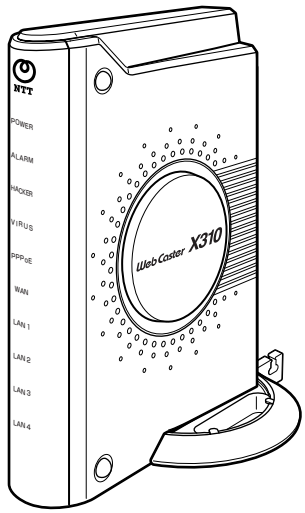
NTT

Web Caster X310
詳細取扱説明書

このたびは、Web Caster X310をお買い求めいただきまして、まことにありがとうございます。

- ●ご使用の前に、この「詳細取扱説明書」をよくお読みのうえ、内容を理解してからお使いください。
- ●お読みになったあとも、本商品のそばなどいつも手もとに置いてお使いください。



技術基準適合認証品

目　次

2 こんなときにはこの設定

3 付録

マニュアルの見かた

本商品のマニュアルの見かたについて説明します。
本書は下記のように構成されています。

1 Web 設定

Web 設定について説明します。
この章では画面単位で用途や操作方法について説明しています。

2 こんなときにはこの設定

本商品の機能を使うときの設定方法について説明します。

3 付録

本商品の設定に関連する用語集です。

1 Web設定

Web 設定画面について

本商品は、Web ブラウザで Web 設定画面を開いて、各種設定を行います。

ログインする

Web 設定画面を開くには、ログインの操作を行います。

1 本商品に接続したパソコンで Web ブラウザを起動する。

2 Web ブラウザのアドレス欄に「http://192.168.0.1」と入力し、[Enter] キーを押す。

または、「http://wbc_x310」と入力します。

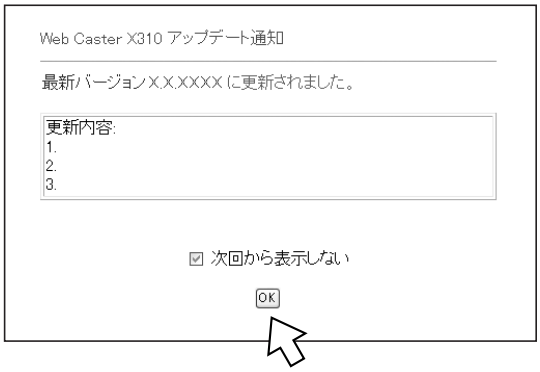
3 ログインパスワードを入力し、[OK] をクリックする。

ログインパスワードは、かんたん設定（☛P1-6）手順３で設定したパスワードを入力します。
Web 設定画面のホーム画面が表示されます。

ワンポイント

● **手順３のあとにアップデート通知画面が表示されたときは**
「対象ファイルのアップデートについて」のワンポイント「●アップデート通知画面」（☛P1-22）へ進んでください。

● **手順３のあとに最新バージョンへ更新されたことをお知らせする画面が表示されたときは**
最新バージョンへ更新されたことをお知らせする画面が表示されたときは、[OK] をクリックします。Web 設定画面のホーム画面が表示されます。



※画面は例です。

お知らせ

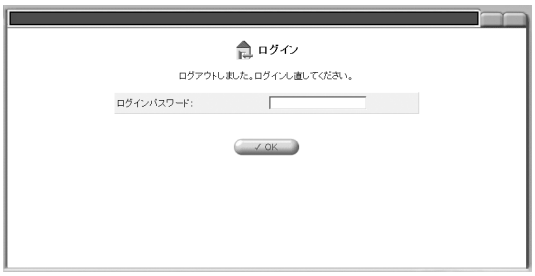
● Web 設定画面は、本商品の設定画面を Web ブラウザで表示する画面ですので、インターネットに接続する必要はありません。
● Web ブラウザは、ホームページを見るためのソフトウェアです。代表的なブラウザとして、Microsoft® Internet Explorer、Netscape Navigator® があります。

ログアウトする

本商品の設定を終了するときは、ログアウトの操作を行います。

1 [ログアウト] をクリックする。

右の画面が表示されたら、ウィンドウを閉じて終了します。



お知らせ

● ログアウトする前に Web ブラウザを閉じた場合は、次回 Web 設定画面を開くときにログインが必要です。

Web 設定画面について

ホーム画面について

ログインすると、Web 設定画面のホーム画面が表示されます。
ホーム画面では、本商品のファームウェア、セキュリティ対策ファイルの現在のバージョンと最新バージョンを確認することができます。

[対象ファイルのバージョン]
ファームウェアとセキュリティ対策ファイルの「現在のバージョン」と「最新バージョン」が表示されています。

[最新情報の取得]
バージョン情報を更新するときにクリックします。

[最新バージョンのダウンロード]
対象ファイルの手動アップデートを実行します。（☛P1-65）

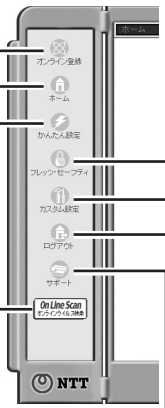
「ホーム画面」

お知らせ

- 本商品を再起動（☛P1-75）した場合、最初にログインしたときはホーム画面の最新バージョン欄に「更新の確認に失敗しました。」と表示されます。［最新情報の取得］をクリックすると、最新バージョンが表示されます。
- 最新バージョン欄に「更新の確認に失敗しました。」と表示されているときは、フレッツ・セーフティのオンライン登録をしていないか、または最新情報の取得に失敗したことを示しています。
- フレッツ・セーフティのオンライン登録済の場合で、「更新の確認に失敗しました。」と表示されるときは、サーバとの接続に失敗した可能性がありますので、しばらく待ってからもう一度確認してください。
- フレッツ・セーフティのオンライン登録をしていない場合は、セキュリティ対策ファイルの最新バージョンの取得はできません。
- Web ブラウザのキャッシュのタイムアウトなどにより、Web 設定画面が正しく表示されないことがあります。このときは、Web ブラウザの［更新］ボタンなどを押して、再度 Web 設定画面を表示してください。
- 画面はお使いのパソコンによって一部異なる場合があります。

Web 設定画面の基本操作

Web 設定の各画面では、左側のアイコンをクリックすると、各機能の画面へ移動することができます。



[オンライン登録]
オンライン登録や状態についてのメッセージが表示されます。
クリックすると、サーバにアクセスします。

[ホーム]
ホーム画面に戻ります。

[かんたん設定]
本商品を接続してご利用開始になるまでに最低限必要な設定を行います。

[オンラインウイルス検索]
オンラインウイルス検索を行います。

[フレッツ・セーフティ]
フレッツ・セーフティの設定を行います。

[カスタム設定]
ログインパスワードの変更、設定情報の読み込み／保存、ファームウェアのアップデートなどを行います。

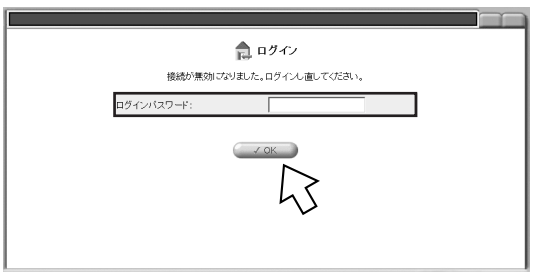
[ログアウト]
ログアウトします。

[サポート]
サポート情報を表示します。

ワンポイント

● **前の画面に戻るには**
［戻る］をクリックすると、1 つ前の画面に戻ります。

● **約 15 分間、なにも操作しないと**
約 15 分間、なにも操作をしないと、ログアウトします。Web 設定画面のいずれかのボタンをクリックすると、ログイン画面が表示されます。ログインパスワードを入力し、［OK］をクリックすると、ホーム画面に戻ります。



かんたん設定

本商品に初めてログインしたときは、かんたん設定でログインパスワードの設定、エリアの選択、接続方法の設定、フレッツ・セーフティの設定を行います。

1 本商品に接続したパソコンで Web ブラウザを起動する。

2 Web ブラウザのアドレス欄に「http://192.168.0.1」と入力し、[Enter] キーを押す。

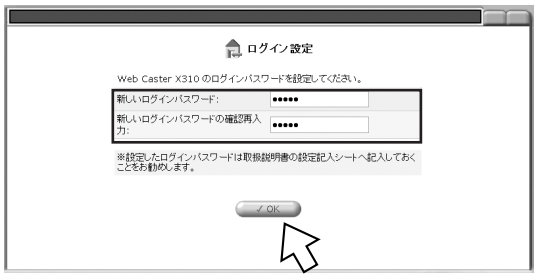
または、「http://wbc_x310」と入力します。

3 ログインパスワードを設定する。

本商品の Web 設定にログインするためのパスワードを設定します。
［新しいログインパスワード］に、任意の文字を半角英数字記号 64 文字以内で入力します。半角スペースも入力できます。
入力したパスワードは、●●●または＊＊＊で 18 桁まで表示されます。
18 文字を超えて入力された場合、18 桁以上は表示されませんが、入力したパスワードは記録されていますので問題ありません。

［新しいログインパスワードの確認再入力］に、もう一度、同じパスワードを入力し、［OK］をクリックします。

※パスワードを空欄のままにすることもできますが、パスワードを設定しないとセキュリティ上のリスクを高めることになります。
※パスワードは、忘れないように必ずメモして安全な場所に保管してください。設定記入シートに記入しておくことをお勧めします。（☛ 取扱説明書 P6-3）
※パスワードを忘れた場合は、本商品を初期化して設定を初めからやり直してください。（☛P1-76「初期化」）



お知らせ

- Web 設定画面は、本商品の設定画面を Web ブラウザで表示する画面ですので、インターネットに接続する必要はありません。
- 入力したパスワードの表示桁数は、お使いのパソコンによって異なる場合があります。
- 画面はお使いのパソコンによって一部異なる場合があります。

4 ホーム画面が表示されたら、［かんたん設定］をクリックする。

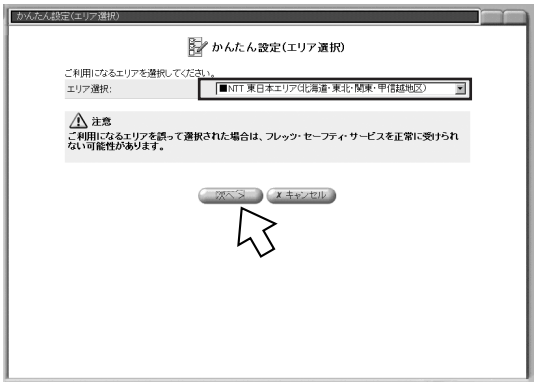
5 エリアを選択する。

お住まいの地域に合わせて次のどちらかのエリアを選択し、［次へ］をクリックします。

［NTT 東日本エリア（北海道・東北・関東・甲信越地区）］：
北海道、東北、関東、甲信越地区にお住まいのお客様

［NTT 西日本エリア（東海・北陸・近畿・中国・四国・九州地区）］：
東海、北陸、近畿、中国、四国、九州地区にお住まいのお客様

※エリアを誤って選択された場合は、フレッツ・セーフティのサービスを正常に受けられない可能性があります。



ワンポイント

● 前の画面に戻るには

［戻る］をクリックすると、1 つ前の画面に戻り、設定し直すことができます。

6 インターネットへの接続方法を選択する。

ここでは［PPPoE を使用して接続する場合］を選択し、［次へ］をクリックします。

（次ページへ続きます）

かんたん設定

ワンポイント

● **PPPoE を使用しないで接続する場合**

IP 電話対応 ADSL モデムをすでにご利用のお客様は、［PPPoE を使用しないで接続する場合］を選択して［次へ］をクリックしてください。次の画面で［動的な IP アドレス設定］を選択し、［次へ］をクリックして手順 8 へ進みます。

※ IP 電話対応 ADSL モデムと本商品の詳しい設定については、2 章を参照してください。（☛P2-2「IP 電話対応 ADSL モデムと本商品を接続して利用するには」）

● **PPPoE 以外の接続で固定の IP アドレスを設定する場合（☛P1-10）**

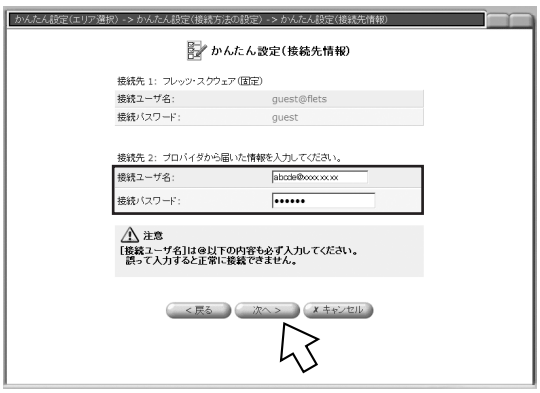
7 接続先を設定する。

①［接続先 1］は、フレッツ・セーフティに接続するため、フレッツ・スクウェアに固定されています。選択したエリアによって自動設定されます。

②［接続先 2］の［接続ユーザ名］、［接続パスワード］に、プロバイダから通知された情報を入力し、［次へ］をクリックします。

プロバイダによっては、呼び方が異なる場合がありますのでご注意ください。
［接続ユーザ名］は、@ 以下の内容も必ず入力してください。誤って入力すると、正常に接続できません。
＜例＞ abc@xxxxx.xx.xx

［接続ユーザ名］は、半角英数字記号（「;」、「"」を除く）64 文字まで入力できます。
［接続パスワード］は、半角英数字記号 64 文字まで入力できます。半角スペースも入力できます。
入力したパスワードは、●●●または＊＊＊で 19 桁まで表示されます。
19 文字を超えて入力された場合、19 桁以上は表示されませんが、入力したパスワードは記録されていますので問題ありません。

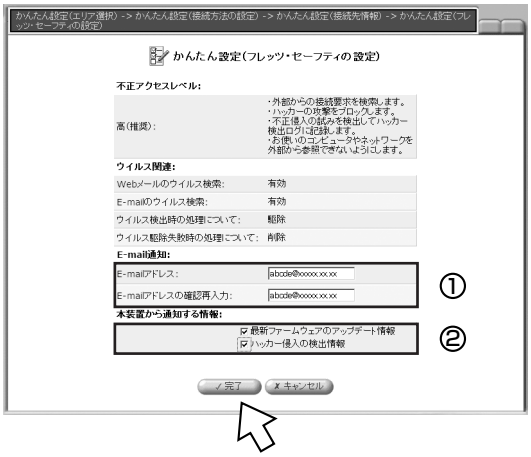


お知らせ

● 入力したパスワードの表示桁数は、お使いのパソコンによって異なる場合があります。

8 フレッツ・セーフティの設定をする。

本商品のファームウェアがアップデートできるようになったとき、ハッカーの不正アクセスが検出されたときに、メールで通知されるようにします。



●E-mail 通知／本装置から通知する情報：

① [E-mail アドレス] に、お持ちの E-mail アドレスを入力します。
　半角英数字記号 100 文字まで入力できます。
　[E-mail アドレスの確認再入力] に、もう一度、同じ E-mail アドレスを入力します。

② [本装置から通知する情報] の項目をチェックし、[完了] をクリックします。
- [最新ファームウェアのアップデート情報]
  本商品の新しいバージョンのファームウェアに関する情報をメールで受け取ります。
  （お買い求め時：チェックなし）
- [ハッカー侵入の検出情報]
  使用しているパソコンやネットワークへの不正アクセスを検出したときに、通知をメールで受け取ります。（お買い求め時：チェックなし）

■不正アクセスレベル、ウイルス関連の機能は、かんたん設定では自動的に下記のように設定されます。

●不正アクセスレベル：高（推奨）
- 外部からの接続要求を検索します。
- ハッカーの攻撃をブロックします。
- 不正侵入の試みを検出してハッカー検出ログに記録します。
- お使いのコンピュータやネットワークを外部から参照できないようにします。

●ウイルス関連：
送受信メールと Web メールを検索し、ウイルスが検出された場合は駆除します。駆除に失敗したときは感染したファイルを削除します。
- Web メールのウイルス検索：有効
  （Web メールは、Yahoo!メール、HotMail、AOL メールのみに対応しています）
- E-mail のウイルス検索：有効
- ウイルス検出時の処理について：駆除
- ウイルス駆除失敗時の処理について：削除

■設定を変更する場合は、かんたん設定の終了後、「フレッツ・セーフティの設定を変更するには」を参照して設定を変更してください。（☛P1-24）

お知らせ

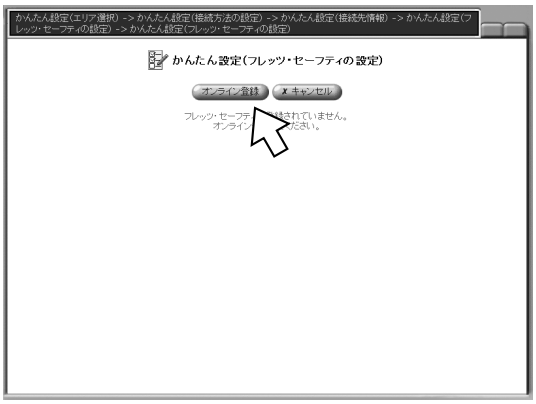
●E-mail アドレスを入力しないと、以下のメールが送られてきません。
- フレッツ・セーフティにオンライン登録がお済みでないお客様あての未登録通知
- [本装置から通知する情報] でチェックした情報

（次ページへ続きます）

かんたん設定

9 右の画面を確認する。

これでかんたん設定は完了です。
本商品を最新のセキュリティ対策機能でお使いいただくためには、本商品のオンライン登録を行い、フレッツ・セーフティへのご契約が必要です。
PPPoE ランプが橙点灯したら、［オンライン登録］をクリックして、登録を行ってください。
「フレッツ・セーフティにオンライン登録する」へ進んでください。（☛P1-12）

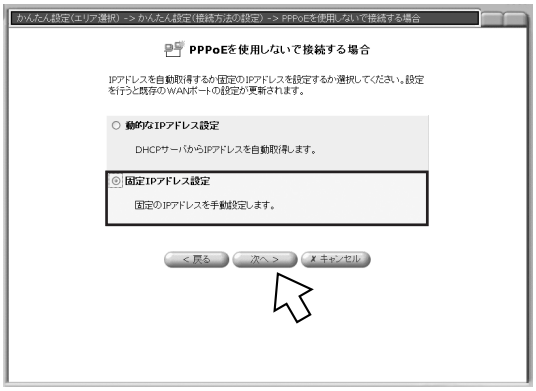


PPPoE 以外の接続で固定の IP アドレスを設定する場合

かんたん設定で次のように設定します。

1 かんたん設定（接続方法の設定）画面で、［PPPoE を使用しないで接続する場合］を選択し、［次へ］をクリックする。

2 ［固定 IP アドレス設定］を選択し、［次へ］をクリックする。



3 IPアドレス、ネットマスク、デフォルトゲートウェイ、DNSサーバなどを設定し、［次へ］をクリックする。

プロバイダから通知された情報を元に入力してください。
ご不明の場合は、ご契約のプロバイダにお問い合わせください。

かんたん設定（フレッツ・セーフティの設定）の画面が表示されます。
以降の操作は、PPPoEを使用して接続した場合と同じです。手順８へ進んでください。（☛P1-9）

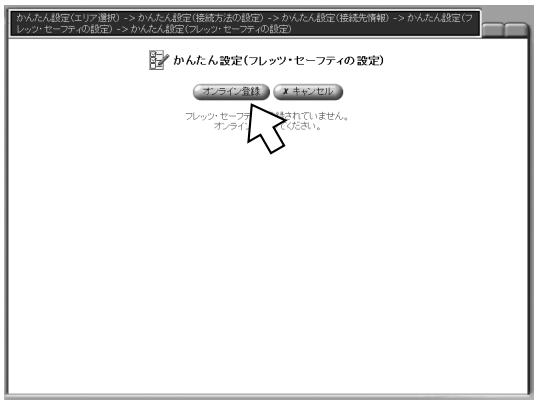
フレッツ・セーフティにオンライン登録する

かんたん設定に引き続き、フレッツ・セーフティにオンライン登録します。
本商品を最新のセキュリティ対策機能でお使いいただくためには、本商品のオンライン登録を行い、フレッツ・セーフティにご契約いただくことが必要です。

1 「かんたん設定（フレッツ・セーフティの設定）」で右の画面を確認したあと、PPPoE ランプが橙点灯したら、［オンライン登録］をクリックする。

［オンライン登録］をクリックしたあと、NTT 東日本、NTT 西日本のホームページが表示されるまでしばらくお待ちください。

以降の手順は、NTT 東日本、NTT 西日本によって異なります。
NTT 西日本をご利用のお客様は P1-19 を参照してください。
NTT 東日本をご利用のお客様は下記へ進みます。



NTT 東日本をご利用のお客様（116 番等で事前に申し込みされている場合）

［オンライン登録］をクリックすると、サービス申込受付ページが表示されます。
フレッツ・セーフティを 116 番等で事前にお申し込みされていない場合は、登録手順が異なりますので、「NTT 東日本をご利用のお客様（116 番等で事前に申し込みされていない場合）」（☛P1-15）を参照してください。

1 お客さま ID とアクセスキーを入力し、［ログイン］をクリックする。

「フレッツ・セーフティご利用状況詳細」画面が表示されます。

お客さま ID（半角英大文字 3 桁＋半角数字 8 桁）とアクセスキー（半角英数字 8 桁）は、B フレッツ、フレッツ・ADSL の開通前にあらかじめお送りした「開通のご案内」をご覧ください。

ワンポイント

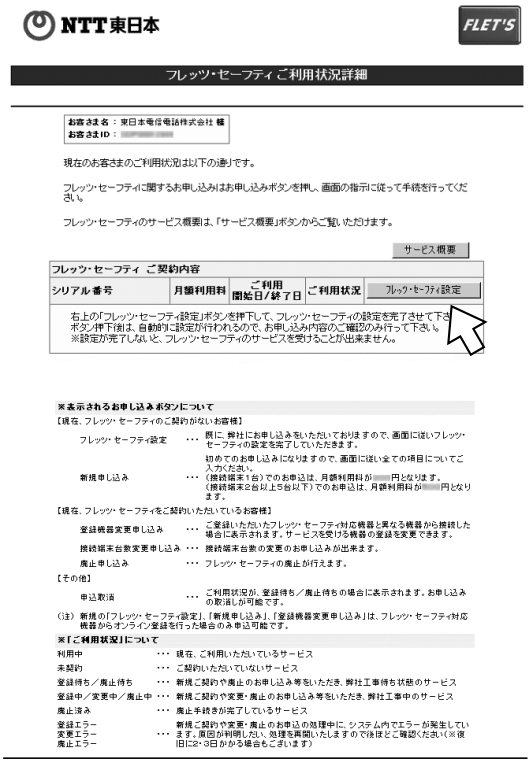
●「開通のご案内」を紛失した場合は
局番なしの「116 番」へご連絡ください。ご本人様確認後、再度「開通のご案内」を送付させていただきます。

お知らせ

- NTT 東日本のお客様で、「接続中のフレッツ・セーフティ対応機器は既に他の回線でご登録中です」と表示された場合は、「セキュリティに関するお問い合わせ（03-5442-7533）」へご連絡ください。NTT 西日本のお客様は、お問い合わせいただいてもご回答できません。
- サービス申込受付ページが正常に表示されないときは、Web ブラウザの［更新］ボタンなどを押して、再度ホームページを表示してください。
- NTT 東日本の各画面は平成 17 年 1 月現在の画面です。

2 [フレッツ・セーフティ設定] をクリックする。

「フレッツ・セーフティ申し込み内容確認」画面が表示されます。



3 ご利用開始日時を確認し、[申し込み] をクリックする。

「フレッツ・セーフティ受付完了」画面が表示されます。

[申し込み] をクリックしたあとは、申し込みの取消・修正はできません。

(次ページへ続きます)

フレッツ・セーフティにオンライン登録する

4 内容を確認し、［閉じる］をクリックする。

これでフレッツ・セーフティの登録は完了です。
お問い合わせの際に、この画面に表示されている情報が必要となることがありますので、印刷するなどして情報を保存してください。

NTT東日本をご利用のお客様（116番等で事前に申し込みされていない場合）

オンライン登録が行われていない場合、または機器交換により登録情報が必要になった場合は、Web設定画面の左上の［オンライン登録］ボタンの上に「フレッツ・セーフティの設定がされていません。」というメッセージが表示されます。
116番等でNTT東日本にフレッツ・セーフティを事前に申し込みされていない場合は、以下の手順でオンライン登録します。

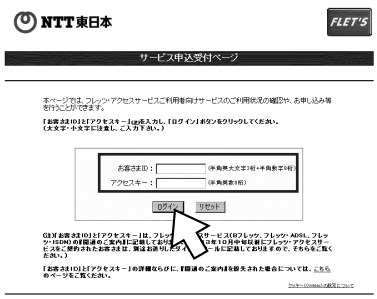
1 Web設定画面で［オンライン登録］をクリックする。

サービス申込受付ページが表示されます。

2 お客さまIDとアクセスキーを入力し、［ログイン］をクリックする。

「フレッツ・セーフティご利用状況詳細」画面が表示されます。

お客さまIDとアクセスキーは、Bフレッツ、フレッツ・ADSLの開通前にあらかじめお送りした「開通のご案内」をご覧ください。



ワンポイント

●**「開通のご案内」を紛失した場合は**
116番へご連絡ください。ご本人様確認後、再度「開通のご案内」を送付させていただきます。

お知らせ

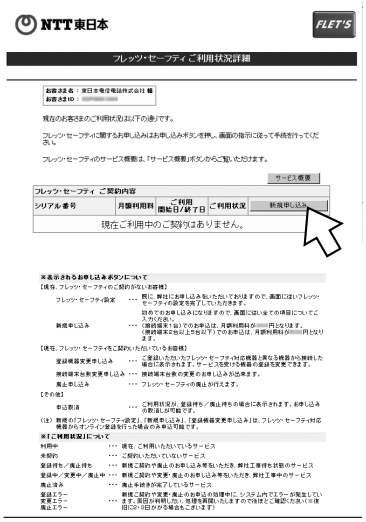
●NTT東日本のお客様で、手順2で「接続中のフレッツ・セーフティ対応機器は既に他の回線でご登録中です」と表示された場合は、「フレッツ・セーフティに関するお問い合わせ（03-5442-7533）」へご連絡ください。NTT西日本のお客様は、お問い合わせいただいてもご回答できません。
●NTT東日本の各画面は平成17年1月現在の画面です。

（次ページへ続きます）

フレッツ・セーフティにオンライン登録する

3 [新規申し込み] をクリックする。

「フレッツ・セーフティ同意書」画面が表示されます。



4 同意書の内容を読み、[同意する] をクリックする。

「フレッツ・セーフティ申込者情報入力」画面が表示されます。

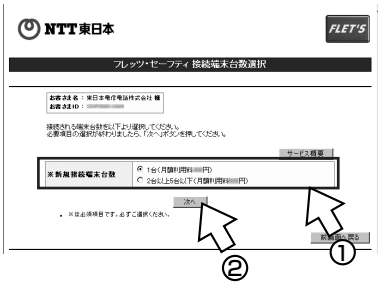
[同意しない] をクリックすると、申し込み手続きをせずに「フレッツ・セーフティご利用状況詳細」画面へ戻ります。

5 申し込まれる方の情報を入力し、［次へ］をクリックする。

「フレッツ・セーフティ接続端末台数選択」画面が表示されます。

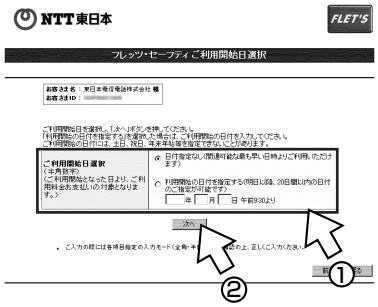
6 接続する端末の台数を入力し、［次へ］をクリックする。

「フレッツ・セーフティご利用開始日選択」画面が表示されます。



7 ご利用開始日を選択し、［次へ］をクリックする。

「フレッツ・セーフティ申し込み内容確認」画面が表示されます。



（次ページへ続きます）

フレッツ・セーフティにオンライン登録する

8 内容を確認し、［申し込み］をクリックする。

「フレッツ・セーフティ受付完了」画面が表示されます。

9 内容を確認し、［閉じる］をクリックする。

これでフレッツ・セーフティの登録は完了です。
お問い合わせの際に、この画面に表示されている情報が必要となることがありますので、印刷するなどして情報を保存してください。

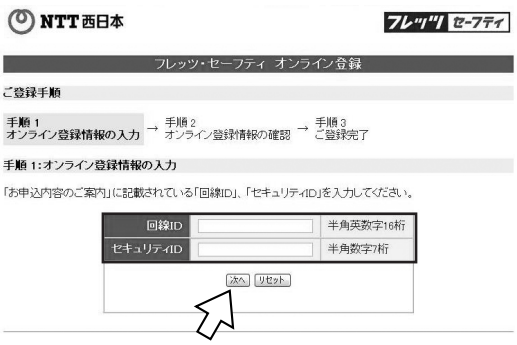
NTT 西日本をご利用のお客様

［オンライン登録］をクリックすると、「フレッツ・セーフティ　オンライン登録　手順 1」画面が表示されます。
オンライン登録を行うには、フレッツ・セーフティを事前にお申し込みいただく必要があります。

1 回線 ID とセキュリティ ID を入力し、［次へ］をクリックする。

「フレッツ・セーフティ　オンライン登録　手順 2」画面が表示されます。

回線 ID（半角英数字 16 桁）とセキュリティ ID（半角数字 7 桁）は、フレッツ・セーフティお申し込み後に NTT 西日本よりお送りした「お申込内容のご案内」をご覧ください。



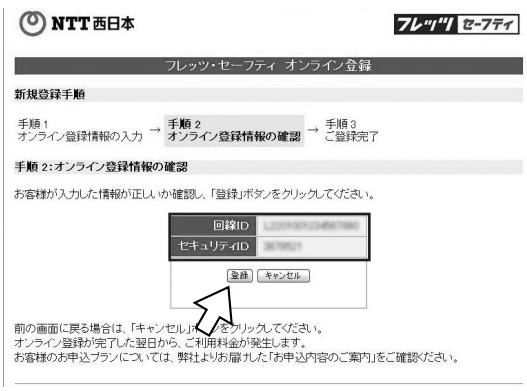
ワンポイント

●「お申込内容のご案内」を紛失した場合は
局番なしの 116 番へご連絡ください。ご本人様確認後、再度「お申込内容のご案内」を送付させていただきます。

2 回線 ID とセキュリティ ID が正しく入力されていることを確認し、［登録］をクリックする。

「フレッツ・セーフティ　オンライン登録　手順 3」画面が表示されます。

間違えて入力した場合は、［キャンセル］をクリックし、前の画面で入力し直します。



お知らせ

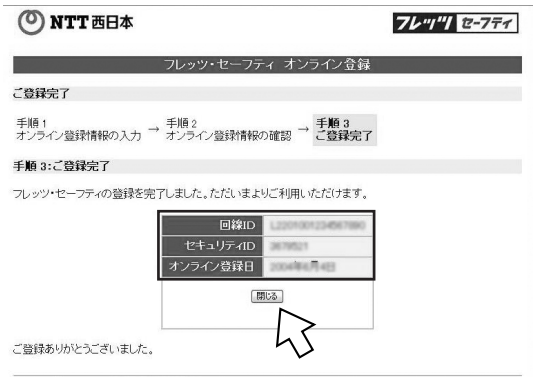
- NTT 西日本の各画面は平成 17 年 1 月現在の画面です。
- フレッツ・セーフティ オンライン登録ページが正常に表示されないときは、Web ブラウザの［更新］ボタンなどを押して、再度ホームページを表示してください。

（次ページへ続きます）

フレッツ・セーフティにオンライン登録する

3 内容を確認し、［閉じる］をクリックする。

これでフレッツ・セーフティの登録は完了です。
お問い合わせの際に、この画面に表示されている情報が必要となることがありますので、印刷するなどして情報を保存してください。



対象ファイルのアップデートについて

本商品は定期的にサーバにアクセスし、最新のファームウェアおよびセキュリティ対策ファイル（パターンファイル、検索エンジン、ファイアウォールルール）のアップデートを実行します。アップデートの対象ファイルと方法は、下記のとおりです。

●アップデートの種類

対象ファイル / アップデートの方法	ファームウェア	セキュリティ対策ファイル※		
		パターンファイル	検索エンジン	ファイアウォールルール
Ⓐ インテリジェントアップデート	—	○	○	○
Ⓑ ファームウェアの自動アップデート	○	—	—	—
Ⓒ 手動アップデート	○	○	○	○
Ⓓ ローカルファイルからの更新	○	—	—	—

※セキュリティ対策ファイルのアップデートを実行するには、フレッツ・セーフティのご契約が必要です。

Ⓐ インテリジェントアップデート

セキュリティ対策ファイル（ウイルスのパターンファイル、検索エンジン、ファイアウォールルール）の最新情報を定期的に取得し、バージョンが更新された場合に、自動的にアップデートが実行されます。最新情報を取得する間隔は、「フレッツ・セーフティのアップデート」のアップデート間隔で設定できます。（☛P1-26）

セキュリティ対策ファイルのアップデートにあたり、ファームウェアのアップデートが必要な場合は、ファームウェアのアップデートが実行されたあとにセキュリティ対策ファイルのアップデートを実行します。

Ⓑ ファームウェアの自動アップデート

お買い求め時は、「最新ファームウェアのアップデート情報」のアップデートの確認が「手動」に設定されています。（☛P1-26）

「自動」に設定している場合は、ファームウェアのバージョンの確認を一日一回行い、バージョンが更新されていたときは、自動的にアップデートを実行します。

また、「手動」に設定されている場合も、ファームウェアのバージョンの確認を一日一回行い、ファームウェアのアップデート内容によっては、自動的にアップデートを実行します。

Ⓒ 手動アップデート

Web 設定のホーム画面で最新情報を取得し、更新されたバージョンがある場合、手動アップデートができます。

Ⓓ ローカルファイルからの更新

当社ホームページからファームウェアをパソコンへダウンロードし、パソコンからアップデートを実行します。ファームウェアの自動アップデートができない場合に使用する方法です。（「ローカルファイルからアップデートする」（☛P1-68））

お知らせ

- フレッツ・セーフティにご契約いただいていないお客様は、本商品のウイルスパターン、検索エンジン、ファイアウォールルールの更新はできません。
- ホームページの閲覧中、メールの送受信中、ストリーミング再生やダウンロードなどを実行しているときにファームウェアおよびセキュリティ対策ファイルのアップデートが実行されると、接続が切断されることがあります。
- セキュリティ対策ファイルのアップデート中にネットワークケーブルを抜いた場合、ランプの点滅が継続して表示されることがあります。ランプが長時間に渡って点滅している場合は、本商品を再起動してください。
- 検索エンジンやファイアウォールルールがアップデートされた場合、本商品が再起動することがあります。
- ファームウェアがアップデートされた場合、本商品が再起動します。
- アップデートおよび再起動中は、本商品の電源アダプタは絶対に抜かないでください。
- セキュリティ対策ファイルのアップデート中に本商品の電源アダプタを抜いたり、本商品を再起動した場合は、セキュリティ対策ファイルが破損することがあります。セキュリティ対策ファイルが破損した場合は、セキュリティ対策ファイルの現在のバージョンが 0.000 等になります。
  このときはウイルス検索を行うことができませんので、手動アップデート等でセキュリティ対策ファイルを最新バージョンにアップデートしてください。

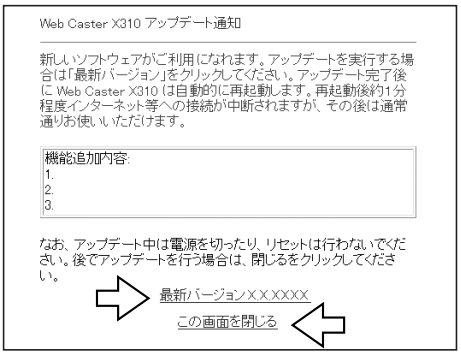
対象ファイルのアップデートについて

ワンポイント

●アップデート通知画面

新しいファームウェアが公開されると、アップデート内容をお知らせするアップデート通知画面が表示されます。アップデート通知画面は、Web ブラウザを起動したときと、Web 設定画面を開いたとき（☛P1-2）に表示されます。

・画面の「最新バージョン」をクリックすると、新たにアップデート中画面が表示され、アップデートを開始します。アップデートが完了すると本商品が再起動し、ログイン画面が表示されます。
「対象ファイルの手動アップデート」の手順６へ進んでください。（☛P1-67）
・画面の「この画面を閉じる」をクリックすると、アップデートを実行しないで画面を閉じます。
・アップデート実行後は、Web ブラウザを起動したときと、Web 設定画面を開いたとき（☛P1-2）に、最新バージョンへ更新されたことをお知らせする画面が表示されます。



※画面は例です。

●アップデート中のランプ表示は

アップデート中は、VIRUS ランプと HACKER ランプが同時に点滅します。
・セキュリティ対策ファイルのアップデート中：遅い点滅（緑）
・ファームウェアのアップデート中：速い点滅（緑）

●アップデートしたファームウェアの詳細について

アップデートを実行すると、最新バージョンへ更新されたことをお知らせする画面が表示されます。
最新バージョンへ更新されたことをお知らせする画面は、Web ブラウザを起動したときと、Web 設定画面を開いたとき（☛P1-2）に表示されます。

また、当社のホームページでも更新内容を確認できます。
・NTT 東日本のホームページ： http://www.ntt-east.co.jp/ced/
・NTT 西日本のホームページ： http://www.ntt-west.co.jp/kiki/

●対象ファイルのバージョンを確認するには

ホーム画面で対象ファイルの現在のバージョン、最新バージョンを確認することができます。（☛P1-4）

お知らせ

●最新バージョン欄に「更新の確認に失敗しました。」と表示されているときは、フレッツ・セーフティのオンライン登録をしていないか、または最新情報の取得に失敗したことを示しています。
●フレッツ・セーフティのオンライン登録済の場合で、最新バージョン欄に［更新の確認に失敗しました。］と表示されるときは、サーバとの接続に失敗した可能性がありますので、しばらく待ってからもう一度確認してください。
●フレッツ・セーフティのオンライン登録をしていない場合は、セキュリティ対策ファイルの最新バージョンの取得はできません。
●お客様のご利用状況などによって、正常にアップデートできない場合があります。

サポート情報

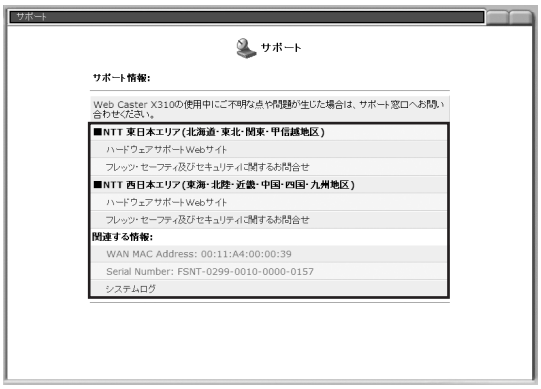
Web設定画面の［サポート］をクリックすると、サポート画面が表示されます。本商品の使用中にご不明な点や問題が生じた場合は、サポート窓口へお問い合わせください。

1 **Web設定画面で［サポート］をクリックする。**

2 **サポート窓口のリンクをクリックする。**

サポート窓口のリンクと本商品に関する情報が表示されます。

問題が生じた場合は、お住まいのエリアのサポート窓口へお問い合わせください。



ワンポイント

● **システムログを確認するには**

サポート画面の［システムログ］をクリックすると、システムログ画面が表示されます。

フレッツ・セーフティの設定を変更するには

フレッツ・セーフティの設定を変更することができます。

フレッツ・セーフティの設定を変更する

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P1-2）

2 ［フレッツ・セーフティ］をクリックする。

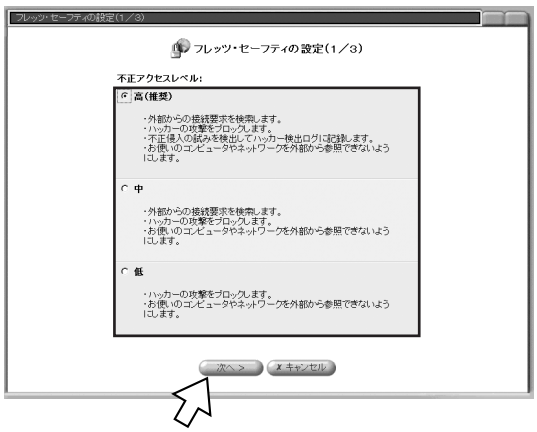
3 不正アクセスレベルを設定し、［次へ］をクリックする。

不正アクセス対策に関する設定を選択します。お買い求め時は、［高（推奨）］に設定されています。

［高（推奨）］：
- 外部からの接続要求を検索します。
- ハッカーの攻撃をブロックします。
- 不正侵入の試みを検出してハッカー検出ログに記録します。
- お使いのコンピュータやネットワークを外部から参照できないようにします。

［中］：
- 外部からの接続要求を検索します。
- ハッカーの攻撃をブロックします。
- お使いのコンピュータやネットワークを外部から参照できないようにします。

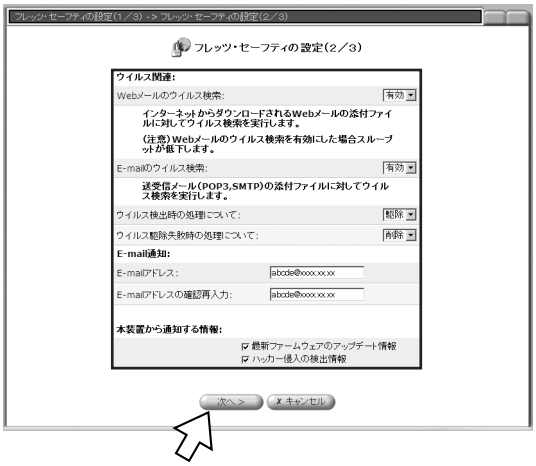
［低］：
- ハッカーの攻撃をブロックします。
- お使いのコンピュータやネットワークを外部から参照できないようにします。



お知らせ

- お客様の環境によっては、Web メールのウイルス検索をオフにすると、Web 閲覧（HTTP）のスループットが向上する場合があります。
- フレッツ・セーフティにご契約いただいているお客様は、Unnumbered 接続時でも、セキュリティ対策ファイル （パターンファイル、検索エンジン、ファイアウォールルール）の ダウンロードを行うことができます。

4 各項目を設定し、［次へ］をクリックする。



●**ウイルス関連：**

［Web メールのウイルス検索］：

インターネットからダウンロードされる Web メールの添付ファイルに対してウイルス検索を実行することができます。ただし、通常の E-mail と異なり、Web メールの添付ファイルからウイルスを駆除することはできますが、感染ファイルを放置することはできません（駆除できない場合は削除します）。Web メールは、Yahoo!メール、Hotmail、AOL メールのみに対応しています。

有効：ウイルス検索をする（お買い求め時の設定）

無効：ウイルス検索をしない

［E-mail のウイルス検索］：

本商品では、お買い求め時の設定で、受信メールと送信メールに対するウイルス検索をするかどうかを設定します。使用しているパソコン環境をウイルスから保護し続けるには、常に［有効］にしておくことを強くお勧めいたします。

有効：ウイルス検索をする（お買い求め時の設定）

無効：ウイルス検索をしない

［ウイルス検出時の処理について］

ウイルス検索が有効の場合、ウイルス検出時の処理を選択します。

駆除：感染したファイルを修復する（お買い求め時の設定）

削除：感染したファイルを削除する

放置：なにもしないで放置する

［ウイルス駆除失敗時の処理について］

ウイルス検出時の処理が「駆除」の場合、ウイルスを駆除できないときの処理を選択します。

駆除：感染したファイルを削除する（お買い求め時の設定）

放置：なにもしないで放置する

●**E-mail 通知：**

通知先の E-mail アドレスを設定すると、［本装置から通知する情報］でチェックした情報が E-mail で通知されます。E-mail による通知をしない場合は、［E-mail アドレス］、［E-mail アドレスの確認再入力］を空欄のままにしておきます。

［E-mail アドレス］：

お持ちの E-mail アドレスを入力します。半角英数記号 100 文字まで入力できます。

［E-mail アドレスの確認再入力］：

もう一度、同じ E-mail アドレスを入力します。

●**本装置から通知する情報：**

本装置から通知する情報をチェックします。

［最新ファームウェアのアップデート情報］：

ファームウェアの最新バージョンがあるときに通知する（お買い求め時はチェックなし）

［ハッカー侵入の検出情報］：

ハッカーが検出されたときに通知する（お買い求め時はチェックなし）

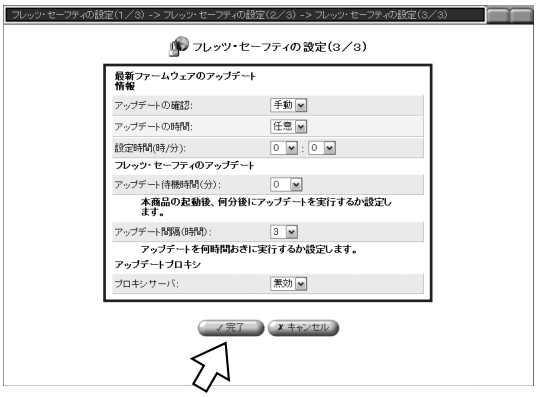
お知らせ

- E-mail アドレスを入力しないと、以下のメールが送られてきません。
  - ・フレッツ・セーフティにオンライン登録がお済みでないお客様あての未登録通知
  - ・［本装置から通知する情報］でチェックした情報
- E-mail アドレスの@マーク以下は、半角英数字、-（ハイフン）、_（アンダースコア）、.（ドット）が使用できます。

（次ページへ続きます）

フレッツ・セーフティの設定を変更するには

5 各項目を設定し、［完了］をクリックする。



●最新ファームウェアのアップデート情報：

［アップデートの確認］：

本商品のファームウェアのアップデート方法を選択します。「自動」でご使用になることを推奨します。

自動：アップデートが必要な場合に自動的にアップデートする

手動：アップデートの通知画面が表示されたら画面の［最新バージョン］をクリックしてアップデートする（お買い求め時の設定）

ただし、ファームウェアのアップデート内容によっては、「手動」に設定している場合でも自動的にアップデートが行われます。

［アップデートの時間］：

固定：AM4:00 ～ 5:00 にアップデートを開始する（お買い求め時の設定）

任意：設定した時間にアップデートを開始する（時間は 0 ～ 23 時、分は 0、10、20、30、40、50 分で設定可能）

●フレッツ・セーフティのアップデート：

セキュリティ対策ファイル（☛P1-21）のアップデートについて設定します。

［アップデート待機時間（分）］：

本商品を起動してから何分後にアップデートを実行するかを設定します。0 ／ 15 ／ 30 ／ 60 ／ 120 から選択します。お買い求め時は「0」に設定されています。

［アップデート間隔（時間）］：

アップデートの確認を何時間おきに実行するかを設定します。1 ／ 3 ／ 6 ／ 12 ／ 24 から選択します。お買い求め時は「3」に設定されています。

●アップデートプロキシ：

［プロキシサーバ］：

アップデートサーバとの通信にプロキシサーバが必要かどうかを設定します。

無効：プロキシサーバが必要でない場合（お買い求め時の設定）

有効：プロキシサーバが必要な場合に選択し、以下の項目を設定する

［ホスト名］：

ホスト名を半角英数字記号 100 文字以内で設定します。－（ハイフン）、_（アンダースコア）、.（ドット）を使用できます。

＜例＞ proxy.co.jp または 10.21.254.30

［ポート番号］：

ポート番号を 1 ～ 65535 の範囲で設定します。

［認証］：

プロキシサーバへの接続に認証が必要な場合は、［する］を選択し、［接続ユーザ名］、［接続パスワード］を設定します。

［接続ユーザ名］：

接続ユーザ名を半角英数字記号 64 文字以内で設定します。

［接続パスワード］：

接続パスワードを半角英数字記号 64 文字以内で設定します。

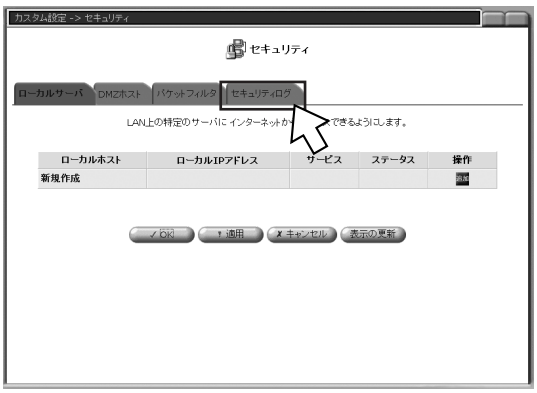
ウイルスや不正アクセスが検出されたとき

ウイルスが検出されたときはVIRUSランプ、不正アクセスが検出されたときはHACKERランプがそれぞれ赤点灯します。次の手順でセキュリティログの内容を確認してください。
セキュリティログを確認すると、VIRUSランプ、HACKERランプがそれぞれ緑点灯に変わります。

1 Web設定画面で［カスタム設定］をクリックする。

2 ［セキュリティ］をクリックする。

3 ［セキュリティログ］をクリックする。

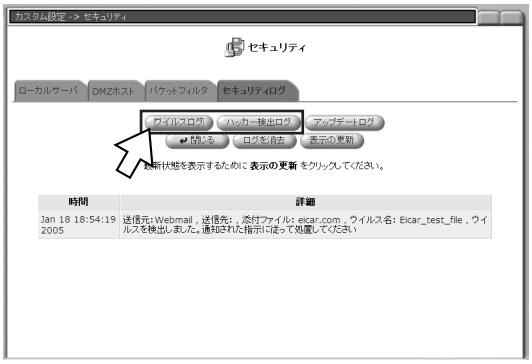


（次ページへ続きます）

フレッツ・セーフティの設定を変更するには

4 [ウイルスログ] または [ハッカー検出ログ] をクリックする。

VIRUS ランプが赤点灯しているときは［ウイルスログ］、HACKER ランプが赤点灯しているときは［ハッカー検出ログ］をクリックします。



ウイルスログ画面（例）

5 セキュリティログの内容を確認する。

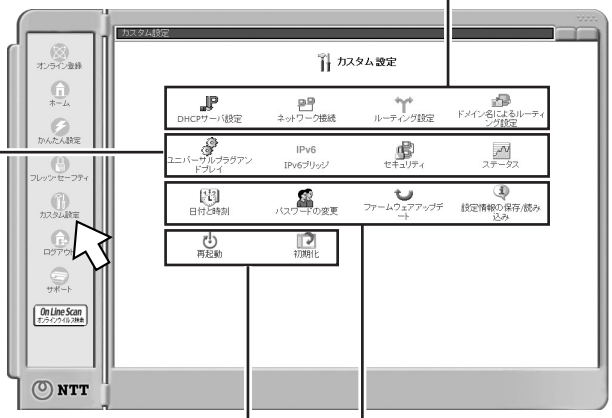
セキュリティログを表示すると、VIRUS ランプ、HACKER ランプがそれぞれ緑点灯に変わります。

ウイルスログ画面（例）

ハッカー検出ログ画面（例）

カスタム設定画面

Web 設定画面の［カスタム設定］をクリックして、本商品のさまざまな機能を設定することができます。



［ユニバーサルプラグアンドプレイ］
UPnP 機能の有効／無効を設定します。

［IPv6 ブリッジ］
IPv6 ブリッジの有効／無効を設定します。

［セキュリティ］
ローカルサーバ、DMZ ホスト、パケットフィルタの設定、セキュリティログを表示します。

［ステータス］
接続状況、システムログ、LAN ／ WAN リンク状態を表示します。

［DHCP サーバ設定］
DHCP サーバの有効／無効などを設定します。

［ネットワーク接続］
PPPoE の最大接続数などを設定します。

［ルーティング設定］
ルーティングの設定を行います。

［ドメイン名によるルーティング設定］
ドメイン名によるルーティングを設定します。

［日付と時刻］
システムの日付と時刻を設定します。

［パスワードの変更］
Web 設定画面のログインパスワードを変更します。

［ファームウェアアップデート］
パソコンにダウンロードしたファイルを使用して、本商品のファームウェアをアップデートします。

［設定情報の保存／読み込み］
本商品の設定情報の保存と読み込みを行います。

［再起動］
本商品を再起動します。

［初期化］
本商品の設定情報、ネットワーク情報、各種ログを消去して、お買い求め時の状態に戻します。

DHCP サーバ設定

DHCP サーバ設定を有効にすると、LAN 内のパソコンやネットワーク機器が LAN に接続されるたびに、他のどれとも重複しない IP アドレスを自動で割り当てることができます。
お買い求め時は、次のように設定されています。

- DHCP サーバ機能：有効
- IP アドレスの割り当て範囲： 192.168.0.11 ～ 192.168.0.99
- ネットマスク： 255.255.255.0

DHCP サーバ設定画面

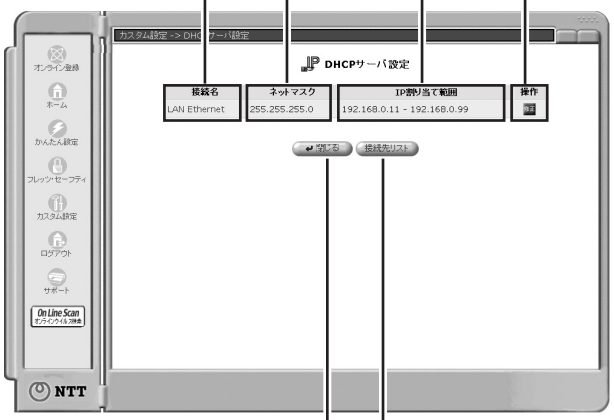
カスタム設定画面の［DHCP サーバ設定］をクリックすると、DHCP サーバ設定画面が表示されます。
この画面では、現在の DHCP サーバのネットマスク、IP アドレスの割り当て範囲を確認することができます。

［ネットマスク］
使用するネットマスクが表示されます。

［IP 割り当て範囲］
割り当てる IP アドレスの範囲が表示されます。

［接続名］
設定済みの接続名が表示されます。接続名をクリックすると、その接続の設定を変更できます。

［操作］
各アイコンをクリックすると、次の操作が行えます。
・修正
その接続での設定を修正します。



［閉じる］
作業を中止して、カスタム設定のトップ画面へ戻ります。

［接続先リスト］
［DHCP 接続］画面を表示して、LAN 側の DHCP 接続を設定します。

お知らせ

- DHCP サーバ機能を使用しないときは、LAN 側に接続されているパソコンすべてに手動で IP アドレスを割り当ててください。
- パソコンに手動で IP アドレスを設定した場合、そのパソコンのホスト名や IP アドレスを本商品で管理することはできません。
- WAN PPPoE 詳細設定の「IP 設定」（☛P2-32）で「Unnumbered 接続を使う」を選択した場合は、「DHCP サーバ設定」（☛P1-31）が「無効」に設定されます。

DHCP サーバの設定を変更する

DHCP サーバには、LAN 上のパソコンに割り当てる IP アドレスの範囲、ネットマスクなどを設定します。パソコンがネットワークに接続されると、DHCP サーバから自動的に IP アドレスが割り当てられます。
DHCP サーバの有効／無効、IP アドレスの割り当て範囲などを変更することができます。

1 DHCP サーバ設定画面で［修正］をクリックする。

2 DHCP サーバの設定をする。

IP 設定：

［IP アドレス］：
本商品の IP アドレスを入力します。

［ネットマスク］：
本商品のネットマスクを入力します。

サービス：

［DHCP サーバ設定］：
DHCP サーバ機能の有効／無効を選択します。

DHCP サーバ：

［割り当て開始 IP アドレス］：
パソコンに割り当てる IP アドレス範囲の最初の IP アドレスを入力します。

［割り当て終了 IP アドレス］：
パソコンに割り当てる IP アドレス範囲の最後の IP アドレスを入力します。

［ネットマスク］：
パソコンに割り当てるネットマスクを入力します。

［WINS サーバ IP アドレス］：
WINS サーバの IP アドレスを入力します。

［リース時間（分）］：
DHCP サーバ機能で割り当てる IP アドレスの有効期限を分単位で入力します。

［クライアントにホスト名が設定されていないときにホスト名を自動的に割り当てる］：
ホスト名が設定されていないパソコンに自動的にホスト名を割り当てる場合にチェックします。

お知らせ

- LAN イーサネットの設定を変更した場合は、変更の内容に応じて DHCP サーバの設定を見直してください。
- DHCP サーバ設定を無効に変更した場合は、パソコン側に固定 IP アドレスを設定してください。
- パソコン側に固定 IP アドレスを設定した場合、フレッツ・セーフティのオンライン登録ページが正常に表示されないことがありますので、パソコン側の DNS 設定の中のサフィックス設定に「home」を設定してください。

（次ページへ続きます）

DHCP サーバ設定

3 [OK] をクリックする。

4 [OK] をクリックする。
[OK] をクリックすると、設定内容が反映されます。設定の内容を変更する場合は、手順 1 から再度設定し直してください。

DHCP サーバから固定の IP アドレスを割り当てる

特定のパソコンやネットワーク機器に、DHCP サーバから常に固定の IP アドレスを割り当てることができます。

1 DHCP サーバ設定画面で［接続先リスト］をクリックする。

2 ［新規作成］または［追加］をクリックする。

3 追加するパソコンのホスト名、IP アドレス、MAC アドレスを入力し、［OK］をクリックする。

［ホスト名］：
パソコン等のホスト名を入力します。半角英数字、-（ハイフン）、_（アンダースコア）、.（ドット）を使用できます。ハイフン、アンダースコア、ドットは先頭や末尾には使えません。ドットで区切られた文字は最大 63 文字、全体の最大文字数は 255 文字です。

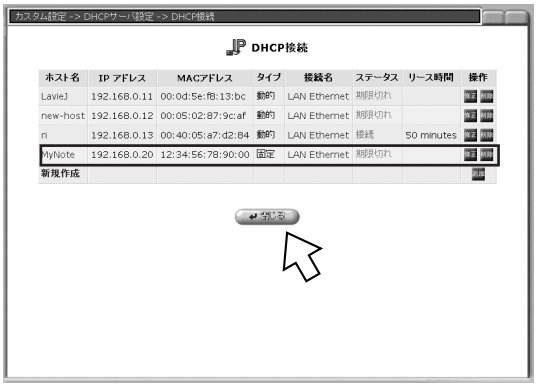
［IP アドレス］：
パソコン等に割り当てる IP アドレスを入力します。

［MAC アドレス］：
IP アドレスを割り当てるパソコン等の MAC アドレスを入力します。

お知らせ

- パソコンに手動で IP アドレスを設定する場合、DHCP サーバから固定で割り当てられる IP アドレスと重複しないようにしてください。重複した場合、接続リストが正しく表示されないことがあります。

4 追加したホストが表示されていることを確認して、［閉じる］をクリックする。



IPアドレスを修正する

DHCPサーバから自動的にIPアドレスが割り当てられているパソコンのIPアドレスを固定設定します。

1 DHCPサーバ設定画面で［接続先リスト］をクリックする。

2 設定を変更したいホストの［修正］をクリックする。

（次ページへ続きます）

DHCP サーバ設定

3 [固定割り当て] にチェックし、[OK] をクリックする。

4 設定を変更したいホストの [修正] をクリックする。

5 IP アドレスを修正し、[OK] をクリックする。

IPアドレスを削除する

登録済みのIPアドレスとホスト名の対応を削除します。

1 DHCPサーバ設定画面で［接続先リスト］をクリックする。

2 削除したいホストの［削除］をクリックする。

ネットワーク接続

本商品は、PPPoE マルチセッションに対応しています。マルチセッション利用時は、複数のプロバイダを登録し、同時に接続することができます。PPPoE の接続数は２～５の範囲で設定できます。ただし、WAN PPPoE 1 はフレッツ・スクウェアに固定されています。

ネットワーク接続画面

カスタム設定画面の［ネットワーク接続］をクリックすると、ネットワーク接続画面が表示されます。
この画面では、接続先を追加したり、登録されている接続先を確認することができます。

［PPPoE セッション最大接続数］
２～５の範囲で設定します。設定した数に連動して設定変更できる接続が表示されます。

［接続名］
接続名が表示されます。

［ステータス］
現在の状態が表示されます。

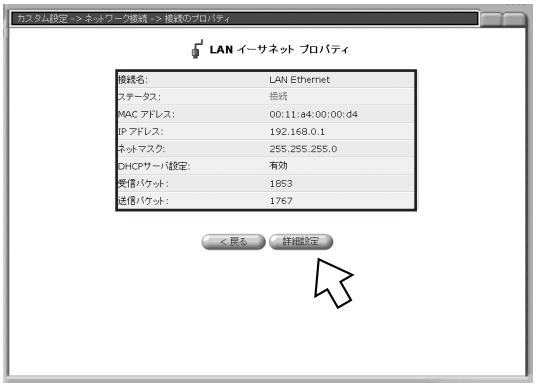
［操作］
各アイコンをクリックすると、次の操作が行えます。
・修正
　設定を修正します。
・初期化
　設定を初期化します。

［戻る］
作業を中止して、カスタム設定のトップ画面へ戻ります。

LAN イーサネットの設定を確認／変更する

1 ［LAN Ethernet］の［修正］をクリックする。

2 **[LAN イーサネット プロパティ] の内容を確認する。詳細な設定を確認するには、[詳細設定] をクリックする。**



3 **設定を確認し、必要に応じて変更する。**

基本設定：

[ステータス] ：

現在の LAN イーサネットの状態が表示されます。

IP 設定：

[IP アドレス] ：

本商品の IP アドレスを入力します。

[ネットマスク] ：

本商品のネットマスクを入力します。

[デバイスメトリック] ：

メトリックの値を入力します。

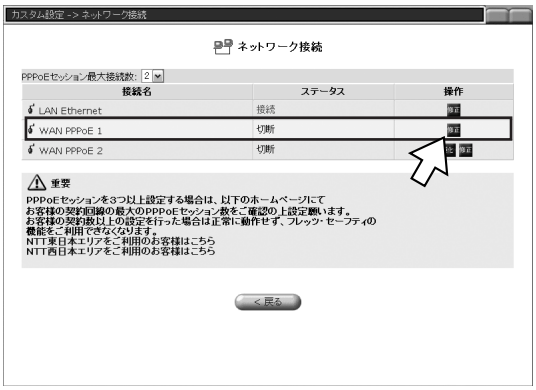
4 **[OK] をクリックする。**

ネットワーク接続

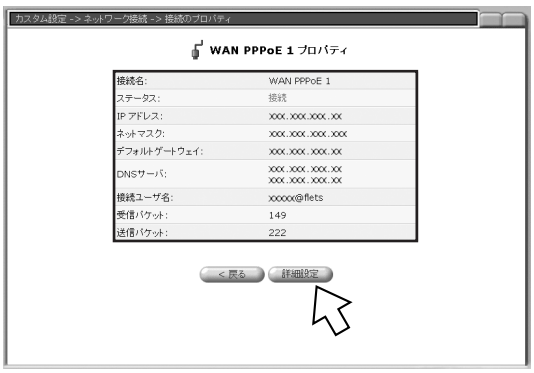
WAN PPPoE 1 の設定を確認／変更する

フレッツ・スクウェアの接続状態を確認／変更します。
WAN PPPoE 1 はフレッツ・スクウェアに固定されていますので、削除/初期化はできません。

1 [WAN PPPoE 1] の［修正］をクリックする。



2 [WAN PPPoE 1 プロパティ] を確認する。詳細な設定を確認するには、[詳細設定] をクリックする。



3 設定を確認し、必要に応じて変更する。

［無通信監視タイマ（分）］：
設定した時間内にデータの送受信がないと、自動的に回線が切断されます。
1／5／10／30 から選択します。
お買い求め時は「1」に設定されています。

お知らせ

- 自動切断されたあとに、セキュリティ対策ファイル（☛P1-21）のアップデートを行ったり、フレッツ・スクウェアにアクセスすると、自動的に接続します。

4 [OK] をクリックする。

WAN PPPoEの接続先を追加する

フレッツ・スクウェアとご利用のプロバイダが登録されている場合に、３つ目以降の接続先を追加登録します。

1 **ネットワーク接続画面で、[PPPoEセッション最大接続数]を「3」に変更する。**

[WAN PPPoE 3]が追加されます。

ネットワーク接続

WAN PPPoE2 ～ 5 の設定を確認／変更する

WAN PPPoE2 ～ 5 の詳細な接続状態を確認し、設定を変更することができます。

1 ネットワーク接続画面で、変更したい［WAN PPPoE X］の［修正］をクリックする。

2 ［WAN PPPoE X プロパティ］を確認する。詳細な設定を確認する場合は、［詳細設定］をクリックする。

［無効］をクリックすると、回線が切断されます。再び接続するには、［有効］をクリックします。

3 接続先を設定する。

●**基本設定：**

［ステータス］：
現在の WAN PPPoE の状態が表示されます。

［MTU］：
自動／手動を選択します。

●**PPP：**

［サービス名］：
プロバイダによってサービス名を指定された場合に入力します。

［無通信監視タイマ（分）］：
設定した時間内にデータの送受信がないと、自動的に回線が切断されます。
0／5／10／30 から選択します。
「0」を選択した場合、回線は切断されません。
お買い求め時は「0」に設定されています。

●**PPP 認証：**

［接続ユーザ名（大文字・小文字区別）］：
プロバイダから指定されたユーザ名を入力します。

［接続パスワード］：
プロバイダから指定されたパスワードを入力します。

［PAP 認証を許可する（PAP）］：
PAP 認証を使用しないときはチェックを外します。

［CHAP 認証を許可する（CHAP）］：
CHAP 認証を使用しないときはチェックを外します。

●**IP 設定**：次のいずれかを選択します。

・［Unnumbered 接続を使う］：
Unnumbered 接続で使用する IP アドレスを設定します。
ネットマスクを置き換えるときは［ネットマスクを置き換える］をチェックして、ネットマスクを入力します。

・［IP アドレスを自動取得する］：
ネットマスクを置き換えるときは［ネットマスクを置き換える］をチェックして、ネットマスクを入力します。

・［IP アドレスを固定設定する］：
IP アドレスを設定します。
ネットマスクを置き換えるときは［ネットマスクを置き換える］をチェックして、ネットマスクを入力します。

●**DNS サーバ**：次のいずれかを選択します。

・DNS サーバアドレスを自動取得する
・DNS サーバアドレスを固定設定する

［NAPT］：
NAPT 機能の有効／無効を選択します。

［デバイスメトリック］：
デバイスメトリックは、PPPoE2 ～ 5 の接続順位を設定します。
値が小さい方が優先順位が高くなります。同じ値は設定しないでください。

お知らせ

● 接続ユーザ名と接続パスワードは、大文字小文字の区別を確認のうえ、入力してください。

（次ページへ続きます）

4 [OK] をクリックする。

5 [有効] をクリックする。

WAN イーサネットの設定を確認／変更する

PPPoE を使用しない接続がすでに登録されている場合は、WAN イーサネットの設定を変更することができます。

1 ネットワーク接続画面で、[WAN Ethernet] の [修正] をクリックする。

2 接続状況を確認し、変更する場合は［詳細設定］をクリックする。

3 WANイーサネットの設定を変更する。

●基本設定：

［ステータス］：
　現在のWANイーサネットの状態が表示されます。

［MTU］：
　自動／手動を選択します。

● **IP設定**：次のいずれかを選択します。
- ［IPアドレスを自動取得する］：
  本商品のWAN側IPアドレスを自動的に取得する場合に選択します。ネットマスクを置き換えるときは、［ネットマスクを置き換える］をチェックします。
- ［IPアドレスを固定設定する］：
  本商品のWAN側IPアドレスを設定します。IPアドレス、ネットマスク、デフォルトゲートウェイを入力します。

［DHCP Lease］：
- ［Renew］をクリックして、DHCPの更新を行います。
- ［Release］をクリックして、DHCPの解放を行います。

● **DNSサーバ**：次のいずれかを選択します。
- ［DNSサーバアドレスを自動取得する］：
  DNSサーバのIPアドレスを自動的に取得する場合に選択します。
- ［DNSサーバアドレスを固定設定する］：
  DNSサーバのIPアドレスを指定する場合に選択します。プライマリDNSサーバ、セカンダリDNSサーバのIPアドレスを入力します。

［NAPT］：
　有効／無効を選択します。

［デバイスメトリック］：
　ここでは設定不要です。

4 ［OK］をクリックする。

ネットワーク接続

WAN PPPoE 2～5の設定を初期化する

WAN PPPoE 2～5の設定を初期化することができます。

1 ネットワーク接続画面で初期化したい［WAN PPPoE X］の［初期化］をクリックする。

2 ［OK］をクリックする。

ルーティング設定

本商品は、ダイナミックルーティングのプロトコルとして RIP に対応しています。また、スタティックルーティングにも対応しています。

ルーティング設定画面

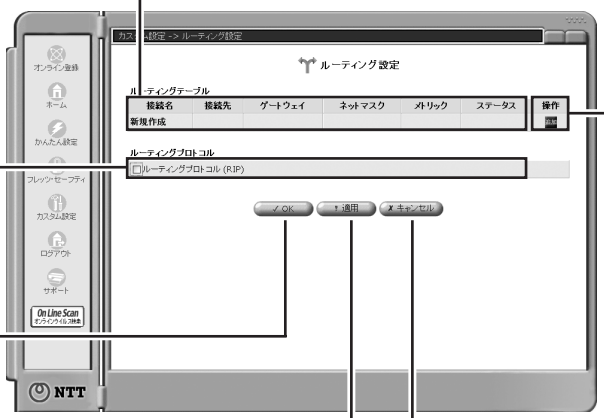
カスタム設定画面の［ルーティング設定］をクリックすると、ルーティング設定画面が表示されます。この画面では、経路情報を追加したり、登録されている経路情報を確認することができます。

［ルーティングテーブル］
作成済みのルーティングテーブルを表示します。新規作成する場合は、［新規作成］または［操作］の［追加］をクリックします。

［ルーティングプロトコル］
ルーティングプロトコル（RIP）を有効にする場合はチェックします。

［OK］
設定を確定して、カスタム設定のトップ画面へ戻ります。

［適用］
設定内容を適用します。



［操作］
各アイコンをクリックすると、次の操作が行えます。
・追加
　設定を追加します。
・修正
　設定を修正します。
・削除
　設定を削除します。

［キャンセル］
作業を中止して、カスタム設定のトップ画面へ戻ります。

ダイナミックルーティングの有効／無効を設定する

ダイナミックルーティングを有効に設定し、動的に経路情報を登録します。お買い求め時は、「無効」に設定されています。

1 ルーティング設定画面で、ルーティングプロトコルを設定する。

ダイナミックルーティングを有効にする場合は、［ルーティングプロトコル（RIP）］をチェックします。

2 ［OK］をクリックする。

ルーティング設定

スタティックルーティングの経路情報を追加する

スタティックルーティングの経路情報を手動で設定します。

1 ルーティング設定画面で、[新規作成] または [追加] をクリックする。

2 経路情報を設定する。

[接続名] :
スタティックルーティングを設定する転送先のインタフェースを [LAN Ethernet]、[WAN PPPoE 1] ～ [WAN PPPoE 5] から選択します。
かんたん設定（接続方法の設定）画面で、[PPPoE を使用しないで接続する場合] を選択したときは（☛P1-10、2-22）、[WAN Ethernet] も選択できます。

[接続先] :
パケットの送信先となるネットワークアドレスを入力します。

[ネットマスク] :
パケットの送信先のネットマスクを入力します。

[ゲートウェイ] :
宛先のネットワークに到達するための、最初のゲートウェイのアドレスを入力します。

[メトリック] :
宛先のネットワークに到達するまでのホップカウント（経由するゲートウェイの数）を入力します。

3 [OK] をクリックする。

ドメイン名によるルーティング設定

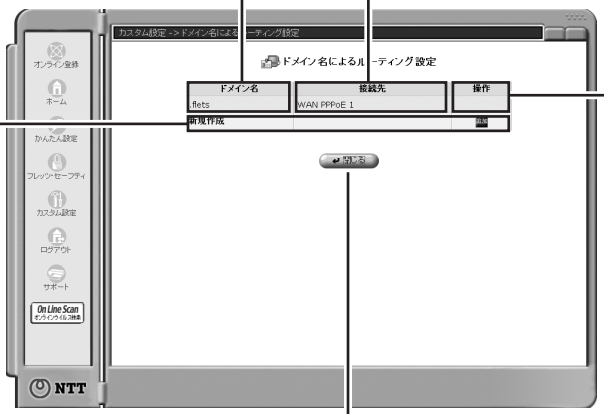
ドメイン名に対応する IP アドレスの問い合わせをマルチセッション対応で行うことができます。フレッツ・スクウェアのために、あらかじめドメイン名「.flets」と接続先「WAN PPPoE 1」が設定されています。

ドメイン名によるルーティング設定画面

カスタム設定画面の［ドメイン名によるルーティング設定］をクリックすると、ドメイン名によるルーティング設定画面が表示されます。
この画面では、設定されているドメイン名と接続先を確認することができます。

［ドメイン名］
作成済みのドメイン名が表示されます。
ドメイン名を修正するには、ドメイン名または［操作］の［修正］をクリックします。
・新規作成
新規にルーティング設定を作成するには、［新規作成］または［操作］の［追加］をクリックします。

［接続先］
接続先のセッションが表示されます。



［操作］
各アイコンをクリックして、次の操作が行えます。
・修正
作成済みの設定を修正します。
・削除
作成済みの設定を削除します。
・追加
設定を新規作成します。

［閉じる］
作業を中止して、カスタム設定のトップ画面へ戻ります。

ドメイン名によるルーティングを追加する

ドメイン名によるルーティングを新規に作成します。

1 ドメイン名によるルーティング設定画面で、［新規作成］または［追加］をクリックする。

（次ページへ続きます）

ドメイン名によるルーティング設定

2 ドメイン名を入力し、接続先を選択する。

［ドメイン名］：
ドメイン名を入力します。半角英数字、-（ハイフン）、_（アンダースコア）、.（ドット）を使用できます。
先頭はドットにしてください。ドットは末尾には使用できません。
全体の最大文字数は 255 文字です。
＜例＞
.X310.co.jp
［接続先］：
WAN PPPoE 2 ～ 5 から選択します。WAN PPPoE 1 はフレッツ・スクウェアで使用しているため、設定できません。

3 [OK] をクリックする。

ユニバーサルプラグアンドプレイ

ユニバーサルプラグアンドプレイ（UPnP：Universal Plug and Play）は、ネットワークに接続するだけで、ネットワーク上の機器同士で簡単に通信できるようにする規格です。本商品はユニバーサルプラグアンドプレイに対応しており、次の機能を使用できます。

- UPnPに対応しているOS（Windows® XP、Windows® Me）から、本商品を検出できます。
- 本商品に接続されているLAN内のパソコンから、Windows® MessengerやMSN® Messengerなど、UPnPに対応しているアプリケーションを使用できます。

ユニバーサルプラグアンドプレイ画面

カスタム設定画面の［ユニバーサルプラグアンドプレイ］をクリックすると、ユニバーサルプラグアンドプレイ画面が表示されます。

［UPnP機能を適用する接続先］
UPnP機能を適用する接続先を選択します。

［UPnP機能を有効にする］
UPnP機能を有効にする場合はチェックします。

［OK］
設定を確定して、カスタム設定のトップ画面へ戻ります。

［キャンセル］
作業を中止して、カスタム設定のトップ画面へ戻ります。

［適用］
設定内容を適用します。

お知らせ

- Windows® 2000／98 Second Editon／98およびMacintoshはUPnPに対応していないため、本商品のUPnP機能を使用することはできません。
- UPnP機能を［有効］に設定すると、UPnPで利用するポート等に対して不正アクセスの防止機能が動作しませんので、ご注意ください。
- WANイーサネットでご利用の場合は、この機能は対応していません。

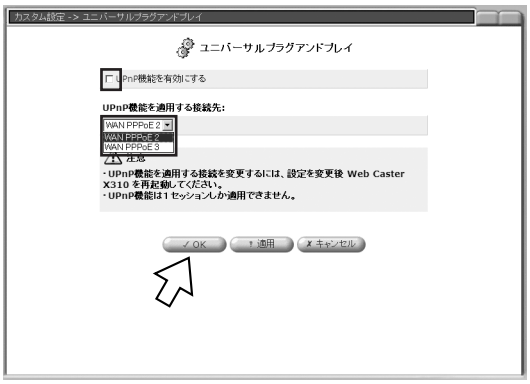
ユニバーサルプラグアンドプレイ

UPnP 機能の有効／無効を設定する

UPnP 機能の有効／無効を設定します。お買い求め時は「無効」に設定されています。

1 ユニバーサルプラグアンドプレイ画面で UPnP 機能の有効／無効を設定し、［OK］をクリックする。

UPnP 機能を有効にするには、［UPnP 機能を有効にする］をチェックします。
接続先を追加している場合は、［UPnP 機能を適用する接続先］から、UPnP 機能を設定する接続先を選択します。
UPnP 機能を適用できる接続先は 1 つのみです。



2 ［OK］をクリックする。

設定を変更した後は、本商品を再起動してください。（自動では再起動しません。）

お知らせ

- UPnP 機能を「有効」に設定すると、UPnP で利用するポート等に対して不正アクセスの防止機能が動作しませんので、ご注意ください。
- WAN イーサネットでご利用の場合は、この機能は対応していません。

IPv6 ブリッジ

NTT 東日本エリアで提供しているフレッツ・ドットネットおよび NTT 西日本エリアで提供しているフレッツ・ v6 アプリを本商品の LAN ポートに接続したパソコンで使用するには、IPv6 ブリッジ機能を有効にする必要があります。

IPv6 ブリッジ画面

カスタム設定画面の［IPv6 ブリッジ］をクリックすると、IPv6 ブリッジ画面が表示されます。

［IPv6 ブリッジ機能を有効にする］
IPv6 ブリッジを有効にする場合はチェックします。

［キャンセル］
作業を中止して、カスタム設定のトップ画面へ戻ります。

［OK］
設定内容を適用し、カスタム設定のトップ画面へ戻ります。

［適用］
設定内容を適用します。

IPv6 ブリッジ機能の有効／無効を設定する

IPv6 ブリッジ機能の有効／無効を設定します。お買い求め時は無効に設定されています。

1 IPv6 ブリッジ画面で IPv6 ブリッジ機能の有効／無効を設定する。

IPv6 ブリッジ機能を有効にするには、［IPv6 ブリッジ機能を有効にする］にチェックをつけます。

2 ［OK］をクリックする。

セキュリティ

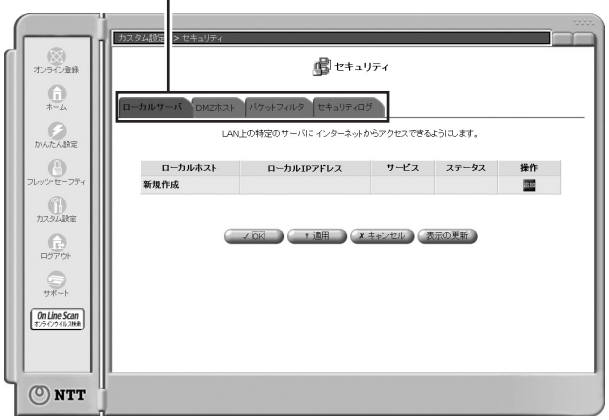
インターネットに接続すると、LAN 内のパソコンがインターネットからの攻撃を受けたり、不正なアクセスをされたりという危険があります。本商品では、インターネットへの常時接続を行ううえでのセキュリティ対策として、次の機能を搭載しています。

名称	機能
NAPT（IP マスカレード）	グローバルアドレスに割り当てられた IP アドレスをプライベート側にある端末が共有する仕組みです。これにより、複数の機器が 1 つのグローバルアドレスを利用して接続できるようになります。
ステートフルパケットインスペクション	ファイアウォール方式として、ステートフルパケットインスペクション方式を採用しています。 通過セッションごとにパケットの整合性を確認し、必要なポートだけ開くようにします。通信が終了すると、利用したポートを遮断します。
ローカルサーバ機能 （☛P1-53、2-25、2-39）	ポート番号別に転送先のパソコンを指定し、サーバをインターネット上に公開できます。
DMZ ホスト機能 （☛P1-53）	LAN 内の 1 台のパソコンを DMZ ホストとすると、WAN 側からのすべての接続要求が DMZ ホストに転送されるようになります。
パケットフィルタ （☛P1-54）	LAN 側から送られてきたパケットを検査して、通過させるかどうかを判断する機能です。 どのような条件でパケットを通過させるか、遮断させるかをプロトコル／ポートごとに任意に設定できます。
セキュリティログ （☛P1-54）	ウイルスログ、ハッカー検出ログ、セキュリティ対策ファイルのアップデートログを表示できます。

セキュリティ画面

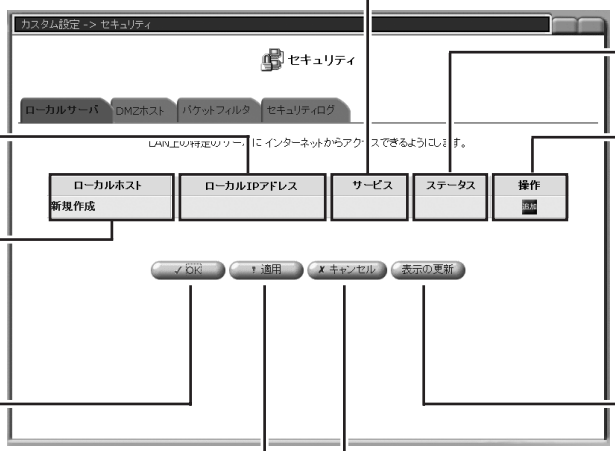
カスタム設定画面の［セキュリティ］をクリックすると、セキュリティ画面が表示されます。
セキュリティ画面では、［ローカルサーバ］、［DMZ ホスト］、［パケットフィルタ］、［セキュリティログ］の各タブをクリックすると、画面が切り替わります。

［ローカルサーバ］タブ
［DMZ ホスト］タブ
［パケットフィルタ］タブ
［セキュリティログ］タブ



ローカルサーバ画面

ローカルサーバ画面では、ローカルサーバを設定することができます。



[ローカルIPアドレス]
パソコンのIPアドレス／ホスト名を表示します。

[ローカルホスト]
［新規作成］をクリックして、ローカルサーバを追加します。

[OK]
設定を確定して、カスタム設定のトップ画面へ戻ります。

[適用]
設定内容を適用します。

[サービス]
サービスを表示します。

[ステータス]
現在の状態を表示します。

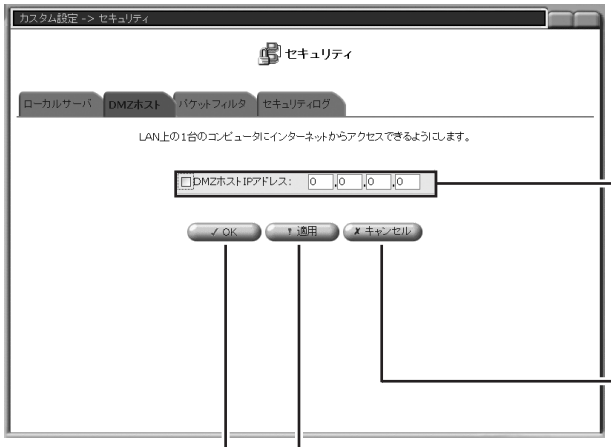
[操作]
各アイコンをクリックすると、次の操作が行えます。
- 修正
  設定を修正します。
- 削除
  設定を削除します。
- 追加
  設定を追加します。

[表示の更新]
最新の情報を表示します。

[キャンセル]
作業を中止して、カスタム設定のトップ画面へ戻ります。

DMZホスト画面

DMZホスト画面では、DMZホストのIPアドレスを設定することができます。



[DMZホストIPアドレス]
DMZホストIPアドレスを有効にする場合はチェックし、DMZホストにするパソコンのIPアドレスを入力します。

[キャンセル]
作業を中止して、カスタム設定のトップ画面へ戻ります。

[適用]
設定内容を適用します。

[OK]
設定を確定して、カスタム設定のトップ画面へ戻ります。

セキュリティ

パケットフィルタ画面

パケットフィルタ画面では、パケットフィルタルールを作成することができます。

[ローカル IP アドレス]
パソコンの IP アドレス／ホスト名を表示します。

[ローカルホスト]
［新規作成］をクリックして、フィルタリングルールを追加します。

[OK]
設定を確定して、カスタム設定のトップ画面へ戻ります。

[適用]
設定内容を適用します。

[拒否されるサービス]
拒否されるサービスを表示します。

[ステータス]
現在の状態を表示します。

[操作]
各アイコンをクリックすると、次の操作が行えます。
・修正
　設定を修正します。
・削除
　設定を削除します。
・追加
　設定を追加します。

[表示の更新]
最新の情報を表示します。

[キャンセル]
作業を中止して、カスタム設定のトップ画面へ戻ります。

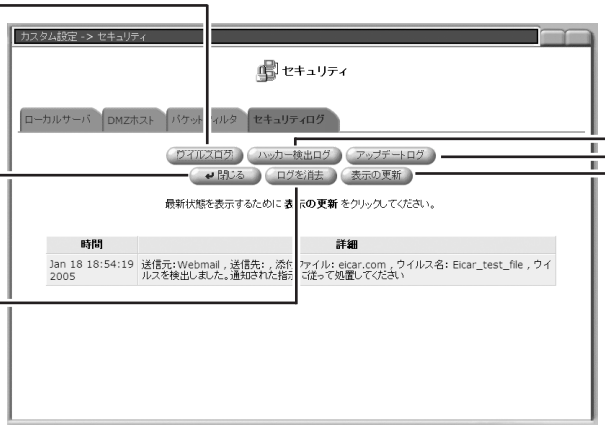
セキュリティログ画面

セキュリティログ画面では、ウイルスログ、ハッカー検出ログ、アップデートログを確認することができます。

[ウイルスログ]
ウイルス検出のログを表示します。

[閉じる]
作業を中止して、カスタム設定のトップ画面へ戻ります。

[ログを消去]
セキュリティログを消去します。



[ハッカー検出ログ]
不正アクセス検出のログを表示します。

[アップデートログ]
アップデートのログを表示します。

[表示の更新]
最新の情報を表示します。

※画面は例です。

ローカルサーバを設定する

LAN側のサーバをインターネット上に公開するときや、ネットワークゲームやチャットなどのアプリケーションを使うときは、ローカルサーバ機能を設定し、新規ユーザ定義サービスを追加します。

1 セキュリティのローカルサーバ画面で、[新規作成]または[追加]をクリックする。(☛P1-53)

2 ローカルサーバの追加の各項目を設定する。

[ローカルホスト]:
ローカルサーバを設定するパソコンのIPアドレス、またはドメイン名を入力します。
Unnumbered接続を設定している接続先を選択した場合のみ、ローカルホストの範囲指定が可能です。

[転送ポート]:
ポート番号を入力します。

[接続先]:
ローカルサーバを外部に公開する接続先(すべて、WAN PPPoE2～5)を選択します。

[サービス名]:
[アプリケーションサポート]
ローカルサーバを設定するアプリケーション(FTP、Ping、Traceroute、Windows共有フィルタ)を選択することができます。

3 [新規ユーザ定義サービス]をクリックする。

(次ページへ続きます)

4 [サービス名]、[サービスの説明] を入力し、[新規作成] をクリックする。

サービスの説明は入力しなくてもかまいません。

5 プロトコルを設定する。

[プロトコル] ：
対象にするプロトコルを TCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。TCP、UDP を選択したときは、送信元ポートと送信先ポートを選択し、入力してください。ICMP を選択したときは、ICMP メッセージを選択してください。

[送信元ポート] ／ [送信先ポート] ：
次のいずれかを選択し、サービスやアプリケーションのポート番号を入力します。

- すべて　　：すべてのポートを指定する
- 1 個を指定 ：1 つのポート番号を指定する
- 範囲を指定 ：ポート番号の範囲を指定する

6 [OK] をクリックする。

サービスの編集画面に戻ります。

7 [OK] をクリックする。

8 ユーザ定義サービスのサービス名をチェックし、[OK] をクリックする。

サービスを無効にする場合は、サービス名のチェックを外します。
ローカルホストにはパソコンのIPアドレス、またはホスト名が入力されていることを確認してください。

9 ローカルサーバ画面で、ローカルホストの設定を確認し、[OK] をクリックする。

ワンポイント

● 登録した［サービス］を削除する場合、［ローカルサーバの追加］画面の［ユーザ定義サービス］をクリックし、［ユーザ定義サービス］画面で削除してください。

セキュリティ

LAN 側のパソコンを DMZ ホストに設定する

DMZ ホスト機能を使用すると、LAN 側にある 1 台のパソコンをインターネット上に公開できます。次のようなときに DMZ ホスト機能を指定します。

・ネットワークやチャットのアプリケーションで、使用するポートの情報が公開されていない場合
・セキュリティの制限なしに、1 台のパソコンですべてのサービスをインターネットに公開する場合

インターネットから LAN 側へのアクセスを受け取ると、本商品はローカルサーバ機能で登録されている宛先を除き、すべて DMZ ホストへその要求を転送します。
ここでは、LAN 側のパソコンをインターネットに公開するための DMZ ホストの設定について説明します。

1 セキュリティの DMZ ホスト画面で、[DMZ ホスト IP アドレス] をチェックし、DMZ ホスト機能に設定するパソコンの IP アドレスを入力し、[OK] をクリックする。(☛P1-53)

[接続先] は、DMZ ホストを設定する接続先（すべて、WAN PPPoE2 ～ 5）を選択します。

2 [OK] をクリックする。

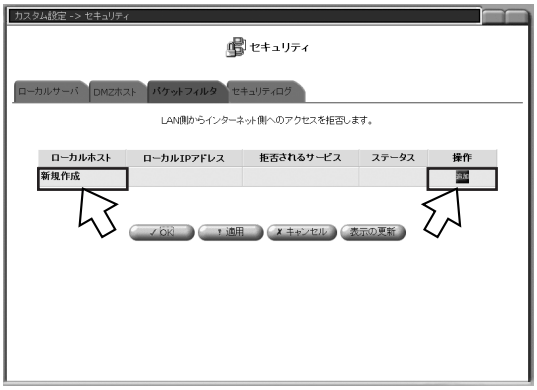
お知らせ

- DMZ ホストとして、複数のパソコンを設定することはできません。
- DMZ ホストとして設定したパソコンは、ファイアウォールで保護されていないため、外部から攻撃を受ける可能性があります。
- DMZ ホストとして設定したパソコンに対しては、不正アクセス検出はできません。

パケットフィルタルールを作成する

パケットフィルタルールを作成して、LAN側のパソコンがWAN側の特定のサービスにアクセスするのを防ぐことができます。

1 セキュリティのパケットフィルタ画面で、［新規作成］または［追加］をクリックする。（☛P1-54）



2 パケットフィルタルールを編集する。

［適用するIPアドレス］：
ルールを適用するIPアドレスを選択します。
［すべてのIPアドレス］を選択すると、LAN全体のIPを選択できます。一覧にないIPアドレスを適用する場合は、［新規］をクリックしてIPアドレスを設定するか、［編集］をクリックしてIPアドレスを編集します。
設定できる範囲は、0.0.0.1～255.255.255.255です。

［ユーザ定義サービス］：
本商品に登録されているサービスです。対象とするサービスをチェックします。

［アプリケーションサポート］：
本商品に登録されているアプリケーションです。対象とするアプリケーションをチェックします。
設定可能なアプリケーションは、FTP、Ping、Traceroute、Windows共有フィルタです。

3 ［OK］をクリックする。

ワンポイント

● 新規ユーザ定義サービスを登録するには

パケットフィルタルールの編集画面で［新規ユーザ定義サービス］をクリックして、サービスを追加することができます。

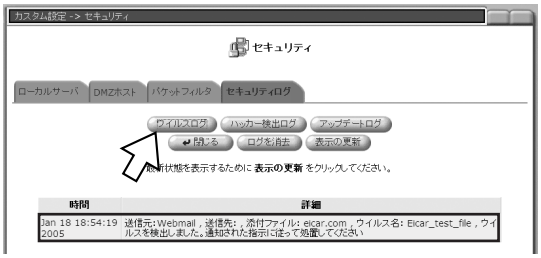
セキュリティ

セキュリティログを確認する

本商品では、セキュリティ関連のログを記録することができます。

●ウイルスが検出されたとき

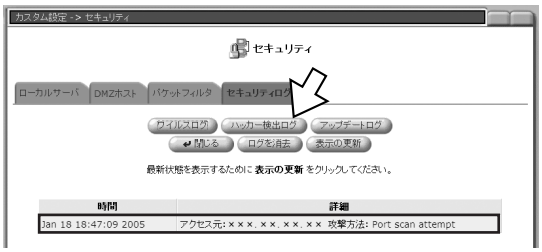
ウイルスが検出されると、本商品の VIRUS ランプが赤点灯し、ウイルスログに記録されます。
セキュリティログ画面の［ウイルスログ］をクリックしてウイルスログを表示することで、VIRUS ランプが緑点灯に変わります。



ウイルスログ（例）

●不正アクセスが検出されたとき

不正アクセスが検出されると、本商品の HACKER ランプが赤点灯し、ハッカー検出ログに記録されます。
セキュリティログ画面の［ハッカー検出ログ］をクリックしてハッカー検出ログを表示することで、HACKER ランプが緑点灯に変わります。



ハッカー検出ログ（例）

●アップデートが実行されたとき

セキュリティ対策ファイルのアップデートが実行されると、アップデートログに記録されます。セキュリティログ画面の［アップデートログ］をクリックして確認することができます。

アップデートログ（例）

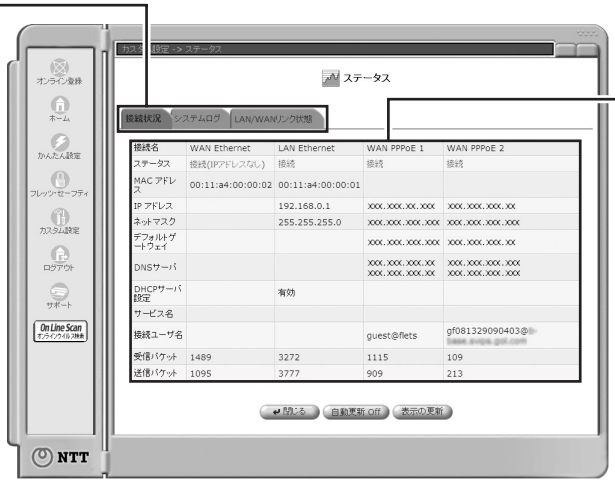
ステータス

ステータス画面では、ネットワークの接続状況、システムログ、LAN／WAN リンク状態を確認することができます。

ステータス画面

カスタム設定画面の［ステータス］をクリックすると、ステータス画面が表示されます。
ステータス画面では、［接続状況］、［システムログ］、［LAN／WAN リンク状態］の各タブをクリックすると、画面が切り替わります。

［接続状況］タブ
［システムログ］タブ
［LAN/WAN リンク状態］タブ



各ネットワークの接続状況が表示されます。

※画面は例です。

接続状況画面

接続状況画面では、ネットワークの接続状況を確認することができます。

ネットワークの接続状況が表示されます。

※画面は例です。

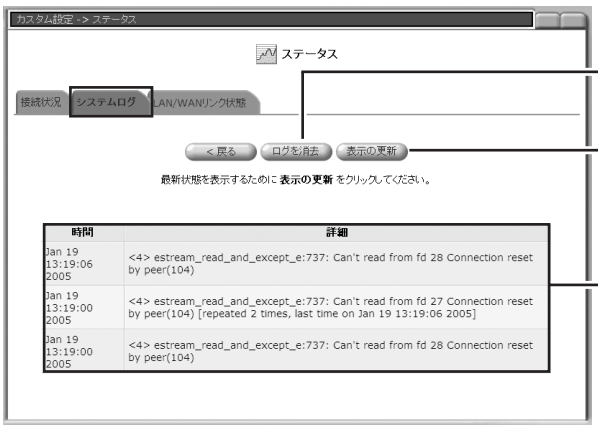
［自動更新 on］／［自動更新 off］
表示の自動更新のオン／オフを切り替えます。

［表示の更新］
最新の情報を表示します。

ステータス

システムログ画面

ステータス画面の［システムログ］タブをクリックすると、システムログ画面が表示されます。



［ログを消去］
システムログを消去します。

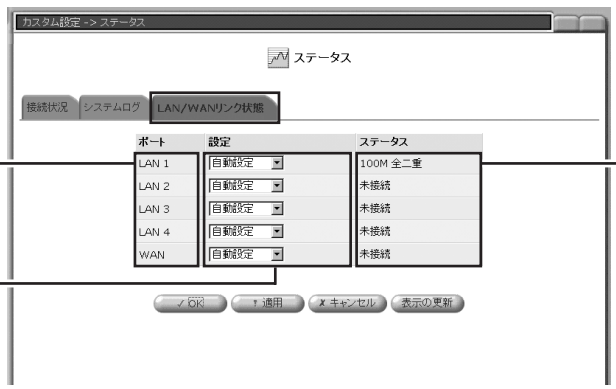
［表示の更新］
最新の情報を表示します。

システムログ画面が表示されます。

※画面は例です。

LAN／WAN リンク状態画面

ステータス画面の［LAN／WAN リンク状態］タブをクリックすると、LAN／WAN リンク状態画面が表示されます。



［ポート］
本商品の LAN1 ～ 4 ポート、WAN ポートを示します。

［設定］
［自動設定］、［100M 全二重］、［10M 全二重］、［100M 半二重］、［10M 半二重］のいずれかを選択します。お買い求め時は「自動設定」に設定されています。通常は変更する必要はありません。

［ステータス］
選択している接続の状態を示します。

※画面は例です。

ワンポイント

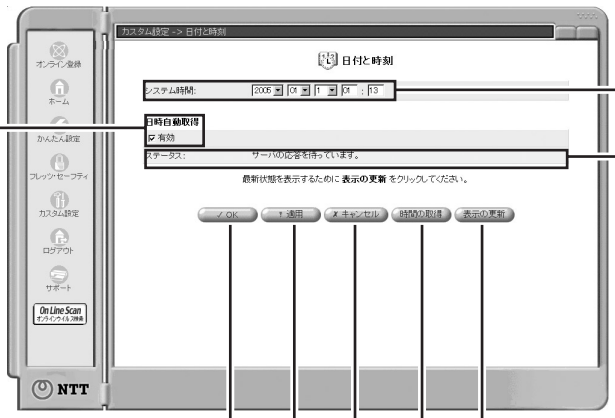
● **WAN ランプ、LAN ランプの表示について**
100 Mbps の場合は緑色、10 Mbps の場合は橙色のランプが点灯／点滅します。

日付と時刻

本商品はインターネット上のタイムサーバから日時を自動的に取得し、24 時間ごとに更新されます。5 か所のタイムサーバが登録されており、日時の取得に失敗した場合は、順次サーバを切り替えてアクセスします。
また、日時を手動で設定することもできます。お買い求め時は、日時自動取得が有効に設定されています。

日付と時刻画面

カスタム設定画面の［日付と時刻］をクリックすると、日付と時刻画面が表示されます。



[日時自動取得]
タイムサーバにアクセスして、日時の情報を自動取得するかどうかを設定します。
自動取得する場合は、［有効］をチェックします。

[システム時間]
年月日、時刻を指定します。

[ステータス]
現在の状態を表示します。

[OK]
日付と時刻を変更して、カスタム設定のトップ画面へ戻ります。

[適用]
設定した日付と時刻を適用します。

[表示の更新]
表示を更新します。

[時間の取得]
タイムサーバにアクセスして日時情報を取得します。

[キャンセル]
作業を中止して、カスタム設定のトップ画面へ戻ります。

日付と時刻を設定する

タイムサーバから日時を自動的に取得しないで、日付と時刻を手動で設定します。

1 日付と時刻画面で、［日時自動取得］で［有効］のチェックを外し、システム時間を設定する。

2 ［OK］をクリックする。

パスワードの変更

本商品の Web 設定画面にログインするためのログインパスワードを変更することができます。

パスワードの設定画面

カスタム設定画面の［パスワードの変更］をクリックすると、パスワードの変更画面が表示されます。

［新しいログインパスワード］
新しいパスワードを入力します。任意の文字を半角英数字 64 文字以内で入力します。半角スペースも入力できます。

［新しいログインパスワードの確認再入力］
同じパスワードをもう一度入力します。

［OK］
設定を変更してログイン画面へ戻ります。
パスワードを変更していない場合はカスタム設定のトップ画面へ戻ります。

［キャンセル］
作業を中止して、カスタム設定のトップ画面へ戻ります。

パスワードを変更する

ログインパスワードを変更します。設定したログインパスワードは、取扱説明書の設定記入シートへ記入しておくことをお勧めします。

1 パスワードの変更画面で、［新しいログインパスワード］、［新しいログインパスワードの確認再入力］にパスワードを入力する。

以前設定したパスワードが●●●●●●●●または＊＊＊＊＊＊＊＊と表示されますので、消去してから、新しいパスワードを半角英数字 64 文字以内で入力します。
入力したパスワードは、●●●または＊＊＊で 18 桁まで表示されます。
18 文字を超えて入力された場合、18 桁以上は表示されませんが、入力したパスワードは記録されていますので問題ありません。

※パスワードを空欄のままにすることもできますが、パスワードを設定しないとセキュリティ上のリスクを高めることになります。
※パスワードは、忘れないように必ずメモして安全な場所に保管してください。
※パスワードを忘れた場合は、本商品を初期化して設定を初めからやり直してください。（☛P1-76）

お知らせ

- 入力したパスワードの表示桁数は、お使いのパソコンによって異なる場合があります。

2 ［OK］をクリックする。

対象ファイルの手動アップデート

対象ファイルを手動でアップデートするときは下記の方法でアップデートします。

手動でアップデートする

Web 設定のホーム画面で、ファームウェアおよびセキュリティ対策ファイル（パターンファイル、検索エンジン、ファイアウォールルール）の最新情報を取得した際に、更新されたバージョンがある場合は、手動でアップデートができます。

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P1-2）

2 ホーム画面の［最新情報の取得］をクリックする。

バージョン情報が更新されます。

お知らせ

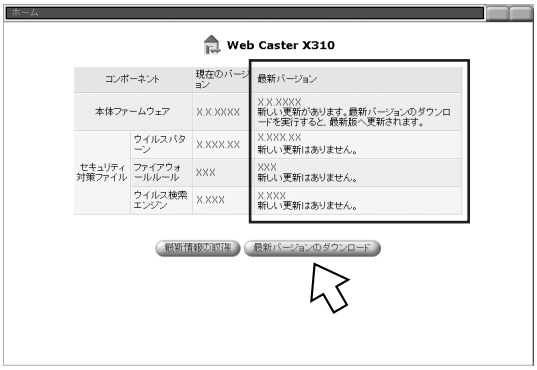
- 最新バージョン欄に「更新の確認に失敗しました。」と表示されているときは、フレッツ・セーフティのオンライン登録をしていないか、または最新情報の取得に失敗したことを示しています。
- フレッツ・セーフティのオンライン登録済の場合で、最新バージョン欄に［更新の確認に失敗しました。］と表示されるときは、サーバとの接続に失敗した可能性がありますので、しばらく待ってからもう一度確認してください。
- フレッツ・セーフティのオンライン登録をしていない場合は、セキュリティ対策ファイルの最新バージョンの取得はできません。

（次ページへ続きます）

対象ファイルの手動アップデート

3 ファームウェアとセキュリティ対策ファイルのバージョンを確認し、新しいバージョンがあるときは、[最新バージョンのダウンロード] をクリックし、ダウンロードとアップデートを実行する。

・新しいバージョンのセキュリティ対策ファイルがある場合：
手順４へ進みます。
・新しいバージョンのファームウェアがある場合：
手順５へ進みます。



4 新しいバージョンのセキュリティ対策ファイルがある場合、VIRUS ランプと HACKER ランプが遅い点滅（緑）をし、アップデートを行う。

アップデートが完了するとセキュリティ対策ファイルの現在のバージョンが更新されます。
・手順８へ進みます。

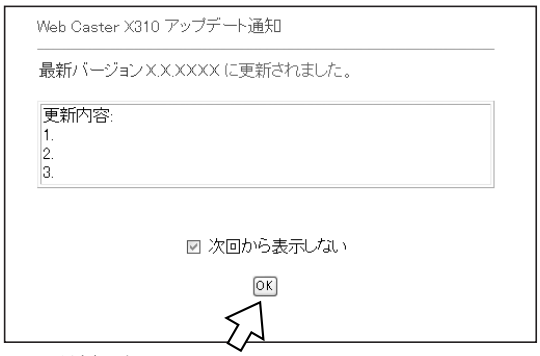
5 新しいバージョンのファームウェアがある場合、VIRUS ランプと HACKER ランプが早い点滅（緑）をし、アップデートを行う。

6 アップデートが完了すると、本商品が再起動し、ログイン画面が表示されるので、パスワードを入力し、ログインする。(☛P1-2)

ログイン画面が表示されない場合は、Web ブラウザの［更新］ボタンなどを押してください。

7 最新バージョンへ更新されたことをお知らせする画面が表示されるので［OK］をクリックする。

Web 設定画面のホーム画面が表示されます。



※画面は例です。

8 ホーム画面の［最新情報の取得］をクリックする。

バージョン情報が更新されます。

9 現在のバージョンと最新バージョンが同じであることを確認する。

お知らせ

● ダウンロードとアップデートが完了するまで本商品の電源アダプタは絶対に抜かないでください。

対象ファイルの手動アップデート

ローカルファイルからアップデートする

当社ホームページから最新のファームウェアファイルをパソコンへダウンロードし、本商品をアップデートすることができます。
ダウンロードの方法など、詳しくは当社のホームページを参照してください。

- NTT 東日本のホームページ： http://www.ntt-east.co.jp/ced/
- NTT 西日本のホームページ： http://www.ntt-west.co.jp/kiki/

1 当社のホームページより最新のファームウェアをダウンロードする。

ハードディスクの任意のフォルダにファームウェアファイルをダウンロードします。

2 Web ブラウザを起動して、Web 設定画面を開く。（☛P1-2）

ホーム画面で、ダウンロードしたファームウェアのバージョンが、現在使用しているファームウェアよりも新しいことを確認してください。

3 [カスタム設定] をクリックする。

お知らせ

- 最新バージョン欄に「更新の確認に失敗しました。」と表示されているときは、フレッツ・セーフティのオンライン登録をしていないか、または最新情報の取得に失敗したことを示しています。
- フレッツ・セーフティのオンライン登録済の場合で、「更新の確認に失敗しました。」と表示されるときは、サーバとの接続に失敗した可能性がありますので、しばらく待ってからもう一度確認してください。
- フレッツ・セーフティのオンライン登録をしていない場合は、セキュリティ対策ファイルの最新バージョンの取得はできません。

4 [ファームウェアアップデート] をクリックする。

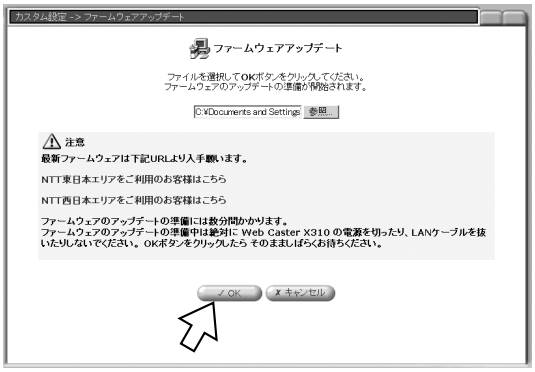
5 [参照] をクリックする。

6 ファームウェアファイルを選択し、[開く] をクリックする。

OS によって画面や操作が異なります。

7 [OK] をクリックする。

ファームウェアのアップデートの準備が開始されます。



お知らせ

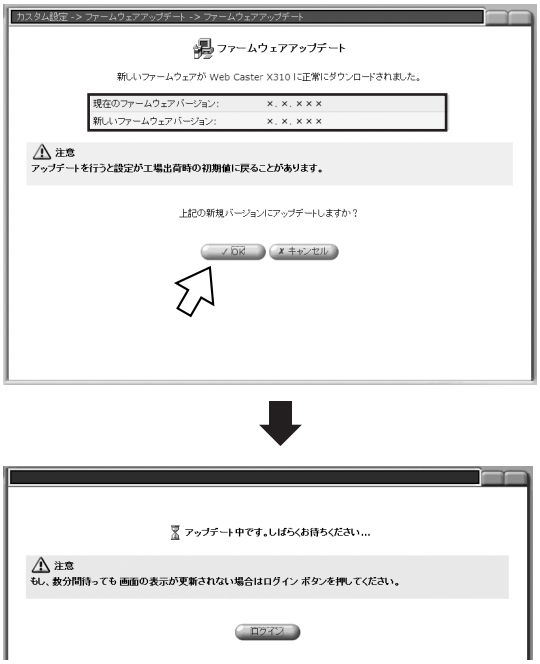
- ファームウェアのアップデートの準備中は、絶対に本商品の電源アダプタを抜いたり、LAN ケーブルを抜いたりしないでください。ファームウェアのアップデートの準備には、数十秒間かかります。[OK] をクリックしたら、そのままお待ちください。

（次ページへ続きます）

対象ファイルの手動アップデート

8 ファームウェアのバージョンを確認し、［OK］をクリックする。

ファームウェアがアップデートされます。
アップデート中は VIRUS ランプと HACKER ランプが速い点滅（緑）をします。



9 アップデートが完了すると、本商品が再起動し、ログイン画面が表示されるので、パスワードを入力し、ログインする。（☛P1-2）

10 ホーム画面の［最新情報の取得］をクリックする。

バージョン情報が更新されます。

11 現在のバージョンと最新バージョンが同じであることを確認する。

お知らせ

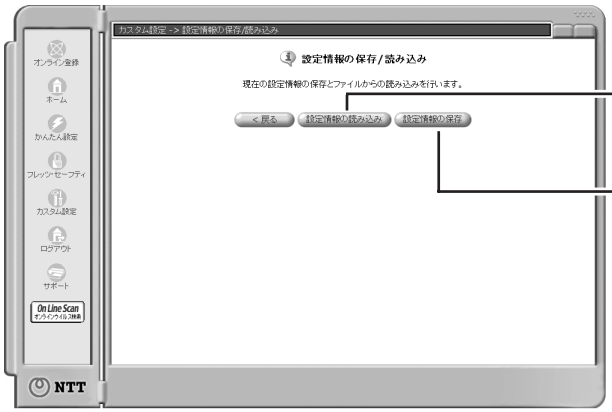
● アップデートが完了するまで本商品の電源アダプタは絶対に抜かないでください。

設定情報の保存／読み込み

本商品の設定情報の保存、読み込みを行います。

設定情報の保存／読み込み画面

カスタム設定画面の［設定情報の保存／読み込み］をクリックすると、設定情報の保存／読み込み画面が表示されます。



［設定情報の読み込み］
保存した設定情報を読み込みます。

［設定情報の保存］
設定情報を保存します。

設定情報を保存する

1 設定情報の保存／読み込み画面で、［設定情報の保存］をクリックする。

（次ページへ続きます）

設定情報の保存／読み込み

2 [保存] をクリックする。

※表示される画面は、パソコンの OS によって異なります。画面の指示に従って操作してください。

3 ファイル名を入力し、[保存] をクリックする。

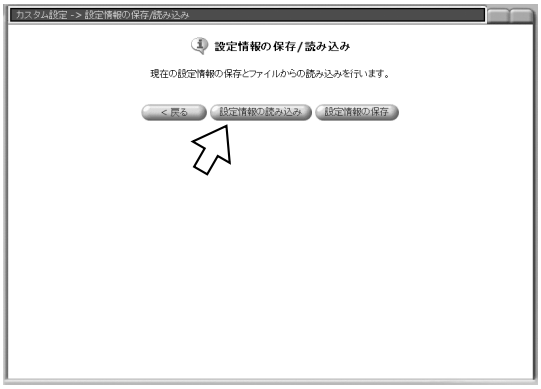
「ダウンロードの完了」画面が表示された場合は、[閉じる] をクリックします。

お知らせ

● 保存した情報には、プロバイダの接続ユーザ名、パスワードなどが含まれていますのでご注意ください。

設定情報を読み込む

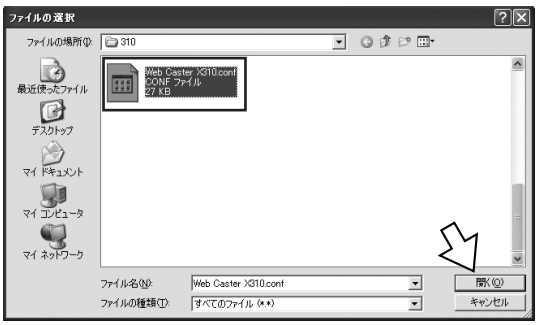
1 設定情報の保存／読み込み画面で、［設定情報の読み込み］をクリックする。



2 ［参照］をクリックする。

3 設定情報ファイルを選択し、［開く］をクリックする。

※表示される画面は、パソコンのOSによって異なります。画面の指示に従って操作してください。

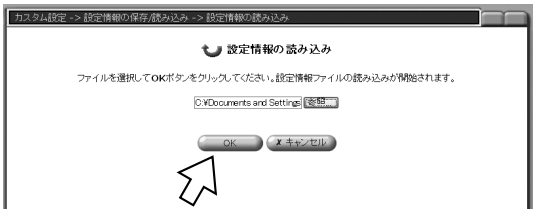


（次ページへ続きます）

設定情報の保存／読み込み

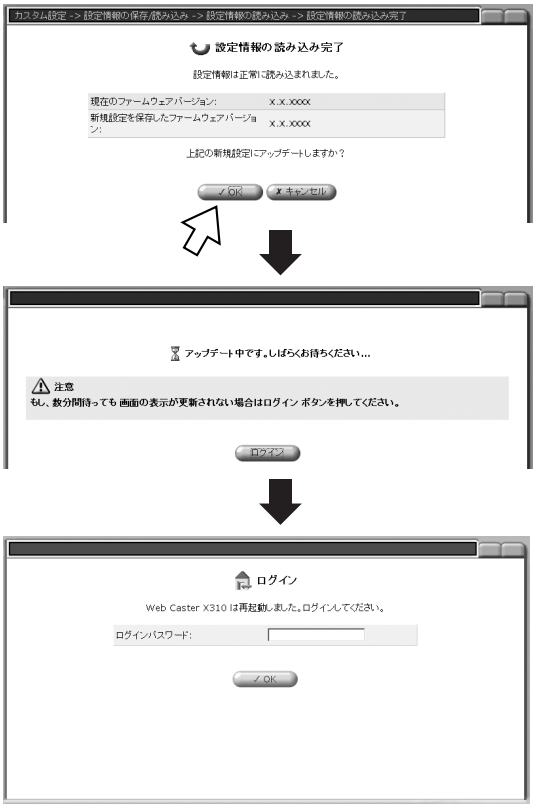
4 **[OK] をクリックする。**

設定情報ファイルの読み込みが開始されます。



5 **[OK] をクリックする。**

アップデート後本商品が再起動され、ログイン画面が表示されます。



お知らせ

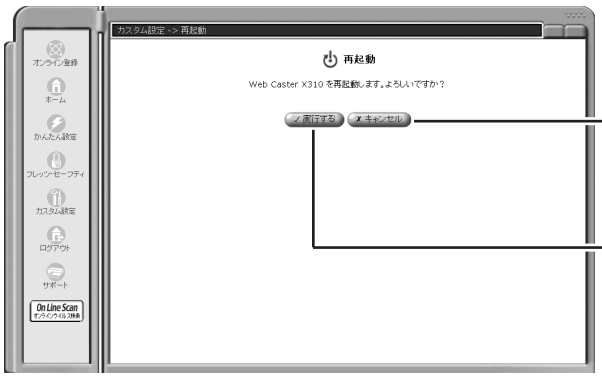
- アップデートが完了するまで本商品の電源アダプタは絶対に抜かないでください。

再起動

設定内容を保存して、本商品を再起動します。
再起動には、本商品の RESET スイッチを使う方法、Web 設定画面から行う方法があります。

再起動画面

カスタム設定画面の［再起動］をクリックすると、再起動画面が表示されます。

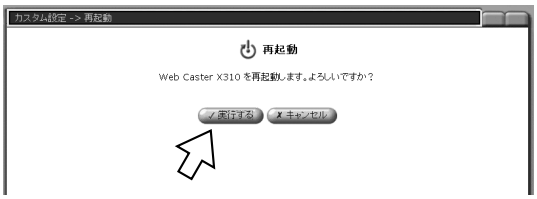


［キャンセル］
作業を中止して、カスタム設定のトップ画面へ戻ります。

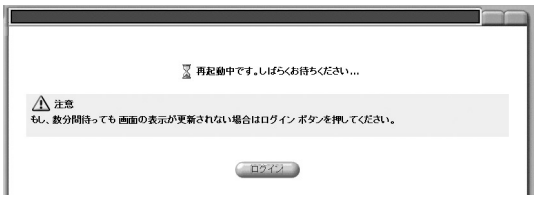
［実行する］
本商品を再起動して、ログイン画面へ戻ります。

本商品を再起動する

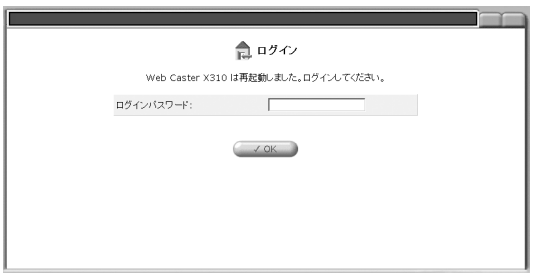
1 再起動画面で［実行する］をクリックする。



本商品が再起動されます。



再起動後、ログイン画面が表示されます。



ワンポイント

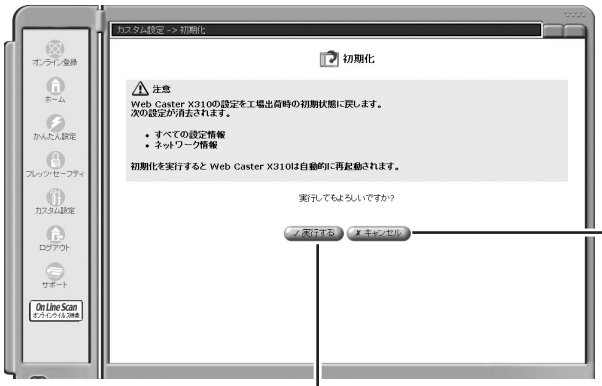
● **RESET スイッチを使って再起動するには**
先のとがったもので、本商品の背面にある RESET スイッチを押して再起動することもできます。

初期化

本商品の設定情報、ネットワーク情報、および各種ログ情報をすべて消去して、お買い求め時の状態に戻します。

初期化画面

カスタム設定画面の［初期化］をクリックすると、初期化画面が表示されます。
この画面では、本商品を初期化することができます。



[キャンセル]
作業を中止して、カスタム設定のトップ画面へ戻ります。

[実行する]
設定情報、ネットワーク情報、および各種ログ情報を初期化して、自動的に再起動します。

本商品を初期化する

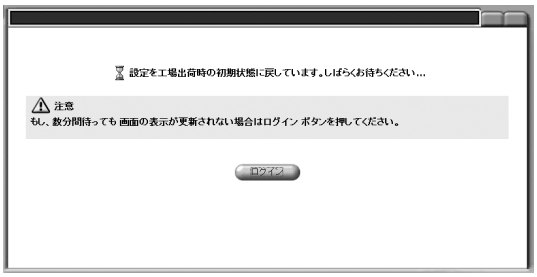
本商品を初期化します。

1 初期化画面で［実行する］をクリックする。

お知らせ

- 本商品が正常に動作しない場合や、今までとは異なる回線に接続し直す場合は、本商品を初期化して初めから設定し直すことをお勧めします。
  いったん初期化すると、それまでに設定した値はすべて消去され、お買い求め時の状態に戻りますのでご注意ください。

初期化が開始されます。終了すると、自動的に本商品が再起動し、ログイン画面が表示されます。



初期化には約３分かかります。
HACKER ランプと VIRUS ランプが緑点灯したままになったら、初期化は完了です。

※初期化が完了するまで、本商品の電源アダプタは絶対に抜かないでください。

ワンポイント

● RESET スイッチを使って初期化するには

先のとがったもので、本商品の背面にある RESET スイッチを押しながら、電源アダプタを差し込んで初期化することもできます。

① 先のとがったもので RESET スイッチを押しながら、電源アダプタのプラグを差し込みます。
HACKER ランプ、VIRUS ランプ、PPPoE ランプが点灯したら RESET スイッチを離します。
② 初期化が終了すると本商品が再起動されます。
③ HACKER ランプと VIRUS ランプが緑点灯したままになったら、初期化は完了です。
初期化には約３分かかります。
※初期化が完了するまで、本商品の電源アダプタは絶対に抜かないでください。

● 設定が初期化される情報

初期化を実行すると、すべての設定情報、ネットワーク情報、および各種ログ情報が消去されます。

お知らせ

- お使いの Web ブラウザによっては、ログイン画面が表示されない場合があります。
この場合は、あらためてログインしてください。（☛P1-2）
- 本商品に設定するユーザ名やパスワードは重要な個人情報です。情報を盗まれると悪用される可能性がありますので、情報の管理には十分お気をつけください。本商品を当社に返却したり破棄したりする場合など、本商品の利用をやめる際は、必ず初期化を行い、設定された情報を消去してください。
- 本商品を初期化しても、フレッツ・セーフティのオンライン登録を再度行っていただく必要はありません。

オンラインウイルス検索

パソコンのウイルスを検索、駆除するオンラインウイルス検索を提供しています。オンラインウイルス検索は、ActiveX コントロールを利用してウイルスを検出するツールです。
本商品のセキュリティ機能とオンラインウイルス検索を併用することで、より強固なウイルス対策を実現することができます。本商品で E-mail、Web メールに対してウイルス検索を実行する一方、オンラインウイルス検索でお使いのパソコンおよびネットワーク上のドライブに対してウイルス検索を実行することができます。
※オンラインウイルス検索の動作や内容に関してのお問い合わせについては、フレッツ・セーフティと本商品のサポート対象外です。

1 Web ブラウザを起動して、Web 設定画面を開く。(☛P1-2)

2 Web 設定画面左下の[オンラインウイルス検索]をクリックする。

オンラインウイルス検索を行うために必要なコンポーネントをダウンロードします。ダウンロードが始まると右のような画面が表示されます。
※サーバの混雑具合などにより、ダウンロード開始までに時間がかかることがあります。

セキュリティ警告の画面が表示された場合は、[はい]をクリックします。
「Cookie を有効にする必要があります。」の画面が表示された場合は、Cookie を有効にしてから再度実行してください。
Windows® XP サービスパック２の場合は、情報バーにメッセージが表示される場合があります。画面の指示に従って、ActiveX コントロールをインストールしてください。

お知らせ

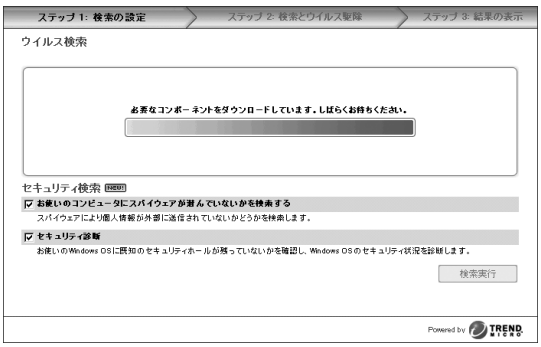
- オンラインウイルス検索を実行するには、下記の条件を満たすパソコンが必要です。
  - ・OS ： Windows® XP/Me/98SE/98、Windows® 2000 Professional
  - ・ソフトウェア： Internet Explorer 5.5 サービスパック２以降
  - ・CPU ： 386 DX（486 DX以上推奨）
  - ・RAM ： 4MB（8 MB以上推奨）
  - ・ハードディスク： 10 MB以上のディスク空き容量

  オンラインウイルス検索は、Mac OS には対応していません。
- 手順２で、ActiveX コントロールのダウンロード画面が表示される場合があります。
- Internet Explorer で ActiveX コントロールを有効にしてください。[ツール] メニューの「インターネットオプション」をクリックし、[セキュリティ]タブの［レベルのカスタマイズ］をクリックし、有効になっているかどうかを確認してください。
- フレッツ・セーフティにご契約いただいていない場合は、オンラインウイルス検索の一部の機能はご利用になれません。本商品のオンライン登録を行い、フレッツ・セーフティに契約してください。(☛P1-12)
- フレッツ・セーフティにご契約いただいていない場合は、手順と画面が一部異なりますので、画面の指示に従って操作してください。
- オンラインウイルス検索の画面は例です。

3 ウイルスバスターオンラインスキャン画面のボタンをクリックする。

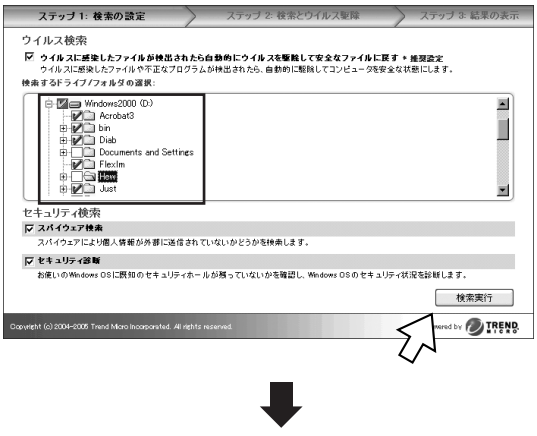
オンラインウイルス検索を行うために必要なコンポーネントをダウンロードします。ダウンロードが始まると右のような画面が表示されます。

※サーバの混雑具合などにより、ダウンロード開始までに時間がかかることがあります。



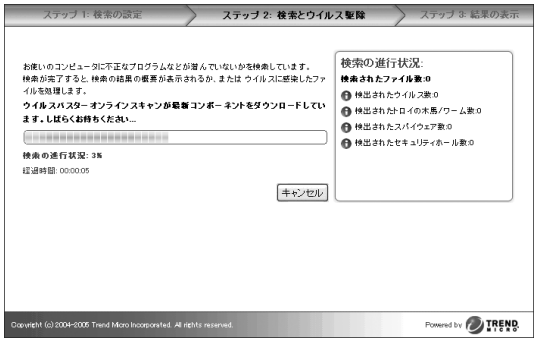
4 ウイルス検索を行うドライブまたはフォルダをチェックし、［検索実行］をクリックする。

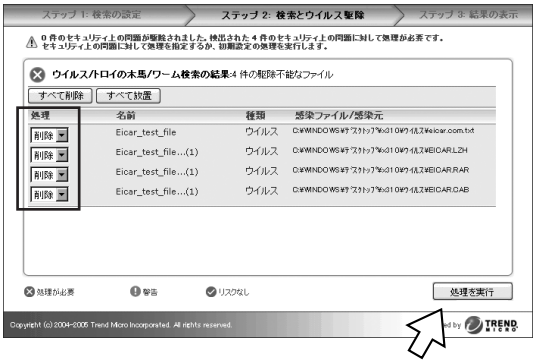
はじめてオンラインウイルス検索を行う場合は、ウイルスの検出に時間がかかることがあります。



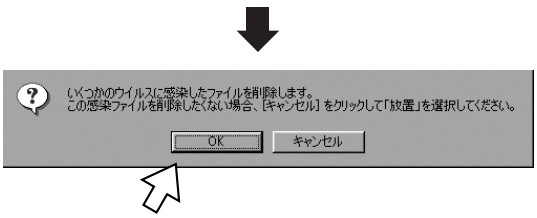
（次ページへ続きます）

オンラインウイルス検索





感染ファイルが発見された場合：
検出されたファイルのリストが表示されます。処理を選択し、［処理を実行］をクリックし、［OK］をクリックします。

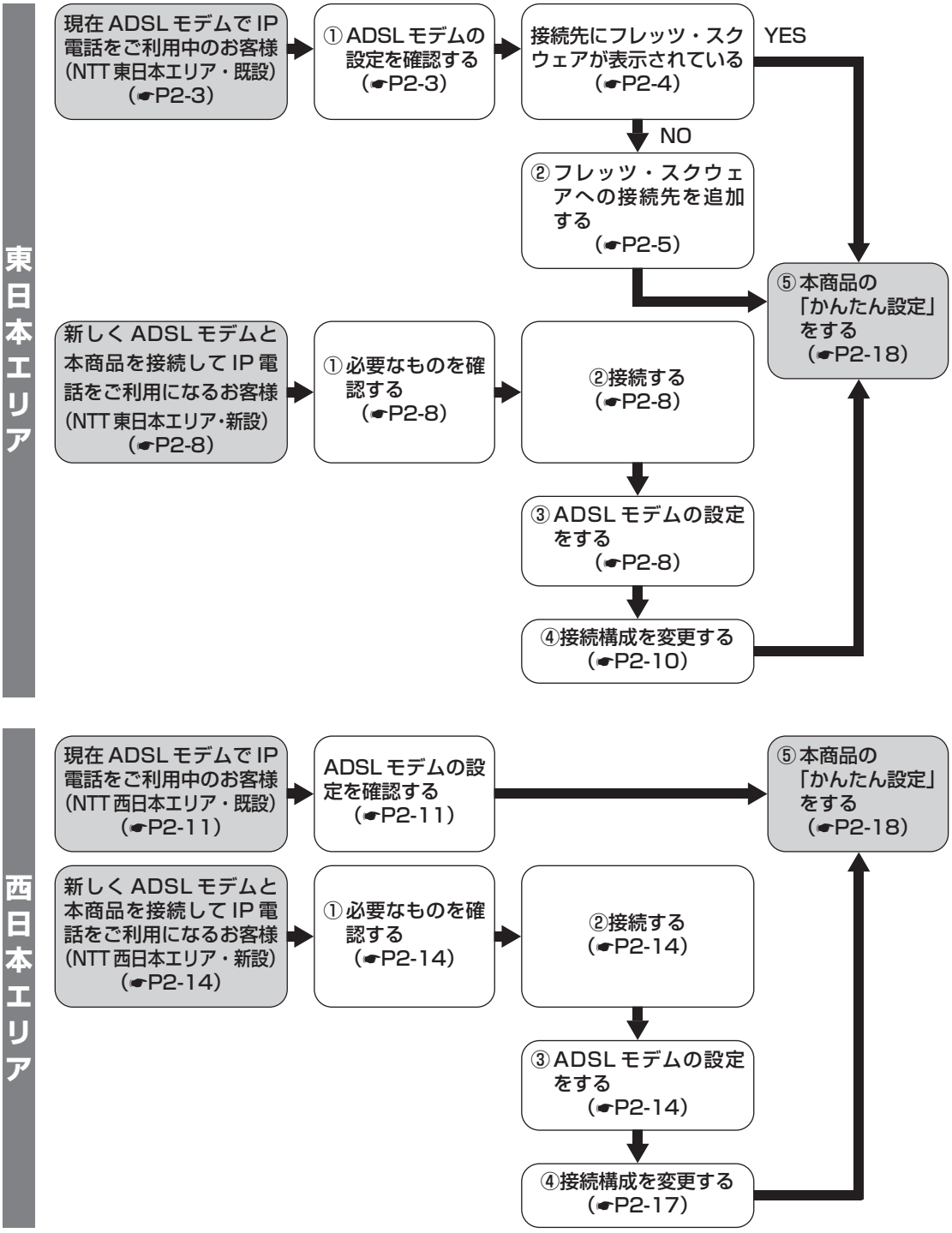


5 ウイルスが検出されなかった場合は、［閉じる］をクリックして終了する。

2 こんなときにはこの設定

IP電話対応ADSLモデムと本商品を接続して利用するには

ここでは、IP電話対応ADSLモデムと本商品を接続してご利用になる場合の設定方法について説明します。代表的な例として、ADSLモデムNVⅢ（NTT東日本エリア）とADSLモデムSVⅢ（NTT西日本エリア）の設定方法を紹介しますので、他のADSLモデムをお使いの場合は、参考にしてください。
次の図を参照し、該当するページをお読みください。

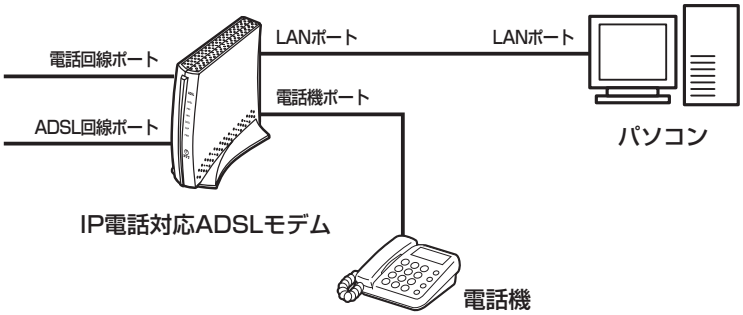


現在 ADSL モデムで IP 電話をご利用中のお客様（NTT 東日本エリア・既設）

現在の ADSL モデムの設定でフレッツ・スクウェアへの接続先が設定されているかどうかを確認し、設定されていない場合は接続先を追加します。操作手順は、ADSL モデム NV Ⅲをお使いになる場合の例です。

①接続を確認する

IP 電話対応 ADSL モデムとパソコン、電話機が下図のように接続されていることを確認してください。



② ADSL モデムの設定を確認する

1 Web ブラウザを起動し、アドレス欄に「http://ntt.setup/」と入力して［Enter］キーを押す。

2 ユーザー名「user」と管理者パスワードを入力し、［OK］をクリックする。

NV Ⅲの Web 設定画面が表示されます。

ワンポイント

●管理者パスワードを忘れた場合は

NV Ⅲを初期化して、設定を初めからやり直してください。

お知らせ

●手順と画面の詳細は、ADSL モデム NV Ⅲの取扱説明書を参照してください。

（次ページへ続きます）

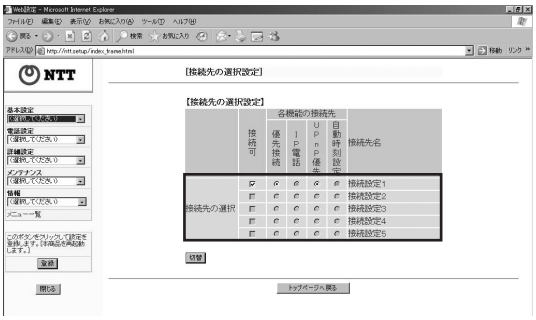
IP電話対応ADSLモデムと本商品を接続して利用するには

3 基本設定の［接続先の選択設定］をクリックする。

4 「フレッツ・スクウェア（東日本）」が表示されているかどうかを確認する。

●「フレッツ・スクウェア」が表示されている場合
これでADSLモデムの設定は完了です。
引き続き、「⑤本商品のかんたん設定をする」へ進んでください。（☛P2-18）

●「フレッツ・スクウェア」が表示されていない場合
「②フレッツ・スクウェアへの接続先を追加する」へ進んでください。（☛P2-5）



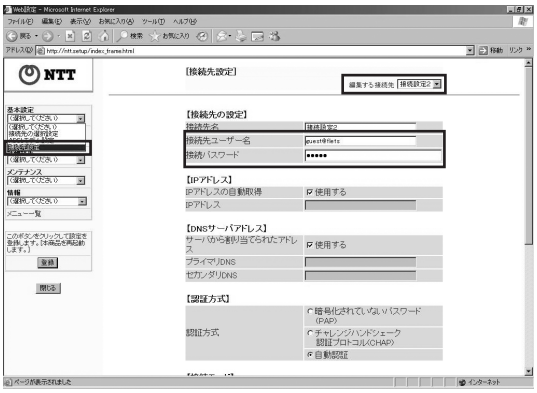
ワンポイント

●初期化について
初期化とは、NV Ⅲに設定した内容を消去してお買い求め時の状態に戻すことをいいます。NV Ⅲが正常に動作しない場合や今までとは異なる回線に接続し直す場合は、NV Ⅲを初期化して初めから設定し直すことをお勧めします。いったん初期化すると、それまでに設定した値はすべて消去され、お買い求め時の状態に戻りますのでご注意ください。
初期化を行った場合は、「新しくADSLモデムと本商品を接続してIP電話をご利用になるお客様（NTT東日本エリア・新設）」（☛P2-8）の手順により設定してください。
①いったんNV Ⅲの電源アダプタを抜く。
②NV Ⅲの電源アダプタを差し込む。
③PPPランプが緑点灯している間にINITスイッチを押す。
（NV ⅢのPWRランプ以外の全ランプが緑点滅を開始するまで押し続ける）
NV Ⅲの全ランプが緑点灯してお買い求め時の状態に初期化されます。
ADSLランプが緑点滅を開始したら初期化は完了です。
※初期化が完了するまでNV Ⅲの電源アダプタは絶対に抜かないでください。

②フレッツ・スクウェアへの接続先を追加する

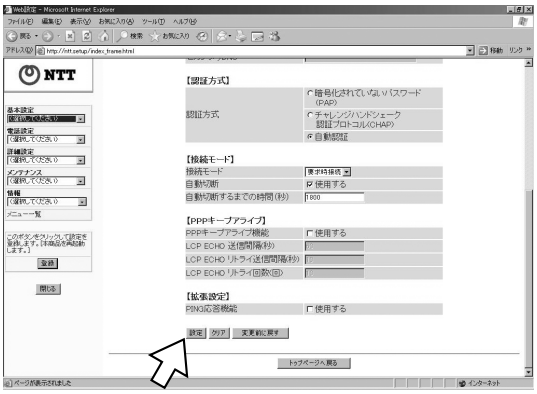
1 基本設定の［接続先設定］をクリックして、［接続設定2］を選択する。

［接続先ユーザー名］、［接続パスワード］を入力します。
お住まいのエリアに合わせて、次のように入力してください。
・NTT東日本エリアのお客様
［接続先ユーザー名］：guest@flets
［接続パスワード］　：guest

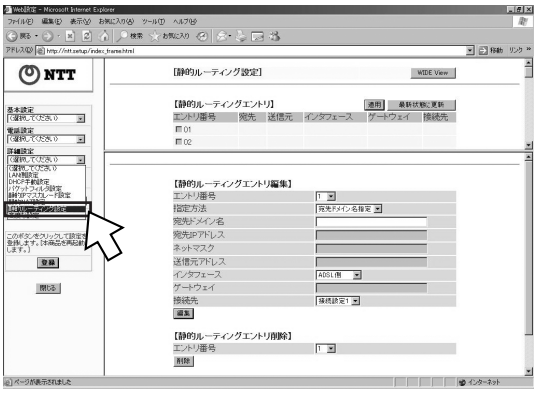


2 ［設定］をクリックする。

続けてフレッツ・スクウェアへの接続ルールを追加します。



3 詳細設定の［静的ルーティング設定］をクリックする。

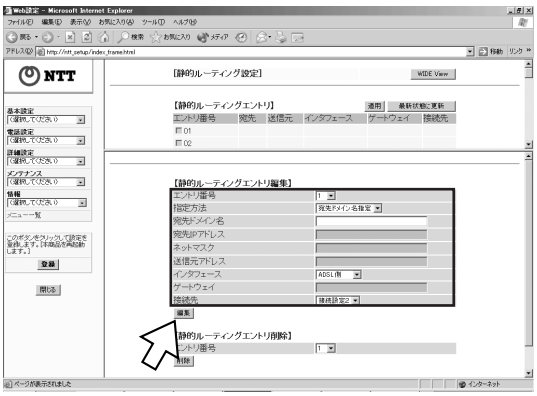


（次ページへ続きます）

IP 電話対応 ADSL モデムと本商品を接続して利用するには

4 静的ルーティングエントリ編集の設定をして、［編集］をクリックする。

次のように設定してください。
［エントリ番号］　：「1」を選択します。
［指定方法］　：「宛先ドメイン名指定」を選択します。
［宛先ドメイン名］：「.flets」と入力します。
［インタフェース］：「ADSL 側」を選択します。
［接続先］　：「接続設定 2」を選択します。



5 ［最新状態に更新］をクリックする。

6 ［エントリ番号 01］をチェックし、［適用］をクリックする。

7 ［基本設定］のメニューから［接続先の選択設定］をクリックする。

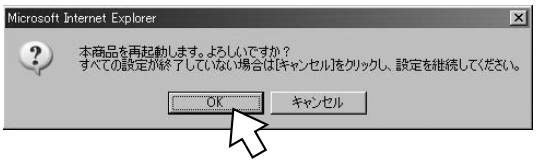
8 ［接続先の選択設定］の［接続設定 2］の［接続可］をチェックし、［切替］をクリックする。

9 ［OK］をクリックする。

10 ［登録］をクリックする。

11 ［OK］をクリックする。

NV Ⅲが再起動されます。



12 [OK] をクリックする。

13 Web ブラウザを起動し、アドレス欄に「http://ntt.setup/」と入力して［Enter］キーを押す。

14 ユーザ名「user」と管理者パスワードを入力し、［OK］をクリックする。
NV ⅢのWeb設定画面が表示されます。

15 接続先２の［接続］をクリックする。

16 [OK] をクリックする。

17 [最新状態に更新] をクリックする。
引き続き、「④接続構成を変更する」へ進んでください。（☛P2-17）

IP 電話対応 ADSL モデムと本商品を接続して利用するには

新しく ADSL モデムと本商品を接続して IP 電話をご利用になるお客様（NTT 東日本エリア・新設）

IP 電話対応 ADSL モデムと本商品を接続して IP 電話をご利用になる場合は、次のように接続、設定してください。

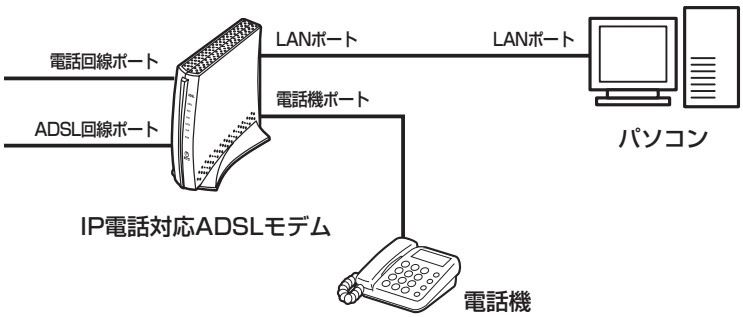
①必要なものを確認する

事前に次のものをご準備ください。

・フレッツ・ ADSL 開通時に送付される**「開通のご案内」（NTT 東日本）**
・インターネット接続のための**プロバイダ情報**
・ADSL モデム付属の**マニュアル**

②接続する

ADSL モデム付属のマニュアルに従って、IP 電話対応 ADSL モデムとパソコン、電話機を下図のように接続します。

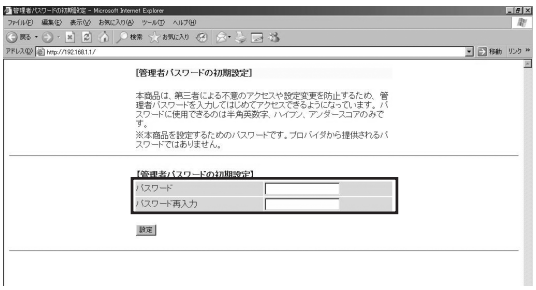


③ ADSL モデムの設定をする

操作手順は、NTT 東日本エリアで ADSL モデム NV Ⅲをお使いになる場合の例です。

1 Web ブラウザを起動し、アドレス欄に「http://ntt.setup/」と入力して［Enter］キーを押す。

2 管理者パスワードを設定する。



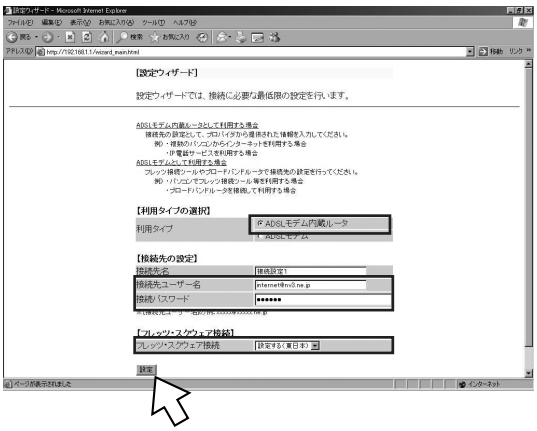
お知らせ

● 手順と画面の詳細は、ADSL モデム NV Ⅲの取扱説明書を参照してください。

3 設定ウィザードで次のように設定し、［設定］をクリックする。

［利用タイプ］：
「ADSL モデム内蔵ルータ」を選択します。
［接続先ユーザー名］、［接続パスワード］：
プロバイダ情報に従って入力します。
［フレッツ・スクウェア接続］：
「設定する（東日本）」を選択します。

設定が反映され、NV Ⅲが自動的に再起動します。



お知らせ

●接続先ユーザー名、接続パスワードを誤って入力すると、インターネットに正常に接続できません。

4 IP 電話の設定をする。

ADSL モデム付属のマニュアルに従って、IP 電話の設定を行ってください。

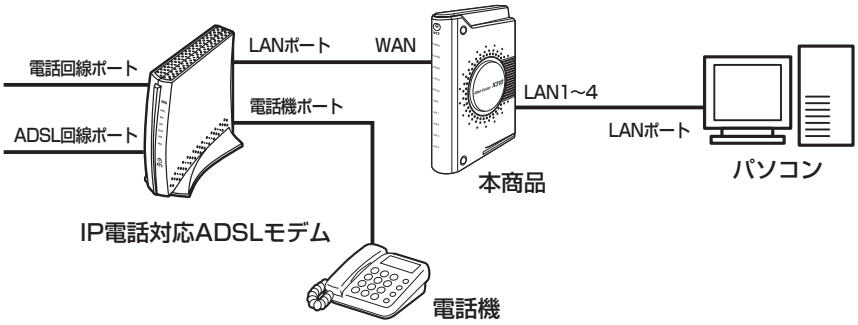
これで ADSL モデムの接続、設定は完了です。

（次ページへ続きます）

IP 電話対応 ADSL モデムと本商品を接続して利用するには

④接続構成を変更する

本商品を設定するために、下図のように接続構成を変更します。IP 電話対応 ADSL モデムとパソコンの間に本商品を接続してください。



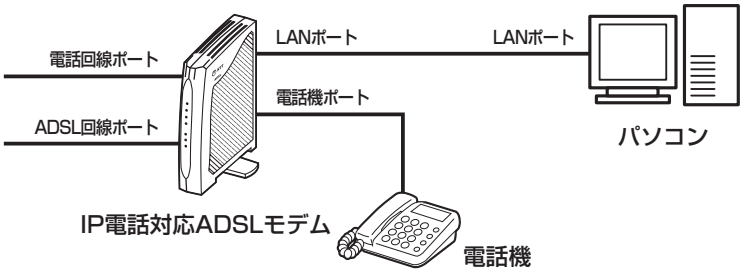
引き続き、「⑤本商品のかんたん設定をする」へ進んでください。（☛P2-18）

現在 ADSL モデムで IP 電話をご利用中のお客様（NTT 西日本エリア・既設）

現在の ADSL モデムの設定でフレッツ・スクウェアへの接続先が設定されているかどうかを確認し、設定されていない場合は接続先を追加します。操作手順は、ADSL モデム SV Ⅲをお使いになる場合の例です。

①接続を確認する

IP 電話対応 ADSL モデムとパソコン、電話機が下図のように接続されていることを確認してください。



② ADSL モデムの設定を確認する

1 Web ブラウザを起動し、アドレス欄に「http://ntt.setup/」と入力して［Enter］キーを押す。

2 ユーザー名「user」と管理者パスワードを入力し、［OK］をクリックする。

SV Ⅲの基本設定画面が表示されます。

ワンポイント

● 管理者パスワードを忘れた場合は

SV Ⅲを初期化して、設定を初めからやり直してください。

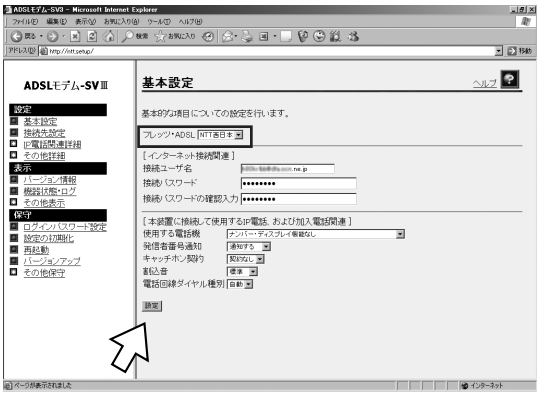
お知らせ

● 手順と画面の詳細は、ADSL モデム SV Ⅲの取扱説明書を参照してください。

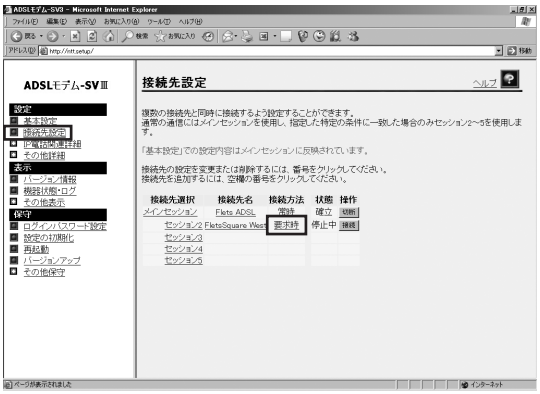
（次ページへ続きます）

IP電話対応ADSLモデムと本商品を接続して利用するには

3 「フレッツ・ADSL（NTT西日本）」が表示されているかどうかを確認し、［設定］をクリックする。



4 左側メニューの［接続先設定］をクリックして、セッション２の接続方法が［要求時］になっていることを確認する。



ワンポイント

●初期化について

初期化とは、SV Ⅲに設定した内容を消去してお買い求め時の状態に戻すことをいいます。SV Ⅲが正常に動作しない場合や今までとは異なる回線に接続し直す場合は、SV Ⅲを初期化して初めから設定し直すことをお勧めします。いったん初期化すると、それまでに設定した値はすべて消去され、お買い求め時の状態に戻りますのでご注意ください。

初期化を行った場合は、「新しくADSLモデムと本商品を接続してIP電話をご利用になるお客様（NTT西日本エリア・新設）」（☛P2-14）の手順により設定してください。

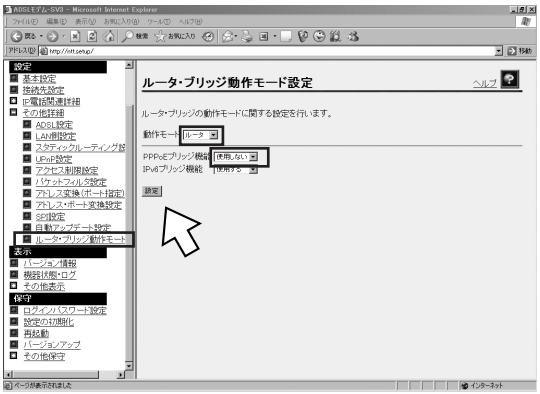
①SV Ⅲに電源をいれた状態で本体背面にある初期化スイッチ（INIT）を前面のADSL、PPP、LANおよびアラームの各ランプが点滅するまで約５秒間押します。

②SV Ⅲの情報を初期化して初期設定で再起動します。初期設定で起動するとPPPランプが橙色に点滅します。（ADSLのトレーニングが開始されると消灯します。）

※初期化が完了するまでSV Ⅲの電源アダプタは絶対に抜かないでください。

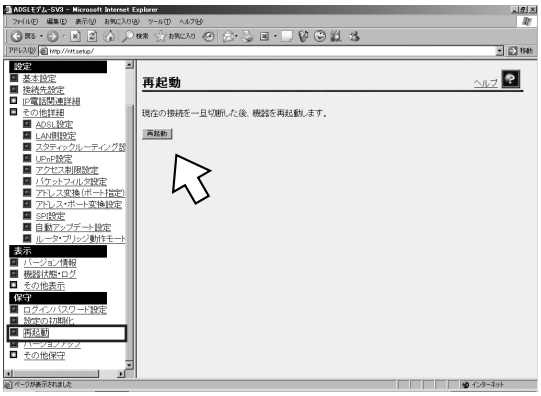
5 その他詳細のルータ・ブリッジ動作モードをクリックし、必要事項を入力する。

・動作モード
［ルータ］を選択
・PPPoE ブリッジ機能
［使用しない］を選択
入力後、［設定］ボタンをクリックします。

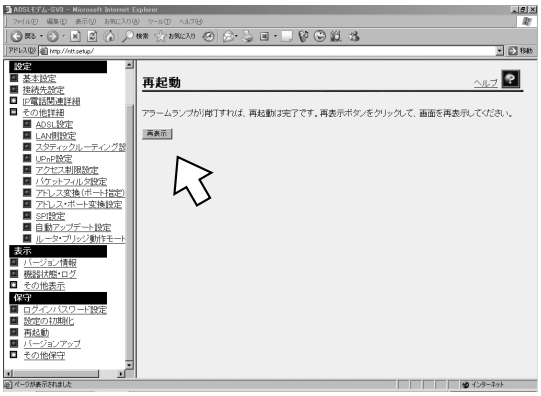


6 左側メニューの［再起動］をクリックし、［再起動］ボタンをクリックする。

SV Ⅲが再起動されます。



7 ［再表示］ボタンをクリックする。



引き続き、「④接続構成を変更する」へ進んでください。（☛P2-17）

IP 電話対応 ADSL モデムと本商品を接続して利用するには

新しく ADSL モデムと本商品を接続して IP 電話をご利用になるお客様（NTT 西日本エリア・新設）

IP 電話対応 ADSL モデムと本商品を接続して IP 電話をご利用になる場合は、次のように接続、設定してください。

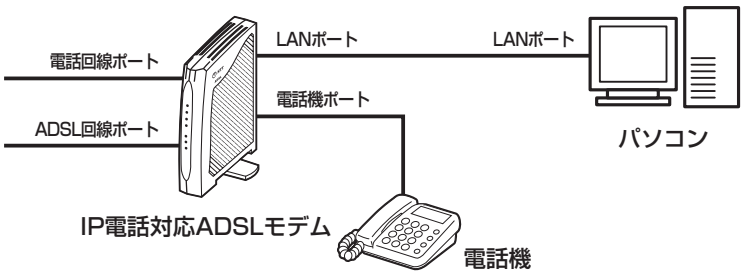
①必要なものを確認する

事前に次のものをご準備ください。

・フレッツ・ ADSL 開通時に送付される「お申込内容のご案内」（NTT 西日本）
・インターネット接続のための**プロバイダ情報**
・ADSL モデム付属の**マニュアル**

②接続する

ADSL モデム付属のマニュアルに従って、IP 電話対応 ADSL モデムとパソコン、電話機を下図のように接続します。



③ ADSL モデムの設定をする

操作手順は、NTT 西日本エリアで ADSL モデム SV Ⅲをお使いになる場合の例です。

1 Web ブラウザを起動し、アドレス欄に「http://ntt.setup/」と入力して［Enter］キーを押す。

2 ユーザー名「user」と管理者パスワードを入力し、［OK］をクリックする。

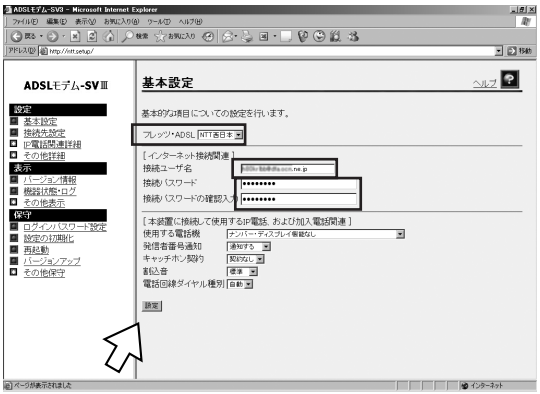
SV Ⅲの基本設定画面が表示されます。

お知らせ

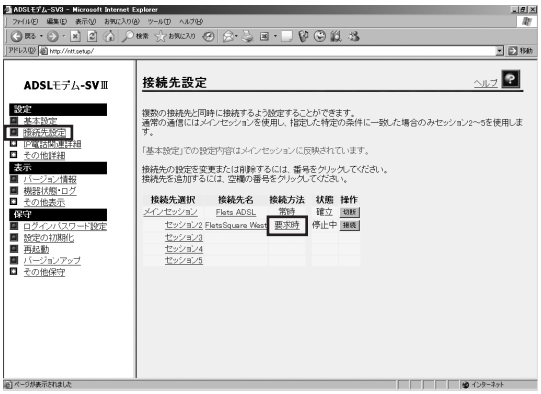
● 手順と画面の詳細は、ADSL モデム SV Ⅲの取扱説明書を参照してください。

3 基本設定で次のように設定し、［設定］をクリックする。

［フレッツ・ADSL］：
　［NTT 西日本］を選択します。
［接続ユーザ名］、［接続パスワード］：
　プロバイダ情報に従って入力します。
再起動を促す指示が表示されますが、引き続き他の設定を行いますので再起動しないでください。

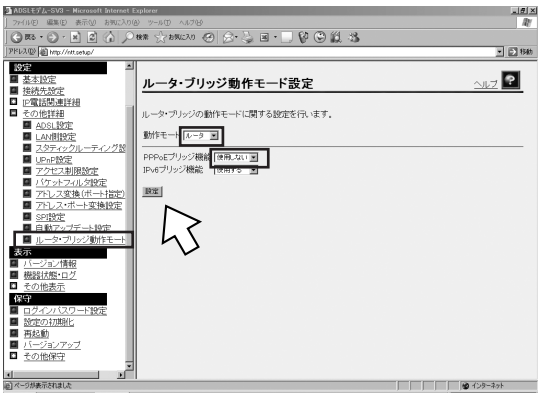


4 左側メニューの［接続先設定］をクリックして、セッション２の接続方法が［要求時］になっていることを確認する。



5 その他詳細のルータ・ブリッジ動作モードをクリックし、必要事項を入力する。

・動作モード
　［ルータ］を選択
・PPPoE ブリッジ機能
　［使用しない］を選択
入力後、［設定］ボタンをクリックします。



（次ページへ続きます）

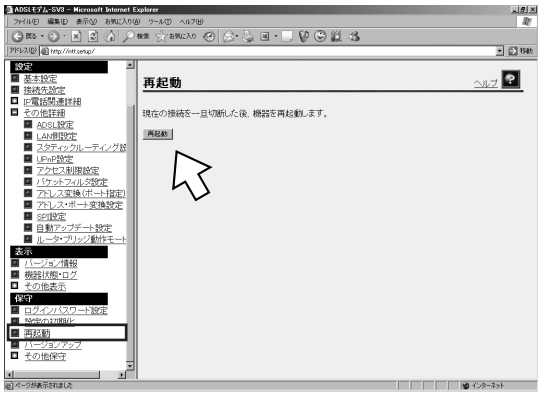
IP 電話対応 ADSL モデムと本商品を接続して利用するには

6 必要に応じて IP 電話の設定を行う。

ADSL モデム付属のマニュアルを参照してください。

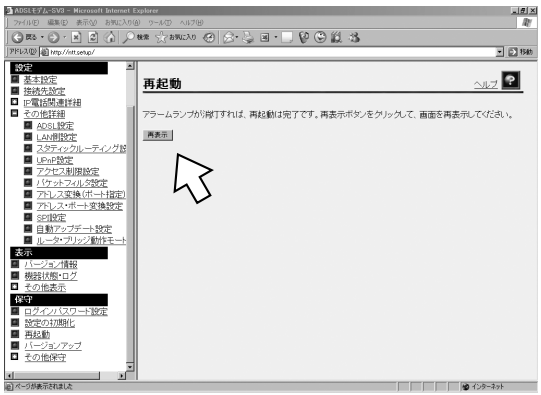
7 左側メニューの［再起動］をクリックし、［再起動］ボタンをクリックする。

SV Ⅲが再起動されます。



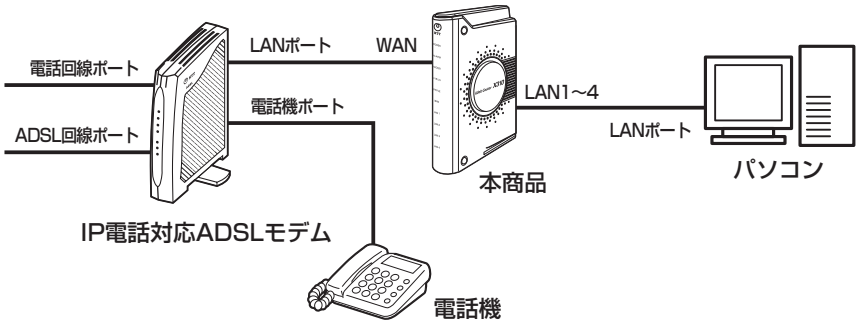
8 ［再表示］ボタンをクリックする。

これで ADSL モデムの接続、設定は完了です。



④接続構成を変更する

本商品を設定するために、下図のように接続構成を変更します。IP 電話対応 ADSL モデムとパソコンの間に本商品を接続してください。



引き続き、「⑤本商品のかんたん設定をする」へ進んでください。（☛P2-18）

⑤本商品のかんたん設定をする

1 本商品に接続したパソコンで Web ブラウザを起動する。

2 Web ブラウザのアドレス欄に「http://192.168.0.1」と入力し、[Enter] キーを押す。

または、「http://wbc_x310」と入力します。

3 ログインパスワードを設定する。

本商品の Web 設定にログインするためのパスワードを設定します。
[新しいログインパスワード] に、任意の文字を半角英数字記号 64 文字以内で入力します。半角スペースも入力できます。
入力したパスワードは、●●●または＊＊＊で 18 桁まで表示されます。
18 文字を超えて入力された場合、18 桁以上は表示されませんが、入力したパスワードは記録されていますので問題ありません。
[新しいログインパスワードの確認再入力] に、もう一度、同じパスワードを入力し、[OK] をクリックします。

※パスワードを空欄のままにすることもできますが、パスワードを設定しないとセキュリティ上のリスクを高めることになります。
※パスワードは、忘れないように必ずメモして安全な場所に保管してください。設定記入シートに記入しておくことをお勧めします。(取扱説明書 ☛P6-3)
※パスワードを忘れた場合は、本商品を初期化して設定を初めからやり直してください。(☛P1-76)

お知らせ

- Web 設定画面は、本商品の設定画面を Web ブラウザで表示する画面ですのでインターネットに接続する必要はありません。
- 入力したパスワードの表示桁数は、お使いのパソコンによって異なる場合があります。

4 ホーム画面が表示されたら、[かんたん設定] をクリックする。

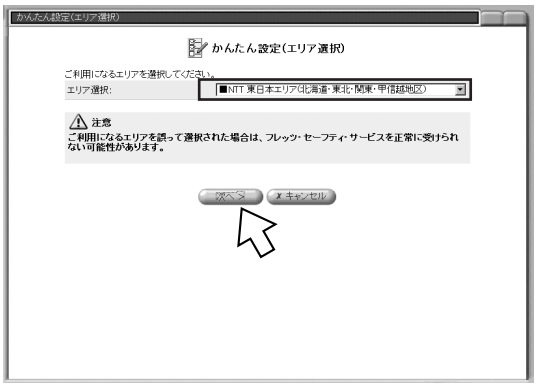
5 エリアを選択する。

お住まいの地域に合わせて次のどちらかのエリアを選択し、［次へ］をクリックします。

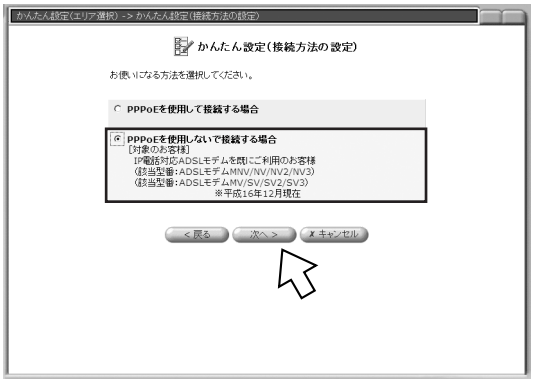
［NTT 東日本エリア
（北海道・東北・関東・甲信越地区）］：
北海道、東北、関東、甲信越地区にお住まいのお客様

［NTT 西日本エリア
（東海・北陸・近畿・中国・四国・九州地区）］：
東海、北陸、近畿、中国、四国、九州地区にお住まいのお客様

※エリアを誤って選択された場合は、フレッツ・セーフティのサービスを正常に受けられない可能性があります。



6 ［PPPoE を使用しないで接続する場合］を選択し、［次へ］をクリックする。



7 ［動的な IP アドレス設定］を選択し、［次へ］をクリックする。

●PPPoE 以外の接続で固定の IP アドレスを設定する場合（☛P2-22）

ワンポイント

● 前の画面に戻るには

［戻る］をクリックすると、1 つ前の画面に戻り、設定し直すことができます。

（次ページへ続きます）

IP 電話対応 ADSL モデムと本商品を接続して利用するには

8 フレッツ・セーフティの設定をする。

本商品のファームウェアがアップデートできるようになったときや、ハッカーの不正アクセスが検出されたときに、メールで通知されるようにします。

●E-mail 通知／本装置から通知する情報：

①［E-mail アドレス］に、お持ちの E-mail アドレスを入力します。
　半角英数字記号 100 文字まで入力できます。
　［E-mail アドレスの確認再入力］に、もう一度、同じ E-mail アドレスを入力します。

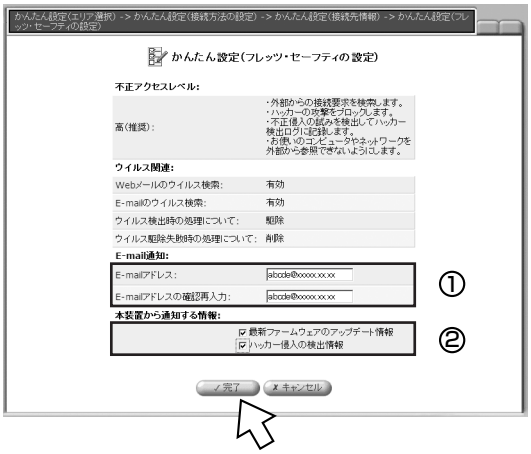
②［本装置から通知する情報］の項目をチェックし、［完了］をクリックします。
- ［最新ファームウェアのアップデート情報］
  本商品の新しいバージョンのファームウェアに関する情報をメールで受け取ります。
  （お買い求め時：チェックなし）
- ［ハッカー侵入の検出情報］
  使用しているパソコンやネットワークへの不正アクセスを検出したときに、通知をメールで受け取ります。（お買い求め時：チェックなし）

■不正アクセスレベル、ウイルス関連の機能は、かんたん設定では自動的に下記のように設定されます。

●不正アクセスレベル：高（推奨）
- 外部からの接続要求を検索します。
- ハッカーの攻撃をブロックします。
- 不正侵入の試みを検出してハッカー検出ログに記録します。
- お使いのコンピュータやネットワークを外部から参照できないようにします。

●ウイルス関連：
送受信メールと Web メールを検索し、ウイルスが検出された場合は駆除します。駆除に失敗したときは感染したファイルを削除します。
- Web メールのウイルス検索：有効
  （Web メールは、Yahoo!メール、HotMail、AOL メールのみに対応しています）
- E-mail のウイルス検索：有効
- ウイルス検出時の処理について：駆除
- ウイルス駆除失敗時の処理について：削除

■設定を変更する場合は、かんたん設定の終了後、「フレッツ・セーフティの設定を変更するには」を参照して設定を変更してください。（☛P1-24）

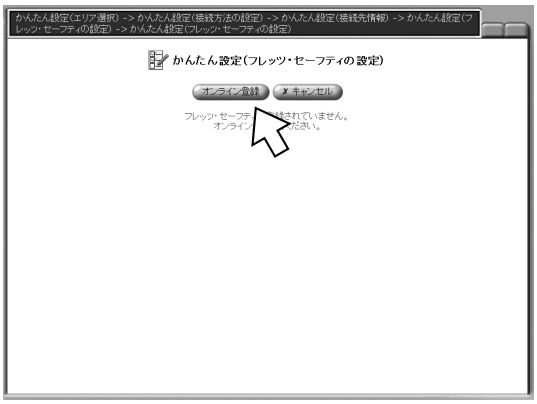


お知らせ

- E-mail アドレスを入力しないと、以下のメールが送られてきません。
  - フレッツ・セーフティにオンライン登録がお済みでないお客様あての未登録通知
  - ［本装置から通知する情報］でチェックした情報
- E-mail アドレスの@マーク以下は、半角英数字、-（ハイフン）、_（アンダースコア）、.（ドット）が使用できます。

9 右の画面を確認する。

これでかんたん設定は完了です。
本商品を最新のセキュリティ対策機能でお使いいただくためには、本商品のオンライン登録を行い、フレッツ・セーフティへのご契約が必要です。
［オンライン登録］をクリックして、登録を行ってください。
「フレッツ・セーフティにオンライン登録する」（☛P1-12）へ進んでください。



（次ページへ続きます）

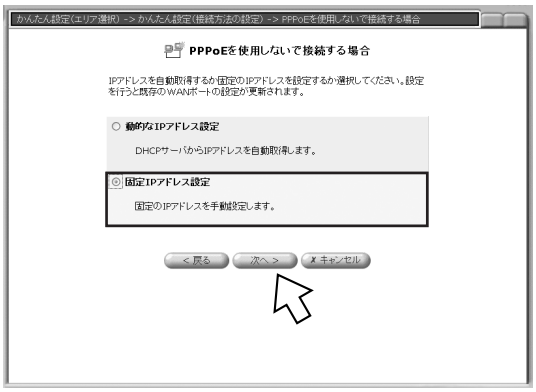
IP 電話対応 ADSL モデムと本商品を接続して利用するには

PPPoE 以外の接続で固定の IP アドレスを設定する場合

かんたん設定で次のように設定します。

1 かんたん設定（接続方法の設定）画面で、［PPPoE を使用しないで接続する場合］を選択し、［次へ］をクリックする。

2 ［固定 IP アドレス設定］を選択し、［次へ］をクリックする。



3 IP アドレス、ネットマスク、デフォルトゲートウェイ、DNS サーバなどを設定し、［次へ］をクリックする。

IP 電話対応 ADSL モデムの LAN ポートの情報を元に入力してください。
ご不明の場合は、ご契約のプロバイダにお問い合わせください。

かんたん設定（フレッツ・セーフティの設定）の画面が表示されます。
以降の操作は、P2-20 の手順８へ進んでください。

音声／ビデオチャットなどのツールを利用するには

Windows Messenger、MSN Messengerなどの音声／ビデオチャットを利用することができます。

Windows Messenger、MSN Messenger を使う

本商品とユニバーサルプラグアンドプレイ（UPnP）機能を利用すると、Windows Messenger Version5.1 以降、MSN Messenger7.0 以降を利用することができます。
本商品のUPnP機能を「有効」に設定する必要があります。

お知らせ

- UPnPを利用できるOSは、Windows® XPおよびWindows® Meです。Windows® Meの場合は、［コントロールパネル］の［アプリケーションの追加と削除］―［Windowsファイル］タブ―［通信］―［詳細］で［ユニバーサルプラグアンドプレイ］をクリックし、インストールしてください。
- 音声チャットを行うには、マイク／スピーカー、またはヘッドセットが別途必要です。
- ビデオチャットを行うには、マイク／スピーカー、またはヘッドセット、カメラ（USBカメラ）などが必要です。
- ご利用の環境によっては、Webメールのウイルス検索を有効に設定すると、正常に利用できないことがあります。
- UPnP機能を［有効］に設定すると、UPnPで利用するポート等に対して不正アクセスの防止機能が動作しませんので、ご注意ください。
- WANイーサネットでご利用の場合は、この機能は対応していません。

音声／ビデオチャットなどのツールを利用するには

1 Web 設定画面で［カスタム設定］をクリックする。（☛P1-29）

2 ［ユニバーサルプラグアンドプレイ］をクリックする。

3 ［UPnP 機能を有効にする］をチェックし、［OK］をクリックする。

UPnP 機能を有効にするには、［UPnP 機能を有効にする］をチェックします。
接続先を追加している場合は、［UPnP 機能を適用する接続先］から、UPnP 機能を設定する接続先を選択します。
UPnP 機能を適用できる接続先は 1 つのみです。

4 ［OK］をクリックする。

設定を変更した後は、本商品を再起動してください。（自動では再起動しません。）

お知らせ

- UPnP 機能を「有効」に設定すると、UPnP で利用するポート等に対して不正アクセスの防止機能が動作しませんので、ご注意ください。
- WAN イーサネットでご利用の場合は、この機能は対応していません。

外部にサーバを公開するには

ここでは、外部にサーバを公開するときに必要な設定について説明します。

LANに接続されたパソコンをサーバとして公開する

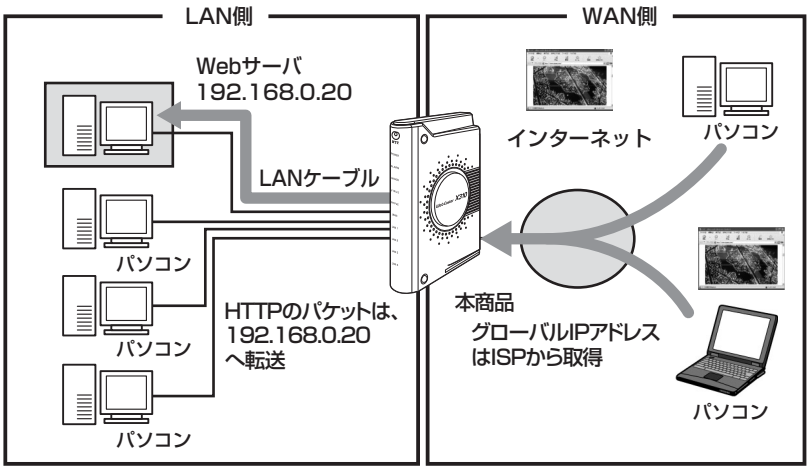
LAN側に構築したサーバをインターネットに公開するには、インターネットからLAN側のサーバへのアクセスを許可する必要があります。

お知らせ

- インターネットにサーバを公開すると、外部からの侵入や盗聴、データの消失などの被害に遭う可能性があります。十分なセキュリティ設定を行ってください。
- 外部にサーバを公開するには、本商品にグローバルIPアドレスが割り当てられている必要があります。プライベートIPアドレスを利用する一部のプロバイダをご利用の場合は、サーバを公開できないことがあります。

ローカルサーバを使ったサーバの公開

ここでは、LAN上のパソコン（192.168.0.20）をWebサーバとして外部に公開する場合の設定について説明します。



外部にサーバを公開するには

1 Web 設定画面で［カスタム設定］をクリックする。（☛P1-29）

2 ［セキュリティ］をクリックする。

3 ローカルサーバ画面の［新規作成］をクリックする。

4 ［ローカルホスト］に使用するパソコンの IP アドレスを入力し、［転送ポート］にポート番号を入力する。

ここでは、［ローカルホスト］に「192.168.0.20」と入力します。
ポート番号は、Web サーバとして外部に公開する場合は、「80」と入力します。
接続先は、ローカルサーバを外部に公開する接続先（すべて、WAN PPPoE2 ～ 5）を選択します。
サービス名のアプリケーションサポートは、ローカルサーバを設定するアプリケーション（FTP、Ping、Traceroute、Windows 共有フィルタを選択することができます。

5 ［新規ユーザ定義サービス］をクリックする。

6 ［サービス名］と［サービスの説明］を入力する。

7 ［新規作成］をクリックする。

8 ［プロトコル］から対象とするプロトコルを選択する。

Web サーバとして外部に公開する場合は、［TCP］を選択します。

（次ページへ続きます）

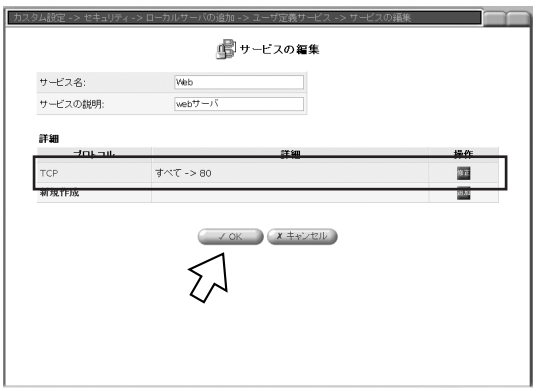
外部にサーバを公開するには

9 送信元ポートと送信先ポートを設定する。

Web サーバとして外部に公開する場合は、次のように設定します。
［送信元ポート］：
　［すべて］を選択します。
［送信先ポート］：
　［1 個を指定］を選択し、「80」と入力します。

10 ［OK］をクリックする。

11 サービスの編集画面に追加されたことを確認し、［OK］をクリックする。



12 追加したサービスをチェックし、［OK］をクリックする。

13 [表示の更新] をクリックする。

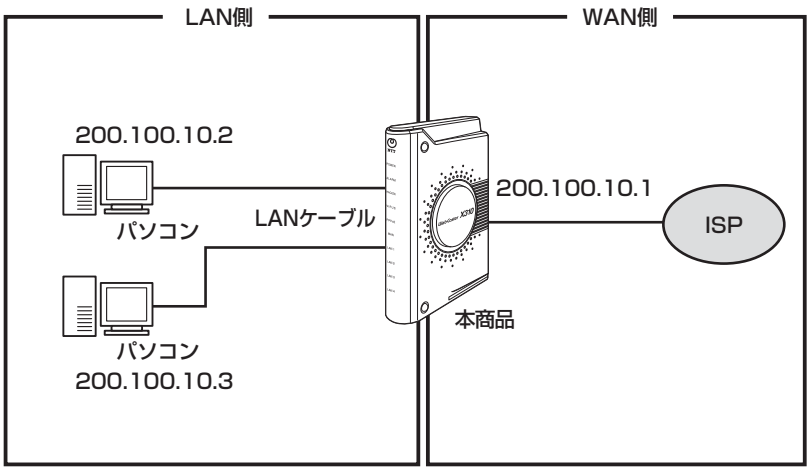
14 追加したサービスが［サービス］欄に表示され、［ステータス］欄に「接続」と表示されていることを確認する。

複数の固定IPアドレスサービスを利用するには

各プロバイダが提供する複数固定IPアドレスサービスを利用することにより、プロバイダから割り当てられた複数のグローバル固定IPアドレスを本商品および本商品に接続されたパソコンにそれぞれ設定して、サーバ公開などが可能になります。

PPPoE接続でUnnumbered接続を使用する

ここでは、プロバイダから割り当てられたIPアドレス（200.100.10.0/29）の場合、本商品に設定するIPアドレス（200.100.10.1）のネットワーク構成例について説明します。



1 Web設定画面で［カスタム設定］をクリックする。（☛P1-29）

2 ［ネットワーク接続］をクリックする。

お知らせ

- WAN PPPoE詳細設定の「IP設定」（☛P2-32）で「Unnumbered接続を使う」を選択した場合は、「DHCPサーバ設定」（☛P1-31）が「無効」に設定されます。
- Unnumbered接続を利用するには、パソコン側に固定IPアドレスを設定してください。
- パソコン側に固定IPアドレスを設定した場合、フレッツ・セーフティのオンライン登録ページが正常に表示されないことがありますので、パソコン側のDNS設定の中のサフィックス設定に「home」を設定してください。
- フレッツ・セーフティにご契約いただいているお客様は、Unnumbered接続時でも、セキュリティ対策ファイル（パターンファイル、検索エンジン、ファイアウォールルール）のダウンロードを行うことができます。

3 対象とする接続先の［WAN PPPoE］をクリックする。

4 ［詳細設定］をクリックする。

（次ページへ続きます）

複数の固定 IP アドレスサービスを利用するには

5 接続情報を設定する。

●**基本設定：**

［ステータス］：
接続状態が表示されます。

［MTU］：
［自動］を選択します。

●**PPP：**

［サービス名］：
プロバイダから指定された場合のみサービス名を入力します。

［無通信監視タイマ（分）］：
0 ／ 5 ／ 10 ／ 30 から選択します。
「0」を選択した場合、回線は切断されません。
お買い求め時は「0」に設定されています。

●**PPP 認証：**

［接続ユーザ名（大文字・小文字区別）］：
PPP 接続を行うユーザ名を入力します。

［接続パスワード］：
PPP 接続を行うパスワードを入力します。

［PAP 認証を許可する（PAP）］：
PAP 認証を使用しないときはチェックを外します。

［CHAP 認証を許可する（CHAP）］：
CHAP 認証を使用しないときはチェックを外します。

●**IP 設定**：

・「Unnumbered 接続を使う」を選択します。

［IP アドレス］：
「200.100.10.1」と入力します。
（プロバイダから割り当てられた 2 番目の IP アドレスを入力します）

［ネットマスク］：
「255.255.255.248」と入力します。

●**DNS サーバ**：次のいずれかを選択します。

・ DNS サーバアドレスを自動取得する
・ DNS サーバアドレスを固定設定する

［デバイスメトリック］：
デバイスメトリックは、PPPoE2 ～ 5 の接続順位を設定します。
値が小さい方が優先順位が高くなります。同じ値は設定しないでください。

6 ［OK］をクリックする。

ワンポイント

●**本商品の Web 設定画面を開くには**

Web ブラウザのアドレス欄に手順 5 で設定した IP アドレスを入力し（この例では「http://200.100.10.1」）、［Enter］キーを押します。

お知らせ

● 接続ユーザ名と接続パスワードは、大文字小文字の区別を確認のうえ、入力してください。

7 [注意] 画面が表示されたら [OK] をクリックする。

IP アドレスが変更されるため、Web 設定画面は表示されません。

8 パソコン側に固定 IP アドレスを設定する。

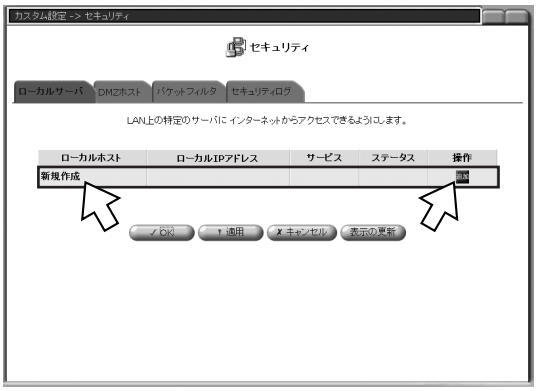
・WAN PPPoE 詳細設定の「IP 設定」(☛P2-32) で「Unnumbered 接続を使う」を選択すると、「DHCP サーバ設定」(☛P1-31) が「無効」に設定されますので、パソコン側に固定 IP アドレスを設定します。

9 Web ブラウザを起動し、今回設定した IP アドレスを入力して Web 設定画面を開く。

10 [カスタム設定] をクリックする。

■続いてローカルサーバの設定を行います。

11 セキュリティのローカルサーバ画面で、[新規作成] または [追加] をクリックする。(☛P1-53)



(次ページへ続きます)

12 [ローカルサーバの追加画面] の各項目を設定する。

[接続先] :
Unnumbered 接続を設定した回線を選択します。
[ローカルホスト] :
ローカルサーバを設定するパソコンのIPアドレスを入力します。
[転送ポート] :
ポート番号を入力します。
[アプリケーションサポート] :
ローカルサーバを設定するアプリケーション（FTP、Ping、Traceroute、Windows 共有フィルタ）を選択することができます。

13 [新規ユーザ定義サービス] をクリックする。

14 [サービス名]、[サービスの説明] を入力し、[新規作成] をクリックする。

サービスの説明は入力しなくてもかまいません。

15 プロトコルを設定する。

［プロトコル］：
対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。TCP、UDPを選択したときは、送信元ポートと送信先ポートを選択し、入力してください。ICMPを選択したときは、ICMPメッセージを選択してください。

［送信元ポート］／［送信先ポート］：
次のいずれかを選択し、サービスやアプリケーションのポート番号を入力します。

・すべて　　：すべてのポートを指定する
・1個を指定：1つのポート番号を指定する
・範囲指定　：ポート番号の範囲を指定する

16 [OK] をクリックする。

サービスの編集画面に戻ります。

17 [OK] をクリックする。

18 ユーザ定義サービスのサービス名をチェックし、[OK] をクリックする。

サービスを無効にする場合は、サービス名のチェックを外します。
ローカルホストにはパソコンのIPアドレスが入力されていることを確認してください。

複数の接続先を使い分けるには（マルチセッション）

本商品は、接続先を５つまで登録することができます。通常は、かんたん設定でご契約のプロバイダを登録することにより、フレッツ・スクウェアとプロバイダの２か所に接続することができます。
PPPoEの接続先を追加するには、最大接続数を変更し、接続先を登録します。

1 Webブラウザを起動して、Web設定画面を開く。（☛P1-2）

2 ［カスタム設定］をクリックする。

3 ［ネットワーク接続］をクリックする。

4 ［PPPoEセッション最大接続数］を変更する。

２～５の範囲で設定できます。お買い求め時は２に設定されています。
最大接続数を変更すると、接続名の数が増減します。

5 追加した接続名の［修正］をクリックする。

6 ［詳細設定］をクリックする。

お知らせ

- PPPoE セッション最大接続数を変更してもご利用環境によっては正常に動作しません。NTT 東日本エリアでは最大２セッション（B フレッツ・ビジネスタイプを除く）です。NTT 西日本エリアでは通常２セッション（B フレッツ・ビジネスタイプを除く）ですが、フレッツ・プラス（別途お申し込みが必要）により５セッションまで追加可能です。
- PPPoE セッションを３つ以上設定する場合は、以下のホームページでお客様の契約回線の最大の PPPoE セッション数をご確認のうえ設定してください。
  お客様の契約数以上の設定を行った場合は正常に動作せず、フレッツ・セーフティの機能をご利用できなくなります。
  NTT 東日本エリアをご利用のお客様
  http://flets.com/customer/tec/safety/helpdesk/safety_news_002.html
  NTT 西日本エリアをご利用のお客様
  http://flets-w.com/plus/
- お客様が本商品を利用する環境によっては、ルーティングテーブルの設定など、他の機能の設定が必要になる場合があります。

（次ページへ続きます）

複数の接続先を使い分けるには（マルチセッション）

7 接続先を設定し、［OK］をクリックする。

●**基本設定：**

［ステータス］：
現在の WAN PPPoE の状態が表示されます。

［MTU］：
自動／手動を選択します。

●**PPP：**

［サービス名］：
プロバイダによってサービス名を指定された場合に入力します。

［無通信監視タイマ（分）］：
0／5／10／30 から選択します。
「0」を選択した場合、回線は切断されません。
お買い求め時は「0」に設定されています。

●**PPP 認証：**

［接続ユーザ名（大文字・小文字区別）］：
プロバイダから指定されたユーザ名を入力します。

［接続パスワード］：
プロバイダから指定されたパスワードを入力します。

［PAP 認証を許可する（PAP）］：
PAP 認証を使用しないときはチェックを外します。

［CHAP 認証を許可する（CHAP）］：
CHAP 認証を使用しないときはチェックを外します。

●**IP 設定**：次のいずれかを選択します。

・［Unnumbered 接続を使う］：
Unnumbered 接続で使用する IP アドレスを設定します。
ネットマスクを置き換えるときは［ネットマスクを置き換える］をチェックして、ネットマスクを入力します。

・［IP アドレスを自動取得する］：
ネットマスクを置き換えるときは［ネットマスクを置き換える］をチェックして、ネットマスクを入力します。

・［IP アドレスを固定設定する］：
IP アドレスを設定します。ネットマスクを置き換えるときは［ネットマスクを置き換える］をチェックして、ネットマスクを入力します。

●**DNS サーバ**：次のいずれかを選択します。

・DNS サーバアドレスを自動取得する
・DNS サーバアドレスを固定設定する

［NAPT］：
NAPT 機能の有効／無効を選択します。

［デバイスメトリック］：
デバイスメトリックは、PPPoE2 ～ 5 の接続順位を設定します。
値が小さい方が優先順位が高くなります。同じ値は設定しないでください。

お知らせ

●接続ユーザ名と接続パスワードは、大文字小文字の区別を確認のうえ、入力してください。

ネットワークゲームをするには

ネットワーク上から各パソコンに直接アクセスするネットワークゲームを利用することができます。

UPnP に対応しているネットワークゲームの場合

本商品はユニバーサルプラグアンドプレイ（UPnP）に対応していますので、UPnP 対応のアプリケーションを利用することができます。
本商品の UPnP 機能を「有効」に設定する必要があります。

お知らせ

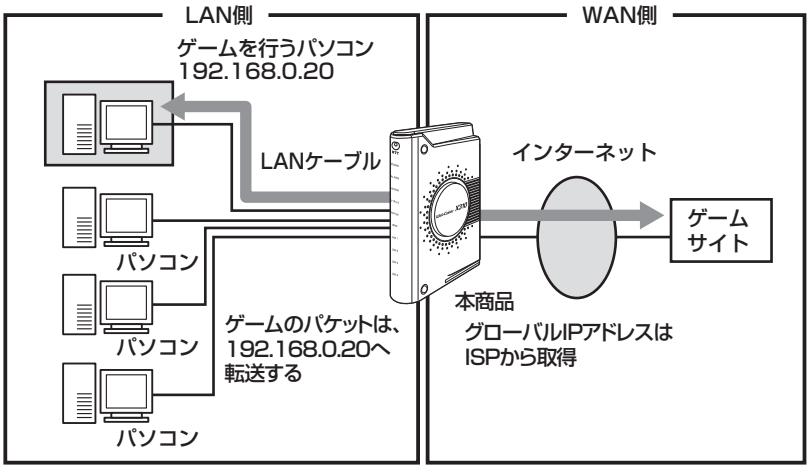
- UPnP を利用できる OS は、Windows® XP および Windows® Me です。Windows® Me の場合は、［コントロールパネル］の［アプリケーションの追加と削除］―［Windows ファイル］タブ―［通信］―［詳細］で［ユニバーサルプラグアンドプレイ］をクリックし、インストールしてください。

UPnP に対応していないネットワークゲームの場合

ネットワークゲームを行うパソコンに、インターネットからのアクセスを許可する必要があります。
本商品はローカルサーバ機能に対応していますので、ローカルサーバ機能に使用するゲームのポート情報やパソコンの IP アドレスを設定するだけでご利用できます。

ローカルサーバを使ったネットワークゲームの設定

ここでは、LAN 上のパソコン（192.168.0.20）からネットワークゲームのサイトにアクセスする場合の設定について説明します。



お知らせ

- ネットワークゲームを行う場合は、本商品にグローバル IP アドレスが割り当てられている必要があります。プライベート IP アドレスを利用する一部のプロバイダをご利用の場合は、ネットワークゲームを行えない場合があります。グローバル IP アドレスが割り当てられているかのご確認は、ご利用のプロバイダへお問い合わせください。

ネットワークゲームをするには

1 Web 設定画面で［カスタム設定］をクリックする。（☛P1-29）

2 ［セキュリティ］をクリックする。

3 ローカルサーバ画面の［新規作成］をクリックする。

4 ［ローカルホスト］に使用するパソコンの IP アドレスを入力し、［転送ポート］にポート番号を入力する。

ネットワークゲームが使用するポート番号については、ネットワークゲームのサービスセンターなどにお問い合わせください。

5 [新規ユーザ定義サービス] をクリックする。

6 [サービス名] と [サービスの説明] を入力する。

サービスの説明は入力しなくてもかまいません。

7 [新規作成] をクリックする。

8 [プロトコル] から対象とするプロトコルを選択し、[OK] をクリックする。

TCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。
ネットワークゲームが使用するプロトコルについては、ネットワークゲームのサービスセンターなどにお問い合わせください。

（次ページへ続きます）

ネットワークゲームをするには

9 [OK] をクリックする。

10 追加したサービスをチェックし、[OK] をクリックする。

お知らせ

- サービスを新規作成する場合は、ネットワークゲームなどで使用するポート情報が必要です。詳しくは、ネットワークゲームのサポートセンターなどにお問い合わせください。
- 登録したいネットワークゲームのポート情報などが公開されていないときは、DMZ ホスト機能を設定してください。

3 付録

用語解説

ADSL モデム

コンピュータを ADSL 回線に接続する際に必要になる信号変換機を表します。
具体的には、加入電話回線を通じて送られてくる ADSL 信号を Ethernet（10BASE-T/100BASE-TX）の信号に変換したり、その逆を行い、ADSL モデムとコンピュータの間は Ethernet で繋ぎます。

DHCP

LAN 上のコンピュータに動的に IP アドレスを割り当てる方法です。DHCP サーバに割り当てる IP アドレスの範囲、ネットマスクなどが設定されていて、コンピュータがネットワークに接続されると、DHCP サーバから自動的に IP アドレスが割り当てられます。

DMZ ホスト

1 つのローカルコンピュータをインターネットに見えるようにする機能です。

DNS

TCP/IP ネットワークで用いる名前を解決する仕組みです。DNS サーバを利用して行われます。

DNS サーバ

ドメイン名と IP アドレスとの対応表を持っており、ドメイン名の問い合わせに対して IP アドレスを通知するサーバです。

HTTP

WWW サーバとブラウザの間で HTML（hypertext markup language）ファイルなどを転送する時に利用するプロトコル。TCP 上で動作します。

IP

異なるネットワークの間でパケットの転送を行うための取り決めを表します。IP アドレスにより相手先を判断します。

IP アドレス

ネットワーク上で機器を特定するためのアドレスです。例えば、192.168.1.1 のようにピリオドを挟んだ 4 つの数字（0 ～ 255）で表します。

LAN

会社内や家庭内などの狭い空間でコンピュータや周辺機器を接続したネットワークシステムです。ファイルやプリンタなどを共有することが可能となります。

MTU

ネットワークにおいて、1 回で送信できる 1 パケットのデータの最大値を示します。RFC791 で定義されています。MTU の単位はバイト。PPPoE では通常 1454 といわれていますが、Web サイトにより 1454 ではアクセスできず、4 の倍数で 1454 より小さい値を推奨しているものがあります。

NAPT

LANで利用されるプライベートIPアドレスをグローバルIPアドレスに変換する仕組みです。これにより、複数の機器が1つのグローバルアドレスを利用して接続ができるようになります。

NTP

ネットワークを介して時刻を調整するプロトコルです。
具体的には、クライアントの内部時計を、インターネット上に存在するNTPサーバを介して時刻を調整します。

PING

TCP/IPネットワークにおいてパケットの送受信テストを行うコマンドです。接続されているかどうかの確認に利用します。

PPP

2地点間での通信に利用するWAN用のプロトコルです。主にダイヤルアップ接続などに利用されます。

PPPoE

イーサネット上にPPPコネクションを構築し、PPPによる認証を経て通信が可能になる方式です。一般的に、接続の際にPPPoEユーザ名とパスワードが必要になります。
Bフレッツやフレッツ・ADSLはこの方式を採用しています。この方式は、プロバイダ側のPPPoEサーバとの1対1接続になるため、ネットマスクやデフォルトゲートウェイという概念はありません。一方、IPアドレスやDNSサーバアドレス（プライマリ/セカンダリ）に関しては、PPP（IPCP）ネゴシエーション中にプロバイダのサーバから自動取得する場合がほとんどですが、自動取得せずに常に同じIPアドレス、DNSサーバアドレスを利用するサービスもあります。

TCP

データの転送を制御するプロトコルです。送信先に接続してデータ送信をします。
受信側は受け取ったパケットの到達確認を行い、エラーを訂正する機能を持つので、信頼性の高い通信を実現できます。

TCP/IP

インターネットでの標準プロトコルです。TCP/UDPとIPというそれぞれのプロトコルを用いて通信を行います。

Unnumbered接続

他のネットワークに接続するルータのWAN側ポートにIPアドレスを割り当てず、2台のルータを見かけ上1台のルータのように扱う接続方式です。Unnumberedで運用されているルータはLAN側にのみIPアドレスを持ちます。
Unnumbered接続を行う場合、2台のルータが繋がっているネットワークに他のコンピュータがいるとパケットの行き先が確定しなくなるため、ルータどうしが直結している必要があります。

UPnP（ユニバーサルプラグアンドプレイ）

特別な設定なしに機器をLANに接続して通信することができます。アプリケーションがアドレス変換を考慮して送受信パケットを作成するため、NAPT機能などを実装していても通信が可能です。

URL

インターネット上の情報資源（文書や画像など）の場所を指し示す記述方式です。

用語解説

WAN
広域のネットワークを意味します。LAN と対比して利用されることがあり、伝送距離に制限がないことが特徴です。

Web ブラウザ
Web ページ（WWW システムを使ってインターネット上で公開されている文書）を閲覧するためのソフトウェアです。代表的なものとして Internet Explorer があります。

アカウント
ネットワークに接続（ログイン）する際の権利を意味します。具体的にはユーザ ID を指し、プロバイダと契約した際のユーザ ID のことです。

イーサネット
現在、最も普及している LAN です。10BASE-T や 100BASE-TX などの規格があります。

オンライン登録
フレッツ・セーフティ対応のサービスをご利用になる際に、ユーザ登録を Web ブラウザで実施する登録サービスです。

回線終端装置
ディジタル回線に端末装置を接続するための終端装置です。B フレッツでは ONU（Optical Network Unit）などを指します。

ゲートウェイ
プロトコルの異なる LAN と LAN や、LAN と WAN とを接続する装置です。

ネットマスク
ネットワークで接続された複数のコンピュータが同じネットワーク部であるかを判断するための値です。例えば、255.255.255.0 のようにピリオドを挟んだ 4 つの数字（0 ～ 255）で表します。

ネットワークアドレス
IP アドレスの中のネットワークを識別する部分です。例えばサブネットマスクが 255.255.255.0 の場合は、IP アドレスの 3 つ目のピリオドまでの数字がネットワークアドレスになります。

ハッカー
元来はコンピュータ分野において優れた技術を発揮する人のことを指していましたが、他人のコンピュータに不正なやり方で侵入し、破壊活動などを行う人をも指すようになった名称です。

パケット
一定のサイズに分割されたデータの先頭に、データの属性や宛先などを付けたものです。

パケットフィルタ
ネットワークを流れるデータ（IP パケット）を選別し、そのデータを通過させるか（許可）、させないか（拒否）を指定することで、外部から流れてくる不要なデータを遮断したり、逆に内部からのデータ漏洩を防ぐ技術です。

パスワード
コンピュータ・システムの安全性や信頼性を維持するために利用される、数字や文字列による符号です。パスワードを設定する際は、名詞や単純な数字、文字は避け、文字、数字、記号を組み合わせて設定することや、定期的にパスワードを変更することが望まれます。

フレッツ・スクウェア
フレッツ・スクウェアは、NTT 東日本／NTT 西日本のフレッツ網に開設しているフレッツ・シリーズご利用者専用サイトです。お客様宅までの回線速度測定など、さまざまなコンテンツが用意されています。

フレッツ・セーフティ
フレッツ・セーフティは B フレッツまたはフレッツ・ ADSL ご利用のお客様に対し、NTT 東日本／NTT 西日本のフレッツ網上に設置したフレッツ・セーフティ専用装置よりお客様宅に設置されたフレッツ・セーフティ対応機器のメールのウイルス検出・駆除機能、不正アクセス防止機能の維持・管理をオンラインで行うサービスです。
本商品の設定画面からオンライン登録を実施していただくことでご利用いただけます。
フレッツ・セーフティのご利用には、申込時の初期費用と月額料金が別途必要となります。

プロトコル
データ通信を行うために必要な取り決めを意味します。TCP や UDP、IP などがあります。

プロバイダ
インターネットの接続サービスを提供している事業者を表します。

ポート番号
TCP/IP において、ユーザやアプリケーションなどを識別するために利用する番号です。

ホスト名
ネットワークを利用している機器に付加される名前です。DNS サーバにより、IP アドレスと対応付けられています。

マルチセッション
インターネットとフレッツ・スクウェアのように、同時に複数の接続先に接続することができる機能です。

ルータ
LAN と LAN、LAN と WAN を接続するための中継装置です。

ルーティング
パケットを宛先に届けるための経路を選択する機能です。

ルーティングテーブル
ルーティングの際に参照するデータです。このデータにもとづいてルーティングを実行します。

索引

アルファベット

五十音

ア行

カ行

サ行

タ行

ナ行

ハ行

マ行

ヤ行

ラ行

注　意
本商品は、外国為替および外国貿易法が定める規制貨物に該当いたします。
本商品は、国内でのご利用を前提としたものでありますので、日本国外へ持ち出す場合は、同法に基づく輸出許可等必要な手続きをお取りください。

NOTICE
This product, which is intended for use in Japan, is a controlled product regulated under the Japanese Foreign Exchange and Foreign Trade Law. When you plan to export or take this product out of Japan, please obtain a permission, as required by the Law and related regulations, from the Japanese Government.

当社ホームページでは、各種商品の最新の情報やバージョンアップサービスなどを提供しています。本商品を最適にご利用いただくために、定期的にご覧いただくことをお勧めします。

当社ホームページ（NTT東日本）　：http://www.ntt-east.co.jp/ced/
（NTT西日本）　：http://www.ntt-west.co.jp/kiki/
フレッツ・セーフティに関するホームページ
（NTT東日本）　：http://flets.com/safety/
（NTT西日本）　：http://flets-w.com/safety/

使い方でご不明の点がございましたら、下記へお気軽にご相談ください。
■NTT東日本エリア（北海道、東北、関東、甲信越地区）でご利用のお客様

●本端末機器の取り扱い、および設定方法に関するお問い合わせ
0120−970413
（03−5667−7100※）
※携帯電話・PHS・050IP電話用　通話料金がかかります。
受付時間は9：00〜21：00
年末年始（12月29日〜1月3日）は休業とさせていただきます。

●故障に関するお問い合わせ
0120−242751（24時間　年中無休 ※）
故障修理等の対応時間は平日9：00〜17：00
※土・日・祝日および年始（1月1日〜1月3日）は休業とさせていただきます。

●フレッツ・セーフティおよびセキュリティに関するお問い合わせ
03−5442−7533
受付時間は平日9：00〜17：00
土・日・祝日および年末年始（12月29日〜1月3日）は休業とさせていただきます。

■NTT西日本エリア（東海、北陸、近畿、中国、四国、九州地区）でご利用のお客様

●本端末機器の取り扱い、および設定方法に関するお問い合わせ
0120−109217（トークニィーナ）
受付時間は9：00〜17：00
年末年始（12月29日〜1月3日）は休業とさせていただきます。

●故障に関するお問い合わせ
0120−248995（24時間　年中無休）

●セキュリティに関するお問い合わせ
0120−248303
受付時間は9：00〜17：00
年末年始（12月29日〜1月3日）は休業とさせていただきます。

電話番号をお間違えにならないように、ご注意願います。

NTT

本2667-3 (2005.10)
SEC-WBC4＜X310＞トリセツ