」テキストボックスに **access-list 23 permit 192.168.0.0 0.0.0.255** を入力します。「コマンドを実行」ボタンをクリックします。コマンドが正常に終了した場合は、「コマンドは正常に完了しました。」が表示されます。



図 5 アクセス制御エントリの作成

3.2 新しいネットワークオブジェクトグループエントリの作成

IP マスカレード用の既定のセキュリティ ACL に紐付くネットワークオブジェクトグループに、新しいアドレス体系で使用するネットワークオブジェクトグループエントリを作成します。

(1) CLI コマンドの実行画面に移動します。「任意のコマンド」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「CLI の設定」ボタンをクリックしてください。



図 6 CCP Express のホーム（任意のコマンド）



図 7 CCP Express のショートカット（ホームとCLIの設定）

(2) 新しいネットワークオブジェクトグループエントリーを作成します。「Configure」ラジオボタンをクリックします。「Configure」テキストボックスに **object-group network local_lan_subnets** と **192.168.0.0 255.255.255.0** を複数行で入力します。「コマンドを実行」ボタンをクリックします。コマンドが正常に終了した場合は、「コマンドは正常に完了しました。」が表示されます。



図 8 ネットワークオブジェクトグループエントリーの作成

3.3 管理 IP アドレスの変更

VLAN1 の SVI の IP アドレスとサブネットを変更します。この設定を CCP Express から変更すると、以下のリモートアクセス用の既定のセキュリティ ACL の設定が削除されます。これらの設定は、次節以降で復元します。

- リモートアクセス用の既定のセキュリティ ACL (access-list 23 permit 10.10.10.0 0.0.0.127 / access-list 23 permit 192.168.0.0 0.0.0.255)
- CCP Express に接続するための上記のセキュリティ ACL 設定 (ip http access-class 23)
- SSH または TELNET に接続するための上記のセキュリティ ACL 設定 (line vty 0 15 / access class 23 in)

(1) インターフェイスの設定画面に移動します。「インターフェイスと接続」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「インターフェイス」ボタンをクリックしてください。



図 9 CCP Express のホーム（インターフェイスと接続）



図 10 CCP Express のショートカット（ホームとインターフェイス）

(2) 管理 IP アドレスとサブネットを変更します。「Vlan1」ラベルの行の「編集」ボタンをクリックします。



インターフェイス

ループバックの追加 VLAN の追加 編集 削除

 プライマリWAN: GigabitEthernet0/4(Dialer1)
  バックアップWAN: 未構成
  [ゾーン](#)

*注意: 複数選択できません。

インターフェイス	IPv4 アドレス	IPv6 アドレス	管理状態	操作状態	説明	アクション
構成可能なインターフェイス						
<input type="checkbox"/>	GigabitEthernet0/0			up		 
<input type="checkbox"/>	GigabitEthernet0/1			down		 
<input type="checkbox"/>	GigabitEthernet0/2			down		 
<input type="checkbox"/>	GigabitEthernet0/3			down		 
<input type="checkbox"/>	GigabitEthernet0/4			up		 
<input type="checkbox"/>	GigabitEthernet0/5			down		 
<input type="checkbox"/>	Vlan1	10.10.10.1		up	\$ETH_LAN\$1	 
読み取り専用のインターフェイス						
<input type="checkbox"/>	NVI0			up		
<input type="checkbox"/>	Virtual-Access1			up		
<input type="checkbox"/>	Virtual-Access2			up		
<input type="checkbox"/>	Dialer1	192.0.2.1		up		

図 11 管理 IP アドレスとサブネットの変更

(3) 管理 IP アドレスとサブネットを編集します。「*」ラベルが記載された設定は、必須の設定です。

- ① 「IPv4 アドレス」ドロップダウンをクリックします。
- ② 「タイプ」ドロップダウンリストから**静的 IP アドレス**を選択します。
- ③ 「静的 IP アドレス」テキストボックスに **192.168.0.1** を入力します。
- ④ 管理 IP アドレスを変更した場合の警告が表示されたら、「はい」ボタンをクリックします。
- ⑤ 「サブネットマスク」テキストボックスに **255.255.255.0** を入力します。
- ⑥ 「NAT の有効化」チェックボックスにチェックを入れます。
- ⑦ 「はい」ボタンをクリックします。




図 12 管理 IP アドレスとサブネットの変更 (詳細)

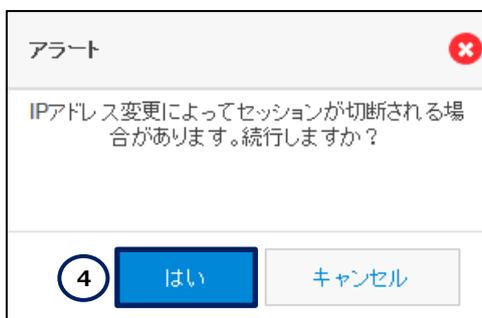


図 13 管理 IP アドレスとサブネットの変更の警告

(4) PC の IP アドレスを変更し、CCP Express に再接続します。

- ① 「次の IP アドレスを使う」ラジオボタンをクリックします。
- ② 「IP アドレス」テキストボックスに **192.168.0.2** を入力します。
- ③ 「サブネットマスク」テキストボックスに **255.255.255.0** を入力します。
- ④ 「デフォルトゲートウェイ」テキストボックスに **192.168.0.1** を入力します。
- ⑤ 「次の DNS サーバーのアドレスを使う」ラジオボタンをクリックします。
- ⑥ 「優先 DNS サーバー」テキストボックスに **192.168.0.1** を入力します。
- ⑦ 「OK」ボタンをクリックします。

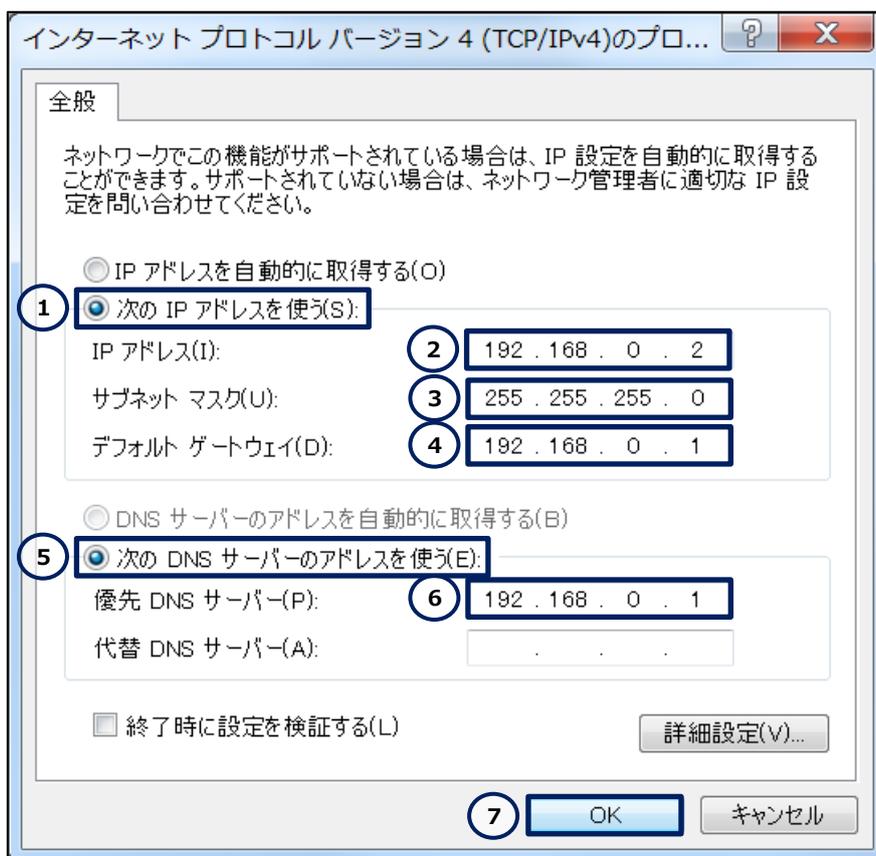


図 14 PC の新しい IP アドレス

3.4 古いネットワークオブジェクトグループエントリーの削除

IP マスカレード用の既定のセキュリティ ACL に紐付くネットワークオブジェクトグループから、古いアドレス体系で使用していたネットワークオブジェクトグループエントリーを削除します。

(1) CLI コマンドの実行画面に移動します。「任意のコマンド」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「CLI の設定」ボタンをクリックしてください。



図 15 CCP Express のホーム（任意のコマンド）



図 16 CCP Express のショートカット（ホームと CLI の設定）

(2) 古いネットワークオブジェクトグループエントリを削除します。「Configure」ラジオボタンをクリックします。「Configure」テキストボックスに **object-group network local_lan_subnets** と **10.10.10.0 255.255.255.128** を複数行で入力します。「コマンドを実行」ボタンをクリックします。コマンドが正常に終了した場合は、「コマンドは正常に完了しました。」が表示されます。



図 17 ネットワークオブジェクトグループエントリーの削除

3.5 古いアクセス制御エントリーの削除

リモートアクセス用の既定のセキュリティ ACL から、古いアドレス体系で使用していたアクセス制御エントリーを削除します。

(1) CLI コマンドの実行画面に移動します。「任意のコマンド」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「CLI の設定」ボタンをクリックしてください。



図 18 CCP Express のホーム (任意のコマンド)



図 19 CCP Express のショートカット (ホームと CLI の設定)

(2) 古いアクセス制御エントリを削除します。「Configure」ラジオボタンをクリックします。「Configure」テキストボックスに **no access-list 23 permit 10.10.10.0 0.0.0.127** を入力します。「コマンドを実行」ボタンをクリックします。コマンドが正常に終了した場合は、「コマンドは正常に完了しました。」が表示されます。



図 20 アクセス制御エントリーの削除

3.6 セキュリティ ACL の設定

CCP Express を使用した管理 IP アドレスの変更によって削除されたセキュリティ ACL とその関連設定の復元を実行します。

(1) CLI コマンドの実行画面に移動します。「任意のコマンド」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「CLI の設定」ボタンをクリックしてください。



図 21 CCP Express のホーム（任意のコマンド）



図 22 CCP Express のショートカット（ホームと CLI の設定）

(2) 新しいアクセス制御エントリを再作成します。「Configure」ラジオボタンをクリックします。「Configure」テキストボックスに **access-list 23 permit 192.168.0.0 0.0.0.255** を入力します。「コマンドを実行」ボタンをクリックします。コマンドが正常に終了した場合は、「コマンドは正常に完了しました。」が表示されます。



図 23 アクセス制御エントリーの再作成

(3) CCP Express に接続するためのセキュリティ ACL を再設定します。「Configure」ラジオボタンをクリックします。「Configure」テキストボックスに **ip http access-class 23** を入力します。「コマンドを実行」ボタンをクリックします。コマンドが正常に終了した場合は、「コマンドは正常に完了しました。」が表示されます。



図 24 CCP Express に接続するためのセキュリティ ACL の再設定

(4) SSH または TELNET に接続するためのセキュリティ ACL を再設定します。「Configure」ラジオボタンをクリックします。「Configure」テキストボックスに **line vty 0 15** と **access-class 23 in** を



複数行で入力します。「コマンドを実行」ボタンをクリックします。コマンドが正常に終了した場合は、「コマンドは正常に完了しました。」が表示されます。



図 25 SSH または TELNET に接続するためのセキュリティ ACL の再設定

3.7 新しい DHCP プールの作成

必要に応じて、新しいアドレス体系で使用する DHCP プールを作成します。

(1) DHCP プールの設定画面に移動します。「DNS/DHCP/ホスト名」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「DHCP/DNS/ホスト名」ボタンをクリックしてください。



図 26 CCP Express のホーム (DNS/DHCP/ホスト名)



図 27 CCP Express のショートカット (ホームと DHCP/DNS/ホスト名)

(2) 新しい DHCP プールを作成します。「追加」ボタンをクリックします。



DHCP/DNS/ホスト名

ホスト名/ドメイン名

ホスト名*:

ドメイン名:

DNS

ネットワーク管理者またはインターネットサービスプロバイダが提供したプライマリおよびセカンダリサーバアドレスを入力してください。

プライマリ DNS:

セカンダリ DNS:

DHCP ①

<input type="checkbox"/>	プール名	プールネットワーク	サブネットマスク	デフォルトルータ	アクション
<input type="checkbox"/>	ccp-pool	10.10.10.0	255.255.255.128	10.10.10.1	✎ 🗑

図 28 DHCP プールの作成

(3) 新しい DHCP プールを編集します。「*」ラベルが記載された設定は、必須の設定です。

- ① 「プール名」テキストボックスに DHCP プールの名前を入力します。
- ② 「プールネットワーク」テキストボックスに **192.168.0.0** を入力します。
- ③ 「サブネットマスク」テキストボックスに **255.255.255.0** を入力します。
- ④ 「デフォルトルート」テキストボックスに **192.168.0.1** を入力します。
- ⑤ 「この DHCP プールにある DNS 値を含める」チェックボックスのチェックを外します。
- ⑥ 「DNS プライマリアドレス」テキストボックスに **192.168.0.1** を入力します。製品は DNS フォワーダーとして機能します。
- ⑦ 必要に応じて、「DNS セカンダリアドレス」テキストボックスに代替 DNS サーバーの IP アドレスを入力します。
- ⑧ 「DHCP サーバデータベースに全ての DHCP オプションをインポートする」チェックボックスにチェックを入れます。
- ⑨ 「はい」ボタンをクリックします。



DHCP プールの追加 ✕

プール名 *: 1 networld-pool

プールネットワーク *: 2 192.168.0.0

サブネットマスク: 3 255.255.255.0

デフォルトルート: 4 192.168.0.1

この DHCP プールにあるDNS値を含める: 5

DNS プライマリアドレス: 6 192.168.0.1 ✕

DNS セカンダリアドレス: 7 例: 10.70.180.1

DHCP サーバデータベースに全ての DHCP オプションをインポートする: 8

9 はい
キャンセル

図 29 DHCP プールの作成 (詳細)

3.8 古い DHCP プールの削除

必要に応じて、古いアドレス体系で使用していた DHCP プールを削除します

(1) DHCP プールの設定画面に移動します。「DNS/DHCP/ホスト名」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「DHCP/DNS/ホスト名」ボタンをクリックしてください。



図 30 CCP Express のホーム (DNS/DHCP/ホスト名)



図 31 CCP Express のショートカット (ホームと DHCP/DNS/ホスト名)

(2) 古い DHCP プールを削除します。

- ① 「ccp-pool」チェックボックスにチェックを入れます。
- ② 「ccp-pool」ラベルの行の「削除」ボタンをクリックします。
- ③ DHCP プールの削除の確認が表示されたら、「はい」ボタンを入力します。



DHCP/DNS/ホスト名

ホスト名ドメイン名

ホスト名:

ドメイン名:

DNS

ネットワーク管理者またはインターネットサービスプロバイダが提供したプライマリおよびセカンダリサーバアドレスを入力してください。

プライマリ DNS:

セカンダリ DNS:

DHCP

	プール名	プールネットワーク	サブネットマスク	デフォルトルータ	アクション
1	<input checked="" type="checkbox"/> ccp-pool	10.10.10.0	255.255.255.128	10.10.10.1	2 <input type="button" value="削除"/>
	<input type="checkbox"/> networkd-pool	192.168.0.0	255.255.255.0	192.168.0.1	<input type="button" value="編集"/> <input type="button" value="削除"/>

図 32 DHCP プールの削除

Alert ✖

このDHCPデータは削除されます。続行しますか？

3

図 33 DHCP プールの削除の確認

設定は以上です。必要に応じて、PC の IP アドレスを DHCP に変更してください。



4. 設定ファイル

本書で追加または変更される設定（クイックスタートガイドを使用した設定との差分）は、以下のとおりです。

```
001: ip dhcp excluded-address 192.168.0.1
002: ip dhcp pool networkd-pool
003: network 192.168.0.0 255.255.255.0
004: dns-server 192.168.0.1
005: default-router 192.168.0.1
006: object-group network local_lan_subnets
007: 192.168.0.0 255.255.255.0
008: zone security VPN
009: zone security DMZ
010: interface Vlan1
011: ip address 192.168.0.1 255.255.255.0
012: access-list 23 permit 192.168.0.0 0.0.0.255
```

お問い合わせ

Q 製品のご購入に関するお問い合わせ

<https://info-networld.smartseminar.jp/public/application/add/152>

Q ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q 製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

本書に記載されているロゴ、会社名、製品名、サービス名は、一般に各社の登録商標または商標です。
本書では、®、™、©マークを省略しています。

www.networld.co.jp

株式会社ネットワーク

