MR814v2 ケーブル /DSL ワイヤレスルータ用リファレンスマニュアル

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

SM-MR814NA-2
バージョン 4.12
2003 年 4 月

商標

NETGEAR は Netgear, Inc. の商標です。

Microsoft、Windows、Windows NT は Microsoft Corporation の登録商標です。

その他のブランド名と製品名は、それぞれの所有者の登録商標または商標です。

条件の通知

内部設計、操作機能、信頼性を改良するために、NETGEAR は本書で説明した製品を予告なしに変更する権利を留保します。

NETGEAR は、本書で記載した製品または回路レイアウトの使用または適用によって発生したことに関して、責任を負うことはありません。

米連邦通信委員会 (FCC) への準拠通知：無線周波数通知

本装置は、FCC 基準パート 15 に準ずる Class B のデジタル電子機器の制限事項に準じています。これらの制限事項は、住宅地域で使用した場合に生じる可能性のある電磁障害を規制するために制定されたものです。本装置は高周波エネルギーを生成し使用しています。また、高周波エネルギーを放射する可能性があるため、指示に従って正しく設置しなかった場合は、無線通信に障害を及ぼす可能性があります。しかしながら、特定の設置状況においては電波障害を起こさないという保証はありません。本装置がラジオやテレビの受信に障害を与えていないかを判断するには、本装置の電源をオンオフしてみます。受信障害が発生している場合には、以下の方法で受信障害を改善することをお薦めします。

- 受信アンテナの方向または設置位置を変える。
- 本装置と受信機の距離を離す。
- 本装置と受信機の電源系列を別の回路にする。
- 販売店やラジオ / ビデオの専門技術者に問い合わせる。

EN 55 022 適合性の通知

本通知は、MR814v2 ケーブル /DSL ワイヤレスルータが理事会指令 89/336/EEC, Article 4a の適用に基づき、無線周波数の生成に対してシールドされています。適合性は EN 55 022 Class B (CISPR 22) の適用によって宣言されています。

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das MR814v2 ケーブル /DSL ワイヤレスルータ gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

メーカー / 輸入業者の証明書

MR814v2 ケーブル /DSL ワイヤレスルータが BMPT-AmtsblVfg 243/1991 および Vfg 46/1992 で指定された条件 に従って抑制されていることをここに証明します。しかしながら、規制に基づく一部の装置（例えば、テストトランスミッタ）の操作は、規制に従うものとします。操作説明書の注を参照してください。

電気通信認可連邦局は、本装置を販売する旨の通知を受け、規制に準拠するために一連のテストを行う権利を与えられています。

障害 (VCCI) 声明に対する自主規制制御

本装置は第 2 カテゴリ（住宅地域または住宅に隣接する地域で使用する情報装置）に属し、かかる住宅地域で無線周波数を妨げる目的で、データ処理装置およびエレクトロニックオフィスマシンにより、障害自主規制委員会が設定した基準に準拠しています。

ラジオやテレビの傍で使用するとき、電波障害を引き起こすことがあります。

正しい操作については、説明書をお読みください。

カスタマサポート

MR814v2 ケーブル /DSL ワイヤレスルータに付属するサポート情報カードを参照してください。

ワールドワイドウェッブ

NETGEAR は WWW ホームページを保有し、URL でアクセスできます。
http://www.netgear.com. Internet Explorer や Netscape などのインターネットおよびウェブブラウザに直接接続する必要があります。

目次

はじめに
本書について

NETGEAR® MR814v2 ケーブル /DSL ワイヤレスルータをお買い上げいただきありがとうございます。

MR814v2 ルータは、通常単一 PC で使用するように意図された外部ブロードバンドアクセスデバイス（ケーブルモデムや DSL モデムなど）を通して、複数のパソコン (PC) がインターネットに接続できるようにしています。

対象読者

このリファレンスマニュアルは、読者が中間コンピュータやインターネットスキルに対する基礎知識を持っていることを前提としています。ただし、基礎のコンピュータネットワーク、インターネット、ファイヤウォール、VPN テクノロジのチュートリアル情報を、付録や Netgear のウェブサイトで提供しています。

表記方法

このガイドは、次の表記方法を使用します。

イタリック	メディアのタイトルと URL
ボールド　タイムズローマン	ユーザー入力
クーリエフォント	スクリーンテキスト。
[Enter]	テキストの指定されたキーは、角括弧で囲まれています。記号 [Enter] は、Enter キーと Return キー用に使用されます。
[Ctrl]+C	2 つ以上のキーを同時に押す動作は、(+) 記号でリンクされたテキストで表示されます。
小文字	ファイルとディレクトリ名。

特殊なメッセージフォーマット

本ガイドは、次のフォーマットを使用して特別なメッセージを強調表示します。

	**注**：このフォーマットは、重要なまたは特定関心事の情報を強調表示するために使用されます。

第 1 章
はじめに

本章では、NETGEAR MR814v2 ケーブル /DSL ワイヤレスルータの機能について説明します。

ルータの主な機能

4 ポートスイッチを搭載する MR814v2 ケーブル /DSL ワイヤレスルータは、ケーブルモデムや DSL モデムなどの外部アクセスデバイスを通して、構内通信網 (LAN) をインターネットに接続します。

MR814v2 ルータはユーザーに複数のウェブコンテンツフィルタリングオプション、およびブラウジングアクティビティリポーティング、電子メールによるインスタントアラートを提供します。両親とネットワーク管理者は日時、ウェブサイトアドレス、アドレスキーワードに基づく制限されたアクセスポリシーを確立し、最大 253 台のパソコンで高速ケーブル /DSL インターネットアクセスを共有します。ネットワークアドレス変換 (NAT) 機能の他に、内蔵のファイヤウォールがハッカーから保護します。

最小のセットアップで、ルータを数分でインストールして使用できます。

MR814v2 ルータは次の機能を提供します。

- 802.11b 標準ベースのワイヤレスネットワーキング
- インストールと管理が簡単な、ウェブベースのセットアップ
- コンテンツフィルタリングとサイトブロッキングセキュリティ
- 内蔵の 4 ポート 10/100 Mbps スイッチ
- ケーブルモデムや DSL モデムなどの、広域ネットワーク (WAN) デバイスへのイーサネット接続
- 広範囲なプロトコルサポート
- ログイン機能
- ステータスとアクティビティを簡単に監視するためのフロントパネル LED
- フラッシュメモリファームウェアのアップグレード用

802.11b 標準ベースのワイヤレスネットワーキング

MR814v2 ルータには、802.11b 準拠のワイヤレスアクセスポイントが組み込まれ、ワイヤレスとイーサネットデバイス間に連続した、高速 11 Mbps アクセスを提供します。アクセスポイントは以下を提供します。

- 最大 11 Mbps の速度の 802.11b 標準ベースのワイヤレスネットワーキング
- 64 ビットと 128 ビット WEP 暗号化セキュリティ
- WEP キーは、手動でまたはパスフレーズで生成できます。
- ワイヤレスアクセスは、MAC アドレスによって制限できます。
- ワイヤレスネットワーク名ブロードキャストは、ネットワーク名 (SSID) を持つデバイスのみが接続できるように、オフにすることができます。

協力で、真のファイヤウォールコンテンツフィルタリング付き

単純なインターネット共有 NAT ルータとは異なり、MR814v2 はハッカーの攻撃から守るためのステートフルパケットインスペクションを使用する、真のファイヤウォールです。そのファイヤウォール機能には、次のものが含まれます。

- サービス拒絶 (DoS) 保護

  Ping of Death、SYN Flood、LAND Attack、IP Spoofing などの DoS 攻撃を自動的に検出して阻止します。
- インターネットから LAN への好ましからざるトラヒックをブロックします。
- LAN からオフリミットとして指定した、インターネットの場所またはサービスへのアクセスをブロックします。
- セキュリティインシデントをログします。

  MR814v2 はブロックされた着信トラヒック、ポートスキャン、攻撃、管理者ログインなどのセキュリティイベントをログします。ルータを設定して指定した間隔でログを電子メール送信できます。重要なイベントが発生した場合は常に、電子メールアドレスや電子メールページャにアラートメッセージを瞬時に送信するように、ルータを設定することもできます。
- コンテンツフィルタリング機能を使用して、MR814v2 は好ましくないコンテンツが PC に届くのを防ぎます。ルータにより、ウェブアドレス内のキーワードをふるいにかけることによって、インターネットコンテンツへのアクセスを制御できます。好ましくないインターネットサイトへのアクセスの試みをログし報告するように、ルータを設定できます。

セキュリティ

MR814v2 ルータには、本項で説明したように、セキュリティを保持するために設計されたいくつかの機能が組み込まれています。

- NAT により非表示された PC
  NAT はローカルネットワークから発せられる要求に対して、インターネットへの一時的パスを開きます。LAN の外部から発せられる要求は廃棄され、LAN 外部のユーザーは LAN の PC を検索し直接アクセスすることができません。
- NAT を組み込んだポートフォーワーディング
  NAT は、インターネットロケーションが LAN に接続された PC にアクセスできないようにしますが、ルータは入力トラヒックが着信要求のサービスポート番号に基づく特定の PC に、または指定された 1 台の「DMZ」ホストコンピュータに送信することを可能にします。単一ポートまたはさまざまなポートの転送を指定できます。

Auto Uplinkô でイーサネット接続を自動検出する

内部 8 ポートの 10/100 スイッチを使用して、MR814v2 は 10 Mbps の標準イーサネットネットワークまたは 100 Mbps のファーストイーサネットネットワークに接続できます。LAN と WAN インターフェイスはどちらも、全二重または半二重操作を自動検出し可能にします。

ルータには、Auto Uplink™ テクノロジが組み込まれています。それぞれのローカルイーサネットポートは、ポートに接続されるイーサネットケーブルが PC などへの「標準の」接続を持っているのか、スイッチやハブなどへの「アップリンク」接続を持っているかを検出します。そのポートは、次に正しい設定にそれ自身を設定します。この機能は、クロスオーバーケーブルに関する心配を不要のものとしていますが、それは Auto Uplink がケーブルのどちらかのタイプを受け入れて正しい接続を行っているからです。

広範囲なプロトコルサポート

MR814v2 ルータは伝送制御プロトコル / インターネットプロトコル (TCP/IP) とルーティング情報プロトコル (RIP) をサポートします。TCP/IP に関する詳細については、付録 B、「ネットワーク、ルーティング、ファイアウォール、ベーシック」を参照してください。

- NAT による IP アドレス共有
  MR814v2 ルータにより、複数のネットワークに接続された PC は、インターネットサービスプロバイダ (ISP) により静的または動的に割り当てられるたった 1 つの IP アドレスを使用して、インターネットアカウントを共有することができます。NAT として知られているこの技術は、安価な単一ユーザー ISP アカウントの使用を可能にします。
- DHCP により接続された PC の自動設定
  MR814v2 ルータは IP、ゲートウェイ、ドメイン名サーバー (DNS) などのネットワーク設定情報をダイナミックに割り当て、ダイナミックホスト設定プロトコル (DHCP) を使用して、PC を LAN に接続します。この機能は、ローカルネットワーク上の PC の設定を大幅に単純化しています。
- DNS プロキシ
  DHCP が有効で DNS アドレスが 1 つも指定されていないとき、ルータは独自のアドレスを接続された PC への DNS サーバーとして提供します。ルータは接続セットアップの間 ISP から実際の DNS アドレスを取得し、LAN から DNS 要求を転送します。
- PPP オーバーイーサネット (PPPoE)
  PPPoE は、ダイヤルアップ接続をシミュレートして、リモートホストを DSL 接続のインターネットに接続するためのプロトコルです。この機能は、PC の Entersys や WinPOET などのログインプログラムを実行する必要を排除します。

簡単なインストールと管理

ネットワークに接続した後、数分で MR814v2 ケーブル /DSL ワイヤレスルータをインストール、設定、操作することができます。次の機能は、インストールと管理タスクを単純化します。

- ブラウザベースの管理
  ブラウザベースの設定により、Windows、Macintosh、Linux などほとんど全てのタイプのパソコンからルータを簡単に設定することができます。ブラウザベースのウェブ管理インターフェイスには、使い勝手のいいセットアップウィザードが提供され、オンラインのヘルプ文書が組み込まれています。
- スマートなウィザード
  MR814v2 ルータはインターネット接続のタイプを自動的に検出し、お使いのタイプの ISP アカウントで要求される情報のみを問い合わせます。
- ビジュアル監視
  MR814v2 ルータのフロントパネル LED は、そのステータスとアクティビティをモニタするための簡単な方法を提供します。

メンテナンスとサポート

NETGEAR は次の機能を提供して、MR814v2 ルータを最大限利用できるようにしています。

- ファームウェアアップグレード用フラッシュメモリ
- 1 週 7 日、1 日 24 時間の、無料技術サポート

パッケージの内容

製品パッケージには、次のアイテムが入っています。

- MR814v2 ケーブル /DSL ワイヤレスルータ .
- AC 電源アダプタ
- カテゴリ 5(CAT5) イーサネットケーブル
- *MR814v2 リソース CD* には、次のものが含まれています。
  - 本書。
  - アプリケーションの注とその他の役に立つ情報。
- 登録カードと保証書。
- サポート情報カード。

付属品が間違っていたり、不足または破損しているときは、NETGEAR の販売店にご連絡ください。修理のためにルータを送り返すときに必要となる場合があるので、製品を梱包していた箱と梱包材料は捨てずに保管して置いてください。

ルータのフロントパネル

MR814v2 ルータのフロントパネルには、下で説明するステータス LED が含まれています。

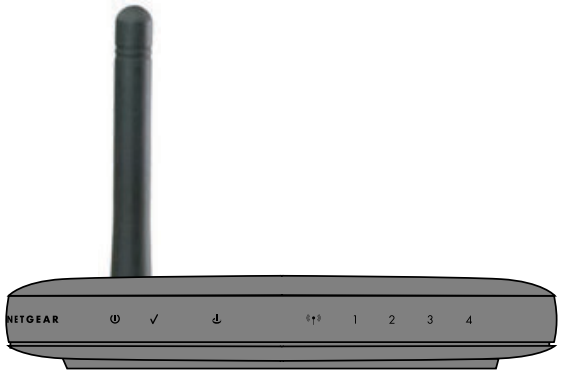


図 1-1 MR814v2 フロントパネル

いくつかの LED を使用して接続を確認できます。左から右に表示されているように、表 1-1 はルータのフロントパネルの LED を説明しています。これらの LED は、点灯中は緑になっています。

表 1-1. LED の説明

ラベル	アクティビティ	説明
電源	オン オフ	電源はルータに付属しています。 電源はルータに付属していません。
インターネット	オン 点滅	インターネット（広域ネットワーク）ポートが接続されているデバイスと共にリンクを検出しました。 データは、インターネットポートにより送受信されています。

表 1-1. LED の説明

ワイヤレス	オン	ワイヤレスポートが初期化されていることを示します。
ローカル	オン（緑） 点滅（緑） オン（茶色） 点滅（茶色） オフ	ローカル (LAN) ポートは、100 Mbps デバイスを持つリンクを検出しました。 データは 100 Mbps で送受信されています。 ローカルポートは、10 Mbps デバイスを持つリンクを検出しました。 データは 10 Mbps で送受信されています。 このポートで、リンクは検出されません。

ルータのリアパネル

モデル RP614 ルータのリアパネルには、下に一覧するポート接続が含まれています。

図 1-2: MR814v2 リア パネル

左から右へ表示されているように、リアパネルには次の機能が含まれています。

- AC 電源アダプタコンセント
- ルータをローカルの PC に接続するための 4 つのローカル (LAN) イーサネットポート
- ルータをケーブルや DSL モデムに接続するためのインターネット (WAN) イーサネットポート
- 出荷時設定のリセットプッシュボタン
- ワイヤレスアンテナ

第 2 章
ルータをインターネットに接続する

本章では、構内通信網 (LAN) でルータをセットアップしインターネットに接続する方法を説明します。セットアップウィザードを使用してインターネットアクセス用に MR814v2 ケーブル /DSL ワイヤレスルータを設定する方法、またはインターネット接続を手動で設定する方法が表示されます。

始める前に必要なもの

始める前にこれら 3 つのものを準備する必要があります。

1. ケーブルまたはブロードキャストアカウントによって提供されるインターネットサービスをアクティブにします。
2. DSL アカウント用のインターネットサービスプロバイダ (ISP) の設定情報を検索します。
3. 下で説明するように、ルータをケーブルまたは DSL モデムとコンピュータに接続します。

ケーブル配線とコンピュータハードウェアの要件

ネットワークで MR814v2 ルータを使用するには、各コンピュータはイーサネットネットワークインターフェイス (NIC) とイーサネットケーブルをインストールする必要があります。コンピュータを 100 Mbps でネットワークに接続する場合、ルータに付属するカテゴリ 5 (CAT5) ケーブルを使用する必要があります。

コンピュータネットワーク設定要件

MR814v2 には、内蔵のウェブ設定マネージャが組み込まれています。MR814v2 の設定メニューにアクセスするには、Java 対応のウェブブラウザプログラムを使用する必要があります。このプログラムは Microsoft Internet Explorer または Netscape Navigator などの HTTP アップロードをサポートしています。NETGEAR は、Internet Explorer または Netscape Navigator 4.0 以降を使用することを推奨します。無料のブラウザプログラムは、Windows、Macintosh、UNIX/Linux ですぐ使用することができます。

インターネットに始めて接続しルータを設定する場合、ルータにコンピュータを接続すると、DHCP を介してルータからその TCP/IP 設定を自動的に取得するように設定されます。

注：DHCP 設定のヘルプについては、付録 C、「ネットワークの準備をする」を参照してください。

ケーブルまたは DSL モデムのブロードバンドアクセスデバイスは、標準の 10 Mbps (10BASE-T) イーサネットインターフェイスを提供する必要があります。

インターネット設定要件

ISP がインターネットアカウントをセットアップする方法に従って、インターネットにルータを接続するためには、1 つまたは複数の設定パラメータが必要になります。

- ホストおよびドメイン名
- ISP ログイン名とパスワード
- ISP ドメイン名サーバー (DNS) アドレス
- スタティック IP アドレスとしても知られている固定 IP アドレス

インターネット設定パラメータは、どこで入手できますか？

必要なインターネット接続情報を収集する方法は、いくつかあります。

- ISP は、インターネットに接続するために必要な全ての情報を提供します。この情報が見つからない場合、それを ISP に要求したり、下のどれかのオプションを試みることができます。
- アクティブなインターネットアクセスアカウントを使用してコンピュータをすでに接続している場合、そのコンピュータから設定情報を収集できます。

  - — Windows 95/98/ME の場合、[ネットワーク] コントロールパネルを開き、イーサネットアダプタ用の TCP/IP エントリを選択し、[プロパティ] をクリックします。各タブページに対する全ての設定を記録します。
  - — Windows 2000/XP の場合、構内通信網 (LAN) 接続を開き、イーサネットアダプタ用の TCP/IP エントリを選択し、[プロパティ] をクリックします。各タブページに対する全ての設定を記録します。
  - — Macintosh コンピュターの場合、TCP/IP またはネットワークコントロールパネルを開きます。各セクションに対する全ての設定を記録します。
- 多くの ISP に対してインターネット接続情報を提供する NETGEAR ルータ ISP ガイドについては、*MR814v2 リソース CD* を参照することもできます。

インターネット設定パラメータが見つかったら、下のページにそれを記録することができます。

インターネット接続情報を記録する

このページを印刷します。インターネットサービスプロバイダ (ISP) から得た設定パラメータを記入してください。

ISP ログイン名 ログイン名とパスワードは大文字と小文字を区別し、ISP から提供されたとおりに入力する必要があります。サービス名は、全ての ISP に必要なわけではありません。ログイン名とパスワードを使用して接続する場合、次の情報を入力してください。

ログイン名：_____

パスワード：_____

サービス名：_____

固定またはスタティック IP アドレス： スタティック IP アドレスを持っている場合、次の情報を記録してください。例えば、169.254.141.148 は有効な IP アドレスかもしれません。

固定またはスタティックインターネット IP アドレス：_____ . _____ . _____ . _____

ゲートウェイ IP アドレス：_____ . _____ . _____ . _____
サブネットマスク：_____ . _____ . _____ . _____

ISP DNS サーバーアドレス DNS サーバーアドレスを与えられている場合、次の情報を入力してください。

プライマリ DNS サーバー IP アドレス：_____ . _____ . _____ . _____

セカンダリ DNS サーバー IP アドレス：_____ . _____ . _____ . _____

ホストおよびドメイン名：一部の ISP は、**CCA7324-A** または **ÉzÅ[ÉÄ** のような特定ホストまたはドメイン名を使用します。ホスト名やドメイン名を与えられていない場合、次の例をガイドとして使用できます。

- ISP でのメインの電子メールアカウントが **aaa@yyy.com** なら、ホスト名として **aaa** を使用します。ISP はこれをユーザーのアカウント、ユーザー名、ホスト名、コンピュータ名、システム名と呼ぶこともあります。
- ISP のメールサービスが **mail.xxx.yyy.com** なら、ドメイン名として **xxx.yyy.com** を使用します。

ISP ホスト名：_____

ISP ドメイン名：_____

ワイヤレスアクセス***の場合：***ワイヤレスネットワークの設定については、次の情報を記録してください。
ワイヤレスネットワーク名 (SSID)：_____
暗号化（サークルワン）：WEP 64、WEP 128、または IPSec
WEP パスフレーズまたはキー：_____

LAN に MR814v2 を接続する

本項では、MR814v2 ルータを接続するため手順を説明します。また、ルータに付属する *MR814v2 リソース CD* には、この手順を簡単に実行するためのアニメ付きインストールアシスタントが含まれています。

手順： ルータを接続する

ルータの接続には、3 つのステップがあります。

1. ネットワークにルータを接続する
2. ルータにログインする
3. インターネットに接続する

ルータをネットワークに接続するには、下のステップに従ってください。ルータに付属するリソース CD を参照すると、アニメ付きインストールアシスタントでこの手順を簡単に実行することもできます。

1. ネットワークにルータを接続します。

a. コンピュータの電源およびケーブルまたは DSL モデムをオフにします。

b. ケーブルまたは DSL モデムに接続するコンピュータから、イーサネットケーブル **(A)** を切り離します。

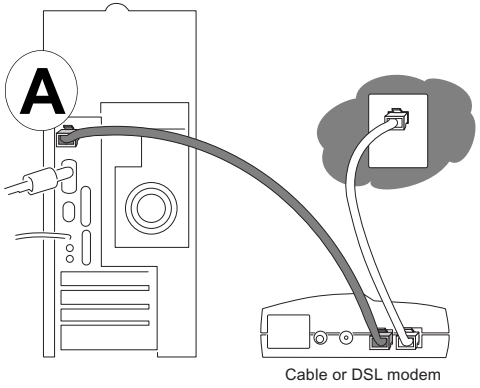


図 2-1 ケーブルまたは DSL モデムを切り離す

c. ケーブルまたは DSL モデムから MR814v2 のインターネットポート (A**)** にイーサネットケーブルを接続します。

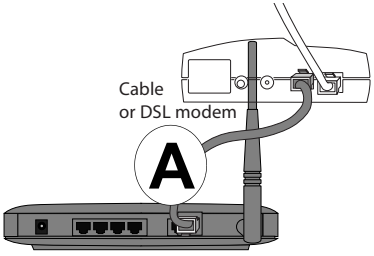


図 2-2 ケーブルまたは DSL モデムをルータに接続する

d. ルータ (B**)** のローカルポートからルータに付属するイーサネットケーブルをコンピュータに接続します。

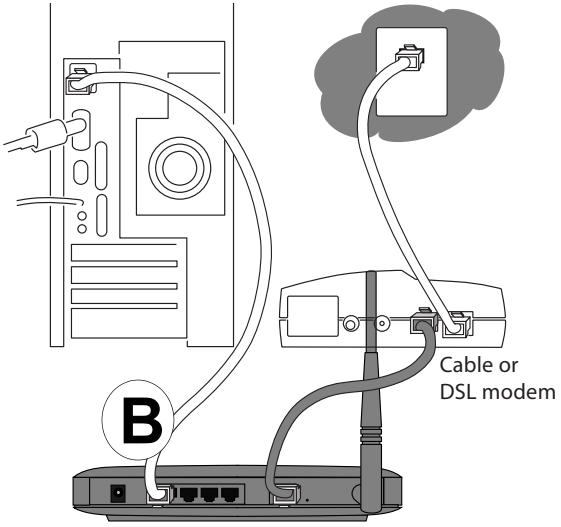


図 2-3 ネットワークのコンピュータをルータに接続する

注：MR814v2 ルータには、Auto Uplink™ テクノロジが組み込まれています。それぞれのローカルイーサネットポートは、ケーブルが標準接続を使用しているかアップリンク接続を使用しているかを自動的に検出します。この機能では、Auto Uplink がどちらのタイプのケーブルも正しく接続するために、クロスオーバーケーブルについて心配する必要はありません。

e. コンピュータの電源をオンにしてください。ソフトウェアを使用してインターネット接続にログインする場合、自動的にスタートしても、そのソフトウェアを実行しないかキャンセルしてください。

f. 次を確認します。

ルータの電源をオンにすると、電源ライトが点灯します。

ルータのローカルのライトは、接続されている全てのコンピュータで点灯します。

ルータのインターネットライトが点灯し、リンクがケーブルまたは DSL モデムに対して確立されていることを示します。

注：ワイヤレス配置と範囲のガイドライン、ワイヤレス設定の説明については、第 3 章、「ワイヤレス設定」をご覧ください。

2. ルータにログインす

注：ルータに接続するには、コンピュータが DHCP を介して IP アドレスを自動的に取得するように設定する必要があります。これを行う方法の説明については、付録 C、「ネットワークの準備をする」を参照してください。

a. Internet Explorer または Netscape® Navigator のアドレスフィールドに *http://192.168.0.1* を入力して、ルータに接続します。

図 2-4 ルータにログインする

b. 安全のために、ルータは独自のユーザー名とパスワードを使用します。要求されたら、ルータパスワードのルータ ユーザー名と **パスワード**に対して、どちらも小文字で **admin** を入力してください。

注：ルータのユーザー名とパスワードは、インターネット接続にログインするために使用するユーザー名またはパスワードと同じではありません。

下に示すログインウィンドウが開きます。

図 2-5 ログインウィンドウ

3. インターネットに接続する

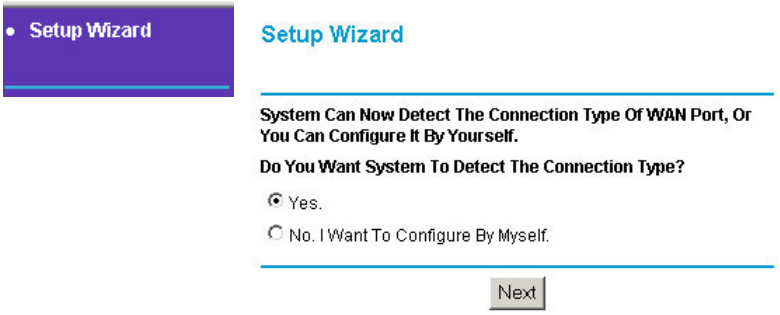


図 2-6 セットアップウィザード

a. これで、ルータに接続されました。上のメニューが表示されない場合、メインメニューの左上にある [セットアップウィザード] リンクをクリックしてください。

b. [次へ] をクリックし、[セットアップウィザード] のステップに従って ISP から取得した設定パラメータを入力し、インターネットに接続してください。

注：[セットアップウィザード] を使用しないを選択した場合、2-15 ページの「インターネット接続を手動で設定する」手順に従うことによって、インターネット接続を手動で設定することができます。

ISP が DHCP を介して設定を自動的に割り当てない限り、2-3 ページの「インターネット接続情報を記録する」で以前記録した ISP の設定パラメータが必要になります。

c. ルータがアクティブなインターネットサービスを正常に検出すると、ルータのインターネット LED が点灯します。[セットアップウィザード] はどの接続タイプが見つかったかを報告し、適切な設定メニューを表示します。[セットアップウィザード] が接続を検出できなかった場合、ルータとケーブルまたは DSL 線の間の物理接続をチェックするように要求されます。

d. [セットアップ] ウィザードは、見つかった接続のタイプを報告します。オプションには、次のものがあります。

- 以下のようなプロトコルを使用したログインが必要な接続：PPPoE、PPTP、Telstra、または Bigpond ブロードバンド接続。
- ダイナミック IP アドレス割り当てを使用する接続。
- 固定した IP アドレス割り当てを使用する接続。

接続の各タイプに対して設定メニューに入力する手順には、以下のものがあります。

PPPoE ウィザード検出オプション

[セットアップウィザード] が ISP の使用する PPPoE を発見したら、このメニューが表示されます。

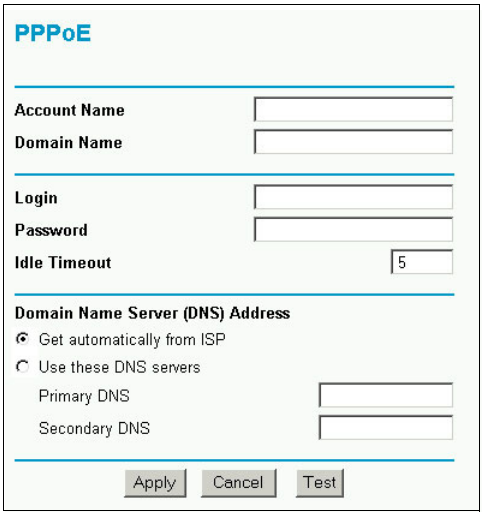


図 2-7 PPPoE アカウントに対する [セットアップウィザード]

- ISP が提供したアカウント名、ドメイン名、ログイン、パスワードを入力します。これらのフィールドは、大文字と小文字を区別します。ドメイン名をブランクにしておくと、ルータはドメインを自動的に発見しようとします。発見しない場合、ドメインを手動で入力する必要があります。
- ログインタイムアウトを変更するには、分で新しい値を入力してください。ログインタイムアウトは、LAN からのインターネット活動がない場合、ルータがインターネット接続活動を維持する時間を決定します。ゼロのタイムアウト値を入力すると、決してログアウトしません。

  注：インターネットに接続するために、PC で ISP のログインプログラムを実行する必要はありません。インターネットアプリケーションを起動すると、ルータが自動的にログインします。

- ログイン中に ISP が DNS アドレスをルータに自動的に送信しない場合、「これらの DNS サーバーを使用」を選択し、ISP のプライマリ DNS サーバーの IP アドレスを入力します。セカンダリ DNS サーバーアドレスが利用できる場合、それも入力してください。

  注：DNS アドレスを入力したら、コンピュータを再起動してこれらの設定が有効にしてください。
- [適用] をクリックして、自分の設定を保存します。
- [テスト] をクリックして、インターネット接続が機能することを確認します。NETGEAR のウェブサイトが 1 分以内に表示されない場合、第 7 章、「トラブルシューティング」を参照してください。

Telstra Bigpond ケーブルウィザード検出オプション

[セットアップウィザード] が Telstra Bigpond ケーブルが ISP であることを発見したら、このメニューが表示されます。

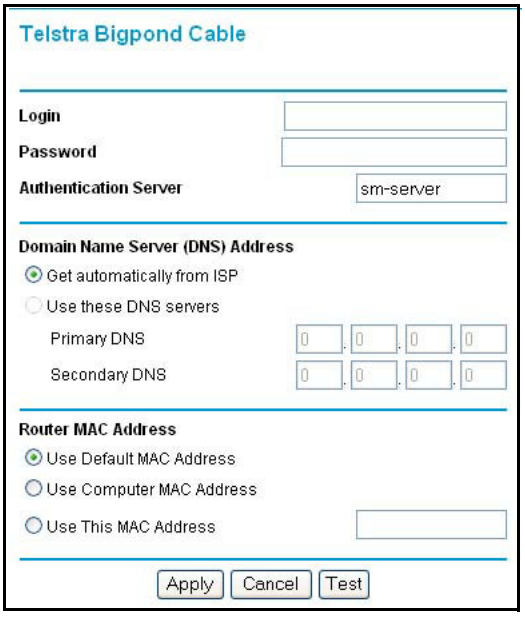


図 2-8 Telstra Bigpond ケーブルアカウントに対する [セットアップウィザード] メニュー

- ログイン、パスワードおよび 認証サーバーを入力します。これらのフィールドは、大文字と小文字を区別します。

  注：インターネットに接続するために、PC で ISP のログインプログラムを起動する必要はありません。インターネットアプリケーションを起動すると、ルータが自動的にログインします。

- ドメイン名サーバーの (DNS) アドレスパラメータは、メールや新しいサーバーなどの ISP のサービスにアクセスする必要があります。
  注：DNS アドレスを入力したら、コンピュータを再起動してこれらの設定が有効にしてください。

- ルータ MAC アドレス
  本項では、インターネットポートのルータによって使用されるイーサネット MAC アドレスを説明します。一部の ISP は、アカウントを始めて開くとき、PC のネットワークインターフェイスカードのイーサネット MAC アドレスを登録します。そして、その PC の MAC アドレスからくるトラヒックのみを受け入れます。この機能により、ルータはその PC を装うことができます。

  MAC アドレスを変更するには、「このコンピュータの MAC アドレスを使用」を選択します。ルータは、現在使用している PC の MAC アドレスをキャプチャし使用します。ISP が許可する 1 台の PC を使用する必要があります。または、「この MAC アドレスを使用」を選択して、入力します。
- [適用] をクリックして、自分の設定を保存します。
- [テスト] をクリックして、インターネット接続をテストします。NETGEAR のウェブサイトが 1 分以内に表示されない場合、第 7 章、「トラブルシューティング」を参照してください。

ダイナミック IP ウィザード検出オプション

[セットアップウィザード] が ISP の使用するダイナミック IP 割り当てを発見したら、このメニューが表示されます。

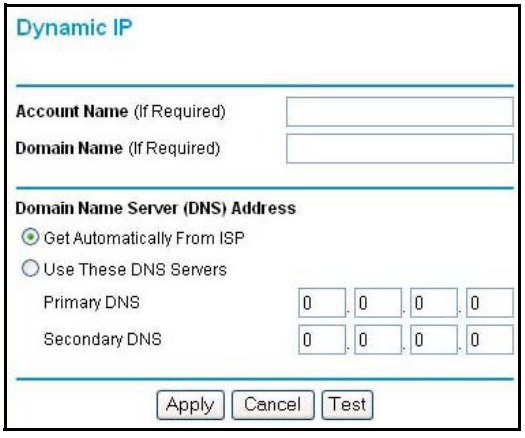


図 2-9 ダイナミック IP アドレスアカウントの [セットアップウィザード] メニュー

- アカウント名（ホスト名とも呼ばれます）およびドメイン名を入力します。これらのパラメータは、メールや新しいサーバーなどの ISP のサービスにアクセスする必要があります。[ドメイン名] フィールドがブランクになっていると、ルータはドメインを発見しようとします。発見しない場合、ドメインを手動で入力する必要があります。
- ログイン中に ISP が DNS アドレスをルータに自動的に送信しない場合、「これらの DNS サーバーを使用」を選択し、ISP のプライマリ DNS サーバーの IP アドレスを入力します。セカンダリ DNS サーバーアドレスが利用できる場合、それも入力してください。

  注：DNS アドレスを入力したら、コンピュータを再起動してこれらの設定が有効にしてください。
- [適用] をクリックして、自分の設定を保存します。
- [テスト] をクリックして、インターネット接続をテストします。NETGEAR のウェブサイトが 1 分以内に表示されない場合、第 7 章、「トラブルシューティング」を参照してください。

固定 IP ウィザード検出オプション

[セットアップウィザード] が ISP の使用する固定 IP 割り当てを発見したら、このメニューが表示されます。

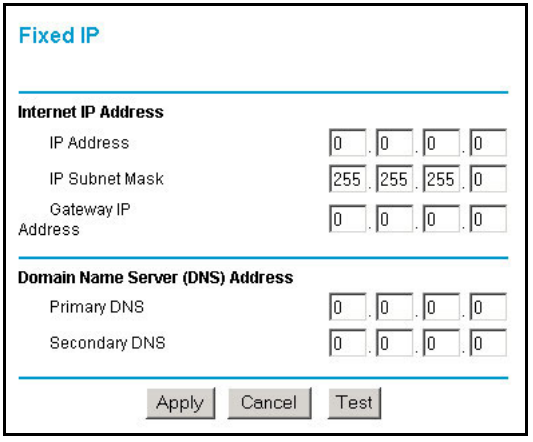


図 2-10 固定 IP アドレスアカウントの [セットアップウィザード] メニュー

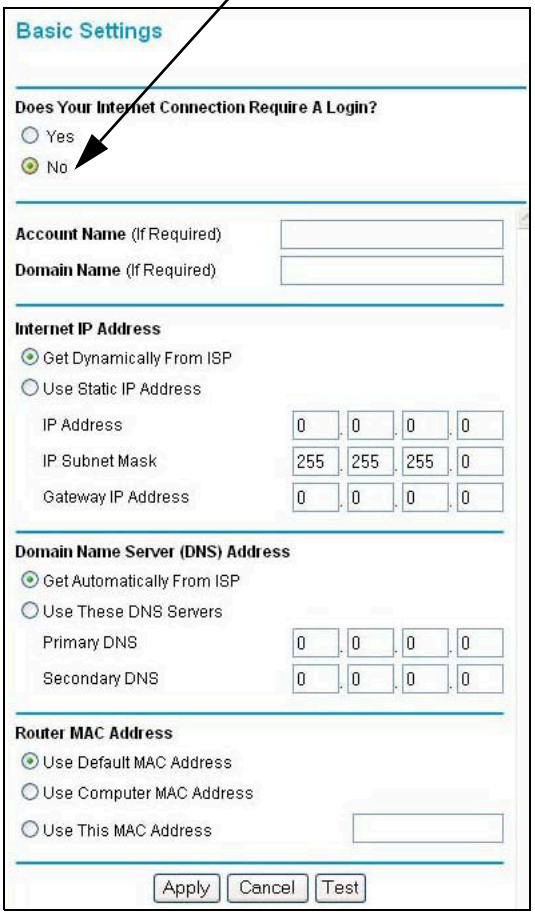
- 固定 IP は、スタティック IP とも呼ばれます。割り当てられた IP アドレス、サブネットマスク、ISP のゲートウェイルータの IP アドレスを入力してください。この情報は、ISP によって提供される必要があります。2-3 ページの「インターネット接続情報を記録する」で記録した ISP から設定パラメータが必要となります。
- ISP のプライマリおよびセカンダリ DNS サーバーアドレスの IP アドレスを入力してください。

  注：これらの設定が有効になるように、ネットワークのコンピュータを再起動してください。
- [適用] をクリックして、その設定を保存します。
- [テスト] をクリックして、インターネット接続をテストします。NETGEAR のウェブサイトが 1 分以内に表示されない場合、第 7 章、「トラブルシューティング」を参照してください。

インターネット接続を手動で設定する

下のメニューを使用してルータを手動で設定するか、[セットアップウィザード] に前項で説明したように設定を決定させることもできます。

ISP *はログイン*を要求しません



ISP *は*ログインを要求します

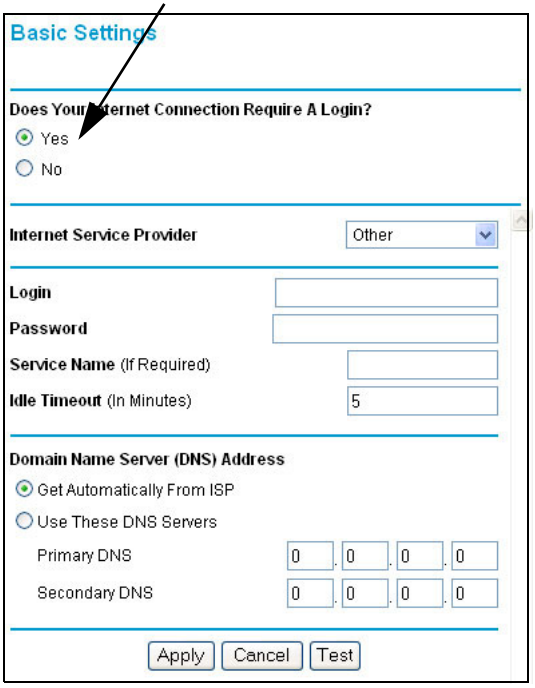


図 2-11 ブラウザベースの設定ベーシック設定メニュー

これらのステップを使用して図 2-11 に表示される [基本設定] メニューを使用して、ルータを手動で設定することができます。

1. [セットアップ] メニューで [基本設定] リンクをクリックします。
2. インターネット接続がログインを要求しない場合、[基本設定] メニューの上部で [いいえ] をクリックし、下の指示に従って設定を入力してください。インターネット接続がログインを要求する場合、[はい] をクリックし、ステップ 3 にスキップしてください。

   a. アカウント名（ホスト名とも呼ばれます）およびドメイン名を入力します。これらのパラメータは、メールや新しいサーバーなどの ISP のサービスにアクセスする必要があります。

   b. インターネット IP アドレス：
   ISP が永久的な、PC の固定（スタティック）IP アドレスを割り当てる場合、「静的 IP アドレスを使用」を選択してください。ISP が割り当てた IP アドレスを入力します。また、ネットマスクとゲートウェイ IP アドレスも入力してください。ゲートウェイは、ルータが接続する ISP のルータです。

   c. ISP ドメイン名サーバー (DNS) アドレス
   ログイン中に ISP が DNS アドレスをルータに自動的に送信しない場合、「これらの DNS サーバーを使用」を選択し、ISP のプライマリ DNS サーバーの IP アドレスを入力します。セカンダリ DNS サーバーアドレスが利用できる場合、それも入力してください。

   注：アドレスをここに入力したら、ネットワークのコンピュータを再起動してこれらの設定が有効にしてください。

   d. ゲートウェイの MAC アドレス：
   本項では、インターネットポートのルータによって使用されるイーサネット MAC アドレスを説明します。一部の ISP は、アカウントを始めて開くとき、PC のネットワークインターフェイスカードのイーサネット MAC アドレスを登録します。そして、その PC の MAC アドレスからくるトラヒックのみを受け入れます。この機能により、ルータはその MAC アドレスを「閉じる」ことによってその PC を装うことができます。

   MAC アドレスを変更するには、「このコンピュータの MAC アドレスを使用」を選択します。ルータは、現在使用している PC の MAC アドレスをキャプチャし使用します。ISP が許可する 1 台の PC を使用する必要があります。または、「この MAC アドレスを使用」を選択して、入力します。

   e. [適用] をクリックして、自分の設定を保存します。

3. インターネットせつぞくがログインを要求しない場合、下の指示に従って設定を記入してください。インターネットに接続するために、イーサネットまたは WinPOET などのログインプログラムを起動する必要がある場合は、[はい] を選択してください。

   注：ルータのセットアップが終了したら、インターネットにアクセスするために PC で ISP のログインプログラムを起動する必要はありません。インターネットアプリケーションを起動すると、ルータが自動的にログインします。

   a. ドロップダウンリストから、仮のインターネットサービスを選択してください。

   b. 画面は、選択する ISP の ISP 設定要件に従って変わります。

   c. 2-9 ページで開始したウィザード検出手順に従って ISP のパラメータを記入してください。

   d. [適用] をクリックして、自分の設定を保存します。

第 3 章
ワイヤレス設定

本章では、MR814v2 ルータのワイヤレス機能の設定方法を説明します。

ワイヤレスネットワークに対する考慮

ワイヤレスネットワークを計画する上で、必要なセキュリティのレベルを考慮する必要があります。ネットワーク速度を最大限にするために、ファイヤウォールの物理的配置を選択する必要もあります。ワイヤレスネットワーキングの詳細については、付録 D、「ワイヤレスネットワーキングベーシック」を参照してください。

監視パフォーマンス、配置、レンジガイドライン

操作距離またはワイヤレス接続の範囲は、ワイヤレスファイヤウォールの物理的配置に基づいて大幅に異なります。冗長、データスループットパフォーマンス、ノートブックの消費電力も、設定の選択によって異なります。

	**注**：これらのガイドラインに従わなければ、パフォーマンスが大幅に落ちたりルータにワイヤレス接続できなくなったりすることがあります。完全なレンジ / パフォーマンスの仕様については、付録 A、「技術仕様」をご覧ください。

最高の結果を得るために、ファイヤウォールを配置してください。

- PC が動作する領域の中心付近。
- ワイヤレスで接続されている PC がラインオブサイトアクセス（壁を通してた場合も可）を持っている高い棚などの高い位置。
- PC、マイクロ波、2.4 GHz コードレス電話などの障害のソースから離れたところ。
- 広い金属面から離れたところ。

ワイヤレス接続の確立に時間は、セキュリティ設定と配置によって異なります。WEP 接続の確立には、少し時間がかかります。また、WEP 暗号化はノートブック PC ではバッテリを消耗します。

適切なワイヤレスセキュリティの実装

注：室内では、コンピュータは最大 150m の範囲を超えて、802.11b ワイヤレスネットワークを接続することはできません。150m を超えると、すぐ近くの部外者がネットワークにアクセスするのが可能になります。

有線接続されたネットワークデータとは異なり、ワイヤレスデータ送信は壁を越えて届き、互換アダプタを持っている者ならだれでも受信することができます。この理由で、ワイヤレス装置のセキュリティ機能を使用してください。MR814v2 ルータでは、本章で詳しく説明するように、効率的なセキュリティ機能を提供しています。ニーズに合ったセキュリティ機能を装備してください。

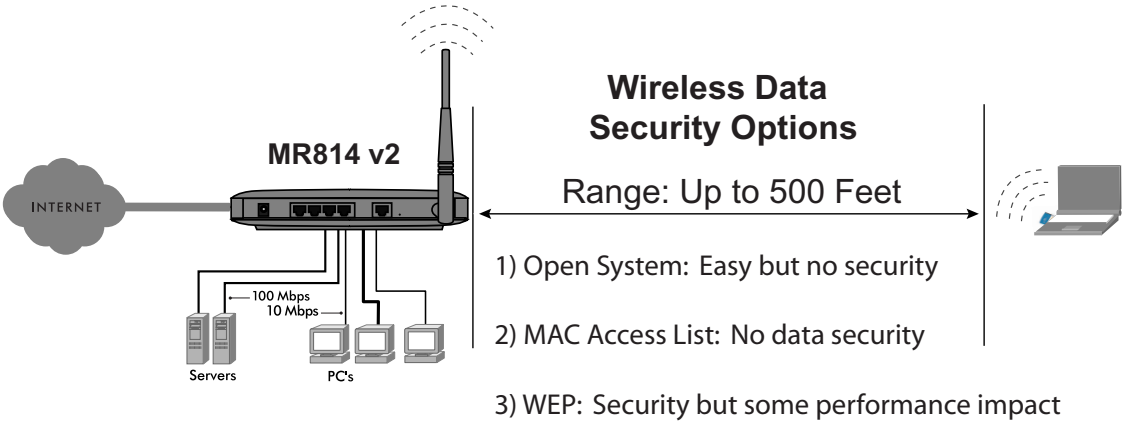


図 3-1.　　MR814v2 ワイヤレスデータのセキュリティオプション

MAC アドレスによるアクセスを制限することでネットワークへの好ましくないアクセスに対して障害が追加されますが、ワイヤレスリンクを介してブロードキャストされるデータは丸裸にされます。意図的な盗聴者をブロックするために、ファイヤウォールのデータ暗号化オプションのどれかを使用する必要があります。有線同等プライバシ (WEP) データ暗号化は、データセキュリティを提供します。

ワイヤレス設定を理解する

ファイヤウォールのワイヤレス設定を設定するには、ブラウザインターフェイスのメインメニューでワイヤレスリンクをクリックします。ワイヤレス設定メニューが表示されます。

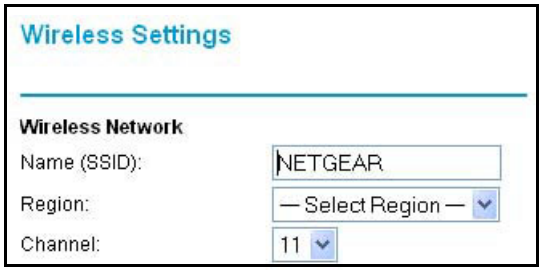


図 3-2.　　ワイヤレス設定メニュー

ワイヤレスネットワークメニュー項については、以下で説明します。

- **名前 (SSID)**。サービスセット識別子は、ワイヤレスネットワーク名としても知られています。最大 32 文字の英数字を入力してください。複数のワイヤレスネットワークがある設定で、異なるワイヤレスネットワーク名はトラヒックを分離するための手段を提供します。このワイヤレスネットワークに参加させたいどのデバイスも、この SSID を使用する必要があります。MR814v2 デフォルトの SSID は、次の通りです：NETGEAR 。
- **地域** このフィールドは、MR814v2 を使用できる地域を確認します。このドロップダウンリストで確認されていない地域でルータのワイヤレス機能を操作することは、違法行為になることがあります。
- **チャネル** このフィールドは、どの操作機能を使用するかを決定します。近くにある他のアクセスポイントで障害の問題が認められない限り、ワイヤレスチャネルを変更する必要はありません。ワイヤレスチャネル周波数の詳細については、D-7 ページの「ワイヤレスチャネル」を参照してください。

ネットワークへのワイヤレスアクセスを制限する

MR814v2 ケーブル /DSL ワイヤレスルータは、ネットワークへのワイヤレスアクセスを制限する方法をいくつか提供します。

- ワイヤレス接続性を完全にオフにする

- ワイヤレスネットワーク名 (SSID) に基づくアクセスの制限
- ワイヤレスカードアクセスリストに基づくアクセスの制限

以上のオプションを次に説明します。

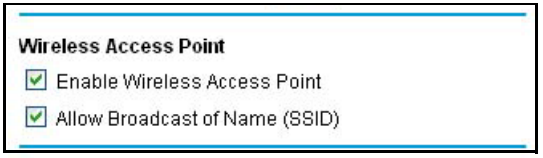


図 3-3.　　ワイヤレスアクセスポイントの設定

ワイヤレス接続性をオフにすることにより、ネット枠へのアクセスを制限する

MR814v2 のワイヤレス部分を完全にオフにすることができます。例えば、ノートブック PC をルータにワイヤレス接続して使用しているときに商用旅行する場合、旅行中はルータのワイヤレス部分をオフにすることができます。イーサネットケーブルを介してルータに接続されたコンピュータを使用する他の家族は、ルータを使用することができます。

ワイヤレスネットワーク名 (SSID) に基づきワイヤレスアクセスを制限する

MR814v2 は、ワイヤレスネットワーク名 (SSID) をブロードキャストしないことにより、ネットワークへのワイヤレスアクセスを制限することができます。ただし、デフォルトで、この機能はオフになっています。この機能をオンにすると、ワイヤレスデバイスは MR814v2 を「表示」しません。ワイヤレスデバイスは、MR814v2 ルータで設定したワイヤレスネットワーク名 (SSID) に一致するように設定する必要があります。

注：ワイヤレスアクセスアダプタの SSID は、MR814v2 ケーブル /DSL ワイヤレスルータで設定した SSID に一致する必要があります。一致しない場合、MR814v2 にワイヤレス接続を確認できません。

ワイヤレスアクセスリストに基づきワイヤレスアクセスを制限する

このリストは、どのワイヤレスハードウェアデバイスがファイヤウォールへの接続を許可されるかを決定します。

1. この機能をアクティブにするには、[アクセスリストのセットアップ] ボタンをクリックします。

図 3-4.　　ワイヤレスカードアクセスリスト

2. [アクセス制御をオンにする] チェックボックスをクリックします。
3. [追加] をクリックすると、[ワイヤレスカードアクセスセットアップ] 画面が表示されます。

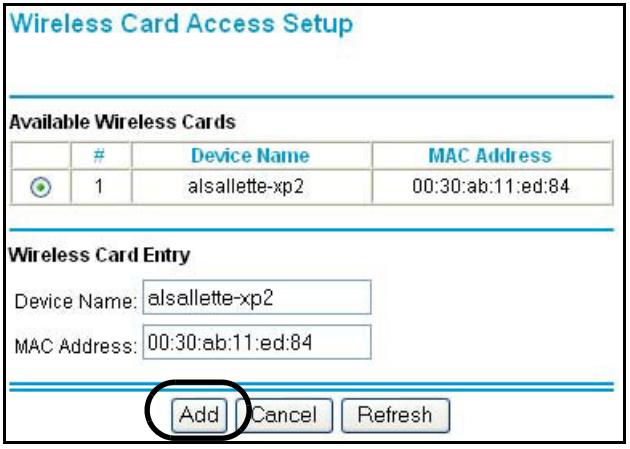


図 3-5.　　ワイヤレスカードアクセスリストのセットアップ

次に、MR814v2 が現在の地域で検出した利用可能なワイヤレスカードのリストから選択するか、使用するつもりの MAC アドレスとデバイス名を入力します。MAC アドレスは、通常ワイヤレスアダプタに印刷されています。[追加] をクリックすると、[ワイヤレスカードアクセスリスト] 画面に戻ります。

図 3-6.　　ワイヤレスカードアクセスリスト

設定を実装して保存するには、必ず [適用] をクリックしてください。

リストのデバイスのみが MR814v2 にワイヤレス接続を許可されるようになりました。これで、ネットワークへの無断アクセスを防ぐことができます。

認証とセキュリティ暗号化方式を選択する

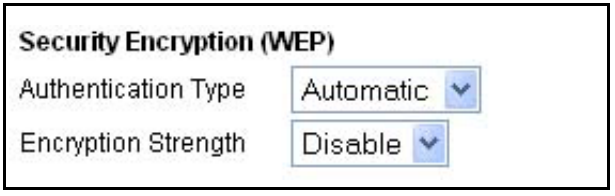


図 3-7.　　暗号化の強度

ネットワークへのワイヤレスアクセスを制限することにより、侵入者はネットワークに接続できなくなります。ただし、ワイヤレスデータ送信は偽装攻撃には無防備です。以下で説明するウェブデータ暗号化設定を使用すると、意図的な侵入者はワイヤレスデータ通信を盗聴できなくなります。また、買い物や銀行取引のような活動でインターネットを使用する場合、これらのインターネットサイトは SSL と呼ばれる他のレベルの高い安全な暗号化を使用します。そのウェブアドレスは HTTP ではなく HTTPS で始まるので、ウェブサイトが SSL を使用しているかどうかは一目で分かります。

認証計画の選択

MR814v2 では、次のワイヤレス認証計画を使用します。

- 自動。
- オープンシステム。
- 共有キー。

	**注**：認証計画は、データ暗号化とは別のものです。共有キーを要求する認証計画を選択しながら、データ送信を暗号化しないままにしておくこともできます。強力な暗号化が必要な場合、共有キーと WEP 暗号化設定を同時に使用してください。

MR814v2 ルータに対して選択する認証計画に従って、ワイヤレスアダプタを設定してください。IEEE 802.11b ワイヤレス通信基準で定義されている、それぞれのオプションの完全な説明については、D-2 ページの「認証と WEP」を参照してください。

暗号化強度の選択

ドロップダウンリストリストから暗号化の強度を選択します。IEEE 802.11b ワイヤレス通信基準で定義されている、それぞれのオプションの完全な説明については、D-5 ページの「WEP パラメータの概要」を参照してください。

無効

暗号化は適用されません。この設定はワイヤレス接続の障害を解決するには役に立ちますが、ワイヤレスデータは無防備にさらされます。

64 または 128 ビット WEP

64 ビット WEP または 128 ビット WEP を選択しているとき、WEP 暗号化が適用されます。

WEP はあるレベルのプライバシを提供しますが、さしたる困難もなく破られます。WEP が有効になっていると、4 つの暗号化キーを手動でまたは自動的にプログラムすることができます。これらの値は、ネットワークの全ての PC およびアクセスポイントで同じでなければなりません。

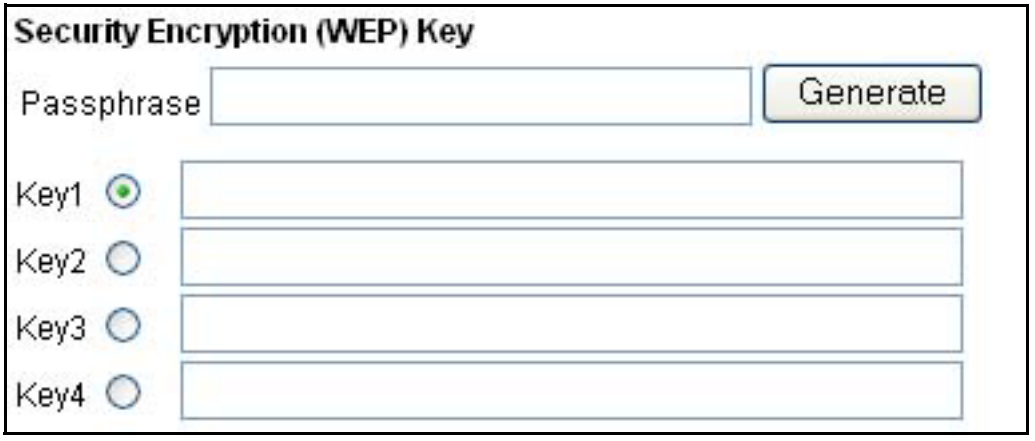


図 3-8.　　64 または 128 ビット WEP 暗号化強度

WEP 暗号化キーの作成方式は、2 通りあります。

- パスフレーズ。[パスフレーズ] ボックスに単語または印刷可能な文字のグループを入力し、[生成] ボタンをクリックします。
- 手動。64 ビット WEP：10 の 16 進数字（0-9、a-f、A-F の任意の組み合わせ）を入力します。
  128 ビット WEP：26 の 16 進数字（0-9、a-f、A-F の任意の組み合わせ）を入力します。

ラジオボタンをクリックすると、4 つのキーのどれをアクティブにするかを選択できます。

ベーシックワイヤレス接続性をセットアップしてテストする方法

下の指示に従って、ベーシックワイヤレス接続性セットアップしてテストしてください。ベーシックワイヤレス接続性を確立したら、ニーズにふさわしいセキュリティ設定を有効にできます。

1. そのデフォルトのユーザー名 **admin** およびデフォルトのパスワード**パスワード**を持つデフォルトの LAN アドレス *http://192.168.0.1* で、またはセットアップした LAN アドレスとパスワードを使用して、MR814v2 ファイヤウォールにログインします。
2. MR814v2 ファイヤウォールのメインメニューで、[ワイヤレス設定] リンクをクリックしてください。

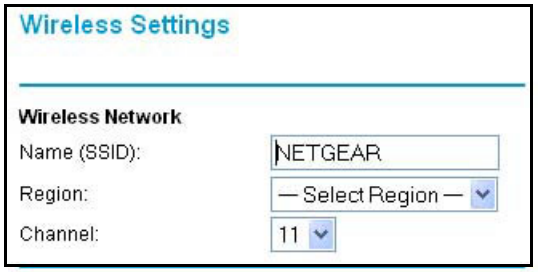


図 3-9.　　ワイヤレス設定メニュー

3. ワイヤレスネットワーク名 (SSID) にふさわしい記述名を選択してください。SSID ボックスに、最大 32 文字の英数字を入力してください。デフォルトの SSID はワイヤレスです。

   注：ワイヤレスアクセスアダプタの SSID は、MR814v2 ケーブル /DSL ワイヤレスルータで設定した SSID に一致する必要があります。一致しない場合、MR814v2 にワイヤレス接続を確認できません。

4. 地域の設定。ワイヤレスインターフェイスが動作する地域を選択します。
5. チャネルの設定。デフォルトのチャネルは 6 です。

   このフィールドは、どの操作機能を使用するかを決定します。近くにある他のワイヤレスルータまたはアクセスポイントで障害の問題が認められない限り、ワイヤレスチャネルを変更する必要はありません。ファイヤウォールから 100 メートル以内にある他のワイヤレスネットワークで使用されていないチャネルを選択してください。ワイヤレスチャネル周波数の詳細については、D-7 ページの「ワイヤレスチャネル」を参照してください。

6. 初期設定とテストの場合、ワイヤレスカードアクセスリストを「全員」に設定し、暗号化強度を「無効」に設定しておいてください。
7. [適用] をクリックして、変更を保存します。

	**注：**ワイヤレス PC からファイヤウォールを設定しているときにファイヤウォールの SSID、チャネル、またはセキュリティ設定を変更すると、[適用] をクリックするとワイヤレス接続を失います。ファイヤウォールの新しい設定を一致させるには、PC のワイヤレス設定を変更する必要があります。

8. ワイヤレス接続に対して、PC を設定してテストしてください。

PC のワイヤレスアダプタがルータで設定したものと同じ SSID とチャネルを持つようにプログラムしてください。PC がワイヤレスリンクを持ちファイヤウォールから DHCP による IP アドレスを取得できるか ¡™Ø³ します。

PC がファイヤウォールに対してベーシックワイヤレス接続性を持ったら、ファイヤウォールの先進的ワイヤレスセキュリティ機能を設定できます。

MAC アドレスによるワイヤレスアクセスを制限する方法

MAC アドレスに基づくアクセスを制限するには、次のステップに従ってください。

1. そのデフォルトのユーザー名 **admin** およびデフォルトのパスワード**パスワード**を持つデフォルトの LAN アドレス *http://192.168.0.1* で、またはセットアップした LAN アドレスとパスワードを使用して、MR814v2 ファイヤウォールにログインします。
2. MR814v2 ファイヤウォールのメインメニューで、[ワイヤレス設定] リンクをクリックしてください。
3. ワイヤレス設定メニューから、[アクセスのセットアップリスト] ボタンをクリックし、下で示すように、[ワイヤレスアクセス] メニューを表示します。

図 3-10。　　ワイヤレスアクセスメニュー

4. [追加] をクリックして、ワイヤレスデバイスをワイヤレスアクセス制御リストに追加します。利用可能なワイヤレスカードのリストが表示されます。

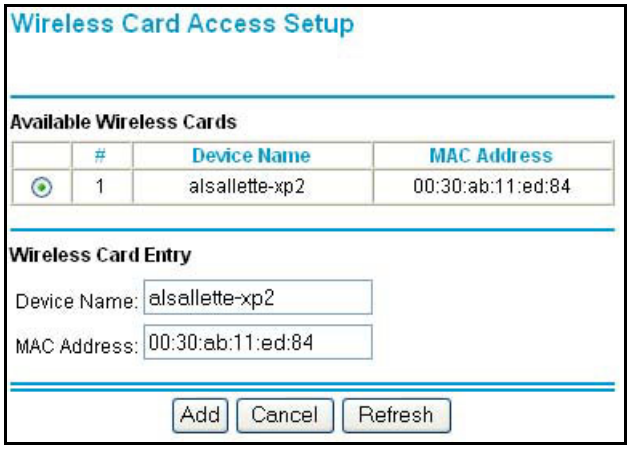


図 3-11.　　ワイヤレスアクセスメニュー

5. リストのデバイスの隣りにあるラジオボタンをクリックし、[追加] をクリックしてこのデバイスをリストに追加します。

   注：ファイヤウォールの [接続されたデバイス] メニューから MAC アドレスをこのメニューの [MAC アドレス] ボックスにコピーして張り付けることができます。これを行うには、それぞれのワイヤレス PC を設定してファイヤウォールに対するワイヤレスリンクを取得してください。PC は、[接続されたデバイス] メニューに表示されます。

6. [適用] をクリックし、ワイヤレスアクセス制御リスト設定を必ず保存してください。

表から MAC アドレスを編集するには、そのアドレスをクリックして選択し、[編集] または [削除] ボタンをクリックします。

注：MAC アドレスが [信頼された PC] リストにないワイヤレス PC からファイヤウォールを設定し [アクセス制御をオンにする] を選択しているとき、[適用] をクリックすると、ワイヤレス接続が失われます。アクセス制御リストにある有線 PC またはワイヤレス PC からルータにアクセスして、詳細変更を行う必要があります。

WEP の設定

WEP データ暗号化を設定するには、次のステップに従ってください。

1. そのデフォルトのユーザー名 **admin** およびデフォルトのパスワード**パスワード**を持つデフォルトの LAN アドレス *http://192.168.0.1* で、またはセットアップした LAN アドレスとパスワードを使用して、MR814v2 ファイヤウォールにログインします。
2. MR814v2 ルータのメインメニューで、[ワイヤレス設定] リンクをクリックしてください。
3. [セキュリティ暗号化] メニューで、認証および暗号化強度を選択します。IEEE 802.11b ワイヤレス通信基準で定義されている、それぞれのオプションの完全な説明については、D-5 ページの「WEP パラメータの概要」を参照してください。

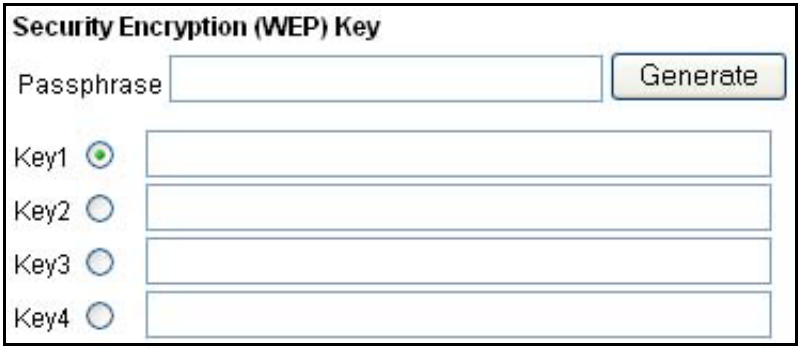


図 3-12。　　ワイヤレス設定暗号化メニュー

4. 4 つのデータ暗号化キーを手動でまたは自動的にプログラムすることができます。これらの値は、ネットワークの全ての PC およびアクセスポイントで同じでなければなりません。
   - 自動 - [パスフレーズ] ボックスに単語または印刷可能な文字のグループを入力し、[生成] ボタンをクリックします。4 つのキーボックスに、キーの値が自動的に入力されます。
   - マニュアル - 10 の 16 進数字（0-9、a-f、A-F の任意の組み合わせ）を入力します。
     4 つのキーのどれをアクティブにするか選択します。

   WEP キー設定がワイヤレスアダプ A でどのように設定されているか、はっきり理解してください。Windows XP に組み込まれているワイヤレスアダプタ設定ユーティリティのみが、MR814v2 で設定したデフォルトキーに一致する 1 つのキーのエントリを許可します。

5. [適用] をクリックして、自分の設定を保存します。

	**注：**ワイヤレス PC からルータを設定して WEP 設定を設定しているとき、[適用] をクリックするとワイヤレス接続が失われます。ワイヤレスアダプタがルータ WEP 設定に一致するように設定するか、有線 PC からルータにアクセスして詳細な変更を行う必要があります。

第 4 章
コンテンツフィルタリング

本章では、ネットワークを保護するために MR814v2 ケーブル /DSL ワイヤレスルータのコンテンツフィルタリング機能を使用する方法を説明します。これらの機能は、ブラウザインターフェイスのメインメニューのコンテンツフィルタリング見出しをクリックすることにより、検出できます。

コンテンツフィルタリングの概要

MR814v2 ケーブル /DSL ワイヤレスルータはユーザーにウェブコンテンツフィルタリングオプション、およびブラウジングアクティビティリポーティング、電子メールによるインスタントアラートを提供します。両親とネットワーク管理者は、日時、ウェブアドレス、ウェブアドレスのキーワードに基づき、アクセスの制限を確立できます。チャットやゲームなどの、アプリケーションやサービスによりインターネットアクセスをブロックすることもできます。

ルータのこれらの機能を設定するには、ブラウザインターフェイスの [メインメニュー] の [コンテンツフィルタリング] 見出しの下で、小見出しをクリックしてください。小見出しを下で説明します。

インターネットサイトへのアクセスをブロックする

MR814v2 ルータにより、ウェブアドレスおよびウェブアドレスのキーワードに基づき、アクセスを制限することができます。最大 255 のエントリが、キーワードリストでサポートされています。[ブロックサイト] メニューを、図 4-1 下に表示します。

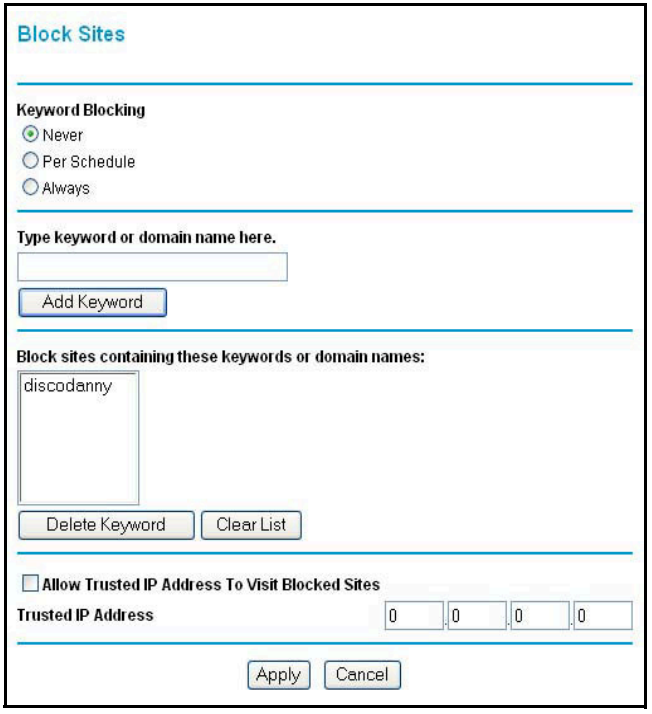


図 4-1 ブロックサイトメニュー

キーワードのブロッキングを有効にするには、[スケジュールごと] または [常に] を選択し、[適用] をクリックします。スケジュールごとでブロックしたい場合、時間が [スケジュール] メニューで指定されていることを確認してください。

キーワードまたはドメインを追加するには、[キーワード] ボックスにそれを入力し、[キーワードの追加] をクリックし、[適用] をクリックします。

キーワードまたはドメインを削除するには、リストからそれを選択し、[キーワードの削除] をクリックし、[適用] をクリックします。

キーワードアプリケーションの例：

- キーワード「XXX」が指定されている場合、URL <http://www.badstuff.com/xxx.html> がブロックされます。
- キーワード「.com」が指定されている場合、他のドメイン接尾辞（例：.edu または .gov）を持つウェブサイトのみが表示されます。
- スケジュールされた期間に全てのインターネットブラウジングアクセスをブロックしたい場合、キーワード「.」を入力し、[スケジュール] メニューでスケジュールを設定します。

信頼できるユーザーを指定するには、[信頼できるユーザー] ボックスにその PC の IP アドレスを入力し、[適用] をクリックします。

1 つの信頼できるユーザーを指定できます。これは、ブロッキングとロギングを免じる PC です。[信頼できるユーザー] は IP アドレスによって識別されるため、固定 IP アドレスでその PC を設定する必要があります。

インターネットサービスへのアクセスをブロックする

MR814v2 ルータにより、ネットワークの PC によるインターネットサービスの使用をブロックできます。これは、サービスのブロッキングまたはポートフィルタリングと呼ばれます。[ブロックサービス] メニューを、下に表示します。

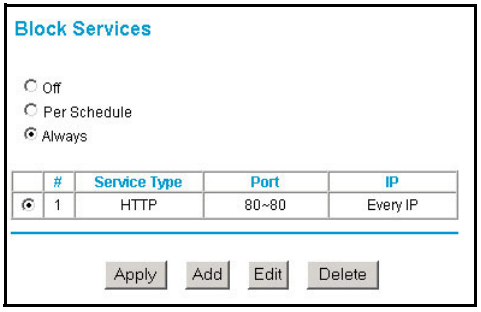


図 4-2 ブロックサービスメニュー

サービスは、クライアントコンピュータの要求でサーバーコンピュータにより実行される機能です。例えば、ウェブサーバーはウェブページを管理し、時間サーバーは時間と日付情報を管理し、ゲームホストは他のプレーヤーの動きに関するデータを管理します。ネットワークのコンピュータがインターネット上のサーバーコンピュータにサービスの要求を送信するとき、要求されたサービスはサービスまたはポート番号によって識別されます。この番号は、転送された IP アドレスの送信先ポート番号として表示されます。例えば、送信先ポート番号 80 で送信されたパケットは HTTP（ウェブサーバー）要求です。

サービスのブロッキングを有効にするには、[スケジュールごと] または [常に] を選択し、[適用] をクリックします。スケジュールごとでブロックしたい場合、時間が [スケジュール] メニューで指定されていることを確認してください。

ブロッキング用にサービスを指定するには、[追加] をクリックします。[サービスの追加] メニューは、下に示すように表示されます。

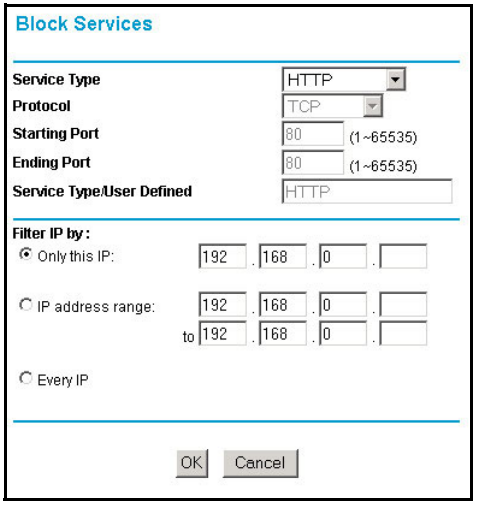


図 4-3 サービスの追加メニュー

[サービスのタイプ] リストから、許可またはブロックされるアプリケーションやサービスを選択します。リストはいくつかの共通サービスを表示しますが、これらの選択に制限されることはありません。まだ表示されていないその他のサービスまたはアプリケーションを追加するには、[ユーザー定義] を選択してください。

ユーザー定義サービスを設定する

サービスを定義するには、まずどのポート番号または数字の範囲がアプリケーションによって使用されているかを決定する必要があります。多くの共通プロトコルに対するサービス番号は、インターネットタスクフォース (IETE) により定義され、RFC1700,「割り当て番号」で公表されています。他のアプリケーションに対するサービス番号は、アプリケーションの著者によって 1024 から 65535 の範囲まで一般的に選択されています。この情報は、アプリケーションの発行者に連絡することにより、またはニュースグループのユーザーグループから、一般的には決定できます。

開始ポートと終了ポートの番号を入力します。アプリケーションが単一のポート番号を使用する場合、両方のボックスにその番号を入力してください。

アプリケーションが TCP か UDP のどちらかを使用するかを知っていれば、適切なプロトコルを選択してください。確信がもてない場合は、[両方] を選択してください。

IP アドレス範囲によるサービスブロッキングを設定する

「フィルタサービス」の下で、ネットワークの単一 PC、ある範囲の PC（連続した IP アドレスを持つ）、全ての PC に対して指定されたサービスをブロックできます。

ブロッキングが実行されるときをスケジュールする

MR814v2 ルータにより、ブロッキングを実行するときを指定できます。[スケジュール] メニューを、下に表示します。

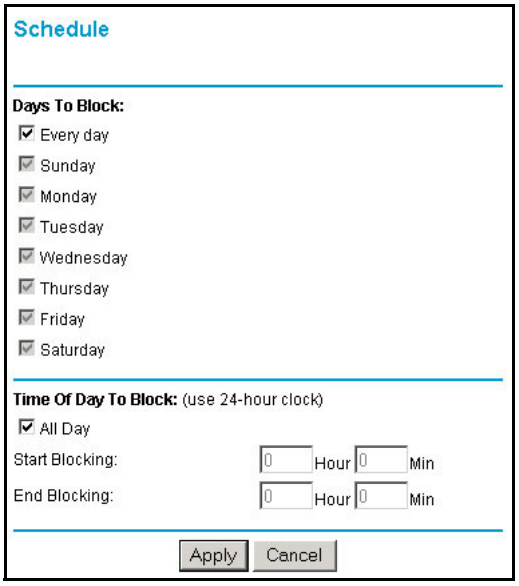


図 4-4 スケジュールメニュー

- ブロッキングコンテンツに対してこのスケジュールを使用します。コンテンツフィルタリング用にスケジュールを有効にしたい場合、このボックスにチェックマークを入れてください。[適用] をクリックします。
- ブロックする日数。適切なボックスにチェックマークを入れてブロックする日数を選択します。全ての日に対するボックスをチェックすると、[毎日] が選択されます。[適用] をクリックします。
- ブロックする日時。23:59 形式で開始時間と終了時間を選択します。24 時間のブロッキングに対しては、[毎日] を選択します。[適用] をクリックします。

電子メールメニューで自分のタイムゾーンを選択していることを確認します。

ウェブアクセスまたは試みられたウェブアクセスのログを表示する

ログはアクセスしたまたはアクセスを試みたウェブサイトの詳細な記録です。最大 128 のエントリがログに格納されます。ログエントリは、キーワードブロッキングが有効になっているときのみ表示され、[信頼できるユーザー] に対してはエントリは作成されません。一例を下に示します。

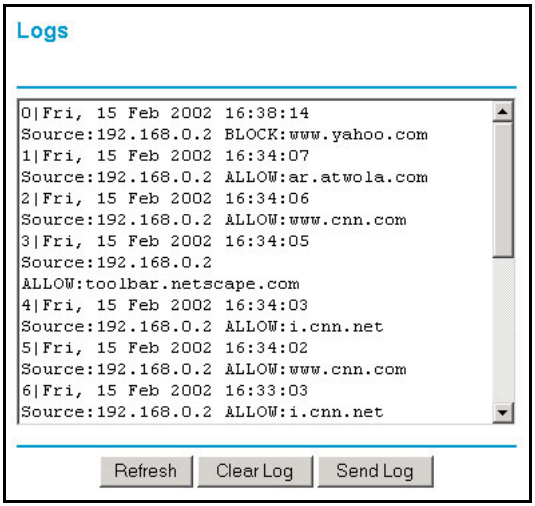


図 4-5 ログメニュー

ログエントリは、表 4-1 に記述されています。

表 4-1. ログエントリの説明

フィールド	説明
番号	コンテンツフィルタログエントリのインデックス番号。0 から 127 まで、128 のエントリを利用できます。ログは、最新の 128 のエントリの記録を維持します。
日と時間	ログエントリが記録された日と時間。
ソース IP	このログエントリに対する開始デバイスの IP アドレス。

表 4-1. ログエントリの説明

フィールド	説明
アクション	このフィールドは、アクセスがブロックされるのか許可されるのかを表示します。
	アクセスされたまたはアクセスを試みられたウェブサイトまたはニュースグループの IP アドレスの名前。

ログアクションは、表 4-2 に記述されています。

表 4-2. ログアクションボタン

フィールド	説明
再生	このボタンをクリックすると、ログ画面を再生します。
ログのクリア	このボタンをクリックすると、ログエントリをクリアします。
ログの送信	このボタンをクリックすると、ログを直ちに電子メールで送信します。

電子メールアラートとウェブアクセスログ通知を設定する

電子メールでログとアラートを受信するためには、下に示すように、電子メールメニューに電子メール情報を提供する必要があります。

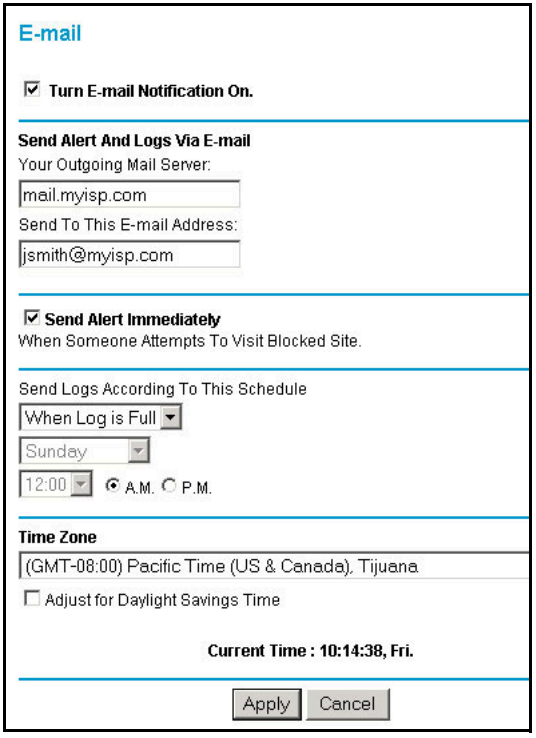


図 4-6 電子メールメニュー

- 電子メール通知をオンにする
  ルータから電子メールログとアラートを受信する場合、このボックスにチェックマークを入れます。
- 送信メールサーバー
  ISP の送信 (SMTP) メールサーバー（mail.myISP.com など）の名前を入力します。電子メールプログラムの設定メニューで、この情報を検出できます。このボックスをブランクにしておくと、ログとアラートメッセージは電子メールを介して送信されません。

- この電子メールアドレスに送信する
  ログとアラートを送信する電子メールアドレスを入力します。この電子メールアドレスは、[送信元] アドレスとしても使用されます。このボックスをブランクにしておくと、ログとアラートメッセージは電子メールを介して送信されません。

ログは、これらのオプションと共に指定された電子メールアドレスに自動的に送信されることを指定できます。

- アラートを直ちに送信する
  ブロックされたサイトへの試みられたアクセスを直ちに通知したい場合、このボックスにチェックマークを入れてください。
- このスケジュールに従ってログを送信
  ログを送信する頻度を指定します。毎時間、毎日、毎週、一杯になったとき。
  - ログを送信する日
    ログを送信する曜日を指定します。ログが毎週または毎日送信されるときに関連
  - ログを送信する時間
    ログを送信する日時を指定します。ログが毎日または毎週送信されるときに関連

  指定された期間の前に、毎週、毎日、毎時間のオプションが選択されログが一杯になった場合、ログは指定された電子メールアドレスに自動的に送信されます。ログを送信後、ログはルータのメモリから消去されます。ルータがログファイルを電子メール送信できない場合、ログバッファは一杯になります。この場合、ルータはログを上書きしそのコンテンツを廃棄します。

MR814v2 ルータはネットワークタイムプロトコル (NTP) を使用して、インターネットのいくつかのネットワークタイムサーバーのどれかから現在の時間と日を取得します。ログエントリの時間をローカライズするには、タイムゾーンを指定する必要があります。

- タイムゾーン
  ローカルのタイムゾーンを選択します。この設定は、ブロッキングスケジュールとタイムスタンピングログエントリ用に使用されます。
- 夏時間
  タイムゾーンが現在夏時間の下にある場合は、このボックスにチェックマークを入れてください。

第 5 章
メンテナンス

本章では、MR814v2 ケーブル /DSL ワイヤレスルータのメンテナンス機能の使用方法を説明します。これらの機能は、ブラウザインターフェイスのメインメニューのメンテナンス見出しをクリックすることにより、検出できます。

ルータステータス情報を表示する

ルータステータスメニューでは、限られた量のステータスと使用情報を提供します。ブラウザインターフェイスの [メインメニュー] から、[メンテナンス] をクリックし、[システムステータス] を選択して、下に示すように [システムステータス] 画面を表示します。

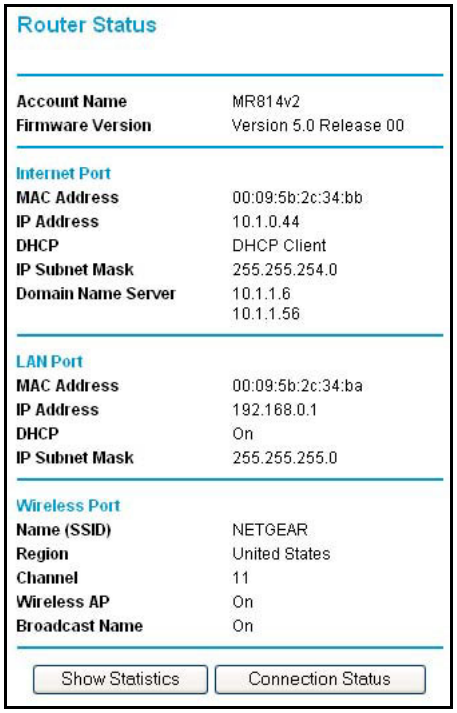


図 5-1 ルータステータス画面

この画面は、次のパラメータを表示します。

表 5-1. ルータ ステータスフィールド

フィールド	説明
アカウント名	このフィールドは、ルータに割り当てられたホスト名を表示します。
ファームウェアバージョン	このフィールドは、ルータのファームウェアバージョンを表示します。
インターネットポート	これらのパラメータは、ルータのインターネット (WAN) ポートに適用されます。
MAC アドレス	このフィールドは、ルータのインターネット (WAN) ポートにより使用されるメディアアクセスコントロールアドレスを表示します。
IP アドレス	このフィールドは、ルータのインターネット (WAN) ポートにより使用される IP アドレスを表示します。アドレスが表示されない場合、ルータはインターネットに接続できません。
IP サブネットマスク	このフィールドは、ルータのインターネット (WAN) ポートにより使用される IP サブネットマスクを表示します。
DHCP	[なし] に設定されている場合、ルータは WAN の固定 IP アドレスを使用するように設定されます。 [クライアント] に設定されている場合、ルータは ISP から IP アドレスを動的に取得するように設定されます。
LAN ポート	これらのパラメータは、ルータのローカル (WAN) ポートに適用されます。
MAC アドレス	このフィールドは、ルータの LAN ポートにより使用されるメディアアクセスコントロールアドレスを表示します。
IP アドレス	このフィールドは、ルータのローカル (LAN) ポートにより使用される IP アドレスを表示します。デフォルトは 192.168.0.1 です。
IP サブネットマスク	このフィールドは、ルータのローカル (LAN) ポートにより使用される IP サブネットマスクを表示します。デフォルトは 255.255.255.0 です。
DHCP	ルータの内蔵 DHCP サーバーが、LAN に接続されたデバイスに対してアクティブになっていることを確認します。

表 5-1.　　ルータ ステータスフィールド

フィールド	説明
ワイヤレスポート	これらのパラメータは、ルータのワイヤレスポートに適用されます。
MAC アドレス	このフィールドは、ルータのワイヤレスポートにより使用されるメディアアクセスコントロールアドレスを表示します。
名前 (SSID)	このフィールドは、ルータのワイヤレスポートにより使用されるワイヤレスネットワーク名 (SSID) を表示します。デフォルトはワイヤレスです。
地域	このフィールドは、ルータが使用されている地理的地域を表示します。国によっては、ルータのワイヤレス機能の使用が法によって認められていない場合もあります。
チャネル	ワイヤレスポートが使用しているチャネルかどうかを確認します。各チャネルで使用されている周波数については、D-7 ページの「ワイヤレスチャネル」をご覧ください。

[接続ステータスの表示] ボタンをクリックすると、下に示すように、接続ステータスが表示されます。

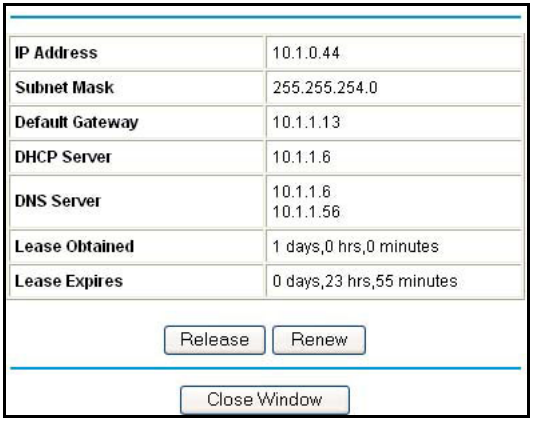


図 5-2 接続テータス画面

この画面は、次の統計値を表示します。

表 5-2 : 接続テータスアイテム

アイテム	説明
IP アドレス	ルータに割り当てられている WAN（インターネット）IP アドレス。
サブネットマスク	ルータに割り当てられている WAN（インターネット）サブネットマスク。
デフォルトのゲートウェイ	ルータが通信を行っている WAN（インターネット）のデフォルトゲートウェイ。
DHCP サーバー	IP 設定アドレスを提供する DHCP サーバーの IP アドレス。
DNS サーバー	IP アドレス変換に対してネットワーク名を提供する DNS サーバーの IP アドレス。
取得したリース	DHCP リースを取得したとき。
リースの使用期限	DHCP リースの期限が切れたとき。
解除	解除ボタンをクリックすると、DHCP リースが解除されます。
更新	更新ボタンをクリックすると、DHCP リースが更新されます。

[統計値の表示] ボタンをクリックすると、下に示すように、ルータの使用統計値が表示されます。

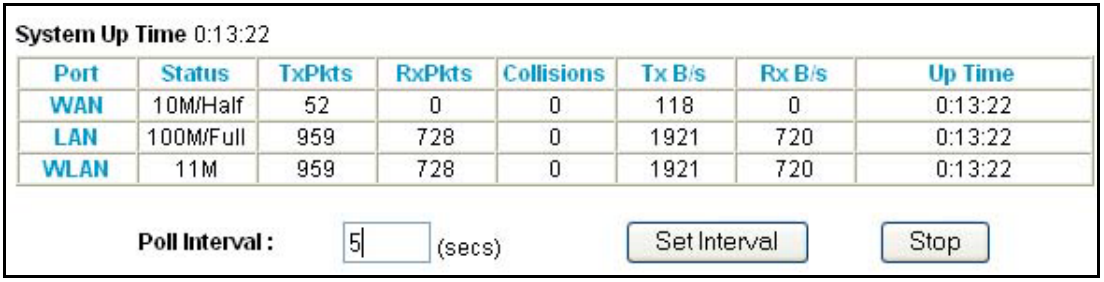


図 5-3 ルータス統計値画面

この画面は、次の統計値を表示します。

表 5-3： ルータス統計値アイテム

アイテム	説明
ポート	WAN（インターネット）と LAN（ローカル）ポートの統計値。各ポートに対して、画面は次を表示します。
ステータス	ポートのリンクステータス。
TxPkts	リセットまたは手動クリアからこのポートに送信されたパケット数。
RxPkts	リセットまたは手動クリアからこのポートで受信したパケット数。
衝突	リセットまたは手動クリアからこのポートで衝突したパケット数。
Tx B/s	WAN および LAN ポートで使用されている現在の送信（下り）バンド幅。
Rx B/s	WAN および LAN ポートで使用されている現在の受信（上り）バンド幅。
動作可能時間	ルータが最後に再起動してから経過した時間数。
動作可能時間	このポートがリンクを獲得してから経過した時間。
世論調査結果	統計値がこのウィンドウで更新された間隔を指定します。[停止] をクリックすると、ディスプレイが動かなくなります。
間隔の設定	時間を入力しボタンをクリックすると、世論調査の頻度が設定されます。
停止	[停止] ボタンをクリックすると、世論調査情報が停止します。

接続されたデバイスのリストを表示する

[接続されたデバイス] メニューには、ローカルネットワークでルータが検出した全ての IP デバイスの表が含まれています。ブラウザインターフェイスの [メインメニュー] から [メンテナンス] 見出しの下で、下に示すように、[接続されたデバイス] を選択して表を表示します。

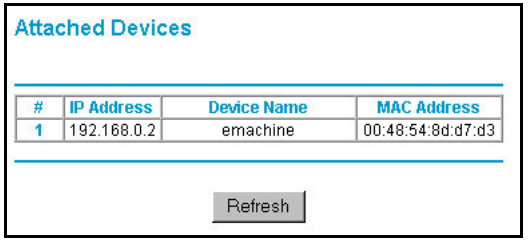


図 5-4 [接続されたデバイス] メニュー

各デバイスに対し、表は IP アドレス、NetBIOS ホスト名（利用可能な場合）、イーサネット MAC アドレスを表示します。ルータを再起動する場合、表のデータはルータがデバイスを再び検出するまで表示されません。ルータに接続するデバイスを強制的に検索させるには、[更新] ボタンをクリックします。

ルータのソフトウェアをアップグレードする

MR814v2 ルータの経路指定ソフトウェアは [フラッシュ] メモリに格納され、新しいソフトウェアが NETGEAR により発表されるとアップグレードできます。アップグレードファイルは Netgear のウェブサイトからダウンロードできます。アップグレードファイルが圧縮（.ZIP ファイル）されている場合、ルータに送信する前にまずバイナリファイルを解凍する必要があります。アップグレードファイルは、ブラウザを使用してルータに送信できます。

注：新しいファームウェアを MR814v2 ルータにアップロードするために使用するウェブブラウザは、HTTP アップロードをサポートする必要があります。NETGEAR は、Microsoft Internet Explorer または Netscape Navigator 3.0 以降を使用することを推奨します。

ブラウザインターフェイスの [メインメニュー] から [メンテナンス] 見出しの下で、下に示すように、[ルータのアップグレード] を選択してメニューを表示します。

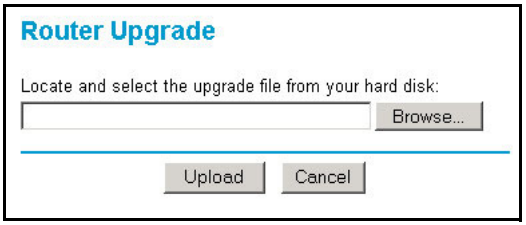


図 5-5 ルータのアップグレードメニュー

新しいファームウェアをアップロードするには、次の手順に従います。

1. NETGEAR から新しいソフトウェアファイルをダウンロードして解凍します。
2. [ルータのアップグレード] メニューで、[ブラウザ] ボタンをクリックしてバイナリ (.BIN) アップグレードファイルの場所に移動します。
3. [アップロード] をクリックします。

   注：ソフトウェアを MR814v2 ルータにアップロードするとき、ウィンドウを閉じたり、リンクをクリックしたり、新しいページをロードしてウェブブラウザを中断しないことが重要です。ブラウザが中断されると、ソフトウェアが破損することがあります。アップロードが完了したら、ルータが自動的に再起動します。アップグレードプロセスは、通常約 1 分かかります。

ある場合、アップグレードした後ルータを再設定する必要があります。

設定ファイルの管理

MR814v2 ルータの設定は、設定ファイルのルータ内に保管されます。このファイルはユーザーの PC に保存（バックアップ）され、ユーザーの PC から回復（復元）されたり、消去されて出荷時設定になります。

ブラウザインターフェイスの [メインメニュー] から [メンテナンス] 見出しの下で、[バックアップの設定] 見出しを選択して、下に示すように、メニューをポップアップ表示します。

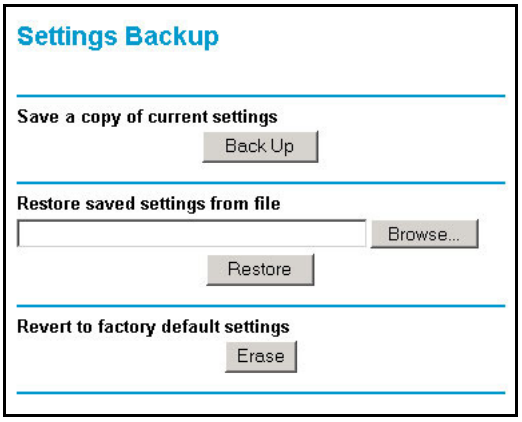


図 5-6 バックアップメニューを設定する

利用可能な 3 つのオプションを、次項以降で説明します。

設定を復元しバックアップする

[バックアップの設定] メニューの [復元] および [バックアップ] オプションは、ルータの設定に含まれるファイルを保存し回復します。

設定を保存するには、[バックアップ] タブを選択します。[バックアップ] ボタンをクリックします。ブラウザがルータから設定ファイルを展開し、ファイルを格納する PC の場所を問い合わせます。このとき、pacbell.cfg などの意味のある名前をファイルに付けることができます。

保存された設定ファイルから設定を復元するには、PC のファイルに完全パスを入力するか [参照] ボタンをクリックしてファイルを検索します。ファイルが見つかったら、[復元] ボタンをクリックしてファイルをルータに送信します。ルータが自動的に再ブートします。

設定を消去する

ルータを既知のブランク状態に復元する方が望ましいこともときどきあります。これは [消去] 機能を使用して実行され、全ての出荷時設定を復元します。消去後、ルータのパスワードが**パスワード**になり、LAN IP アドレスは 192.168.0.1 になり、ルータの DHCP クライアントが有効になります。

設定を消去するには、[消去] ボタンをクリックします。

ログインパスワードや IP アドレスを知らずに出荷時設定を復元するには、ルータの背面パネルの [デフォルトのリセット] ボタンを使用します。7-7 ページの「初期設定とパスワードを復元する」をご覧ください。

管理者パスワードを変更する

ルータのウェブ設定マネージャのデフォルトのパスワードは、**パスワード**です。Netgear では、このパスワードをより安全なパスワードに変更することをお勧めします。

ブラウザインターフェイスの [メインメニュー] から [メンテナンス] 見出しの下で、[パスワードの設定] を選択して、下に示すように、メニューをポップアップ表示します。

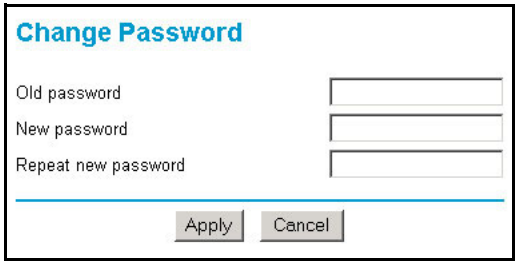


図 5-7 パスワードメニューの設定

パスワードを変更するには、まず古いパスワードを入力し、新しいパスワードを 2 回入力します。[適用] をクリックします。

第 6 章
ルータの詳細設定

本章では、MR814v2 ケーブル /DSL ワイヤレスルータの先進的機能の設定方法を説明します。これらの機能は、ブラウザインターフェイスのメインメニューの詳細設定見出しの下にあります。

ポートフォーワーディングをローカルサーバーに設定する

ルータによりローカルネットワーク全体がインターネットへの単一マシンとして表示されますが、ローカルサーバー（例えば、ウェブサーバーやゲームサーバー）を表示に設定してインターネットで使用することができます。これは、ポートフォーワーディングメニューを使用して実行できます。ブラウザインターフェイスのメインメニューから、詳細設定の下で、ポートフォーワーディングをクリックして、下に示すようにポートフォーワーディングメニューを表示します。

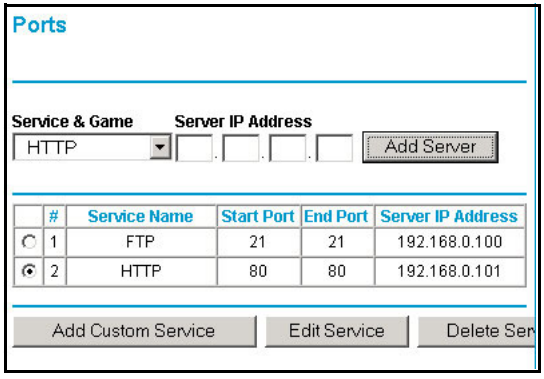


図 6-1.　　ポートフォーワーディングメニュー

注：ネットワーキングとルーティングに精通していない場合、付録 B、「ネットワーク、ルーティング、ファイアウォール、ベーシック」を参照して本書で使用されている用語や手順に習熟する必要があります。

ポートフォーワーディングメニューを使用してルータを設定し、着信プロトコルをローカルネットワークのコンピュータに転送します。特定アプリケーションに対するサーバーだけでなく、デフォルトの DMZ サーバーを他の全ての入力プロトコルを転送するサーバーに指定することもできます。DMZ サーバーは、セキュリティメニューで設定されます。

開始する前に、どのタイプのサービスやアプリケーション、ゲームを提供するかを、またどのコンピュータの IP アドレスがそれぞれのサービスを提供するかを決定する必要があります。コンピュータの IP アドレスを変更していないことを確認してください。ポートフォーワーディングをローカルサーバーに設定するには、次の手順に従います。

1. サーバーとゲームボックスから、ネットワークでホストするサービスやゲームを選択します。
   そのサービスがリストに表示されない場合、次項、「カスタムサービスを追加する」を参照してください。
2. 対応するサーバーIP アドレスボックスにローカルサーバーの IP アドレスを入力します。
3. 追加ボタンをクリックします。

カスタムサービスを追加する

サービスとゲームリストに表示されないサービスやゲーム、アプリケーションを定義するには、どのポート番号がサービスによって使用されるかを決定する必要があります。この情報に対して、使用したいプログラムのメーカーに問い合わせる必要があります。ポート番号の情報を持っているとき、次のステップに従ってください。

1. カスタムサービスの追加ボタンをクリックします。
2. 未使用のポートの開始ボックスに最初のポート番号を入力します。
3. １つのポートだけを転送するには、ポートの終了ボックスにそのポートを再入力します。ポートの範囲を指定するには、ポートの終了ボックスに転送する最後のポートを入力します。
4. 対応するサーバーIP アドレスボックスにローカルサーバーの IP アドレスを入力します。
5. サービスの名前を入力します。
6. メニュー下部で適用をクリックします。

ポートフォーワーディングエントリを編集するまたは削除する

ポートフォーワーディングエントリを編集または削除するには、次のステップに従います。

1. 表で、サービス名の隣りのボタンを選択します。
2. 編集または削除をクリックします。

ローカルウェブと FTP サーバーの例

192.168.0.33 のプライベート IP アドレスを持つローカル PC がウェブおよび FTP サーバーとして機能する場合、ポートメニューを転送 HTTP（ポート 80）に、FPT（ポート 21）をローカルアドレス 192.168.0.33 に設定します。

リモートユーザーがインターネットからこのサーバーにアクセスできるためには、リモートユーザーがあなたの ISP によって割り当てられた IP アドレスを知っている必要があります。例えば、このアドレスが 172.16.1.23 である場合、インターネットユーザーはブラウザを http://172.16.1.23 に送信することによってあなたのウェブサーバーにアクセスできます。割り当てられた IP アドレスが保守ステータスメニューで検出されると、そのメニューに WAN IP アドレスとして表示されます。

このアプリケーションに対して、次のことを考慮する必要があります。

- アカウントの IP アドレスが ISP におって動的に割り当てられていれば、IP アドレスは DHCP リース期間が終了するときに周期的に変更されます。
- ローカル PC の IP アドレスが DHCP によって割り当てられている場合、アドレスは PC が再起動するときに変更されます。これを避けるために、固定アドレスを使用するために PC を手動で設定することができます。
- ローカル PC は、PC のローカル LAN アドレス（この例では、192.168.0.33）を使用してローカルサーバーにアクセスする必要があります。外部 IP アドレス（この例では、172.16.1.23）を使用してサーバーにアクセスするローカル PC による試み。

Half Life、KALI または Quake III Example 用の複数のコンピュータ

追加コンピュータをセットアップして Half Life, KALI or Quake III をプレーするには、次の手順に従います。

1. 表の未使用ポートのボタンをクリックします。
2. サービス / ゲームリストから再びゲーム j を選択します。

3. ポートの開始ボックスで開始ポート番号を変更します。
これらのゲームの場合、デフォルトリストに供給された番号を使用して、それぞれの追加コンピュータに対して +1 を追加してください。例えば、Hexen II（26900 を使用して）をプレーするために 1 台のコンピュータをすでに設定する場合、2 台目のコンピュータのポート番号は 26901 になり、3 台目のコンピュータは 26902 になります。
4. ポートの終了ボックスにポートの開始ボックスに入力したものと同じポート番号を入力してください。
5. サーバー IP アドレスボックスに追加コンピュータの IP アドレスを入力します。
6. 適用をクリックします。

オンラインゲームと TV 会議アプリケーションの中には NAT と互換性のないものもあります。MR814v2 ルータはこれらのアプリケーションの一部を認識してそれと共に正しく機能するようにプログラムされていますが、まったく機能しないアプリケーションもあります。場合によっては、1 台のローカル PC はその PC の IP アドレスが PORTS メニューにデフォルトとして入力されていれば、そのアプリケーションを正しく実行することができます。1 台のローカル PC がゲームまたは TV 会議ホストとして機能する場合、その IP アドレスをデフォルトとして入力してください。

WAN セットアップオプションを設定する

WAN セットアップオプションでは、DMZ サーバーを設定し、MTU サイズを変更し、ルータを有効にして WAN ポートのピングに応答させることができます。以上のオプションを次に説明します。

デフォルトの DMZ サーバーをセットアップする

デフォルトの DMZ サーバー機能は、NAT と互換性のないオンラインゲームや TV 会議アプリケーションを使用しているときに役に立ちます。ルータはこれらのアプリケーションの一部を認識してそれと共に正しく機能するようにプログラムされていますが、まったく機能しないアプリケーションもあります。場合によっては、1 台のローカル PC はその PC の IP アドレスがデフォルトの DMZ サーバーとして入力されていれば、そのアプリケーションを正しく実行することができます。

注：DMZ サーバーはセキュリティリスクの原因となります。デフォルトの DMZ サーバーとして指定されたコンピュータはファイアウォールの大部分の保護を失い、インターネットから利用するときに危険にさらされます。その場合、DMZ サーバーはネットワークを攻撃するために使用できます。

インターネットから着信するトラヒックは通常、そのトラヒックがローカルコンピュータの 1 台にまたは、ポートメニューで設定したサービスに応答しない場合、ルータによって廃棄されます。このトラヒックを廃棄する代わりに、ネットワークの 1 台のコンピュータに転送することもできます。このコンピュータは、デフォルトの DMZ サーバーと呼ばれます。

下に示した WAN セットアップメニューにより、デフォルトの DMZ サーバーを設定することができます。

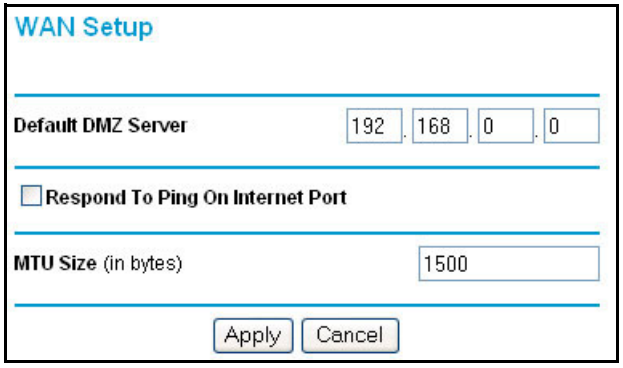


図 6-2.　　WAN セットアップメニュー。

コンピュータやサーバーをデフォルトの DMZ サーバーとして割り当てるには、次のステップに従ってください。

1. メインメニューの詳細設定の WAN セットアップリンクをクリックします。
2. そのサーバーに対する IP アドレスを入力します。デフォルトの DMZ サーバーを取り除くには、IP アドレス番号をすべてゼロで置き換えます。
3. 適用をクリックします。

インターネット WAN ポートのピングに応答

ルータをインターネットから「ピング」に応答させたいとき、「インターネット WAN ポートのピングに応答」チェックボックスをクリックします。これは、ルータを発見できるため、診断ツールとしてのみ使用する必要があります。そうするだけの明確な理由がない限り、このチェックボックスをチェックしないでください。

MTU サイズを設定する

デフォルトの MTU サイズは通常ファインです。ほとんどのイーサネットネットワークに対する標準の MTU（最大転送単位）値は 1500 バイトです。一部の ISP の場合、特に PPPoE を使用した ISP の場合、MTU を小さくする必要があります。これは、ISP に絶対必要でない限り行ってはなりません。

設定した MTU サイズより大きなルータを通して送信されたパケットは、MTU 要件を満たすためにより小さなパケットに再パッケージ化されます。MTU サイズを変更するには、次の手順を実行します。

1. MTU サイズの元で、64 から 1500 までの新しいサイズを入力します。
2. 適用をクリックして、新しい設定を保存します。

LAN IP セットアップオプションを使用する

詳細設定見出しの下の 2 番目の機能カテゴリは LAN IP セットアップです。このメニューにより、DHCP や RIP などの LAN IP サービスを設定できます。ブラウザインターフェイスのメインメニューから、詳細設定の下で、LAN IP セットアップをクリックして、下に示すように LAN IP セットアップメニューを表示します。

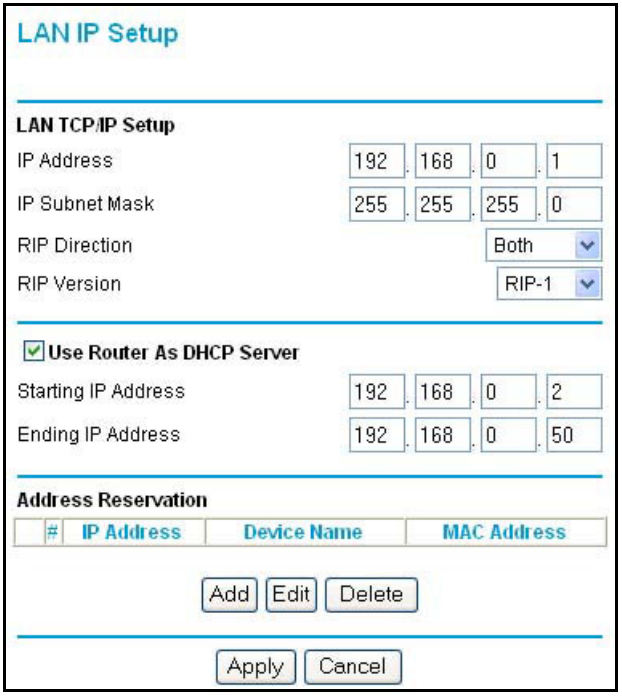


図 6-3.　　LAN IP セットアップメニュー

LAN TCP/IP セットアップパラメータを設定する

ルータは、LAN サイドのプライベート IP アドレスを使用し、DHCP サーバーとして機能するために出荷時に事前設定されています。ルータのデフォルトの LAN IP 設定は、次のようになっています。

- LAN IP アドレス - 192.168.0.1
- サブネットマスク - 255.255.255.0

これらのアドレスはプライベートネットワークで使用するために IETF 指定されたプライベートアドレス範囲の一部で、ほとんどのアプリケーションに適合している必要があります。ネットワークが異なる IP アドレッシング方式を使用する必要がある場合、このメニューでこれらの変更を行うことができます。

LAN IP パラメータは次のようになっています。

- IP アドレス
  これは、ルータの LAN IP のアドレスです。
- IP サブネットマスク
  これは、ルータの LAN IP のアドレスです。IP アドレスと結合された IP サブネットマスクにより、デバイスはどのアドレスがデバイスに対してローカルになっているか、どれがゲートウェイやルータを通して到達する必要があるかを知ることがあります。
- RIP Direction
  RIP（ルータ情報プロトコル）では、ルータがルーティング情報を他のルータに変換できます。RIP Direction 選択は、ルータが RIP パケットを送受信する方法をコントロールします。デフォルトは双方向です。
  - 双方向または出力のみに設定されているとき、ルータはそのルーティング表を周期的にブロードキャストします。
  - 双方向または入力のみに設定されているとき、受信する RIP 情報を組み込みます。
  - なしに設定されているとき、どの RIP パケットも送信せず、受信したすべての RIP パケットを無視します。
- RIP バージョン
  これは、ルータが送信する RIP パケットのフォーマットとブロードキャスティング方式をコントロールします。（受信しているとき、両方のフォーマットを認識します）。デフォルトで、これは RIP-1 に対して設定されます。
  - RIP-1 は広くサポートされています。RIP-1 は、一般的でないネットワークのセットアップを行っていない限り、ほとんどのネットワークで十分に役立つもとの考えられます。
  - RIP-2 はさらに多くの情報を転送します。RIP-2B はサブネットブロードキャスティングを使用します。

注：ブラウザを通して接続されている間、ルータの LAN IP アドレスを変更すると、切断されます。新しい IP アドレスに対して新しい接続を開き、再びログインする必要があります。

DHCP サーバーとしてルータを使用する

デフォルトで、ルータは DHCP（ダイナミックホスト設定プロトコル）サーバーとして機能し、IP、DNS サーバー、デフォルトのゲートウェイアドレスをルータの LAN に接続されている全てのコンピュータに割り当てることができます。割り当てられたデフォルトのゲートウェイアドレスは、ルータの LAN アドレスです。IP アドレスは、このメニューで指定されたアドレスのプールから接続された PC に割り当てられます。それぞれのプールアドレスは、LAN に同じアドレスが複製されないように、割り当てられる前にテストされます。

ほとんどのアプリケーションの場合、ルータのデフォルトの DHCP と TCP/IP 設定を変える必要はありません。DHCP の説明およびネットワークに IP アドレスを割り当てる方法の詳細については、B-11 ページの「DHCP による IP 設定」をご覧ください。

ネットワークの他のデバイスは DHCP サーバーになります。全てのコンピュータのネットワーク設定を手動で設定する場合、「DHCP サーバーとしてルータを使用」チェックボックスを外してください。相でない場合は、チェックマークを残してください。

IP アドレスの開始と IP アドレスの終了を設定することによって、割り当てる IP アドレスのプールを指定してください。これらのアドレスは、ルータの LAN IP アドレスと同じ IP サブネットの一部となる必要があります。デフォルトのアドレッシング方式を使用して、192.168.0.2 から 192.168.0.253 までの範囲を定義する必要がありますが、固定アドレスを持つデバイスに対する範囲の部分を保存することもできます。

ルータは、次のパラメータを DHCP を要求する LAN デバイスに提供します。

- 定義した範囲からの IP アドレス
- サブネットマスク
- ゲートウェイ IP アドレス（ルータ LAN IP のアドレス）
- プライマリ DNS サーバー（基本設定メニューにプライマリ DNS アドレスを入力した場合。そうでない場合、ルータの LAN IP アドレス）
- セカンダリ DNS サーバー（基本設定メニューにセカンダリ DNS アドレスを入力した場合）

アドレス予約を使用する

LAN 上の PC に対して予約済み IP アドレスを指定する場合、その PC はルータの DHCP サーバーにアクセスするたびに、同じ IP アドレスを常に受け取ります。予約済み IP アドレスは、永久的な IP 設定を要求するサーバーに割り当てられる必要があります。

IP アドレスを予約するには、次の手順に従います。

1. 追加ボタンをクリックします。
2. IP アドレスボックスで、IP アドレスを入力して PC またはサーバーに割り当てます。（ルータの LAN サブネットから、192.168.0.X などの IP アドレスを選択してください）
3. PC またはサーバーの MAC アドレスを入力します。
(ヒント : PC がネットワークにすでに存在する場合、接続されたデバイスメニューからその MAC アドレスをコピーしてここに貼り付けることができます)。
4. 適用をクリックして、予約済みアドレスを表に入力します。

注 : 予約済みアドレスは、次に PC がルータの DHCP サーバーに接続するまで割り当てられません。PC を再起動するか、その IP 設定にアクセスして DHCP を強制的にリリースし更新してください。

予約済みアドレスエントリを編集または削除するには、次の手順に従います。

1. 編集または削除したい予約済みアドレスの隣りにあるボタンをクリックします。
2. 編集または削除をクリックします。

ダイナミック DNS サービスを使用する

ネットワークが永久的に割り当てられた IP アドレスを持っている場合、ドメイン名を登録してその名前をパブリックドメイン名サーバー (DNS) によって IP アドレスにリンクすることができます。ただし、インターネットアカウントが動的に割り当てられた IP アドレスを使用している場合、自分の IP アドレスがどうなるのかを前もって知ることはできず、アドレスは頻繁に変更されます。この場合、商用のダイナミック DNS サービスを使用すると、ドメインをその IP アドレスに登録して、自分のドメインに向けられたトラヒックを頻繁に変更される IP アドレスに転送することができます。

注：ISP がプライベート WAN IP アドレス（192.168.x.x または 10.x.x.x など）を割り当てている場合、ダイナミック DNS サービスは、プライベートアドレスがインターネット上で経路指定されないために、機能しません。

ルータには、多くの一般的ダイナミック DNS サービスに接続できるクライアントが含まれています。これらのサービスのどれかを選択して、そのサービスと共にアカウントを取得することができます。次に、ISP を割り当てられた IP アドレスが変更されるときは常に、ルータがダイナミック DNS サービスプロバイダに自動的に接続され、自分のアカウントにログインし、新しい IP アドレスを登録します。

ブラウザインターフェイスのメインメニューから、詳細設定の下で、ダイナミック DNS をクリックしてください。ダイナミック DNS を設定するには、次の手順に従います。

1. その名前が「サービスプロバイダ」ボックスに表示されているダイナミック DNS サービスプロバイダのどれかで、アカウントを登録します。例えば、dyndns.org の場合、www.dyndns.org に移動します。
2. ダイナミック DNS サービスの使用チェックボックスを選択します。
3. 自分の使用しているダイナミック DNS サービスプロバイダの名前を選択します。
4. ダイナミック DNS サービスプロバイダから与えられたホスト名（またはドメイン名）を入力します。
5. ダイナミック DNS アカウントのユーザー名を入力します。
6. ダイナミック DNS アカウントのパスワード（またはキー）を入力します。
7. ダイナミック DNS プロバイダが URL を分割する際にワイルドカードの使用を許可するバ秋、ワイルドカードの使用チェックボックスを選択してこの機能をアクティブにすることができます。
   例えば、ワイルドカード機能を使うと、*.yourhost.dyndns.org は yourhost.dyndns.org と同じ IP アドレスになります。
8. 適用をクリックして、自分の設定を保存します。

スタティックルートを設定する

スタティックルートは、ルータに新たな経路指定情報を提供します。標準の環境の下で、ルータにはインターネットアクセス用に設定された後の適切な経路指定情報があり、スタティックルートを新たに設定する必要はありません。スタティックルートは、ネットワークに配置されている複数のルータまたは複数の IP サブネットなどのまれなケースに対してのみ設定する必要があります。

ブラウザインターフェイスのメインメニューから、詳細設定の下で、スタティックルートをクリックして、下に示すようにスタティックルートメニューを表示します。

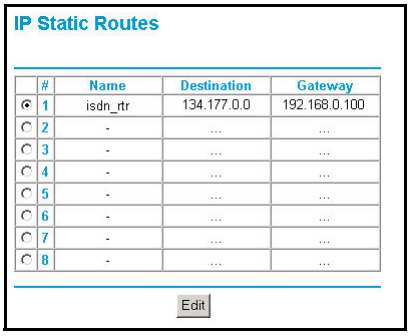


図 6-4.　　スタティックルートの概要表

スタティックルートを追加または編集するには、次の手順に従います。

1. 追加ボタンをクリックして、下に示すように、追加 / 編集メニューを開きます。

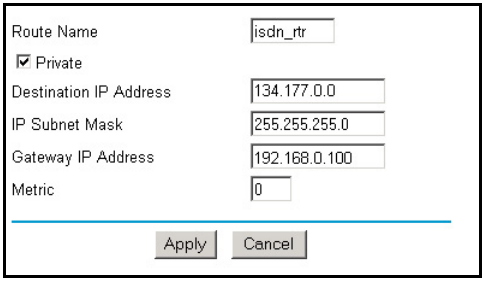


図 6-5.　　スタティックルートエントリと編集メニュー

2. 表の下のルート名ボックスに、このスタティックルートのルート名を入力します。（これは、識別目的用です）。
3. LAN のみへのアクセスを制限するには、プライベートを選択します。スタティックルートは、RIP に報告されません。
4. アクティブを選択して、このルートを有効にします。
5. 最終送信先の送信先 IP アドレスを入力します。
6. この送信先用の IP サブネットマスクを入力します。
送信先が単一ホストの場合、255.255.255.255 を入力します。
7. ルータと同じ LAN セグメント上のルータである、ゲートウェイ IP アドレスを入力します。
8. メートル法の数値として、1 から 15 までの数字を入力します。
この数字は、ネットワークと送信先の間のルータ数を表します。通常、2 または 3 の設定が正常に動作しますが、この設定が直接接続である場合、1 に設定してください。
9. 適用をクリックして、スタティックルートを表に入力します。

スタティックルートが必要な例として、次の場合を考慮します。

- プライマリインターネットアクセスは、ケーブルモデムを通して ISP に経路指定されます。
- 雇用されている会社に接続するための家庭ネットワーク上に、ISDN ルータを用います。LAN のこのルータのアドレスは 192.168.0.100 です。
- 勤務している会社のネットワークは 134.177.0.0 です。

自分のルータをはじめて設定したとき、2 つの間接的なスタティックルートが作成されました。デフォルトのルートがゲートウェイとして ISP で作成され、2 番目のスタティックルートがすべての 192.168.0.x アドレスに対してローカルネットワークに対して作成されました。この設定を使用して、134.177.0.0 ネットワークのデバイスへのアクセスを試みる場合、ルータは自分の要求を ISP に転送します。ISP は雇用されている会社に要求を転送し、その要求は会社のファイアウォールによって拒絶される可能性があります。

この場合、スタティックルートを定義し、134.177.0.0 が 192.168.0.100 で ISDN ルータを通してアクセスされる必要があることを自分のルータに通知する必要があります。スタティックルートは、図 6-5 のように見えます。

例：

- 送信先 IP アドレスと IP サブネットマスクフィールドは、このスタティックルートが全ての 134.177.x.x アドレスに適用されることを指定します。
- ゲートウェイ IP アドレスフィールドは、これらのアドレスに対する全てのトラヒックが 192.168.0.100 で ISDN ルータに転送されることを指定します。
- 1 のメートル法の数値は、ISDN ルータが LAN 上にあるために機能します。
- プライベートは、RIP がアクティブになっている場合、予防的セキュリティ測定としてのみ選択されます。

リモート管理アクセスを有効にする

リモート管理ページを使用して、インターネット上の単数または複数のユーザーが MR814v2 ルータのスタータスを設定、アップグレート、チェックすることができます。

	**注**：ルータのデフォルト設定パスワードがきわめて安全なパスワードに変更されていることを確認してください。理想的なパスワードは、いかなる言語であれ辞書に載っている言葉を含まず、文字（大文字と小文字）、数字、記号を組み合わせたものが望ましいといえます。パスワードは、最大 30 文字まで入力できます。

リモート管理に対してルータを設定するには、次の手順に従います。

1. リモート管理をオンにするチェックボックスを選択します。
2. 外部アドレスを指定すると、ルータのリモート管理にアクセスすることができます。

   注：セキュリティを強化するために、外部 IP アドレスへのアクセスをできるだけ制限してください。

   a. インターネット上の任意の IP アドレスからアクセスを許可するには、全員を選択します。

   b. インターネット上のある範囲の IP アドレスからアクセスを許可するには、IP アドレス範囲を選択します。
   開始および終了 IP アドレスを入力して、許可された範囲を定義します。

   c. インターネット上の単一 IP アドレスからアクセスを許可するには、この PC のみを選択します。
   アクセスを許可された IP アドレスを入力します。

3. 管理インターフェイスにアクセスするために使用されるポート番号を指定します。

   ウェブブラウザへのアクセスは通常、標準の HTTP サービスポート 80 を使用します。セキュリティを高めるために、提供されたボックスにその番号を入力することにより、リモート管理ウェブインターフェイスをカスタムポートに変更することができます。1024 から 65535 まえの数字を選択できますが、ただし、共通サービスポートの数字は使用しないでください。デフォルトは 8080 で、この数字は HTTP に対する共通の代替数字です。

4. 適用をクリックすると、変更が有効になります。

注：インターネットからルータにアクセスするとき、ルータの WAN IP アドレスをブラウザのアドレスまたは（IE で）またはロケーション（Netscape で）ボックスに入力できます。例えば、外部アドレスが 134.177.0.123 でポート番号 8080 を使用している場合、ブラウザに入力する必要があります。

```
http://134.177.0.123:8080
```

ユニバーサルプラグアンドプレイ (UPnP) を使用する

ユニバーサルプラグアンドプレイ (UPnP) により、インターネット器具やコンピュータなどのデバイスがネットワークにアクセスし、必要に応じて他のデバイスに接続することが可能になります。UPnP デバイスは、ネットワーク上の他の登録済み UPnP デバイスからデバイスを自動的に検出できます。

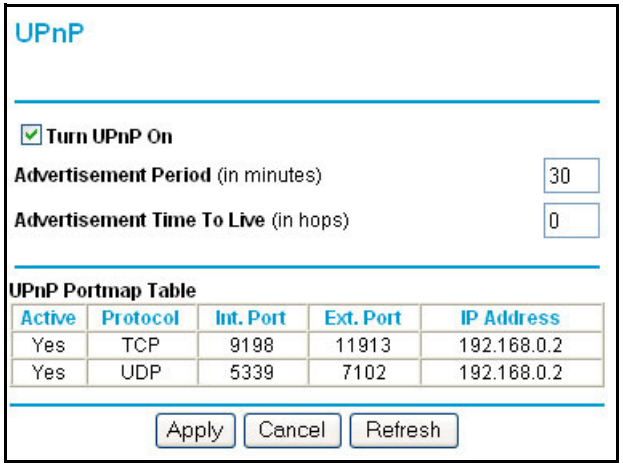


図 6-6.　　UPnP メニュー

ブラウザインターフェイスのメインメニューから、詳細設定の下で、UPnP をクリックしてください。下のガイドラインに従って UPnP をセットアップします。

UPnP をオンにする。UPnP は、自動デバイス設定に対して有効または無効に設定できます。UPnP に対するデフォルトの設定は有効にするです。無効にした場合、ルータはどのデバイスにも、ルータのポートフォーワーディング（マッピング）などのリソースを自動的にコントロールすることを許可しません。

広告期間：広告期間は、ルータがその UPnP 情報をブロードキャストする頻度です。この値は、1 から 1440 分までの範囲を取ります。デフォルトの期間は 30 分です。間隔を短くすると、コントロールポイントが追加ネットワークトラヒックを犠牲にして現在のデバイスステータスを確実に維持できます。間隔を長くするとデバイスステータスの新しさが犠牲になりますが、ネットワークトラヒックを大幅に削減できます。

広告時間をライブに：間隔がライブになる時間は、送信されるそれぞれの UPnP パケットに対してホップ（ステップ）で測定されます。ホップカウントがライブになる時間は、ブロードキャストパケットが非表示になる前に、それぞれの UPnP 広告に対して宣伝を許可するステップの数です。ホップの数は、1 から 255 までの範囲を取ることができます。ライブになる広告時間のデフォルト値は 4 ホップで、この数字はほとんどの家庭ネットワークに対して最高の値です。いくつかのデバイスが正しく更新されていなかったり到達していない場合、この値を少し増加する必要があります。

UPnP ポートマップ表：UPnP ポートマップ表は、現在ルータにアクセスしているそれぞれの UPnP デバイスの IP アドレス、およびデバイスが開いているポート（内部および外部）を表示します。UPnP ポートマップ表は、開いているポートのタイプと、そのポートがそれぞれの IP アドレスに対してまだアクティブになっているかどうかを表示します。

第 7 章
トラブルシューティング

本章では、MR814v2 ケーブル /DSL ワイヤレスルータのトラブルシューティングに関する情報を提供します。それぞれの問題を説明した後で、問題を診断し解決するために役に立つ指示が提供されます。

基本機能

ルータの電源をオンにすると、イベントの次のシーケンスが発生します。

1. 電源を初めて入れたとき、電源 LED がオンになっていることを確認してください。
2. 約 10 秒後、次を確認してください。
   a. テスト LED が点灯しない。
   b. LAN ポート LED が、接続されているすべてのローカルポートで点灯する。
   c. WAN ポート LED が点灯する。

   ポートの LED が点灯する場合、接続されているデバイスに対してリンクが確立されています。LAN ポートが 100 Mbps デバイスに接続されている場合、ポートの LED が緑になっていることを確認してください。ポートが 10 Mbps の場合、LED はオレンジ色になります。

これらの状態が発生しない場合、次項を参照してください。

電源 LED が点灯しない

ルータの電源がオンで、電源とその他の LED がオフになっている場合：

- 電源コードがルータに正しく接続され、電源装置のアダプタが正常なコンセントに正しく接続されているか確認します。
- 本製品用に NETGEAR が供給する 7.5 V DC の電源アダプタを使用していることをチェックします。

それでもエラーが発生する場合、ハードウェアに問題がありますので技術サポートにお問い合わせください。

LED がオフにならない

ルータの電源がオンになっているとき、LED は約秒オンになり、その後オフになります。全ての LED がオンになったままであれば、ルータ内部に障害があります。

電源を入れた後、全ての LED が 1 分間オンになっている場合：

- 電源を一度切ってすぐに入れなおし、ルータが正常な状態に戻るかを確認します。
- ルータの設定を消去して出荷時設定に戻します。これは、ルータの IP±ƒ?⁄¾ を 192.168.0.1 に設定します。この手順は、7-7 ページの「初期設定とパスワードを復元する」で説明いたします。

それでもエラーが発生する場合、ハードウェアの問題が考えられますので技術サポートにお問い合わせください。

LAN または WAN ポート LED がオンにならない

イーサネット接続が行われているときに LAN LED または WAN LED が点灯しない場合、次のチェックしてください。

- イーサネット接続がルータおよびハブまたはワークステーションでしっかりしていることを確認してください。
- 接続されたハブまたはワークステーションに対して、電源がオンになっていることを確認してください。
- 正しいケーブルを使用していることを確認してください。
  - ルータの WAN ポートをケーブルまたは DSL モデムに接続しているとき、ケーブルまたは DSL モデムに付属するケーブルを使用してください。このケーブルは、標準のストレートスルーイーサネットケーブルでもイーサネットクロスオーバーケーブルでもかまいません。

ウェブ設定インターフェイスのトラブルシューティング

ローカルネットワークの PC からルータのウェブ設定インターフェイスにアクセスできない場合、次をチェックしてください。

- 前項で説明したように、PC とルータの間のイーサネット接続をチェックしてください。
- PC と IP アドレスがルータと同じサブネットにあることを確認してください。推奨されるアドレッシング方式を使用している場合、PC のアドレスは 192.168.0.2 から 192.168.0.254 の範囲になければなりません。C-6 ページの「TCP/IP プロパティを確認する」または C-18 ページの「Macintosh コンピュータ用の TCP/IP プロパティを確認する」を参照して、PC の IP アドレスを検出してください。付録 C の指示に従って、PC を設定してください。

  注：PC の IP アドレスが 169.254.x.x として表示される場合：Windows と MacOS の最新バージョンは、コンピュータが DHCP サーバーにアクセスできない場合、IP アドレスを生成し割り当てます。これらの自動生成アドレスは 169.254.x.x の範囲内にあります。IP アドレスがこの範囲にある場合、PC からルータへの接続をチェックし PC を再起動してください。
- ルータの IP アドレスが変更され現在の IP アドレスがわからない場合、ルータの設定を消去して出荷時設定に戻してください。これは、ルータの IP±ƒ?⁄¾ を 192.168.0.1 に設定します。この手順は、7-7 ページの「初期設定とパスワードを復元する」で説明いたします。
- お使いのブラウザが Java、JavaScript、ActiveX を有効にしていることを確認してください。Internet Explorer を使用している場合、[更新] をクリックして Java アプレットがロードされていることを確認してください。
- ブラウザを終了した後に再び起動してください。
- 現在のログイン情報を使用していることを確認してください。出荷時設定のログイン名は **admin** で、パスワードは**パスワード**です。この情報を入力しているとき、CAPS LOCK がオフになっていることを確認してください。

ルータがウェブ設定インターフェイスで行われた変更を保存していない場合、次のチェックしてください。

- 設定を入力しているとき、他のメニューやタブに移動する前に、または変更が失われる前に、[適用] ボタンを必ずクリックしてください。
- ウェブブラウザの [更新] または [リロード] ボタンをクリックしてください。変更は行われても、ウェブブラウザが古い設定をキャッシュすることもあります。

ISP 設定をトラブルシューティングする

ルータがインターネットにアクセスできない場合、ルータが ISP から WAN IP アドレスを取得できるかどうかをまず決定する必要があります。スタティック IP アドレスを割り当てられていない限り、ルータは ISP から IP アドレスを要求する必要があります。ウェブ設定マネージャを使用して、その要求が正常に達成されたかどうかを判断することができます。

WAN IP アドレスをチェックするには、次の手順に従います。

1. ブラウザを起動し、www.netgear.com などの外部サイトを選択します
2. http://192.168.0.1 でルータの設定の [メインメニュー] にアクセスします
3. [メンテナンス] 見出しの元で、[ルータステータス] を選択します。
4. IP アドレスが WAN ポートに表示されているかチェックします。
   0.0.0.0 が表示される場合、ルータは ISP から IP アドレスをまだ取得していません。

ルータが ISP から IP アドレスを取得できない場合、次の手順を実行して、ケーブルや DSL モデムに新しいルータを認識させる必要があります。

1. ケーブルまたは DSL モデムの電源をオフにします。
2. ルータの電源をオフにします。
3. 5 分待って、ケーブルまたは DSL モデムの電源を再び入れてください。
4. モデムの LED が ISP との同期を再び取得していることを示しているとき、ルータの電源を再び入れてください。

ルータが ISP から IP アドレスをそれでも取得できない場合、問題は次のどれかである可能性があります。

- ISP がログインプログラムを要求している。
  ISP が PPP オーバーイーサネット (PPPoE) または他のタイプのログインのどちらを要求しているのか尋ねてください。
- ISP がログインを要求する場合、ログイン名とパスワードを間違って設定していることが考えられます。
- ISP が PC のホスト名をチェックすることがあります。
  ISP アカウントの PC ホスト名を [基本設定] メニューのアカウント名として割り当てます。
- ISP のみがイーサネット MAC アドレスをインターネットに接続でき、PC の MAC アドレスをチェックできます。この場合 :

新しいネットワークデバイスを購入したことを ISP に通知し、ルータの MAC アドレスを使用するように求めてください。

または

ルータを設定して、PC の MAC アドレスを偽装します。これは、[基本設定] メニューで行われます。2-15 ページの「インターネット接続を手動で設定する」を参照してください。

ルータは IP アドレスを取得できるが、PC がインターネットからウェブページをロードできません。

- PC が DNS サーバーのアドレスを認識していないことが考えられます。

  DNS サーバーは、数値 IP アドレスに対してインターネット名（例えば、www など）を変換するインターネット上のホストです。一般的に、ISP は 1 つまたは 2 つの DNS サーバーのアドレスをユーザーの使用のために提供します。ルータの設定中に DNS アドレスを入力する場合、PC を再起動し C-6 ページの「TCP/IP プロパティを確認する」で説明したように、DNS アドレスを確認してください。または、お使いのオペレーティングシステムのマニュアルで説明されているように、DNS アドレスで PC を手動で設定することもできます。

- お使いの PC が、ルータをその TCP/IP ゲートウェイとして設定していないことが考えられます。

  PC が DHCP によりルータからその情報を取得する場合、PC を再起動し、C-6 ページの「TCP/IP プロパティを確認する」で説明したようにゲートウェイアドレスを確認してください。

ピングユーティリティを使用した TCP/IP ネットワークのトラブルシューティング

ほとんどの TCP/IP 端末デバイスとルータには、指定されたデバイスにエコー要求パケットを送信するピングユーティリティが含まれています。デバイスは、エコーの返事に応答します。TCP/IP ネットワークのトラブルシューティングは、PC またはワークステーションのピングユーティリティを使用して、非常に簡単に実行できます。

ルータへの LAN パスをテストする

PC からのルータをピングして、ルータに対する LAN パスが正しくセットアップされているか確認できます。

Windows 95 以降で作動する PC からルータをピングするには、次の手順に従います。

1. Windows ツールバーから、[スタート] ボタンをクリックし [ファイル名を指定して実行] を選択します。
2. 提供されたフィールドに、次の例のように、まずピングを続いてルータの IP アドレスを入力します。

   ピング 192.168.0.1

3. [OK] をクリックします。

   次のようなメッセージが表示されます。

   32 バイトのデータを持つ <IP アドレス > をピングする

   パスが機能している場合、次のメッセージが表示されます。

   <IP アドレス > からの応答 バイト =32 時間 =NN ms TTL=xxx

   パスが機能していない場合、次のメッセージが表示されます。

   要求はタイムアウトになりました

   パスが正しく機能していない場合、次の問題のどれかが考えられます。

   - 不正な物理的接続
     - LAN ポートの LED がオンになっていることを確認します。LED がオフになっている場合、ページ 7-2 の「LAN または WAN ポート LED がオンにならない」の従ってください。
     - 対応する Link LED がネットワークインターフェイスカードおよびハブポート（もし、あれば）に対してオンになっており、ワークステーションとルータに接続されていることをチェックします。
   - 不正なネットワーク接続
     - イーサネットカードのドライバソフトウェアと TCP/IP ソフトウェアがどちらも、PC またはワークステーションにインストールされ設定されているかを確認します。
     - ルータとワークステーションの IP アドレスが正しくて、そのアドレスが同じサブネットにあることを確認します。

PC からリモートデバイスへのパスをテストする

LAN のパスが正しく機能していることを確認した後、PC からリモートデバイスへのパスをテストします。Windows の実行メニューから、次を入力します。

PING -n 10 *<IP アドレス>*

<IP アドレス> は、ISP の DNS サーバーなどのリモートデバイスの IP アドレスです。

パスが正しく機能していれば、前項の返答が表示されます。返答がない場合、次の手順を実行します。

予 tPC が、デフォルトのゲートウェイで一覧されたルータの IP アドレスをもっていることをチェックします。PC の IP 設定が DHCP により割り当てられている場合、この情報は PC のネットワークコントロールパネルに表示されません。ルータの IP アドレスが C-6 ページの「TCP/IP プロパティを確認する」で説明したように、デフォルトのゲートウェイとして一覧されていることを確認します。

予 tPC のネットワークアドレス（ネットマスクによって指定された IP アドレスの部分）がリモートデバイスのネットワークアドレスと違っていることを確認してください。

予 t ケーブルまたは DSL モデムが接続され機能しているかをチェックしてください。

予 tISP が PC にホスト名を割り当てている場合、[基本設定] メニューにアカウント名としてホスト名を入力してください。

予 tISP は、PC の 1 つだけ除いて全部のイーサネット MAC アドレスを拒絶することもあります。多くのブロードバンド ISP はブロードバンドの MAC アドレスからくるトラヒックのみを許可することによってアクセスを制限していますが、一部の ISP ではそのモデムに接続されている単一 PC の MAC アドレスへのアクセスをさらに制限しています。この場合、ルータを認証された PC の MAC アドレスを「コピー」または「偽装」するように設定する必要があります。2-15 ページの「インターネット接続を手動で設定する」を参照してください。

初期設定とパスワードを復元する

本項では、出荷時設定を復元する方法、ルータの管理者パスワードを**パスワード**にまたIP アドレスを 192.168.0.1 に変更する方法について説明しています。現在の設定を消去して、出荷時設定を次の 2 通りで復元できます。

- ルータの [消去] 機能を使用する（5-9 ページの「設定を消去する」をご覧ください）。
- ルータのリアパネルの [デフォルトのリセット] ボタンを使用します。管理者パスワードまたは IP アドレスが分からないときは、この方式を使用して消去してください。

管理者パスワードや IP アドレスを知らずに出荷時設定を復元するには、ルータの背面パネルの [デフォルトのリセット] ボタンを使用します。

1. Test LED がオンになるまで（約、10 秒）[デフォルトのリセット] ボタンを押し続けてください。
2. [デフォルトのリセット] ボタンを離して、ルータが再起動するのをお待ちください。

日付と時間に関する問題

コンテンツフィルタリング項の電子メールメニューには、現在の日付と時間表示されます。MR814v2 ルータはネットワークタイムプロトコル (NTP) を使用して、インターネットのいくつかのネットワークタイムサーバーのどれかから現在の時間を取得します。ログの各エントリには、日付と時間がスタンプされています。日付と時間機能に関する問題には、次のものが含まれます。

- 表示される日付が 2000 年 1 月 1 日になる。原因：ルータがネットワークタイムサーバーにまだ正常に接続されていません。インターネットアクセス設定が正しく設定されているか、チェックしてください。ルータの設定が完了したら、少なくとも 5 分待って、日付と時間を再びチェックしてください。
- 時間が 1 時間ずれる。原因：ルータが夏時間を自動的に検出していません。電子メールメニューで、「夏時間の調整」とマークされているボックスにチェックマークを入れたり外したりしてください。

付録 A
技術仕様

この付録は、MR814v2 ケーブル /DSL ワイヤレスルータに対する技術仕様を提供します。

ネットワークプロトコルと標準互換性

データとルーティングプロトコル	TCP/IP、RIP-1、RIP-2、DHCP PPP オーバーイーサネット (PPPoE)

電源アダプタ

北米：	120V、60 Hz、入力
英国、オーストラリア：	240V、50 Hz、入力
ヨーロッパ：	230V、50 Hz、入力
日本：	100V、50/60 Hz、入力
全ての地域（出力）：	7.5 V DC @ 1A 出力、20W 最大

物理仕様

寸法：	28 x 175 x 118 mm (1.1 x 6.89 x 4.65 インチ)
重量：	0.3 kg (0.66 lb)

環境仕様

動作温度：	0° ～ 40°C (32° ～ 104°F)
動作湿度	90% 最大相対湿度、結露なきこと

電磁気放出

適合要件：	FCC パート 15 Class B

	VCCI Class B
	EN 55 022 (CISPR 22)、Class B
インターフェイス仕様	
LAN:	10BASE-T または 100BASE-Tx、RJ-45
WAN：	10BASE-T、RJ-45
ワイヤレス	
無線データ転送速度	1、2、5.5、11Mbps 自動速度感知
周波数	2.4-2.5Ghz
データ暗号化：	直接シーケンススペクトラム拡散 (DSSS)
802.11b 動作範囲	屋外環境 室内環境 @ 11 Mbps 120 m 60 m @ 5.5 Mbps 170 m 80 m @ 2 Mbps 270 m 130 m @ 1 Mbps 450 m 200 m
ワイヤレスネットワークあたりの最大のコンピュータ数：	各ノードによって生成されるワイヤレスネットワークトラヒックの総数によって制限。一般的に 30-70 ノード。
802.11b 動作周波数範囲	2.412~2.462 GHz （米国） 2.457~2.462 GHz（スペイン） 2.412~2.484 GHz （日本） 2.457~2.472 GHz （フランス） 2.412~2.472 GHz （ヨーロッパ ETSI）
802.11b 暗号化	40 ビット （64 ビットとも呼ばれる）、128 ビット WEP データ暗号化

付録 B
ネットワーク、ルーティング、ファイアウォール、ベーシック

本章では、IP ネットワーク、ルーティング、ネットワーキングの概要を説明します。

関連出版物

本書を読み進むうちに、詳細についてさまざまな RFC 文書を参照するように求められることがあります。RFC は、インターネットのアーキテクチャと操作を定義する組織、Internet Engineering Task Force：インターネットエンジニアリングタスクフォース (IETF) が出版した Request For Comment ：コメント要請 (RFC) です。RFC 文書は、インターネットの標準プロトコルと手順を要約し定義しています。文書は WWW の *www.ietf.org* にリストされ、他の多くのウェブサイトで映され索引を付けられています。

基本ルータの概念

大量のバンド幅を構内通信網 (LAN) に簡単かつ比較的安価に提供することができます。しかし、ローカルネットワークとインターネット間に高いバンド幅を提供するには、膨大な費用がかかります。この費用のために、インターネットアクセスは一般にケーブルや DSL モデムのような、低速の広域ネットワーク (WAN) により、提供されています。遅い WAN リンクを最大限に使用するために、インターネット専用のデータトラヒックを選択して送信するメカニズムを構築する必要があります。このデータを選択して転送する機能は、ルータによって実行されます。

ルータとは何ですか？

ルータとは、データ内のネットワーク層情報およびルータにより保持されるルーティングテーブルに基づくネットワーク間で、トラヒックを転送するデバイスです。これらのルーティングテーブルで、ルータはネットワークの他のルータで情報を収集しかつ変換することによって、ネットワーク全体の論理図式を確立します。この機能を使用して、ルータはネットワークトラヒックを転送する最高のパスを選択します。

ルータは、性能と規模、サポートされるルーティングプロトコルの数、サポートする物理的 WAN 接続の種類によって異なります。MR814v2 ケーブル /DSL ワイヤレスルータは、単一ユーザーのブロードバンド接続を介して IP プロトコルを経路指定する、小規模オフィスルータです。

ルーティング情報プロトコル

ネットワークの図式を構築して保持するルータで使用されるプロトコルの 1 つは、ルーティング情報プロトコル (RIP) です。RIP を使用して、各ルータは相互に定期的な更新を実行し、変更をチェックしてルーティングテーブルに追加します。

MR814v2 ルータは、古い RIP-1 と新しい RIP-2 プロトコルを共にサポートします。RIP-2 は強化点の中でも、特にサブネットとマルチキャストプロトコルをサポートします。RIP は、ほとんどの家庭では必要ありません。

IP アドレスとインターネット

TCP/IP ネットワークは全世界で相互接続されているため、インターネット上の各マシンは送信されたデータが正しい送信先に達していることを確認するために、唯一のアドレスを持つ必要があります。アドレスのブロックは、インターネットアサインドナンバーズオーソリティ：Internet Assigned Numbers Authority (IANA) により、割り当てられ管理されています。個人ユーザーと小さな組織は、IANA またはインターネットサービスプロバイダ (ISP) からアドレスを取得することができます。IANA:www.iana.org にお問い合わせください。

インターネットプロトコル (IP) は 32 ビットのアドレス構造を使用します。アドレスは通常、ドット付き表記（ドット付き 10 進表記とも呼ばれる）で記述され、8 ビットからなる各グループは小数点で分割された 10 進数の形式で記述されます。

例えば、次はバイナリアドレスです。

```
11000011  00100010  00001100  00000111
```

は、通常次のように記述されます。

```
195.34.12.7
```

後者の方が、覚えるのもコンピュータに入力するのも簡単です。

さらに、アドレスの 32 ビットは 2 つの部分に再分割されます。アドレスの最初の部分はネットワークとして識別され、2 番目の部分はホストノードまたはネットワークの端末を識別します。分割点は、アドレス範囲と用途によって変わります。

IP アドレスには、5 つの標準クラスがあります。これらのアドレスクラスは、ネットワークとアドレスのホストセクションを決定する上で異なる方法を持つため、ネットワークに異なる数のホストが存在できます。各アドレスタイプは独特のビットパターンで始まり、アドレスクラスを識別するために TCP/IP ソフトウェアによって使用されています。アドレスクラスを決定した後、ソフトウェアはアドレスのホストセクションを正しく識別できます。次の図は、各アドレスタイプに対するアドレスのネットワークとホストセクションを含め、3 つの主なアドレスクラスを示しています。

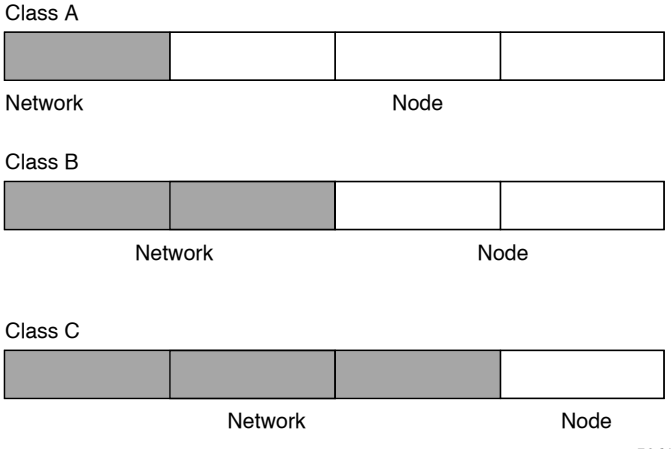


図 7-1 3 つの主なアドレスクラス

5 つのアドレスクラスは、次のとおりです。

- クラス A
  クラス A アドレスは、単一ネットワーク上に最大 16,777,214 のホストを持つことができます。8 ビットのネットワーク数と 24 ビットのノード数を使用します。クラス A アドレスは、この範囲内にあります。

  ```
  1.x.x.x ~ 126.x.x.x.
  ```

- クラス B
  クラス B アドレスは、1 つのネットワーク上に最大 65,354 のホストを持つことができます。クラス B アドレスは、16 ビットのネットワーク数と 16 ビットのノード数を使用します。クラス B アドレスは、この範囲内にあります。

  `128.1.x.x ~ 191.254.x.x.`

- クラス C
  クラス C アドレスは、1 つのネットワーク上に 254 のホストを持つことができます。クラス C アドレスは、ネットワークに対して 24 ビットおよびノードに対して 8 ビットを使用します。クラス C アドレスは、この範囲にあります。

  `192.0.1.x ~ 223.255.254.x.`

- クラス D
  クラス D アドレスは、マルチキャストに対して使用されます（多くのホストに対して送信されたメッセージ）。クラス D アドレスは、この範囲内にあります。

  `224.0.0.0 ~ 239.255.255.255.`

- クラス E
  クラス E アドレスは、実験用に使用されます。

このアドレッシング構造により、IP アドレスは各物理ネットワークと各物理ネットワーク上の各ノードを独自に識別することができます。

アドレスのネットワーク部分の各固有値の場合、範囲のベースアドレス（全てのゼロのホストアドレス）はネットワークアドレスとして知られ、通常ホストには割り当てられません。また、範囲のトップアドレス（全ての 1 のホストアドレス）は割り当てられていませんが、同じネットワークアドレスを使って全てのホストにパケットを同時に送信するためのブロードキャストアドレスとして使用されています。

ネットマスク

前に述べたそれぞれのアドレスクラスで、2 つの部分（ネットワークアドレスとホストアドレス）のサイズはクラスによって示されています。この分割計画は、IP アドレスに関連付けられたネットマスクによっても表現できます。ネットマスクは 32 ビットの量で、IP アドレスと（AND 演算子を使用して）論理的に結合するとき、ネットワークアドレスを生じます。例えば、クラス A、B、C のネットマスクはそれぞれ 255.0.0.0、255.255.0.0、255.255.255.0 です。

一例を挙げると、アドレス 192.168.170.237 はクラス C の IP アドレスで、そのネットワーク部分は上位 24 ビットです。ここに示すように、クラス C マスクと（AND 演算子を使用して）結合されたとき、アドレスのネットワーク部分のみが残ります。

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

以下と結合されています。

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

以下と同じです。

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

ドット付き 10 進表記の短縮形式として、ネットマスクは左から 1 の数字に置き換えて表すこともできます。この数字は、後方スラッシュ (/) に続いて IP アドレスに付加され、ì/n 狽ý して表記されます。例えば、アドレスを 192.168.170.237/24 と記述すると、ネットマスクは 24 の後にゼロが 8 つ付いたものとして示されます。

サブネットアドレッシング

アドレッシング構造を調べることによって、クラス C アドレスでさえも、ネットワークごとに多くのホストがあるとこが分かります。経路指定されたリンクの各端末が異なるネットワーク番号を要求する場合、そのような構造はアドレスを効率よく使用することができません。小さなオフィス LAN がそのように多くのデバイスを使うことはありえません。サブネットアドレッシングとして知られている技術を用いることにより、この問題を解決できます。

サブネットアドレッシングにより、1 つの IP ネットワークアドレスをサブネットワークとして知られている複数の物理ネットワークに分割することができます。一部のノード番号は、サブネット番号の代わりとしても使用されます。クラス B アドレスは、64,000 ノードに変換された 16 ビットのノード番号を提供します。64,000 ノードを使用する組織はほとんどないため、再割り当て可能なフリービットができます。サブネットアドレッシングマスクは、次に示すように自由なこれらのビットを使用します。

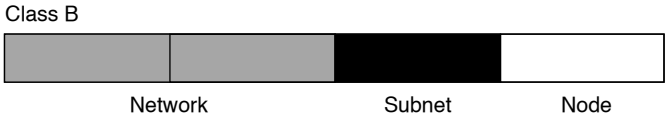


図 7-2 クラス B アドレスをサブネットする例

クラス B アドレスは、複数のクラス C アドレスに効率的に変換できます。例えば、172.16.0.0 の IP アドレスを割り当てても、ノードアドレスは最大 255 に制限されているため、8 つの特別なビットをサブネットアドレスとして使用できます。172.16.97.235 の IP アドレスは IP ネットワークアドレス 172.16、サブネット番号 97、ノード番号 235 として解釈されます。利用できるアドレスの 数字を拡張するだけでなく、サブネットアドレッシングは他の利点も提供しています。サブネットアドレッシングにより、ネットワークマネージャは、ネットワーク内の他の地理的位置または組織内の他の部門に対して異なるサブネットを使用することによって、ネットワークのアドレス計画を構築できます。

前の例はサブネットアドレスに対して第 3 オクテット全体を使用していますが、サブネットする際にはオクテット境界に制限されていることにご注意ください。ネットワーク番号を新たに作成するには、ホストアドレスからネットワークアドレスまでいくつかのビットを移すだけの手間しかかかりません。例えば、クラス C のネットワーク番号 (192.68.135.0) を 29 つに分割するには、1 ビットをホストアドレスからネットワークアドレスに移してください。新しいネットマスク（またはサブネットマスク）は 255.255.255.128 です。最初のサブネットには 192.68.135.1 から 129.68.135.126 までのホストを持つネットワーク番号 192.68.135.0 が、第 2 のサブネットには 192.68.135.129 から 192.68.135.254 までのホストを持つネットワーク番号 192.68.135.128 があります。

注：番号 192.68.135.127 は、最初のサブネットのブロードキャストアドレスであるため、割り当てられません。番号 192.68.135.128 は、第 2 のサブネットのネットワークアドレスであるため、割り当てられません。

次の表は、ドット付き 10 進表記の追加サブネットマスクビットを一覧表示しています。表を使用するには、オリジナルクラスのネットマスクを記録し、0 の値のオクテットを追加サブネットビットのドット付き 10 進値で置き換えます。例えば、サブネットマスク 255.255.255.0 を持つクラス C ネットワークを 16 のサブネット（4 ビット）に分割するために、新しいサブネットマスクは 255.255.255.240 になります。

表 7-1. 1 オクテットに対するネットマスク表記変換表

ビット数	ドット付き 10 進値
1	128
2	192
3	224
4	240
5	248

表 7-1. 1 オクテットに対するネットマスク表記変換表

6	252
7	254
8	255

次の表は、ドット付き 10 進およびマスク長 形式の両方で、いくつかの一般的なネットマスク値を表示しています。

表 7-2. ネットマスク形式

ドット付き 10 進数	マスク長
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

次の理由に対して同じネットマスクを使用するために、LAN セグメントに全てのホストを設定。

- ホストがローカル IP ブロードキャストパケットを認識できるように

  デバイスがそのセグメント近傍に一斉通信するとき、ホストアドレスに対して全ての 1 でローカルネットワークアドレスの送信先アドレスを使用します。この図式が機能するには、セグメントの全てのデバイスはどのビットがホストアドレスを構成するかについて一致をみる必要があります。

- 従って、ローカルルータまたはブリッジは、どのアドレスがローカルでありどのアドレスがリモートであるかを識別できます。

プライベート IP アドレス

お使いのローカルネットワークがインターネットから分離している場合（例えば、NAT を使用しているとき）、任意の IP アドレスを問題なしにホストに割り当てることができます。ただし、IANA はプライベートネットワーク用に次の 3 つのブロックの IP アドレスを予約しています。

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

この範囲から、ご自分のプライベートネットワーク番号を選択してください。MR814v2 ルータの DHCP サーバーは、プライベートアドレスを自動的に割り当てるために事前設定されています。

ユーザーの特定状況には関わりなく、任意の IP アドレスを作成せずに、常にここで説明したガイドラインに従ってください。アドレス割り当てに関する詳細については、RFC 1597、*プライベートインターネットに対するアドレス割り当て*、および RFC 1466、*IP アドレススペースの管理用ガイドライン*を参照してください。インターネットエンジニアリングタスクフォース (IETF) はその Web サイト www.ietf.org で RFC を公表しています。

NAT を使用した単一の IP アドレス操作

過去は、LAN の複数の PC がインターネットに同時にアクセスする必要が生じた場合、ISP からある範囲の IP アドレスを取得する必要がありました。このタイプのインターネットアカウントは、ルータではなくモデムを取り付けた単一ユーザーにより、一般的に使用されている単一アドレスのアカウントより高価です。MR814v2 ルータは、ネットワークアドレス変換（NAT）と呼ばれるアドレス共有方式を採用しています。この方式により、複数のネットワークに接続された PC は、ISP により静的または動的に割り当てられるたった 1 つの IP アドレスを使用して、インターネットアカウントを共有することができます。

ルータは、内部 LAN IP アドレスをインターネット上に 2 つとない単一アドレスに変換することによって、このアドレス共有を達成します。内部 LAN IP アドレスは、プライベートアドレスのことも登録済みアドレスのこともあります。IP アドレス変換に関する詳細については、RFC 1631、*IP ネットワークアドレス変換 (NAT)* を参照してください。

次の表は、単一 IP アドレス操作を説明しています。

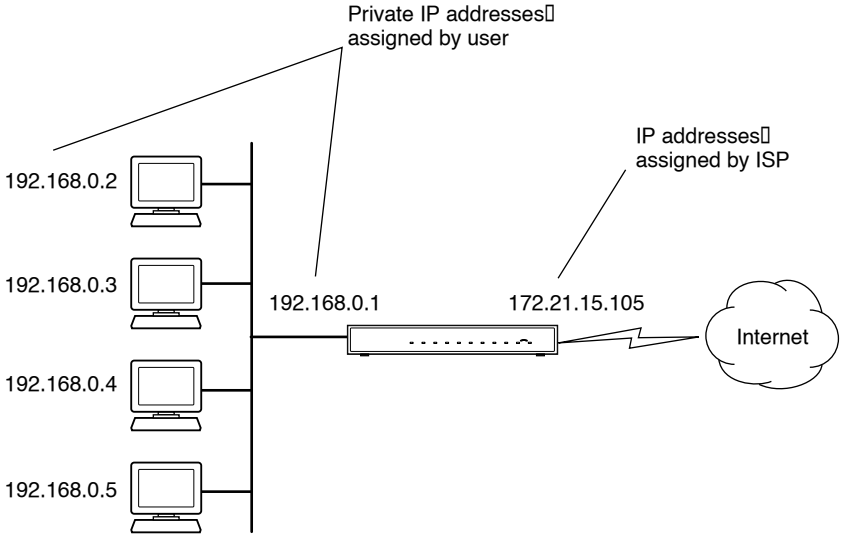


図 7-3 NAT を使用した単一の IP アドレス操作

内部 LAN アドレスが変換された接続によりインターネットで利用できないため、この図式はファイヤウォールに似た保護機能も追加しています。全ての着信要求は、ルータにより濾過されます。このフィルタリングにより侵入者がシステムに入り込むのを防ぐことができます。ただし、ポートフォーワーディングを使用すると、ローカルネットワークの 1 台の PC（例えば、Web サーバー）が外部ユーザーにアクセスすることができます。

MAC アドレスとアドレス解決プロトコル

1 つの LAN デバイスを他の LAN デバイスにデータを転送するために、IP アドレスだけを使用することはできません。複数の LAN デバイス間でデータを送信するためには、送信先デバイスの IP アドレスをそのメディアアクセスコントロール (MAC) アドレスに変換する必要があります。イーサネットネットワークの各デバイスは、メーカーが各デバイスに割り当てた 48 ビット数である、唯一の MAC アドレスを持っています。IP アドレスを MAC アドレスに関連付ける技術は、アドレス解決として知られています。インターネットプロトコルはアドレス解決プロトコル (ARP) を使用して、MAC アドレスを解決します。

デバイスがネットワーク上の他の端末にデータを送信し送信先 MAC アドレスがまだ記録されていない場合、APR が使用されます。ARP 要求は、ネットワーク上のブロードキャストです。ネットワーク上の全ての端末は、その要求を受信して読み込みます。選択した端末の送信先 IP アドレスはメッセージの一部として組み込まれており、この IP アドレスを持つ端末のみが ARP 要求に応答します。他の全ての端末は、要求を廃棄します。

関連文書

正しい IP アドレスを持つ端末は、送信デバイスにそれ自身の MAC アドレスで直接応答します 受信端末は、要求された送信先 MAC アドレスを持つ送信端末を提供します。各端末の IP アドレスデータと MAC アドレスデータは、ARP 表に保持されます。次にデータが送信されるとき、アドレスは表のアドレス情報から取得できます。

アドレス割り当てに関する詳細については、IETF 文書 RFC 1597、*プライベートインターネットに対するアドレス割り当て*、および RFC 1466、*IP アドレススペースの管理用ガイドライン*を参照してください。

IP アドレス変換に関する詳細については、RFC 1631、*IP ネットワークアドレス変換 (NAT)* を参照してください。

ドメイン名サーバー

インターネットの多くのリソースは、*www.NETGEAR.com* などの単一記述名によってアドレス指定することができます。このアドレスはアプリケーションレベルではとても役に立ちますが、ユーザーが実際にリソースと連絡を取るためには、記述名を IP アドレスに変換する必要があります。電話帳としてだけ名前を電話番号にマップするか、ARP 表として IP アドレスを MAC アドレスにマップすると、ドメイン名システム (DNSA) サーバーは IP アドレスにネットワークリソースの記述名をマップします。

PC がその記述名によってリソースにアクセスするとき、まず DNS サーバーと連絡を取り、リソースの IP アドレスを取得します。PC は、IP アドレスを使用して希望するメッセージを送信します。ISP などの多くの大規模組織は独自の DNS サーバーを保持し、顧客がアドレスを調べるためにサーバーを使用できるようにしています。

DHCP による IP 設定

IP ベースの構内通信網 (LAN) を取り付けるとき、各 PC は IP アドレスを使用して設定される必要があります。PC がインターネットにアクセスする必要がある場合、ゲートウェイアドレスおよび 1 つまたは複数の DNS サーバーアドレスで設定する必要もあります。手動設定に代わる方法として、ネットワークの各 PC がこの設定情報を自動的に取得できる方法があります。ネットワーク上のデバイスは、ダイナミックホスト設定プロトコル (DHCP) サーバーとして機能することもあります。DHCP サーバーは他の情報（ゲートウェイや DNS アドレスなど）と共に、IP アドレスのリストやプールを格納し、ネットワークの他のデバイスに割り当てることができます。MR814v2 ルータは、DHCP サーバーとして機能する能力があります。

MR814v2 ルータは、ISP に接続しているとき DHCP クライアントとしても機能します。ファイヤウォールは、ISP が DHCP によりこの情報を提供する場合、IP アドレス、サブネットマスク、DNS サーバーアドレス、ゲートウェイアドレスを自動的に取得します。

インターネットセキュリティとファイヤウォール

LAN がルータを通してインターネットに接続する場合、部外者がユーザーのネットワークにアクセスしたり混乱させるチャンスが生まれます。NAT ルータはプロセスの特性によりいくらかの保護を提供し、ルータの背後にあるネットワークはインターネットの部外者によるアクセスから保護されます。しかし、ハッカーがネットワークに関する情報を取得したり、少なくともインターネットアクセスを破壊する方法はないとはいえません。さらに大きなレベルの保護は、ファイヤウォールルータによって提供されます。

ファイヤウォールとは何ですか？

ファイヤウォールは他のネットワークからあるネットワークを保護するデバイスで、2 つのネットワーク間で通信を可能にしています。ファイヤウォールは NAT ルータの機能を組み込んで、ハッカー侵入や攻撃を処理する機能を追加しています。いくつかの既知の侵入または攻撃が報告されています。侵入や攻撃が検出されると、ファイヤウォールはその試みの詳細のログを取り、管理者にその試みを通知する電子メールをオプションで送信できます。ログの情報を使用して、管理者はハッカーの ISP で行動を起こすことができます。いくつかのタイプの侵入では、ファイヤウォールは一定期間ハッカーの IP アドレスからその後の全てのパケットを廃棄することによってハッカーを回避できます。

ステートフルパケットインスペクション

単純なインターネット共有ルータとは異なり、ファイヤウォールはステートフルパケットインスペクションと呼ばれるプロセスを使用して、攻撃や侵入からネットワークを保護します。FTP と Web ブラウザなどのユーザーレベルアプリケーションがネットワークトラヒックの複雑なパターンを作成できるため、ファイヤウォールはネットワーク接続状態のグループを分析することができます。ステートフルパケットインスペクションを使用して、着信パケットはネットワーク層で食い止められ、全てのネットワーク接続に関連する状態関連の情報を分析されます。ファイヤウォールの中央キャッシュは、全てのネットワーク接続と関連する状態情報を絶えず監視します。ファイヤウォールを通過する全てのトラヒックは、通過を許可するか拒絶するかを判断するために、これらの接続の状態に対して分析されます。

サービス拒絶攻撃

ハッカーはサービス拒絶 (DoS) 攻撃を起動することにより、ユーザーのネットワークの操作や通信を不能にすることができます。そのような攻撃で使用されている方式は、処理できる以上の要求でサイトをあふれされるのと同じくらい単純です。さらに複雑な攻撃は、ルータやゲートウェイで使用されるオペレーティングシステムの弱点を利用しようとします。オペレーティングシステムの中には、不正な長さの情報を含むパケットを送信するだけで混乱をきたすものもあります。

イーサネットケーブリング

イーサネットネットワークは元々、太いまたは細い同軸ケーブルを使用していましたが、現在はほとんどがシールドなしより対線 (UTP) ケーブリングを使用しています。UTP ケーブルには、4 つのより対線に配置され、RJ45 タイプのコネクタで終端処理された、8 つの導線が含まれています。標準のストレートスルー UTP イーサネットケーブルは、表 7-1 で説明したように EIA568B 規格のワイヤリングとピンアウトに従っています。

表 7-1. UTP イーサネットケーブルワイヤリング、ストレートスルー

ピン	ワイヤの色	信号
1	オレンジ / 白	送信 (Tx) +
2	オレンジ	送信 (Tx) -
3	緑 / 白	受信 (Rx) +
4	青	

表 7-1. UTP イーサネットケーブルワイヤリング、ストレートスルー

ピン	ワイヤの色	信号
5	青 / 白	
6	緑	受信 (Rx) -
7	茶色 / 白	
8	茶色	

アップリンクスイッチ、クロスオーバー、MDI/MDIX スイッチング

上のワイヤリング表で、送受信の概念はメディア依存インターフェイス (MDI) として接続された、PC の透視に基づいています。このワイヤリングで、PC はピン 1 と 2 上で送信します。ハブで、透視は逆になっており、ハブはピン 1 と 2 上で受信します。この接続はメディア依存インターフェイス - クロスオーバー (MDI-X) と呼ばれています。

PC と PC を接続するとき、ハブを他のハブポートに接続するとき、送信ペアは受信ペアで変換される必要があります。この変換は、2 つのメカニズムのどちらかによって行われます。ほとんどのハブは 1 つのポートのペアを変換するアップリンクスイッチを提供し、標準のイーサネットケーブルを使用して他のハブにそのポートを接続できます。2 番目の方式では、クロスオーバーケーブルを使用します。このケーブルは、送受信ペアが 2 つのケーブルコネクタの 1 つで変換される特殊なケーブルです。クロスオーバーケーブルはそれ自体では印が付いていないことがしばしばあるため、2 つのコネクタを比較することによって確認する必要があります。ケーブルコネクタは透明プラスチックであるため、並べて配置しそれぞれのワイヤの色の順番を見ることが簡単です。ストレートスルーケーブル上で、色の順番は両方のコネクタと同じになります。クロスオーバーケーブル上で、オレンジと青ペアは 1 つのコネクタから他のコネクタに変換されます。

MR814v2 ルータは自動アップリンク™ テクノロジ（MDI/MDIX とも呼ばれます）を組み込んでいます。それぞれのローカルイーサネットポートは、ポートに接続されるイーサネットケーブルが標準の接続（例えば、PC への接続）を持っているのか、アップリンク接続（例えば、ルータ、スイッチ、ハブへの接続）を持っているかを検出します。そのポートは、次に正しい設定にそれ自身を設定します。この機能は、クロスオーバーケーブルに関する心配を不要のものとしていますが、それは自動アップリンク™ がケーブルのどちらかのタイプを受け入れて正しい接続を行っているからです。

ケーブル品質

10 Mbits/ 秒 (10BASE-T) で動作するツイストペアイーサネットネットワークは低品質のケーブルを許容しますが、100 Mbits/ 秒 (10BASE-Tx) でケーブルは、エレクトロニックインダストリーアソシエーション (EIA) カテゴリ 5（Cat 5 または Cat V）として定格される必要があります。この定格は、ケーブル外被に印刷されます。カテゴリ 5 ケーブルは、ロスおよびクロストークに関する特定の要件を満たします。さらに、10 および 100 Mbits/ 秒ネットワークの両方に対して最大のケーブル長の制約があります。

付録 C
ネットワークの準備をする

この付録では、MR814v2 ケーブル /DSL ワイヤレスルータを通してインターネットに接続するためにネットワークを準備する方法と、インターネットサービスプロバイダ (ISP) からブロードバンドインターネットサービスの準備を確認する方法を説明します。

注：ブロードバンドモデムをインストールしている間に ISP 技術者がお使いのコンピュータを設定した場合、またはユーザーの側で ISP が提供した指示を使用してコンピュータを設定した場合、ユーザーのファイヤウォールの設定で使用するために、現在の設定情報をコピーする必要があります。お使いのコンピュータを再設定する前に、この情報を書き留めてください。詳細については、ページ C-20 の「Windows コンピュータ用の ISP 設定情報を取得する」を、またはページ C-21 の「Macintosh コンピュータ用の ISP 設定情報を取得する」を参照してください。

TCP/IP ネットワーキング用にコンピュータを準備する

コンピュータは TCP/IP（伝送制御プロトコル / インターネットプロトコル）と呼ばれるプロトコルを使用して、インターネットにアクセスします。ネットワーク上の各コンピュータは、TCP/IP をインストールずみで、そのネットワーキングプロトコルとして選択されている必要があります。ネットワークインターフェイスカード (NIC) が PC にすでにインストールされている場合、TCP/IP も同様にインストールされている必要があります。

ほとんどのオペレーティングシステムには、TCP/IP でネットワークを組むために必要なソフトウェアコンポーネントが含まれています。

- Windows® 95 以降のバージョンには、TCP/IP ネットワークを確立するためのソフトウェアコンポーネントが含まれています。
- Windows 3.1 には、TCP/IP コンポーネントは含まれていません。NetManage Chameleon などのサードパーティ製の TCP/IP アプリケーションパッケージを購入する必要があります。

- Macintosh Operating System 7 以降のバージョンには、TCP/IP ネットワークを確立するためのソフトウェアコンポーネントが含まれています。
- UNIX または Linux の全てのバージョンには、TCP/IP コンポーネントが含まれています。お使いのオペレーティングシステムまたはネットワーキングソフトウェアに付属する説明書に従って、コンピュータに TCP/IP をインストールしてください。

IP ネットワークで、各 PC とファイヤウォールには固有の IP アドレスを割り当てる必要があります。各 PC は、サブネットマスク（ネットマスク）、ドメイン名サーバー（DNS）アドレス、デフォルトのゲートウェイアドレスなどの、その他の IP 設定情報を使用する必要があります。ほとんどの場合、起動中に DHCP サーバーからその特定のネットワーク設定情報を PC が自動的に取得するために、TCP/IP をインストールする必要があります。これらの設定アイテムの意味と目的に関する詳細については、付録 B、「ネットワーク、ルーティング、ファイアウォール、ベーシック」を参照してください。

MR814v2 ルータは、DHCP サーバーとして出荷時に事前設定済みです。ファイヤウォールは、PC が再起動するときに次の TCP/IP 設定情報を自動的に割り当てます。

- PC またはワークステーションの IP アドレス ó192.168.0.2 から 192.168.0.254 まで
- サブネットマスク ó255.255.255.0
- ゲートウェイアドレス (ファイヤウォール)ó192.168.0.1

これらのアドレスは、プライベートネットワークで使用するための、IETF 指定のプライベートアドレス範囲の一部です。

TCP/IP ネットワーキングに対して Windows 95、98、Me を設定する

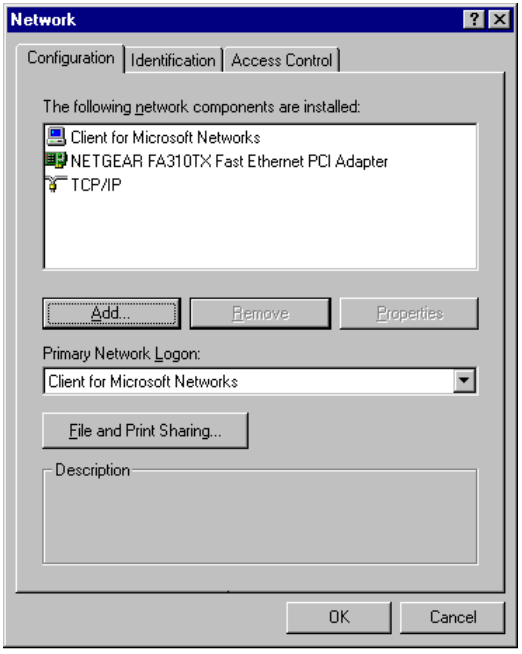
PC 準備プロセスの一部として、ネットワーク接続された各 PC で、TCP/IP を手動でインストールおよび設定する必要があります。開始する前に、Windows CD を用意してください。TCP/IP インストールプロセスの間にその CD を挿入する必要が生じる場合もあります。

Windows ネットワーキングコンポーネントをインストールまたは確認する

IP ネットワーキングに必要なコンポーネントをインストールまたは確認するには、次の手順に従います。

1. Windows タスクバーで、[スタート] ボタンをクリックし、[設定] をポイントし、[コントロール パネル] をクリックします。
2. [ネットワーク] アイコンをダブルクリックします。

   [ネットワーク] ウィンドウが開き、インストールされたコンポーネントのリストを表示します。



イーサネットアダプタ、TCP/IP プロトコル、Client for Microsoft Networks が組み込まれている必要があります。

注：アダプタ、TCP/IP、Client for Microsoft Networks をインストールするために、[ネットワーク] ウィンドウに表示されたその他のネットワークコンポーネントを取り外す必要はありません。

新しいアダプタをインストールする必要がある場合には、次のステップに従います。

a. 追加ボタンをクリックします。

b. [アダプタ] を選択し、[追加] をクリックします。

c. イーサネットアダプタのメーカーとモデルを選択し、[OK] をクリックします。

TCP/IP が必要な場合、次の手順に従います。

a. 追加ボタンをクリックします。

b. [プロトコル] を選択し、[追加] をクリックします。

c. Microsoft を選択します。

d. TCP/IP を選択し、[OK] をクリックします。

Client for Microsoft Networks が必要な場合、次の手順に従います。

a. 追加ボタンをクリックします。

b. [クライアント] を選択し、[追加] をクリックします。

c. Microsoft を選択します。

d. Microsoft Networks に対するクライアントを選択し、[OK] をクリックします。

3. 変更を有効にするには、PC を再起動します。

DHCP を有効にすると、Windows 95B、98、Me の TCP/IP 設定が自動的に設定されます。

TCP/IP プロトコルコンポーネントがインストールされた後、各 PC はそれ自体に関する特定の情報とそのネットワークで利用可能なリソースを割り当てる必要があります。この情報を設定するもっとも簡単な方法は、PC がネットワークの DHCP サーバーから情報を取得できるようにすることです。

TCP/IP を設定するために DHCP を使用しているとき、異なる Windows システムに関しては多くの似たような手順があります。

次のステップは、Windows のこれらのバージョンに対して設定プロセスをガイドします。

1

ネットワークコンピュータアイコンを検索します。

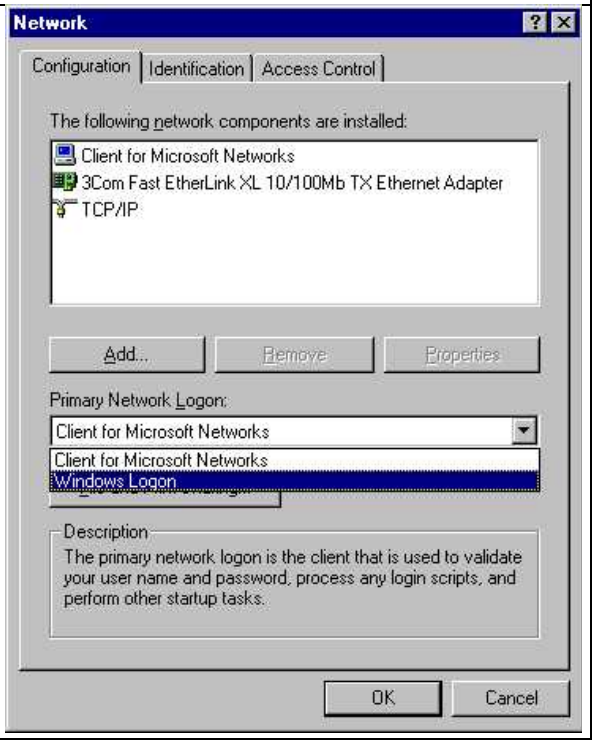
- [ネットワークコンピュータ] アイコンが Windlws デスクトップにある場合、マウスポインタをその上に置きマウスの右ボタンをクリックしてください。
- そのアイコンがデスクトップにない場合、
  - ウィンドウの左下にあるタスクバーの**スタート**をクリックします。
  - **設定**を選択し、次に**コントロール パネル**を選択します。
  - **ネットワークコンピュータ**アイコンを探し、それをクリックします。これは、下に示すように [ネットワーク] パネルを開きます。

2

図に示すように、次の設定を確認します。

- Client for Microsoft Network の存在
- イーサネットアダプタの存在
- TCP/IP の存在
- **プライマリネットワークログオン**が Windows ログオンに設定されている

プロパティボタンをクリックします。次の TCP/IP プロパティウィンドウが表示されます。



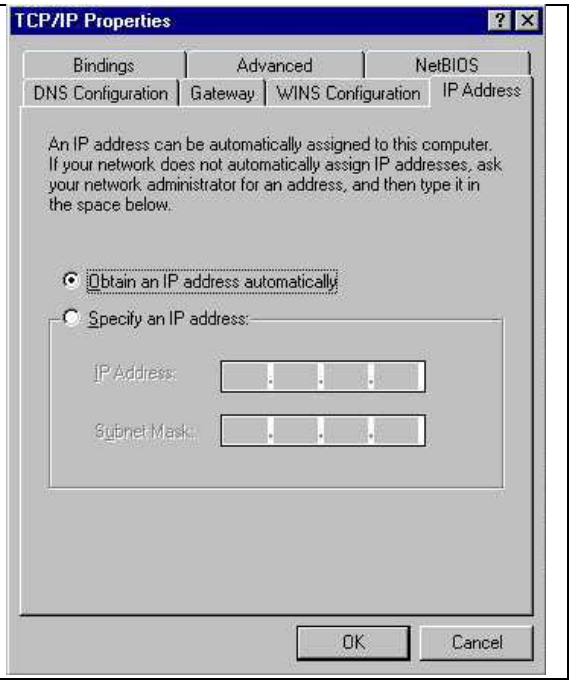
3

- デフォルトで、**IP アドレス**タブがこのウィンドウに表示されます。
- 次を確認します。

  IP アドレスを自動的に取得するが選択されます。選択されない場合、その左にあるラジオボタンをクリックして選択します。この設定は IP アドレスを自動的に割り当てるために、DHCP サーバーを有効にするように要求されます。
- **OK** をクリックして続行します。

PC を再起動します。

ネットワークのコンバージョンの Windows で各 PC 用のこれらのステップを繰り返します。



Windows のインターネットアクセス方式を選択する

1. Windows タスクバーで、[スタート] ボタンをクリックし、[設定] をポイントし、[コントロール パネル] をクリックします。
2. [インターネットオプション] アイコンをダブルクリックします。
3. [インターネット接続を手動でセットアップする] または [構内通信網 (LAN) を通して接続する] を選択し、[次へ] をクリックします。
4. [構内通信網 (LAN) を通して接続する] を選択して、[次へ] をクリックします。
5. LAN インターネット設定画面の全てのボックスのチェックマークを外し、[次へ] をクリックします。
6. ウィザードの最後まで続行します。

TCP/IP プロパティを確認する

PC を設定し再起動した後、ユーティリティ *winipcfg.exe* を使用して TCP/IP 設定をチェックできます。

1. Windows タスクバーで、[スタート] ボタンを、次に [ファイル名を指定して実行] をクリックします。
2. **winipcfg** を入力し、[OK] をクリックします。

   IP 設定ウィンドウが開き、（他の設定の中で）IP アドレス、サブネットマスク、デフォルトのゲートウェイを一覧表示します。
3. ドロップダウンボックスから、[イーサネット] アダプタを選択します。

   ウィンドウが更新され、NETGEAR がルータまたはゲートウェイにより接続することを推奨するデフォルトの TCP/IP 設定を使用している場合、下の値に一致する設定を表示します。

   - IP アドレスは、192.168.0.2 から 192.168.0.254 までの範囲です。
   - サブネットマスクは 255.255.255.0 です。
   - デフォルトのゲートウェイは 192.168.0.1 です。

IP ネットワーキング用に Windows NT4、2000 または XP を設定する

PC 準備プロセスの一部として、インストールして設定する必要があります。
各ネットワーク接続された PC の TCP/IP。開始する前に、Windows CD を用意してください。TCP/IP インストールプロセスの間にその CD を挿入する必要が生じる場合もあります。

Windows ネットワーキングコンポーネントをインストールまたは確認する

IP ネットワーキングに必要なコンポーネントをインストールまたは確認するには、次の手順に従います。

1. Windows タスクバーで、[スタート] ボタンをクリックし、[設定] をポイントし、[コントロール パネル] をクリックします。
2. [ネットワーク] アイコンと [ダイヤルアップ接続] アイコンをダブルクリックします。
3. イーサネットアダプタが PC にある場合、ローカルエリア接続に対するエントリが表示されます。そのエントリをダブルクリックします。
4. プロパティを選択します。

5. [Client for Microsoft Networks] と [インターネットプロトコル(TCP/IP)] があることを確認します。ない場合、[インストール] を選択して追加します。
6. [インターネットプロトコル (TCP/IP)] を選択し、[プロパティ] をクリックし、[IP アドレスを自動的に取得する] が選択されていることを確認します。
7. [OK] をクリックし、全ての [ネットワークとダイヤルアップ接続] ウィンドウを閉じます。
8. 次に、PC を再起動します。

Windows XP、2000、または NT4 における TCP/IP の DHCP 設定

TCP/IP を設定するために DHCP を使用しているとき、異なる Windows システムに関しては多くの似たような手順があります。

次のステップは、Windows のこれらのバージョンに対して設定プロセスをガイドします。

Windows XP における TCP/IP の DHCP 設定

1

ネットワークコンピュータアイコンを検索します。

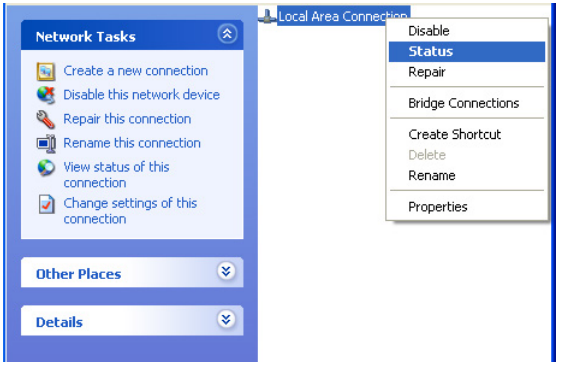
- Windows XP の新しい [スタート] メニューから**コントロール パネル**を選択します。
- コントロール パネルの**ネットワーク接続**アイコンを選択します。次のステップに進みます。

2

- [ネットワーク接続] ウィンドウが表示されます。

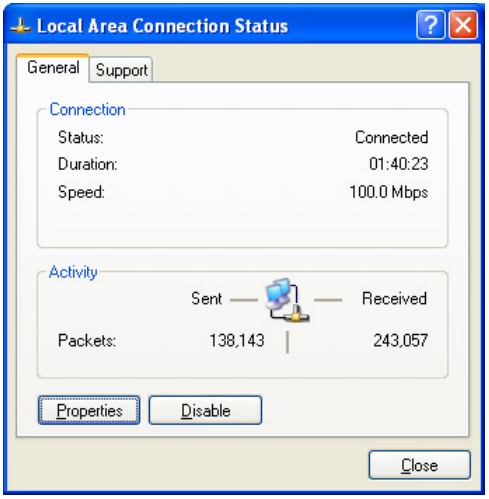
  ウィンドウの右側にある接続リストは、PC の全てのネットワーク接続セットアップを示します。

- 使用する**接続**を右クリックし、**ステータス**を選択します。



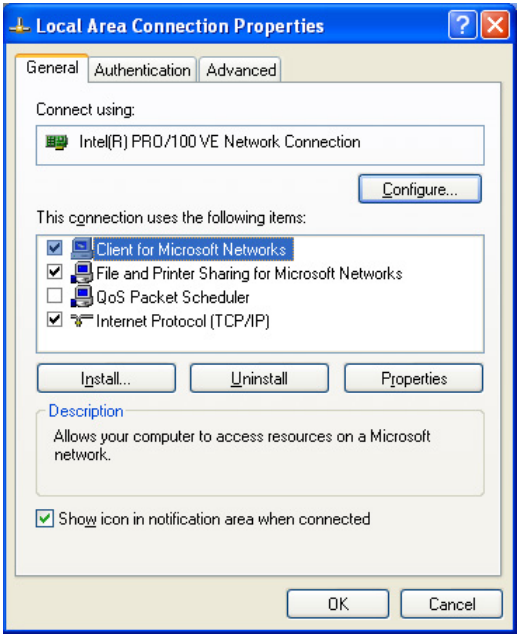
3

- ローカルエリア接続ステータスウィンドウが表示されます。このボックスは、接続ステータス、期間、速度、アクティビティ統計値を表示します。
- このウィンドウを使用するには、管理者ログオンアクセス権が必要になります。
- **プロパティボタン**をクリックすると、接続に関する詳細が表示されます。



4

- TCP/IP の詳細が、[サポート] タブページに表示されます。
- **インターネットプロトコル**を選択し、**プロパティ**をクリックして設定情報を表示します。

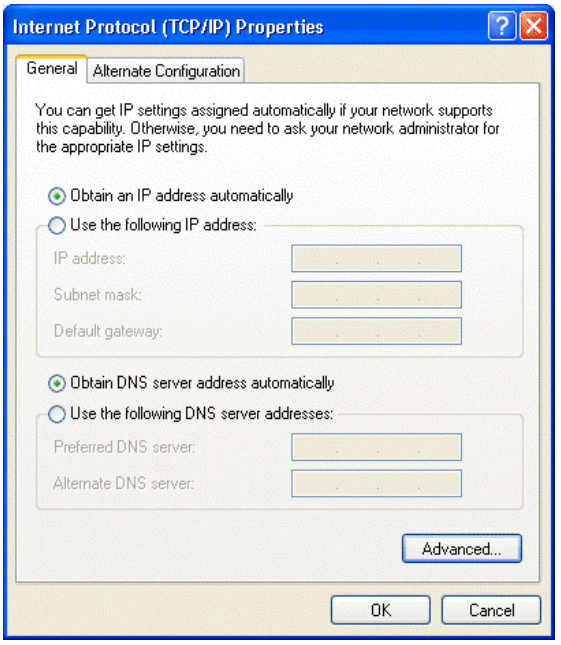


5

- **IP アドレスを自動的に取得する**ラジオボタンが選択されていることを確認します。
- **DNS サーバーアドレスを自動的に取得する**ラジオボタンが選択されていることを確認します。
- **OK** ボタンをクリックします。

これで、Windows XP の TCP/IP の DHCP 設定が完了しました。

ネットワークのコンバージョンの Windows で各 PC 用のこれらのステップを繰り返します。



Windows 2000 における TCP/IP の DHCP 設定

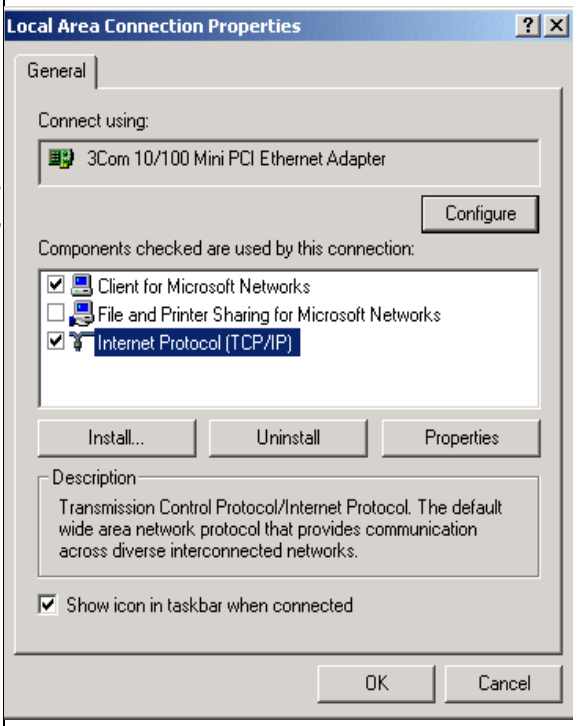
再び、ネットワークカードをインストールした後、Windows 2000 の TCP/IP が設定されます。TCP/IP がデフォルトで追加され、設定しなくても DHCP に設定されます。しかし、問題が発生したら、次のステップに従って Windows 2000 用 DHCP で TCP/IP を設定してください。

1

- Windows デスクトップの**マイネットワーク**アイコンをクリックします。[ネットワークとダイヤルアップ接続] と呼ばれるウィンドウが表示されます。
- **ローカルエリア接続**を右クリックし、**プロパティ**を選択します。

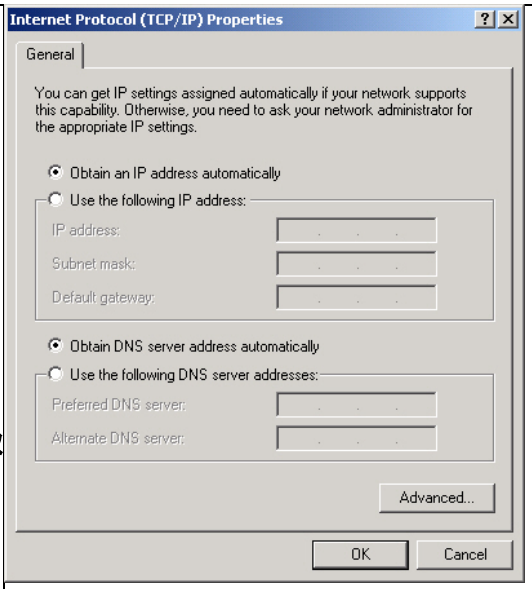
2

- **ローカルエリア接続プロパティ**ダイアログボックスが表示されます。
- **使用されている接続**で選択された正しいイーサネットカードがインストールされているか確認してください。ボックス。
- 少なくとも次の 2 つのアイテムが、「チェックされたコンポーネントがこの接続によって使用」のボックスに表示され選択されていることを確認します。
  - Client for Microsoft Network および
  - インターネットプロトコル (TCP/IP)
- **OK** をクリックします。



3

- インターネットプロトコル (TCP/IP) を選択したら、**プロパティ**をクリックしてインターネットプロトコル (TCP/IP) プロパティダイアログボックスを開きます。
- 次を確認します
  - **IP アドレスを自動的に取得する**が選択されます。
  - **DNS サーバーアドレスを自動的に取得する**が選択されます。
- **OK** をクリックしてローカルエリア接続プロパティに戻ります。

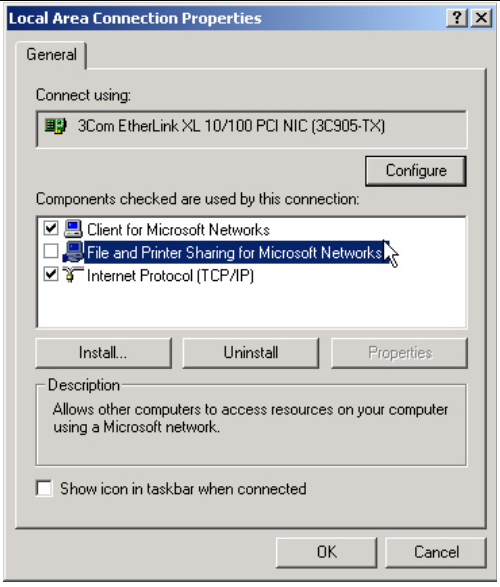


4

- **OK** を再びクリックして、Windows 2000 の設定プロセスを完了します。

PC を再起動します。

ネットワークのコンバージョンの Windows で各 PC 用のこれらのステップを繰り返します。



Windows NT4 における TCP/IP の DHCP 設定

ネットワークカードを設定すると、Windows NT 4.0 の TCP/IP 環境を設定する必要があります。この手順に従って、Windows NT 4.0 の DHCP で TCP/IP を設定します。

1

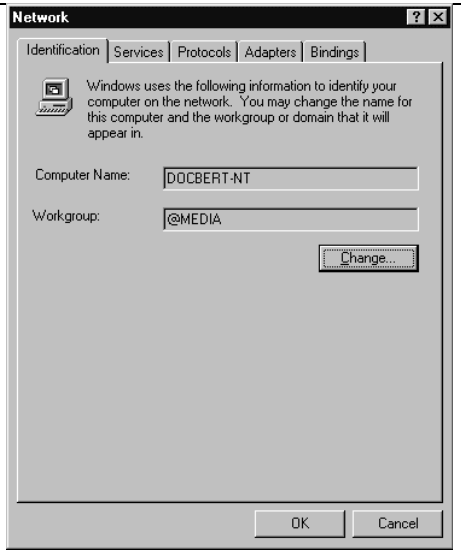
- [スタート] メニューから**設定**を選択し、次に**コントロール パネル**を選択します。[コントロール パネル] ウィンドウが表示されます。

2

- [コントロール パネル] ウィンドウで**ネットワーク**アイコンをダブルクリックします。

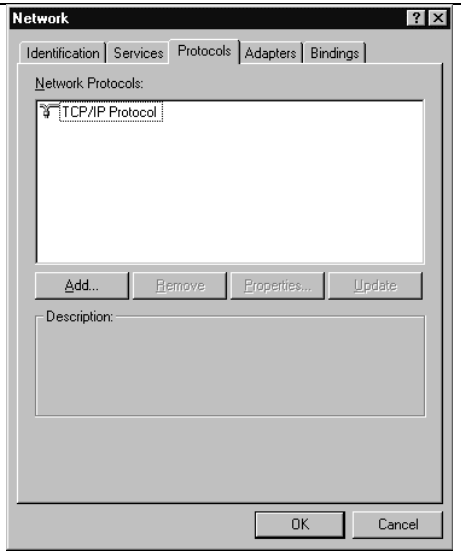
  ネットワークパネルが表示されます。

- **プロトコル**タブを選択して続行します。



3

- **ネットワークプロトコル**ボックスで **TCP/IP プロトコル**を強調表示し、**プロパティ**ボタンをクリックします。

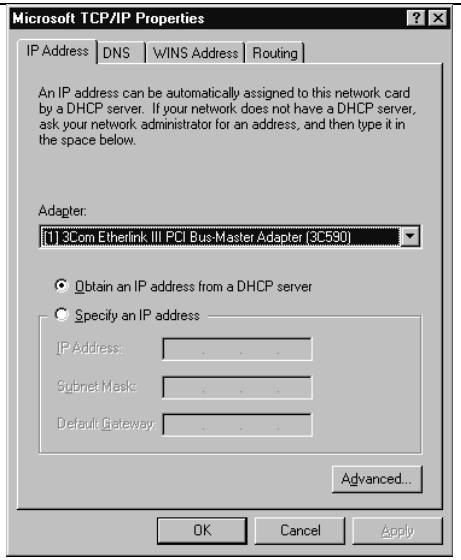


4

- **TCP/IP プロパティ**ダイアログボックスが表示されます。
- **IP アドレス**タブをクリックします。
- **DHCP サーバーから IP アドレスを取得する**とマークされたラジオボタンを選択します。
- **OK** をクリックします。これで、Windows NT の TCP/IP の DHCP 設定が完了しました。

PC を再起動します。

ネットワークのコンバージョンの Windows で各 PC 用のこれらのステップを繰り返します。



Windows XP、2000、NT4 の TCP/IP プロパティを確認する

PC の TCP/IP 設定をチェックするには、次の手順に従います。

1. Windows タスクバーで、[スタート] ボタンを、次に [ファイル名を指定して実行] をクリックします。

   [ファイル名を指定して実行] ウィンドウが開きます。

2. `cmd` を入力し、[OK] をクリックします。

   コマンドウィンドウが開きます。

3. `ipconfig /all` を入力します

   IP アドレス情報が一覧表示され、NETGEAR がルータまたはゲートウェイにより接続することを推奨するデフォルトの TCP/IP 設定を使用している場合、下の値に一致する設定を表示します。

   - IP アドレスは、192.168.0.2 から 192.168.0.254 までの範囲です。

- サブネットマスクは 255.255.255.0 です。
- デフォルトのゲートウェイは 192.168.0.1 です。

4. 終了を入力します。

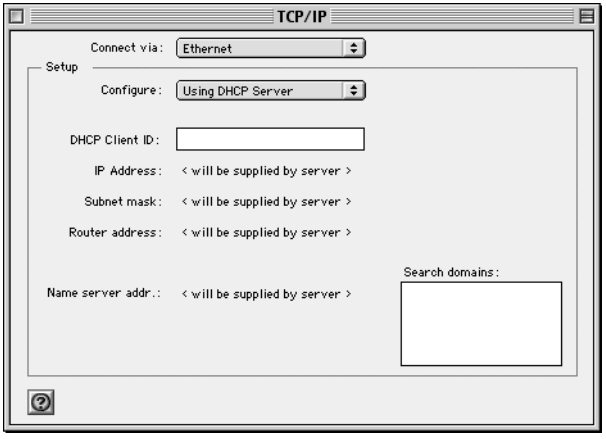
Macintosh for TCP/IP Networking を設定する

Macintosh Operating System 7 では、TCP/IP は Macintosh にすでにインストールされています。それぞれネットワーク接続された Macintosh 上で、TCP/IP を設定して DHCP を使用する必要があります。

MacOS 8.6 または 9.x

1. Apple メニューから、[コントロール パネル] を、次に TCP/IP を選択します。

   TCP/IP コントロール パネルが開きます。



2. [Connect via: 経由先] ボックスから、Macintosh のイーサネットインターフェイスを選択します。
3. [設定] ボックスから、[DHCP サーバーを使用する] を選択します。

   DHCP クライアント ID ボックスは、空のままにしておいてもかまいません

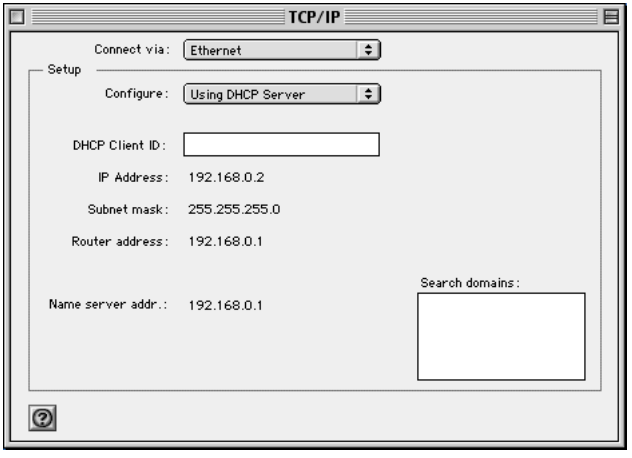
4. TCP/IP コントロール パネルを閉じます。
5. ネットワーク上の各 Macintosh に対して、これを繰り返します。

MacOS X

1. Apple メニューから、[System Preferences：システム環境設定] を、次に [ネットワーク] を選択します。
2. まだ選択していない場合、[設定] リストで [内蔵イーサネット] を選択します。
3. まだ選択していない場合、TCP/IP タブで [DHCP を使用する] を選択します。
4. [保存] をクリックします。

Macintosh コンピュータ用の TCP/IP プロパティを確認する

Macintosh を設定して再起動した後、TCP/IP コントロール パネルに戻ることによって、TCP/IP 設定をチェックできます。Apple メニューから、[コントロール パネル] を、次に TCP/IP を選択します。



パネルが更新され、NETGEAR が推奨するデフォルトの TCP/IP 設定を使用している場合、下の値に一致する設定を表示します。

- IP アドレスは、192.168.0.2 から 192.168.0.254 までの範囲です。
- サブネットマスクは 255.255.255.0 です。
- ルータアドレスは 192.168.0.1 です。

これらの値が表示されない場合、Macintosh を再起動、または [設定] を他のオプションに切り替え、次に [DHCP サーバーを使用する] に戻る必要があります。

インターネットアカウントの準備を確認する

インターネットにブロードバンドアクセスを行うには、ケーブルモデムまたは DSL モデムを使用してインターネットサービスプロバイダ (ISP) と契約して、単一ユーザーのインターネットアクセスアカウントを取得する必要があります。このモデムは個別の物理ボックス（カードではなく）で、コンピュータのネットワークインターフェイスカード (NIC) に接続するためのイーサネットポートを提供する必要があります。ファイヤウォールは USB 接続されたブロードバンドモデムをサポートしません。

単一ユーザーのインターネットアカウントの場合、ISP は 1 台のコンピュータに対し TCP/IP 設定情報を提供します。一般的アカウントでは、設定情報の多くは PC が ISP に接続されている間に始めて起動するときに動的に割り当てられ、その動的な情報を知る必要はありません。

複数のコンピュータ間でインターネット接続を共有するには、ファイヤウォールが単一 PC の代わりをし、それを単一 PC が通常使用する TCP/IP 情報で設定する必要があります。ファイヤウォールのインターネットポートがブロードバンドモデムに接続されているとき、ファイヤウォールは ISP に対して単一 PC として表示されます。ファイヤウォールは、ローカルネットワークの PC が単一 PC の振りをしてブロードバンドモデムを通してインターネットにアクセスできるようにします。これを達成するためにファイヤウォールが使用する方式は、ネットワークアドレス変換 (NAT) または IP マスカレード機能と呼ばれています。

ログインプロトコルは使用されていますか？

一部の ISP は特殊なログインプロトコルを要求し、インターネットにアクセスするためにはそのプロトコルにログイン名とパスワードを入力する必要があります。WinPOET または EnterNet などのプログラムを実行することによりインターネットアカウントにログインする場合、アカウントは PPP オーバーイーサネット (PPPoE) を使用します。

ルータを設定するとき、ルータの設定メニューにログイン名とパスワードを入力する必要があります。ネットワークとファイヤウォールを設定した後、ファイヤウォールは必要なときにログインタスクを実行し、PC からログインプログラムを実行する必要はありません。ログインプログアムをアンインストールする必要はありません。

ユーザーの設定情報とは何ですか？

ISP は、ますます設定情報を動的に割り当てるようになっています。ただし、ISP が設定情報を動的に割り当てず、その代わりに固定設定を使用する場合、ISP はアカウントに対する次の基本情報を与えます。

- IP アドレスとサブネットマスク
- ISP のルータのアドレスである、ゲートウェイ IP アドレス
- 1 つまたは複数のドメイン名サーバー (DNS)IP アドレス
- ホスト名とドメインの接尾辞

  例えば、アカウントの完全なサーバー名は次のように表示されます。

  `mail.xxx.yyy.com`

  この例で、ドメインの接尾辞は `xxx.yyy.com` です。

これらのアイテムのどれかが ISP によって動的に供給される場合、ファイヤウォールは自動的にそれを取得します。

ISP 技術者がブロードバンドモデムのインストール中に PC を設定した場合、または ISP が提供する説明書を使用してユーザーが自分で設定した場合、ファイヤウォールで使用するために PC を再設定する前に、PC のネットワーク TCP/IP プロパティウィンドウまたは Macintosh TCP/IP コントロール パネルから設定情報をコピーする必要があります。これらの手順を次に説明します。

Windows コンピュータ用の ISP 設定情報を取得する

上で述べたように、MR814v2 ルータを設定するときにこの情報を使用できるように、PC から設定情報を収集する必要があります。お使いの ISP がアカウント情報を動的に提供しないとき、この手順に従う必要があります。

インターネットアクセスに対してファイヤウォールを設定する必要がある情報を取得するには、次の手順に従います。

1. Windows タスクバーで、[スタート] ボタンをクリックし、[設定] をポイントし、[コントロール パネル] をクリックします。
2. [ネットワーク] アイコンをダブルクリックします。

   [ネットワーク] ウィンドウが開き、インストールされたコンポーネントのリストを表示します。

3. TCP/IP を選択し、[プロパティ] をクリックします。

   TCP/IP プロパティダイアログボックスが開きます。

4. IP アドレスタブを選択します。

   IP アドレスとサブネットマスクが表示されたら、その情報を書き留めてください。アドレスが存在する場合、アカウントは固定した（静的）IP アドレスを使用します。アドレスが存在しない場合、アカウントは動的に割り当てた IP アドレスを使用します。[IP アドレスを自動的に取得する] をクリックします。

5. ゲートウェイタブを選択します。

   インストールされたゲートウェイの元で IP アドレスが表示されたら、そのアドレスを書き留めてください。これは、ISP のゲートウェイアドレスです。アドレスを選択し、次に [削除] をクリックしてゲートウェイアドレスを削除します。

6. DNS 設定タブを選択します。

   どれかの DNS サーバーアドレスが表示されたら、そのアドレスを書き留めてください。ホストまたはドメイン情報ボックスにどれかの情報が表示されたら、それを書き留めてください。DNS を無効にするをクリックします。

7. [OK] をクリックして変更を保存し、[TCP/IP プロパティ] ダイアログボックスを閉じます。

   ネットワークウィンドウに戻ります。

8. [OK] をクリックします。

9. 指示されたら、PC を再起動します。また、Windows CD を挿入するようにも求められます。

Macintosh コンピュータ用の ISP 設定情報を取得する

上で述べたように、MR814v2 ルータを設定するときにこの情報を使用できるように、Macintosh から設定情報を収集する必要があります。お使いの ISP がアカウント情報を動的に提供しないとき、この手順に従う必要があります。

インターネットアクセスに対してファイヤウォールを設定する必要がある情報を取得するには、次の手順に従います。

1. Apple メニューから、[コントロール パネル] を、次に TCP/IP を選択します。

TCP/IP コントロール パネルが開き、設定のリストを表示します。[設定] が [DHCP サーバーを使用する] である場合、アカウントは動的に割り当てられた IP アドレスを使用します。この場合、[コントロール パネル] を閉じ、本項の残りをスキップします。

2. IP アドレスとサブネットマスクが表示されたら、その情報を書き留めてください。
3. ルータアドレスの元で IP アドレスが表示されたら、そのアドレスを書き留めてください。これは、ISP のゲートウェイアドレスです。
4. どれかの名前サーバーアドレスが表示されたら、そのアドレスを書き留めてください。これらは、ISP の DNS アドレスです。
5. [検索] ドメイン情報ボックスにどれかの情報が表示されたら、それを書き留めてください。
6. [設定] を [DHCP サーバーを使用する] に変更します。
7. TCP/IP コントロール パネルを閉じます。

ネットワークを再起動する

ファイヤウォールで機能するようにコンピュータをセットアップしたら、デバイスが正しく通信できるようにネットワークをリセットする必要があります。ファイヤウォールに接続されているコンピュータを再起動します。

TCP/IP ネットワーキングに対して全てのコンピュータを設定し再起動した後、MR814v2 ルータのローカルネットワークにそれらのコンピュータを接続したら、ファイヤウォールにアクセスし設定することができます。

付録 D
ワイヤレスネットワーキングベーシック

本章では、ワイヤレスネットワーキングの概要を提供します。

ワイヤレスネットワーキングの概要

MR814v2 ルータはワイヤレス LAN(WLAN) に対する、米電気電子技術者協会（IEEE）802.11b の規格に準拠しています。802.11b ワイヤレスリンク上で、データは直接シーケンススペクトラム拡散方式 (DSSS) テクノロジを使用して、2.5GHz で無許可の無線周波スペクトルに送信されます。ワイヤレスリンクに対する最大のデータ転送速度は 11 Mbps ですが、無線信号が弱いときや電波障害が検出されるときは、11 Mbps から 5.5、2、1 Mbps に自動的に速度を落とします。

802.11b 規格は、802.11b デバイス間の業界標準のグループプログラミング相互運用である、ワイヤレスイーサネット製品互換性推進協議会 (WECA,*http://www.wi-fi.net* をご覧ください) によるワイヤレスイーサネットまたは Wi-Fi とも呼ばれています。802.11b 規格は、ワイヤレスネットワーク - アドホックとインフラストラクチャを設定するための 2 つの方式を提供します。

インフラモード

ワイヤレスアクセスポイントを使えば、インフラモードでワイヤレス LAN を操作することができます。このモードは、固定範囲内のまたは受信地域内の複数のワイヤレスネットワークデバイスに対してワイヤレス接続性を提供し、アンテナを介してワイヤレスノードと相互に作用します。

インフラモードで、ワイヤレスアクセスポイントはエアウェーブデータを有線イーサネットデータに変換し、有線 LAN とワイヤレスクライアント間のブリッジとして機能します。有線イーサネットバックボーンを介して複数のアクセスポイントを接続すると、ワイヤレスネットワーク範囲をさらに広げることができます。モバイルコンピューティングデバイスが 1 つのアクセスポイントの範囲から移動すると、他のアクセスポイントの範囲に入ります。その結果、ワイヤレスクライアントは 1 つのアクセスポイントドメインから他のアクセスポイントドメインに自由にローミングし、シームレスなネットワーク接続を保持できます。

アドホックモード（ピアツーピアワークグループ）

アドホックネットワークで、複数のコンピュータは必要に応じて 1 まとまりにされるため、ネットワークに対する構造や固定ポイントはありません。各ノードは他のノードと広く通信することができます。この設定に含まれるアクセスポイントはありません。このモードは小さなワイヤレスワークグループをすばやくセットアップし、さまざまな Windows オペレーティングシステムの Microsoft ネットワーキングによりサポートされているように、ワークグループのメンバーがデータを変換したりプリンタを共有することを可能にしています。一部のメーカーは、ピアツーピアグループネットワーキングとしてアドホックネットワーキングとも呼ばれます。

この設定で、ネットワークパケットは送受信端末によって直接送受信されます。端末がお互いの範囲内にいる間、この設定はワイヤレスネットワークをセットアップするもっとも簡単で費用のかからない方法です。

ネットワーク名。拡張サービスセット識別子 (ESSID)

拡張サービスセット識別子 (ESSID) は、サービスセット識別子 (SSID) の 2 つのタイプの 1 つです。アクセスポイントがないアドホックワイヤレスネットワークでは、ベーシックサービスセット識別子 (BSSID) が使用されます。アクセスポイントを含むインフラワイヤレスネットワークで、ESSID が使用されますが、SSID として参照することもできます。

SSID は、ワイヤレス構内通信網（LAN）の名前を識別する 32 文字の（最大）英数字キーです。ベンダーの中には、SSID をネットワーク名と呼ぶところもあります。互いに通信するネットワークのワイヤレスデバイスの場合、全てのデバイスは同じ SSID を使って構成する必要があります。

認証と WEP

ノード間で物理接続がないと、ワイヤレスリンクが盗聴や情報盗難にあいやすくなります。セキュリティのあるレベルを提供するために、IEEE 802.11 規格は 2 つのタイプの認証方式、オープンシステム、共有キーを定義しています。オープンシステム認証を使用すると、ワイヤレス PC は全てのネットワークを結合して暗号化されていない全てのメッセージを受信できます。共有キー認証を使用すると、正しい認証キーを所有するこれらの PC のみがネットワークに参加することができます。デフォルトで、IEEE 802.11 ワイヤレスデバイスはオープンシステムネットワークで作動します。

有線同等プライバシ (WEP) データ暗号化は、ワイヤレスデバイスが共有キー認証モードで動作するように設定されます。市販されているほとんどの製品には、2 つの共有キー方式（64 ビットおよび 128 ビット WEP データ暗号化）が実装されています。

802.11b 認証

802.11b 規格は、2 つの 802.11b デバイスが通信する方法を管理する複数のサービスを定義します。次のイベントは、802.11b 端末が MR814v2 に構築されたアクセスポイントを通したイーサネットネットワークで通信する前に、発生する必要があります。

1. ワイヤレス端末の電源をオンにします。
2. 端末は、範囲内にある任意のアクセスポイントからメッセージを聞きます。
3. 端末は、SSID に一致するアクセスポイントからメッセージを見つけます。
4. 端末は、アクセスポイントに認証要求を送信します。
5. アクセスポイントは端末を認証します。
6. 端末は、アクセスポイントに関連要求を送信します。
7. アクセスポイントは端末と関連しています。
8. 端末は、アクセスポイントを通してイーサネットネットワークと通信を行えるようになりました。

アクセスポイントは、端末がアクセスポイントに関連付けられる前にまたはネットワークと通信する前に、端末を認証する必要があります。IEEE 802.11b 規格は、次の 2 つのタイプの認証を定義します。オープンシステムと共有キー。

- オープンシステム認証により、デバイス SSID がアクセスポイント SSID に一致するとすれば、デバイスはネットワークを接続することができます。また、デバイスは鄭 NYî SSID オプションを使用して、その SSID には関わりなく、範囲内の利用できるアクセスポイントと関連付けることができます。
- 共有キー認証は、その端末とアクセスポイントが同じ WEP キーを使用して認証することを要求します。これらの 2 つの認証手順を、下で説明します。

オープンシステム認証

次のステップは、2 つのデバイスがオープンシステム認証を使用するときに発生します。

1. 端末は、アクセスポイントに認証要求を送信します。
2. アクセスポイントは端末を認証します。
3. 端末は、アクセスポイントに関連付けてネットワークに参加します。

このプロセスを、下で説明します。

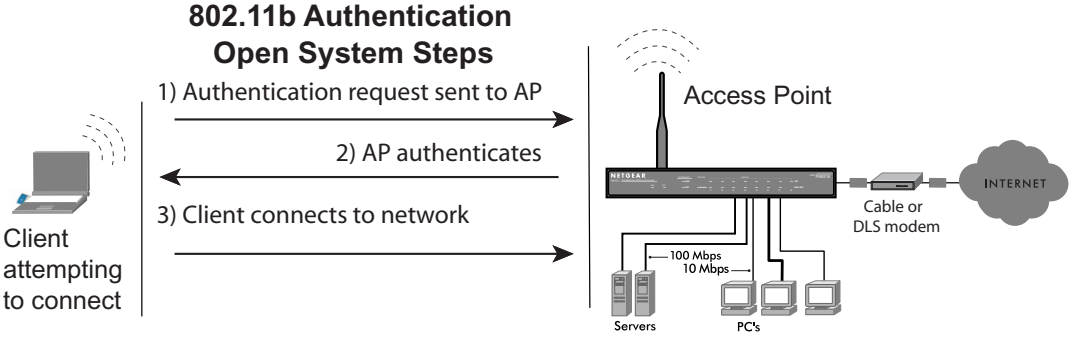


図 7-4 802.11b はシステム認証を開きます。

共有キー認証

次のステップは、2 つのデバイスが共有キー認証を使用するときに発生します。

1. 端末は、アクセスポイントに認証要求を送信します。
2. アクセスポイントは、チャレンジテキストを送信します。
3. 端末は設定済み 64 ビットまたは 128 ビットのデフォルトキーを使用してチャレンジテキストを暗号化し、暗号化されたテキストをアクセスポイントに送信します。
4. アクセスポイントは、端末のデフォルトキーに対応する設定済み WEP キーを使用して、暗号化されたテキストを復号化します。アクセスポイントは、オリジナルのチャレンジテキストと暗号化されたテキストを比較します。暗号化されたテキストがオリジナルのチャレンジテキストに一致する場合、アクセスポイントと端末は同じ WEP キーを共有し、アクセスポイントは端末を認証します。

5. 端末はネットワークに接続します。

暗号化されたテキストがオリジナルのチャレンジテキストに一致しない場合（つまり、アクセスポイントと端末が同じ WEP キーを共有しない場合）、アクセスポイントは端末の認証を拒絶し、端末は 802.11b ネットワークまたはイーサネットネットワークと通信することができません。

このプロセスを、下で説明します。

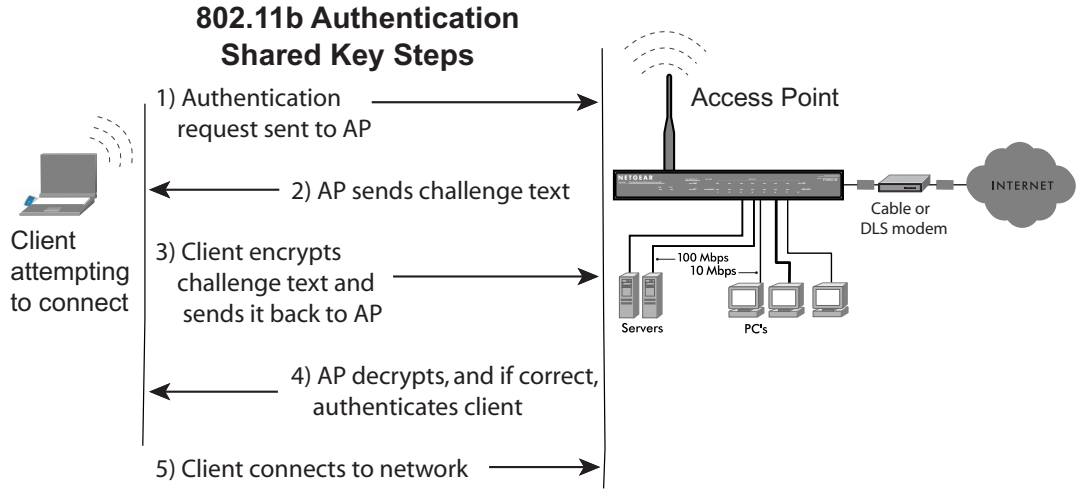


図 7-5 802.11b 共有キー認証

WEP パラメータの概要

802.11b ネットワーク上で WEP を有効にする前に、どのタイプの暗号化を要求しどのキーサイズを使用するかをまず考慮する必要があります。通常、802.11b 製品に対しては 3 つの WEP 暗号化オプションを利用できます。

1. **WEP を使用しない**：802.11b ネットワークはデータを暗号化しません。認証目的のために、ネットワークはオープンシステム認証を使用します。

2. **暗号化に対して WEP を使用する**：送信される 802.11b デバイスは、設定済み WEP キーを使用して、送信する全てのパケットのデータ部分を暗号化します。受信する 802.11b デバイスは、同じ WEP キーを使用してデータを復号化します。認証目的のために、802.11b ネットワークはオープンシステム認証を使用します。

3. **認証と暗号化に対して WEP を使用する**：送信される 802.11b デバイスは、設定済み WEP キーを使用して、送信する全てのパケットのデータ部分を暗号化します。受信する 802.11b デバイスは、同じ WEP キーを使用してデータを復号化します。認証目的のために、802.11b ネットワークは共有キー認証を使用します。

注：一部の 802.11b アクセスポイントは**認証用のみに WEP を使用**（データを暗号化せずに共有キー認証）をサポートします

キーサイズ

IEEE 802.11b 規格は、次の 2 つのタイプの WEP 暗号化をサポートします。40 ビットと 128 ビット

64 ビット WEP データ暗号化方式では、5 文字（40 ビット）入力が可能です。さらに、24 の出荷時設定ビットを 40 ビットの入力に追加すると、64 ビットの暗号化キーを生成します。（24 の出荷時設定ビットはユーザー設定できません）。この暗号化キーは、ワイヤレスインターフェイスを介して送信される全てのデータを暗号化 / 複合化するために使用されます。暗号化キーのユーザー設定可能な部分が 40 ビット幅であるため、ベンダーの中には 64 ビットの WEP データ暗号化を 40 ビット WEP データ暗号化として呼ぶところもあります。

128 ビットの WEP データ暗号化方式は、104 のユーザー設定可能ビットから構成されています。40 ビットの WEP データ暗号化方式と同様、残りの 24 ビットは出荷時設定されており、ユーザーの側で設定することはできません。一部のベンダーは、パスフレーズを秘密の 16 進数文字の変わりに入力して暗号化キー入力を簡単にしています。

128 ビット暗号化は 40 ビット暗号化より協力ですが、128 ビット暗号化は米国輸出規制により米国以外では利用できない場合もあります。

40 ビット暗号化向けに設定されているとき、802.11b 製品は一般的に 4 つの WEP キーまでサポートします。それぞれの 40 ビット WEP キーは、5 セットからなる 2 桁の 16 進数字（0-9 と A-F）として表現されます。例えば、「12 34 56 78 90」は 40 ビットの WEP キーです。

128 ビット暗号化に対して設定されているとき、802.11b 製品は一般的に 4 つの WEP キーをサポートしますが、い恥部のメーカーは 1 つの 128 ビットキーのみをサポートします。128 ビット WEP キーは、13 セットからなる 2 桁の 16 進数字（0-9 と A-F）として表現されます。例えば、「12 34 56 78 90 AB CD EF 12 34 56 78 90」は 128 ビット WEP キーです。

注：一般的に、802.11b アクセスポイントは最大 4 つの 128 ビット WEP キーを格納できますが、一部の 802.11b クライアントアダプタは 1 つしか格納できません。従って、お使いの 802.11b アクセスとクライアントアダプタ設定が一致することを確認してください。

WEP 設定オプション

WEP 設定は、SSID によって確認されたものと同じワイヤレスネットワーク内にある全ての 802.11b デバイスに一致する必要があります。一般的に、モバイルクライアントがアクセスポイント間でローミングする場合、ネットワークの全ての 802.11b アクセスポイントと全ての 802.11b クライアントアダプタは、同じ WEP 設定になっている必要があります。

注：AP にどのキーを入力しようとも、同じ順序のクライアントアダプタに対して同じキーを入力する必要もあります。言い換えると、AP の WEP キー 1 はクライアントアダプタの WEP キー 1 に一致し、AP の WEP キー 2 はクライアントアダプタの WEP キー 2 に一致する必要があります。

注：AP とクライアントアダプタは、キーが同じ順序になっている限り異なるデフォルトの WEP キーを持つことができます。言い換えると、AP はそのデフォルトキーとして WEP2 キーを使用して送信し、一方クライアントアダプタは WEP キー 3 をそのデフォルトキーとして使用して送信を行います。2 つのデバイスは、AP の WEP キー 2 がクライアントの WEP キー 2 と同じで、また AP の WEP キー 3 がクライアントの WEP キー 3 と同じである限り、通信を行います。

ワイヤレスチャネル

802.11 ワイヤレスノードは 2.4 GHz and 2.5 GHz の間の ISM（工業・化学・医療用）バンドの無線周波数を使用して互いに通信を行います。隣接するチャネルは 5 MHz 離れています。ただし、信号のスペクトラム拡散効果により、特定のチャネルを使用して信号を送信するノードは中心チャネル周波数より 12.5 MHz 上のまたは下の周波数スペクトルを利用します。その結果、同じ範囲内にある隣接チャネル（例えば、チャネル 1 とチャネル 2）を使用する 2 つの異なるワイヤレスネットワークは、互いに干渉することになります。最大のチャネル分離を許可する 2 つのチャネルを適用すると、チャネルのクロストークの量が減少し、最小のチャネル分離でネットワークに顕著なパフォーマンスの向上を提供します。

使用される無線周波数チャネルは、表 7-1 に一覧表示されています。

表 7-1. 802.11 無線周波数チャネル

チャネル	中心周波数	周波数拡散
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz -2429.5 MHz
3	2422 MHz	2409.5 MHz -2434.5 MHz
4	2427 MHz	2414.5 MHz -2439.5 MHz
5	2432 MHz	2419.5 MHz -2444.5 MHz
6	2437 MHz	2424.5 MHz -2449.5 MHz
7	2442 MHz	2429.5 MHz -2454.5 MHz
8	2447 MHz	2434.5 MHz -2459.5 MHz
9	2452 MHz	2439.5 MHz -2464.5 MHz
10	2457 MHz	2444.5 MHz -2469.5 MHz
11	2462 MHz	2449.5 MHz -2474.5 MHz
12	2467 MHz	2454.5 MHz -2479.5 MHz
13	2472 MHz	2459.5 MHz -2484.5 MHz

注：さまざまな国のワイヤレス製品でサポートされる利用可能なチャネルは異なっています。

近接するワイヤレスネットワークのチャネル間で優先されるチャネル分離は、25 MHz（5 チャネル）です。これは、ワイヤレスネットワーク内では最大 3 つの異なるチャネルを適用できることを意味します。米国では、使用可能なワイヤレスチャネルは 11 しかありません。まずチャネル 1 から始め、必要に応じてチャネル 6、そして 11 へと増やしていくことをお勧めします。これらの 3 つのチャネルは重なり合いません。

用語解説

10BASE-T	ツイストペア配線を介した 10 Mbps イーサネット用の IEEE 802.3 仕様
100BASE-Tx	ツイストペア配線を介した 100 Mbps イーサネット用の IEEE 802.3 仕様
802.11b	直接シーケンススペクトラム拡散 (DSSS) テクノロジを使用して 11 Mbps でワイヤレスネットワーキングを行うための、また 2.5GHz で無許可の無線周波スペクトルを操作するための IEEE 仕様。
サービス拒絶攻撃	DoS. コンピュータやネットワークが操作または通信できなくするために意図されたハッカーの攻撃。
DHCP	ダイナミックホスト設定プロトコルをご覧ください。
DNS	ドメイン名サーバーをご覧ください。
ドメイン名	インターネットのアドレスまたはアドレスのグループ用の記述名。ドメイン名は登録された団体名および .com、.edu、.uk などの定義済みトップレベル接尾辞の 1 つからなります。例えば、mail.NETGEAR.com というアドレスで、mail はサーバー名で NETGEAR.com はドメインです。
ドメイン名サーバー	ドメイン名サーバー (DNS) は（www.NETGEAR.com などの）ネットワークリソースの記述名を数値 IP アドレスに分解します。
ダイナミックホスト設定プロトコル	DHCP. 標準化された DHCP サーバーが、ネットワーク設定情報を複数の DHCP クライアントに割り当てる方法を指定するイーサネットプロトコル。割り当てられた情報には、IP アドレス、DNS アドレス、ゲートウェイ（ルータ）アドレスが含まれます。
ゲートウェイ	ローカルデバイスで、通常ローカルネットワークを他のネットワークのホストを接続するルータ。
IP	インターネットプロトコルをご覧ください。
IP アドレス	インターネットの各ホストを独自に定義する 4 バイトの数字。アドレスの範囲は、この目的のために形成された組織、Internic により割り当てられています。通常、バイトを分割するピリオドを使用したドット付き 10 進表記で記述されています（例：134.177.244.57）。

ISP	インターネットサービスプロバイダ。
インターネットプロトコル	インターネットで使用される主要な相互接続ネットワークプロトコル。伝送制御プロトコルと共に使用して TCP/IP を形成。
LAN:	構内通信網 (LAN) をご覧ください。
構内通信網 (LAN)	LAN: ビルのワンフロアなどの、限られた領域内のユーザーに提供する通信ネットワーク。LAN は、一般的に複数のパソコンや記憶装置やプリンタなどの共有ネットワークデバイスを接続します。多くのテクノロジは LAN を実装するために存在しますが、イーサネットはパソコンの接続にもっとも広く普及しています。
MAC アドレス	メディアアクセス制御アドレス。全てのイーサネットノードに割り当てられた 48 ビットの固有ハードウェアアドレス。通常、01:23:45:67:89:ab の形式で記述されます。
Mbps	毎秒のメガビット。
MTU	最大の送信単位をご覧ください。
最大の送信単位	送受信できる最大のパケットの、バイトによるサイズ。
NAT	ネットワークアドレス変換をご覧ください。
ネットマスク	どの部分の IP アドレスがネットワークアドレスを構成し、どの部分がネットワークのホストアドレスであるかを説明する数字。ドット付き 10 進表記または IP アドレスに付加される番号として 表すことができます。例えば、MSB から始まる 28 ビットマスクは 255.255.255.192 として、または IP アドレスに付加された /28 として表示できます。
ネットワークアドレス変換	複数のホストが、インターネットにアクセスするための単一の IP アドレスを共有する技術。
パケット	ネットワークを介して送信される情報のブロック。パケットは一般的に、ソースと送信先ネットワークアドレス、一部のプロトコルと長さ情報、データのブロック、チェックサムを含みます。
PPP	ポイントツーポイントプロトコルをご覧ください。
PPP オーバーイーサネット	PPPoE. PPP オーバーイーサネットは、ダイヤルアップ接続をシミュレートして、リモートホストを常時接続のインターネットに接続するためのプロトコルです。

PPTP	ポイントツーポイントトンネルプロトコル。Microsoft のネットワークプロトコルをインターネットパケットに埋め込むことにより、仮想プライベートネットワーク (VPN) を確立するための方式。
ポイントツーポイントプロトコル。	PPP. TCP/IP を使用してコンピュータがインターネットに直接接続できるようにするプロトコル。
RFC	注釈要求 インターネット用の標準プロトコルと手順を提案する、インターネットエンジニアリングタスクフォール (IETF) が発行する文書を参照してください。RFC は、www.ietf.org でご覧になれます。
RIP	ルーティング情報プロトコルをご覧ください。
ルータ	ネットワーク間でデータを転送するデバイス。IP ルータは、IP ソースと送信先アドレスに基づくデータを転送します。
ルーティング情報プロトコル	ルータがソースと送信先の間で最小の経路を決定できるように、互いの情報を周期的に変換する プロトコル。
サブネットマスク	ネットマスクをご覧ください。
UPnP	ユニバーサルプラグアンドプレイをご覧ください。
ユニバーサルプラグアンドプレイ	UPnP. ユニバーサルプラグアンドプレイフォーラムの一部で、400 以上のベンダーのネットワーク装置、ソフトウェア、周辺装置間で互換性を提供するネットワーキングアーキテクチャ。UpnP 準拠ルータは、家庭や小企業のブロードバンドユーザーに、オンラインゲーム、テレビ会議、およびその他のピアツーピアサービスに参加するためのシームレスな方法を提供します。
UTP	シールドなしツイストペア。10BASE-T と 100BASE-Tx イーサネットネットワークで使用されるケーブル。
WAN	広域ネットワーク (WAN) をご覧ください。
WEP	有線同等プライバシ。WEP は、802.11b ワイヤレスネットワーク用のデータ暗号化プロトコルです。ネットワークの全てのワイヤレスノードとアクセスポイントは、データ暗号化用に、64 ビットまたは 128 ビットの共有キーで設定されます。
広域ネットワーク	WAN. リモートで配置された構内通信網を延長または接続するために使用される長距離リンク。インターネットは大規模 WAN です。

Windows インターネットネーミングサービス

WINS. Windows インターネットネーミングサービスは、Windows ベースのコンピュータ名を IP アドレスに分解するためのサーバープロセスです。リモートネットワークが WINS サーバーを含んでいる場合、お使いの Windows PC はそのローカルホストに関する WINS サーバーから情報を収集します。これにより、PC は [ネットワークコンピュータ] を使用してそのリモートネットワークを検索することができます。

WINS.

Windows インターネットネーミングサービスをご覧ください。

索引

漢字