Cisco モデル DPC3825 8x4 DOCSIS 3.0 ワイヤレス レジデンシャル ゲートウェイ 取扱説明書

目次

ご使用になる前に

このたびは、弊社製品をご使用いただき、誠にありがとうございます。本冊子では、誤った取り扱いによる事故を未然に防ぐための安全上の注意事項、および製品輸出時と廃棄時の注意事項を説明しています。弊社製品をご使用になる前に必ず本冊子をよくお読みください。

本製品をご使用になるにあたり以下の点にご留意ください

1) この取り扱い説明書は保管しておいてください。
2) すべての警告に注意してください。
3) すべての説明に従ってください。

設置作業実施者への注意事項

本通知の作業説明は、資格のあるサービス技術者のみによって使用されることを目的としています。感電の危険を避けるため、有資格者を除いて、操作説明書に記載の保守修理以外は行わないでください。

製品の安全性確認

本製品の設置、保守または修理が完了したら、サービス技術者は安全性確認を行い、本製品が適切に動作できる状況であることを判定する必要があります。

安全上の注意

本冊子で使用している**警告・注意**表示の意味は次のようになります

警告  この表示の注意事項を守らないと、火災・感電などにより人が死亡または大けがを負う可能性がある内容を示しています。

注意  この表示の注意事項を守らないと、人がけがをしたり、物的損害が発生したりする可能性がある内容を示しています。

警告 

1. 本製品を分解したり、改造したりしないでください。
   - 火災、感電、動作不良の原因となります。修理は弊社の代理店にご相談ください。分解したり、改造した場合、保証期間内であっても有償修理となる場合があります。

2. 保守修理に関する警告
   - 感電にご注意ください。本製品のカバーを開けないでください。カバーを開けたり取り外したりすると、危険電圧が加わるおそれがあります。カバーを開けた場合、お客様の保証は無効となります。本製品には、ユーザが保守修理できる部品は含まれていません。

3. 煙が出たり、変な臭いや音がしたら、すぐにコンセントから電源プラグを抜いてください。
   - そのまま使用を続けると、火災や感電の原因となります。

4. 接続ケーブル、電源ケーブル、ACアダプタの取り扱いには注意して下さい。
   - 接続ケーブル、電源ケーブル、ACアダプタなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となります。
   - コネクタやケーブルは正しく接続してください。正しく接続されていないと、火災や感電の原因となることがあります。

5. 本製品の設置、移動は、必ずACアダプタの電源コードをACコンセントから抜いた状態で行ってください。
   - 電源コードをACコンセントに接続したまま行うと、感電や故障の原因になることがあります。

6. 電源コードの扱い方を誤ると火災、感電の原因となることがありますので、以下の注意を守ってお使いください。
   - 電源コードをACコンセントから抜くときは、必ずプラグ部分を持って抜いてください。
   - 電源コードに重いものをのせたり加熱したりしないで下さい。
   - 電源コードのプラグは、濡れた手でACコンセントに接続したり、抜いたりしないでください。
   - 近くで引火性の物質（ガソリン、シンナー、プロパンガスなど）を扱う場合、プラグをはずしたときの電気アークで引火や爆発のおそれがあります。プラグをはずす場合は引火性の物質を遠ざけてください。
   - 電源プラグからアース線が出ている場合、必ず接地してください。アースは雷から本製品を保護し、感電を防止するために必要です。

7. 風呂場や台所など水分の多いところ、水がかかる場所では、本製品は使用しないで下さい。 火災、感電、故障の原因となります。

8. 無線LAN製品に関しては以下の注意事項を守ってお使いください。
   - 使用禁止区域や使用制限区域での注意

     航空機内や病院内などの無線機器の使用を禁止、制限された区域では、その区域における規則および現場の責任者の指示に従ってください。電波が電子機器や医療機器に影響を与え、誤動作による事故の原因になります。
   - ペースメーカー等の医療機器を装着されている方への注意

     心臓ペースメーカー等の医療機器を装着されている方は、本製品を装着部から十分離して使用してください。電波によりペースメーカー等が誤作動するなど影響を受けるおそれがあります

9. AC主電源の過負荷を防止して下さい。
   - 感電および火災にご注意ください。AC主電源、ACコンセント、延長コード、または一体型コンセントが過負荷にならないようにしてください。製品をバッテリーその他の電源で動作させる必要がある場合は、その製品の取り扱い説明書を参照してください。

10. 電源に関して以下の注意をお守りください。
    - 本製品に適した電源が本製品のラベルに記載されています。製品を扱う場合は、製品ラベルで指定された電圧と周波数の電気コンセントのみを使用してください。自宅または会社の電源タイプが不明な場合は、ケーブルテレビ局または現地の電力会社にご相談ください。
    - 機器背面のACアダプタ接続口およびACコンセントは、常に手が届いてオペレーション使用可能な状態にしておいてください。

11. 清掃には乾いた布のみを使用してください。

12. 通気孔をふさがないでください。本取扱説明書の注意書きに従って設置してください。

13. ラジエータ、暖房装置の送風口、調理用コンロ、アンプなど、熱を発する機器の近くには設置しないでください。
14. 電源コードを保護して下さい。人に踏まれたり、特にプラグ、コンセント、コードが機器に接続されている部分が挟まれたりしないようにしてください。
15. メーカー指定の付属品/アクセサリ以外は使用しないでください。
16. カート、スタンド、三脚、ブラケット、テーブルはメーカー指定のもの、または本製品と併せて購入したものだけを使用してください。本製品をカートに載せて移動する際は、転倒によるケガに十分ご注意ください。
17. 雷の発生時や長期間使用しない場合は、本製品のACアダプタをACコンセントから抜いてください。
18. 本製品を分解したり、改造したりしないでください。
    - 火災、感電、動作不良の原因となります。修理は弊社の代理店にご相談ください。分解したり、改造した場合、保証期間内であっても有償修理となる場合があります。
    - すべての保守修理は資格を持ったサービス担当者に依頼してください。電源コードやプラグが損傷した、水が浸入した、異物が製品内に落下した、製品が雨や湿気にさらされた、正常に動作しない、本製品を落としたなど、本製品が何らかの形で損傷した場合は、保守修理が必要です。
19. 雷から製品を保護して下さい。
    - 雷が鳴りだしたら本機やケーブルには触れないでください。感電の原因になります。
    - 落雷の恐れがある時は、本製品のコンセントから ACアダプタを取り外すだけでなく、回線ケーブルを抜いてご使用をお控え下さい。雷によって、本製品の故障、火災、感電の恐れがあります。
    - その場合、物的・人的被害について、当社は責任を負いかねますので予めご了承ください。
20. オン/オフ電源ライトの確認をして下さい。
    - オン/オフ電源ライトが点灯していなくても、製品はまだコンセントに接続されている可能性があります。ACアダプタの電源コードをお確かめください。

21. 空調の整備と設置場所の選択をお願いします。
    - 製品への通電前に、包装材をすべて取り除いてください。
    - 本製品をベッド、ソファー、じゅうたんなどの上には設置しないでください。
    - 本製品を不安定な面に設置しないでください。
    - 適切な通気ができない限り、書棚やラックなど囲いのある場所に本製品を設置しないでください。
    - 本製品の上に他の電化製品（VCR や DVD など）、照明器具、書籍、水の入った花びんなどを置かないでください。
    - 通気孔をふさがないでください。

22. 湿気および異物から製品を保護して下さい。
    - 感電および火災にご注意ください。本製品を水漏れ、水はね、雨、湿気にさらさないでください。花びんなど液体の入ったものを本製品の上に置かないでください。
    - 感電および火災にご注意ください。清掃前に本製品のプラグを電源から抜いてください。液体洗剤や噴霧型洗剤は使用しないでください。製品の清掃に磁気や静電気を帯びた清掃機器（除塵機）を使用してしないでください。
    - 感電および火災にご注意ください。本製品の開口部から異物を入れないでください。異物が入ると、漏電して感電や火災を引き起こすおそれがあります。

注意 ⚠

⚠ 1. 本製品は以下のような場所では使用しないでください。故障の原因になることがあります。

- 振動や衝撃が加わる場所
- 直射日光のあたる場所
- 湿気やホコリが多い場所
- 温度差の激しい場所
- 熱を発生するもの（暖房器具など）の近く
- 強い磁力、電波が発生するもの（磁石、ディスプレイ、スピーカー、ラジオ、無線機など）の近く
- 湿気の多い場所
- 傾いた場所
- 製品に通風孔がある場合は、その通風孔がふさがる場所

⚠ 2. 無線LAN製品に関する注意（電波による干渉に関する注意）

- 本製品をコードレス電話機やテレビ、ラジオ、無線機などの近くでご使用になると電波の干渉により互いに影響を与える場合があります。

⚠ 3. 製品輸出時の注意

- 外国為替および外国貿易法（外為法）に係わる許可申請などが必要な場合がありますので、輸出される場合はご購入いただいた弊社の代理店にご相談ください。

⚠ 4. 廃棄時の注意

- 弊社製品の廃棄は、各自治体の廃棄ルールに従ってください。詳しくは各自治体にお問い合わせください。

⚠ 5. 電波障害自主規制について

- この装置は、クラス B 情報技術装置です。この装置は、家庭環境で使用する事を目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
- 取り扱い説明書に従って正しい取り扱いをして下さい。

VCCI-B

6. アンテナについて

- 製品に付属するアンテナのみをご使用ください。

はじめに

エキサイティングな高速インターネット サービスの世界にようこそ。Cisco® Model DPC3825 DOCSIS® 3.0 ワイヤレス レジデンシャル ゲートウェイは、高速データ接続を実現する業界標準ケーブル モデムです。DPC3825 レジデンシャル ゲートウェイは、データ ゲートウェイおよび有線（イーサネット）または無線ゲートウェイ機能を提供することで自宅および小規模オフィス デバイスに接続し、高速のデータ アクセスをサポートするオール イン ワン デバイスです。DPC3825 レジデンシャル ゲートウェイは、インターネットの使用、自宅やビジネスにおけるコミュニケーション、および生産性の向上をサポートします。

このガイドでは、自宅およびオフィスにおいて高速インターネットをサポートする、DPC3825 レジデンシャル ゲートウェイの設置、インストール、設定、運用、およびトラブルシューティング手順と推奨事項について説明します。本ガイドは、操作の内容別に記載されています。必要に応じて該当する章を参照してください。またこれらのサービスのお申し込みについては、ケーブルテレビ局まで直接お問い合わせください。

利点および特長

DPC3825 レジデンシャル ゲートウェイには、以下のような優れた利点および特長があります。

- 高速パフォーマンスと信頼性を実現する PacketCable™ 仕様と DOCSIS 3.0、2.0、1.x 標準への準拠
- オンライン エクスペリエンスを活性化する高性能のブロードバンド インターネット接続
- 4 つの 1000/100/10BASE-T イーサネット ポートによる有線接続
- 802.11n ワイヤレス アクセス ポイント
- プッシュ ボタン スイッチによる WPS の有効化など、簡単かつセキュアなワイヤレス設定を実現する Wireless Protected Setup（WPS）
- ユーザ設定が可能なペアレンタル コントロールにより、不適切なインターネット サイトへのアクセスをブロック
- 高度なファイアウォール テクノロジーによるハッカーへの抑止および不正アクセスからの自宅ネットワークの保護
- 魅力的なコンパクト設計により、縦、横、または壁面取り付けによる柔軟な運用

- 見やすい色別のインターフェイス ポートとケーブルにより、簡単な取り付けおよび設定処理
- 一目で動作状況を確認でき、トラブルシューティングも実行できる DOCSIS-5 準拠 LED
- ケーブルテレビ局によるソフトウェアの自動アップグレード

梱包内容

ワイヤレス レジデンシャル ゲートウェイをお受け取りになったら、装置と付属品に欠品がないこと、および製品に損傷がないことを確認してください。製品パッケージには以下のアイテムが梱包されています。

DPC3825 レジデンシャル ゲートウェイ

デスクトップ用の電源 AC アダプタ 1 個

イーサネット ケーブル（CAT5/RJ-45）1 本

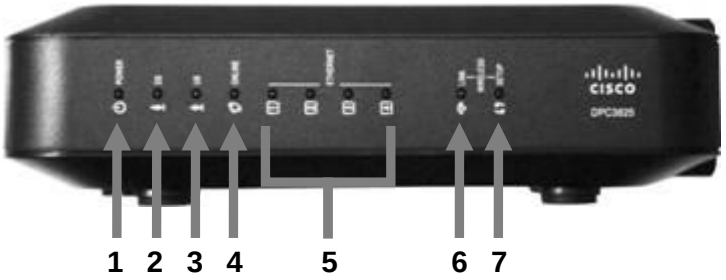
CD-ROM 1 枚

以上のアイテムのいずれかが不足している、または損傷している場合は、ケーブルテレビ局にお問い合わせください。

注：お使いのワイヤレス レジデンシャル ゲートウェイと同じケーブルに、VCR、Digital Home Communications Terminal（DHCT）またはセットトップ コンバータ、あるいは TV を接続する場合は、別売のケーブル信号スプリッタと標準の RF 同軸ケーブルが必要になります。

前面パネルの説明

レジデンシャル ゲートウェイの前面パネルには、レジデンシャル ゲートウェイの動作の調子と状態を示す LED ステータス インジケータが配置されています。前面パネルの LED ステータス インジケータの機能については、「***前面パネルの LED ステータス インジケータの機能***」（89 ページ）を参照してください。



モデル DPC3825

1 **POWER**：点灯。ワイヤレス レジデンシャル ゲートウェイに電力が供給されています。

2 **DS**：点灯。ワイヤレス レジデンシャル ゲートウェイはケーブルネットワークからデータを受信しています。

3 **US**：点灯。ワイヤレス レジデンシャル ゲートウェイはケーブルネットワークにデータを送信しています。

4 **ONLINE**：点灯。ワイヤレス レジデンシャル ゲートウェイはネットワークに登録され、完全に動作可能な状態です。

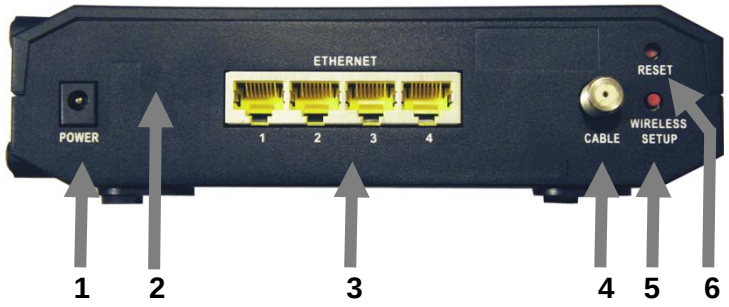
5 **ETHERNET 1 ～ 4**：点灯。デバイスはいずれかのイーサネット ポートに接続されています。点滅は、イーサネット接続を介してデータ転送されていることを示します。

6 **WIRELESS LINK**：点灯。ワイヤレス アクセス ポイントは動作可能な状態です。点滅は、データがワイヤレス接続を介して転送されていることを示します。消灯は、ワイヤレス アクセス ポイントがユーザによって無効になっていることを示します。

7 **WIRELESS SETUP**：消灯（正常な状態）。ワイヤレス設定はアクティブではありません。点滅は、ワイヤレス ネットワークにワイヤレス クライアントを追加するために、ユーザがワイヤレス設定機能をアクティブにしたことを示します。

背面パネルの説明

Cisco DPC3825 レジデンシャル ゲートウェイの背面パネルのコンポーネントの説明と機能を次の図に示します。



1 **POWER**:レジデンシャル ゲートウェイに付属の AC アダプタを接続。

> **注意:**
> **装置を損傷しないよう気をつけてください。レジデンシャル ゲートウェイ付属の電源装置のみを使用してください。**

2 **MAC アドレス ラベル**:レジデンシャル ゲートウェイの MAC アドレスを表示します。

3 **ETHERNET**:4 つの RJ-45 イーサネット ポートがお使いの PC またはホーム ネットワークに接続されます。

4 **CABLE**:F コネクタがケーブルテレビ局からのアクティブ ケーブル信号に接続されます。

5 **WIRELESS SETUP**:このスイッチを押すと、ワイヤレス設定が開始されます。この機能により、Wireless Protected Setup(WPS)準拠のワイヤレス クライアントをホーム ネットワークに接続できます。

6 **RESET**:このスイッチを 1 ～ 2 秒押すと、レジデンシャル ゲートウェイがリブートされます。10 秒以上このスイッチを押し続けると、すべての設定が工場出荷時設定にリセットされ、ゲートウェイがリブートされます。

> **注意:**
> **リセット ボタンは保守専用です。ケーブルテレビ局からの指示がない限りこのボタンは使用しないでください。これを使用すると、選択したケーブル モデムの設定が失われる可能性があります。**

インターネット サービスのシステム要件

レジデンシャル ゲートウェイが高速インターネット サービスを利用して適切に動作するためには、システム上のすべてのインターネット デバイスのハードウェアおよびソフトウェア最小要件が満たされていることを確認する必要があります。

注: 以下の最小要件のほか、有効なケーブル入力回線とインターネット接続が必要となります。

PC の最小システム要件

- Pentium MMX 133 以上のプロセッサが搭載された PC
- 32 MB の RAM
- Web 閲覧ソフトウェア
- CD-ROM ドライブ

Macintosh の最小システム要件

- MAC OS 7.5 以降
- 32 MB の RAM

イーサネット接続の最小システム要件

- Microsoft Windows 2000 オペレーティング システム（またはそれ以降）を搭載し、TCP/IP プロトコルがインストールされた PC、または TCP/IP プロトコルがインストールされた Apple Macintosh コンピュータ
- 有効な 10/100/1000BASE-T イーサネット ネットワーク インターフェイス カード（NIC）

DOCSIS レジデンシャル ゲートウェイの設置場所

レジデンシャル ゲートウェイは、コンセントおよびその他のデバイスを利用しやすいところに設置することをお勧めします。自宅またはオフィスのレイアウトを検討し、お使いのレジデンシャル ゲートウェイに最も適した場所についてケーブルテレビ局とご相談ください。またレジデンシャル ゲートウェイの設置場所を決定する前に、この取扱説明書をよくお読みください。

以下の事項を考慮してください。

- レジデンシャル ゲートウェイを高速インターネット サービスにも使用する場合は、お使いのコンピュータに近い場所をお選びください。
- RF 同軸コンセントを追加する必要がないように、既存の RF 同軸接続に近い場所をお選びください。
- クローゼットや地下室、なんらかの保護が施されたエリアなど、不測の障害や損傷を受けにくい場所をお選びください。
- ケーブルを引っ張ったり、折り曲げたりしなくても、モデムからケーブルを取り外すための十分なスペースがある場所をお選びください。
- レジデンシャル ゲートウェイ周辺の通気が遮らない場所をお選びください。
- レジデンシャル ゲートウェイを設置する前に、この取扱説明書に記載してある警告および注意事項をよくお読みください。

壁面へのモデムの取り付け方法（オプション）

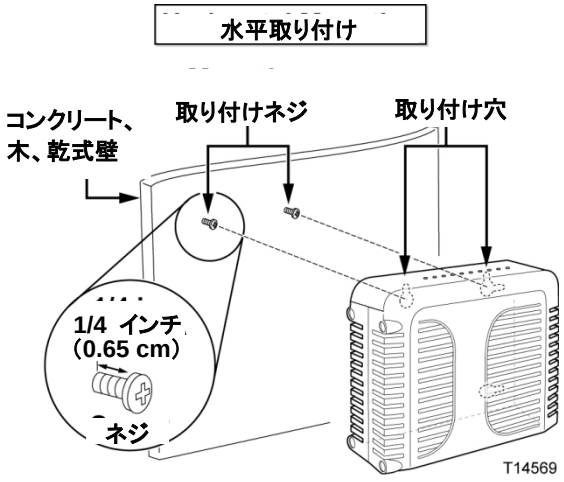
レジデンシャル ゲートウェイを壁面に取り付けるには、2 個の壁面取り付け金具、2 本のネジ、およびユニット上の取り付けスロットを使用します。このモデムは垂直または水平のいずれの方向にでも取り付けることができます。

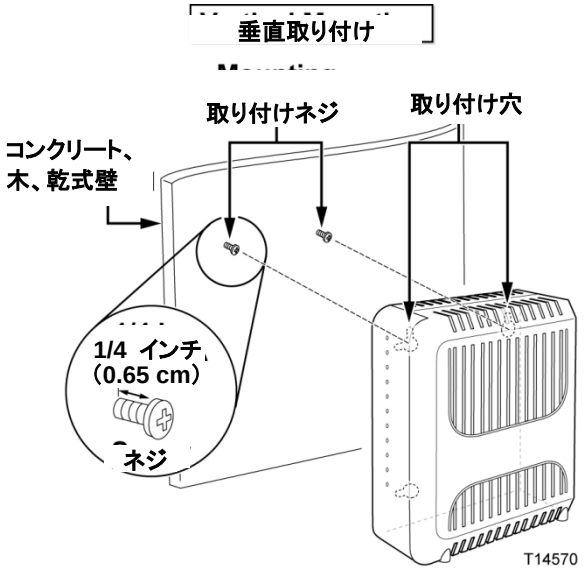
作業を開始する前に

作業を開始する前に、モデムを取り付けるための適切な場所を選択します。壁の材質は、セメント、木、乾式壁のいずれでもかまいません。取り付け場所のすべての面に異物がなく、ケーブルが無理なくレジデンシャル ゲートウェイに届くことを確認してください。レジデンシャル ゲートウェイの底部とその下の床または棚の間には、ケーブルの取り扱いができるだけの十分な空間があることを確認してください。さらに、何らかのメンテナンスが必要な場合に、ケーブルを取り外さなくてもレジデンシャル ゲートウェイを移動できるよう、すべてのケーブルに十分なゆとりを残してください。以下のアイテムがあることも確認してください。

- #8 x 1 インチ ネジ用の壁面取り付け金具 2 個
- #8 x 1 インチの板金用なベネジ 2 個
- 3/16 インチの 木工またはコンクリート用のドリルの刃（壁の材質に適しているもの）
- 次に壁面への取り付け図を示します。

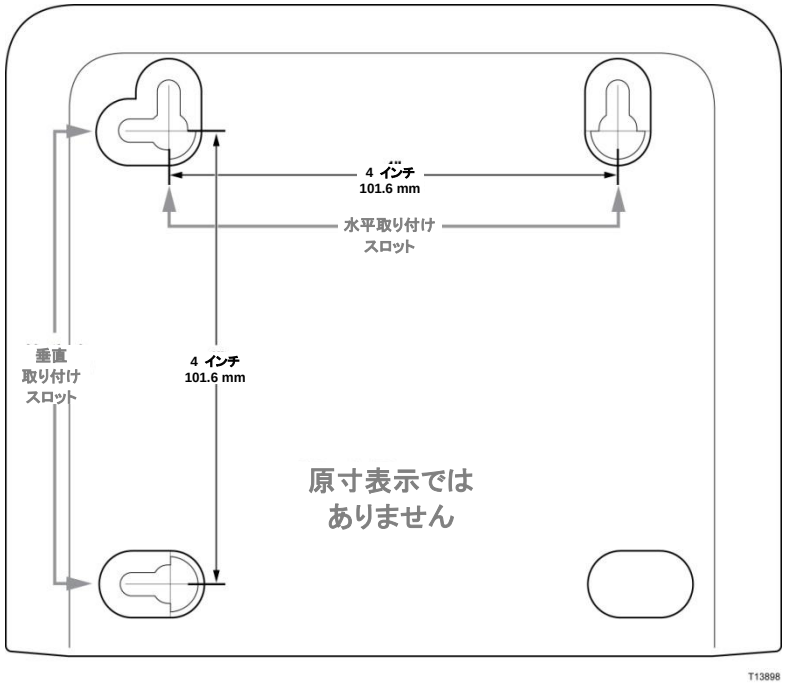
以下の図に示すいずれかの方法でモデムを取り付けます。





壁面取り付けスロットの位置と寸法

次の図は、モデムの底部にある壁面取り付けスロットの位置と寸法を示しています。このページの情報を壁面へのモデム取り付けのガイドとして使用してください。



レジデンシャル ゲートウェイの壁面への取り付け

1 3/16 インチのドリルの刃を使用して、2 つの穴を同じ高さのところに 4 インチ離して開けます。

注:前出の図は、レジデンシャル ゲートウェイ背面にある取り付け穴の位置を示しています。

2 レジデンシャル ゲートウェイを、木製の止め金具が使用できる乾式壁またはコンクリート面に取り付けますか?

- 回答が**「はい」**である場合はステップ 3 に進みます。
- **「いいえ」**である場合は、アンカー ボルトを壁に打ち込み、取り付けネジをアンカー ボルトに差し込みます。ネジ山と壁の間に約 1/4 インチのすき間を残しておきます。ステップ 4 に進みます。

3 取り付けネジを壁に差し込みます。ネジ山と壁の間に約 1/4 インチのすき間を残しておきます。ステップ 4 に進みます。

4 ケーブルまたはワイヤーがレジデンシャル ゲートウェイに接続されていないことを確認します。

5 レジデンシャル ゲートウェイを所定の位置に持ち上げます。レジデンシャル ゲートウェイの背面にある 2 つの取り付けスロットの大きい方の先端部を取り付けネジの上から滑り込ませ、キーホール スロットの狭い方の先端部がネジ軸に当たるまでレジデンシャル ゲートウェイを下方向へスライドさせます。

重要:レジデンシャル ゲートウェイが取り付けネジでしっかり支えられていることを確認してから、ユニットから手を離してください。

インターネット サービス用のゲートウェイの接続方法

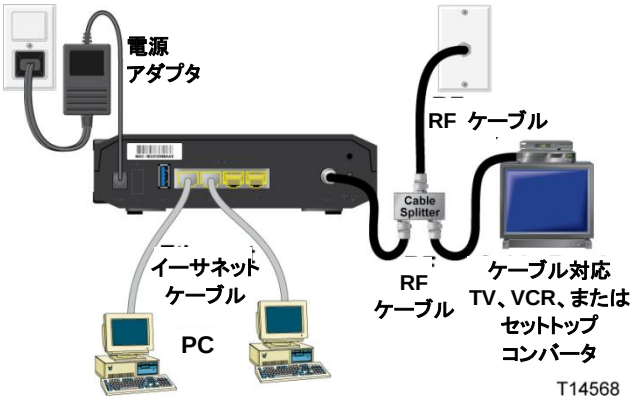
レジデンシャル ゲートウェイを使用することでインターネットにアクセスできます。また、そのインターネット接続を、自宅またはオフィスのその他のインターネット デバイスと共有できます。複数のデバイスで 1 つの接続を共有することを「ネットワーキング」といいます。

インターネット デバイスの接続と取り付け

専門家による取り付けをご利用いただける場合があります。詳しくはご契約のケーブルテレビ局までご相談ください。

デバイスの接続方法

次の図は、使用可能な各種ネットワーキング オプションのうちの一つを示しています。



高速データ サービス向けレジデンシャル ゲートウェイの接続

次の手順を使用して、レジデンシャル ゲートウェイを適切にセットアップおよび設定します。

1 レジデンシャル ゲートウェイを取り付けるための適切かつ安全な場所を選びます（高速インターネットを使用している場合は、電源、ケーブル接続、PC の近く）。

> **警告:**
> - **けがを防ぐために、記載されている取り付け順序を守ってください。**
> - **感電を防ぐために、配線および接続は適切に断熱してください。**
> - **デバイスを接続する前に、レジデンシャル ゲートウェイの電源を切断してください。**

2 お使いの PC およびその他のネットワーキング デバイスの電源をオフにしてから、それらのデバイスのプラグを電源から抜きます。

3 ケーブルテレビ局の RF 同軸ケーブルを、レジデンシャル ゲートウェイ背面の **CABLE** というラベルが貼られた同軸コネクタに接続します。

注:同じケーブル接続から TV、DHCT、セットトップ、または VCR を接続するには、ケーブル信号スプリッタ(別売)を取り付ける必要があります。スプリッタは信号品質を低下させる可能性があるため、使用する場合は必ず事前にケーブルテレビ局にご確認ください。

4 次のいずれかの方法を使用して、PC をレジデンシャル ゲートウェイに接続します。

- **イーサネット接続**:イーサネット ケーブルの一端を PC のイーサネット ポートに接続し、もう一端をレジデンシャル ゲートウェイ背面の黄色いイーサネット ポートに接続します。

  注:取り付けるイーサネット デバイスの数がレジデンシャル ゲートウェイのポート数よりも多い場合は、外部のマルチポート イーサネット スイッチを使用します。
- **ワイヤレス**:お使いのワイヤレス デバイスに電源が投入されていることを確認します。ワイヤレス ゲートウェイが動作可能になったら、ワイヤレス デバイスとワイヤレス ゲートウェイを関連付ける必要があります。ワイヤレス アクセス ポイントを関連付けるには、お使いのワイヤレス デバイスに付属の説明書に従って操作してください。

  ワイヤレス ゲートウェイの工場出荷時設定については、この取扱説明書の「***ワイヤレス設定の構成***」で説明されています。

5 レジデンシャル ゲートウェイの AC アダプタの一端をレジデンシャル ゲートウェイ背面の POWER コネクタに差し込みます。その後、AC アダプタのもう一端を AC コンセントに差し込みます。電源が入ると、レジデンシャル ゲートウェイが自動検索を実行してブロードバンド データ ネットワークの初期化をします。このプロセスは 2 ～ 5 分かかることがあります。レジデンシャル ゲートウェイの前面パネルの **POWER**、**DS**、**US**、および **ONLINE** LED の点滅が停止して点灯状態になると、モデムは使用可能です。

6 PC およびその他のネットワーク デバイスのプラグを差し込んで電源を ON にします。接続されたデバイスに対応するレジデンシャル ゲートウェイの **LINK** LED は、点灯または点滅しているはずです。

7 レジデンシャル ゲートウェイがオンラインになると、ほぼすべてのインターネット デバイスはただちにインターネットにアクセスできます。

注:お使いの PC がインターネットにアクセスできない場合は、ご契約のケーブルテレビ局までご相談ください。

DOCSIS レジデンシャル ゲートウェイの設定方法

レジデンシャル ゲートウェイを設定するには、まず WebWizard 設定ページにアクセスする必要があります。ここでは、WebWizard ページへのアクセスと、レジデンシャル ゲートウェイを正しく動作するよう設定する方法について、詳しく説明します。また、各 WebWizard 設定ページの例と説明も示します。WebWizard ページを使用すると、初期設定を使用する代わりに、レジデンシャル ゲートウェイをユーザ自身のニーズに合わせてカスタマイズできます。ここでは、[設定] ページに表示される順序で WebWizard ページについて説明します。

重要:この項に示す WebWizard ページとその例は一例にすぎません。実際のページは、このガイドで示すものとは異なる場合がありますのでご注意ください。このガイドで示すページには、デバイスの初期値が表示されています。

注:この項で説明されているネットワークの設定手順がよくわからない、または自信がないという場合は、レジデンシャル ゲートウェイの初期設定を変更する前にケーブルテレビ局までご相談ください。

ゲートウェイへの初回ログイン

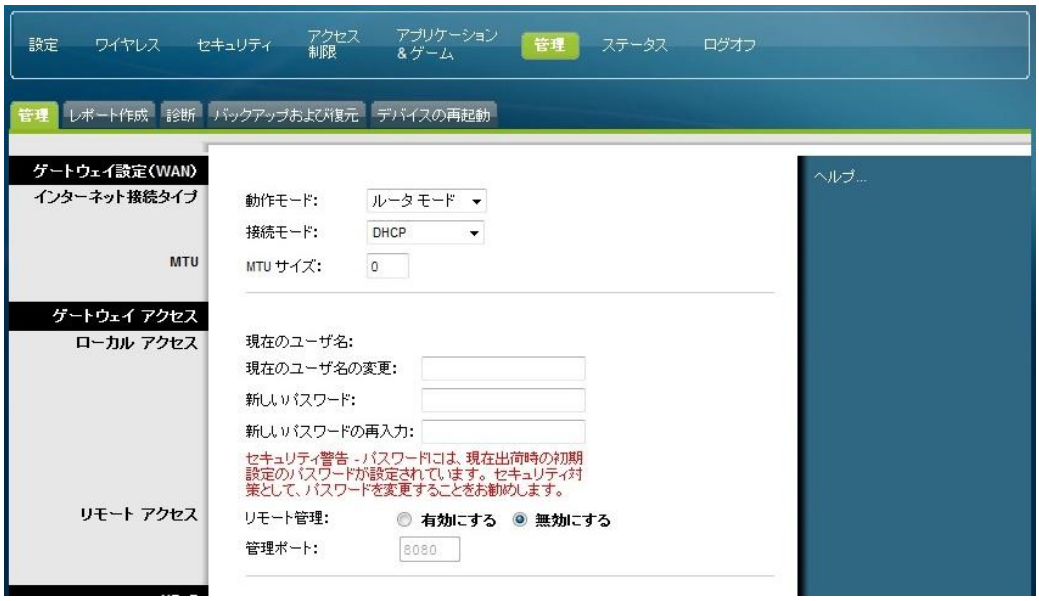
ゲートウェイの初期設定では、IP アドレス 192.168.0.1 を使用します。ゲートウェイに正しく接続しており、お使いのコンピュータが適切に設定されている場合は、次の手順を使用して管理者としてゲートウェイにログイン可能です。

1 お使いの PC で Web ブラウザを開きます。

2 アドレス フィールドに IP アドレス **192.168.0.1** を入力します。以下のページのような [ステータス] - [DOCSIS WAN] ログイン ページが開きます。

3 [ステータス] - [DOCSIS WAN] ページの [ユーザ名] および [パスワード] フィールドを空白にしたまま、[ログイン] をクリックします。ゲートウェイが開き、[管理] - [管理] ページが表示されます。[管理] - [管理] ページでは、ユーザ名とパスワードを設定できます。

重要:工場出荷時のユーザ名およびパスワードを利用したインターネット攻撃を防ぐためにも、新しいパスワードを設定することを強くお勧めします。



4 [管理] - [管理] ページでユーザ名とパスワードを作成し、[設定の保存] をクリックします。[管理] - [管理] ページでユーザ名とパスワードの設定を保存すると、[設定] - [クイック設定] ページが開きます。

重要:パスワード フィールドは空白(工場出荷時設定)のままにしておくこともできます。ただし、ユーザ名とパスワードを変更しなかった場合は、ゲートウェイにアクセスするたびに [管理] - [管理] ページへ誘導されます。これは、パスワードのカスタマイズを忘れずに行うための確認の役割があります。

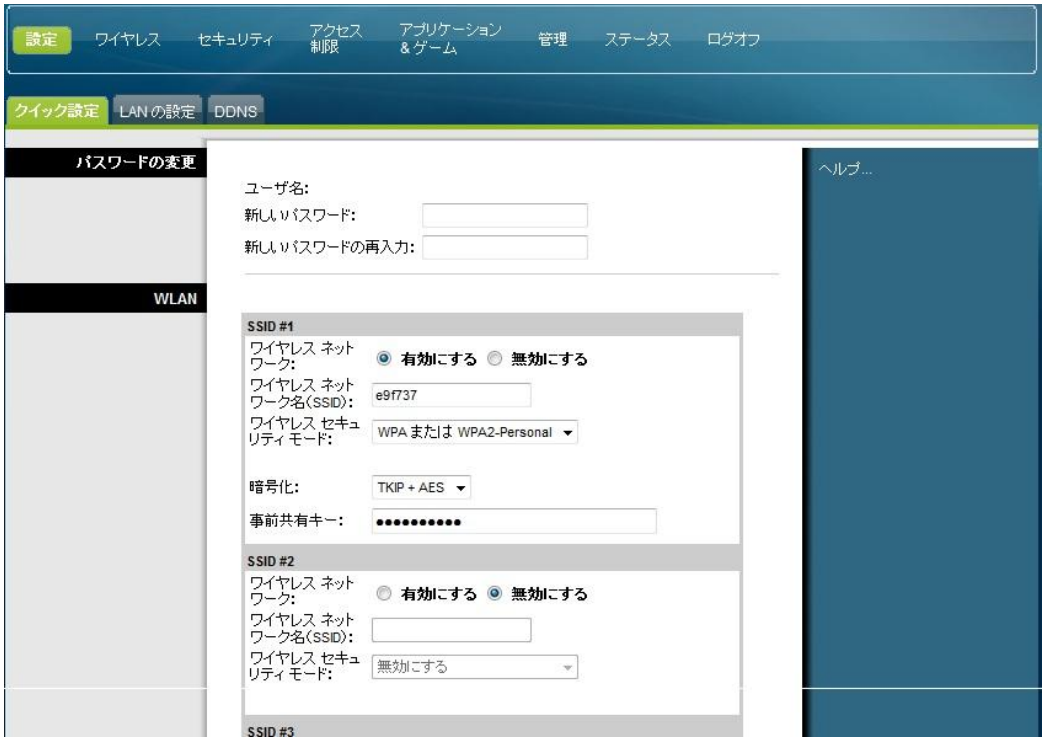
自分用のパスワードを設定した場合は、ログイン後に [設定] - [クイック設定] ページが表示されます。

5 必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

[設定] > [クイック設定]

[設定] - [クイック設定] ページは、ゲートウェイへのログオン後、最初に表示されるページです。このページを使用することにより、パスワードの変更と WLAN の設定を実行できます。

重要:このページに表示される設定は、お使いのデバイスごとに異なります。このページを選択した場合、設定内容を変更する必要は一切ありません。これらの初期設定は、すべてセキュアなワイヤレス ネットワークを運用するために必要な設定です。



クイック設定の構成

次の表の説明と手順を使用して、デバイスのネットワーク設定を構成します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[パスワードの変更]	[ユーザ名] 現在ログインしているオペレータのユーザ名が表示されます。 [新しいパスワード] パスワードを変更できます。 [新しいパスワードの再入力] 新しいパスワードを再入力します。[新しいパスワード] フィールドで入力したものと同じパスワードを入力する必要があります。

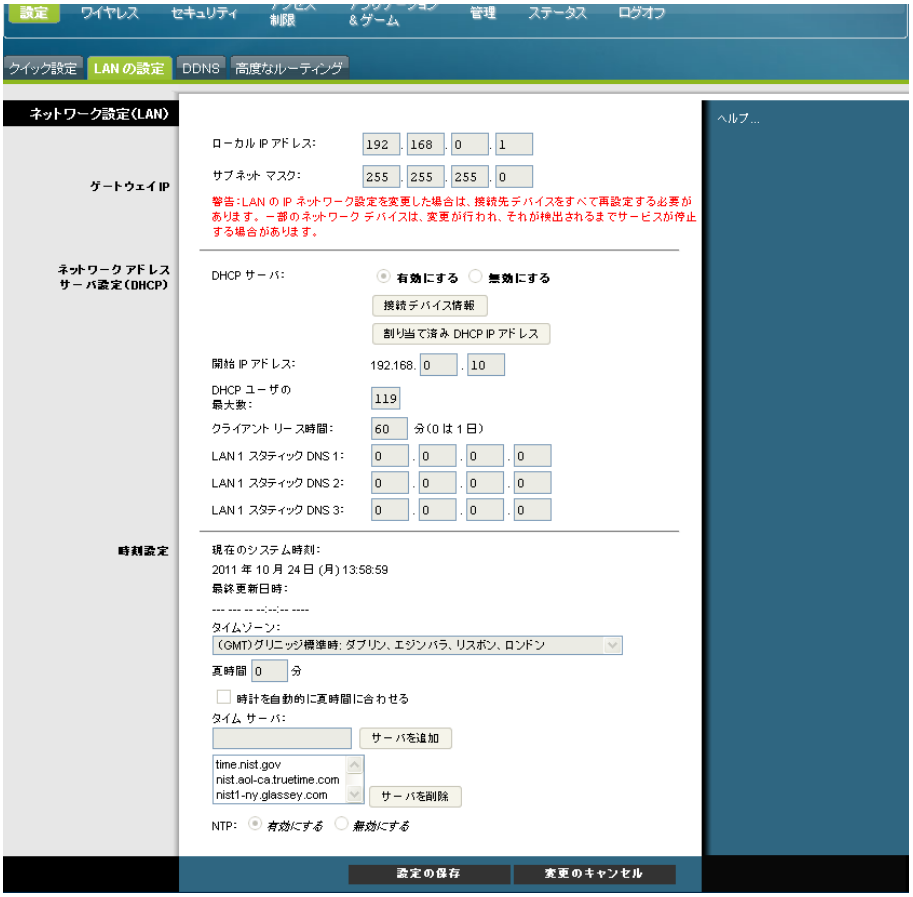
セクション	フィールドの説明
[WLAN]	[ワイヤレス ネットワーク] ワイヤレス ネットワークを有効または無効にできます。次のオプションから希望するものを選択します。 ■ [有効にする] ■ [無効にする] [ワイヤレス ネットワーク名(SSID)] ワイヤレス ネットワークの名前を入力するか、初期値を使用します。ワイヤレス ネットワーク名などの値は、PC およびその他のワイヤレス クライアント デバイスに表示されます。 **注:** Service Set Identifier(SSID)は、合計 4 つまで登録できます。工場出荷時設定の SSID は、製品ラベルに記載された CM MAC アドレスまたは SSID の末尾 6 文字です。 ケーブルテレビ局によっては、SSID 情報とワイヤレス セキュリティ情報が記載された特別のワイヤレス設定カードを提供する場合があります。 [ワイヤレス セキュリティ モード] ワイヤレス セキュリティ モードを選択することにより、ネットワークを保護できます。[無効にする] を選択すると、ワイヤレス ネットワークへの保護は行われず、範囲内のすべてのワイヤレス デバイスがそのネットワークに接続できます。ワイヤレス セキュリティ モードの詳細については、「***ワイヤレス セキュリティ***」(34 ページ)を参照してください。 **注:** 工場出荷時設定のワイヤレス セキュリティ モードは、WPA または WPA2-Personal です。 [暗号化] 選択したワイヤレス セキュリティ モードに基づいて、暗号化のレベルを選択できます。暗号化の詳細については、「***ワイヤレス セキュリティ***」(34 ページ)を参照してください。 [事前共有キー] デバイスの事前共有キーです。キーは 8 ～ 63 文字で設定できます。工場出荷時設定の事前共有キーは、お使いのゲートウェイの 9 桁のシリアル番号です。このシリアル番号は、ワイヤレス ゲートウェイに貼付された定格ラベルに記載されています。 **注:** ケーブルテレビ局によっては、ワイヤレス設定カードを提供する場合があります。このカードには、お使いのホーム ネットワークの SSID とワイヤレス セキュリティ設定に関する情報が含まれ、上記の説明とは異なる場合があります。

[設定] > [LAN の設定]

[設定] - [LAN の設定] ページでは、自宅のローカル エリア ネットワーク(LAN)を設定できます。これらの設定には、LAN そのものを定義する IP アドレスの範囲と、新規デバイスがネットワークに追加されたときにアドレスを割り当てる方法(DHCP による自動割り当てまたは手動操作)が含まれます。

重要:IP アドレスの管理に精通している場合を除き、これらの設定は変更しないことをお勧めします。これらの値を不適切に変更すると、インターネットにアクセスできなくなる場合があります。

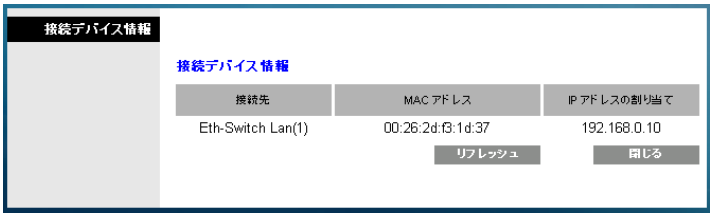
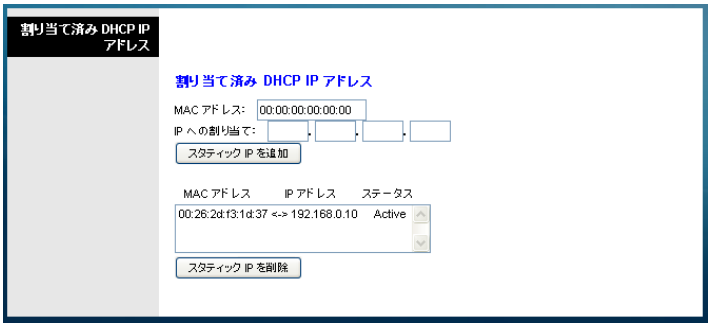
[LAN の設定] を選択し、[設定] - [LAN の設定] ページを開きます。



ネットワーク設定の構成

次の表の説明と手順を使用して、レジデンシャル ゲートウェイのネットワーク設定を構成します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[ネットワーク設定（LAN）] [ゲートウェイ IP]	[ローカル IP アドレス] プライベート ホーム LAN の基本 IP アドレスです。工場出荷時設定の LAN IP アドレスは 192.168.0.1 です。 [サブネット マスク] お使いの LAN のサブネット マスクです。

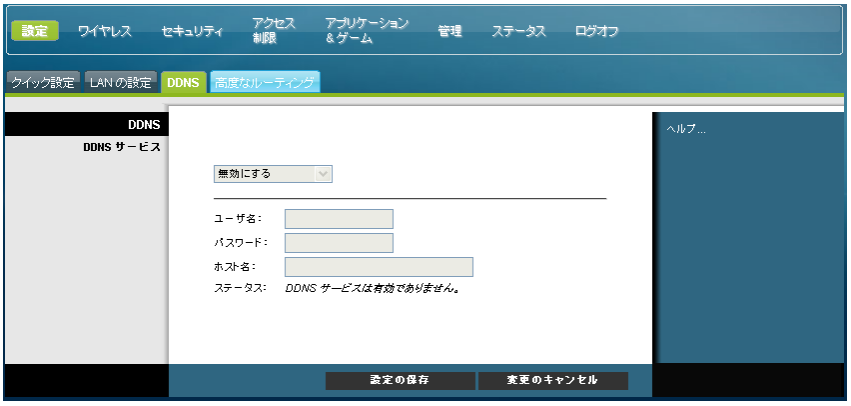
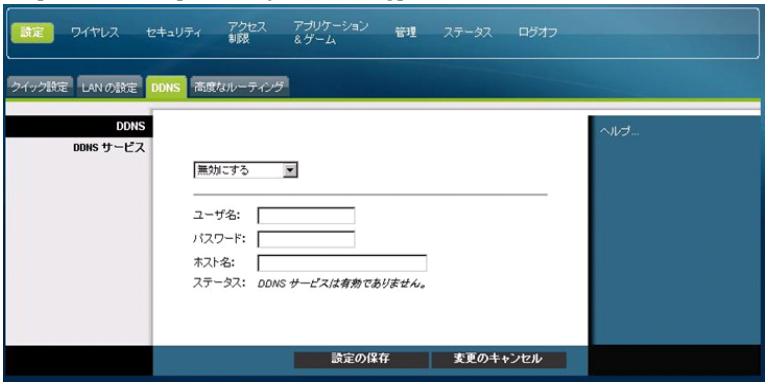
セクション	フィールドの説明
[ネットワーク アドレス サーバ設定(DHCP)]	[DHCP サーバ] レジデンシャル ゲートウェイの DHCP サーバを有効または無効にできます。DHCP サーバは、デバイスがホーム ネットワークに追加されたとき、そのデバイスに IP アドレスを自動的に割り当てるために使用されます。 ■ [接続デバイス情報] ページ [LAN の設定] ページの [接続デバイス情報] をクリックします。[接続デバイス情報] ページが開きます。このページはポップアップ ウィンドウで、レジデンシャル ゲートウェイに接続されたデバイスの MAC アドレスと IP アドレスが表示されます。  ■ [割り当て済み DHCP IP アドレス] ページ [LAN の設定] ページの [割り当て済み DHCP IP アドレス] をクリックします。[割り当て済み DHCP IP アドレス] ページが開きます。このページでは、DHCP を使用して IP アドレスが要求された場合に、特定の IP アドレスを PC またはその他のデバイスに割り当てることができます。この機能で予約されているのは、ゲートウェイの DHCP アドレス プールの範囲内にあるアドレスだけです。  **注:** – [スタティック IP を追加] ボタンを使用すると、事前に割り当てられた IP アドレスにスタティック IP アドレスが追加されます。 – [スタティック IP を削除] ボタンは、事前に割り当てられた IP アドレスからスタティック IP アドレスを削除します。 [開始 IP アドレス] 組み込みの DHCP サーバがプライベート LAN IP アドレスの配布に使用する開始アドレスが表示されます。ゲートウェイのデバイスのデフォルト IP アドレスが **192.168.0.1** であるため、開始 IP アドレスは、**192.168.0.2** 以上で、なおかつ **192.168.0.253** 未満にする必要があります。[開始 IP アドレス] の初期値は **192.168.0.10** です。

セクション	フィールドの説明
	[DHCP ユーザの最大数] DHCP サーバが LAN で使用する IP アドレスを割り当てることができる最大ユーザ数を入力します。この数は、254 から前述の開始 IP アドレスを差し引いた値までしか指定できません。 [クライアント リース時間] [クライアント リース時間] は、IP アドレスが有効である期間です。IP アドレス リースは、IP アドレスを取得するために DHCP を使用している PC などのデバイスによって自動的に更新されます。リースの期限が切れると、その IP アドレスは使用可能 IP アドレスのプールに返却され、新しいデバイスがネットワークに追加されたときに DHCP サーバが割り当てできるようになります。ゲートウェイのオンライン時の初期値は 60 分です。 [LAN1 スタティック DNS 1] [LAN1 スタティック DNS 2] [LAN1 スタティック DNS 3] DNS は、PC などのクライアント デバイスが Web サイトの URL または名前ベースのアドレスに関連付けられたパブリック IP アドレスを検出するために使用されます。これらのフィールドに DNS サーバの IP アドレスを入力することにより、自分のネットワーク内のデバイスが使用する DNS サーバを手動で指定できます。指定しない場合、このゲートウェイは、ご使用のケーブルテレビ局から DNS サーバ情報を自動的に転送します。初期値では、これらのフィールドは空白となっています。
[時刻設定]	[タイム ゾーン] システムを使用する国または地域のタイム ゾーンを選択します。その国または地域で夏時間が採用されている場合は、[時計を自動的に夏時間に合わせる] を選択します。

[設定] > [DDNS]

Dynamic Domain Name Service（DDNS）は、異なる IP アドレスを持つ可能性のあるレジデンシャル ゲートウェイに対し、ネットワーク アプリケーションから標準的な DNS クエリーで解決できるホスト名または URL を提供します。DDNS は、独自の Web サイト、FTP サーバ、またはデバイスの背後にあるその他のサーバをホストする場合に便利です。この機能を使用するには、まず DDNS サービスにサインアップする必要があります。

[DDNS] タブを選択して、[設定] - [DDNS] ページを開きます。

セクション	フィールドの説明
[DDNS サービス]	**DDNS の無効化**（工場出荷時設定） DDNS を無効化するには、ドロップダウン リストから [無効にする] を選択し、[設定の保存] を選択します。  **DDNS の有効化** **注**:DDNS 機能を使用するには、まず www.DynDNS.org でアカウントを作成し、URL を用意しておく必要があります。有効なアカウントがない場合、DDNS 機能は動作しません。 DDNS アカウントを作成するには、ご使用のブラウザを開き、そのアドレス バーに www.DynDNS.org と入力します。Web サイトの指示に従って、アカウントを作成します。 DDNS を有効にするには、次の手順に従います。 [DDNS] ページで、[www.DynDNS.org] を DDNS サーバとして選択します。  次のフィールドを設定します。 ■ [ユーザ名] ■ [パスワード] ■ [ホスト名] [設定の保存] をクリックします。これで、現在の WAN（インターネット）IP アドレスが変更されるたびに、デバイスが DDNS に対してアドレスを通知します。 **重要**:ウィンドウの [ステータス] エリアに、DDNS サービス接続のステータスが表示されます。

ワイヤレス設定の構成

ここでは、[ワイヤレス] ページから使用可能なオプションについて説明します。これらのオプションを使用することにより、WAP のパラメータをユーザのニーズと要件に合わせて設定できます。

[ワイヤレス] > [基本設定]

レジデンシャル ゲートウェイをワイヤレス通信用にセットアップすると、WAP の範囲内であれば有線接続なしで任意の場所から自由にインターネットへ接続できるようになります。[基本設定] タブを選択して、[ワイヤレス] - [基本設定] ページを開きます。

[ワイヤレス] - [基本設定] ページでは、使用するワイヤレス ネットワーク モードやその他の基本機能を選択できます。

- [ワイヤレス ネットワーク]:[有効にする] または [無効にする]
- [ワイヤレス設定]:[手動] または [Wi-Fi 保護セットアップ]
- [ネットワーク モード]
- [無線帯域]
- [チャネル幅]
- [標準チャネル]
- [ワイヤレス ネットワーク名(SSID)]

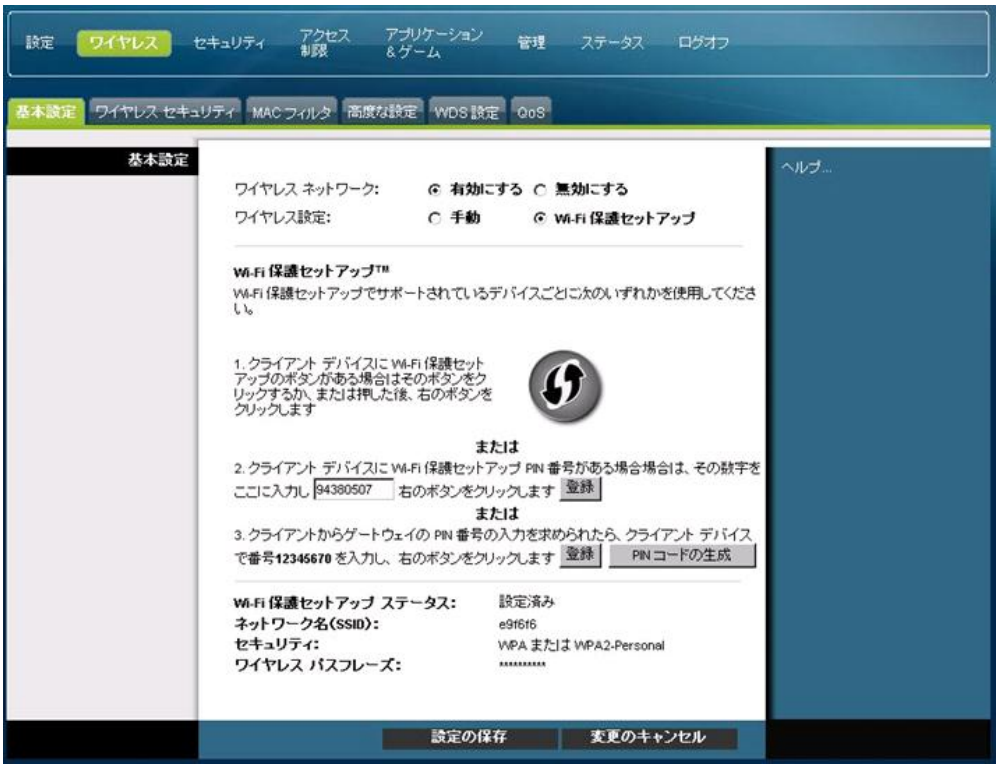
Wi-Fi 保護セットアップ(WPS)

ワイヤレス設定に Wi-Fi 保護セットアップを選択した場合、設定の多くが事前に設定されます。WPS によってセットアップが単純化され、簡単に WPA 対応デバイスをネットワークに接続できるようになります。

重要:WPS モードを使用した場合、WEP はサポートされません。WEP 暗号化を使用する必要がある場合は、[ワイヤレス設定] を [手動] に設定して WPS を無効にする必要があります。

注:WPS は初期値の設定です。

ワイヤレス設定の Wi-Fi 保護セットアップの例



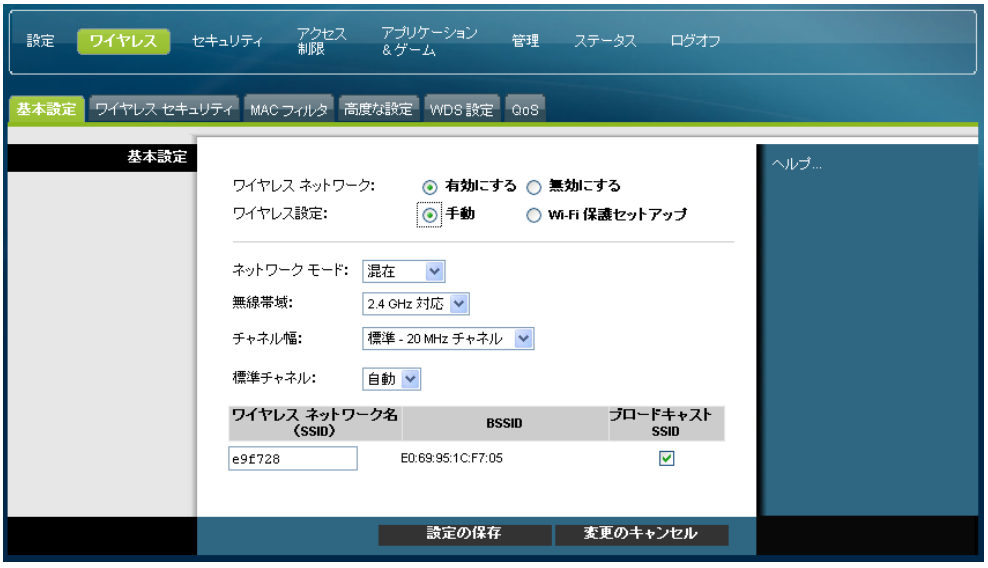
ワイヤレス設定の Wi-Fi 保護セットアップのページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイの Wi-Fi 保護セットアップの基本設定を行います。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[基本設定]	ワイヤレス ネットワークを [有効にする] または [無効にする] にします。 **Wi-Fi 保護セットアップの設定** Wi-Fi 保護セットアップ機能は、暗号化により保護されたワイヤレス ネットワークを自動的に設定します。Wi-Fi 保護セットアップを使用するには、Wi-Fi 保護セットアップをサポートする別のデバイスが同じネットワーク内に少なくとも 1 つ存在する必要があります。Wi-Fi 保護セットアップ デバイスを設定した後、他のデバイスを手動で設定できます。 **WPS プッシュ ボタンのセットアップ(オプション 1)** [ワイヤレス] - [基本設定] ページの [Wi-Fi 保護セットアップ] ボタンまたはゲートウェイの背面パネルにあるボタンを押して、ワイヤレス クライアントをゲートウェイに登録します。ゲートウェイの [Wi-Fi 保護セットアップ] ボタンを押すのと同時に、クライアント側の [Wi-Fi 保護セットアップ] ソフトウェア ボタンを押します。接続が自動的にセットアップされます。

セクション	フィールドの説明
	Wi-Fi アダプタ PIN を使用した WPS セットアップ（オプション 2） これは、ワイヤレス クライアントをゲートウェイに登録する方法として最も安全なオプションです。Wi-Fi 保護セットアップ PIN 番号を必要とします。この番号は、クライアントの Wi-Fi 保護セットアップ ユーティリティで見つかります。クライアントの Wi-Fi 保護セットアップ PIN 番号を入力した後、ゲートウェイに接続できるようになります。 **ゲートウェイ PIN を使用した WPS セットアップ（オプション 3）** [Wi-Fi 保護セットアップ] ページに表示されたゲートウェイの Wi-Fi 保護セットアップ PIN 番号をメモします。オプション 3 の [登録] ボタンをクリックします。その後、任意の Wi-Fi Protected Setup クライアントまたは Microsoft Vista を使用して、クライアント デバイスにゲートウェイの Wi-Fi 保護セットアップ PIN 番号を入力します。これで登録は完了です。

ワイヤレス設定の手動のページ例



[ワイヤレス] - [基本設定] ページの説明

次の表を使用して、レジデンシャル ゲートウェイのワイヤレス通信の基本設定を設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[基本設定]	[ワイヤレス ネットワーク] ワイヤレス ネットワークを [有効にする] または [無効にする] にします。 [ワイヤレス設定] 初期値は **WPS** です。WPS の使用方法の詳細については、「***Wi-Fi 保護セットアップ(WPS)***」(30 ページ)を参照してください。 [手動] を選択して、このオプションによるネットワークのセットアップを手動で行います。
	[ネットワーク モード] 次のオプションのいずれかをネットワーク モードとして選択します。 [G のみ]、[B/G 混在]、[混在](工場出荷時設定) **重要:**TKIP 認証のみが選択されている場合、B/G/N Mixed ネットワーク モードは使用できません。 [無線帯域] [2.4GHz 対応](工場出荷時設定)または [5GHz 対応] を選択します。 **注:**5GHz 無線帯域は、一部のモデルではサポートされていません。 [チャネル幅] [標準 - 20 MHz チャネル] または [ワイド 40 MHz チャンネル] を選択します。 [標準チャネル] ドロップダウン リストから、ご使用のネットワークに対応するチャネルを 1 つ選択します。ワイヤレス ネットワーク内のすべてのデバイスは、通信を可能にするために、同じチャネル上でブロードキャストする必要があります。自動チャネル選択の場合は、[自動](工場出荷時設定)を選択できます。

セクション	フィールドの説明
	[ワイヤレス ネットワーク（SSID）] SSID は、ワイヤレス ネットワークの名前です。ワイヤレス テクノロジーでは、使用するネットワークをエリア内の他のネットワークと区別するために SSID が使用されます。SSID には、32 文字まで使用できます。工場出荷時設定の SSID は、通常ゲートウェイの底面にある定格銘板に記載されている CM MAC アドレスの最後の 6 文字になっています。 この SSID は、一意の ID であり、意図する場合を除いて変更する必要はありません。ケーブルテレビ局によっては、異なる SSID によるワイヤレス セットアップ情報を提供することがあります。 [BSSID] ワイヤレス ネットワークの Basic Service Set Identifier（BSSID）が表示されます。BSSID は、通常ワイヤレス アクセス ポイントの MAC アドレスです。 **注**：この MAC アドレスは、工場出荷時の SSID の決定に使用される CM MAC アドレスと同じでない場合があります。 [ブロードキャスト SSID] このチェックボックスをオンにすると（工場出荷時設定）、ゲートウェイはその存在を他のワイヤレス デバイスに送信またはアドバタイズします。このビーコンが有効になっている場合、クライアント デバイスはアクセス ポイントを自動的に検出できます。 ネットワークをワイヤレス クライアントから隠す場合は、このチェックボックスをオフにします。ネットワークを隠した場合は、ワイヤレス クライアント デバイスを個別に手動で設定する必要があります。 **重要**：チェックボックスは現在使用されていないため、ゲートウェイの動作に影響を与えません。

[ワイヤレス] > [ワイヤレス セキュリティ]

ワイヤレス セキュリティ モードを選択することにより、ネットワークを保護できます。[無効にする] を選択すると、ワイヤレス ネットワークへの保護は行われず、範囲内のすべてのワイヤレス デバイスがそのネットワークに接続できます。

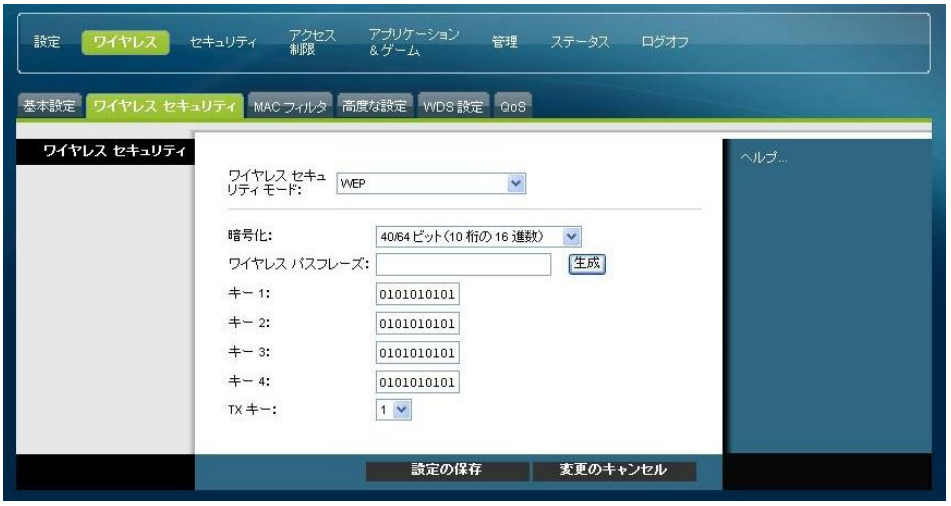
ワイヤレス ネットワークを侵入者から保護するために、[ワイヤレス セキュリティ] ページを使用して、セキュリティ モード（暗号化のレベル）、暗号キー、その他のセキュリティ設定などのセキュリティ パラメータを設定します。

[ワイヤレス セキュリティ] タブを選択して、[ワイヤレス セキュリティ] ページを開きます。次の表に、さまざまなワイヤレス セキュリティ モードを選択した [ワイヤレス セキュリティ] ページの例を示します。

[ワイヤレス セキュリティ] ページの説明

次の表を使用して、レジデンシャル ゲートウェイのワイヤレス セキュリティを設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[ワイヤレス セキュリティ]	[ワイヤレス セキュリティ モード] 次のオプションのいずれかをセキュリティ モードとして選択します。 **WEP** Wired Equivalent Privacy(WEP; 有線と同等のプライバシー)セキュリティ モードは、オリジナルの IEEE 802.11 標準に規定されています。このモードによるセキュリティ保護は脆弱であることが判明したため、その使用は推奨されなくなっています。その代わりとして、WPA-Personal または WPA2-Personal に移行することが推奨されています。



フィールドの説明

- [暗号化]:WEP 暗号化のレベルとして [40/64 ビット(10 桁の 16 進数)] または [104/128 ビット(26 桁の 16 進数)] を選択します。
- [ワイヤレス パスフレーズ]:ワイヤレス セキュリティのセットアップを完了するには、自分には覚えやすく、他人が推測しにくいワイヤレス パスフレーズを選択する必要があります。このパスフレーズは、新しいワイヤレス デバイスをこのネットワークに初めて接続する際、その接続デバイスの適切なセットアップ セクションに入力する必要があります。ネットワークのセキュリティを保護するためにも、このパスフレーズを不正なユーザに対して公開してはなりません。フレーズには、文字や数字で構成される 4 から 24 文字を指定してください。その後、[生成] をクリックして、パスフレーズを生成します。
- [キー 1]～[キー 4]:WEP キーを手動で入力する場合は、すべての所定フィールドに入力します。各 WEP キーには、A から F までの文字と 0 から 9 までの数字を指定できます。40/64 ビット暗号化の場合は 10 文字、104/128 ビット暗号化の場合は 26 文字の長さにする必要があります。

[TX キー]:Transmit(TX)キーを 1 から 4 の中から 1 つ選択します。TX キーとは、自分のデータの暗号化に使用されるキーです。4 つのキーを作成できますが、データの暗号化に使用されるのは 1 つだけです。WEP 暗号化の 4 つのキーのうちの 1 つを選択します。選択した TX キーを使用して、ワイヤレス クライアントをセットアップします。

セクション	フィールドの説明

WPA

パーソナル ネットワーク用のセキュリティ:WPA または WPA2 パーソナル モード

Wi-Fi Protected Access(WPA)は、WEP よりも安全なワイヤレス テクノロジーです。WPA は、エンタープライズ(企業アプリケーション)とパーソナル(ホーム ネットワーク)の両方のワイヤレス ネットワークに使用できます。ホーム ネットワークの場合、ご使用の PC またはワイヤレス クライアント内のワイヤレス アダプタでサポートされているモードに応じて、WPA-Personal または WPA2-Personal のいずれかをセキュリティ モードに選択することを強く推奨します。

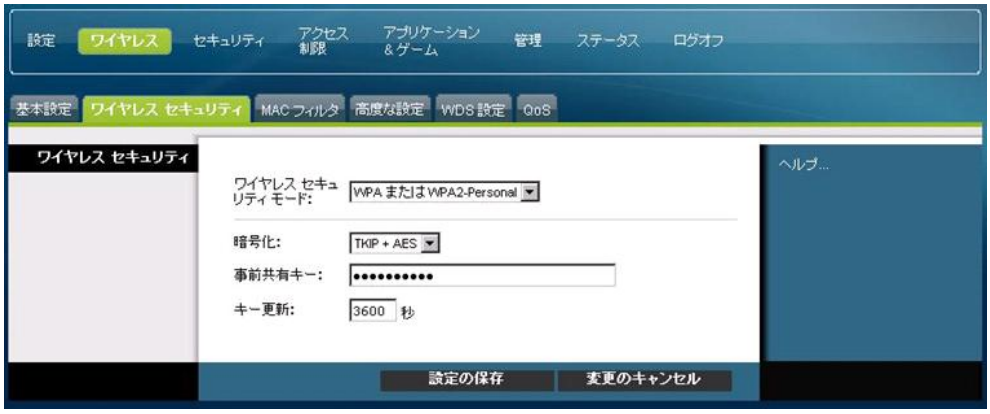
WPA-Personal(別名 WPA-Pre-Shared Key(WPA-PSK; WPA 事前共有キー))は、WEP よりも安全なワイヤレス ネットワークを提供します。WPA-Personal は、TKIP ユーザ認証、および WEP よりも強力な暗号キーを導入します。

WPA2-Personal(別名 WPA2-Pre-Shared Key(WPA2-PSK; WPA2 事前共有キー))は、最も安全な標準ベースのワイヤレス ネットワーキングを提供します。WPA2-Personal には、データ送信用に AES(Advanced Encryption Standard; 高度暗号化規格)が組み込まれています。

注:一部のワイヤレス アダプタは、WPA2 をサポートしていません。WPA は、より幅広い種類のデバイスでサポートされています。WPA と WPA2 のいずれを使用する場合でも、「強固な」パスフレーズを必ず使用してください。強固なパスフレーズとは、21 文字以上のランダムな文字列です。

次の 3 つの WPA または WPA2 パーソナル モードのうち 1 つを選択します。

- [WPA-Personal]
- [WPA2-Personal]
- [WPA または WPA2-Personal]



フィールドの説明

- [暗号化]:初期値は、[TKIP+AES] です。
- [事前共有キー]:8 から 63 文字のキーを入力します。
- [キー更新]:キーの更新期間を入力します。これにより、暗号キーを変更する頻度をデバイスに指示します。初期値は **3600** 秒です。

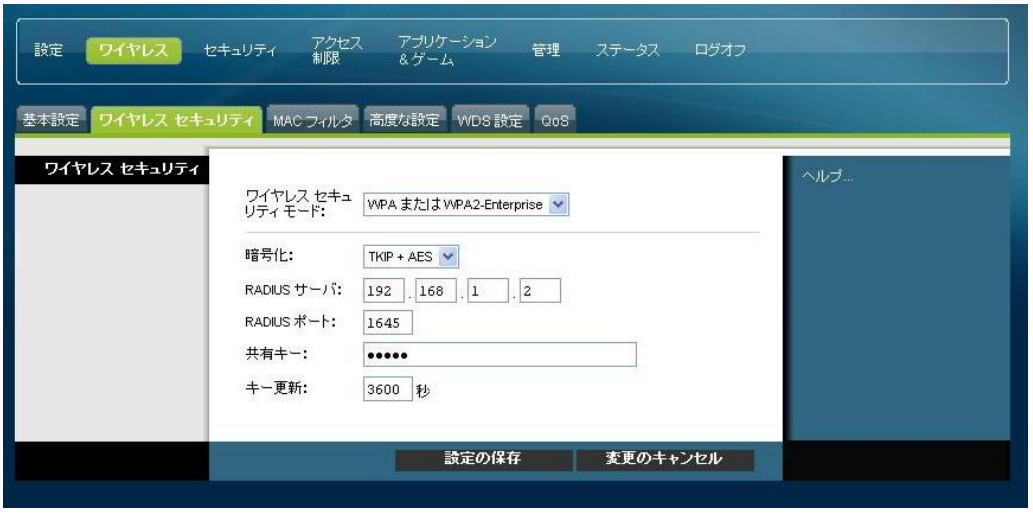
セクション	フィールドの説明

エンタープライズ ネットワーク用のセキュリティ:WPA エンタープライズ モード

このオプションでは、クライアント認証用の RADIUS サーバと連携して WPA が使用されます（使用するには、デバイスが RADIUS サーバに接続されている必要があります）。

次の 3 つの WPA または WPA2 エンタープライズ モードのうち 1 つを選択します。

- [WPA-Enterprise]
- [WPA2-Enterprise]
- [WPA または WPA2-Enterprise]



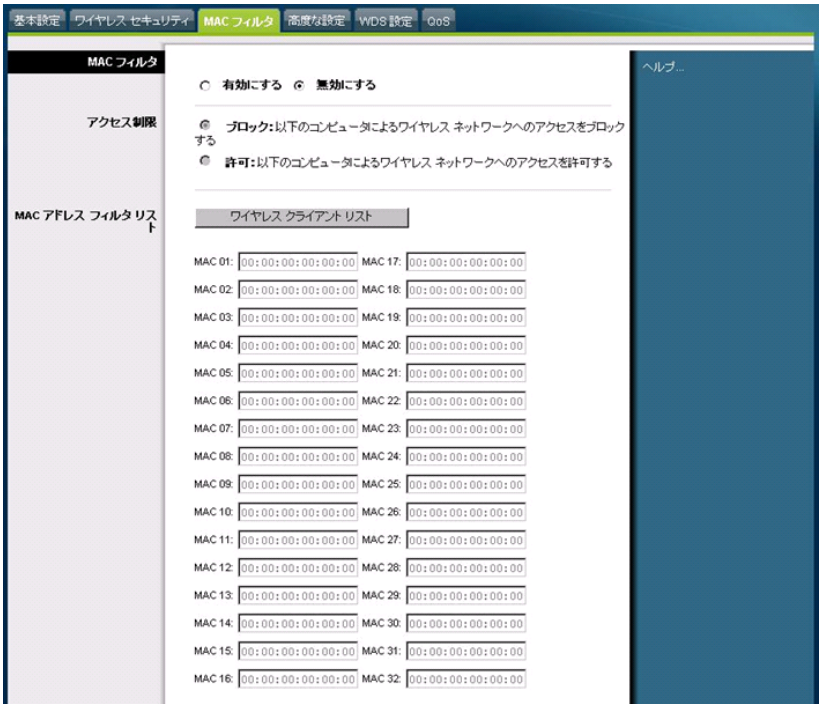
フィールドの説明

- [暗号化]:初期値は、[TKIP + AES] です。
- [RADIUS サーバ]:RADIUS サーバの IP アドレスを入力します。
- [RADIUS ポート]:RADIUS サーバによって使用されるポート番号を入力します。初期値は **1812** です。
- [共有キー]:デバイスと RADIUS サーバによって使用されるキーを入力します。
- [キー更新]:キーの更新期間を入力します。これにより、暗号キーを変更する頻度をデバイスに指示します。初期値は **3600** 秒です。

[ワイヤレス] > [MAC フィルタ]

MAC フィルタ機能は、ワイヤレス クライアント デバイスの MAC アドレスに基づいてワイヤレス LAN へのアクセスを許可またはブロックするために使用します。アクセス リストとしても知られる MAC フィルタ機能は、無認可ユーザがワイヤレス ネットワークにアクセスできないようにするために使用できます。

[MAC フィルタ] タブを選択して、[ワイヤレス] - [MAC フィルタ] ページを開きます。



[ワイヤレス] - [MAC フィルタ] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイのワイヤレス ネットワークの MAC アドレス フィルタリングを設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[MAC フィルタ]	レジデンシャル ゲートウェイの MAC フィルタリング機能を [有効にする] または [無効にする] に設定できます。

セクション	フィールドの説明
[アクセス制限]	**アクセス制限** コンピュータによるワイヤレス ネットワークへのアクセスを許可またはブロックできます。ここで選択したオプションが、同ページに表示されているアドレスに対して施行されます。次のオプションのいずれかを選択します。 ■ [ブロック：以下のコンピュータによるワイヤレス ネットワークへのアクセスをブロックする]：このオプションを選択すると、一覧に表示されているデバイスの MAC アドレスがインターネットにアクセスできなくなります（アクセス拒否）。それ以外のすべての MAC アドレスには、インターネット アクセスが許可されます。 ■ [許可：以下のコンピュータによるワイヤレス ネットワークへのアクセスを許可する]：このオプションを選択すると、一覧に表示されているデバイスの MAC アドレスがインターネットにアクセスできるようになります（アクセス許可）。表示されていない MAC アドレスはすべて、インターネット アクセスを拒否されます。
[MAC アドレス フィルタ リスト]	**MAC アドレス フィルタ リスト** [MAC アドレス フィルタ リスト] には、ワイヤレス アクセスを制御されるユーザが表示されます。[ワイヤレス クライアント リスト] をクリックして、ネットワーク ユーザのリストを MAC アドレスで表示します。[ソート条件] ドロップダウン メニューを使用すると、この一覧を IP アドレス、MAC アドレス、ステータス、インターフェイス、またはクライアント名ごとに並べ替えることができます。最新の情報を表示するには、[リフレッシュ] ボタンをクリックします。

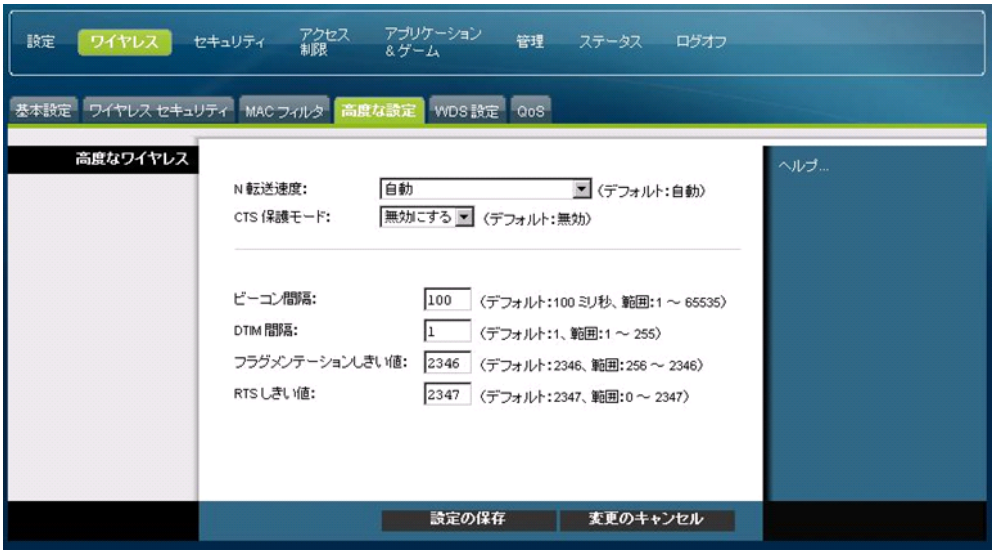
[ワイヤレス] > [高度な設定]

高度なワイヤレス設定は、レジデンシャル ゲートウェイのワイヤレス ネットワークに対してセキュリティの新たな層を追加します。このページは、高度なワイヤレス機能をセットアップするために使用します。これらの設定の調整は、熟練した管理者のみが行う必要があります。設定を誤ると、ワイヤレスのパフォーマンスが低下する可能性があります。

[高度な設定] タブを選択して、[ワイヤレス] - [高度な設定] ページを開きます。

このページを使用して、次のオプションを設定します。

- [N 転送速度]
- [CTS 保護モード]
- [ビーコン間隔]
- [DTM 間隔]
- [フラグメンテーションしきい値]
- [RTS しきい値]



[ワイヤレス] - [高度な設定] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイの高度なワイヤレス設定を行います。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

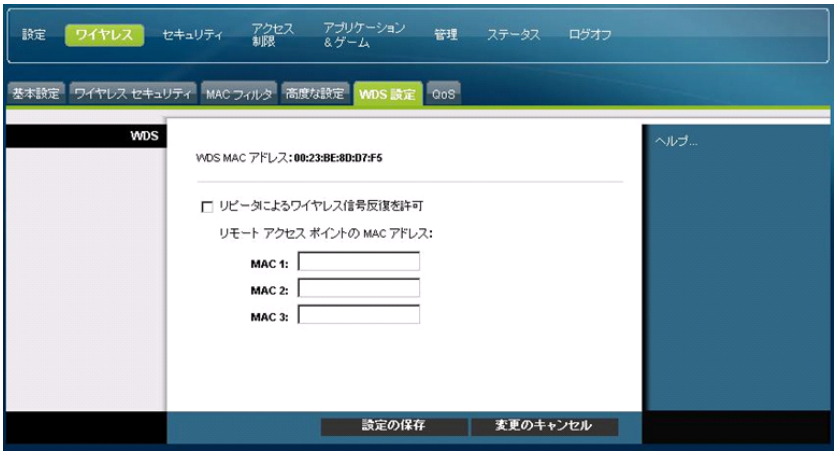
セクション	フィールドの説明
[高度なワイヤレス]	[N 転送速度] データの送信レートは、ご使用の Wireless-N ネットワーキングの速度に応じて設定する必要があります。一連の送信速度の中から選択します。または、[自動] を選択すると、デバイスは利用できる最高速のデータ レートを自動的に適用し、自動フォールバック機能が有効になります。自動フォールバックは、デバイスとワイヤレス クライアントの間で可能な限り高速の接続速度をネゴシエートします。工場出荷時設定は [自動] です。 次のオプションのいずれかを送信レートとして選択します。 ■ [自動](工場出荷時設定) ■ [従来のレートを使用] ■ [0: 6.5 または 13.5 Mbps] ■ [1: 13 または 27 Mbps] ■ [2: 19.5 または 40.5 Mbps] ■ [3: 26 または 54 Mbps] ■ [4: 39 または 81 Mbps] ■ [5: 52 または 108 Mbps] ■ [6: 58.5 または 121.5 Mbps] ■ [7: 65 または 135 Mbps] ■ [8: 13 または 27 Mbps] ■ [9: 26 または 54 Mbps] ■ [10: 39 または 81 Mbps] ■ [11: 52 または 108 Mbps] ■ [12: 78 または 162 Mbps] ■ [13: 104 または 216 Mbps] ■ [14:117 または 243 Mbps] ■ [15: 130 または 270 Mbps]
	[CTS 保護モード] CTS(Clear-To-Send)保護モードは、すべてのワイヤレス波を受信できるようデバイス能力を高めるものの、パフォーマンスを大幅に低下させる可能性があります。802.11b トラフィックの負荷が高い環境において Wireless-N/G 製品がデバイスに送信できない場合、必要に応じてこの機能を使用するように、[自動] を選択します。この機能を常に無効にする場合は、[無効にする] を選択します。
	[ビーコン間隔] ビーコン間隔の値は、ビーコンの周波数間隔を示します。ビーコンとは、デバイスがワイヤレス ネットワークを同期させるためにブロードキャストするパケットです。 (初期値:100 ミリ秒、範囲:20 ～ 1000)

セクション	フィールドの説明
	[DTIM 間隔] Delivery Traffic Indication Message（DTIM）は、ブロードキャスト/マルチキャストの間隔を示します。DTIM フィールドには、次のブロードキャスト メッセージとマルチキャスト メッセージまでのカウントダウンが表示されます。クライアントにブロードキャスト メッセージまたはマルチキャスト メッセージがバッファに存在する場合、デバイスは DTIM 間隔で次の DTIM を送信します。クライアントは、ビーコンを監視し、ブロードキャスト メッセージとマルチキャスト メッセージを受信するためにスリープ状態から復帰します。 （初期値：1、範囲：1 ～ 255）
	[フレグメンテーションしきい値] フラグメンテーションしきい値は、データが複数のパケットに分割される前のパケットの最大サイズを指定します。パケット損失が高い率で発生する場合は、フラグメンテーションしきい値を少し大きくしてください。設定するフラグメンテーションしきい値が小さすぎると、ネットワークのパフォーマンスが低下することがあります。初期値を小さくする場合は、僅差にすることをお勧めします。通常は、値を初期設定（2346）のままにしてください。
	[RTS しきい値] RTS しきい値は、RTS/CTS（送信要求/受信準備完了）メカニズムが作動するパケット サイズを決定します。データ フローが不規則である場合は、初期値（2346）を少しだけ小さくすることが推奨されます。ネットワーク パケットが事前に設定された RTS しきい値サイズよりも小さい場合は、RTS/CTS メカニズムは有効になりません。デバイスは送信要求（RTS）フレームを特定の受信ステーションに送信し、データ フレームの送信をネゴシエートします。RTS を受信すると、ワイヤレス ステーションは受信準備完了（CTS）フレームで応答し、送信開始を承認します。RTS しきい値は初期値（2347）のままにしてください。

[ワイヤレス] > [WDS 設定]

[WDS 設定] ページでは、信号リピータを導入することによりワイヤレス ネットワークのカバレッジを拡大できます。すべての WDS 対応デバイスでチャネル設定が同じであることを確認してください。

[WDS 設定] タブを選択し、[ワイヤレス] - [WDS 設定] ページを開きます。このページでは、WDS を設定します。



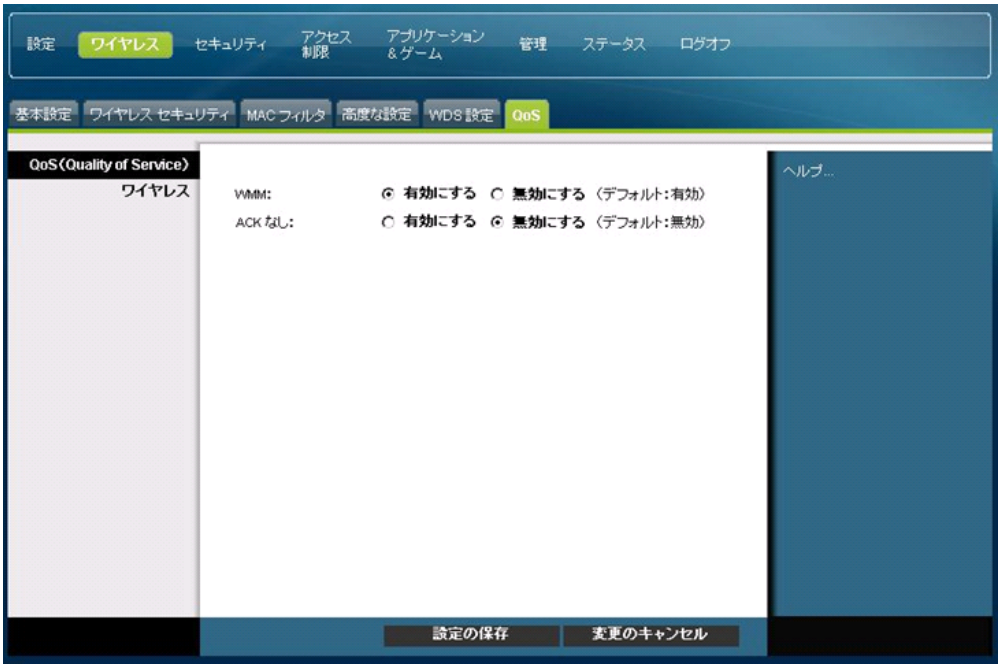
[ワイヤレス] - [WDS 設定] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイの Wireless Distribution System を設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[WDS]	[WDS MAC アドレス] ゲートウェイ アクセス ポイントの WDS MAC アドレス(または BSSID)を表示します。
	[リピータによるワイヤレス信号反復を許可] ワイヤレス クライアントがリピータに接続し、ワイヤレス クライアントとリピータ間のトラフィックをルーティングすることを許可する場合は、このチェックボックスをオンにします。最大 3 つのリピータが許可されます。
	[リモート アクセス ポイントの MAC アドレス](MAC 1 ～ 3) これら 3 つのフィールド(MAC 1、2、および 3)を使用してリピータの MAC アドレスを入力します。

[ワイヤレス] > [QoS]

Quality of Service（QoS）では、優先度が高いネットワーク トラフィック タイプに対して優れたサービスを保証するシステムです。顕著な例に、ビデオ会議など負荷の高いリアルタイムのアプリケーションが挙げられます。QoS の設定では、異なるトラフィック タイプに対して優先度を指定できます。優先度が低いトラフィックを低速にすることで、優先度が高いトラフィックのスループットを向上させたり、優先度が高いトラフィックの遅延を抑えることができます。[QoS] タブを選択し、[ワイヤレス] - [QoS] ページを開きます。



[ワイヤレス] - [QoS] ページの説明

次の表の説明と手順を使用して、QoS を設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[QoS（Quality of Service）]	[WMM]
[ワイヤレス]	Wi-Fi Multimedia（WMM）がワイヤレス クライアントでサポートされている場合にこの機能を有効にすると、マルチメディア トラフィックに対して他のトラフィックよりも高い優先度が割り当てられます。次のオプションから希望するものを選択します。 ■ [有効にする]（工場出荷時設定） ■ [無効にする]

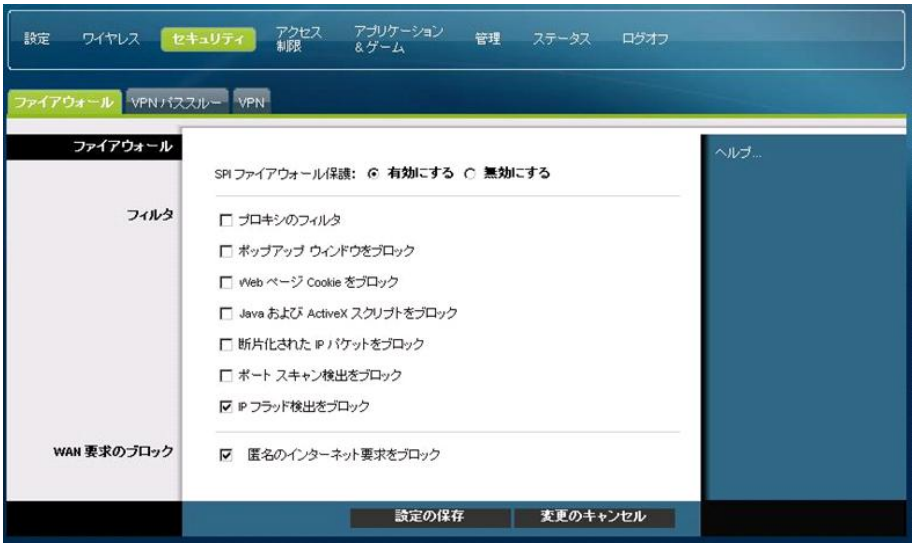
セクション	フィールドの説明
	[ACK なし] NO ACK 機能を有効または無効にできます。この機能は、伝送が重要であり、パケット損失をある程度許容できるデータ サービスに推奨されます。[無効にする] を選択すると、受信されたパケットごとに確認パケットが返信されます。これにより、伝送の信頼性は高くなりますが、トラフィックの負荷が増加し、パフォーマンスは低下します。 次のオプションから希望するものを選択します。 ■ [有効にする] ■ [無効にする]（工場出荷時設定）

セキュリティの設定

[セキュリティ] > [ファイアウォール]

高度なファイアウォール テクノロジーにより、ハッカーの攻撃を抑止し、ホーム ネットワークを不正なアクセスから守ります。このページでは、ゲートウェイのローカル ネットワークのさまざまな種類の不適切なトラフィックをフィルタリングするためのファイアウォールを設定します。

[ファイアウォール] タブを選択し、[セキュリティ] - [ファイアウォール] ページを開きます。



次の表の説明と手順を使用して、レジデンシャル ゲートウェイのファイアウォールを設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

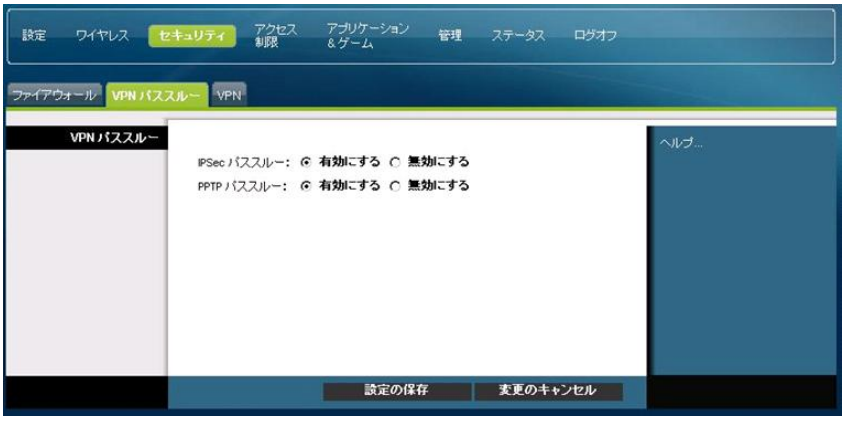
セクション	フィールドの説明
[ファイアウォール]	[SPI ファイアウォールの保護] [SPI ファイアウォールの保護] は Denial of Service（DoS; サービス拒絶）攻撃をブロックします。DoS 攻撃はデータを盗んだり、コンピュータを破壊したりするのではなく、インターネット接続を過負荷状態にし、インターネット接続を使用できなくします。 次のオプションから希望するものを選択します。 ■ [有効にする]（工場出荷時設定） ■ [無効にする]

セクション	フィールドの説明
[フィルタ]	[プロキシのフィルタ] プロキシのフィルタを有効または無効にします。ローカル ユーザが WAN プロキシ サーバにアクセスできる場合、ローカル ユーザはコンテンツ フィルタを回避し、デバイスによりブロックされたインターネット サイトにアクセスできることがあります。[プロキシのフィルタ] 機能を選択すると、すべての WAN プロキシ サーバへのアクセスがブロックされます。 [ポップアップ ウィンドウをブロック] ポップアップ ウィンドウを有効または無効にします。よく使用されるアプリケーションの中には、そのアプリケーションの一部としてポップアップ ウィンドウが実装されているものがあります。ポップアップ ウィンドウを無効にした場合、これらのアプリケーションの一部が影響を受けることがあります。 [Web ページ Cookie をブロック] クッキーのブロックを有効または無効にします。この機能により、インターネットからプライベート ローカル ネットワークのデバイスへの不正なクッキーの配信がフィルタリングされます。クッキーは、個人情報または Web 閲覧に関するデータを含むコンピュータ ファイルです。 [Java および ActiveX スクリプトをブロック] Java アプレットおよび ActiveX スクリプトを有効または無効にします。この機能を使用すると、インターネットからプライベート ネットワークのデバイスに不正に送信された迷惑な Java アプレットまたは悪意のある Java アプレットからプライベート ネットワークのデバイスを守ることができます。これらのアプレットは、PC が受信したときに自動的に実行されます。 Java は Web サイト向けのプログラミング言語です。Filter Java Applets 機能を選択すると、このプログラミング言語を使用して作成されたインターネット サイトにアクセスできないことがあります。 また、この機能を使用すると、インターネットからプライベート ネットワークのデバイスに不正に送信された迷惑な ActiveX コントロールまたは悪意のある ActiveX コントロールからプライベート ネットワークのデバイスを守ることができます。これらの ActiveX コントロールは、PC が受信したときに自動的に実行されます。 [断片化された IP パケットをブロック] 断片化された IP パケットのフィルタリングを有効または無効にします。この機能を使用すると、インターネット ベースのサービス拒絶攻撃からプライベート ローカル ネットワークを守ることができます。 [ポート スキャン検出をブロック] ゲートウェイによるインターネット ベースのポート スキャンへの応答を有効または無効にします。この機能は、ゲートウェイでオープンな IP ポートを検出することによりネットワークに不正にアクセスしようとするインターネット ベースのハッカーからプライベート ローカル ネットワークを守るよう設計されています。 [IP フラッド検出をブロック]（オン：出荷時設定） デバイスまたはネットワークに不正なブロードキャスト パケットを大量に送信しようとする悪意のあるデバイスをブロックします （「ブロードキャスト ストーム」とも呼ばれます）。

セクション	フィールドの説明
[WAN 要求のブロック]	[匿名のインターネット要求をブロック](オン:出荷時設定) ネットワークが「ping」に応答しないようにする、または他のインターネット ユーザがネットワークを検出できないようにする場合は、この機能を有効にします。また、[匿名のインターネット要求をブロック] 機能は、ネットワークのポートを隠します。このため、外部のユーザはネットワークに侵入することが困難になります。

[セキュリティ] > [VPN パススルー]

このページでは、VPN(バーチャル プライベート ネットワーク)サポートを設定します。この設定を有効にすると、ゲートウェイのファイアウォールを通過する、IPsec プロトコルまたは PPTP プロトコルを使用した VPN トンネルが許可されます。[VPN パススルー] タブを選択し、[セキュリティ] - [VPN パススルー] ページを開きます。



次の表の説明と手順を使用して、レジデンシャル ゲートウェイの VPN パススルーを設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[VPN パススルー]	[IPSec パススルー] Internet Protocol Security(IPsec; インターネット プロトコル セキュリティ)を有効または無効にします。IPsec は、IP レイヤでのパケットのセキュアな交換を実現するために使用されるプロトコル スイートです。[IPSec パススルー] を有効にすると、IP Security(IPsec; IP セキュリティ)を使用するアプリケーションがファイアウォールを通過できます。[IPSec パススルー] を無効にするには、[無効にする] を選択します。 次のオプションから希望するものを選択します。 ■ [有効にする](工場出荷時設定) ■ [無効にする]

セクション	フィールドの説明
	[PPTP パススルー] PPTP（Point-to-Point Tunneling Protocol）を有効または無効にします。PPTP を使用すると、PPP（Point-to-Point Protocol）を IP ネットワーク上でトンネリングできます。[PPTP パススルー] を有効にすると、PPTP（Point to Point Tunneling Protocol）を使用するアプリケーションがファイアウォールを通過できます。[PPTP パススルー] を無効にするには、[無効にする] を選択します。 次のオプションから希望するものを選択します。 ■ [有効にする]（工場出荷時設定） ■ [無効にする]

[セキュリティ] > [VPN]

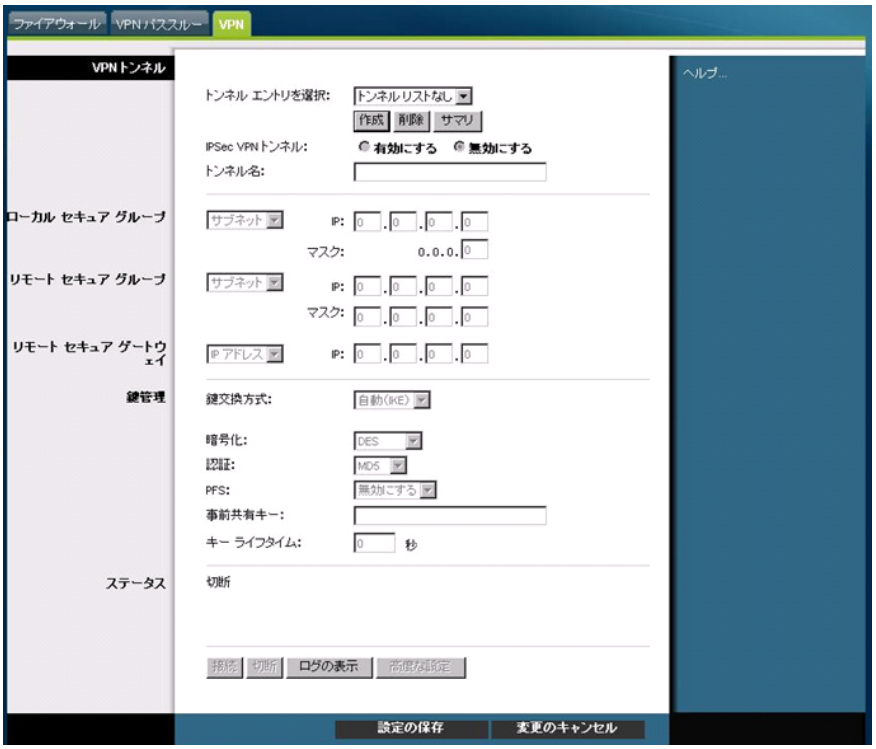
VPN（バーチャル プライベート ネットワーク）は、異なるネットワークの 2 つのエンドポイント間の接続であり、パブリック ネットワークまたは他のプライベート ネットワーク上でプライベート データをセキュアに送信できるようにします。これは「VPN トンネル」を作成することによって実現されます。VPN トンネルは 2 つの PC またはネットワークを接続し、データをプライベート ネットワークで送信するようにインターネットで送信できるようにします。VPN トンネルは IPsec を使用して 2 つのエンドポイント間で送信されるデータを暗号化し、通常のイーサネット/IP フレーム内のデータをカプセル化して、ネットワーク間でデータをセキュアかつシームレスに受け渡すことを可能にします。

VPN は、プライベート ネットワーク向けのプライベートな専用線を使用する代わりに費用効果と安全性が高い方法を提供します。業界標準の暗号化および認証技術を使用して、IPsec VPN はローカル プライベート ネットワークに直接接続しているかのように動作するセキュアな接続を実現します。

たとえば、VPN を使用すると、ユーザは自宅から会社のネットワークに接続し、オフィスで会社の LAN に接続する場合のようにプライベート ネットワークで IP アドレスを受信できます。

[VPN] タブを選択し、[セキュリティ] - [VPN] ページを開きます。

このページでは、レジデンシャル ゲートウェイの VPN を設定します。



[セキュリティ] - [VPN トンネル] ページの説明

次の表の説明と手順を使用して、ゲートウェイの VPN トンネルを設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[VPN トンネル]	[トンネル エントリを選択] 作成された VPN トンネルのリストを表示できます。 [作成] ボタン このボタンをクリックして新しいトンネル エントリを作成します。 [削除] ボタン このボタンをクリックして、選択されたトンネルのすべての設定を削除します。 [サマリ] ボタン このボタンをクリックして、有効なすべてのトンネルの設定とステータスを表示します。 [IPSec VPN トンネル] VPN トンネルのインターネット セキュリティ プロトコルを有効または無効にします。 [トンネル名] このトンネルの名前を入力します。

セクション	フィールドの説明
[ローカル セキュア グループ]	この VPN トンネルを使用できるローカル LAN ユーザを選択します。これには、単一の IP アドレスまたはサブネットワークを指定できます。[ローカル セキュア グループ] の値はリモート ゲートウェイの [リモート セキュア グループ] の値と一致する必要があります。 [IP] ローカル ネットワークの IP アドレスを入力します。 [マスク] [サブネット] オプションが選択されている場合は、ローカル ネットワークの IP アドレスを決定するためにマスクを入力します。
[リモート セキュア グループ]	この VPN トンネルを使用できるリモート ゲートウェイの背後にいるリモート LAN ユーザを選択します。この値として単一の IP アドレス、サブネットワーク、または任意のアドレスを指定できます。[Any] が設定されている場合、ゲートウェイはレスポンダとして動作し、任意のリモート ユーザから要求を受け入れます。[リモート セキュア グループ] の値はリモート ゲートウェイの [ローカル セキュア グループ] の値と一致する必要があります。 [IP] リモート ネットワークの IP アドレスを入力します。 [マスク] [サブネット] オプションが選択されている場合は、リモート ネットワークの IP アドレスを決定するためにマスクを入力します。
[リモート セキュア ゲートウェイ]	[IP アドレス] または [FQDN] のうち、目的のオプションを選択します。リモート ゲートウェイにダイナミック IP アドレスが割り当てられている場合は、[IP アドレス] または [FQDN] を選択します。[IP アドレス] が選択されている場合、ゲートウェイは任意の IP アドレスから要求を受け入れます。 [FQDN] [FQDN] が選択されている場合は、ゲートウェイが DDNS を使用して現在の IP アドレスを見つけることができるようにリモート ゲートウェイのドメイン名を入力します。 [IP アドレス] このフィールドの IP アドレスは、このトンネルのもう一方の端にあるリモート ゲートウェイのパブリック（WAN またはインターネット）IP アドレスに一致する必要があります。
[鍵管理]	[鍵交換方式] ゲートウェイは、自動キー管理と手動キー管理の両方をサポートします。自動キー管理が選択されている場合は、キー データをネゴシエートし Security Association（SA）を実現するために Internet Key Exchange（IKE）が使用されます。手動キー管理が選択されている場合、キーのネゴシエーションは必要ありません。基本的に、手動キー管理は小規模で静的な環境で使用されるか、トラブルシューティングのために使用されます。両サイドで同じキー管理方法を使用する必要があります。

セクション	フィールドの説明
[鍵管理]（続き）	キー交換方法として次のいずれかのオプションを選択します。 ■ [自動（IKE）] – [暗号化]：ESP パケットの暗号化または復号化に使用するキーの長さを決定します。両サイドで同じ方法を使用する必要があります。 – [認証]：ESP（Encapsulating Security Payload）パケットを認証します。[MD5] または [SHA] を選択します。両サイド（VPN エンドポイント）で同じ方法を使用する必要があります。 ▪ [MD5]：128 ビットのダイジェストを生成する一方向ハッシュ アルゴリズム ▪ [SHA]：160 ビットのダイジェストを生成する一方向ハッシュ アルゴリズム – [PFS]：PFS が有効な場合は、IKE フェーズ 2 ネゴシエーションにより IP トラフィックの暗号化と認証のために新しいキー データが生成されます。両サイドで PFS が有効である必要があります。 – [事前共有キー]：IKE は事前共有キーを使用してリモート IKE ピアを認証します。このフィールドでは、文字と 16 進数の値（「My_@123」や「0x4d795f40313233」など）両方を使用できます。両側で同じ事前共有キーを使用する必要があります。 – [キー ライフタイム]：このフィールドは、IKE により生成されたキーのライフタイムを指定します。この時間が経過すると、新しいキーが自動的に再ネゴシエートされます。[キー ライフタイム] の範囲は、300 ～ 100,000,000 秒です。ライフタイムの初期値は **3600** 秒です。 ■ [手動] – [暗号化マニュアル]：ESP パケットの暗号化または復号化に使用するキーの長さを決定します。両サイドで同じ方法を使用する必要があります。 – [暗号化アルゴリズム]：このフィールドは、IP トラフィックの暗号化または復号化に使用するキーを指定します。このフィールドでは、文字と 16 進数の値両方を使用できます。両サイドで同じ暗号化キーを使用する必要があります。 – [認証]：ESP（Encapsulating Security Payload）パケットを認証します。[MD5] または [SHA] を選択します。両サイド（VPN エンドポイント）で同じ方法を使用する必要があります。 ▪ [MD5]：128 ビットのダイジェストを生成する一方向ハッシュ アルゴリズム ▪ [SHA]：160 ビットのダイジェストを生成する一方向ハッシュ アルゴリズム – [認証鍵]：このフィールドは、IP トラフィックの認証に使用するキーを指定します。このフィールドでは、文字と 16 進数の値両方を使用できます。両サイドで同じ認証キーを使用する必要があります。 – [受信 SPI/送信 SPI]：SPI（Security Parameter Index）が ESP ヘッダーに含まれます。これにより、受信側でパケットを処理する必要がある SA を選択できます。SPI は 32 ビットの値です。10 進数の値と 16 進数の値両方を使用できます（「987654321」や「0x3ade68b1」など）。各トンネルの受信 SPI と送信 SPI は一意である必要があります。2 つのトンネルは同じ SPI を共有できません。受信 SPI はリモート ゲートウェイの受信 SPI に一致する必要があり、送信 SPI はリモート ゲートウェイの受信 SPI に一致する必要があります。
[ステータス]	このフィールドには、選択されたトンネルの接続ステータスが表示されます。ステータスは、[接続] または [切断] のいずれかになります。

セクション	フィールドの説明
ボタン	[接続] このボタンをクリックして、現在の VPN トンネルの接続を確立します。変更を行った場合は、[設定の保存] をクリックして最初に変更を適用します。 [切断] このボタンをクリックして、現在の VPN トンネルの接続を解除します。 [ログの表示] このボタンをクリックして、確立された各トンネルの詳細が示された VPN ログを参照します。 [高度な設定] [鍵交換方式] が [自動(IKE)] である場合は、このボタンにより IKE に関連する詳細設定にアクセスできます。ゲートウェイがリモート ゲートウェイに対して VPN トンネルを確立できない場合はこのボタンをクリックし、[高度な設定] の値がリモート ゲートウェイの同様の値に一致することを確認します。 ■ [フェーズ 1 動作モード] リモート VPN エンドポイントに適切な方法を選択します。 – [メイン]:[メイン] モードは低速ですがセキュリティが向上します。 – [アグレッシブ]:[アグレッシブ] モードは高速ですがセキュリティが低下します。 ■ [ローカル ID] このトンネルのもう一方の端の [リモート ID] 設定に一致するように、目的のオプションを選択します。 – [ローカル IP アドレス]:WAN(インターネット)IP アドレス – [名前]:ドメイン名 ■ [リモート ID] このトンネルのもう一方の端の [ローカル ID] 設定に一致するように、目的のオプションを選択します。 – [ローカル IP アドレス]:リモート VPN エンドポイントの WAN(インターネット) IP アドレス – [名前]:リモート VPN エンドポイントのドメイン名 ■ [暗号化] これは IKE SA に使用される暗号化アルゴリズムです。トンネルのもう一方の端で使用される設定に一致する必要があります。

ログの表示

[セキュリティ] - [VPN] - [ログの表示] ページには、ファイアウォールで捕捉されたイベントが表示されます。このログには次の項目が表示されます。

- イベントの説明
- 発生したイベントの数
- 最後に発生したイベント
- 宛先アドレスおよび送信元アドレス

このページでは次のログを参照できます。

- アクセス ログ
- ファイアウォール ログ
- VPN ログ
- ペアレンタル コントロール ログ

ログ データを消去する場合は、[クリア] をクリックします。

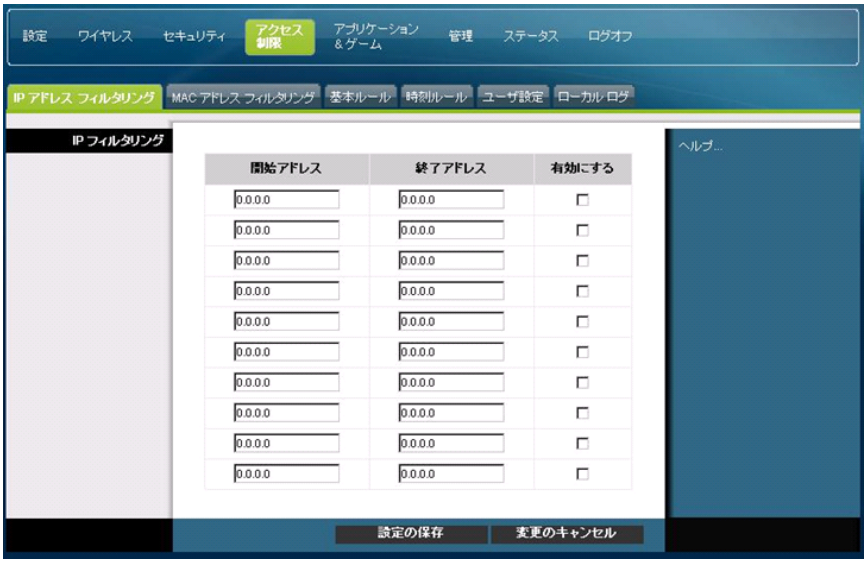
ゲートウェイへのアクセス制御

[アクセス制限] > [IP アドレス フィルタリング]

IP アドレス フィルタを設定する場合は、[アクセス制限] - [IP フィルタリング] ページを使用します。これらのフィルタにより、特定の範囲の IP アドレスがインターネットにアクセスできなくなります。

注:この項で説明されている設定がよくわからないという場合は、レジデンシャル ゲートウェイの IP フィルタリング設定を変更する前にケーブルテレビ局に相談してください。

[IP アドレス フィルタリング] タブを選択し、[アドレス制限] - [IP アドレス フィルタリング] ページを開きます。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。



[アクセス制限] > [MAC アドレス フィルタリング]

MAC アドレス フィルタを設定する場合は、[アクセス制限] - [MAC アドレス フィルタリング] ページを使用します。これらのフィルタを使用すると、ある範囲の MAC アドレスがインターネットにアクセスするのを MAC アドレスに基づいて許可または拒否できます。

注:この項で詳細に説明されている設定がよくわからないという場合は、レジデンシャル ゲートウェイの IP フィルタリング設定を変更する前にケーブルテレビ局に相談してください。

[MAC アドレス フィルタリング] タブを選択し、[アドレス制限] - [MAC アドレス フィルタリング] ページを開きます。

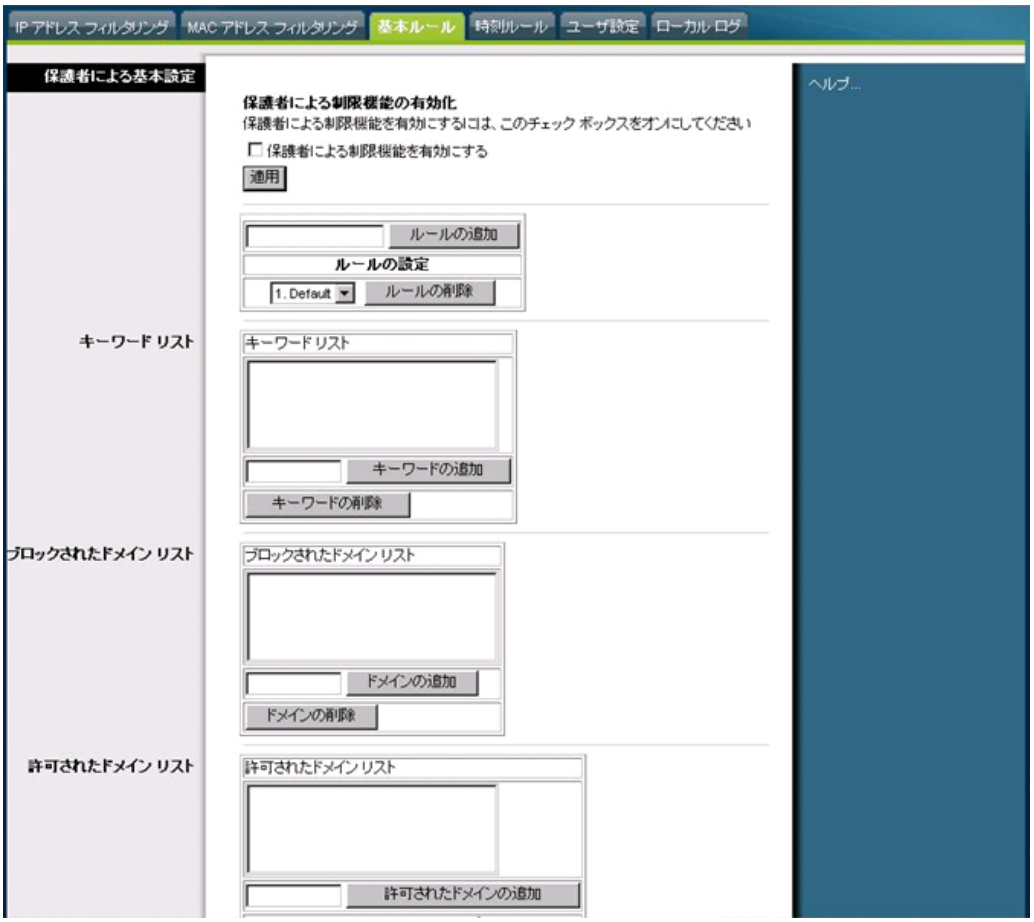
MAC アドレス フィルタの対象となるデバイスの MAC アドレスに対してインターネット アクセスを拒否または許可できます。必要なアドレスを入力した後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

フィールド名	説明
[MAC フィルタリング]	[ブロック]（初期値） デバイスの MAC アドレスに対してインターネット アクセスを拒否する場合は、[ブロック] を選択します。それ以外のすべての MAC アドレスには、インターネット アクセスが許可されます。
	[許可] MAC アドレス フィルター覧に表示されているデバイス MAC アドレスだけにインターネット アクセスを許可する場合は、[許可] を選択します。表示されて*いない* MAC アドレスはすべて、インターネット アクセスを拒否されます。

[アクセス制限] > [基本ルール]

アクセス制限によって、インターネット アクセス、指定アプリケーション、Web サイト、および特定の日付や時間の着信トラフィックなど、特定のインターネット使用やトラフィックをブロックしたり、許可したりすることができます。[アクセス制限] - [基本ルール] ページでは、レジデンシャル ゲートウェイにペアレンタル コントロールを設定し、ペアレンタル コントロールを設定する権限のあるユーザを監視できます。

[基本ルール] タブを選択して、[アクセス制限] - [基本ルール] ページを開きます。



次の表の説明と手順を使用して、レジデンシャル ゲートウェイにアクセス制限の基本ルールを設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[保護者による基本設定]	[保護者による制限機能の有効化] ペアレンタル コントロールを有効または無効にします。ペアレンタル コントロールを有効にするには、[保護者による制限機能を有効にする] チェックボックスをオンにして、[適用] をクリックします。ペアレンタル コントロールを無効にするには、[保護者による制限機能を有効にする] チェックボックスをオフにして、[適用] をクリックします。 [ルールの追加] コンテンツ ルールのリストに新しいルールを追加し、保存します。 [ルールの削除] 選択したルールをコンテンツ ルール リストから削除します。

セクション	フィールドの説明
[キーワード リスト]	[キーワード リスト] キーワードのリストを作成できます。このリスト内のいずれかのキーワードを含む URL にアクセスしようとすると、ゲートウェイでブロックされます。 [キーワードの追加] [キーワードの削除] リストに新しいキーワードを追加したり、選択したキーワードをリストから削除したりできます。
[ブロックされたドメイン リスト]	[ブロックされたドメイン リスト] ゲートウェイでアクセスをブロックするドメインのリストを作成できます。このリスト内のいずれかのドメインにアクセスしようとすると、ゲートウェイでブロックされます。 [ドメインの追加] [ドメインの削除] リストに新しいドメインを追加したり、選択したドメインをリストから削除したりできます。
[許可されたドメイン リスト]	[許可されたドメイン リスト] ゲートウェイでアクセスを許可するドメインのリストを作成できます。 [許可されたドメインの追加] [許可されたドメインの削除] リストに新しいドメインを追加したり、選択したドメインをリストから削除したりできます。
[オーバーライド パスワード]	[パスワード] ブロックされたインターネット サイトへのユーザ アクセス制限を一時的に上書きするパスワードを作成できます。 [パスワードの再入力] 前のフィールドに入力した上書き用パスワードを確認するため、同じパスワードを再入力します。 [アクセス期間] 上書き用パスワードによって、制限されたインターネット サイトへのアクセスを一時的に許可する時間（分数）を指定します。 [適用] すべての追加、編集、および変更を保存します。

キーワードおよびドメイン ブロッキングの使用

キーワードおよびドメイン ブロッキングでは、インターネット サイトへのアクセスに使用する URL に含まれる単語やテキスト文字列によって特定のインターネット サイトへのアクセスを制限できます。

ドメイン ブロッキングでは、サイトのドメイン名に基づいて Web サイトへのアクセスが制限されます。ドメイン名は URL の一部であり、よく知られている .COM、.ORG、または .GOV 拡張子の前に記載されています。

キーワード ブロッキングでは、ドメイン名内に限らず、URL 内のいずれかに存在するキーワードまたはテキスト文字列に基づいて、インターネット サイトへのアクセスをブロックできます。

注:ドメイン ブロッキング機能では、ドメイン リストにあるドメインへのアクセスがブロックされます。また、リスト内のエントリと完全に一致する部分を含むドメインもブロックされます。

たとえば、ドメインとして **example.com** を入力すると、「example.com」を含むすべてのサイトがブロックされます。通常は、ドメイン名に「www.」が含まれないようにします。「www.」を含めると、ブロッキングの対象がそのドメイン名と完全に一致するサイトに限定されてしまいます。たとえば、リストに www.example.com と入力すると、その名前と完全に一致するサイト 1 つだけがブロックされます。「www.」を含めていない場合は、「example.com」内のサイトや関連サイトがすべてブロックされます。

Web サイトへのアクセスのブロック

Web サイトへのアクセスをブロックする場合は、[ブロックされたドメイン リスト] または [キーワード リスト] を使用します。

[ブロックされたドメイン リスト] を使用するには、ブロックする Web サイトの URL またはドメイン名を入力します。

[キーワード リスト] を使用して、ブロックするキーワードを入力します。これらのキーワードのいずれかが Web サイトの URL に含まれている場合、そのサイトへのアクセスはブロックされます。チェックされるのは URL だけであり、各 Web ページのコンテンツはチェックされません。

[アクセス制限] > [時刻ルール]

[アクセス制限] - [時刻ルール] ページを使用して、選択した曜日や時刻の設定に基づいて特定のネットワーク デバイスとの間を行き来するすべてのインターネット トラフィックをブロックするように、Web アクセス フィルタを設定します。

[時刻ルール] タブを選択して、[アクセス制限] - [時刻ルール] ページを開きます。次の図は、[アクセス制限] - [時刻ルール] ページの例です。

注:レジデンシャル ゲートウェイでは、ケーブルテレビ局が管理するネットワーク時刻のクロックが使用されます。製品が正常に動作するためには、時計が実際の時刻に適切に設定されている必要があります。[ステータス] ページや [時刻設定] ページに正確な時刻が反映されていることを確認します。正確な時刻が反映されていない場合は、ケーブルテレビ局に問い合わせてください。または、時間のずれを計算に入れて、設定を調整することもできます。

[アクセス制限] - [時刻ルール] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイに時刻ルールを設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[時刻フィルタ]	[追加] 新規の時刻アクセス フィルタまたはルールを追加できます。フィルタの名前を入力し、[追加] をクリックしてリストにフィルタを追加します。時刻ルールは、曜日と時刻に基づいてインターネット アクセスを制限するために使用します。 [削除] 選択したフィルタを時刻フィルタ リストから削除します。
[スケジュール]	[ブロックする曜日] 曜日に基づいてアクセスを制御できます。 [ブロックする時間] 時刻に基づいてアクセスを制御できます。

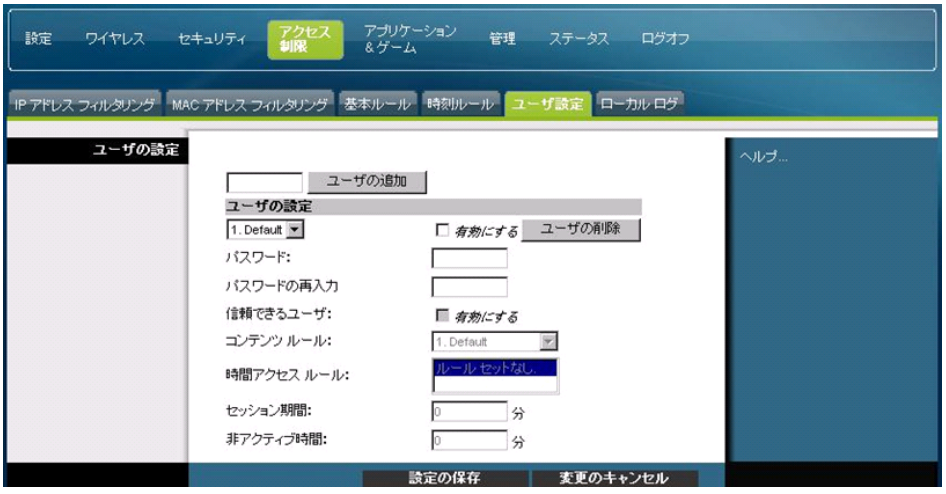
[アクセス制限] > [ユーザ設定]

[アクセス制限] - [ユーザ設定] ページを使用して、ユーザ アカウントとプロファイルを追加で設定します。各プロファイルには、そのユーザのプロファイルに割り当てられているアクセス ルールに見合ったインターネット アクセス レベルを割り当てることができます。

重要:これらの追加のアカウントには、ゲートウェイへの管理アクセス権は付与されません。

注:ユーザ プロファイルを定義および有効にした後は、各ユーザが、インターネットにアクセスしようとするたびにサインオンする必要があります。Web ブラウザにポップアップ サインオン画面が表示されると、サインオンが可能になります。ユーザがインターネットへのアクセス権を得るには、正しいユーザ名とパスワードを入力する必要があります。

[ユーザ設定] タブを選択して、[アクセス制限] - [ユーザ設定] ページを開きます。



[アクセス制限] - [ユーザ設定] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイに対するユーザ設定を行います。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[ユーザの設定]	[ユーザの追加] 新規のユーザ プロファイルを追加できます。ユーザの名前を入力し、[ユーザの追加] ボタンをクリックしてリストにユーザを追加します。 [ユーザの設定] ドロップダウン メニューを使用して、ユーザ プロファイルを編集できます。ドロップダウン メニューから、編集するプロファイルを選択できます。ユーザ名とパスワードは、大文字と小文字が区別されます。 [有効にする] チェックボックスは必ずオンにして、ユーザ プロファイルをアクティブにします。プロファイルがアクティブになっていないと、そのユーザはインターネットにアクセスできません。 ユーザ プロファイルを削除するには、ドロップダウン メニューを使用して削除するユーザを選択し、[ユーザの削除] ボタンをクリックします。 [パスワード] 選択したユーザのパスワードをこのフィールドに入力します。ユーザは、インターネットを使用するたびに、自分のユーザ名とパスワードを入力する必要があります。ユーザ名とパスワードは、大文字と小文字が区別されます。 **注**:レジデンシャル ゲートウェイは、このページで選択するルールに従ってユーザごとにインターネットへのアクセスを許可します。 [パスワードの再入力] 前のフィールドに入力したパスワードを確認するため、同じパスワードを再入力します。 [信頼できるユーザ] 現在の選択ユーザを信頼されるユーザとして指定する場合は、このチェックボックスをオンにします。信頼されるユーザには、インターネット アクセス ルールは適用されません。 [コンテンツ ルール] 現在のユーザ プロファイルに対するコンテンツ ルールを選択します。コンテンツ ルールは、最初にルールの設定ページに移動して定義しておく必要があります。ルールの設定ページにアクセスするには、このページの [基本ルール] タブをクリックします。 [時間アクセス ルール] 現在のユーザ プロファイルに対する時間アクセス ルールを選択します。時間アクセス ルールは、最初に [時刻ルール] ページに移動して定義しておく必要があります。[時刻ルール] ページにアクセスするには、このページの [時刻ルール] タブをクリックします。 [セッション期間] 1440 分(ユーザを作成するときの工場出荷時設定。それ以外は 0(ゼロ)です)。 ユーザがユーザ名とパスワードを使用してサインオンした時刻から始めて、インターネットへのアクセスが許可される時間(分数)を入力します。 **注**:セッション タイムアウトを防止するには、[セッション期間] を 0(ゼロ)に設定します。

セクション	フィールドの説明
	[非アクティブ時間] 60 分(ユーザを作成するときの工場出荷時設定。それ以外は 0(ゼロ)です)。 ユーザ セッション中にインターネット アクセス アクティビティがなく、ユーザがオンラインではなくなったと判断される時間を入力します。非アクティビティ タイマーが起動すると、ユーザ セッションは自動的に終了します。インターネット アクセスを再開するには、ユーザ名とパスワードを使用してログインしなおす必要があります。 **注**:セッション タイムアウトを防止するには、非アクティビティ時間の値を 0(ゼロ)に設定します。

[アクセス制限] > [ローカル ログ]

このページでは、制限されているインターネット サイトにアクセスしようとする試みをユーザ別に追跡できます。このページから、ペアレンタル コントロール イベント レポート機能で取得したイベントを表示することもできます。

[ローカル ログ] タブを選択して、[アクセス制限] - [ローカル ログ] ページを開きます。

次の図は、[アクセス制限] - [ローカル ログ] ページの例です。

セクション	フィールドの説明
[ローカル ログ] [保護者による制限 – イベント ログ]	[最終実行日時] 制限されているインターネット サイトへのアクセスが試みられた最近の時刻を表示します。 [アクション] システムが実施したアクションを表示します。 [ターゲット] 制限されているサイトの URL を表示します。 [ユーザ] 制限されているサイトにアクセスしようとしたユーザを表示します。 [ソース] 制限されている Web サイトへのアクセスを試みたときに使用された PC の IP アドレスを表示します。

アプリケーションおよびゲームの設定

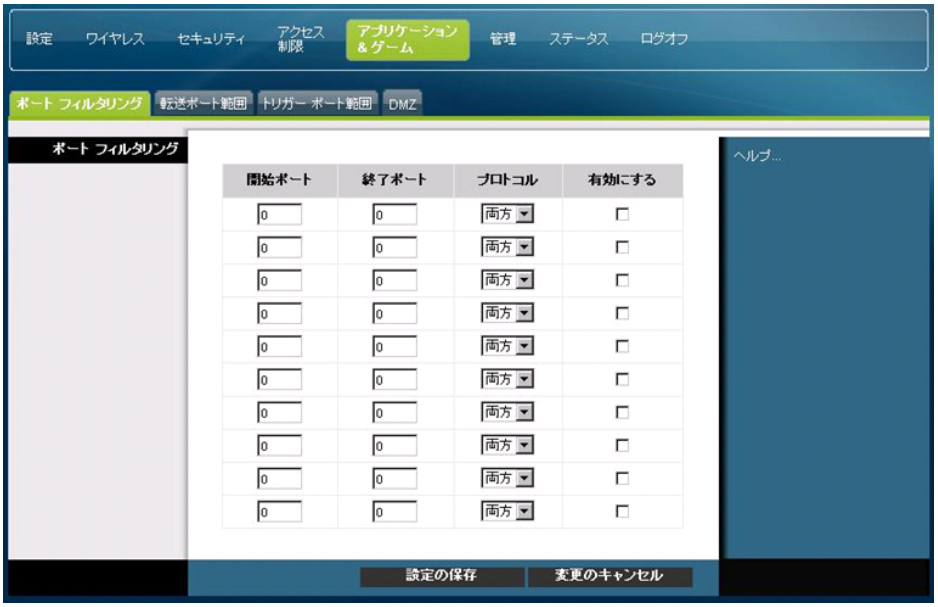
概要

最もよく知られているインターネット アプリケーションは、Application Layer Gateway（ALG; アプリケーション層ゲートウェイ）によってサポートされます。ALG は、カスタム設定を行わずにデータを通過させることができるよう、自動的にゲートウェイ ファイアウォールを調整します。この項の変更を行う前に、お使いのアプリケーションをテストすることをお勧めします。

[アプリケーション & ゲーム] > [ポート フィルタリング]

このウィンドウを使用して、TCP（Transmission Control Protocol）および UDP（User Datagram Protocol）ポート フィルタを設定します。これらのフィルタを利用して、一定範囲の TCP/UDP ポートがインターネットにアクセスできないようにします。また、PC から特定の IP ポート番号で WAN への発信 TCP/UDP トラフィックが送信されないようにすることもできます。このフィルタは、IP アドレス固有でも、MAC アドレス固有でもありません。システムは、すべての PC に対して指定された範囲のポートをブロックします。

[ポート フィルタリング] タブを選択して、[アプリケーション & ゲーム] – [ポート フィルタリング] ページを開きます。



[アプリケーション & ゲーム] - [ポート フィルタリング] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイで使用するアプリケーションおよびゲーム機能にポート フィルタリングを設定します。関連アプリケーションに対してポート転送を有効にするには、[有効にする] チェックボックスをオンにします。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[ポート フィルタリング]	[開始ポート] ポート範囲の始まりです。サーバまたはインターネット アプリケーションによって使用されるポート番号（外部ポート）の範囲の始まりを入力します。必要に応じて、インターネット アプリケーションのソフトウェア マニュアルで詳細を確認してください。
	[終了ポート] ポート範囲の終わりです。サーバまたはインターネット アプリケーションによって使用されるポート番号（外部ポート）の範囲の終わりを入力します。必要に応じて、インターネット アプリケーションのソフトウェア マニュアルで詳細を確認してください。
	[プロトコル] 次のいずれかのプロトコルを選択します。 ■ [TCP] ■ [UDP] ■ [両方]
	[有効にする] 指定したポートでフィルタリングを有効にするには、このチェックボックスをオンにします。

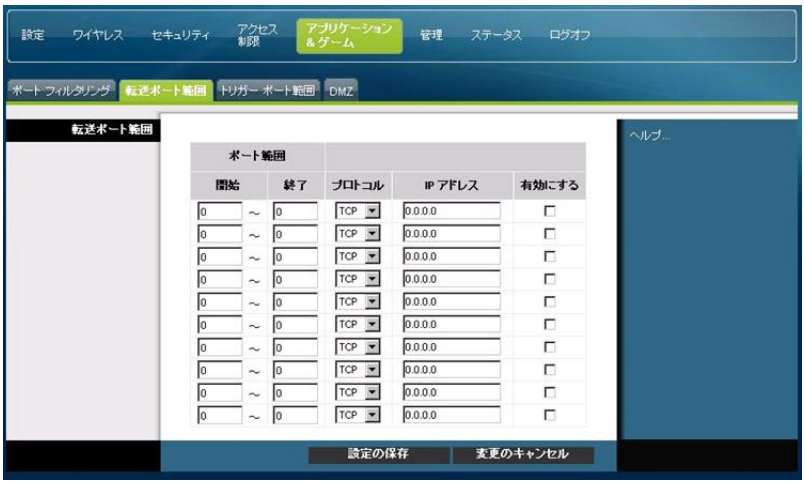
[アプリケーション & ゲーム] > [転送ポート範囲]

重要：ゲートウェイでは通常、ポート変換という機能が実行されます。ポート変換では、LAN上の PC やその他のデバイスで実際にどのポートが使用されているかを監視します。この監視機能によって、ファイアウォールを超えたセキュリティ レベルが提供されます。ただし、特定のポートを使用してインターネット接続することをゲートウェイに要求するアプリケーションもあります。

[転送ポート範囲] を使用して、パブリック インターネットからローカル ネットワーク内の特定の IP アドレスにポートを転送します。[転送ポート範囲] タブを選択して、[アプリケーション & ゲーム] - [転送ポート範囲] ページを開きます。

開始ポートと終了ポートは、推奨される 49152 ～ 65535 の範囲から選択します。使用されるポートはプログラム固有であるため、プログラムがどのポート転送を必要としているかを必ず確認してください。両方のボックスにポート番号または範囲を入力します。[IP アドレス] ボックスに、この設定を適用するコンピュータの IP アドレスを入力します。

注:[転送ポート範囲] によって、選択したポートはパブリック インターネットに継続的に公開されます。つまり、ゲートウェイのファイアウォールはこれらのポートに対して動作しなくなります。ポート範囲が転送されている間は、転送先の IP アドレスを持つデバイスがハッカーの攻撃に晒されるおそれがあります。



[アプリケーション & ゲーム] - [転送ポート範囲] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイにポート範囲の転送を設定します。ポート範囲ごとに [有効にする] を選択します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[転送ポート範囲]	[開始] 開始ポートは、推奨される 49152 ～ 65535 の範囲から選択します。使用されるポートはプログラム固有であるため、プログラムがどのポート転送を必要としているかを必ず確認してください。
	[終了] 終了ポートは、推奨される 49152 ～ 65535 の範囲から選択します。使用されるポートはプログラム固有であるため、プログラムがどのポート転送を必要としているかを必ず確認してください。
	[プロトコル] 次のいずれかのプロトコルを選択します。 ■ [TCP] ■ [UDP] ■ [両方]
	[IP アドレス] この設定を適用するコンピュータの IP アドレスを入力します。
	[有効にする] 指定したポートおよび IP アドレスに対してポート フォワーディングを有効にするには、このチェックボックスをオンにします。

[アプリケーション & ゲーム] > [トリガー ポート範囲]

トリガー ポート範囲は、特定の時間にポートを必要とする LAN PC に対して動的にポートを転送する方法です。この特定の時間とは、ルータを起動するイベントが実行されるアプリケーションの実行時です。このイベントは、特定のポート範囲からの発信アクセスです。

[トリガー ポート範囲] タブを選択して、[アプリケーション & ゲーム] - [トリガー ポート範囲] ページを開きます。

[アプリケーション & ゲーム] - [トリガー ポート範囲] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイにトリガー ポート範囲を設定します。ポート範囲ごとに [有効にする] を選択します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[トリガー ポート範囲]	
[トリガー範囲]	[開始ポート] 開始ポートは、推奨される 49152 ～ 65535 の範囲から選択します。使用されるポートはプログラム固有であるため、プログラムがどのポート転送を必要としているかを必ず確認してください。
	[終了ポート] 終了ポートは、推奨される 49152 ～ 65535 の範囲から選択します。使用されるポートはプログラム固有であるため、プログラムがどのポート転送を必要としているかを必ず確認してください。
[転送範囲]	[開始ポート] 開始ポートは、推奨される 49152 ～ 65535 の範囲から選択します。使用されるポートはプログラム固有であるため、プログラムがどのポート転送を必要としているかを必ず確認してください。

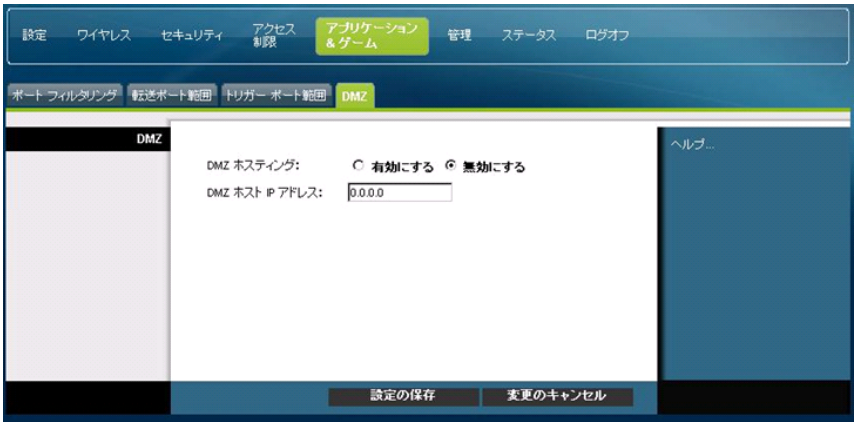
セクション	フィールドの説明
	[終了ポート] 終了ポートは、推奨される 49152 ～ 65535 の範囲から選択します。使用されるポートはプログラム固有であるため、プログラムがどのポート転送を必要としているかを必ず確認してください。
	[プロトコル] 次のいずれかのプロトコルを選択します。 ■ [TCP] ■ [UDP] ■ [両方]
	[有効にする] 関連アプリケーションに対してポート範囲トリガーを有効にするには、[有効にする] チェックボックスをオンにします。

[アプリケーション & ゲーム] > [DMZ]

このページを使用して、ポートをパブリック インターネットまたは WAN(ワイドエリア ネットワーク)に直接公開する IP アドレスを設定します。DMZ(非武装地帯)ホスティングは一般に「公開ホスト」と呼ばれ、これを利用することによって、NAT(ネットワーク アドレス変換)で既知のローカル PC に転送できない WAN トラフィックの受信者を指定できます。

DMZ は通常、独自のインターネット サーバのホストを希望する企業で使用されます。DMZ の利用により、1 つの IP アドレスをゲートウェイ ファイアウォールのインターネットサイドに配置し、その他をファイアウォールの背後で保護されたままにすることができます。

DMZ は、Web(HTTP)サーバ、FTP サーバ、SMTP(電子メール)サーバ、および DNS(Domain Name System)サーバなどのデバイスにインターネット トラフィックが直接アクセスできるようにします。[DMZ] タブを選択して、[アプリケーション & ゲーム] - [DMZ] ページを開きます。



[アプリケーション & ゲーム] - [DMZ] ページの説明

次の表の説明と手順を使用して、レジデンシャル ゲートウェイにポート範囲トリガーを設定します。各 DMZ ホスト IP アドレスに対して [有効にする] を選択します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

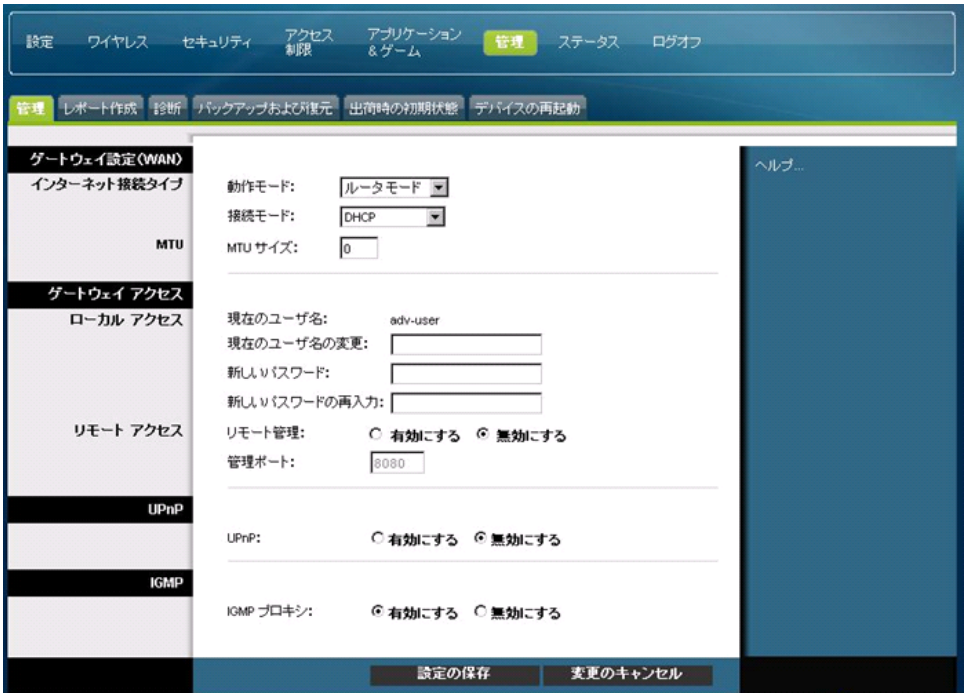
セクション	フィールドの説明
[DMZ]	[DMZ ホスティング] 次のオプションから希望するものを選択します。 ■ [有効にする] ■ [無効にする]（工場出荷時設定）
	[DMZ ホスト IP アドレス] DMZ では、1 つの IP アドレスを保護対象から外し、その他を保護対象のままにすることができます。このフィールドには、インターネットに公開するコンピュータの IP アドレスを入力します。

ゲートウェイの管理

[管理] > [管理]

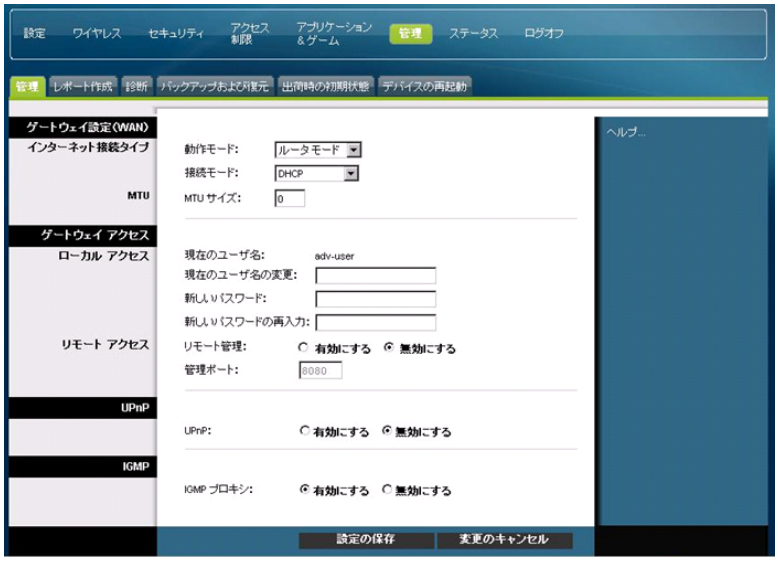
ネットワークの管理者は、[管理] - [管理] ページを利用して、アクセスおよびセキュリティに関する特定のゲートウェイ機能を管理できます。[管理] タブを選択して、[管理] - [管理] ページを開きます。

重要:次のページは、[接続モード] が [DHCP](工場出荷時設定)に設定されているときに表示されます。[スタティック IP] が選択されているときに表示されるページの図とその説明は、この項で後ほど示します。



[管理] - [管理] ページの説明

次の表の説明と手順を使用して、[DHCP] または [スタティック IP] 接続モードが選択されている場合のレジデンシャル ゲートウェイの管理を設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

フィールド	説明
[ゲートウェイ設定（WAN）] [インターネット接続タイプ]	[接続モード]：この設定によって、WAN（またはインターネットに対するゲートウェイ インターフェイス）がどのように IP アドレスを取得するかが決定します。 [DHCP]（工場出荷時設定） ゲートウェイは、パブリック IP アドレスを自動的に取得できます。  [スタティック IP] WAN IP アドレスと対応するサーバ情報を、ゲートウェイがオンラインになるたびに使用されるスタティック値または固定値として指定できます。 

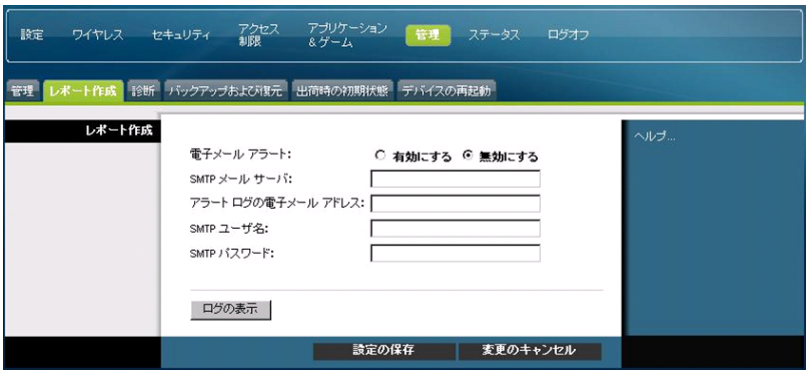
フィールド	説明
	[インターネット IP アドレス] （インターネットに公開される）ゲートウェイの IP アドレスを入力します。 [サブネット マスク] （ケーブルテレビ局など、インターネットに公開される）ゲートウェイのサブネット マスクを入力します。 [デフォルト ゲートウェイ] ケーブルテレビ局のサーバのデフォルト ゲートウェイを入力します。 [プライマリ DNS] ケーブルテレビ局から提供されているプライマリのドメイン ネーム サーバの IP アドレスを入力します。これは必須です。 [セカンダリ DNS] ケーブルテレビ局から提供されているセカンダリのドメイン ネーム サーバの IP アドレスを入力します。これは任意です。
[MTU]	
	[MTU サイズ] MTU とは、Maximum Transmission Unit（最大伝送ユニット）の略です。MTU サイズは、インターネット送信に対して許可される最大パケット サイズを示します。工場出荷時設定 = 0（1500 バイト）
[ゲートウェイ アクセス]	
[ローカル アクセス]	[現在のユーザ名] 現在ログインしているユーザを識別します。 [現在のユーザ名の変更] このフィールドでは、ユーザ名を変更できます。ユーザ名を変更する場合は、このフィールドに新しいユーザ名を入力し、[設定の保存] をクリックして変更を適用します。 **注**：工場出荷時設定のユーザ名のフィールドは空白です。 [新しいパスワード] このフィールドでは、パスワードを変更できます。パスワードを変更する場合は、このフィールドに新しいパスワードを入力します。次に、[新しいパスワードの再入力] フィールドに新しいパスワードを再入力し、[設定の保存] をクリックして変更を適用します。 **注**：工場出荷時設定のパスワードのフィールドは空白です。 [新しいパスワードの再入力] 新しいパスワードを再入力します。[新しいパスワード] フィールドに入力したパスワードと同じパスワードを入力する必要があります。新しいパスワードを入力した後は、[設定の保存] をクリックして変更を適用します。

フィールド	説明
[リモート アクセス]	[リモート管理] リモート管理を有効または無効にすることができます。この機能により、自宅から離れていてもインターネットを介してゲートウェイ設定にアクセスし、管理することができます。リモート アクセスを許可するには、[有効にする] を選択します。許可しない場合は、初期設定の [無効にする] のままにします。リモート管理には、プロトコル HTTP が必要です。デバイスにリモートからアクセスするには、Web ブラウザのアドレス フィールドに、https://xxx.xxx.xxx.xxx:8080（x はデバイスのパブリック インターネット IP アドレスを示し、8080 は指定のポートを示します）と入力します。 [管理ポート] 外部アクセス用に開放するポート番号を入力します。工場出荷時設定は 8080 です。リモート接続を確立するときは、このポートを使用する必要があります。
[UPnP]	[UPnP] Windows XP、Vista および 7 では、ユニバーサル プラグ アンド プレイ（UPnP）を利用することで、ゲームやビデオ会議などの各種のインターネット アプリケーションに対応するようにゲートウェイを自動的に設定できます。UPnP を使用する場合は、初期値の [有効にする] のままにします。使用しない場合は、[無効にする] を選択します。
[IGMP]	[IGMP プロキシ] IGMP（Internet Group Multicast Protocol）は、マルチキャスト グループのメンバーシップを確立するために使用され、通常はマルチキャスト ストリーミング アプリケーションに使用されます。たとえば、同一のローカル ネットワークの複数のセットトップ ボックスで IPTV（Internet Protocol Television）を使用しているとします。これらのセットトップ ボックスでは異なるビデオ ストリームが同時に実行されるため、ルータの IGMP 機能を使用する必要があります。 IGMP フォワーディング（プロキシング）は、LAN 側のクライアントに対するマルチキャストを改善するシステムです。クライアントでこのオプションがサポートされている場合は、初期値の [有効にする] のままにします。サポートされていない場合は、[無効にする] を選択します。

[管理] > [レポート作成]

[管理] - [レポート作成] では、特定の電子メール アドレスに各種のシステム アクティビティが送信されるようにすることができます。

[レポート作成] タブを選択して、[管理] - [レポート作成] ページを開きます。



次の表の説明と手順を使用して、ゲートウェイにレポート機能を設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[レポート作成]	[電子メール アラート] この機能を有効にすると、レポート可能なイベントが検出された場合、ただちに電子メールが送信されます。この機能を使用するには、必要な電子メール アドレス情報を入力します。
	[SMTP メール サーバ] 発信電子メールに使用する SMTP（簡易メール転送プロトコル）サーバのアドレス（ドメイン名）または IP アドレスを入力します。
	[アラート ログの電子メール アドレス] ログを受信する電子メール アドレスを入力します。

ログの表示

ログを表示するには、次の手順を実行します。

1 [ログの表示] をクリックします。新しいウィンドウが開き、ログ データ ページが表示されます。

2 特定のログを表示するには、[タイプ] ドロップダウン メニューから次のいずれかのオプションを選択します。

- [すべて]
- [システム ログ]
- [アクセス ログ]
- [ファイアウォール ログ]
- [VPN ログ]
- [保護者による制限]

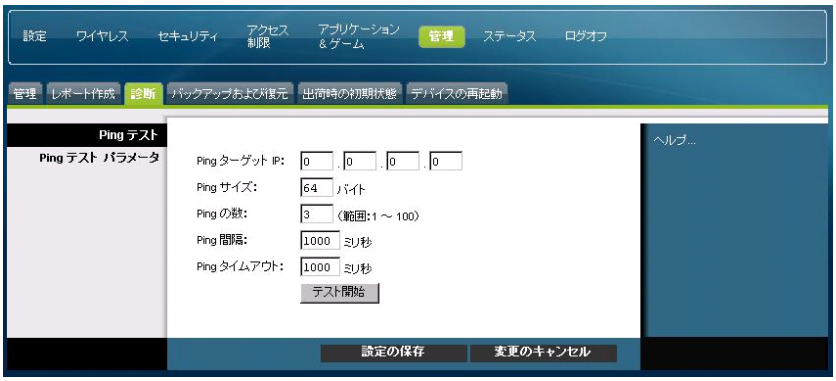
3 ログ データが表示された後は、次のいずれかのオプションを使用します。

- [リフレッシュ] ボタンをクリックすると、ログが更新されます。
- [クリア] ボタンをクリックすると、現在のログの情報がすべてクリアされます。

[管理] > [診断]

[管理] - [診断] では、ping テストを使用してインターネット接続のステータスをチェックできます。

[診断] タブを選択して、[管理] - [診断] ページを開きます。



次の表の説明と手順を使用して、ゲートウェイに診断機能を設定します。必要な選択を行った後は、[設定の保存] をクリックしてそれを適用するか、[変更のキャンセル] をクリックして取り消します。

セクション	フィールドの説明
[Ping テスト]	
[Ping テスト パラメータ]	[Ping ターゲット IP] ping する IP アドレス [Ping サイズ] 使用するパケットのサイズ [Ping の数] ターゲット デバイスを ping する回数 [Ping 間隔] ping から次の ping までの時間(ミリ秒) [Ping タイムアウト] タイムアウトの時間(ミリ秒)。この時間内に何らかの応答がなかった場合、ping テストは失敗と見なされます。 [テスト開始] テストを開始するには、次の手順を実行します。 **1** [テスト開始] をクリックして、テストを開始します。新しいページが開き、テスト結果サマリが表示されます。 **2** [設定の保存] をクリックしてテスト結果を保存するか、[変更のキャンセル] をクリックしてテストを取り消します。

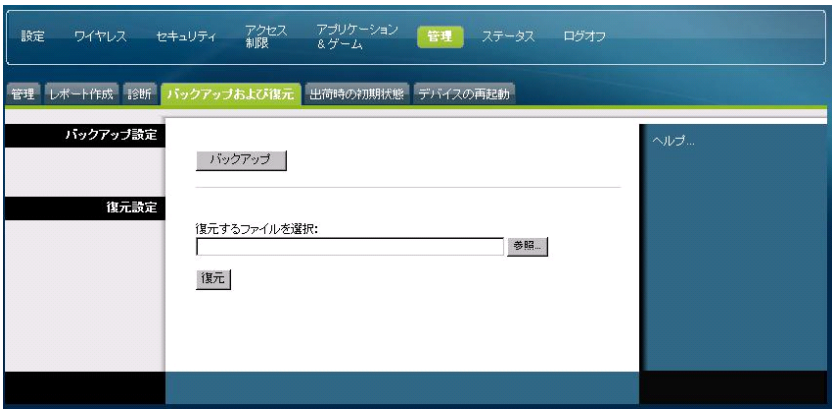
[管理] > [バックアップおよび復元]

[管理] - [バックアップおよび復元] では、ゲートウェイの設定をバックアップしてコンピュータに保存できます。このバックアップ ファイルを使用して、以前に保存したゲートウェイの設定を復元できます。

[バックアップおよび復元] タブを選択して、[管理] - [バックアップおよび復元] ページを開きます。

注意:

コンフィギュレーション ファイルを復元すると、既存の設定がすべて破棄(上書き)されます。



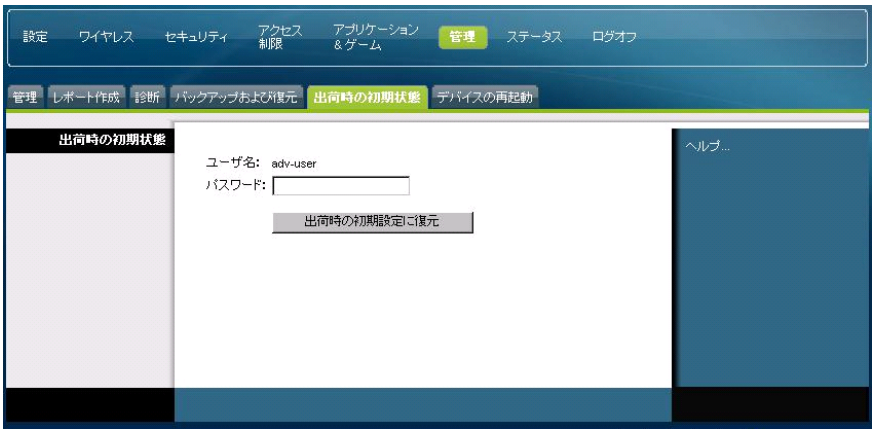
セクション	フィールドの説明
[バックアップ設定]	[バックアップ設定] 機能を使用すると、現在の設定をコピーしてコンピュータに保存できます。[バックアップ] をクリックして、ダウンロードを開始します。
[復元設定]	[復元設定] 機能を使用すると、以前に保存したコンフィギュレーション ファイルを復元できます。[参照] をクリックしてコンフィギュレーション ファイルを選択し、[復元] をクリックしてそのコンフィギュレーション ファイルをデバイスにロードします。

[管理] > [出荷時の初期状態]

[管理] - [出荷時の初期状態] ページでは、設定を工場出荷時設定に戻すことができます。[出荷時の初期状態] タブを選択して、[管理] - [出荷時の初期状態] ページを開きます。

注意:

工場出荷時設定を復元すると、それまでにゲートウェイに入力したすべての設定が失われます。ゲートウェイを工場出荷時設定に戻す前に、カスタム設定をすべて書き留めておいてください。工場出荷時設定が復元された後で、すべてのカスタム設定を再入力する必要があります。



出荷時の初期設定に復元

工場出荷時設定を復元するには、[出荷時の初期設定に復元] をクリックします。これによりすべての設定が初期値に戻されます。初期設定が復元されると、保存していた設定はすべて失われます。

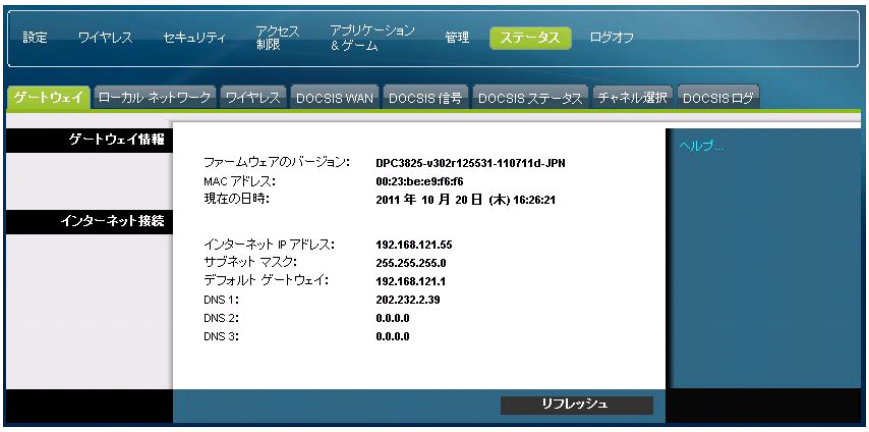
ゲートウェイ ステータスの監視

ここでは、[ステータス] タブで使用できるオプションについて説明します。これらのオプションを使用して、レジデンシャル ゲートウェイのステータスを監視したり、デバイスやネットワークに対して診断を実行したりすることができます。

[ステータス] > [ゲートウェイ]

[ステータス] - [ゲートウェイ] ページには、ゲートウェイに関する情報と現在の設定が表示されます。表示される情報は、使用するインターネット接続のタイプによって異なります。

[ゲートウェイ] タブを選択して、[ステータス] - [ゲートウェイ] 画面を開きます。[リフレッシュ] をクリックして、画面に表示されているデータを更新します。



次の表の説明と手順を使用して、ゲートウェイのステータスとインターネット接続を確認します。

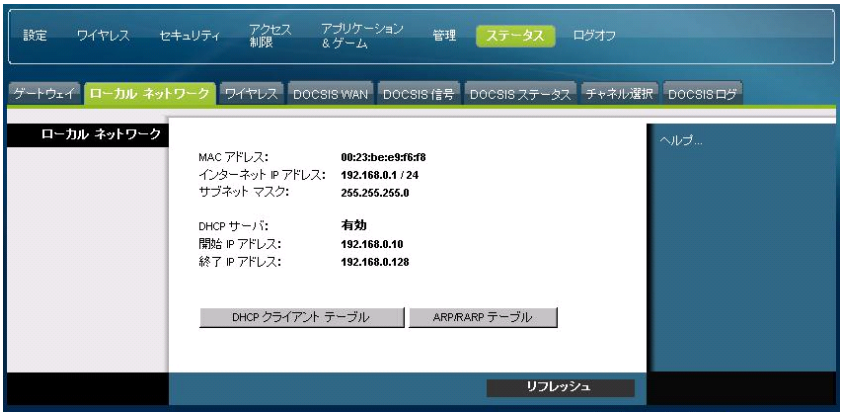
セクション	フィールドの説明
[ゲートウェイ情報]	[ファームウェアのバージョン] ファームウェアのバージョン番号。 [MAC アドレス] ヘッドエンドの CMTS（Cable Modem Termination System）への接続に使用する、ケーブル モデムの同軸インターフェイスに固有の英数字のアドレス。MAC（Media Access Control）アドレスは、ネットワークの各ノードを一意に識別するハードウェアのアドレスです。 [現在の日時] [基本設定] ページで選択したタイムゾーンに基づいた時間が表示されます。

セクション	フィールドの説明
[インターネット接続]	[インターネット IP アドレス] WAN インターフェイスの IP アドレスが表示されます。オンラインになると、このアドレスがゲートウェイに割り当てられます。 [サブネット マスク] WAN ポートのサブネット マスクが表示されます。スタティック IP アドレスが設定されている場合を除き、このアドレスが ISP によって WAN ポートに自動的に割り当てられます。 [デフォルト ゲートウェイ] ISP のデフォルト ゲートウェイの IP アドレス。 [DNS1-3] ゲートウェイで現在使用している DNS IP アドレス。 [WINS] ゲートウェイで現在使用している WINS IP アドレス。

[ステータス] > [ローカル ネットワーク]

[ステータス] - [ローカル ネットワーク] ページには、ローカル エリア ネットワークのステータスに関する情報が表示されます。

[ローカル ネットワーク] タブを選択して、[ステータス] - [ローカル ネットワーク] ページを開きます。[リフレッシュ] をクリックして、ページ上のデータを更新します。

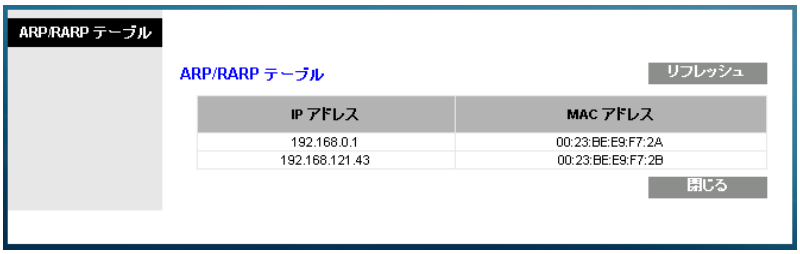


次の表を使用して、ゲートウェイのステータスとインターネット接続を確認します。

セクション	フィールドの説明
[ローカル ネットワーク]	[MAC アドレス] プライベート LAN ホーム ネットワークに固有の英数字のアドレス。MAC アドレスは、ネットワークの各ノードを一意に識別するハードウェア アドレスです。 [インターネット IP アドレス]

セクション	フィールドの説明
	LAN サブネットの IP アドレスが表示されます。 [サブネット マスク] LAN のサブネット マスクが表示されます。 [DHCP サーバ] ローカル DHCP サーバのステータス([有効] または [無効])が表示されます。 [開始 IP アドレス] ゲートウェイの DHCP サーバで使用される IP アドレスの範囲の始まりが表示されます。 [終了 IP アドレス] DHCP サーバで使用される IP アドレスの範囲の終わりが表示されます。
[DHCP クライアント テーブル]	[DHCP クライアント テーブル] をクリックすると、ゲートウェイの DHCP サーバによって IP アドレスが発行されている LAN 接続デバイスが表示されます。[DHCP クライアント テーブル] ページには、DHCP クライアント(コンピュータとその他のネットワーク デバイス)のリストが、クライアント ホスト名、IP アドレス、MAC アドレス、および割り当てられた IP アドレスが期限切れになるまでの時間とともに表示されます。最新の情報を取得するには、[リフレッシュ] をクリックします。このページを終了し、[ローカル ネットワーク] ページに戻るには、[閉じる] をクリックします。 次の図は、[DHCP クライアント テーブル] の例を示しています。 

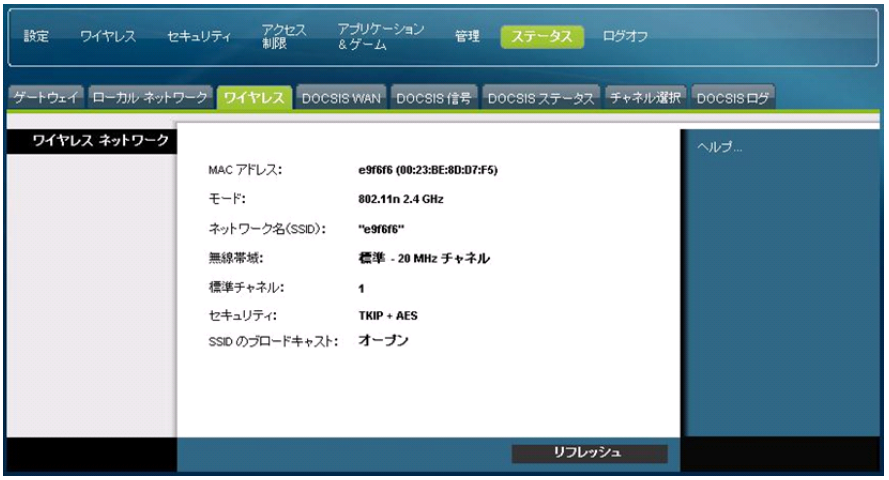
[ARP/RARP テーブル]	[ARP/RARP テーブル] をクリックすると、ネットワークに接続するすべてのデバイスのリストが表示されます。最新の情報を取得するには、[Refresh] をクリックします。このページを終了し、[ローカル ネットワーク] ページに戻るには、[閉じる] をクリックします。 次の図は、[ARP/RARP テーブル] の例を示しています。



[ステータス] > [ワイヤレス]

[ステータス] - [ワイヤレス ネットワーク] ページには、ゲートウェイのワイヤレス ネットワークに関する基本情報が表示されます。

[ワイヤレス] タブを選択して、[ステータス] - [ワイヤレス] ページを開きます。[リフレッシュ] をクリックして、ページ上のデータを更新します。



[ステータス] - [ワイヤレス] ページの説明

次の表を使用して、ワイヤレス ネットワークのステータスを確認します。

セクション	フィールドの説明
[ワイヤレス ネットワーク]	[MAC アドレス] ゲートウェイのローカル ワイヤレス アクセス ポイントの MAC アドレスが表示されます。 [モード] 次のいずれかの現在使用されている無線周波数帯が表示されます。 ■ [2.4 GHz] ■ [5 GHz] ■ [2.4 and 5 GHz] **注**: すべての製品で 5 GHz 無線帯域がサポートされているわけではありません。 [ネットワーク名（SSID）] ワイヤレス アクセス ポイントの名前または Service Set Identifier（SSID）が表示されます。 [無線帯域] [ワイヤレス] - [基本設定] ページで選択したチャネル帯域設定が表示されます。 [標準チャネル] [ワイヤレス] - [基本設定] ページで選択した標準チャネル設定が表示されます。 [セキュリティ] ワイヤレス ネットワークで使用されるセキュリティ方法が表示されます。 [SSID のブロードキャスト] ゲートウェイの SSID ブロードキャスト機能のステータスが表示されます。

[ステータス] > [DOCSIS WAN]

[ステータス] - [DOCSIS WAN] には、ケーブル モデムのシステムに関する情報が表示されます。

[DOCSIS WAN] タブを選択して、[ステータス] - [DOCSIS WAN] ページを開きます。

[DOCSIS WAN] ページの説明

次の表の説明と手順を使用して、DOCSIS WAN ネットワークのステータスを確認します。

セクション	フィールドの説明
[製品情報]	[モデル] レジデンシャル ゲートウェイの名前が表示されます。
	[ベンダー] レジデンシャル ゲートウェイのメーカーが表示されます。
	[ハードウェアのリビジョン] 回路基板設計のリビジョンが表示されます。
	[シリアス ナンバー] レジデンシャル ゲートウェイに固有のシリアル番号が表示されます。

セクション	フィールドの説明
	[MAC アドレス] CM MAC アドレスが表示されます。CM MAC アドレスは、ヘッドエンドで CMTS への接続に使用される、ケーブル モデムの同軸インターフェイスに固有の英数字のアドレスです。MAC アドレスは、ネットワークの各ノードを一意に識別するハードウェア アドレスです。
	[ブートローダのリビジョン] ブートローダのリビジョン コード バージョンが表示されます。
	[現在のソフトウェア リビジョン] ファームウェイのリビジョン バージョンが表示されます。
	[ファームウェア名] ファームウェイの名前が表示されます。
	[ファームウェア ビルド日時] ファームウェアが作成された日時が表示されます。
	[ケーブル モデムのステータス] ゲートウェイの現在のステータスが表示されます。
[ダウンストリーム チャネル]	[チャネル 1-8] アクティブなダウンストリーム チャネルの電力レベルと信号対雑音比が表示されます。
[アップストリーム チャネル]	[チャネル 1-4] アクティブなアップストリーム チャネルの電力レベルが表示されます。

よく寄せられる質問

Q.　ケーブル TV に加入していないと、どうなりますか。

A.　お住まいの地域でケーブル TV を利用できない場合でも、ケーブル TV サービスへの加入の有無にかかわらず、データ サービスを利用できる場合があります。高速インターネット アクセスを含むケーブル サービスの詳細については、お近くのケーブルテレビ局にお問い合わせください。

Q.　インストール（取り付け）を手配するには、どうしたらよいですか。

A.　専門スタッフへのインストール（取り付け）の依頼については、ケーブルテレビ局にお問い合わせください。専門スタッフに依頼することで、モデムや PC へのケーブルの接続やハードウェアおよびソフトウェアの設定を適切に行えます。インストール（取り付け）の詳細については、ケーブルテレビ局にお問い合わせください。

Q.　レジデンシャル ゲートウェイはどのようにコンピュータに接続されますか。

A.　レジデンシャル ゲートウェイは、ワイヤレス接続または PC の 10/100/1000BASE-T イーサネット ポートを使用して PC に接続されます。イーサネットインターフェイスを使用する場合、イーサネット カードはお近くの PC または事務用品販売店、またはケーブルテレビ局から購入できます。イーサネット接続で最適なパフォーマンスを実現するには、PC にギガビット イーサネット カードを取り付ける必要があります。

Q.　レジデンシャル ゲートウェイが接続された後、インターネットにアクセスするにはどうしたらよいですか。

A. 地域のケーブルテレビ局が ISP（インターネット サービス プロバイダー）となります。ケーブルテレビ局は、電子メール、チャット、ニュース、および情報サービスなどの広範なサービスを提供します。また、必要なソフトウェアもケーブルテレビ局から提供されます。

Q.　TV 鑑賞とインターネットを同時に利用することはできますか。

A.　もちろん可能です。ケーブル テレビ サービスに加入している場合は、オプションのケーブル信号スプリッタを使用して TV とレジデンシャル ゲートウェイをケーブル ネットワークに接続することにより、TV 鑑賞とレジデンシャル ゲートウェイの使用を同時に行うことができます。

よくあるトラブルシューティング問題

前面パネルのステータス インジケータの意味がわからない

前面パネルの LED ステータス インジケータの動作と機能の詳細については、「***前面パネルの LED ステータス インジケータの機能***」（89 ページ）を参照してください。

レジデンシャル ゲートウェイでイーサネット接続が登録されない

- コンピュータにイーサネット カードが取り付けられていること、また、イーサネット ドライバ ソフトウェアが適切にインストールされていることを確認します。購入したイーサネット カードを取り付ける場合は、取り付け手順に従って慎重に行ってください。
- 前面パネルのステータス インジケータ ランプのステータスを確認します。

ハブに接続後、レジデンシャル ゲートウェイでイーサネット接続が登録されない

レジデンシャル ゲートウェイに複数の PC を接続している場合は、適切なクロス ケーブルを使用して、最初にモデムをハブのアップリンク ポートに接続する必要があります。ハブの LINK LED が、継続的に点灯します。

レジデンシャル ゲートウェイでケーブル接続が登録されない

- モデムは、標準の 75-ohm RF 同軸ケーブルで動作します。異なるケーブルを使用している場合、レジデンシャル ゲートウェイは正常に機能しません。適切なケーブルを使用しているかどうかを確認するには、ケーブルテレビ局にお問い合わせください。
- NIC カードインターフェイスに不具合がある可能性があります。NIC まのマニュアルのトラブルシューティング情報を参照してください。

パフォーマンス向上のためのヒント

確認と修正

レジデンシャル ゲートウェイが予想どおりに動作しない場合、次のヒントが役に立つことがあります。詳細については、ケーブルテレビ局にお問い合わせください。

- レジデンシャル ゲートウェイの AC 電源のプラグがコンセントにしっかり差し込まれていることを確認します。
- レジデンシャル ゲートウェイの AC 電源のプラグが差し込まれているコンセントが、壁スイッチで制御されていないことを確認します。壁スイッチでコンセントが制御されている場合は、スイッチが **ON** の位置にあることを確認します。
- レジデンシャル ゲートウェイの前面パネルにある **ONLINE** LED ステータス インジケータが点灯していることを確認します。
- ケーブル サービスがアクティブであること、また、双方向サービスがサポートされていることを確認します。
- すべてのケーブルが正しく接続されていること、また、適切なケーブルを使用していることを確認します。
- イーサネット接続を使用している場合は、TCP/IP を正しくインストールし、設定していることを確認します。
- レジデンシャル ゲートウェイのシリアル番号と MAC アドレスをケーブルテレビ局に連絡済みであることを確認します。
- ケーブル信号スプリッタを使用して、他のデバイスにレジデンシャル ゲートウェイを接続できるようにしている場合は、スプリッタを取り外し、レジデンシャル ゲートウェイがケーブル入力に直接接続されるようにケーブルをつなぎなおします。この時点でレジデンシャル ゲートウェイが正常に機能していれば、ケーブル信号スプリッタに欠陥がある可能性があり、交換が必要とされる場合もあります。
- イーサネット接続での最適なパフォーマンスを実現するには、PC にギガビット イーサネット カードを取り付ける必要があります。

前面パネルの LED ステータス インジケータの機能

初期電源投入、キャリブレーション、および登録(AC 電源適用)

次の表は、AC 電源がレジデンシャル ゲートウェイに適用されたときのネットワークでの電源投入、キャリブレーション、および登録時における一連のステップと、対応するレジデンシャル ゲートウェイ前面パネルの LED ステータス インジケータの状態を示します。この表を使用して、レジデンシャル ゲートウェイの電源投入、キャリブレーション、および登録プロセスに対するトラブルシューティングを行ってください。

注:レジデンシャル ゲートウェイでステップ 6(高速データ プロビジョニング ファイルの要求)が完了すると、モデムはただちに通常動作に入ります。「***通常動作(AC 電源適用)***」(91 ページ)を参照してください。

初期電源投入、キャリブレーション、および登録時の前面パネルの LED ステータス インジケータ							
		高速データ登録					
ステップ		1	2	3	4	5	6
前面パネル インジケータ		セルフテスト	ダウンストリーム スキャン	ダウンストリーム信号ロック	レンジング	IP アドレスの要求	高速データ プロビジョニング ファイルの要求
1	POWER	点灯	点灯	点灯	点灯	点灯	点灯
2	DS	点灯	点滅	点灯	点灯	点灯	点灯
3	US	点灯	消灯	消灯	点滅	点灯	点灯
4	ONLINE	点灯	消灯	消灯	消灯	消灯	点滅
5	ETHERNET 1～4	点灯	点灯または点滅	点灯または点滅	点灯または点滅	点灯または点滅	点灯または点滅
6	WIRELESS LINK	消灯	点灯または点滅	点灯または点滅	点灯または点滅	点灯または点滅	点灯または点滅
7	WIRELESS SETUP	消灯	点灯または点滅	点灯または点滅	点灯または点滅	点灯または点滅	点灯または点滅

前面パネルの LED ステータス インジケータの機能

初期電源投入、キャリブレーション、および登録時の前面パネルの LED ステータス インジケータ		
高速データ登録（続き）		
ステップ		7
前面パネル インジケータ		データ ネットワーク登録の完了
1	POWER	点灯
2	DS	点灯
3	US	点灯
4	ONLINE	点灯
5	ETHERNET 1～4	点灯または点滅
6	WIRELESS LINK	点灯または点滅
7	WIRELESS SETUP	消灯

通常動作(AC 電源適用)

次の図は、AC 電源がゲートウェイに適用されたときの通常動作時のレジデンシャル ゲートウェイ前面パネル LED ステータス インジケータの状態を示しています。

通常動作時の前面パネルの LED ステータス インジケータ

前面パネル インジケータ		通常動作
1	POWER	点灯
2	DS	点灯
3	US	点灯
4	ONLINE	点灯
5	ETHERNET 1 ～ 4	■ 点灯:1 台のデバイスがイーサネット ポートに接続され、モデムとの間でデータが送受信されていない場合 ■ 点滅:1 台のイーサネット デバイスだけが接続されており、CPE(宅内機器)とワイヤレス ホーム ゲートウェイの間でデータが送信されている場合 ■ 消灯:イーサネット ポートに接続しているデバイスがない場合
6	WIRELESS LINK	■ 点灯:ワイヤレス アクセス ポイントが有効であり、動作可能である場合 ■ 点滅:CPE とワイヤレス ホーム ゲートウェイの間でデータが送信されている場合 ■ 消灯:ユーザによってワイヤレス アクセス ポイントが無効にされている場合
7	WIRELESS SETUP	■ 消灯:ワイヤレス設定がアクティブでない場合 ■ 点滅:ワイヤレス ネットワーク上に新規のワイヤレス クライアントを追加するためのワイヤレス設定がアクティブである場合

特別な状況

次の表は、ネットワーク アクセスが拒否されていることを示す、特別な状況におけるケーブル モデム前面パネルの LED ステータス インジケータの状態を示します。

特別な状況における前面パネルの LED ステータス インジケータ

前面パネル インジケータ		ネットワーク アクセスの拒否
1	POWER	ゆっくり点滅 1 秒に 1 回
2	DS	ゆっくり点滅 1 秒に 1 回
3	US	ゆっくり点滅 1 秒に 1 回
4	ONLINE	ゆっくり点滅 1 秒に 1 回
5	ETHERNET 1 ～ 4	ゆっくり点滅 1 秒に 1 回
6	WIRELESS LINK	ゆっくり点滅 1 秒に 1 回
7	WIRELESS SETUP	ゆっくり点滅 1 秒に 1 回

通告

商標

Cisco および Cisco ロゴは、米国およびその他の国における Cisco およびその関連会社の商標または登録商標です。Cisco の商標の一覧は **www.cisco.com/go/trademarks** に掲載されています。DOCSIS は Cable Television Laboratories, Inc. の登録商標です。EuroDOCSIS、EuroPacketCable、および PacketCable は Cable Television Laboratories, Inc. の商標です。Wi-Fi Protected Setup マークは Wi-Fi Alliance のマークです。Wi-Fi Protected Setup は Wi-Fi Alliance の商標です。

本書に記載されているその他のサードパーティの商標は各社の所有物です。

本書で使用されている「パートナー」という用語は、シスコとのパートナー関係を意味するものではありません。 1009R

免責事項

Cisco Systems, Inc.（以下、シスコ）は、本書の内容に含まれる誤りまたは不備に関して、いかなる責任も負いません。シスコは、事前に通告することなくいつでも、本書の内容を変更する権利を留保します。

ワイヤレスの最大パフォーマンスは、IEEE 標準 802.11 の仕様から導出されています。低いワイヤレス ネットワーク キャパシティ、データ スループット レート、範囲、およびカバレッジなど、実際のパフォーマンスはさまざまです。パフォーマンスは、アクセス ポイントからの距離、ネットワーク トラフィックの量、建築資材や構造、使用するオペレーティング システム、使用する多様なワイヤレス製品、干渉、およびその他の不利な条件を含むさまざまな要因、条件、および変動要素によって決まります。

マニュアルの著作権情報

本書に記載されている内容は、予告なしに変更されることがあります。本書に記載されている内容は、その形式を問わず、シスコの書面による同意なしに複製することはできません。

ソフトウェアおよびファームウェアの使用

本書に掲載されているソフトウェアは、著作権法によって保護されており、ライセンス契約書に基づいてお客様に提供されます。このソフトウェアは、ライセンス契約書の規定に従って使用またはコピーすることができます。

この機器のファームウェアは、著作権法によって保護されています。この機器に搭載されているファームウェアは、この機器でのみ使用できます。シスコの書面による承諾なしに、このファームウェアまたはその一部を複製または配布することは禁じられています。

お問い合わせ

お問い合わせ先

設定および技術的な質問に関しましては、ご契約のケーブルテレビ局にお問い合わせください。

製品仕様

RF ダウンストリーム	仕様
周波数帯域	88 MHz ～ 1002 MHz
チューナー	32 MHz バンドパス周波数チューナー×2
復調方式	8 デモジュレーション、各モジュレーション 64 QAM または 256 QAM
最大伝送速度	8 下りチャンネル 各チャンネル：43 Mbps（256 QAM）/30 Mbps (64 QAM)
チャンネル帯域幅	6 MHz
動作レベルレンジ	-15 dBmV ～ +15 dBmV
入力インピーダンス	75 ohms
RF アップストリーム	**仕様**
周波数帯域	5 MHz ～ 65 MHz
最大伝送速度	4 上りチャンネル
最大伝送速度/チャンネル	Modulation / Channel Bandwidth (MHz) / Raw Data Rate (Mbps) QPSK 1.6 2.56 16QAM 1.6 5.12 QPSK 3.2 5.12 16QAM 3.2 10.24 32QAM 3.2 12.8 64QAM 3.2 15.4 16QAM 6.4 20.5 32QAM 6.4 25.6 64QAM 6.4 30.72
チャンネル帯域幅	0.2, 0.4, 0.8, 1.6, 3.2, 6.4 MHz
最大信号モデム入力レベル A-TDMA/TDMA	One Channel / 2 Channels / 3 or 4 Channels QPSK +61 dBmV +58 dBmV +55dBmV 8QAM +58 dBmV +55 dBmV +52dBmV 16QAM +58 dBmV +55 dBmV +52dBmV 32QAM +57 dBmV +54 dBmV +51dBmV 64QAM +57 dBmV +54 dBmV +51dBmV
SCDMA	QPSK +56 dBmV +53 dBmV +53 dBmV 8QAM +56 dBmV +53 dBmV +53 dBmV 16QAM +56 dBmV +53 dBmV +53 dBmV 32QAM +56 dBmV +53 dBmV +53 dBmV 64QAM +56 dBmV +53 dBmV +53 dBmV 128QAM +56 dBmV +53 dBmV +53 dBmV
チャンネル帯域幅	0.2, 0.4, 0.8, 1.6, 3.2, 6.4 MHz

無線 LAN インターフェイス	仕様
無線 LAN 規格	802.11 b/g/n
周波数帯	2.4 GHz
アンテナ（内臓アンテナ）	送信 2 × 受信 2
セキュリティ	WPA2-PSK, WPA-PSK
パワーマネージメント機能	WMM Power Save
自動セットアップ	WPS
リピータ機能	Wireless Bridging - WDS (Wireless Distribution System
RADIUS 認証	Client, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MD5
MBSSID 数	8
電気	仕様
AC アダプタ	入力 AC100V（50/60Hz） 36VA 出力 15VDC-1.2A
消費電力	11.54 ワット以下
データーポート	GigE (Auto-negotiate with Auto-MDIX): RJ-45 Ethernet x（4）
RF インターフェイス	F 型
出力インピーダンス	75 Ω
メカ仕様	仕様
寸法	幅 14.5 cm x 奥行 17.6 cm x 高さ 5cm （本体のみ、突起物を除く）
重さ	0.390 kg
動作温度	-0˚ ～ 40˚C
動作湿度	0 ～ 95%（結露がない事）
耐久温度	-20˚ ～ 70˚C
VCCI	VCCI クラス B

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678.277.1120
800 722.2009
www.cisco.com

2011 年 1 月

製品番号 4040246 Rev A