

Cisco Start Router

設定マニュアル クイックスタートガイド／マルチホーム Cisco 841M J

2016年3月11日
第1.0版



www.networld.co.jp

株式会社ネットワーク



Networld



改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016年3月11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.....	2
1.2 CCP Express のシステム要件.....	2
1.3 クイックリンク.....	3
2. システム構成.....	4
2.1 ISP から提供されるネットワーク接続情報	5
2.2 使用した機材	5
3. 設定手順	7
3.1 ケーブルの接続と電源の投入.....	7
3.2 ユーザーの作成とログイン.....	8
3.3 クイックセットアップウィザードの実行	9
4. 設定ファイル.....	20



1. はじめに

本書は、Cisco Configuration Professional Express（以下 CCP Express）のクイックセットアップウィザードを使用して Cisco 841M J シリーズの製品の初期セットアップ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のクイックセットアップウィザードを使用すると、WAN、LAN、およびセキュリティなど、製品の基本設定を迅速に実行できます。CCP Express に初めてログインすると、新しいユーザーの作成が要求されます。製品の初期セットアップは、作成した新しいユーザーの権限で実行します。製品は、PPPoE を使用して 2つの異なる ISP からそれぞれ端末型のパブリック IP アドレスを取得します。製品の初期セットアップが完了すると、製品に接続した PC やサーバーが安全にインターネットに接続できるようになります。

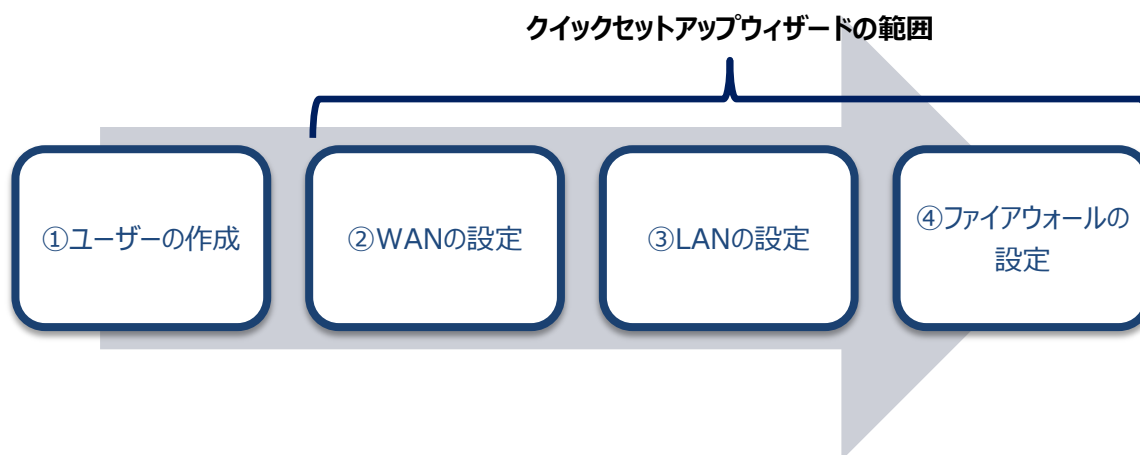


図 1 本書で実行する設定

本書を含む Cisco 841M J シリーズのクイックスタートガイドは、WAN 側インターフェースの IP アドレスの割り当て方式毎、および冗長 WAN 回線用に提供しています。前者は契約先の回線事業者によって、PPPoE、DHCP、および手動設定の 3 つに分類できます。PPPoE は、さらに端末型払い出し方式と LAN 型払い出し方式の 2 つに分類できます。一般的に、PPPoE は NTT、DHCP と手動設定は NTT 以外の回線事業者で使用されます。また、PPPoE の端末型の場合、パブリック IP アドレスが固定されるか、あるいは動的に変わるかは契約内容によります。WAN 回線の契約内容をご確認のうえ、該当するクイックスタートガイドを選択してください。

- クイックスタートガイド／PPPoE／端末型
- クイックスタートガイド／PPPoE／LAN 型
- クイックスタートガイド／DHCP
- クイックスタートガイド／手動設定
- クイックスタートガイド／マルチホーム（本書）



安全上のガイドライン、ハードウェアの機能、および製品の設置については、Cisco Systems（以下 Cisco）社が提供するハードウェアインストールガイドをご参照ください。

- ハードウェアインストールガイド:

http://www.cisco.com/cisco/web/support/JP/docs/RT/BranchRT/800RT/IG/011/800M_HIG.pdf

Cisco 社のハードウェアインストールガイドには、製品の初期セットアップを支援する、次の有用な情報が掲載されています。

- 安全上の重要な注意事項
- 正面図や背面図で説明される、製品の外観と全般的な機能
- LED、メモリー、電源モジュールなどのハードウェアの仕様
- SKU 情報
- ゴム製の脚、ブラケット、皿小ネジなどの、注文毎の製品同梱品
- 卓上、壁面、またはラックへの製品の設置手順
- アースおよび電源の接続手順

1.1 対象製品

本書を使用して製品の初期セットアップ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

製品の初期セットアップの手順は、以下の構成で説明します。

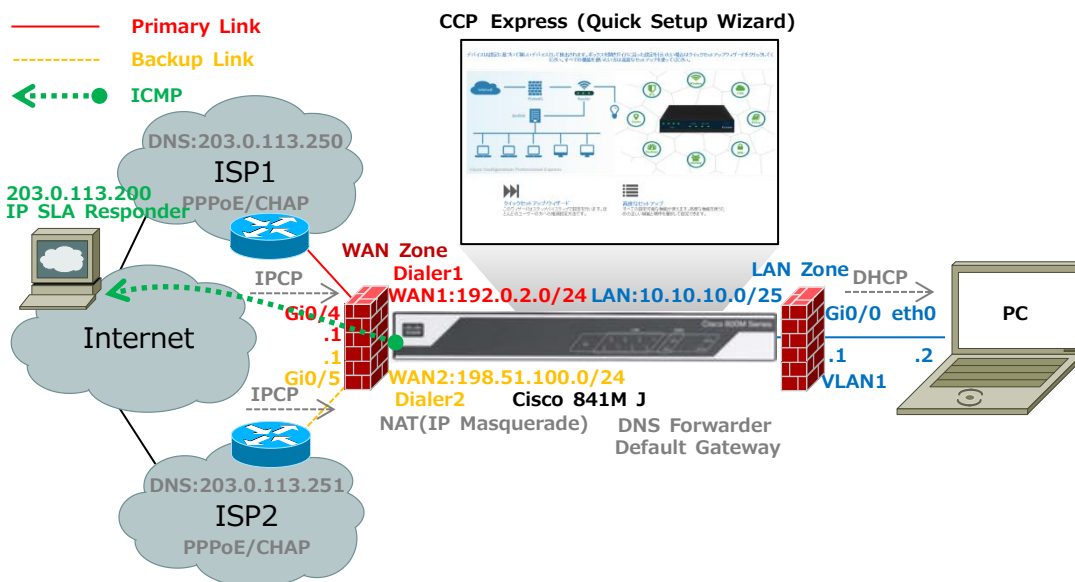


図 2 製品の初期セットアップで構成するシステム

PCは、製品からDHCPで自動的に割り当てられたIPアドレスを使用して、既定のVLANに接続します。DHCPでは、製品のLAN側IPアドレスをDNSサーバー、およびデフォルトゲートウェイとした情報も配布されます。製品の初期セットアップが完了すると、製品は、各ISPにCHAP認証のPPPoEを使用して接続します。PPPoEの接続が確立すると、製品は、各ISPからIPCPで自動的に割り当てられたIPアドレス、およびDNSサーバーを使用して、インターネットに接続します。製品は、一方のISPをデフォルトゲートウェイとして常に優先的に使用し、それが有効かどうかはインターネットの特定のホストに対する死活監視で判断します。死活監視対象のホストへのIP到達性が失われると、製品は他方のISPをデフォルトゲートウェイとして使用します。PCは、製品を経由してインターネットに接続します。このとき、製品のIPマスカレード機能によって、製品のWAN側IPアドレスがPCの送信元IPアドレスとして使用されます。また、製品のDNSフォワーダー機能によって、DNSクエリーがDNSサーバーに転送されます。製品のWAN側とLAN側には既定のファイアウォール設定が適用され、悪意のある接続からネットワークが保護されます。なお、本書は、図3のようなデュアルシングルホームの設定にも対応しています。



図 3 デュアルシングルホーム



2.1 ISP から提供されるネットワーク接続情報

接続先の各 ISP から提供されるネットワーク接続情報は、以下のとおりです。

表 2 本書で使用したネットワーク接続情報 (ISP1)

項目	値	備考
WAN 接続タイプ	PPPoE	端末型払い出し
DNS サーバー	203.0.113.250	IPCP による自動割り当て
IP アドレス	192.0.2.1/24	IPCP による自動割り当て
PPPoE 認証プロトコル	CHAP	
PPPoE ユーザー名	networld@example.com	
PPPoE パスワード	password	
MTU サイズ	1454byte	
MSS サイズ	1414byte	

表 3 本書で使用したネットワーク接続情報 (ISP2)

項目	値	備考
WAN 接続タイプ	PPPoE	端末型払い出し
DNS サーバー	203.0.113.251	IPCP による自動割り当て
IP アドレス	198.51.100.1/24	IPCP による自動割り当て
PPPoE 認証プロトコル	CHAP	
PPPoE ユーザー名	networld@example.jp	
PPPoE パスワード	password	
MTU サイズ	1454byte	
MSS サイズ	1414byte	

2.2 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 4 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	
PPPoE サーバー	ppp 2.4.5-10 x64, rp-pppoe	



	3.10-11 x64	
PC	Windows 7 x64 Professional	DHCP クライアント有効
	SP1	
Web ブラウザー	Internet Explorer x64	
	11.0.9600.18163	



3. 設定手順

Cisco 841M J シリーズの製品の初期セットアップを実行します。

3.1 ケーブルの接続と電源の投入

製品に電源ケーブルと LAN ケーブルを接続し、電源を入れます。

(1) 製品の電源を入れ、「SYS」LED が緑点灯するまでしばらく待ちます。製品の起動には 2 分程度の時間がかかります。



図 4 電源ポート (C841M-8X-JAIS/K9 の場合)



図 5 SYS LED (緑点灯) (C841M-8X-JAIS/K9 の場合)

(2) 製品と WAN 回線、および製品と PC を図 2 のとおりに LAN ケーブルで接続します。PC には、製品の DHCP サーバー機能で 10.10.10.0/25 の範囲内の IP アドレスが自動的に割り当てられます。IP アドレスの割り当てには 1 分程度の時間がかかります。ここでは Gi0/0 に PC を接続していますが、実際は LAN 側のすべてのインターフェースを使用できます。WAN 側のインターフェースは Gi0/4 と Gi0/5 を使用します。WAN 側のインターフェースは既定でシャットダウンされています。LAN が接続されると、「LAN」LED が緑点灯 (接続確立) または緑点滅 (データ伝送中) します。



図 6 WAN ポートと LAN ポート (C841M-8X-JAIS/K9 の場合)



図 7 LAN LED (緑点灯または緑点滅) (C841M-8X-JAIS/K9 の場合)



3.2 ユーザーの作成とログイン

新しいユーザーを作成し、CCP Express にログインします。

(1) PC の Web ブラウザーを起動し、HTTP で CCP Express に接続します。CCP Express の既定の IP アドレスは、**10.10.10.1** です。この IP アドレスを変更すると、CCP Express に接続できなくなるのでご注意ください。なお、HTTPS で CCP Express に接続することもできます。



図 8 HTTP で CCP Express に接続

(2) CCP Express にログインします。ユーザー名に **cisco**、パスワードに **cisco** を入力し、「OK」ボタンをクリックします。このユーザーは製品の初期状態時のみ存在するワンタイムユーザーで、一度でも製品へのログインに使用するとシステムから削除されます。



図 9 ワンタイムユーザーで CCP Express にログイン

(3) 新しいユーザーを作成します。「ユーザ名」テキストボックスに新しいユーザーの名前、「新しいパスワード」テキストボックスに新しいユーザーのパスワード、「新しいパスワードの再入力」テキストボックスに直前でも入力したパスワードと同じパスワードを入力し、「はい」ボタンをクリックします。ここで作成したユーザーには、特権レベルのアクセス権が付与されます。ここで新しいユーザーを作成せずにダイアログを閉じると、再設定の前に製品の初期化が必要になりますのでご注意ください。

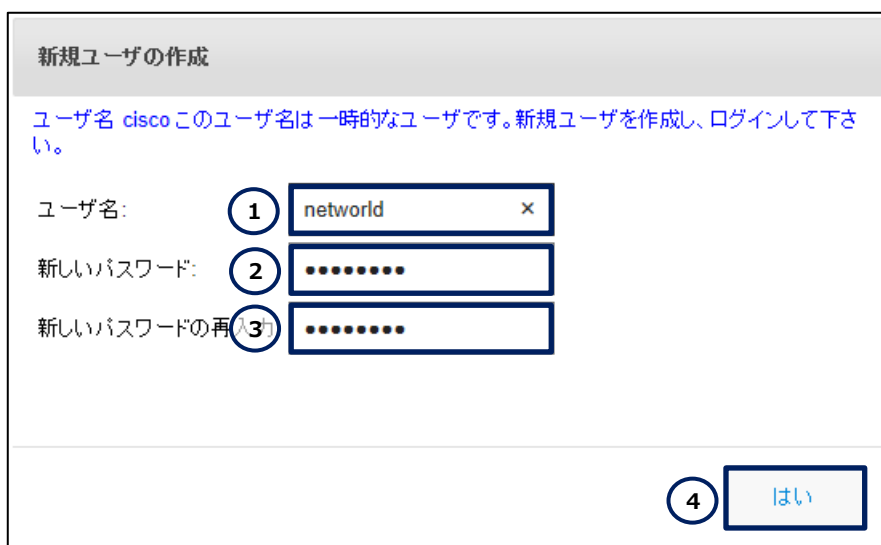



図 10 新しいユーザーの作成

(4) 認証画面が再度表示されるので、先の手順で作成した新しいユーザーで CCP Express にログインします。ユーザー名とパスワードに手順(3)で設定した値を入力し、「OK」ボタンをクリックします。



図 11 新しいユーザーで CCP Express にログイン

3.3 クイックセットアップウィザードの実行

CCP Express のクイックセットアップウィザードを実行し、製品の WAN、LAN、およびセキュリティを設定します。



(1) クイックセットアップウィザードを実行します。「クイックセットアップ・ウィザード」ボタンをクリックします。

デバイスは設定に基づいて新しいデバイスとして検出されます。ボックスを開きガイドに沿った設定を行いたい場合はクイックセットアップウィザードをクリックしてください。すべての機能を使いたい方は高度なセットアップを使ってください。

1

クイックセットアップ・ウィザード
このウィザードはステップバイステップで設定を行います。ほとんどのユーザーの方への推奨設定方法です。

高度なセットアップ
すべての設定可能な機能が使えます。高度な機能を使うための正しい機能と順序を選択して設定できます。

図 12 クイックセットアップウィザードの実行

(2) クイックセットアップウィザードを実行するための注意事項と、必要な情報または環境を確認します。画面に表示されているメッセージと、「チェックリストはこちら」リンクラベルをクリックして表示されるメッセージを確認し、クイックセットアップウィザードを実行する準備をします。準備が完了したら、「始める」ボタンをクリックします。

クイックセットアップウィザードへようこそ

始める前に:

- サービスプロバイダから設定を完了するためのすべての情報を得ていることを確認してください。 [チェックリストはこちら](#)
- 3G/4G以外の WAN接続を設定する場合、サービスプロバイダとの物理的な接続が適切に確認してください。
- 3G/4G WAN接続を設定する場合、SIMカードがルータのスロットに適切に挿入されているか確認してください。
- ウィザードはデフォルトでいくつか推奨設定を行います。特に理由がない限り、設定変更ししないでください。
- このウィザードによって WAN/LAN接続の設定を簡単に行えます。ウィザードによる設定後、いつでも設定変更や拡張機能を追加できます。
- ベストプラクティス(COP Express)による設定時は、コンソール接続による設定変更や削除は行わないでください。

1

2

3 始める

図 13 クイックセットアップウィザードの準備



CheckList
✕

ルータIP アドレス :

- ✓ 静的IPアドレスであるか、動的に割り当てられるかについてはサービスプロバイダに確認してください。
- ✓ もし静的アドレスが割り当てられる場合は、IPアドレスとサブネットマスク情報を手元に控えておいて下さい。
- ✓ 同様にIPv6アドレスを設定する場合はサービスプロバイダから提供されたアドレスを控えておいてください。

DNSサーバ:

- ✓ DNSサーバに静的IPアドレスを使用するかどうか、サービスプロバイダに確認してください

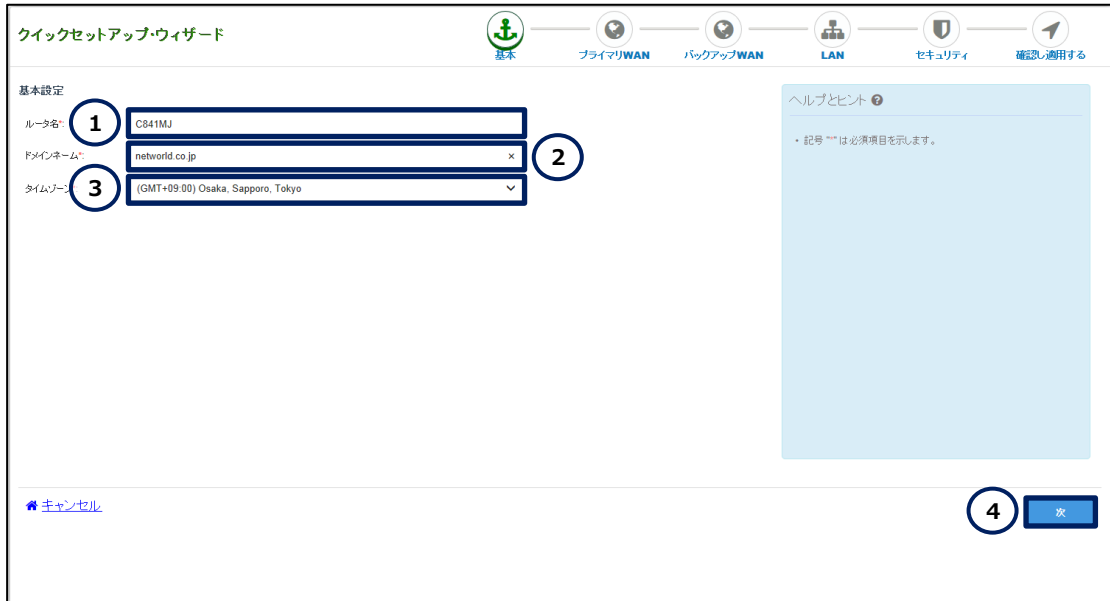
PPPoE ユーザ名とパスワード :

- ✓ PPPoEオプションが有効になっているときはPAP・CHAPの認証メカニズムを選択し、サービスプロバイダから提供されたユーザ名・パスワードを入力してください。

図 14 クイックセットアップウィザードのチェックリスト

(3) 基本設定を実行します。「*」ラベルが記載された設定は、必須の設定です。

- ① 「ルータ名」テキストボックスに製品のホスト名を入力します。
- ② 「ドメインネーム」テキストボックスに製品のドメイン名を入力します。ドメイン名が未定の場合は、仮のドメイン名を入力してください。ドメイン名の設定は、クイックセットアップウィザードによる製品の初期セットアップの完了後に変更できます。
- ③ 「タイムゾーン」ドロップダウンリストで **(GMT+09:00) Osaka, Sapporo, Tokyo** を選択します。
- ④ 「次」ボタンをクリックします。

クイックセットアップ・ウィザード

基本設定

ルータ名: CS41MJ

ドメイン名: network.co.jp

タイムゾーン: (GMT+09:00) Osaka, Sapporo, Tokyo

ヘルプとヒント

・記号 "*" は必須項目を示します。

キャンセル

4 *

図 15 基本設定

(4) プライマリ WAN の設定を実行します。「*」ラベルが記載された設定は、必須の設定です。

- ① 「WAN 接続タイプ」ドロップダウンリストから **Ethernet(Direct / PPPOE)** を選択します。
- ② 「インターフェイス」ドロップダウンリストから **GigabitEthernet0/4** を選択します。
- ③ 「ISP から直接 DNS サーバ情報を取得する」チェックボックスにチェックを入れます。
- ④ 「ISP から自動的に取得する」チェックボックスにチェックを入れます。
- ⑤ 「NAT を有効にする」チェックボックスにチェックを入れます。
- ⑥ 「IPv6 を有効にする」チェックボックスのチェックを外します。
- ⑦ 「PPPoE を有効化」チェックボックスにチェックを入れます。
- ⑧ 「PAP」チェックボックスのチェックを外します。
- ⑨ 「CHAP」チェックボックスにチェックを入れます。
- ⑩ 「ユーザー名」テキストボックスに ISP1 から提供された PPPoE ユーザー名を入力します。本書では、表 2 のとおり、**network@example.com** を使用しています。
- ⑪ 「パスワード」テキストボックスに ISP1 から提供された PPPoE パスワードを入力します。本書では、表 2 のとおり、**password** を使用しています。
- ⑫ 「パスワードを確認」テキストボックスに直前で入力したパスワードと同じパスワードを入力します。
- ⑬ 「詳細設定」リンクラベルをクリックします。
- ⑭ 「MTU サイズ」テキストボックスに ISP1 から指定された MTU サイズを入力します。本書では、表 2 のとおり、**1454** を使用しています。
- ⑮ 「MSS サイズ」テキストボックスに ISP1 から指定された MSS サイズを入力します。本書では、



表 2 のとおり、**1414** を使用しています。

⑯ 「次」ボタンをクリックします。

図 16 プライマリ WAN の設定

図 17 プライマリ WAN の設定（詳細設定）

(5) バックアップ WAN の設定を実行します。「*」ラベルが記載された設定は、必須の設定です。

- ① 「バックアップ WAN を有効化」チェックボックスにチェックを入れます。
- ② 「WAN 接続タイプ」ドロップダウンリストから **Ethernet(Direct / PPPOE)** を選択します。



- ③ 「インターフェイス」ドロップダウンリストから **GigabitEthernet0/5** を選択します。
- ④ 「ISP から自動的に取得する」チェックボックスにチェックを入れます。
- ⑤ 「NAT を有効にする」チェックボックスにチェックを入れます。
- ⑥ 「IPv6 を有効にする」チェックボックスのチェックを外します。
- ⑦ 「IP アドレス」テキストボックスにバックアップ経路への切り替えのトリガーにする死活監視対象の IP アドレスを入力します。本書では、**203.0.113.200** を使用しています。
- ⑧ 「PPPoE を有効化」チェックボックスにチェックを入れます。
- ⑨ 「PAP」チェックボックスのチェックを外します。
- ⑩ 「CHAP」チェックボックスにチェックを入れます。
- ⑪ 「ユーザー名」テキストボックスに ISP2 から提供された PPPoE ユーザー名を入力します。本書では、表 3 のとおり、**networkd@example.jp** を使用しています。
- ⑫ 「パスワード」テキストボックスに ISP2 から提供された PPPoE パスワードを入力します。本書では、表 3 のとおり、**password** を使用しています。
- ⑬ 「パスワードを確認」テキストボックスに直前で入力したパスワードと同じパスワードを入力します。
- ⑭ 「詳細設定」リンクラベルをクリックします。
- ⑮ 「MTU サイズ」テキストボックスに ISP2 から指定された MTU サイズを入力します。本書では、表 3 のとおり、**1454** を使用しています。
- ⑯ 「MSS サイズ」テキストボックスに ISP2 から指定された MSS サイズを入力します。本書では、表 3 のとおり、**1414** を使用しています。
- ⑰ 「次」ボタンをクリックします。

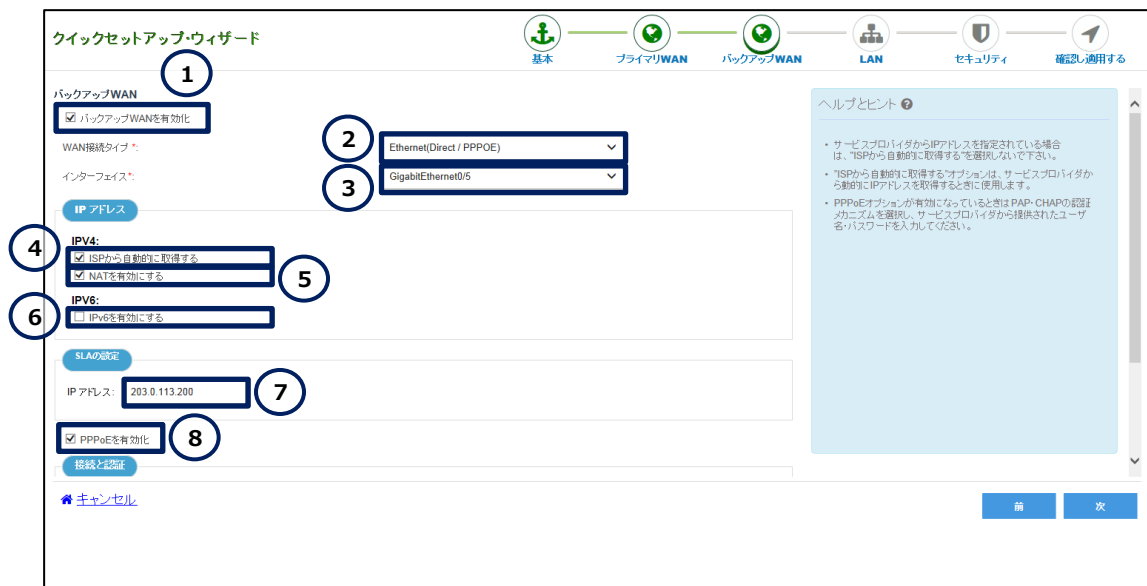


図 18 バックアップ WAN の設定

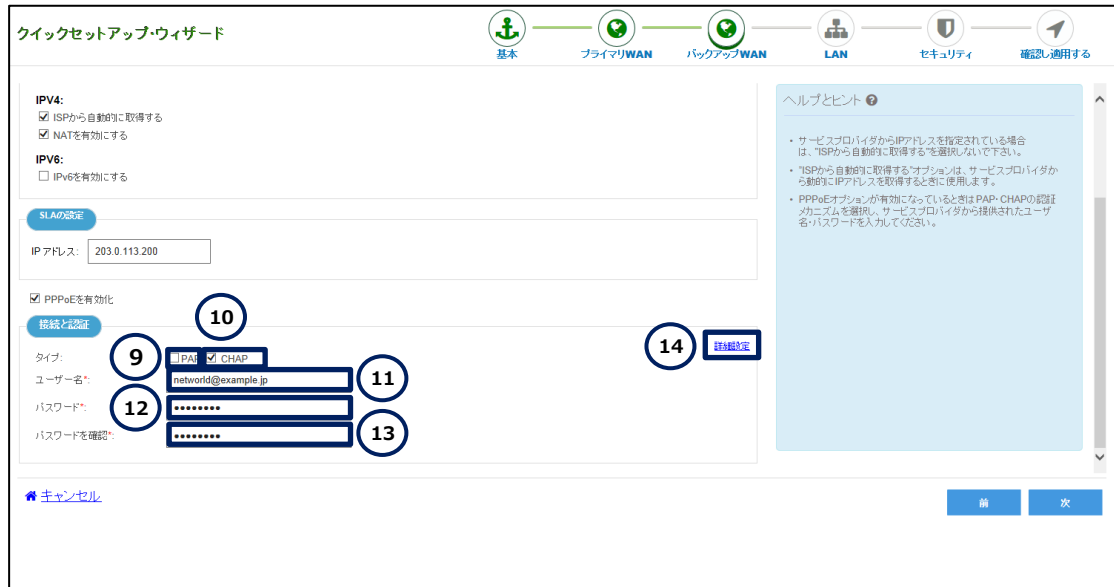


図 19 バックアップ WAN の設定 (つづき)

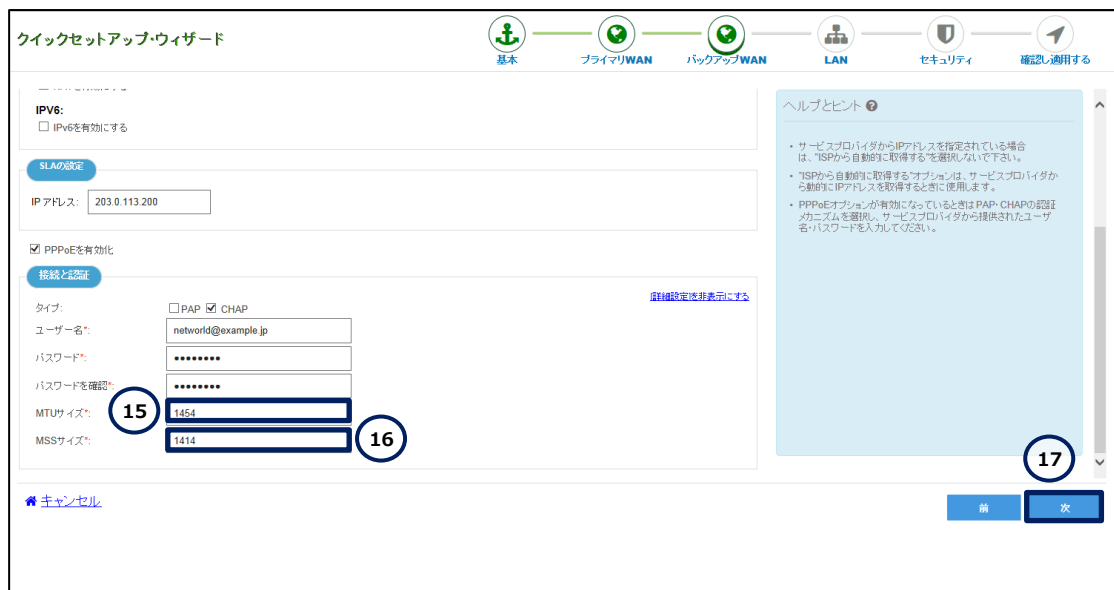


図 20 バックアップ WAN の設定 (詳細設定)

(6) LAN の設定を確認します。ここでは既定の VLAN と既定の DHCP プールを使用します。既定の VLAN では、すべての LAN 側インターフェースが VLAN1 に割り当てられます。既定の DHCP プールでは、10.10.10.0/25 の範囲の IP アドレスが VLAN1 用に確保されます。ただし、製品の既定の LAN 側 IP アドレスである 10.10.10.1 は、DHCP プールから除外されています。VLAN や DHCP プールの設定は、クイックセットアップウィザードによる製品の初期セットアップの完了後に変更できます。「次」ボタンをクリックします。

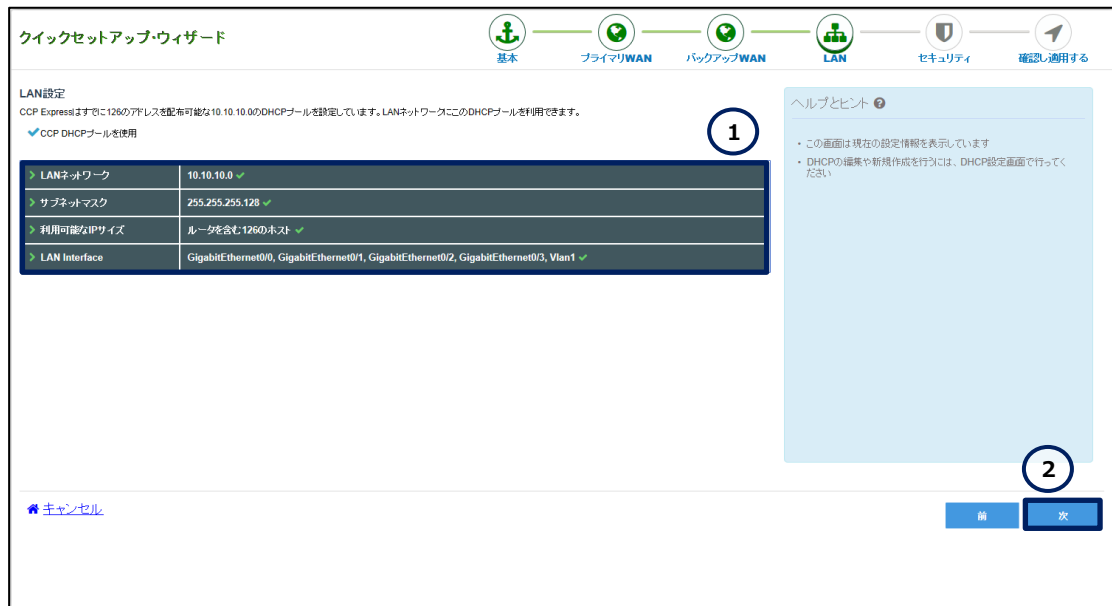


図 21 LAN の設定

(7) ファイアウォールの設定を実行します。既定のファイアウォールポリシーでは、WAN 側から発信されるすべてのトラフィックがブロックされます。また、LAN 側から発信されるトラフィックは、HTTP/HTTPS/S MTP/POP3/IMAP/SIP/FTP/DNS/ICMP のみ許可されます。ファイアウォールポリシーの設定は、クイックセットアップウィザードによる製品の初期セットアップの完了後に変更できます。

- ① 「ファイアウォール機能を有効化」チェックボックスにチェックを入れます。
- ② 「基本的なトラフィックを許可するポリシーを作成する（推奨）」チェックボックスにチェックを入れます。
- ③ 「次」ボタンをクリックします。

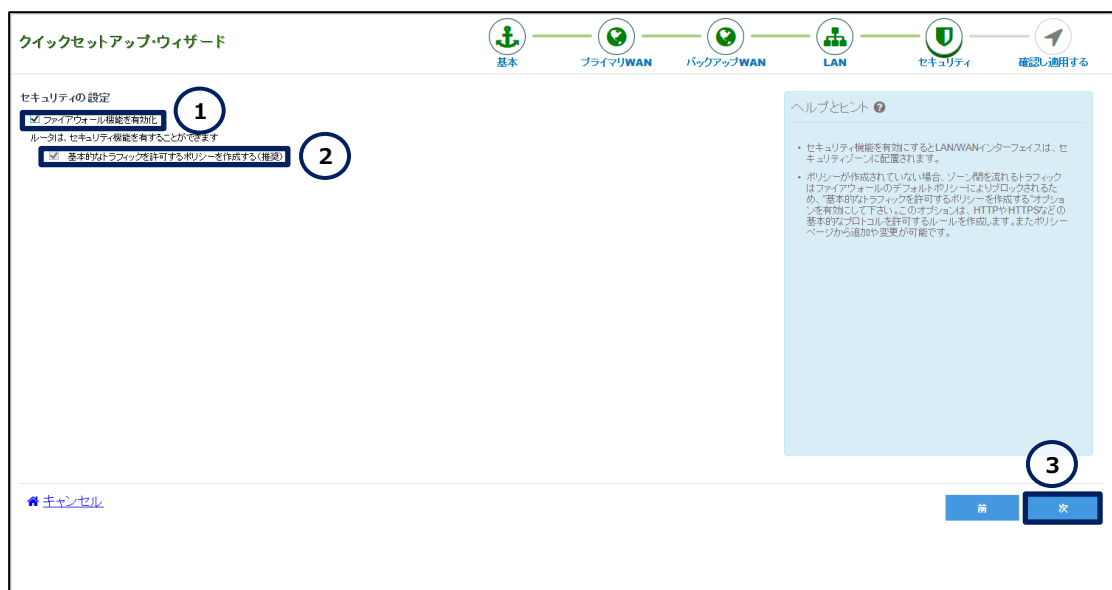




図 22 ファイアウォールの設定

(8) クイックセットアップウィザードで実行する設定内容を確認します。「設定」ボタンをクリックします。

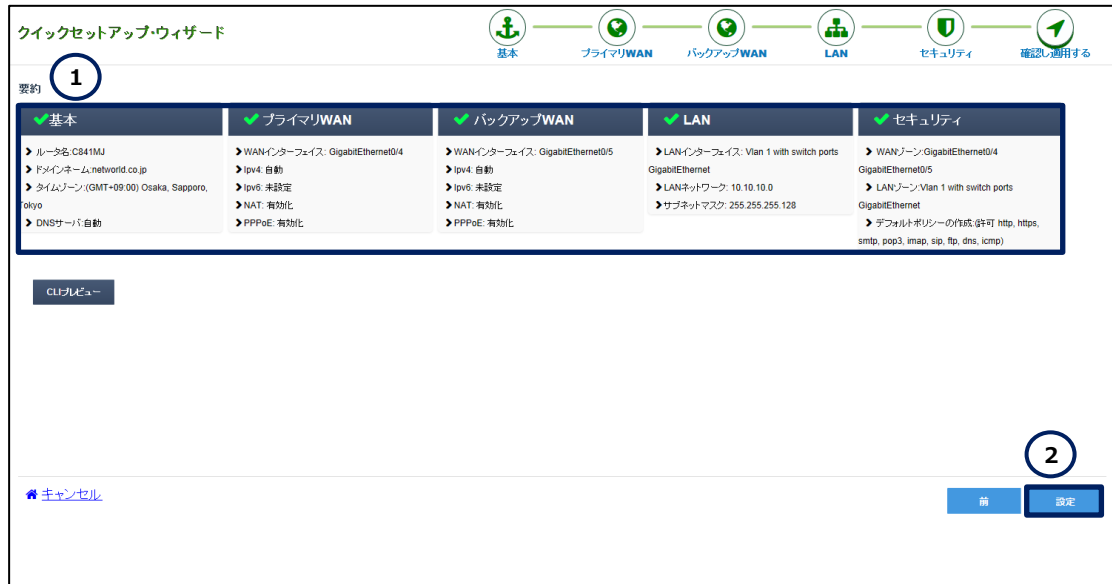


図 23 設定の要約

(9) クイックセットアップウィザードで実行する設定を確定します。「はい」ボタンをクリックします。

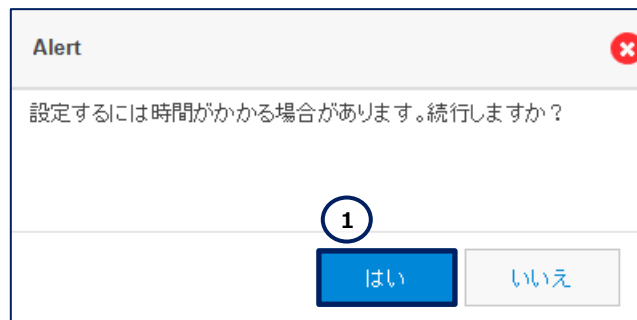


図 24 設定の確定

(10) しばらくすると、クイックスタートアップウィザードで実行した設定が完了します。WAN 接続テストを実行します。「WAN 接続テスト」ボタンをクリックします。何もしないと 10 秒後に自動的に CCP Express のダッシュボードにリダイレクトされてしまうのでご注意ください。



図 25 設定の完了

(11) ISP から割り当てられた IP アドレスと DNS サーバーの情報でインターネットに接続できることを確認します。



図 26 WAN 接続テスト

(12) WANが接続されると、「WAN」LEDが緑点灯（接続確立）または緑点滅（データ伝送中）します。また、ISPとPPPoEで正常に接続された場合、「PPP OK」LEDが緑点灯します。なお、「PPP OK」LEDは、少なくとも1つのPPP接続が確立している場合に緑点灯します。



図 27 WAN LED（緑点灯または緑点滅）と PPP OK LED（緑点灯）（C841M-8X-JAIS/K9 の場合）

以上で設定は完了です。ISP1 から割り当てられた IP アドレスと DNS サーバーの情報でインターネットに接続できることを確認してください。次に、Gi0/4 のケーブルを抜線してデフォルトゲートウェイをフェイルオーバーします。その後、ISP2 から割り当てられた IP アドレスと DNS サーバーの情報でインターネットに接続できることを確認してください。最後に、Gi0/4 のケーブルを結線してデフォルトゲートウェイをフェイルバックします。その後、再び ISP1 から割り当てられた IP アドレスと DNS サーバーの情報でインターネットに接続できることを確認してください。



4. 設定ファイル

本書で追加または変更される設定は、以下のとおりです。

```
001: hostname C841MJ
002: clock timezone GMT 9 0
003: ip dhcp pool ccp-pool
004: dns-server 10.10.10.1
005: ip domain lookup
006: ip domain name networkd.co.jp
007: flow record nbar-appmon
008: match ipv4 source address
009: match ipv4 destination address
010: match application name
011: collect interface output
012: collect counter bytes
013: collect counter packets
014: collect timestamp absolute first
015: collect timestamp absolute last
016: flow monitor application-mon
017: cache timeout active 60
018: record nbar-appmon
019: parameter-map type inspect global
020: max-incomplete low 18000
021: max-incomplete high 20000
022: nbar-classify
023: object-group network Others_dst_net
024: any
025: object-group network Others_src_net
026: any
027: object-group service Others_svc
028: ip
029: object-group network Web_dst_net
030: any
031: object-group network Web_src_net
032: any
```



```
033: object-group service Web_svc
034: ip
035: object-group network local_cws_net
036: object-group network local_lan_subnets
037: 10.10.10.0 255.255.255.128
038: object-group network vpn_remote_subnets
039: any
040: username networkld privilege 15 secret 5 password
041: track 1 ip sla 1 reachability
042: class-map type inspect match-any Others_app
043: match protocol https
044: match protocol smtp
045: match protocol pop3
046: match protocol imap
047: match protocol sip
048: match protocol ftp
049: match protocol dns
050: match protocol icmp
051: class-map type inspect match-any Web_app
052: match protocol http
053: class-map type inspect match-all Others
054: match class-map Others_app
055: match access-group name Others_acl
056: class-map type inspect match-all Web
057: match class-map Web_app
058: match access-group name Web_acl
059: policy-map type inspect LAN-WAN-POLICY
060: class type inspect Web
061: inspect
062: class type inspect Others
063: inspect
064: class class-default
065: drop log
066: zone security LAN
067: zone security WAN
068: zone-pair security LAN-WAN source LAN destination WAN
```



```
069: service-policy type inspect LAN-WAN-POLICY
070: interface GigabitEthernet0/4
071: description PrimaryWANDesc_
072: ip tcp adjust-mss 1414
073: no shutdown
074: pppoe enable group global
075: pppoe-client dial-pool-number 1
076: interface GigabitEthernet0/5
077: description BackupWANDesc_
078: ip tcp adjust-mss 1414
079: no shutdown
080: pppoe enable group global
081: pppoe-client dial-pool-number 2
082: interface Vlan1
083: ip nbar protocol-discovery
084: ip flow monitor application-mon input
085: ip flow ingress
086: ip flow egress
087: ip nat inside
088: ip virtual-reassembly in
089: zone-member security LAN
090: ip tcp adjust-mss 1414
091: load-interval 30
092: interface Dialer1
093: description PrimaryWANDesc__GigabitEthernet0/4
094: ip address negotiated
095: ip mtu 1454
096: ip nat outside
097: ip virtual-reassembly in
098: zone-member security WAN
099: encapsulation ppp
100: dialer pool 1
101: dialer-group 1
102: ppp mtu adaptive
103: ppp authentication chap callin
104: ppp chap hostname networkworld@example.com
```



```
105: ppp chap password 0 password
106: ppp ipcp dns request
107: no cdp enable
108: interface Dialer2
109: description BackupWANDesc__GigabitEthernet0/5
110: ip address negotiated
111: ip mtu 1454
112: ip nat outside
113: ip virtual-reassembly in
114: zone-member security WAN
115: encapsulation ppp
116: dialer pool 2
117: dialer-group 2
118: ppp mtu adaptive
119: ppp chap hostname networkworld@example.jp
120: ppp chap password 0 password
121: ppp ipcp dns request
122: no cdp enable
123: ip local policy route-map track-primary-if
124: ip dns server
125: ip nat inside source route-map nat2backup interface Dialer2 overload
126: ip nat inside source route-map nat2primary interface Dialer1 overload
127: ip route 0.0.0.0 0.0.0.0 Dialer1 track 1
128: ip route 0.0.0.0 0.0.0.0 Dialer2 253
129: ip route 203.0.113.200 255.255.255.255 Dialer1
130: ip access-list extended Others_acl
131: permit object-group Others_svc object-group Others_src_net
    object-group Others_dst_net
132: ip access-list extended Web_acl
133: permit object-group Web_svc object-group Web_src_net object-group
    Web_dst_net
134: ip access-list extended nat-list
135: permit ip object-group local_lan_subnets any
136: deny ip any any
137: ip sla auto discovery
138: ip sla 1
```



```
139: icmp-echo 203.0.113.200 source-interface Dialer1
140: ip sla schedule 1 life forever start-time now
141: dialer-list 1 protocol ip permit
142: dialer-list 2 protocol ip permit
143: route-map track-primary-if permit 1
144: match ip address 197
145: set interface Dialer1
146: route-map nat2primary permit 1
147: match ip address nat-list
148: match interface Dialer1
149: route-map nat2backup permit 1
150: match ip address nat-list
151: match interface Dialer2
152: access-list 197 permit icmp any host 203.0.113.200
```

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

