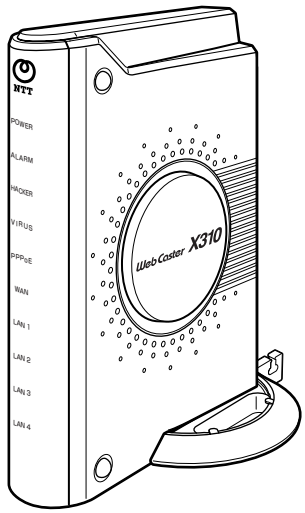
NTT

Web Caster X310
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「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

安全にお使いいただくために必ずお読みください

この取扱説明書には、あなたや他の人々への危害や財産への損害を未然に防ぎ、本商品を安全にお使いいただくために、守っていただきたい事項を示しています。
その表示と図記号の意味は次のようになっています。内容をよく理解してから本文をお読みください。
本書を紛失または損傷したときは、当社のサービス取扱所またはお買い求めになった販売店でお求めください。

本書中のマークの説明

⚠警告	この表示を無視して、誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠注意	この表示を無視して、誤った取り扱いをすると、人が傷害を負う可能性が想定される内容および物的損害のみの発生が想定される内容を示しています。
STOP お願い	この表示を無視して、誤った取り扱いをすると、本商品の本来の性能を発揮できなかったり、機能停止を招く内容を示しています。
お知らせ	この表示は、本商品を取り扱ううえでの注意事項を示しています。
ワンポイント	この表示は、本商品を取り扱ううえで知っておくと便利な内容を示しています。

厳守事項

■パスワードの取り扱いについて

本商品の Web 設定画面で入力していただくログインパスワードはお客様の大切な個人情報です。入力は必ずお客様自身で行ってください。

■取扱説明書の内容について

機能追加などにより本書の内容は予告なく変更されることがあります。機能追加や変更などに関するサポート情報につきましては、以下のホームページの更新情報を定期的に閲覧していただくことをお薦めします。

・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/

ご使用にあたってのお願い

本商品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスＢ情報技術装置です。
本商品は家庭環境で使用することを目的としていますが、本商品がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをしてください。

- ご使用の際は取扱説明書に従って正しい取り扱いをしてください。
- 本商品の仕様は国内向けとなっておりますので、海外ではご利用できません。
  This equipment system is designed for use in Japan only and cannot be used in any other country.
- 本商品の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信などの機会を逸したために生じた損害、または本商品に登録された情報内容の消失などにより生じた損害などの純粋経済損失につきましては、当社は一切その責任を負いかねますので、あらかじめご了承ください。本商品に登録された情報内容は、別にメモをとるなどして保管くださるようお願いします。
- 本商品を設置するための配線工事および修理には、工事担任者資格を必要とします。無資格者の工事、修理は、違法となりまた事故のもととなりますので絶対におやめください。
- 本商品を分解したり改造したりすることは、絶対に行わないでください。
- 本書に他社商品の記載がある場合、これは参考を目的としたものであり、記載商品の使用を強制するものではありません。
- 本書の内容につきましては万全を期しておりますが、お気づきの点がございましたら、当社のサービス取扱所へお申しつけください。
- 本書および本商品のハードウェア、ソフトウェア、外観などの仕様は、お客様にお知らせすることなく変更される場合があります。
- 本商品および本商品に搭載されているソフトウェアについて改変、複製、販売、譲渡を禁止します。

本商品を廃棄、譲渡、返却される場合の留意事項

本商品は、お客様固有の情報を保存または保持可能な商品です。本商品内に保存または保持された情報の流出による不測の損害などを回避するために、本商品を廃棄、譲渡、返却される際には、本商品内に保存または保持された情報を取扱説明書の消去方法（☛P5-2「お買い求め時の設定に戻すには」）に従って消去願います。

記載しているWebブラウザなどの画面はイメージを説明したものです。実際の画面と相違している場合がありますので詳細は実機にてご確認ください。
また、機能向上のためWebブラウザなどの画面は予告なく変更される場合があります。
Windows® 98は、Microsoft® Windows® 98 operating systemの略です。
Windows® 98SEは、Microsoft® Windows® 98 Second Edition operating systemの略です。
Windows® Meは、Microsoft® Windows® Millennium Edition operating systemの略です。
Windows® 2000は、Microsoft® Windows® 2000 operating systemの略です。
Windows® XPは、Microsoft® Windows® XP Home Edition operating systemおよびMicrosoft® Windows® XP Professional operating systemの略です。
Windowsは米国Microsoft Corporationの米国およびその他の国における登録商標です。
Netscape Navigatorは、米国およびその他の諸国のNetscape Communications Corporation社の登録商標です。
Adobe および Acrobat はアドビシステムズ社の商標です。
Internet Explorer は、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
Mac OSは米国Apple Computer Inc.の登録商標または商標です。
画面の使用に際して米国Microsoft Corporationの許諾を得ています。
その他、各会社名、各製品名は各社の商標または登録商標です。
付属品のCD-ROMは日本語OS以外の動作保証はしていません。
付属品のCD-ROMはソフトウェアのバックアップとして保有する場合に限り、複製することができます。
また、ソフトウェアのいかなる改変も禁止とし、それに起因する障害については当社は一切の責任を負いません。

■本商品の設置場所について

⚠警告

● 本商品のそばに、水や液体の入った花びん、植木鉢、コップ、化粧品、薬用品などの容器、または小さな金属類を置かないでください。本商品に水や液体がこぼれたり、小さな金属類が中に入った場合、火災・感電の原因となることがあります。

● 本商品を次のような環境に置かないでください。火災・感電・故障の原因となることがあります。
- 直射日光が当たる場所、暖房設備やボイラーなどの近くや屋外などの温度の上がる場所。
- 調理台のそばなど、油飛びや湯気の当たるような場所。
- 湿気の多い場所や水・油・薬品などのかかる恐れがある場所。
- ごみやほこりの多い場所、鉄粉、有毒ガスなどが発生する場所。
- 製氷倉庫など、特に温度が下がる場所。

⚠注意

● 本商品は次のような場所に置かないでください。また、指定された設置方法以外では設置しないでください。落ちたり倒れたりしてけがの原因となることがあります。
- ぐらついた台の上や傾いた所など、不安定な場所。
- 振動、衝撃の多い場所。

● 本商品を横置きや重ね置きにしないでください。また、本商品の通風孔をふさがないでください。通風孔をふさぐと、内部に熱がこもり、火災・故障の原因となることがあります。次のような設置のしかたはしないでください。
- じゅうたんや布団の上に置く。
- テーブルクロスなどをかける。
- 本棚、タンスの中、押入れの中など風通しの悪い狭い場所に置く。
- 紙、本などをのせたり、立てかけたりする。

STOP お願い

● 本商品を電気製品・AV・OA機器などの磁気を帯びているところや電磁波が発生しているところに置かないでください（電子レンジ、スピーカ、テレビ、ラジオ、蛍光灯、電気こたつ、インバータエアコン、電磁調理器など）。
- 磁気や電気雑音の影響を受けると、通信ができなくなることがあります（特に電子レンジ使用時には影響を受けることがあります）。
- テレビ、ラジオなどに近いと受信障害の原因となったり、テレビ画面が乱れることがあります。

● 硫化水素が発生する場所（温泉地）や、塩分の多いところ（海岸）などでは、本商品の寿命が短くなることがあります。

■本商品のお取り扱いについて

⚠警告

- 電源は、AC100 Vの商用電源以外では、絶対に使用しないでください。火災・感電の原因となることがあります。
- 差込口が２つ以上ある壁のコンセントに他の電気製品の電源アダプタ等を差し込む場合は、合計の電流値がコンセントの最大値を超えないように注意してください。火災・感電の原因となります。
- 電源アダプタは、必ず付属のものを使用し、それ以外のものは絶対にお使いにならないでください。火災・感電の原因となることがあります。
- テーブルタップや分岐コンセント、分岐ソケットを使用した、タコ足配線はしないでください。火災・感電の原因となることがあります。
- 電源アダプタはコンセントの奥まで確実に差し込んでください。差し込みが不完全ですと、火災・感電の原因となることがあります。
- 電源アダプタは、ほこりが付着していないことを確認してからコンセントに差し込んでください。また、半年から１年に１回は、電源アダプタをコンセントから抜いて点検、清掃をしてください。ほこりにより、火災・感電の原因となることがあります。
  なお、点検に関しては当社のサービス取扱所にご相談ください。
- 万一、煙が出ている、変なにおいがするなどの異常状態のまま使用すると、火災・感電の原因となることがあります。電源アダプタをコンセントから抜いて、煙が出なくなるのを確認し、当社のサービス取扱所に修理をご依頼ください。お客様による修理は危険ですから絶対におやめください。
- 本商品から異常音がしたり、キャビネットが熱くなっている状態のまま使用すると、火災・感電の原因となることがあります。すぐに電源アダプタをコンセントから抜いて、当社のサービス取扱所に点検をご依頼ください。
- 万一、本商品を落としたり、本商品を破損した場合、または、内部に異物や水などが入った場合は、電源アダプタをコンセントから抜いて、当社のサービス取扱所に修理をご依頼ください。そのまま使用すると、火災・感電の原因となることがあります。
- 本商品の通風孔などから内部に金属類や燃えやすいものなどの、異物を差し込んだり、落としたりしないでください。万一、異物が入った場合は、すぐに本商品の電源アダプタをコンセントから抜いて、当社のサービス取扱所にご連絡ください。そのまま使用すると、火災・感電の原因となることがあります。特に小さなお子様のいるご家庭ではご注意ください。
- 本商品を分解、改造しないでください。火災・感電の原因となることがあります。内部の点検、調整、清掃、修理は当社のサービス取扱所にご依頼ください（分解、改造された商品は修理に応じられない場合があります）。
- 本商品のキャビネットは外さないでください。感電の原因となることがあります。内部の点検、調整、清掃、修理は当社のサービス取扱所にご依頼ください。
- 本商品の電源アダプタコードを傷つけたり、破損したり、加工したり、無理に曲げたり、引っ張ったり、ねじったり、たばねたりしないでください。また、重い物を乗せたり、加熱したりすると電源アダプタコードが破損し、火災・感電の原因となることがあります。電源アダプタコードが傷んだら、当社のサービス取扱所に修理をご依頼ください。
- 本商品の電源アダプタコードが傷んだ状態（芯線の露出、断線など）のまま使用すると、火災・感電の原因となることがあります。すぐに電源アダプタをコンセントから抜いて、当社のサービス取扱所に修理をご依頼ください。
- 本商品に水をかけたり、ぬれた手で本商品の操作や電源アダプタの抜き差しをしないでください。火災・感電の原因となることがあります。
- 本商品を移動するときは、電源アダプタをコンセントから抜き、LANケーブルなど外部の接続線をすべて抜いたことを確認してから行ってください。電源アダプタ、LANケーブルなどが接続されたまま移動すると、電源アダプタコード、LANケーブルなどが傷つき、火災・感電の原因となることがあります。

安全にお使いいただくために必ずお読みください

⚠警告

- 電源アダプタをコンセントから抜くときは、必ず電源アダプタの本体を持って抜いてください。電源アダプタコードを引っ張るとコードが傷つき、火災・感電や断線の原因となることがあります。
- お客様が用意された機器を本商品に接続してお使いになる場合は、あらかじめ当社のサービス取扱所にご確認ください。確認できない場合は絶対に接続してお使いにならないでください。火災・感電の原因となることがあります。
- 本商品を医療機器や高い安全性が要求される用途では使用しないでください。医療事故や、社会的に大きな混乱が発生する原因となることがあります。
- 本商品に付属の CD − ROM をオーディオ用プレイヤーで再生しないでください。大音量によりスピーカの破損や耳の障害の原因となることがあります。
- 近くに雷が発生したときは、電源アダプタをコンセントから抜いてご使用を控えてください。雷による、火災・感電の原因となることがあります。
- 本商品や電源アダプタを熱器具に近づけないでください。キャビネットやコードの被覆が溶けて、火災・感電の原因となることがあります。
- 本商品の電源アダプタには延長コードを使わないでください。火災の原因となることがあります。
- 本商品をお手入れするときは、電源アダプタをコンセントから抜いて行ってください。火災・感電の原因となることがあります。

⚠注意

- 本書の接続方法に従って、LAN ケーブルの接続や回線の接続を行ってください。間違った接続をすると、接続機器や回線設備の故障の原因となることがあります。
- 専用スタンドの底面にはゴム製のすべり止めを使用していますので、ゴムとの接触面が、まれに変色するおそれがあります。
- 本商品を長期間ご使用にならないときは、安全のため必ず本商品の電源アダプタをコンセントから抜いてください。
- 本商品に乗らないでください。特に、小さなお子様のいるご家庭では、ご注意ください。倒れたり、こわしたりして、けがの原因となることがあります。

STOP お願い

- 本商品を落としたり、強い衝撃を与えないでください。故障の原因となることがあります。
- 本商品をぬれた雑巾、ベンジン、シンナー、アルコールなどでふかないでください。本商品の変色や変形の原因となることがあります。汚れがひどいときは、薄い中性洗剤をつけた布をよくしぼって汚れをふき取り、やわらかい布でからぶきしてください。
- 本商品の電源を再投入する場合、電源を切った状態から５秒以上経った後、電源の再投入をしてください。５秒以内に電源の再投入をすると、故障の原因となることがあります。
- 本商品のプラスチック部品の一部に、光の具合によってはキズに見える部分があります。プラスチック部品の製作過程で生じることがあるものですが、構造上および機能上は問題ありません。安心してお使いください。
- 本商品をご使用中、電源アダプタをさわると温かく感じることがありますが、故障ではありませんので、安心してご使用ください。
- 本商品に水滴が付いた場合は、乾いた布でふき取ってください。水滴が付いたまま使用すると、故障の原因となることがあります。
- 本商品の動作中に接続コード類が外れたり、接続が不安定になると故障や誤動作の原因となることがあります。本商品の動作中は、接続コード類には絶対に触れないでください。

目　次

目　次

5 こんなときは

6 ご参考に

マニュアル構成／マニュアルの見かた

マニュアル構成

本商品のマニュアルは、下記のように構成されています。ご利用の目的に合わせてお読みください。

取扱説明書（本書）
本商品の基本的な使いかたについて説明しています。

詳細取扱説明書（CD-ROM）
本商品の設定方法についての詳細な説明を記載しています。

マニュアルの見かた

本書は下記のように構成されています。

1 お使いになる前に

最初にお読みください。
本商品をご利用になる前に必要な情報を記載しています。

2 本商品の設定

本商品とパソコン、回線を接続する方法や、かんたん設定、フレッツ・セーフティの登録、インターネットとフレッツ・スクウェアに接続する方法を説明しています。

3 その他の設定

Web 設定画面の基本操作、その他の機能を設定する方法について説明しています。

4 フレッツ・セーフティ対応機器の変更／廃止

フレッツ・セーフティに登録した機器を変更する場合、フレッツ・セーフティを廃止する場合の手順を説明しています。

5 こんなときは

接続できないなどのトラブルについて、対処方法などを説明しています。

6 ご参考に

詳細取扱説明書の記載内容と、設定記入シート、本商品の仕様などを記載しています。

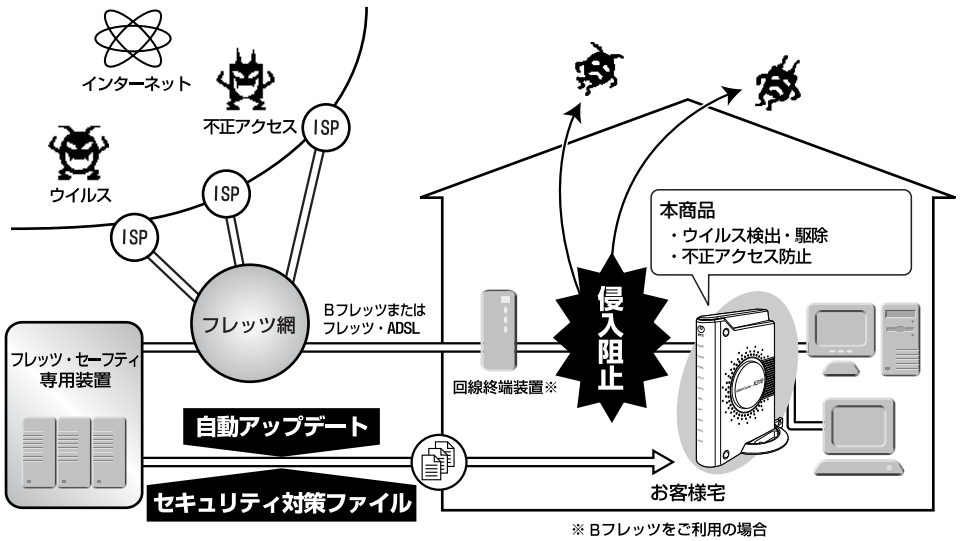
1 お使いになる前に

Web Caster X310 でできること

本商品は、ウイルス対策機能、不正アクセス対策機能を備えた、フレッツ・セーフティ対応のセキュリティ・ルータです。

フレッツ・セーフティ対応

フレッツ・セーフティは、B フレッツまたはフレッツ・ADSL をご利用いただいているお客様に提供するセキュリティサービスです。本商品を最新のセキュリティ対策ファイルでお使いいただくには、フレッツ・セーフティのご契約が必要です。



※ Bフレッツをご利用の場合

●ウイルスと不正アクセスをパソコンの手前でブロック
メールに添付されたファイルのウイルスや不正アクセスをブロックします。
※ホームページを閲覧しているときのホームページからのウイルス感染は防げません。

●常に最新のセキュリティ環境へ自動更新
最新のセキュリティ対策ファイルが自動的にダウンロードされるので、常に最新のセキュリティ環境を維持できます。

●パソコンへのインストールが不要
パソコンごとにウイルス対策ソフトをインストールする必要がありません。パソコンの CPU やメモリに負担をかけずに、インターネットやメールを快適に使えます。

●複数のメールアドレスに対応
回線単位のセキュリティ対策を行うので、メールアドレスごとの設定は不要です。

●万全なウイルスメール対策 ※1 ※2
受信メールだけでなく、送信メールに添付されたファイルもチェックします。Web メールにも対応しています。

●メール通知機能でウイルスをお知らせ
ウイルスメールを検出すると、本商品をご利用のお客様にメールでお知らせします。

※1 対応している Web メールは、Yahoo! メール、Hotmail、AOL メールのみです。
※2 次の 4 つの制限があります。
・メール本体と添付ファイルの合計サイズが 4 MB以上のメール（圧縮ファイルの場合は解凍後のサイズ、また添付ファイルが複数の場合はその合計サイズ）
・暗号化されたメール
・パスワード付きの圧縮メール
・3 階層以上圧縮されたファイル
この制限を超えたメールを処理した場合は、ウイルス検索が実行されていない旨の通知がメールに添付されます。
（1 MB は 1,000,000 B で計算しています）

B フレッツ、フレッツ・ADSL に対応

PPPoEクライアント機能を搭載しています。

複数のパソコンを接続可能

複数のパソコンから同時にインターネットを利用できます。

Unnumbered機能

プロバイダ提供の複数固定 IP アドレスサービスに対応し、サーバをインターネット上に公開できます。

ローカルサーバ機能

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

LAN 上の 1 台のパソコンをインターネット側からアクセスできるようにします。1 対 1 の通信を必要とするネットワークゲームやチャットソフトなどに有効です。また、インターネットでの通信形態（ポート番号）が不明な場合にも有効です。

※ DMZ ホスト機能利用時には、ファイアウォール機能が無効になり、セキュリティが弱くなります。必要なときだけ有効にしてください。

DHCPサーバ機能

LAN側のパソコンへ自動的にIPアドレスを割り当てます。

※手動によるIPアドレスの設定も可能です。

マルチセッション対応

最大5つのPPPoEへ同時に接続できます。

※1つのセッションはフレッツ・スクウェア固定になります。残りの4セッションはお客様が設定できます。

ユニバーサルプラグアンドプレイ機能（UPnP）

Windows Messengerなど UPnP対応アプリケーションを利用することができます。

NAPT機能

プロバイダから提供されるグローバル IP アドレスを LAN 側のプライベートアドレスに変換します。LAN 側の複数のパソコンから同時にインターネットが利用できます。

セキュリティログ

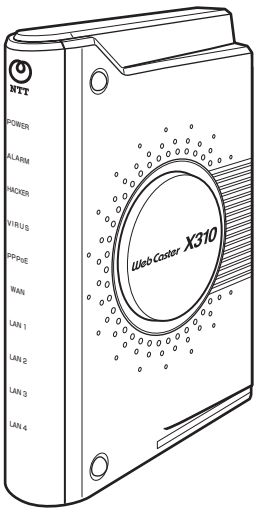
ウイルス検出、セキュリティ対策ファイルのアップデートなど、セキュリティ関連のログを確認できます。

IPv6ブリッジ機能

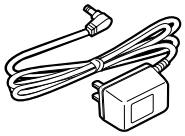
IPv6対応のサービスを利用できます。

セットを確認してください

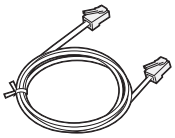
■本体



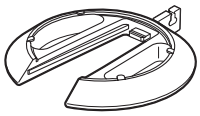
■付属品



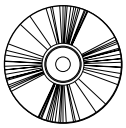
電源アダプタ（1 個）



LAN ケーブル 1.5 m
（1 本：ストレート）



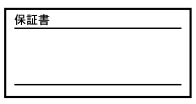
専用スタンド（1 個）



CD-ROM（1 枚）

クイックセットアップ
ガイド（1 部）

取扱説明書（1 部）



保証書（1 枚）

NTT 通信機器
お取扱相談センタ
シール（1 枚）

●セットに足りないものがあったり、取扱説明書に乱丁、落丁があった場合などは、当社のサービス取扱所にご連絡ください。

準備は整っていますか

本商品を接続する前に、以下の項目を確認してください。

チェック１

プロバイダとの契約、工事は完了していますか？

インターネットに接続するには、Bフレッツ、フレッツ・ADSLなどの回線を使ったインターネット接続サービスへの加入が必要です。また、プロバイダによる工事が完了するまでは、インターネットの接続はできません。

チェック２

モデムやケーブルは揃っていますか？

回線と接続するには、回線の種類に応じたモデムなどが必要になります。また、回線への接続が正しくできているか、確認してください。確認方法については、ご契約のプロバイダにお問い合わせください。
本商品とパソコンを接続するには、接続するパソコンの台数分のLANケーブルが必要になります。LANケーブルを購入される場合は、カテゴリ５のLANケーブル（シールドなしツイストペアケーブル、ストレートタイプ）をご購入ください。

チェック３

設定に必要な情報は揃っていますか？

本商品の設定を行う際に、各サービス別に以下の情報が必要です。プロバイダとの契約時に、以下のような情報が提供されますので、契約書類を確認してください。ご不明な場合は、ご契約のプロバイダにお問い合わせください。

●PPPoE接続の場合（Bフレッツ、フレッツ・ADSLなど）

・接続ユーザ名
・接続パスワード
・サービス名（プロバイダから指定された場合のみ）
・DNSサーバのIPアドレス（プロバイダから指定された場合のみ）

お知らせ

● 上記の名称は、プロバイダによって異なる場合があります。ご不明な点は、ご契約のプロバイダにお問い合わせください。
（例）接続ユーザ名：アカウント、ユーザID、ログインIDなど

●NTT東日本をご利用のお客様は

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」を確認してください。

●NTT西日本をご利用のお客様は

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」を確認してください。

（次ページへ続きます）

準備は整っていますか

チェック４

パソコンの準備はできていますか？

本商品と接続するパソコンに、下記のものが揃っていることを確認してください。

●LAN ポート（10BASE-T ／ 100BASE-TX ポート）

ご利用のパソコンに LAN ポートがない場合は、LAN ボード（または LAN カード）を増設してください。詳しくは、LAN ボードの取扱説明書を参照してください。

●OS

本商品は、下記の OS に対応しています。

- Windows® XP ／ 2000 ／ ME ／ 98 Second Edition ／ 98
- Mac OS 9.04 以降
- Mac OS X

●Web ブラウザ

Web ブラウザは、ホームページ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、Netscape Navigator などがあります。
本商品の設定を行うには、下記の Web ブラウザがインストールされている必要があります。

◆Windows® の場合
- Internet Explorer 5.5（サービスパック 2）以降
- Netscape Navigator® 6 以降

◆Mac OS 9.04 以降の場合
Internet Explorer 5.1.6 以降

◆Mac OS X
Internet Explorer 5.2.2 以降

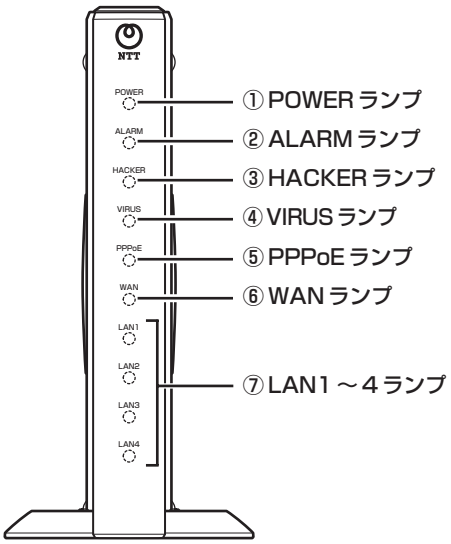
チェック５

フレッツ・セーフティのお申し込みはお済みですか？

本商品を常に最新のセキュリティ環境でお使いいただくためには、フレッツ・セーフティのお申し込みが必要です。
局番なしの「116 番」へお申し込みください。
詳しくは巻末のお問い合わせ一覧をご覧ください。
※NTT 西日本のお客様は、事前にお申し込みが必要です。
※NTT 東日本のお客様は、フレッツ・セーフティの申し込みが済んでいない場合、オンラインで申し込むこともできます。（☛P2-48）

各部の名前

■前面

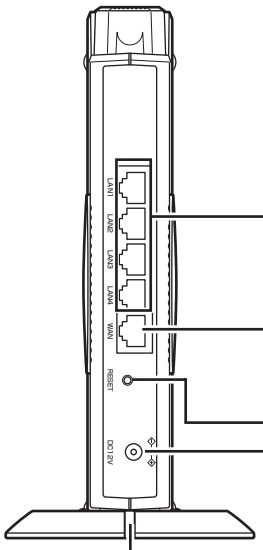


【ランプ表示】

ランプの種類	ランプのつき方（色）	本商品の状態
① POWER ランプ	消灯	電源が切れているとき
	点灯（緑）	電源が入っているとき
② ALARM ランプ	点灯（赤）	起動時のチェックで異常があったとき
③ HACKER ランプ	消灯	不正アクセスレベルが「低」に設定されているとき
	点灯（緑）	不正アクセスレベルが「中」または「高」に設定されているとき
	点灯（赤）	不正アクセスが検出されたとき
④ VIRUS ランプ	消灯	ウイルス検索が無効のとき
	点灯（緑）	ウイルス検索が有効のとき
	点灯（赤）	ウイルスが検出されたとき
⑤ PPPoE ランプ	消灯	オフラインのとき
	点灯（緑）	1 つのセッションで接続中
	点灯（橙）	複数のセッションで接続中
⑥ WAN ランプ	点灯（緑）	100 Mbps リンク
	点灯（橙）	10 Mbps リンク
	点滅（緑）	100 Mbps でデータを送受信しているとき
	点滅（橙）	10 Mbps でデータを送受信しているとき
⑦ LAN1 ～ 4 ランプ	点灯（緑）	100 Mbps リンク
	点灯（橙）	10 Mbps リンク
	点滅（緑）	100 Mbps でデータを送受信しているとき
	点滅（橙）	10 Mbps でデータを送受信しているとき
⑧ VIRUS ランプ ＋ HACKER ランプ	同時に遅い点滅（緑）	セキュリティ対策ファイルを更新しているとき
	同時に速い点滅（緑）	ファームウェアを更新しているとき

各部の名前

■背面



①LAN1 ～4 ポート
パソコンのLAN ポートと接続します。

② WAN ポート
回線終端装置（ONU）などやADSL モデム等のLAN ポートと接続します。

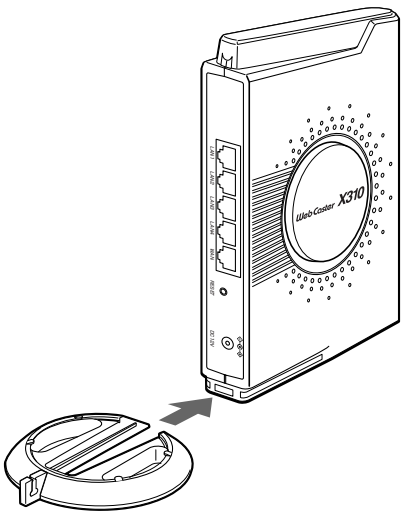
③RESET スイッチ
本商品をお買い求め時の設定に戻すときや（☛P5-2）、再起動するときに使用します。（☛P3-41）

④電源アダプタコード端子
電源アダプタを接続します。

⑤電源アダプタコード固定用溝
電源アダプタコードを固定用溝に差し込み、電源アダプタコードを約 90°曲げて固定します。

専用スタンドを取り付ける

付属品の専用スタンドを使用して、本商品を設置します。
本商品の底面に専用スタンドを取り付けます。



2 本商品の設定

ネットワークに接続するまでの流れ

1 準備は整っていますか？（☛P1-5）

必要なものが揃っているか、あらかじめ確認のうえ、ご契約のプロバイダからの設定情報をお手元にご用意ください。
また、作業の前に必ずパソコンの電源を切ってください。
※本商品を利用する場合は、パソコンにフレッツ接続ツール（PPPoE）をインストールする必要はありません。

↓

2 回線を接続する（☛P2-3）

↓

3 本商品の電源を入れる（☛P2-6）

↓

4 パソコンの電源を入れる（☛P2-7）

↓

5 パソコンを設定する

パソコンの設定について（☛P2-8）

↓

6 Web ブラウザを設定する（☛P2-37）

↓

7 かんたん設定を行う（☛P2-39）

↓

8 インターネットに接続する（☛P2-55）

↓

9 フレッツ・スクウェアに接続する（☛P2-57）

回線を接続する

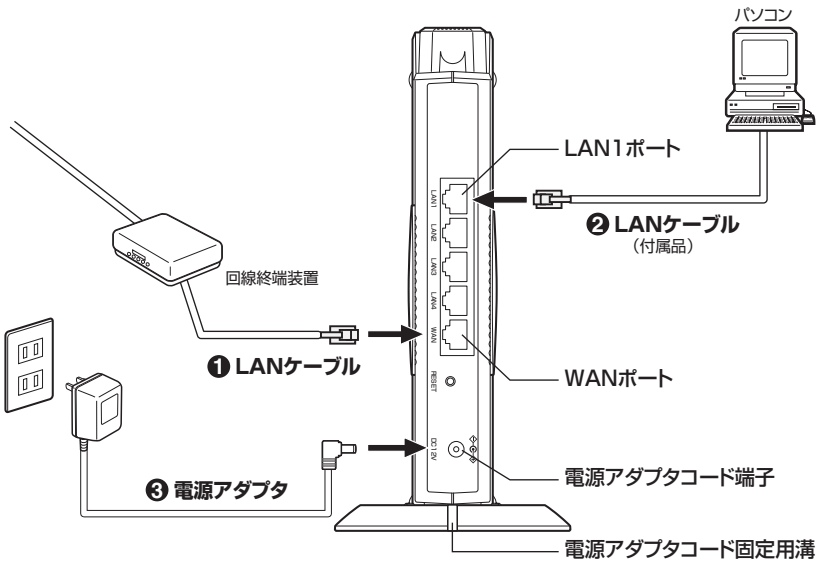
本商品と回線、パソコンを接続します。パソコンの電源を切ってから作業を開始してください。
ご利用の回線によって接続方法が異なります。

Bフレッツ（マンションタイプVDSL方式以外）に接続する…（☛下記）
Bフレッツ（マンションタイプVDSL方式）に接続する…（☛P2-4）
フレッツ・ADSLに接続する…（☛P2-5）

・作業の前に必ずパソコンの電源を切ってください。パソコンの電源を切らずに作業を行うと、パソコンのIPアドレスが取得できず、インターネットに接続できません。
・接続前に、パソコンでインターネットに接続できていることを確認してください。

Bフレッツ（マンションタイプVDSL方式以外）に接続する

本商品は、次のような構成で接続することができます。



1 回線終端装置（ONU）などと本商品を接続する。

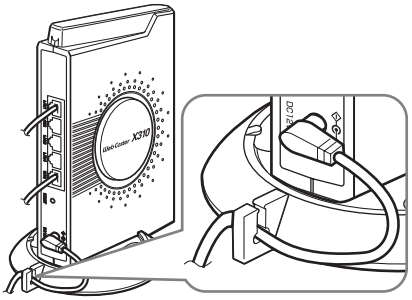
回線終端装置のポートと、本商品のWANポートをLANケーブルで接続します。

2 本商品とパソコンを接続する。

本商品のLAN1ポートとパソコンを付属品のLANケーブルで接続します。
2台以上のパソコンを接続する場合は、市販のLANケーブルで本商品のLAN2～4ポートに接続してください。

3 本商品と電源アダプタを接続する。

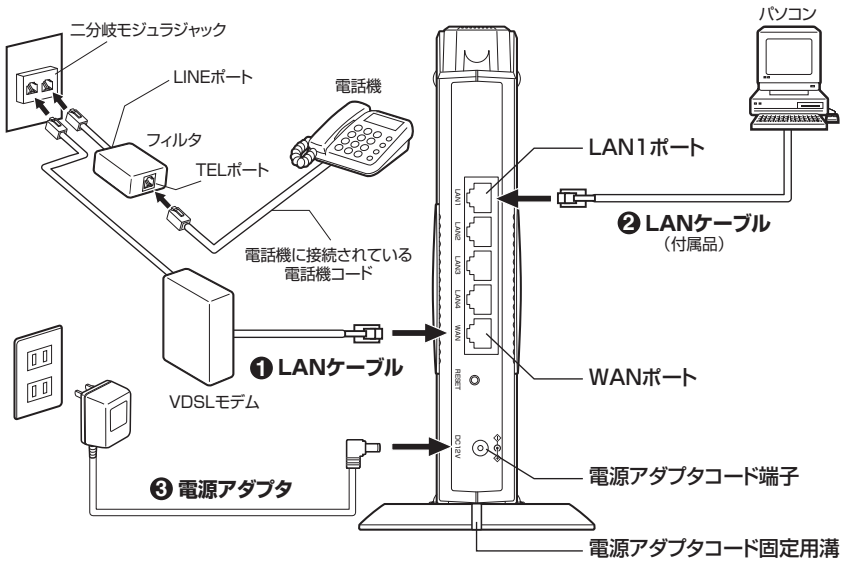
付属品の電源アダプタのプラグを本商品の電源アダプタコード端子に接続し、電源アダプタのコードを電源アダプタコード固定用溝に差し込み、電源アダプタのコードを約90°曲げて固定します。
電源アダプタのプラグは、電源アダプタコード端子にしっかりと差し込んでください。



回線を接続する

B フレッツ（マンションタイプ VDSL 方式）に接続する

本商品は、次のような構成で接続することができます。



1 VDSL モデムと本商品を接続する。

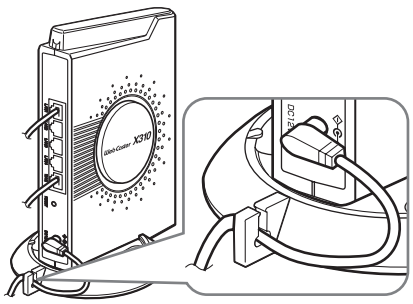
VDSL モデムの LAN ポートと、本商品の WAN ポートを LAN ケーブルで接続します。
VDSL モデム、電話機、フィルタの接続方法と VDSL モデムの設定方法は、各機器の取扱説明書を参照してください。

2 本商品とパソコンを接続する。

本商品の LAN1 ポートとパソコンを付属品の LAN ケーブルで接続します。
2 台以上のパソコンを接続する場合は、市販の LAN ケーブルで本商品の LAN2 ～ 4 ポートに接続してください。

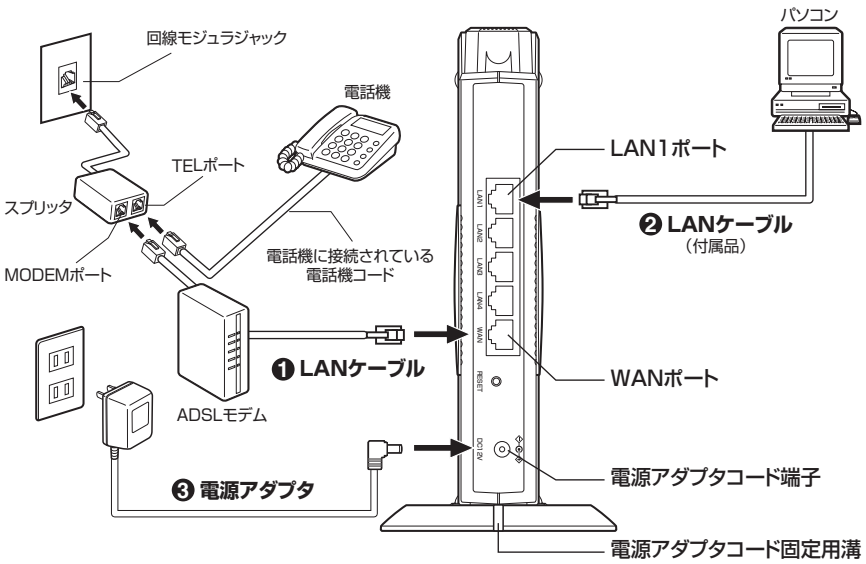
3 本商品と電源アダプタを接続する。

付属品の電源アダプタのプラグを本商品の電源アダプタコード端子に接続し、電源アダプタのコードを電源アダプタコード固定用溝に差し込み、電源アダプタのコードを約 90° 曲げて固定します。
電源アダプタのプラグは、電源アダプタコード端子にしっかりと差し込んでください。



フレッツ・ ADSL に接続する

本商品は、次のような構成で接続することができます。
※ IP 電話対応 ADSL モデムをすでにご利用の場合は、詳細取扱説明書（P2-2）を参照してください。



1 ADSL モデムと本商品を接続する。

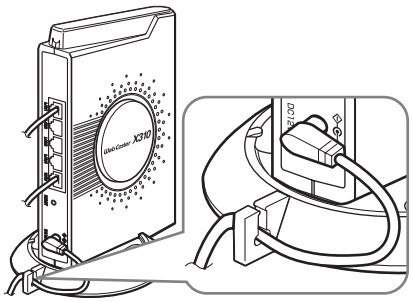
ADSL モデムの LAN ポートと、本商品の WAN ポートを LAN ケーブルで接続します。
ADSL モデム、電話機、スプリッタの接続方法と ADSL モデムの設定方法は、各機器の取扱説明書を参照してください。

2 本商品とパソコンを接続する。

本商品の LAN1 ポートとパソコンを付属品の LAN ケーブルで接続します。
2 台以上のパソコンを接続する場合は、市販の LAN ケーブルで本商品の LAN2 ～ 4 ポートに接続してください。

3 本商品と電源アダプタを接続する。

付属品の電源アダプタのプラグを本商品の電源アダプタコード端子に接続し、電源アダプタのコードを電源アダプタコード固定用溝に差し込み、電源アダプタのコードを約 90° 曲げて固定します。
電源アダプタのプラグは、電源アダプタコード端子にしっかりと差し込んでください。



電源を入れる

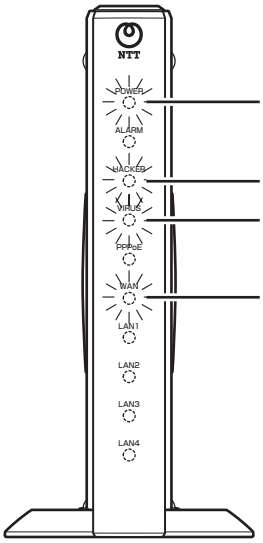
接続が終わったら、本商品の電源を入れてランプの状態を確認します。

本商品の電源を入れる

1 本商品の電源アダプタをコンセントに差し込む。

2 約１～２分後にランプの状態を確認する。

ランプの状態が以下のようになっていることを確認してください。



●POWER ランプ：緑点灯

POWER ランプが点灯しない場合は、コンセントに電源アダプタが接続されていることを確認してください。また、本商品背面の電源アダプタコード端子に電源アダプタのプラグがしっかりと差し込まれていることを確認してください。

●WAN ランプ：緑点灯または橙点灯

WAN ランプが点灯しない場合は、本商品裏面の WAN ポートに LAN ケーブルが確実に接続されていること、および ADSL モデム等の電源が入っていることを確認してください。

●ALARM ランプ：消灯

●HACKER ランプ：緑点灯

●VIRUS ランプ：緑点灯

上記以外の状態になったときは、「回線を接続する」（☛P2-3～2-5）の手順をもう一度ご確認ください。

お知らせ

● 本商品には電源スイッチがありません。電源アダプタをコンセントに差し込むと電源が入りますので、ご注意ください。

お願い

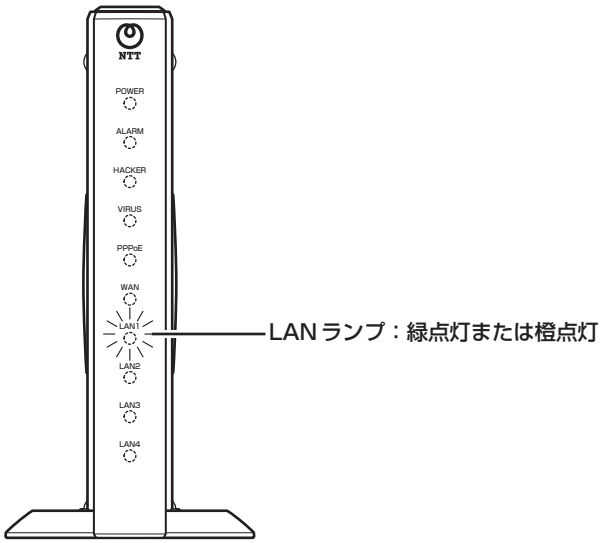
● 本商品は、ファームウェアを常に最新の状態に保つために電源を入れると自動的にファームウェアのアップデートを行う機能を持っています。そのため、本商品の起動直後にファームウェアのアップデートが行われ、本商品が再起動することがあります。
機器故障の原因となるため、アップデート中および再起動中は本商品の電源アダプタは絶対に抜かないでください。

パソコンの電源を入れる

1 本商品のLAN側接続ポートに接続されているパソコンの電源を入れる。

2 ランプの状態を確認する。

ランプの状態が以下のようになっていることを確認してください。

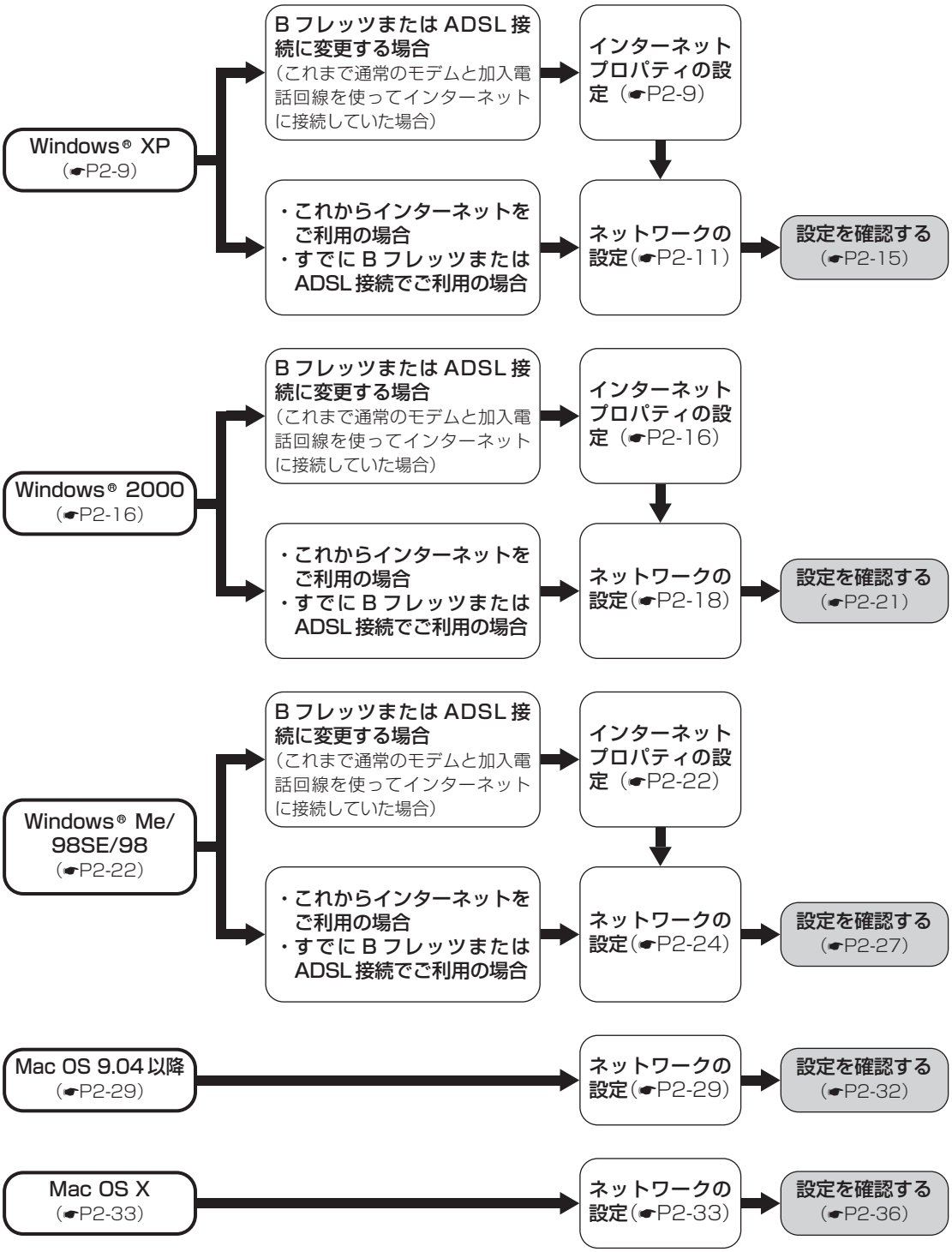


●LANランプ：緑点灯または橙点灯

LANランプが点灯しない場合は、LANポートにLANケーブルが確実に接続されていることを確認してください。

パソコンの設定について

本商品を接続してパソコンの設定を行うまでの基本的な流れを示します。
お使いの OS のページをご参照ください。



パソコンの設定（Windows® XP の場合）

Windows® XP の場合は、下記の手順に従ってパソコンを設定します。
本書では Windows® XP 通常の画面イメージで説明しています。お使いになっているパソコンによっては表示が異なる場合があります。
設定後は「Web ブラウザの設定」に進んでください。（☛P2-37）

インターネットプロパティの設定

これまで通常のモデムと加入電話回線を使ってインターネットに接続していた場合は、下記の方法でインターネットの接続を設定してください。
これまで ADSL 接続でインターネットに接続していた場合は、「ネットワークの設定」（☛P2-11）に進んでください。
以下の画面例は Internet Explorer6.0 です。

1 コントロールパネルを表示する。

Windows® XP を起動し、「スタート」メニューから「コントロールパネル」をクリックします。

2 「ネットワークとインターネット接続」を表示する。

コントロールパネルの「ネットワークとインターネット接続」をクリックします。

お知らせ

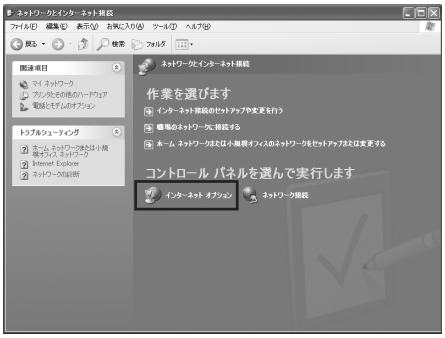
- Windows® XP ではコントロールパネルの表示モードに通常表示モード（カテゴリ表示モード）とクラシック表示モードがあります。この取扱説明書での画面では通常表示モードを前提に記述しています。
- 画面はお使いのパソコンによって一部異なる場合があります。
- Internet Explorer5.5（サービスパック 2）以降、または Netscape Navigator® 6 以降がインストールされていることをご確認ください。
- 「フレッツ接続ツール」を使用する必要はありません。
- Internet Explorer を初めて起動したとき、「インターネット接続ウィザード」というダイアログが起動することがあります。この場合は「キャンセル」をクリックして、ウィザードをいったん終了してください。

（次ページへ続きます）

パソコンの設定（Windows® XP の場合）

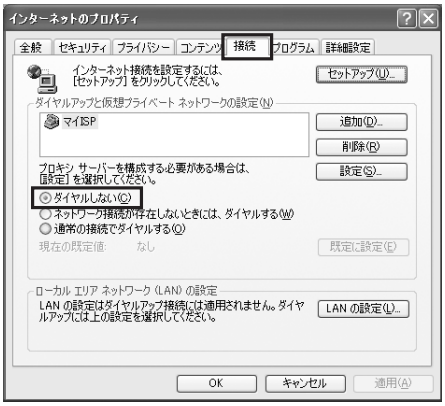
3 「インターネットオプション」を表示する。

「ネットワークとインターネット接続」の「インターネットオプション」をクリックします。

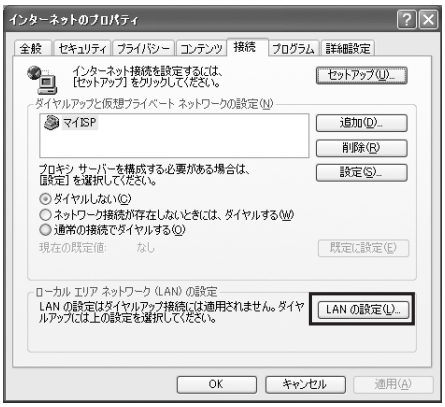


4 「接続」タブで「ダイヤルしない」を選択する。

「インターネットのプロパティ」の「接続」タブをクリックします。
「ダイヤルアップと仮想プライベートネットワークの設定」で「ダイヤルしない」が選択されていることを確認してください。
「ネットワーク接続が存在しないときには、ダイヤルする」や「通常の接続でダイヤルする」が選択されている場合は、「ダイヤルしない」をクリックします。



5 「ローカルエリアネットワーク（LAN）の設定」の「LANの設定」をクリックする。



6 「ローカルエリアネットワーク（LAN）の設定」を設定する。

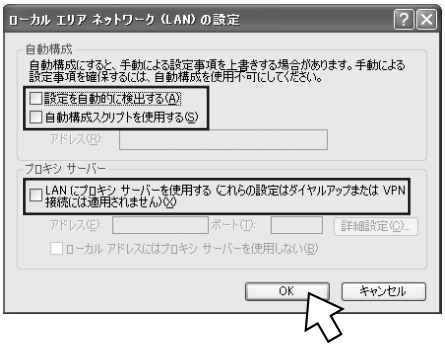
次のように設定します。

①「自動構成」のチェックを外す

「設定を自動的に検出する」、「自動構成スクリプトを使用する」のチェックがついていないことを確認してください。チェックがついている場合は、すべてのチェックを外してください。

②「プロキシサーバー」のチェックを外す

「LANにプロキシサーバーを使用する」のチェックがついていないことを確認してください。チェックがついている場合は、チェックを外し、「OK」をクリックしてください。



お知らせ

● いずれにもチェックがついていないことを確認してください。

③最後に「OK」をクリックする

「インターネットのプロパティ」の設定はこれで終了です。

ネットワークの設定

LANカードの取り付けとドライバのインストールは、ご利用機器メーカのインストール指示に従い、あらかじめ行っておいてください。

1 コントロールパネルを表示する。

Windows® XPを起動し、「スタート」メニューから「コントロールパネル」をクリックします。

（次ページへ続きます）

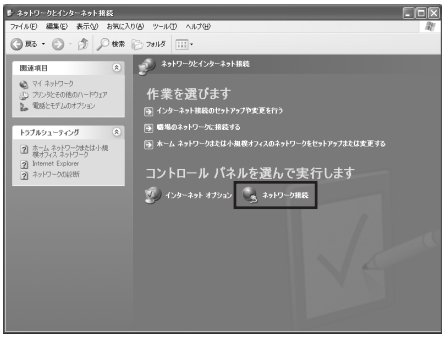
パソコンの設定（Windows® XP の場合）

2 「ネットワークとインターネット接続」を表示する。

コントロールパネルの「ネットワークとインターネット接続」をクリックします。

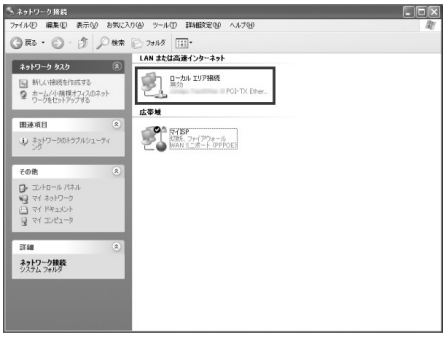
3 「ネットワーク接続」を表示する。

「ネットワークとインターネット接続」の「ネットワーク接続」をクリックします。



4 「ローカルエリア接続の状態」を表示する。

「LANまたは高速インターネット」内の「ローカルエリア接続」をダブルクリックします。



ワンポイント

- 「ネットワーク接続」の「広帯域」の欄に、PPPoE設定がされていて、その設定が既定の接続に設定されている場合には、PPPoEのアイコンを右クリックして、表示されるサブメニューの「既定の接続を解除」を選択し、クリックしてください。（例では、「マイISP」となっています。）本商品を使い、ADSLなどに接続するときは利用しません。

5 「ローカルエリア接続のプロパティ」を表示する。

「ローカルエリア接続の状態」の「プロパティ」をクリックします。

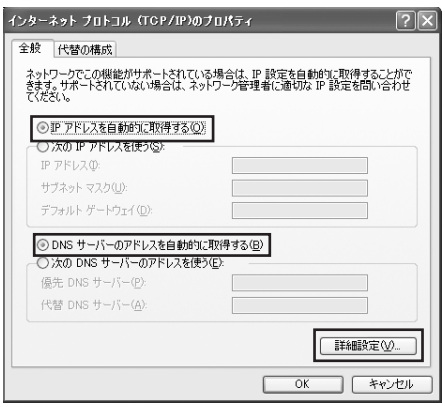
6 「インターネットプロトコル(TCP/IP)のプロパティ」を表示する。

「ローカルエリア接続のプロパティ」の一覧から「インターネットプロトコル(TCP/IP)」を選択し、「プロパティ」をクリックしてください。

※一覧に表示されているチェックは外さないでください。

7 IP アドレスと DNS を設定する。

「インターネットプロトコル(TCP/IP)のプロパティ」の「IP アドレスを自動的に取得する」と、「DNS サーバーのアドレスを自動的に取得する」を選択してください。
IP アドレスと DNS の設定を確認したら「詳細設定」をクリックします。



（次ページへ続きます）

パソコンの設定（Windows® XP の場合）

8 DHCP 設定を確認し、「OK」をクリックする。

「TCP/IP 詳細設定」の「IP 設定」タブをクリックして、一覧に「DHCP 有効」と表示されているか確認します。

ワンポイント

●「DHCP 有効」となっていない場合、手順 7 の画面で「IP アドレスを自動的に取得する」と、「DNS サーバーのアドレスを自動的に取得する」を選択してあるか、再度確認してください。

9 「インターネットプロトコル(TCP/IP)のプロパティ」の［OK］をクリックする。

10 「ローカルエリア接続のプロパティ」の［OK］をクリックする。

11 「ローカルエリア接続の状態」の［閉じる］をクリックする。

ネットワークの設定を確認する

パソコン(LAN カード)と本商品が正しく接続・設定されているか確認する場合、Windows® XP では次の手順で確認します。

1 「ローカルエリア接続の状態」を表示する。

「ネットワークの設定」の手順 1 ～ 4 を行います。(☛P2-11 ～ P2-12)

2 「サポート」タブで「接続状態」を確認する。

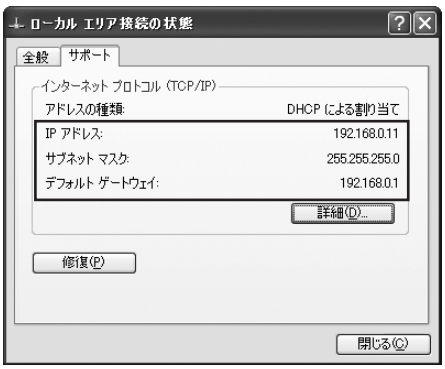
「ローカルエリア接続の状態」の「サポート」タブをクリックします。

3 IP アドレスを確認する。

確認する箇所は以下のとおりです。

・IP アドレス
・サブネットマスク
・デフォルトゲートウェイ

これらのアドレスはすべて自動で設定されます。



ワンポイント

- 各情報が正常に設定されていない場合は、「修復」をクリックしてください。IP アドレス、サブネットマスク、デフォルトゲートウェイの各情報が再度表示されます。
- 「修復」をクリックしても各情報が正常に設定されていない場合は、パソコンの電源を切ってから電源やケーブルなどの接続を確認し、再起動してください。

4 [閉じる] をクリックする。

パソコンの設定（Windows® 2000 の場合）

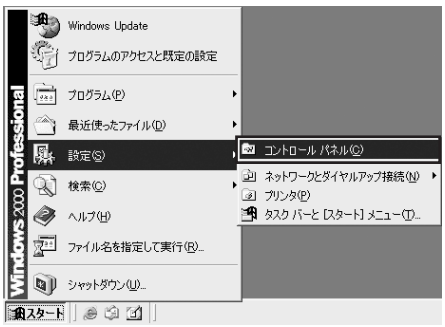
Windows® 2000 の場合は、下記の手順に従ってパソコンを設定します。
設定後は「Web ブラウザの設定」に進んでください。（☛P2-37）
お使いになっているパソコンによっては画面の表示が異なる場合があります。

インターネットプロパティの設定

これまで通常のモデムと加入電話回線を使ってインターネットに接続していた場合は、下記の方法でインターネットの接続を設定してください。
これまで ADSL 接続でインターネットに接続していた場合は、「ネットワークの設定」（☛P2-18）に進んでください。
以下の画面例は Internet Explorer6.0 です。

1 コントロールパネルを表示する。

Windows® 2000 を起動し、「スタート」メニューから「設定」→「コントロールパネル」をクリックします。



2 「インターネットのプロパティ」を表示する。

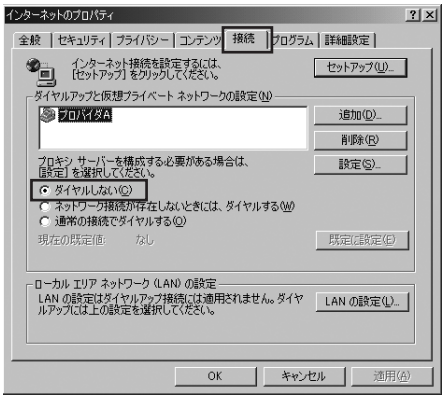
コントロールパネルから「インターネットオプション」のアイコンをダブルクリックします。

お知らせ

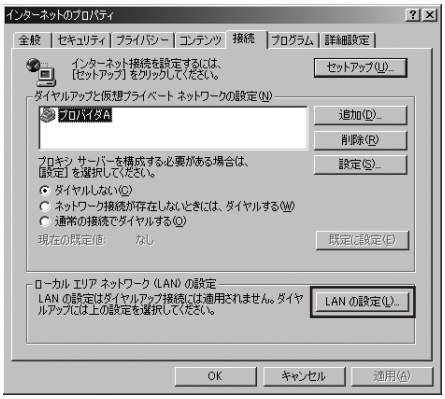
- Internet Explorer5.5（サービスパック 2）以降、または Netscape Navigator® 6 以降がインストールされていることをご確認ください。
- 「フレッツ接続ツール」を使用する必要はありません。
- Internet Explorer を初めて起動したとき、「インターネット接続ウィザード」というダイアログが起動することがあります。この場合は「キャンセル」をクリックして、ウィザードをいったん終了してください。

3 「接続」タブで「ダイヤルしない」を選択する。

「インターネットのプロパティ」の「接続」タブをクリックします。
「ダイヤルアップと仮想プライベートネットワークの設定」で「ダイヤルしない」が選択されていることを確認してください。
「ネットワーク接続が存在しないときには、ダイヤルする」や「通常の接続でダイヤルする」が選択されている場合は、「ダイヤルしない」をクリックします。



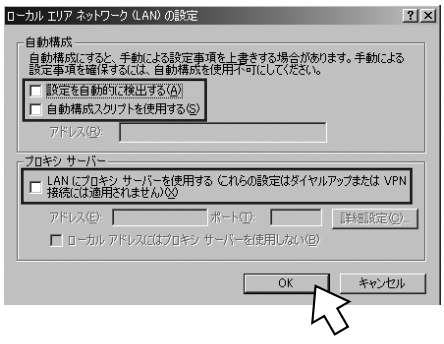
4 「ローカルエリアネットワーク（LAN）の設定」の「LANの設定」をクリックする。



5 ローカルエリアネットワーク（LAN）の設定をする。

次のように設定します。
①「自動構成」のチェックを外す
「設定を自動的に検出する」、「自動構成スクリプトを使用する」のチェックがついていないことを確認してください。チェックがついている場合は、すべてのチェックを外してください。

②「プロキシサーバー」のチェックを外す
「プロキシサーバーを使用する」のチェックがついていないことを確認してください。チェックがついている場合は、チェックを外し、「OK」をクリックしてください。



お知らせ

●いずれにもチェックがついていないことを確認してください。

③最後に「OK」をクリックする
「インターネットのプロパティ」の設定はこれで終了です。

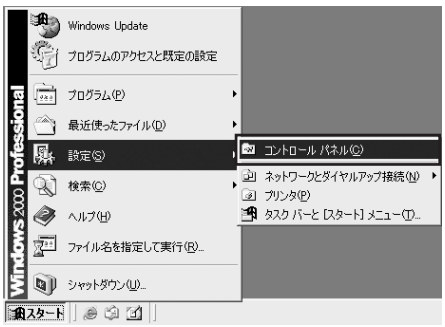
パソコンの設定（Windows® 2000 の場合）

ネットワークの設定

LAN カードの取り付けとドライバのインストールは、ご利用機器メーカのインストール指示に従い、あらかじめ行っておいてください。

1 コントロールパネルを表示する。

Windows® 2000 を起動して「スタート」メニューから「設定」→「コントロールパネル」をクリックします。

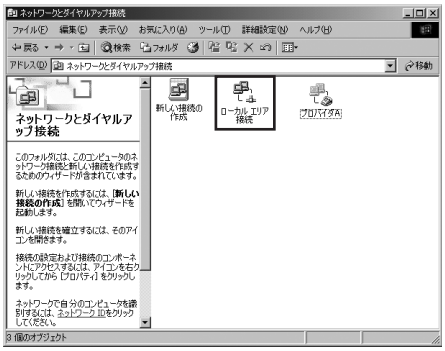


2 「ネットワークとダイヤルアップ接続」を表示する。

コントロールパネルの「ネットワークとダイヤルアップ接続」をダブルクリックします。

3 「ローカルエリア接続」を表示する。

「ネットワークとダイヤルアップ接続」から「ローカルエリア接続」のアイコンをダブルクリックします。



4 「ローカルエリア接続のプロパティ」を表示する。

「ローカルエリア接続状態」の「プロパティ」をクリックします。

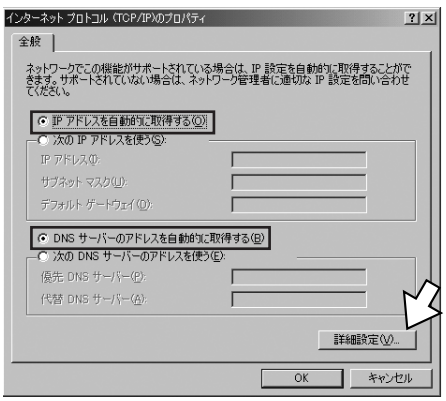
5 「インターネットプロトコル(TCP/IP)のプロパティ」を表示する。

「ローカルエリア接続のプロパティ」の一覧から「インターネットプロトコル(TCP/IP)」を選択し、「プロパティ」をクリックしてください。

※一覧に表示されているチェックは外さないでください。

6 IP アドレスと DNS を設定する。

「インターネットプロトコル(TCP/IP)のプロパティ」の「IP アドレスを自動的に取得する」と、「DNS サーバーのアドレスを自動的に取得する」を選択してください。
IP アドレスと DNS の設定を確認したら「詳細設定」をクリックします。



（次ページへ続きます）

パソコンの設定（Windows® 2000 の場合）

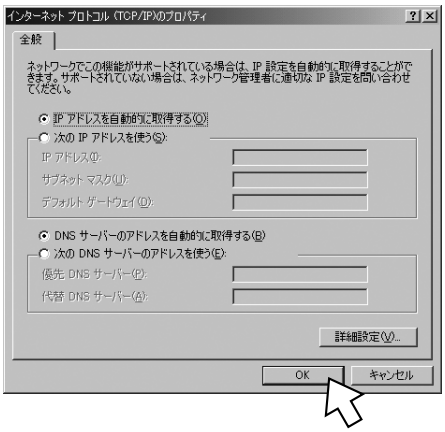
7 DHCP 設定を確認し、［OK］をクリックする。

「TCP/IP 詳細設定」の「IP 設定」タブをクリックして、一覧に「DHCP 有効」と表示されているか確認します。

ワンポイント

●「DHCP 有効」となっていない場合、手順６の画面で「IP アドレスを自動的に取得する」と、「DNS サーバーのアドレスを自動的に取得する」を選択してあるか、再度チェックをしてください。

8 「インターネットプロトコル(TCP/IP)のプロパティ」の［OK］をクリックする。



9 「ローカルエリア接続のプロパティ」の「OK」をクリックする。

10 「ローカルエリア接続状態」の［閉じる］をクリックする。

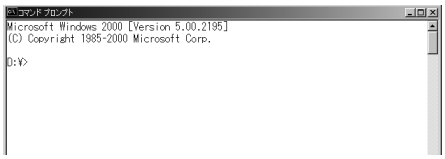
ネットワークの設定を確認する

パソコン(LAN カード)と本商品が正しく接続・設定されているか確認する場合、Windows® 2000 ではコマンドプロンプトを起動して操作します。

1 コマンドプロンプトを起動する。

「スタート」メニューから「プログラム」→「アクセサリ」→「コマンドプロンプト」を順次選択し、「コマンドプロンプト」をクリックします。

コマンドプロンプトが表示されます。



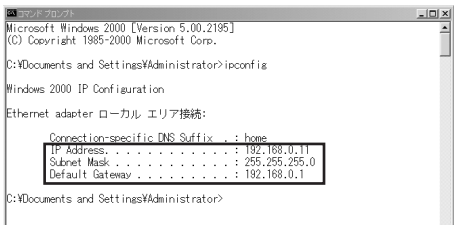
2 ipconfig コマンドを実行する。

コマンドプロンプトが開いたら、キーボードから半角英字で「ipconfig」と入力し、Enter キーを押します。ipconfig コマンドを実行すると、接続している各ネットワークアダプタについて、IP アドレス、サブネットマスク、デフォルトゲートウェイなどの情報が表示されます。

ローカルエリア接続の以下の箇所を確認します。

- IP Address
- Subnet Mask
- Default Gateway

これらの情報はすべて自動で設定されます。



ワンポイント

- 各情報が正しく設定されていない場合は、半角英字で「ipconfig /renew」と入力し、Enter キーを押してください。IP Address、Subnet Mask、Default Gateway の各情報が再度表示されます。
- 「ipconfig /renew」を実行しても各情報が正常に設定されていない場合は、パソコンの電源を切ってから電源やケーブルなどの接続を確認し、再起動してください。

パソコンの設定（Windows® Me/98SE/98 の場合）

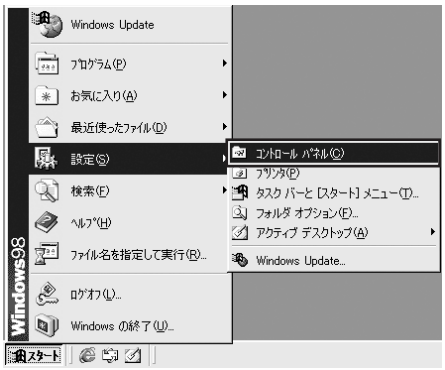
Windows® Me/98SE/98 の場合は、下記の手順に従ってパソコンを設定します。
設定後は「Web ブラウザの設定」に進んでください。（☛P2-37）
画面は Windows® 98SE の例です。
お使いになっているパソコンによっては画面の表示が異なる場合があります。

インターネットプロパティの設定

これまで通常のモデムと加入電話回線を使ってインターネットに接続していた場合は、下記の方法でインターネットの接続を設定してください。
これまで ADSL 接続でインターネットに接続していた場合は、「ネットワークの設定」（☛P2-24）に進んでください。
以下の画面例は Internet Explorer5.5 です。

1 コントロールパネルを表示する。

Windows® Me／98SE／98 を起動し、「スタート」メニューから「設定」→「コントロールパネル」をクリックします。



2 「インターネットのプロパティ」を表示する。

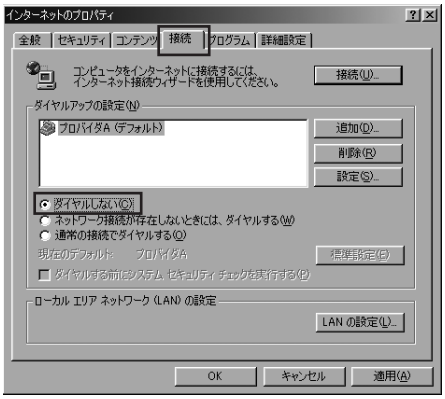
コントロールパネルから「インターネットオプション」のアイコンをダブルクリックします。

お知らせ

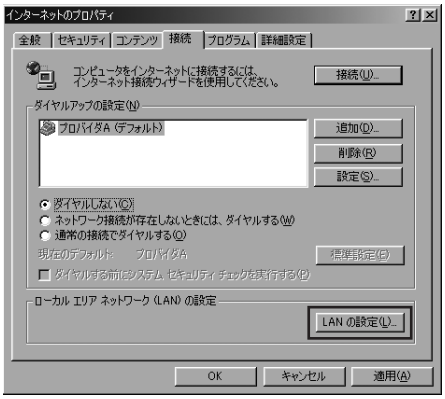
- Internet Explorer5.5（サービスパック 2）以降、または Netscape Navigator® 6 以降がインストールされていることをご確認ください。
- 「フレッツ接続ツール」を使用する必要はありません。
- Internet Explorer を初めて起動したとき、「インターネット接続ウィザード」というダイアログが起動することがあります。この場合は「キャンセル」をクリックして、ウィザードをいったん終了してください。

3 「接続」タブで「ダイヤルしない」を選択する。

「インターネットのプロパティ」の「接続」タブをクリックします。
「ダイヤルアップの設定」で「ダイヤルしない」が選択されていることを確認してください。
「ネットワーク接続が存在しないときには、ダイヤルする」や「通常の接続でダイヤルする」が選択されている場合は、「ダイヤルしない」をクリックします。



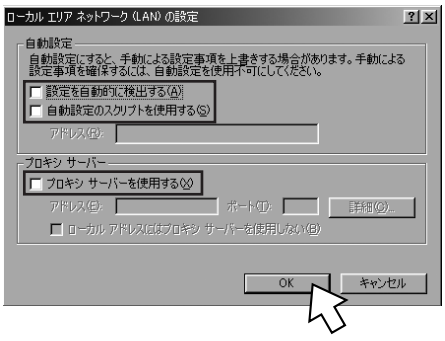
4 「ローカルエリアネットワーク（LAN）の設定」の「LANの設定」をクリックする。



5 ローカルエリアネットワーク（LAN）の設定をする。

次のように設定します。
①「自動設定」のチェックを外す
「設定を自動的に検出する」、「自動設定のスクリプトを使用する」のチェックがついていないことを確認してください。チェックがついている場合は、すべてのチェックを外してください。

②「プロキシサーバー」のチェックを外す
「プロキシサーバーを使用する」のチェックがついていないことを確認してください。チェックがついている場合は、チェックを外し、「OK」をクリックしてください。



お知らせ

●いずれにもチェックがついていないことを確認してください。

③最後に「OK」をクリックする
「インターネットのプロパティ」の設定はこれで終了です。

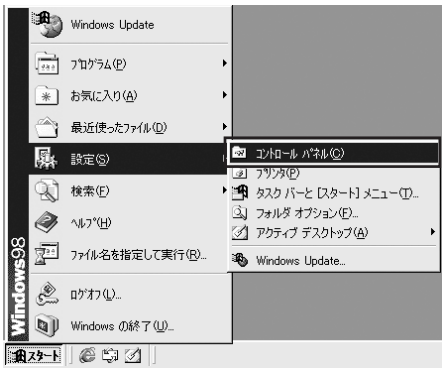
パソコンの設定（Windows® Me/98SE/98 の場合）

ネットワークの設定

LAN カードの取り付けとドライバのインストールは、ご利用機器メーカのインストール指示に従い、あらかじめ行っておいてください。

1 コントロールパネルを表示する。

「スタート」メニューから「設定」→「コントロールパネル」をクリックします。



2 ネットワークを表示する。

コントロールパネルから「ネットワーク」のアイコンをダブルクリックします。

ワンポイント

● Windows® Me において、コントロールパネルに「ネットワーク」のアイコンが表示されていない場合は、画面に表示されている「すべてのコントロールパネルのオプションを表示する。」をクリックしてください。

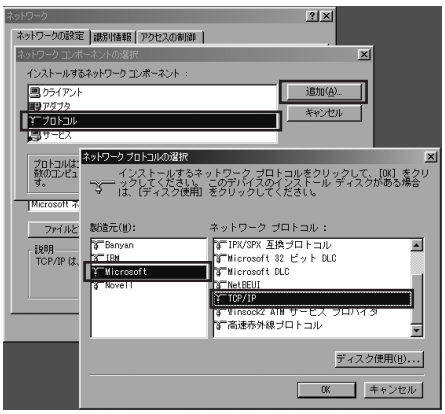
3 TCP/IPのプロパティを表示する。

「現在のネットワークコンポーネント」一覧から「TCP/IP」または「TCP/IP -> <LANドライバ名>※」という項目を選択し、「プロパティ」をクリックします。

※<LANドライバ名>には、パソコンに装着されているLANカードの名称が入ります。

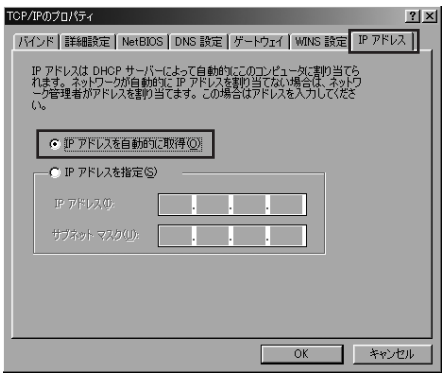
ワンポイント

- 一覧に「TCP/IP -> ダイヤルアップ　アダプタ」という項目が表示されている場合がありますが、これは利用しません。
- 一覧に「TCP/IP」あるいは「TCP/IP -> <LANドライバ名>」という該当の項目がない場合は、「追加」をクリックしてください。
  「インストールするネットワークコンポーネント」の「プロトコル」を選択し、「追加」をクリックします。「製造元」は「Microsoft」を選択し、「ネットワークプロトコル」は「TCP/IP」を選択して「OK」をクリックしてください。
  これで「現在のネットワークコンポーネント」一覧にTCP/IPが追加されます。



4 IPアドレスを設定する。

「TCP/IPのプロパティ」の「IPアドレス」タブをクリックして、「IPアドレスを自動的に取得」を選択します。

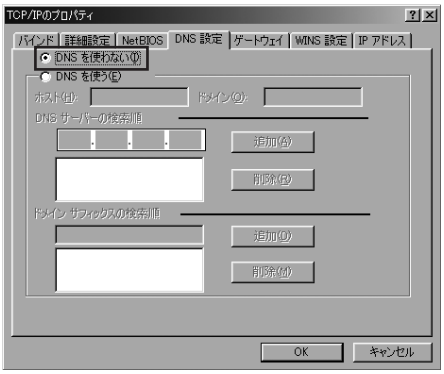


（次ページへ続きます）

パソコンの設定（Windows® Me/98SE/98 の場合）

5 DNS を設定する。

「DNS 設定」タブをクリックして、「DNS を使わない」を選択します。



6 ゲートウェイを設定する。

「ゲートウェイ」タブをクリックして、「インストールされているゲートウェイ」になにも設定されていないことを確認します。この欄に何か設定されている場合は、そのアドレスをクリックして選択してから「削除」をクリックして削除してください。

7 「TCP/IP のプロパティ」を終了する。

IP アドレス、DNS 設定、ゲートウェイを設定後、確認したら「OK」をクリックします。

8 「ネットワーク」を終了する。

「ネットワーク」に戻り、「OK」をクリックします。

ワンポイント

● ご利用中のパソコンによっては Windows® の CD-ROM をセットするようにメッセージが表示されることがあります。その場合は、画面の指示に従って操作してください。

9 パソコンを再起動する。

最後に「今すぐ再起動しますか？」というメッセージが表示されます。「はい」をクリックしてパソコンを再起動してください。

ネットワークの設定変更が必要なかった場合は、再起動を促すメッセージは表示されません。

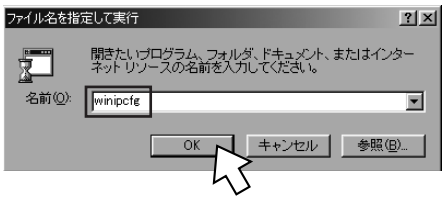
ネットワークの設定を確認する

パソコン(LAN カード)と本商品が正しく接続・設定されているか確認する場合、Windows® Me/98SE/98 では「winipcfg」から確認することができます。

1 「winipcfg」を起動する。

「スタート」メニューから「ファイル名を指定して実行」を選択し、クリックします。

「名前」の入力欄に「winipcfg」と入力し、「OK」をクリックします。

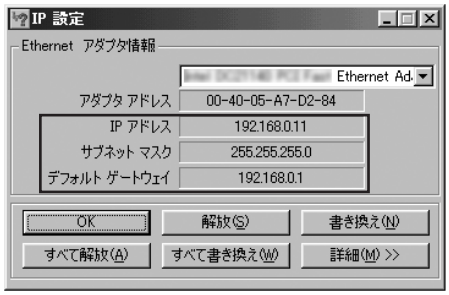


2 IP アドレスを確認する。

winipcfg が起動したら、「Ethernet アダプタ情報」が表示されます。
確認する箇所は以下のとおりです。

- IP アドレス
- サブネットマスク
- デフォルトゲートウェイ

これらの情報はすべて自動で設定されます。
「Ethernet アダプタ情報」が「PPP Adapter.」と表示されている場合は右端のプルダウンメニュー ▼ をクリックして現在ご利用の LAN ドライバ名を選択し、変更してください。



ワンポイント

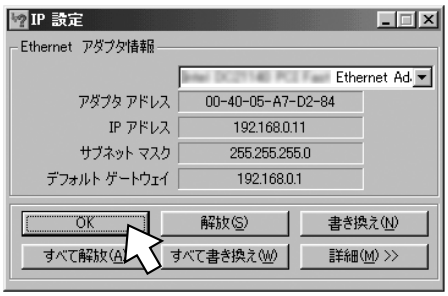
- IP アドレスが「0.0.0.0」となっていたり「デフォルトゲートウェイ」が空白になっていたりする場合は、まず「解放」をクリックして、次に「すべて書き換え」をクリックしてください。この操作で IP アドレスとデフォルトゲートウェイの欄に各情報が表示されれば設定の確認は完了です。
- IP アドレスやデフォルトゲートウェイが正常に設定されていない場合は、パソコンの電源を切ってから電源やケーブルなどの接続を確認し、再起動してください。

（次ページへ続きます）

パソコンの設定（Windows® Me/98SE/98 の場合）

3 「winipcfg」を終了する。

「OK」をクリックします。



パソコンの設定（Mac OS 9.04 以降の場合）

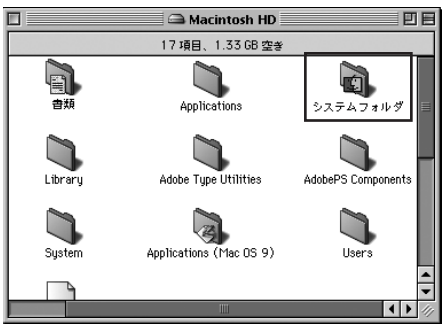
Mac OS 9.04 以降の場合は、下記の手順に従ってパソコンを設定します。お使いになっているパソコンによっては表示が異なる場合があります。
設定後は「Web ブラウザの設定」に進んでください。（☛P2-37）

ネットワークの設定

LAN カードの取り付けとドライバのインストールは、ご利用機器メーカのインストール指示に従い、あらかじめ行っておいてください。

1 「Macintosh HD」をダブルクリックする。

「Macintosh HD」の内容が表示されます。「システムフォルダ」をダブルクリックして「システムフォルダ」を開きます。



2 機能拡張フォルダをダブルクリックする。

本商品を利用するには、「Open Transport」のバージョンが 2.6 以上であることが必要です。ここでは、インストールされている「Open Transport」のバージョンの確認を行います。

3 Open Transport の情報を確認する。

「機能拡張」フォルダの中から「Open Transport」というアイコンをクリックし、メニューバーから「ファイル」→「情報を見る」→「一般情報」を選択します。

（次ページへ続きます）

パソコンの設定（Mac OS 9.04 以降の場合）

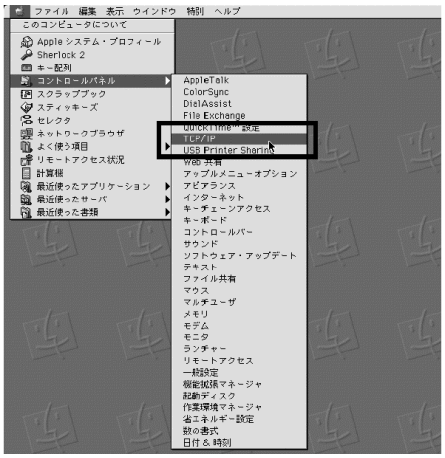
4 Open Transport のバージョンを確認する。

Open Transport のバージョンが 2.6 以降であることを確認します。確認が終わったらウィンドウを閉じます。

※ Open Transport のバージョンが 2.6 以降でなかった場合は、アップルコンピュータのホームページで最新のファイルをダウンロードしてご利用ください。

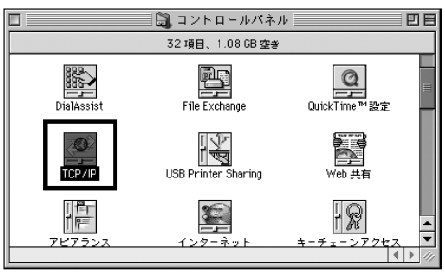
5 TCP/IP 設定ウィンドウを表示する。

「アップル」メニューから「コントロールパネル」→「TCP/IP」を選択して、「TCP/IP」設定ウィンドウを表示します。



ワンポイント

●「アップルメニューオプション」で「サブメニュー」の機能をオフにしている場合は、アップルメニューから「コントロールパネル」を選択し、コントロールパネルのウィンドウが表示されてから「TCP/IP」をダブルクリックします。



6 経由先を選択する。

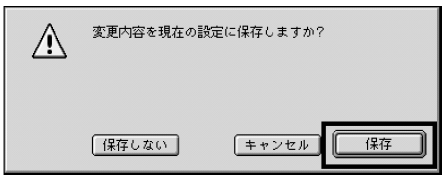
「TCP/IP」設定ウィンドウの「経由先」リストで、「Ethernet」を選択します。

7 設定方法を選択する。

「TCP/IP」設定ウィンドウの「設定方法」リストから「DHCP サーバを参照」を選択します。

8 「TCP/IP」設定ウィンドウを閉じる。

ネットワークの設定が終了したら、「TCP/IP」設定ウィンドウを閉じます。このとき、「変更内容を現在の設定に保存しますか？」というメッセージが表示された場合、「保存」をクリックします。



お知らせ

- Internet Explorer5.1.6 以降がインストールされていることをご確認ください。
- 「フレッツ接続ツール」を使用する必要はありません。

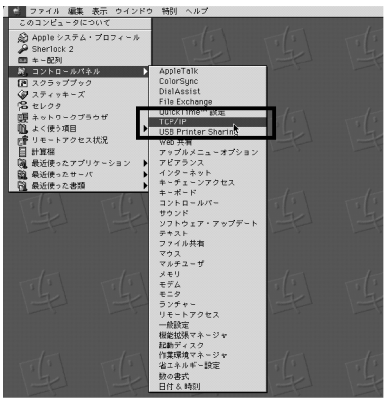
パソコンの設定（Mac OS 9.04 以降の場合）

ネットワークの設定を確認する

Mac OS 9.04 以降でパソコンと本商品が正しく接続されているかどうか確認する場合には、以下のようにしてください。

1 TCP/IP 設定ウィンドウを表示する。

「アップル」メニューから「コントロールパネル」→「TCP/IP」を選択して、「TCP/IP」設定ウィンドウを表示します。

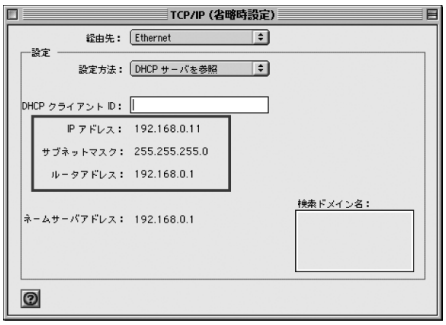


2 ネットワークの設定を確認する。

確認する箇所は以下のとおりです。

・IP アドレス
・サブネットマスク
・ルータアドレス

これらのアドレスはすべて自動で設定されます。



ワンポイント

● 各情報が正常に設定されていない場合は、パソコンの電源を切ってから電源やケーブルなどの接続を確認し、再起動してください。

3 「TCP/IP」設定ウィンドウを閉じる。

ネットワークの設定の確認が終了したら、「TCP/IP」設定ウィンドウを閉じます。このとき、「変更内容を現在の設定に保存しますか？」というメッセージが表示された場合は、「保存しない」をクリックします。

パソコンの設定（Mac OS Xの場合）

Mac OS Xの場合は、下記の手順に従ってパソコンを設定します。お使いになっているパソコンによっては表示が異なる場合があります。
設定後は「Webブラウザの設定」に進んでください。（☛P2-37）
画面はMac OS X（10.3.5）の例です。

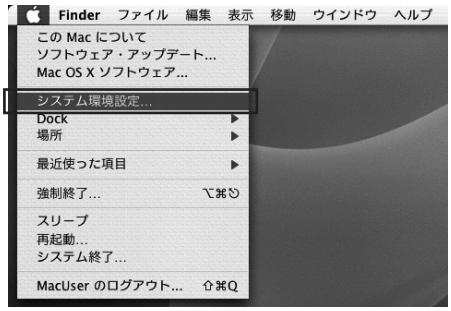
ネットワークの設定

LANカードの取り付けとドライバのインストールは、ご利用機器メーカのインストール指示に従い、あらかじめ行っておいてください。

1 システム環境設定を表示する。

Dock上の「システム環境設定」アイコンをクリックして、「システム環境設定」を表示します。

※ Mac OS Xの標準状態では、Dockに「システム環境設定」のアイコンが登録されています。Dockから削除してしまった場合は、「アップル」メニューから「システム環境設定」を選択します。



2 ネットワークの設定項目をクリックする。

「システム環境設定」のウィンドウから「ネットワーク」をクリックします。

3 ネットワークの種類を選択する。

「ネットワーク」ウィンドウのタブの上部にある「設定」リストから、「内蔵Ethernet」を選択します。

（次ページへ続きます）

パソコンの設定（Mac OS X の場合）

4 「TCP/IP」を設定する。

「TCP/IP」タブをクリックし、TCP/IP の設定画面を表示します。設定内容が以下のようになっていることを確認します。

- 「IPv4 を設定」：「DHCP サーバを参照」
- 「DHCP クライアント ID」：空白
- 「DNS サーバ」：空白
- 「検索ドメイン」：空白

5 「PPPoE」のチェックを外す。

「PPPoE」タブをクリックし、PPPoE の設定画面を表示します。チェックがついている場合は外します。本商品を使い、B フレッツ、フレッツ・ADSL などに接続するときは利用しません。

6 「AppleTalk」のチェックを外す。

「AppleTalk」タブをクリックし、AppleTalk の設定画面を表示します。「AppleTalk 使用」にチェックがついている場合は外します。

7 プロキシを設定する。

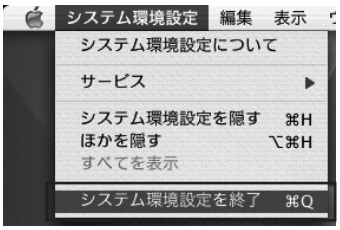
「プロキシ」タブをクリックし、プロキシの設定画面を表示します。ここでチェックがついている場合は、すべて外します。

8 ネットワーク設定を保存する。

右下の「今すぐ適用」（または「保存」）をクリックします。メッセージが表示された場合は、「適用」または「保存する」をクリックします。

9 「システム環境設定」を終了する。

メニューバーの「システム環境設定」→「システム環境設定を終了」を選択して終了します。



お知らせ

- Internet Explorer5.2.2 以降がインストールされていることをご確認ください。
- 「フレッツ接続ツール」を使用する必要はありません。

パソコンの設定（Mac OS X の場合）

ネットワークの設定を確認する

Mac OS X でパソコンと本商品が正しく接続されているかどうか確認する場合には、以下のようにしてください。

1 システム環境設定を表示する。

Dock 上の「システム環境設定」アイコンをクリックして、「システム環境設定」を開きます。「システム環境設定」ウィンドウから「ネットワーク」をクリックします。

2 ネットワークの種類を選択する。

「ネットワーク」ウィンドウのタブの上部にある「設定」リストより、「内蔵 Ethernet」を選択します。

3 「TCP/IP」を確認する。

「TCP/IP」タブをクリックして TCP/IP の設定画面を表示し、IP アドレスが割り当てられていることを確認します。
確認する箇所は以下のとおりです。

- IP アドレス
- サブネットマスク
- ルータ

これらのアドレスはすべて自動で設定されます。

ワンポイント

- 各情報が正常に設定されていない場合は、パソコンの電源を切ってから電源やケーブルなどの接続を確認し、再起動してください。

4 システム環境設定を終了する。

メニューバーの「システム環境設定」→「システム環境設定を終了」を選択して終了します。

Web ブラウザの設定

本商品は、各種の設定、データ変更、状態確認、オンラインウイルス検索などを Web ブラウザで実施します。
設定に必要なブラウザ環境はフレーム表示、JavaScript 対応のものです。

●Windows® をご利用の場合

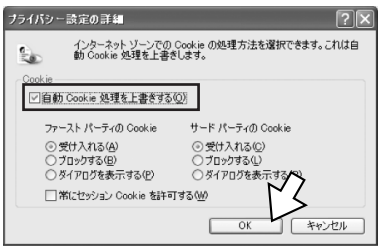
Internet Explorer5.5（サービスパック 2）以降または Netscape Navigator® 6 以降がインストールされていることを確認してください。
ご使用の Web ブラウザで Cookie の設定、JavaScript の設定、キャッシュ機能の設定を確認してください。

＜Cookie の設定＞

（1）Microsoft® Internet Explorer 6 の場合

①Internet Explorer を起動し、ツールバーの「ツール」→「インターネットオプション」をクリックする。

②「プライバシー」タブをクリックし、[詳細設定]をクリックして、「自動 Cookie 処理を上書きする」にチェックがついていることを確認し、［OK］をクリックする。

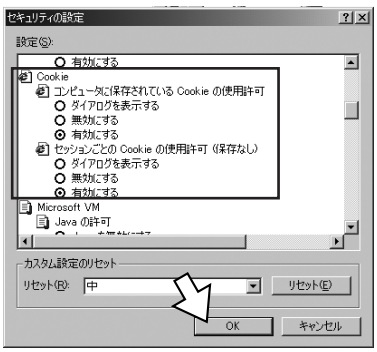


（2）Microsoft® Internet Explorer 5.5 の場合

①Internet Explorer を起動し、ツールバーの「ツール」→「インターネットオプション」をクリックする。

②「セキュリティ」タブをクリックし、「既定のレベル」をクリックしてセキュリティのレベルが「中」になっていることを確認する。

③［レベルのカスタマイズ］をクリックして、Cookie 項目の 2 か所が「有効にする」に設定されていることを確認し、［OK］をクリックする。



お知らせ

- 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。
- Internet Explorer を初めて起動したとき、「インターネット接続ウィザード」というダイアログが起動することがあります。この場合は「キャンセル」をクリックして、ウィザードを終了してください。
- ブラウザの「戻る」、「進む」ボタンは使用しないでください。

（次ページへ続きます）

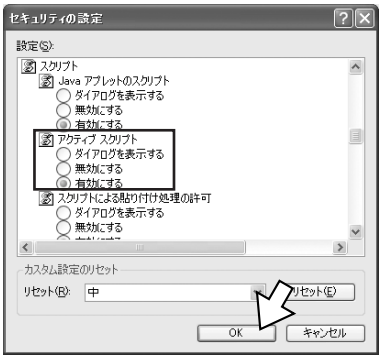
Web ブラウザの設定

＜JavaScript 機能の設定＞

※以下は Internet Explorer 6 のイメージで説明しますが、Internet Explorer 5.5 の場合も同様の手順で実施することができます。

①「セキュリティ」タブをクリックし、［レベルのカスタマイズ］をクリックする。

②スクリプト項目のアクティブスクリプトが「有効にする」に設定されていることを確認し、［OK］をクリックする。

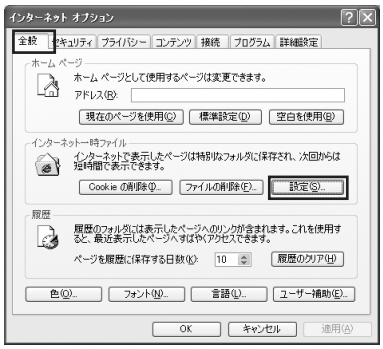


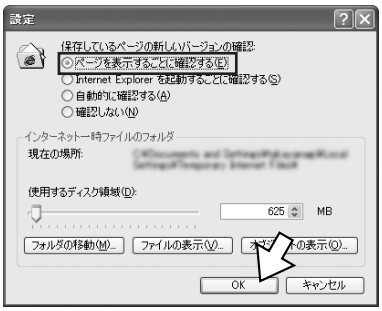
＜キャッシュ機能の設定＞

※以下は Internet Explorer 6 のイメージで説明しますが、Internet Explorer 5.5 の場合も同様の手順で実施することができます。

①「全般」タブをクリックし、［インターネット一時ファイル］の［設定］をクリックする。

②「ページを表示するごとに確認する」にチェックが入っていることを確認し、［OK］をクリックする。





●Macintosh をご利用の場合

Internet Explorer5.1.6 以降（OS X は 5.2.2 以降）がインストールされていることを確認してください。

かんたん設定

Web 設定画面のかんたん設定で、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。

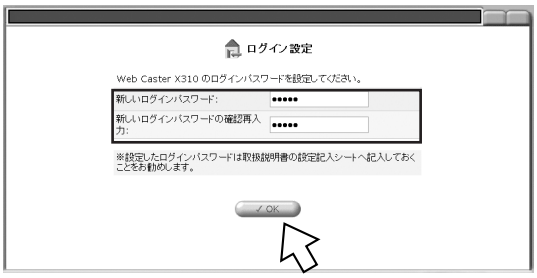
または、「http://wbc_x310」と入力します。

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（☛P6-3）に記入しておくことをお勧めします。
※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。（☛P5-2「お買い求め時の設定に戻すには」）



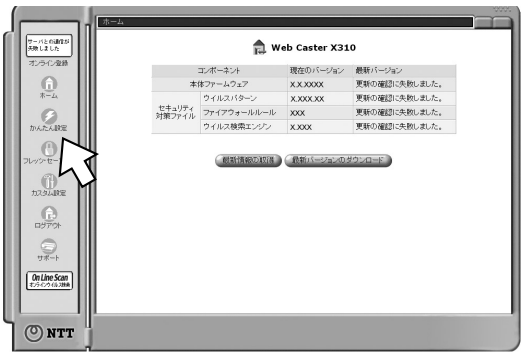
お知らせ

- 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。

（次ページへ続きます）

かんたん設定

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。



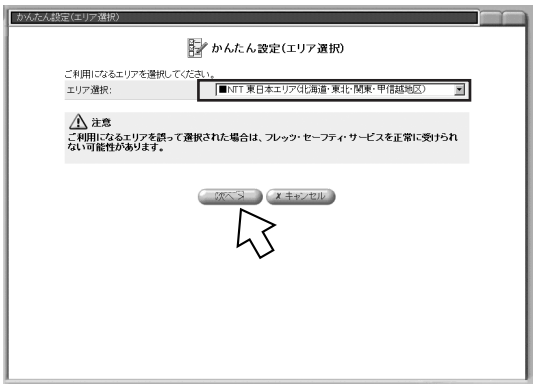
5 エリアを選択する。

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。

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、詳細取扱説明書の２章を参照してください。（詳細取扱説明書 ☛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（☛P2-43）

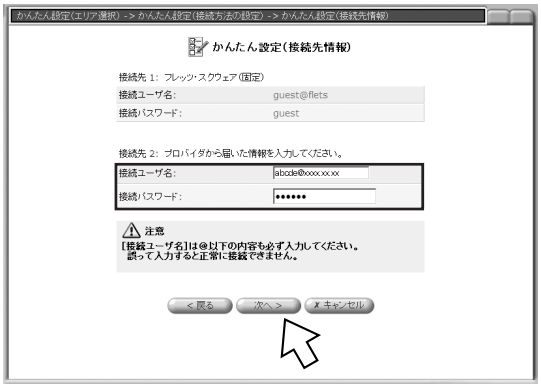
7 接続先を設定する。

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

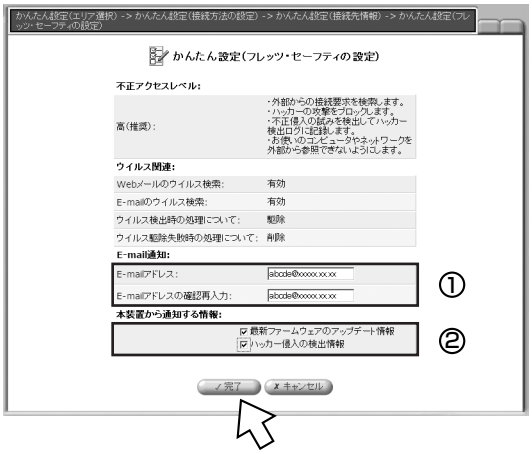
● 入力したパスワードの表示桁数は、お使いのパソコンによって異なる場合があります。

（次ページへ続きます）

かんたん設定

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

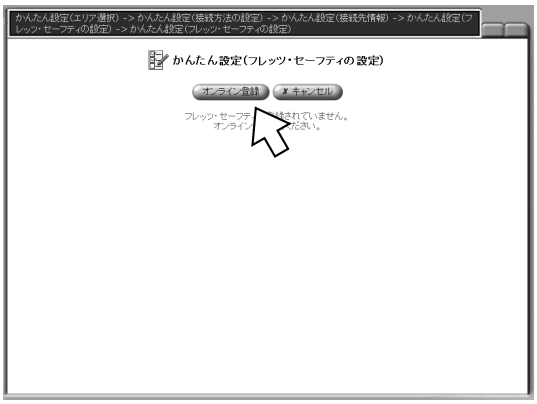
■設定を変更する場合は、かんたん設定の終了後、「フレッツ・セーフティの設定を変更するには」を参照して設定を変更してください。（☛P3-17）

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

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。（☛P2-45）

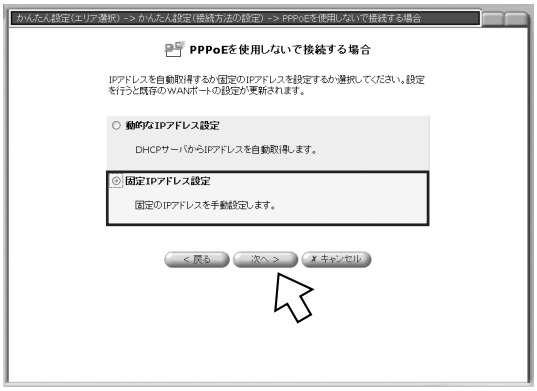


PPPoE 以外の接続で固定の IP アドレスを設定する場合

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。



（次ページへ続きます）

かんたん設定

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。（☛P2-42）

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P2-52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）」（☛P2-48）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

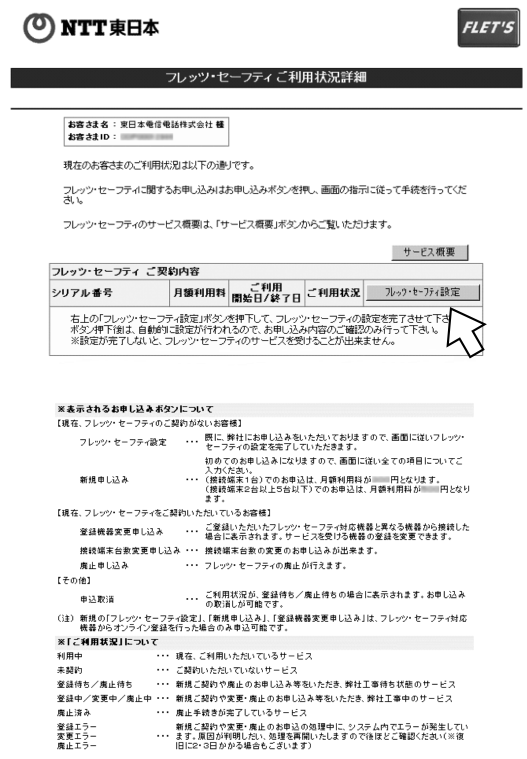
- NTT東日本のお客様で、「接続中のフレッツ・セーフティ対応機器は既に他の回線でご登録中です」と表示された場合は、「セキュリティに関するお問い合わせ（03-5442-7533）」へご連絡ください。NTT西日本のお客様は、お問い合わせいただいてもご回答できません。
- サービス申込受付ページが正常に表示されないときは、Webブラウザの［更新］ボタンなどを押して、再度ホームページを表示してください。
- NTT東日本の各画面は平成17年1月現在の画面です。

（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

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。

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。

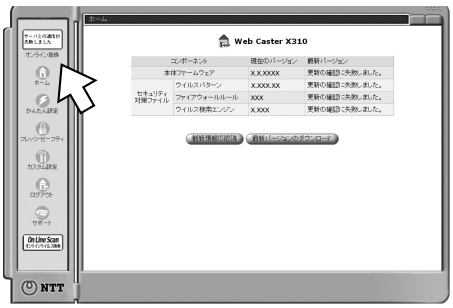
フレッツ・セーフティにオンライン登録する

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

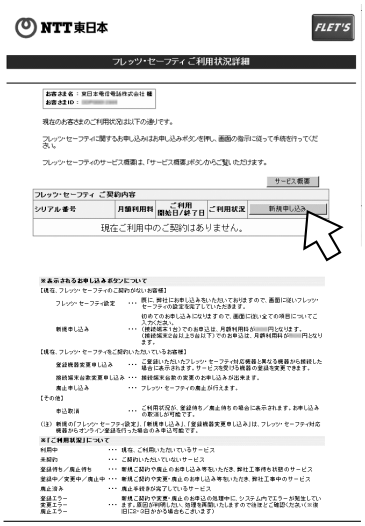
●**「開通のご案内」を紛失した場合は**
116番へご連絡ください。ご本人様確認後、再度「開通のご案内」を送付させていただきます。

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。

3 [新規申し込み] をクリックする。

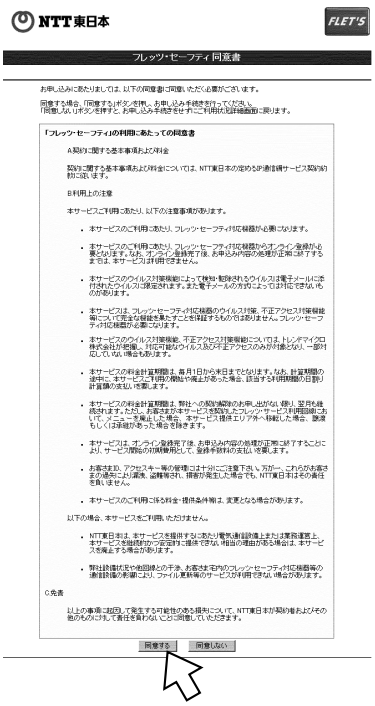
「フレッツ・セーフティ同意書」画面が表示されます。



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。



（次ページへ続きます）

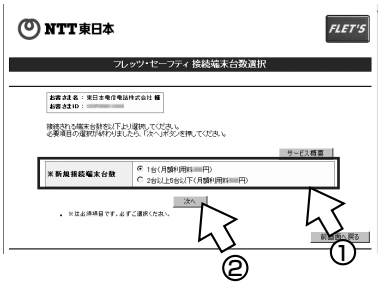
フレッツ・セーフティにオンライン登録する

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。

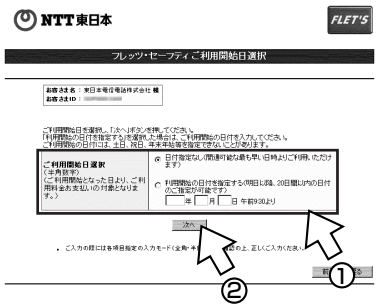
6 接続する端末の台数を入力し、［次へ］をクリックする。

「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。



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。

フレッツ・セーフティにオンライン登録する

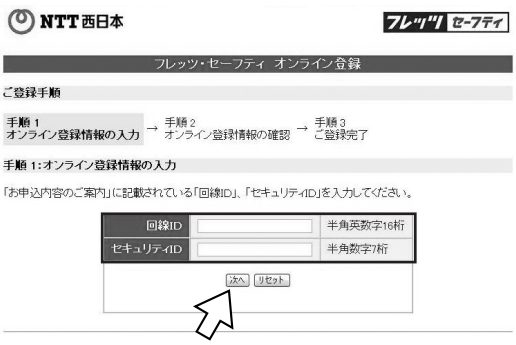
NTT 西日本をご利用のお客様

［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。



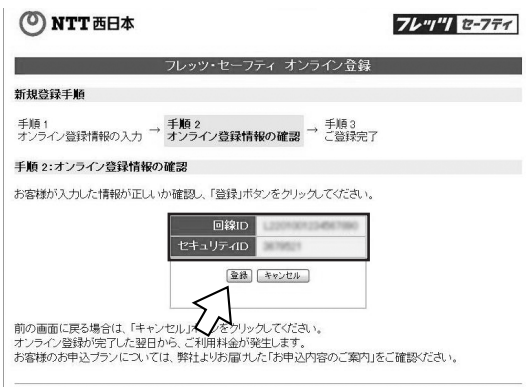
ワンポイント

●「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。

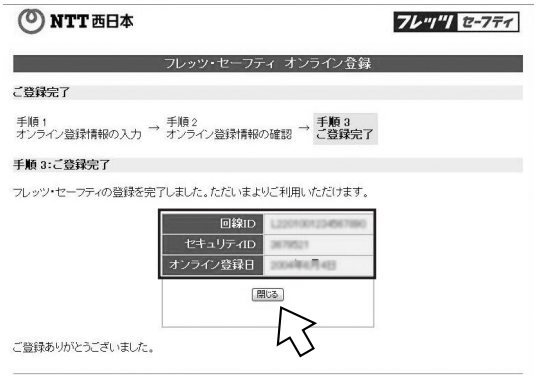


お知らせ

● 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。

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。



フレッツ・セーフティの登録を確認する

本商品のWeb設定画面で、フレッツ・セーフティの登録が完了していることを確認します。

1 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。

2 ログインパスワードを入力し、[OK]をクリックする。

3 [最新情報の取得]をクリックする。

4 [オンライン登録]アイコンが表示されていることを確認する。

フレッツ・セーフティの登録が完了していない場合は、「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。

- フレッツ・セーフティのオンライン登録がお済みの場合は、しばらく待ってからもう一度［最新情報の取得］をクリックしてください。
- フレッツ・セーフティのオンライン登録がお済みでない場合は、［オンライン登録］をクリックして、フレッツ・セーフティの登録を行ってください。

インターネットに接続する

設定が終わったら、インターネットに接続できるかどうかを確認します。

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次の URL を入力し、［Enter］キーを押す。

・NTT 東日本：
http://www.ntt-east.co.jp/
・NTT 西日本：
http://www.ntt-west.co.jp/

3 当社のホームページが表示されることを確認する。

これでインターネットに接続できました。

NTT 東日本

NTT 西日本

（次ページへ続きます）

インターネットに接続する

ワンポイント

● **インターネットに接続できないときは**
「困ったときのQ&A」（☛P5-5）

お知らせ

● ご契約のプロバイダによっては、設定後、インターネットに接続できるようになるまでに時間がかかる場合があります。
● ホームページは平成17年1月現在の画面です。
● Webメールのウイルス検索を有効に設定している場合、画像の多いホームページは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、再度ホームページを表示してください。
● ホームページを表示する際、Webブラウザのキャッシュのタイムアウトなどにより、ホームページが正常に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、再度ホームページを表示してください。

フレッツ・スクウェアに接続する

本商品は、同時に複数の接続先にアクセスすることができます。インターネットに接続しながら、フレッツ・スクウェアに接続できることを確認します。
セキュリティ対策ファイル（☛P3-22）のアップデートを行うためには、フレッツ・スクウェアに接続できることが必要です。

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://www.flets/」と入力し、［Enter］キーを押す。

3 フレッツ・スクウェアのページが表示されることを確認する。

これでフレッツ・スクウェアに接続できました。

以上で基本的な設定は完了です。

NTT 東日本

NTT 西日本

ワンポイント

● **セキュリティ対策ファイルのアップデートを行うには**
対象ファイルを手動でアップデートするには（☛P3-30）の手順により、セキュリティ対策ファイルの最新情報を取得し、更新されたバージョンがある場合は、アップデートを行ってください。

お知らせ

- フレッツ・スクウェアの画面は平成 17 年 1 月現在の画面です。
- ホーム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。

3 その他の設定

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。
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。
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バージョンを確認することができます。

[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。(☛P3-30)

[オンライン登録]
オンライン登録画面が表示されます。
(☛P2-45)

[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。(☛P2-39)

[フレッツ・セーフティ]
フレッツ・セーフティの設定を変更するときにクリックします。
(☛P3-17)

[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。
(☛P3-24)

[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。
(☛P3-30)

[カスタム設定]
DHCP サーバ設定やネットワーク接続、セキュリティの設定、ログインパスワードの変更、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。

お知らせ

- 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。
- 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。
- 本商品を再起動（☛P3-41）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。［最新バージョンのダウンロード］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、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。」と表示される場合は、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。

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を起動し、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。

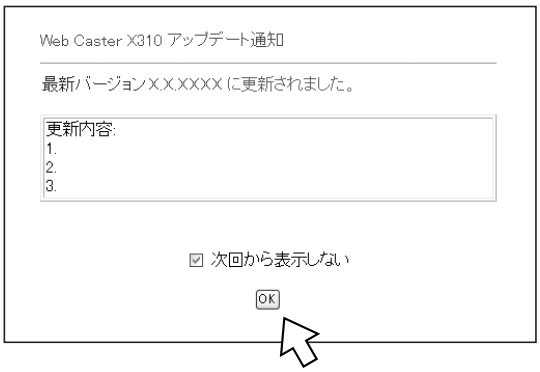
3 ログインパスワードを入力し、［OK］をクリックする。

ログインパスワードには、かんたん設定（☛P2-39）の手順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」（☛P3-23）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。

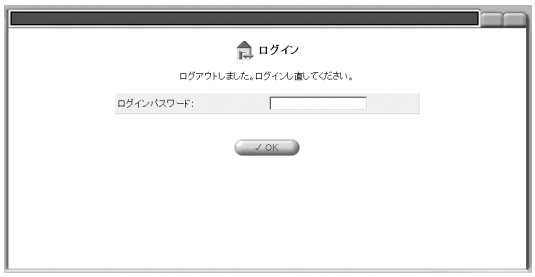
Web 設定画面について

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。

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。

ネットワークの設定を確認するには

LAN、WANの接続状態を確認します。

1 Webブラウザを起動して、Web設定画面を開く。(☛P3-3)

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 ネットワーク接続の画面で、接続状態を確認する。

[PPPoEセッション最大接続数]:
PPPoEの接続数を設定します。お買い求め後、かんたん設定でプロバイダの設定をした場合は、「2」と表示されています。

[LAN Ethernet]:
LAN側の接続状態です。

[WAN PPPoE 1]:
接続先1のフレッツ・スクウェアの接続状態です。

[WAN PPPoE 2]:
接続先2のプロバイダの接続状態です。

※マルチセッションの詳細は、「複数の接続先を使い分けるには(マルチセッション)」を参照してください。(☛P3-14)

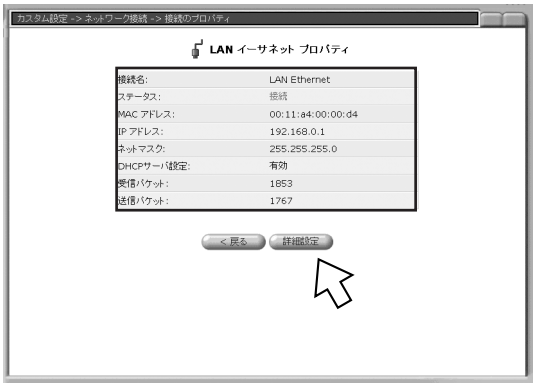
5 [戻る]をクリックする。

カスタム設定のトップ画面に戻ります。

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。

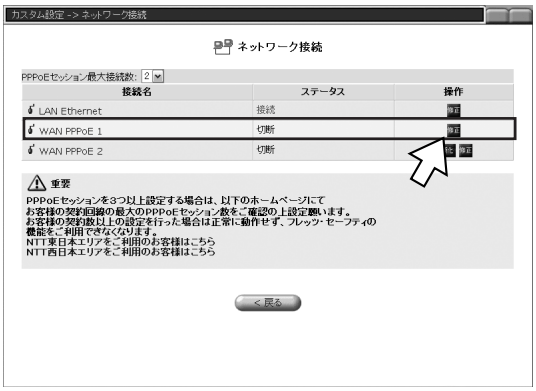
4 [OK]をクリックする。

ネットワークの設定を確認するには

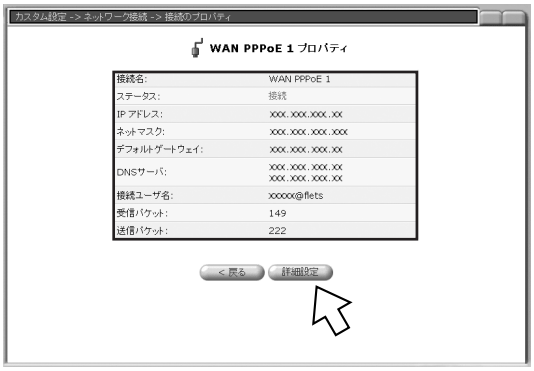
WAN PPPoE 1 の設定を確認／変更する

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（☛P3-22）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 2の設定を確認／変更する

インターネット接続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 [WAN PPPoE 2] の［修正］をクリックする。

2 [WAN PPPoE 2 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。

（次ページへ続きます）

ネットワークの設定を確認するには

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 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。

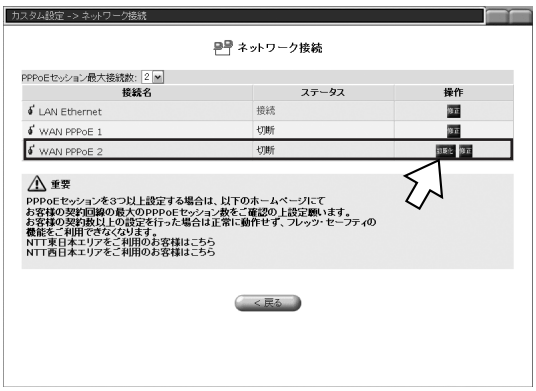
4 [OK] をクリックする。

5 [有効] をクリックする。

WAN PPPoE 2 の設定を初期化する

インターネット接続の設定を初期化することができます。

1 [WAN PPPoE 2] の [初期化] をクリックする。



2 [OK] をクリックする。

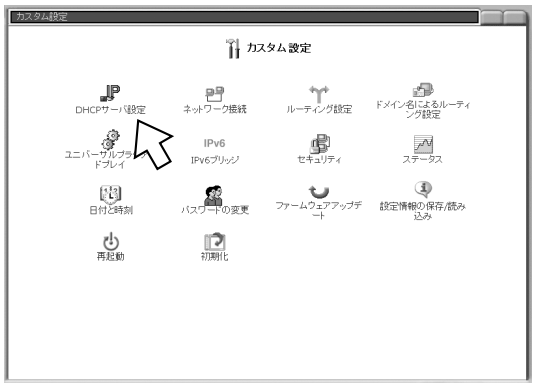
DHCP サーバの設定を変更するには

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 サーバ設定（LAN イーサネット）で、LAN 側の IP アドレスを変更することができます。

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P3-3）

2 [カスタム設定] をクリックする。

3 [DHCP サーバ設定] をクリックする。



4 [修正] をクリックする。

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。

5 [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。

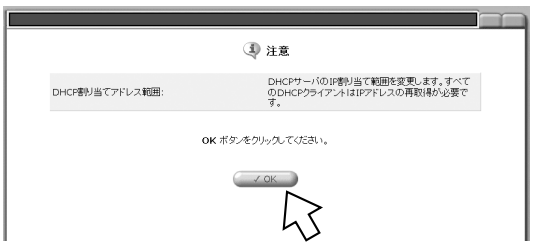
[WINS サーバ IP アドレス] ：
WINS サーバの IP アドレスを入力します。

[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。

6 [OK] をクリックする。

7 [OK] をクリックする。



お知らせ

- 手順 7 で「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 2 から再度設定し直してください。
- 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。

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。（☛P3-3）

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）］：
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。

フレッツ・セーフティの設定を変更するには

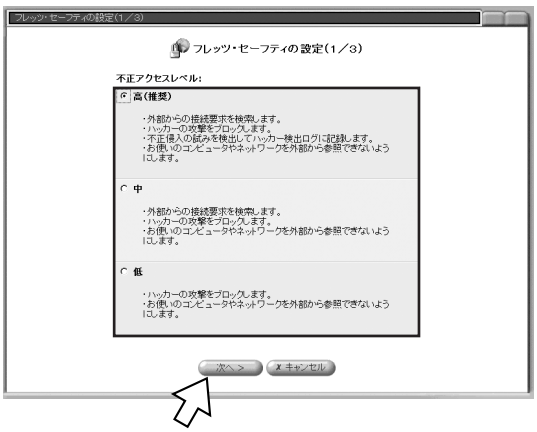
フレッツ・セーフティの設定を変更することができます。

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。（☛P3-3）

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。

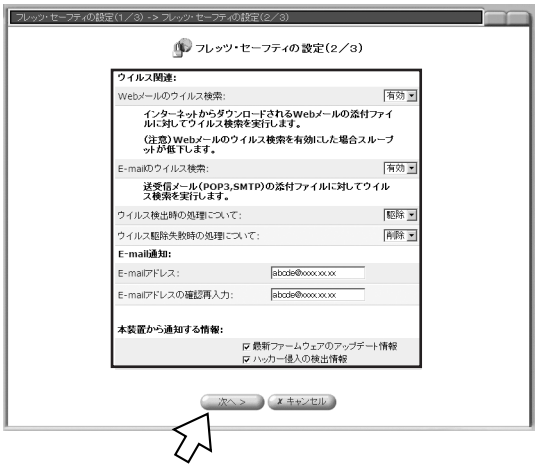
お知らせ

- 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。

（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 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：何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。

削除：感染したファイルを削除する（お買い求め時の設定）
放置：何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）

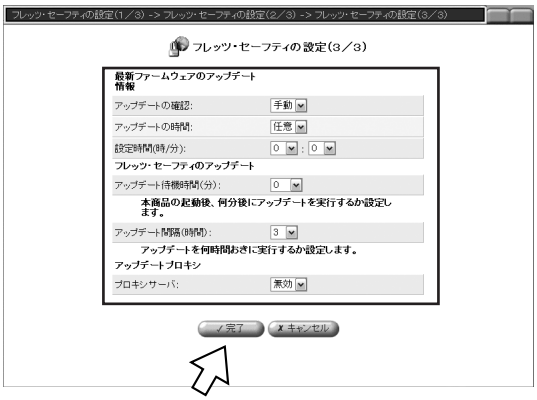
［ハッカー侵入の検出情報］：

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@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。

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（☛P3-22）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。

フレッツ・セーフティの設定を変更するには

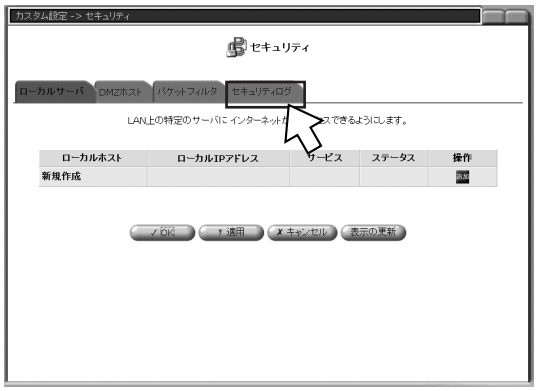
ウイルスや不正アクセスが検出されたとき

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。

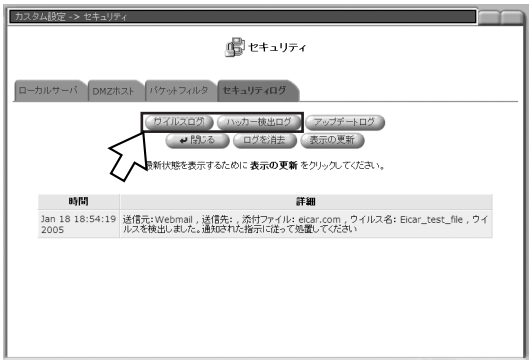
2 ［セキュリティ］をクリックする。

3 ［セキュリティログ］をクリックする。



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）

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。（☛P3-19）

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。（☛P3-19）

「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。（「本商品のファームウェアをローカルファイルからアップデートするには」（☛P3-33））

お知らせ

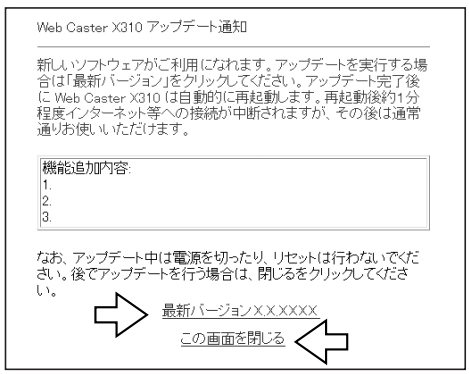
- フレッツ・セーフティにご契約いただいていないお客様は、本商品のウイルスパターン、検索エンジン、ファイアウォールルールの更新はできません。
- ホームページの閲覧中、メールの送受信中、ストリーミング再生やダウンロードなどを実行しているときにファームウェアおよびセキュリティ対策ファイルのアップデートが実行されると、接続が切断されることがあります。
- セキュリティ対策ファイルのアップデート中にネットワークケーブルを抜いた場合、ランプの点滅が継続して表示されることがあります。ランプが長時間に渡って点滅している場合は、本商品を再起動してください。
- 検索エンジンやファイアウォールルールがアップデートされた場合、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。

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（☛P3-3）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。「対象ファイルを手動アップデートするには」の手順６へ進んでください。（☛P3-32）
・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（☛P3-3）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（☛P3-3）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。（☛P3-2）

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。
●お客様のご利用状態などによって、正常にアップデートできない場合があります。

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。(☛P3-3)

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

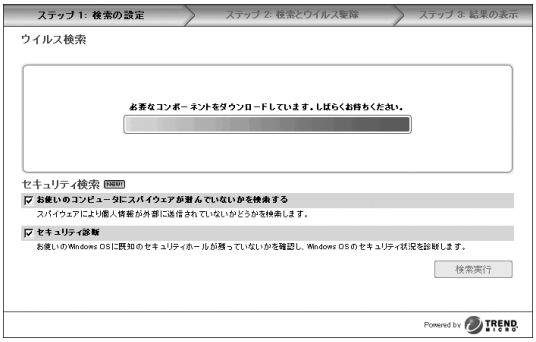
- オンラインウイルス検索を実行するには、下記の条件を満たすパソコンが必要です。
  - ・OS：Windows® XP/Me/98SE/98、Windows® 2000 Professional
  - ・ソフトウェア：Internet Explorer 5.5 サービスパック２以降
  - ・CPU：386 DX（486 DX 以上推奨）
  - ・RAM：4MB（8 MB 以上推奨）
  - ・ハードディスク：10 MB 以上のディスク空き容量

  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。(☛P2-45)
- 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。

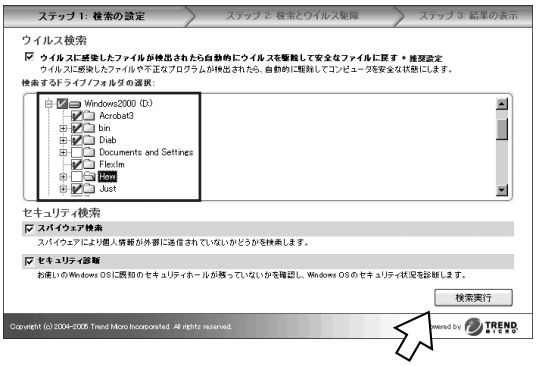
オンラインウイルス検索を行うために必要なコンポーネントをダウンロードします。ダウンロードが始まると右のような画面が表示されます。

※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。



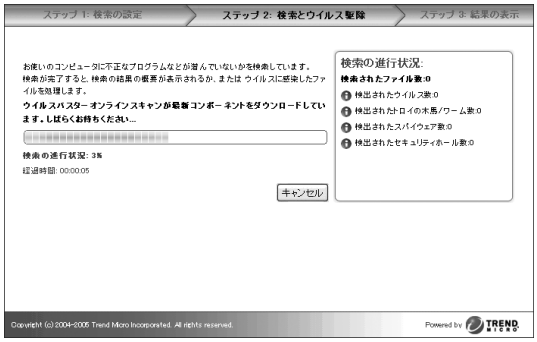
4 ウイルス検索を行うドライブまたはフォルダをチェックし、［検索実行］をクリックする。

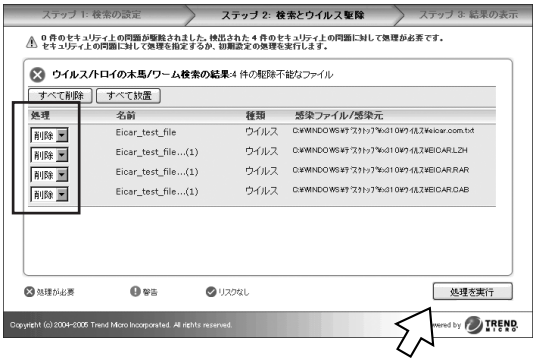
はじめてオンラインウイルス検索を行う場合は、ウイルスの検出に時間がかかることがあります。

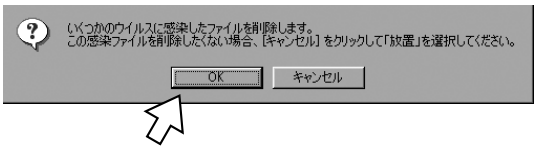


（次ページへ続きます）

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。

ユニバーサルプラグアンドプレイを利用するには

ユニバーサルプラグアンドプレイ（UPnP 機能）に対応しているアプリケーションやネットワークゲームをするには、ユニバーサルプラグアンドプレイを有効にする必要があります。

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P3-3）

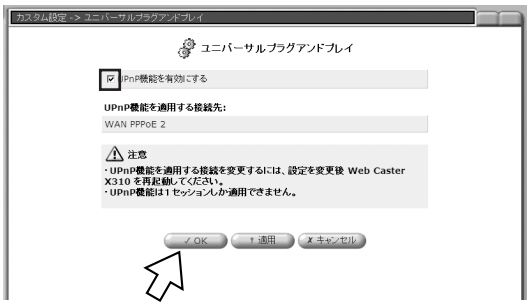
2 ［カスタム設定］をクリックする。

3 ［ユニバーサルプラグアンドプレイ］をクリックする。

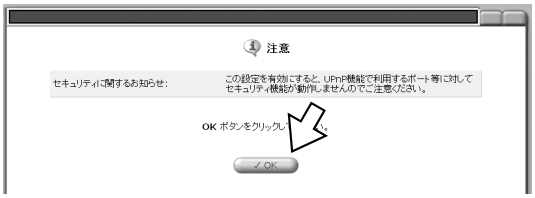
4 ［UPnP 機能を有効にする］をチェックし、［OK］をクリックする。

接続先を追加している場合は、UPnP 機能を適用する接続先を選択してください。
UPnP 機能を適用できる接続先は 1 つのみです。

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



5 ［OK］をクリックする。



お知らせ

- Windows ® 2000 /98 Second Edition/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。

IPv6 サービスに対応するには

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。

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P3-3）

2 [カスタム設定] をクリックする。

3 [IPv6 ブリッジ] をクリックする。

4 [IPv6 ブリッジを有効にする] をチェックし、[OK] をクリックする。

日時を設定するには

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、タイムサーバから日時を自動的に取得しないで、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。

1 Web ブラウザを起動して、Web 設定画面を開く。(☛P3-3)

2 [カスタム設定] をクリックする。

3 [日付と時刻] をクリックする。

4 **手動で設定する場合は、[日時自動取得] の [有効] のチェックを外し、[システム時間] に日付と時刻を入力する。**

自動で設定する場合は、[日時自動取得] の [有効] をチェックし、[時間の取得] をクリックすると、最新の日付と時刻に更新されます。

5 [OK] をクリックする。

対象ファイルを手動アップデートするには

Web 設定画面のホーム画面で、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、手動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。（☛P3-3）

2 ホーム画面の［最新情報の取得］をクリックする。

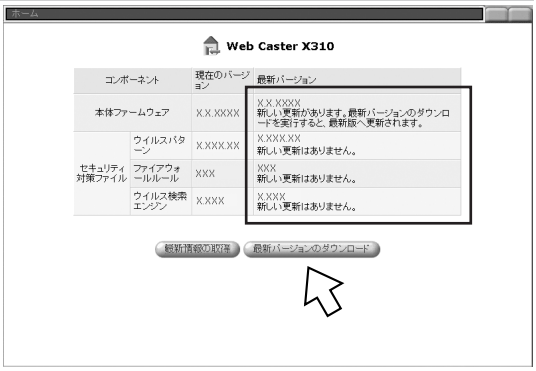
バージョン情報が更新されます。

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。

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。

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。

（次ページへ続きます）

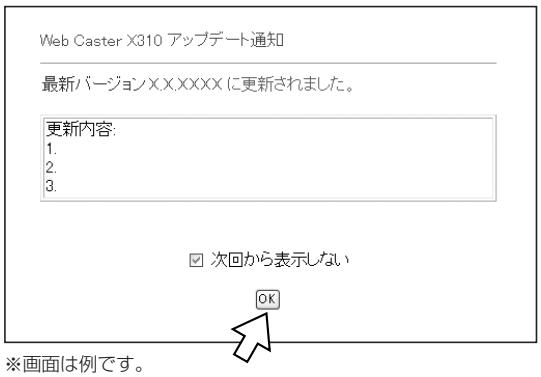
対象ファイルを手動アップデートするには

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。(☛P3-3)

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。

本商品のファームウェアをローカルファイルからアップデートするには

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/

ローカルファイルからアップデートする

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。（☛P3-3）

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。

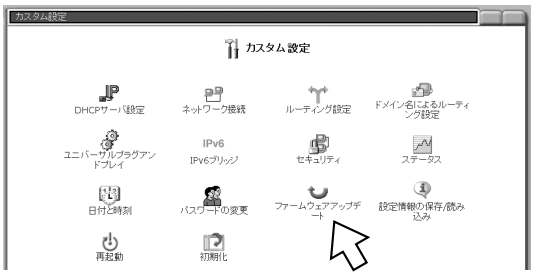
お知らせ

- 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、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）

本商品のファームウェアをローカルファイルからアップデートするには

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。

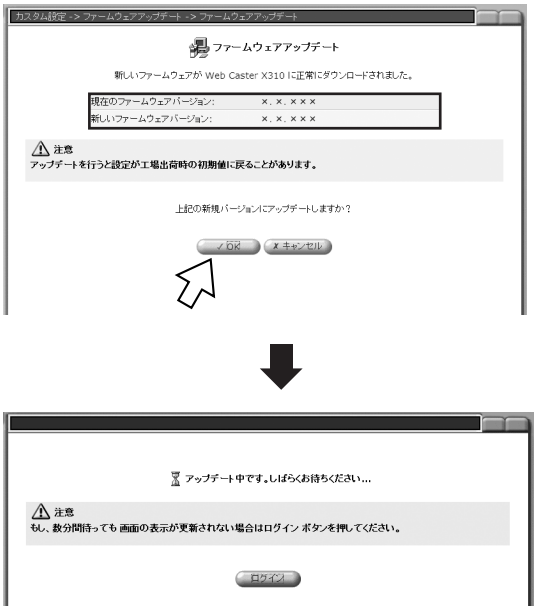
ファームウェアのアップデートの準備が開始されます。

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。

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。（☛P3-3）

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。

設定情報を保存するには

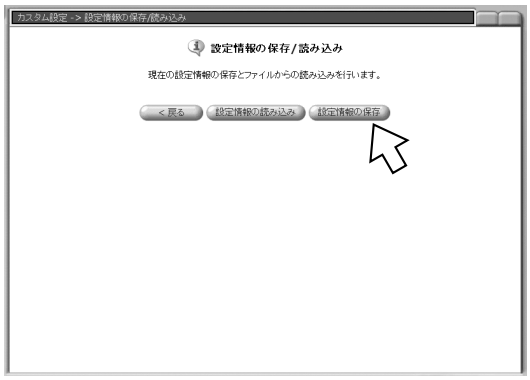
本商品の設定情報ファイルをパソコンに保存します。
画面は Windows® XP の例です。

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P3-3）

2 [カスタム設定] をクリックする。

3 [設定情報の保存／読み込み] をクリックする。

4 [設定情報の保存] をクリックする。



5 [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。

6 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。

保存した設定情報を読み込むには

パソコンに保存した設定情報を読み込みます。
画面は Windows® XP の例です。

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P3-3）

2 [カスタム設定] をクリックする。

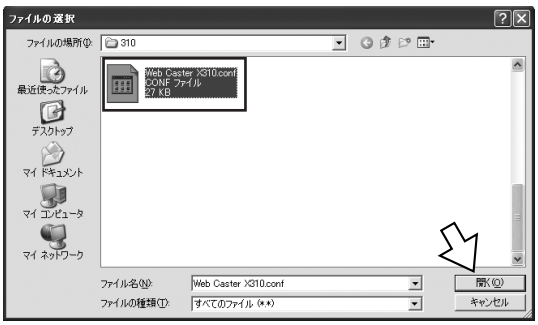
3 [設定情報の保存／読み込み] をクリックする。

4 [設定情報の読み込み] をクリックする。

5 ［参照］をクリックする。

6 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。



7 ［OK］をクリックする。

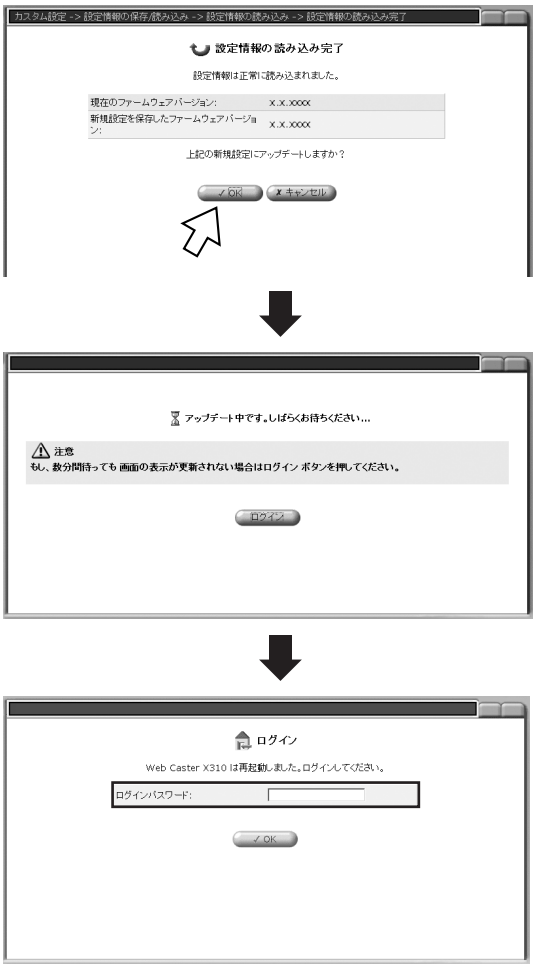
設定情報ファイルの読み込みが開始されます。

（次ページへ続きます）

保存した設定情報を読み込むには

8 [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

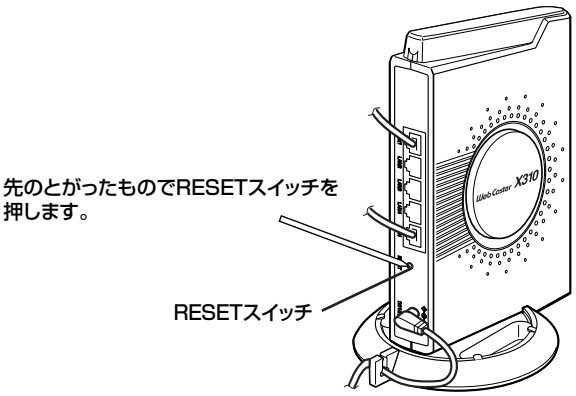
- アップデートが完了するまで本商品の電源アダプタは絶対に抜かないでください。

本商品を再起動するには

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。

RESET スイッチを使って再起動する

1 先のとがったもので背面にある RESET スイッチを押す。



Web 設定画面から再起動する

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P3-3）

2 [カスタム設定] をクリックする。

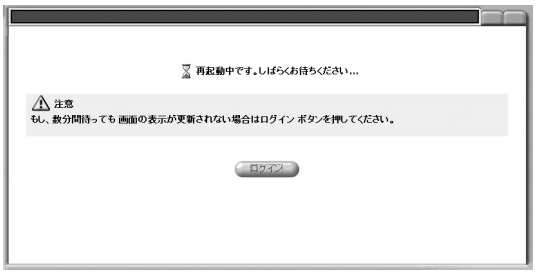
（次ページへ続きます）

本商品を再起動するには

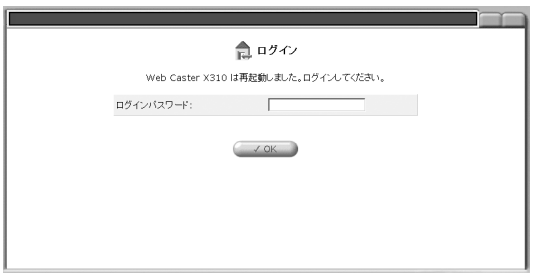
3 [再起動] をクリックする。

4 [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。



4 フレッツ・セーフティ対応機器の変更／廃止

NTT 東日本をご利用のお客様

ここでは、フレッツ・セーフティをご利用のお客様がフレッツ・セーフティ対応機器を変更する方法、およびフレッツ・セーフティを廃止する方法について説明します。

フレッツ・セーフティ対応機器を変更する

フレッツ・セーフティ対応機器を変更した場合は、以下の手順で登録機器の変更を行います。
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。

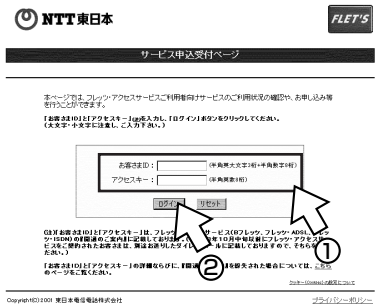
1 Web 設定画面で［オンライン登録］をクリックする。

サービス申込受付ページが表示されます。

2 お客様 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。

お客様 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

● **手順２で「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。

3 [登録機器変更申し込み] をクリックする。

「フレッツ・セーフティ登録機器変更申込者情報入力」画面が表示されます。

4 変更される方の情報を入力し、[次へ] をクリックする。

「フレッツ・セーフティ登録機器変更内容確認」画面が表示されます。

5 変更内容を確認し、[変更] をクリックする。

「フレッツ・セーフティ登録機器変更受付完了」画面が表示されます。

修正する場合は、[前画面へ戻る] をクリックし、入力し直します。

（次ページへ続きます）

NTT 東日本をご利用のお客様

6 変更内容を確認し、［閉じる］をクリックする。

これで登録機器の変更は完了です。
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。

フレッツ・セーフティを廃止する

フレッツ・セーフティを廃止する場合は、以下の手順に従って廃止操作を行います。
この操作を行わずに、116番にご連絡いただいてフレッツ・セーフティを廃止することもできます。

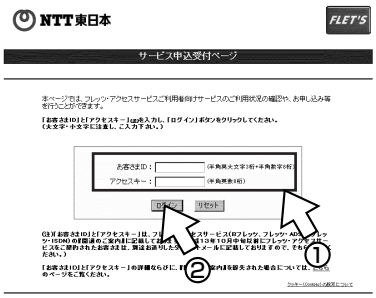
1 Web設定画面で［オンライン登録］をクリックする。

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。



3 ［廃止申し込み］をクリックする。

「フレッツ・セーフティ廃止申込者情報入力」画面が表示されます。

ワンポイント

●**手順2で「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

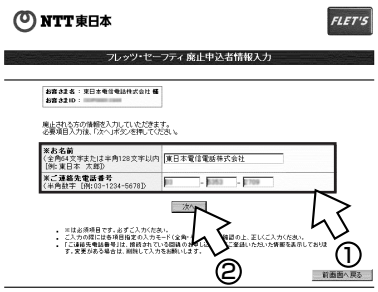
●NTT東日本のお客様で、手順2で「接続中のフレッツ・セーフティ対応機器は既に他の回線でご登録中です」と表示された場合は、「フレッツ・セーフティに関するお問い合わせ（03-5442-7533）」へご連絡ください。NTT西日本のお客様は、お問い合わせいただいてもご回答できません。

（次ページへ続きます）

NTT 東日本をご利用のお客様

4 廃止される方の情報を入力し、［次へ］をクリックする。

「フレッツ・セーフティご利用終了日選択」画面が表示されます。

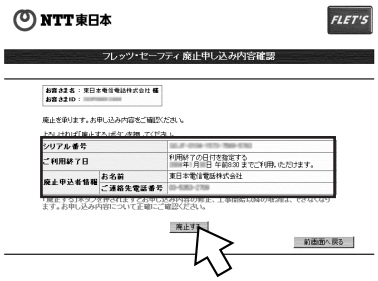


5 ご利用終了日を選択し、［次へ］をクリックする。

「フレッツ・セーフティ廃止申し込み内容確認」画面が表示されます。

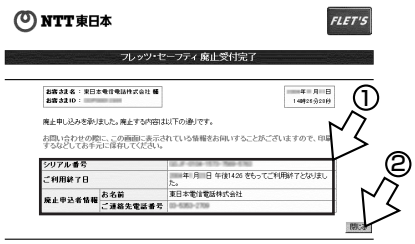
6 内容を確認し、［廃止する］をクリックする。

「フレッツ・セーフティ廃止受付完了」画面が表示されます。



7 内容を確認し、［閉じる］をクリックする。

これでフレッツ・セーフティの廃止は完了です。



お知らせ

- 本商品を利用せずにフレッツ・セーフティを廃止する場合は、回線終端装置または ADSL モデムとパソコンを直接接続し、フレッツ・スクウェアに接続してください。本商品を接続しないでフレッツ・スクウェアに接続する方法は、フレッツ・ADSL または B フレッツ申し込み時に送付された「フレッツ接続ツール（セットアップガイド・付属の CD-ROM）」を参照してください。

NTT 西日本をご利用のお客様

ここでは、フレッツ・セーフティをご利用のお客様がフレッツ・セーフティ対応機器を変更する方法、およびフレッツ・セーフティを廃止する方法について説明します。
なお、フレッツ・セーフティ対応機器を変更するには、事前に 116 番等へお申し出いただく必要があります。

フレッツ・セーフティ対応機器を変更する

フレッツ・セーフティ対応機器を変更した場合は、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。
以下の手順で登録機器の変更を行ってください。

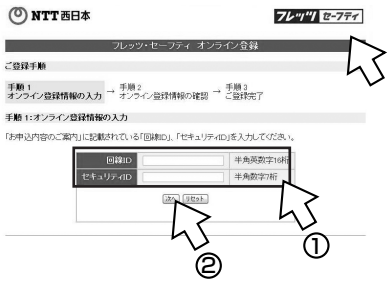
1 Web 設定画面で［オンライン登録］をクリックする。

「フレッツ・セーフティ　オンライン登録　手順 1」画面が表示されます。

2 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　セキュリティ機器登録　手順 2」画面が表示されます。

回線 ID とセキュリティ ID は、フレッツ・セーフティ対応機器変更のお申し込み後に 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

● **手順 2 で「お申込内容のご案内」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「お申込内容のご案内」を送付させていただきます。

お知らせ

●新規にお申し込みいただいた際のセキュリティ ID はご利用いただけません。

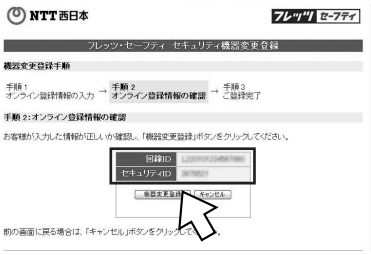
（次ページへ続きます）

NTT 西日本をご利用のお客様

3 手順２で入力した回線 ID とセキュリティ ID を確認し、［機器変更登録］をクリックする。

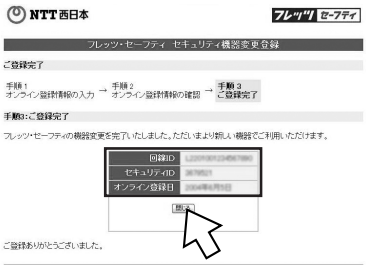
「フレッツ・セーフティ　オンライン登録　手順３」画面が表示されます。

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。



4 変更内容を確認し、［閉じる］をクリックする。

これで登録機器の変更は完了です。
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。



フレッツ・セーフティを廃止する

フレッツ・セーフティを廃止する場合は、局番なしの 116 番等へご連絡ください。
※ Web 設定画面（かんたん設定）からは廃止できません。

ご利用になるエリアを変更される場合

お引越しなどで、本商品をご利用になるエリアがNTT東日本エリアからNTT西日本エリアへ、またはNTT西日本エリアからNTT東日本エリアへ変更される場合は、下記のような手順が必要です。

1 お引越し前のエリアでフレッツ・セーフティを廃止する。

お引越し前がNTT東日本エリアの場合（☛P4-5）
お引越し前がNTT西日本エリアの場合（☛P4-8）

2 お引越し先のエリアでフレッツ・セーフティをオンライン登録する。

お引越し先でフレッツ・セーフティをご利用になるには、新たにお申し込みいただく必要があります。
お引越し先がNTT東日本エリアの場合（☛P2-45）
お引越し先がNTT西日本エリアの場合（☛P2-52）

5 こんなときは

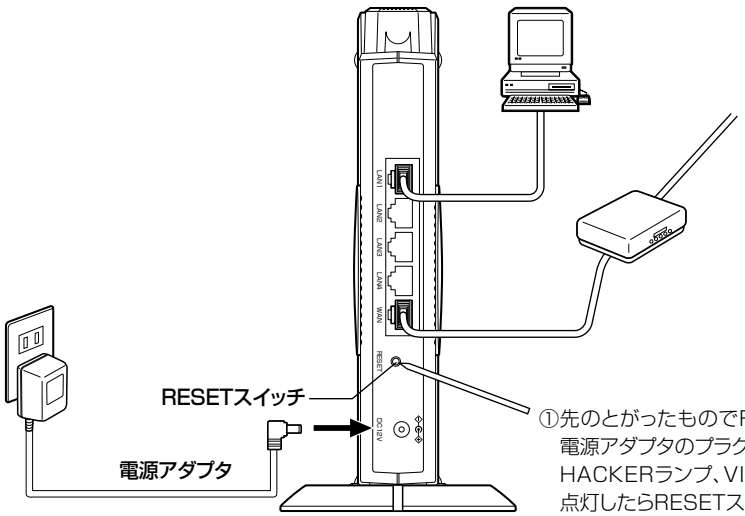
お買い求め時の設定に戻すには

本商品の設定情報、ネットワーク接続情報を初期化して、お買い求め時の状態に戻すことができます。
初期化には、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。
初期化を行うと、本商品のすべての設定情報、ネットワーク情報、および各種ログ情報が消去されますのでご注意ください。

RESETスイッチを使って初期化する

1 本商品から電源アダプタのプラグを抜く。

2 先のとがったもので背面にある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む。



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。

③HACKER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。

ワンポイント

● 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

- 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廃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。
- 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。

Web 設定画面から初期化する

1 Web ブラウザを起動して、Web 設定画面を開く。（☛P3-3）

2 ［カスタム設定］をクリックする。

3 ［初期化］をクリックする。

ワンポイント

● 設定が初期化される情報

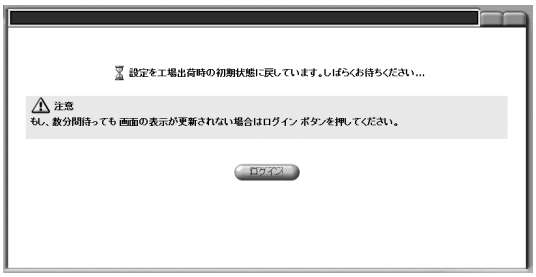
初期化を実行すると、すべての設定情報、ネットワーク情報、および各種ログ情報が消去されます。

（次ページへ続きます）

お買い求め時の設定に戻すには

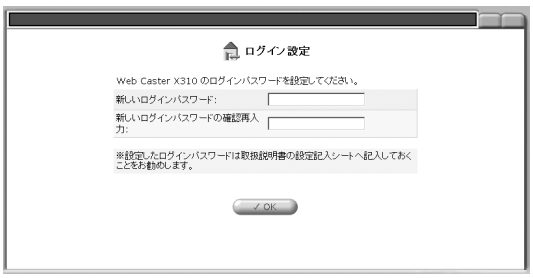
4 [実行する] をクリックする。

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。



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。(☛P3-3)
- 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廃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。
- 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。

困ったときのQ&A

トラブルが起きたときや疑問点があるときは、こちらをお読みください。
該当項目がない場合や、対処をしても問題が解決しない場合は、本商品を初期化して、初めから設定し直してください。
初期化を行うと本商品のすべての設定が消去されますのでご注意ください。初期化を行う場合は現在の設定内容を保存しておくことをお勧めします。初期化の方法については、「お買い求め時の設定に戻すには」（☛P5-2）を参照してください。

パソコンに関するトラブル

質　問	回　答
パソコンからインターネットへアクセスできない（WANランプが消灯している）	本商品と回線終端装置（ONU）、VDSLモデム、ADSLモデム等との接続構成、および接続しているLANケーブルの種類を確認してください。（☛P2-3～P2-5）
パソコンを接続したLANポートのLANランプが消灯している	①「回線を接続する」（☛P2-3～P2-5）を参照して、LANの接続を確認し、接続をやり直してください。 ② 接続に問題がなければ、LANカードが正しく動作しているか確認してください。なお、LANカードについてのトラブルは、パソコンあるいはLANカードのメーカにご相談ください。
ホームページを閲覧できない Web設定画面を開けない	パソコンのIPアドレスが正常に設定されていない場合、ホームページを閲覧したり、Web設定画面を開くことができません。このときは、パソコンの設定を確認してください。それでも復旧しない場合は、パソコンを再起動してください。

ウイルス検出／不正アクセス検出に関するトラブル

質　問	回　答
Webメールとして、MSN Explorerを使用している場合、Webメールの添付ファイルからウイルスを検索することができますか？	MSN Explorerをご使用の場合、本商品でWebメールの添付ファイルを検索することはできません。これは、MSN ExplorerではWebメールの受信に異なるプロトコルを使用しているためです。Microsoft Internet Explorerのご使用をお勧めします。
Microsoft Internet Explorerにウイルス駆除できなかったWebメールの添付ファイルやファイルサイズが4 MB以上の添付ファイルを送信または保存するにはどうしたらよいですか？	ウイルス駆除できなかったWebメールの添付ファイルや4 MB以上のWebメールの添付ファイルを送信または保存するには、本商品のWebメールのウイルス検索機能を無効にする必要があります。ただし、Webメールのウイルス検索を無効にすると、Webメールの添付ファイルに対してウイルス検索が実行されません。 また、Webメールが有効になっているときに、添付ファイルを右クリックし［別名で保存］を選択しても保存できませんので、ご注意ください。 （1 MBは1,000,000 Bで計算しています）
Microsoft Outlook Express、およびOffice OutlookでHotmailメッセージを受信するように設定している場合、本商品ではHotmailの添付ファイルに対してウイルス検索を実行できますか？	できません。Microsoft Outlook Express、およびOffice OutlookでHotmailを受信するように設定している場合、本商品ではそのHotmailに対してウイルス検索を実行することができません。Hotmailの添付ファイルに対してウイルス検索が実行されていないことも通知されません。これはMicrosoft Outlook Expressでは、Hotmailメッセージの受信に異なるポートを使用しているためです。ウイルスに感染しないようにするためにも、Hotmailの受信にはWebブラウザをお使いいただくことをお勧めします。
POP3、SMTP、HTTPは通常、ポート番号110、25、80にそれぞれ割り当てられています。このプロトコルに別のポートを割り当てた場合、本商品では送受信E-mailおよびWebメールに対してウイルス検索を実行することはできますか？	できません。POP3、SMTP、HTTPに別のポートを割り当てた場合、本商品では送受信E-mailおよびWebメールに対してウイルス検索を実行することができなくなります。また、送受信E-mailおよびWebメールに対してウイルス検索が実行されていないことも通知されません。

困ったときのQ&A

質　問	回　答
ウイルスに感染したファイルをダウンロードしようとした場合、本商品はこのウイルスを発見してくれるのでしょうか？	ダウンロードするファイルに対して、リアルタイムでウイルス検索は実行しません。 ダウンロード後、オンラインウイルス検索機能でチェックすることが可能です。
ウイルス検索の対象は何ですか？	ウイルス検索の対象は、送信メール（SMTP）と受信メール（POP3）およびWebメールの添付ファイルとなります。 対応しているWebメールは、Yahoo!メール、Hotmail、AOLメールのみです。
メールのウイルス検索の制限はありますか？	ハードウェア的な制限から次の４つの制限があります。 ・メール本体と添付ファイルの合計サイズが４ MB以上のメール（圧縮ファイルの場合は解凍後のサイズ、また添付ファイルが複数の場合はその合計サイズ） ・暗号化されたメール ・パスワード付きの圧縮ファイル ・３階層以上圧縮されたファイル この制限を超えたメールを処理した場合は、ウイルス検索が実行されていない旨の通知がメールに添付されます。 （1 MBは1,000,000 Bで計算しています）
メールの添付ファイルのエンコード形式は何をサポートしていますか？	エンコード形式としては、次の形式をサポートしています。 ・ Quoted Printable ・ base64 ・ Unencode ・ 7-bit ・ 8-bit ・ binary TNEF ・ Plain Text
オンラインウイルス検索はどうやって行うのですか？	オンラインウイルス検索をお使いになる場合、Web設定画面から起動します。 Web設定画面、左下の［オンラインウイルス検索］をクリックすると使い方が表示されます。 内容をよく読んだうえで、Webブラウザ内で検索対象を選択してください。 ［自動駆除］チェックボックスをオンにしてください。 ［検索］をクリックしてください。検索が始まります。 ＜動作制限事項＞ ・オンラインウイルス検索は、Windows® 98/98SE/Me/2000/XP上で動作します。それ以外のOSでは動作しません。 ・オンラインウイルス検索を実行するには、Microsoft Internet Explorer 5.5（サービスパック２）以降、またはNetscape Navigator® ６以降が必要です。 ・Internet ExplorerのActiveXコントロールは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。

質　問	回　答
オンラインウイルス検索の一部の機能が利用できません	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。(☛P2-45)
本商品を導入すればウイルスバスター等のウイルス対策ソフトは不要になりますか？	本商品は、メールのウイルス検索とファイアウォール機能を持っていますが、ウイルスの検出には制限があるため、ウイルス対策ソフトとの併用をお勧めします。 ウイルス対策ソフトと併用していただいても問題はありません。ただし、ウイルス対策ソフトのパーソナルファイアウォールなどの機能については無効にしていただくことをお勧めします。
Web 閲覧時にもウイルス検索を行いますか？	本商品は、Web 閲覧時などの HTTP 経由、FTP 経由でのウイルスに関しては検出を行いません。 しかし、本商品のオンラインウイルス検索を利用することでダウンロードしたファイルのウイルス検出、駆除が可能となります。また、リアルタイムで感染を防止する場合はパソコンにインストールするタイプのウイルス対策ソフトを導入し、二重にセキュリティ対策を行ってください。
ウイルスに感染したパソコンのウイルス駆除はできますか？	本商品は、ウイルスに感染したパソコンのウイルス駆除はできません。感染後の駆除については、ウイルス対策ソフトを導入してください。
通知されたメールの内容が文字化けしているのですが？	本商品から通知されるメールのエンコード方式は、JIS コードです。 お使いのメールソフトによっては、エンコード方式を JIS コードに設定していただく必要があります。
ファイル名が半角英数字以外の添付ファイルもウイルス検索の対象ですか？	対象です。 ただし、メール通知内容に記載されたファイル名は文字化けすることがあります。
セキュリティ対策ファイルがアップデートしないのですが？	ご利用の環境やネットワークの環境等によっては、正常にアップデートできないことがあります。 このときは、手動でアップデートしてください。(☛ P 3-30)

その他のトラブル

質　問	回　答
電源が入らない	電源アダプタがコンセントから抜けていないか確認してください。
ALARM ランプが点灯している	本商品で異常が発生しています。電源を入れ直してください。
PPPoE ランプが消えている	オフライン状態になっています。接続の設定を確認してください。

6 ご参考に

CD-ROMの「詳細取扱説明書」について

以下の項目については、付属のCD-ROMの「詳細取扱説明書」（PDFファイル）をご覧ください。

1 Web設定

かんたん設定やカスタム設定など、Web設定画面で設定する項目の説明を記載しています。

2 こんなときにはこの設定

IP電話対応のADSLモデムと本商品を接続してご利用になる場合の代表的な設定方法と、音声／ビデオチャットなどのツールを利用する場合などの設定方法を説明しています。

3 付録

取扱説明書、詳細取扱説明書で使われている用語の解説を記載しています。

設定記入シート

保守のための資料として、かんたん設定などの設定内容を記入し、大切に保管してください。
プロバイダの認証パスワードは、お客様の個人情報となります。記入された際は、お取り扱いにご注意ください。

項目			設定記入欄
パスワード			[　　]
エリア選択			□NTT 東日本エリア □NTT 西日本エリア
接続方法			□PPPoE を使用して接続する場合 □PPPoE を使用しないで接続する場合
接続先情報（PPPoE を使用して接続する場合）	接続先 1		フレッツ・スクウェア（固定） 接続ユーザ名 □NTT 東日本［guest@flets］ □NTT 西日本［flets@flets］ 接続パスワード □NTT 東日本［guest］ □NTT 西日本［flets］
	接続先 2		プロバイダ名［　　］ 接続ユーザ名［　　］ 接続パスワード［　　］
	接続先 3		プロバイダ名［　　］ 接続ユーザ名［　　］ 接続パスワード［　　］
	接続先 4		プロバイダ名［　　］ 接続ユーザ名［　　］ 接続パスワード［　　］
	接続先 5		プロバイダ名［　　］ 接続ユーザ名［　　］ 接続パスワード［　　］
フレッツ・セーフティの設定	不正アクセスレベル		□高（推奨）□中　□低
	ウイルス関連	Web メールのウイルス検索	□有効　□無効
		E-mail のウイルス検索	□有効　□無効
		ウイルス検出時の処理について	□駆除　□削除　□放置
		ウイルス駆除失敗時の処理について	□削除　□放置
	E-mail 通知	E-mail アドレス	[　　]
	本装置から通知する情報		□最新ファームウェアのアップデート情報 □ハッカー侵入の検出情報
	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	□自動　□手動
		アップデートの時間	□固定（AM4 ： 00～5 ： 00） □任意　時間［　］（0～23 時） 分［　］（0、10、20、30、40、50 分）
	フレッツ・セーフティのアップデート	アップデート待機時間	□0 分□15 分□30 分□60 分□120 分
		アップデート間隔	□1 時間　□3 時間　□6 時間 □12 時間 □24 時間
DHCP サーバ設定（LAN イーサネット）			□有効　□無効
IP アドレス（LAN イーサネット）			[　　]
割り当て開始、割り当て終了 IP アドレス			[　　] ～ [　　]
ユニバーサルプラグアンドプレイ（UPnP 機能）			□有効　□無効
IPv6 ブリッジ			□有効　□無効
日付と時刻	日時自動取得		□有効　□無効

初期設定内容一覧

かんたん設定等における初期設定値は、下表のとおりです。

項目			初期設定
DHCP サーバ設定（LAN イーサネット）			有効
			192.168.0.11 ～ 192.168.0.99 ネットマスク：255.255.255.0
IP アドレス（LAN イーサネット）			192.168.0.1 ネットマスク：255.255.255.0
接続先の設定 （PPPoE を使用して接続する場合）	接続先 1		フレッツ・スクウェア（固定） 接続ユーザ名 ・NTT 東日本［guest@flets］ ・NTT 西日本［flets@flets］ 接続パスワード ・NTT 東日本［guest］ ・NTT 西日本［flets］
フレッツ・セーフティの設定	不正アクセスレベル		高（推奨）
	ウイルス関連	Web メールのウイルス検索	有効
		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
	E-mail 通知	E-mail アドレス	未設定
	本装置から通知する情報		なし
ユニバーサルプラグアンドプレイ（UPnP 機能）			無効
IPv6 ブリッジ			無効
日付と時刻	日時自動取得		有効

メール通知内容一覧

本商品をご利用のお客様に以下の内容をメールでお知らせします。

項目	タイトル	本文
未登録ユーザへの通知	Web Caster X310通知メール	Web Caster X310 ご利用のお客さま： お客さまのWeb Caster X310 はオンライン登録が完了していないため、製品のアップデート機能をお使いいただけません。 Web Caster X310 のアップデート機能をお使いいただくためには、フレッツ・セーフティのオンライン登録を行っていただく必要があります。 ●オンライン登録を実行するには、次の手順に従ってください。 1．ブラウザを開いて、アドレスバーから http://wbc_x310/ にアクセスしてください。 2．サイドバーから「オンライン登録」をクリックしてください。 ＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊ このE-mailは、Web Caster X310 プログラムより自動送信されています。 Web Caster X310 に関する最新情報は、サイドバーから「サポート情報」をクリックしてください。 ＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
ハッカー検知時通知メール	ハッカーによる侵入試行が検出されました	Web Caster X310 により、お客さまのシステムに対する侵入試行が検出されました： ＊＊日付：XXXX/XX/XX 10:24:05 ＊＊アクセス元：XX.XXX.XX.X ＊＊攻撃方法：MS SQL Server worm 最新のハッカー検出ログについては、Web Caster X310 のハッカー検出ログページを参照してください。 ハッカー検出ログを表示するには、Web Caster X310 設定コンソールのサイドバーから［カスタム設定］→［セキュリティ］→［セキュリティログ］→［ハッカー検出ログ］の順にクリックしてください。 注意：　このE-mailはハッカーによる侵入の試みがあったことをお知らせするためにお送りしています。 Web Caster X310 の不正アクセス対策機能が有効に設定されていれば、改めて対策を講じる必要はありません。
ソフトウェアアップデート通知	ソフトウェアのアップデートについて	Web Caster X310 ユーザのみなさま、 弊社ではこのたび、Web Caster X310 のソフトウェアアップデートモジュールをリリースいたしました。 より万全なウイルス対策およびハッカーの不正侵入対策のために、新しいアップデートファイルを早急にダウンロードしてお使いいただくことをお勧めします。 Web Caster X310 をアップデートするには次の手順に従ってください。 1．Webブラウザを開いて、アドレスバーから http://wbc_x310/ にアクセスしてください。 2．サイドバーから［ホーム］をクリックしてください。 3．［最新バージョンのダウンロード］ボタンをクリックすると、Web Caster X310 の最新プログラムが自動的にダウンロードされアップデートが行われます。 今後とも Web Caster X310 をご愛顧のほどよろしくお願い申し上げます。
ファイル削除（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX Web Caster X310ではXXXX_XXXX_VIRUS を添付ファイル「XXXX_XXX_XXX.exe 」から検出しました。添付ファイルは削除されました。 オリジナルのメール本文はこの通知メールに添付されています。
駆除不可能、感染ファイル削除（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX Web Caster X310ではXXXX_XXXX_VIRUS を添付ファイル「XXXX_XXX_XXX.exe 」から検出しました。ウイルス駆除できないため、感染したファイルは削除されました。 オリジナルのメール本文はこの通知メールに添付されています。

お知らせ

●タイトルと本文は例です。
●お使いのパソコンのDNSサーバ設定が固定に設定されている場合、未登録ユーザへの通知メールに記載されたhttp://wbc_x310/が表示できないことがあります。

メール通知内容一覧

項目	タイトル	本文
駆除（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX Web Caster X310ではXXX_XXXX_VIRUS-C を添付ファイル「XXXX_XXX.COM」から検出しました。感染ファイルからウイルスが駆除されました。 オリジナルのメールの本文とウイルス駆除済みの添付ファイルは、この通知メールに添付されています。
放置（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX Web Caster X310ではXXXX_XXXX_VIRUS を添付ファイル「XXXX_XXX_XXX.exe 」から検出しました。Web Caster X310で感染ファイルを放置するよう設定されているため、感染ファイルには一切の処理が実行されていません。 感染ファイルは、この通知メールに添付されています。 ウイルスの感染被害の拡大を防止するためにも、添付された感染ファイルを削除してください。
駆除不可能、感染ファイル放置（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX Web Caster X310ではXXXX_XXXX_VIRUS を添付ファイル「XXXX_XXX_XXX.exe 」から検出しました。Web Caster X310でウイルス駆除できない感染ファイルを放置するよう設定されているため、感染ファイルには一切の処理が実行されていません。 感染ファイルは、この通知メールに添付されています。 ウイルスの感染被害の拡大を防止するためにも、添付された感染ファイルを削除してください。
感染数が多い（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX Web Caster X310ではXXXX_XXXX_VIRUS を添付ファイル「XXXX.doc 」から検出しました。感染ファイルからウイルスが駆除されました。 オリジナルのメールの本文とウイルス駆除済みの添付ファイルは、この通知メールに添付されています。 Web Caster X310ではXXXX_XXXX_VIRUS を添付ファイル「XXXX.doc 」から検出しました。感染ファイルからウイルスが駆除されました。 オリジナルのメールの本文とウイルス駆除済みの添付ファイルは、この通知メールに添付されています。 Web Caster X310では、感染しているウイルスの数が多いため、ファイル"XXXX.doc"からウイルスを駆除することができません。 いくつかのウイルスは駆除されましたが、まだウイルス感染している可能性があります。 誤って感染ファイルを開かないようご注意ください。
添付ファイルサイズ超え（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX 本メールの添付ファイルのウイルス検索ができませんでした。 ：4Madd1 添付ファイルのファイルサイズが大きすぎるため、ウイルスチェックを行っておりません。 メール送信者に添付ファイルの安全性を確認していただくか、お客様ご自身でOnLine Scan(オンラインウイルス検索)を実行していただいた上で、添付ファイルを開くことをお勧めします。
リソース不足（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX 本メールの添付ファイルのウイルス検索ができませんでした。 ：XXXX_XXXX_XXX.mdb 添付ファイルはウイルスチェックを行っておりません。 これはシステムのリソースが不足しているためです。 ファイルはこの通知メールに添付されています。 メールの送信者に添付ファイルの安全性を確認していただくか、お客様ご自身でOn Line Scan(オンラインウイルス検索)を実行していただいた上で、添付ファイルを開くことをお勧めします。
添付ファイルサイズ制限超え（ウイルス付き）（受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX Web Caster X310がウイルスを発見しました。XXXX_XXXX_VIRUSウイルスを発見した添付ファイル名：XXXX_XXXX_XXX.mdb ファイルサイズが大きいため、ウイルス駆除できませんでした。 ウイルスの感染被害の拡大を防止するためにも、添付された感染ファイルを削除してください。

項目	タイトル	本文
多重圧縮 （受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX 本メールの添付ファイルはウイルスチェックを行っておりません。 添付ファイルが複数回、圧縮されているためです。 メールの送信者に添付ファイルの安全性を確認していただくか、お客様ご自身でOn Line Scan(オンラインウイルス検索)を実行していただいた上で、添付ファイルを開くことをお勧めします。
PWD保護 （受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 オリジナルのメール送信元アドレス：XXX@XXX.XXX 本メールの添付ファイルのウイルス検索ができませんでした。 ：XXXX_XXX.COM 送信したメールの添付ファイルはウイルスチェックを行っておりません。 これは、ファイルがパスワード保護されているか、ファイルフォーマットがサポートされていないのが原因です。 お客様ご自身でOn Line Scan(オンラインウイルス検索)を実行していただいた上で、添付ファイルを開くことをお勧めします。
総メールサイズ 制限サイズ超 （受信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 このメールのファイルサイズがWeb Caster X310の制限サイズを超えているため、ウイルス検索できませんでした。 添付ファイルはウイルス感染の疑いがあります。 お客様ご自身でOn Line Scan(オンラインウイルス検索)を実行していただいた上で、添付ファイルを開くことをお勧めします。
ファイル削除 （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXXX_XXXX_VIRUS を添付ファイル「XXXX_XXX_XXX.exe 」（XXX@XXX.XXX 宛に2005/08/12 10:47 頃に送られたメール）から検出しました。Web Caster X310は、このメールを削除しました。 オリジナルのメールは、送信されませんでした。 ウイルスの感染被害の拡大を防止するためにも、送信メールに添付した感染ファイルを削除することをお勧めします。 誤って感染ファイルを開かないようご注意ください。
駆除不可能・感染ファイル削除 （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXXX_XXXX_VIRUS を添付ファイル「XXXX_XXX_XXX.exe 」（XXX@XXX.XXX 宛に2005/08/12 12:21 頃に送られたメール）から検出しました。Web Caster X310は、このメールを削除しました。 オリジナルのメールは、送信されませんでした。 ウイルスの感染被害の拡大を防止するためにも、送信メールに添付した感染ファイルを削除することをお勧めします。 誤って感染ファイルを開かないようご注意ください。
駆除（送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXX_XXXX_VIRUS-C を添付ファイル「XXXX_XXX.COM 」（XXX@XXX.XXX 宛に2005/08/12 12:22 頃に送られたメール）から検出しました。 Web Caster X310は、このメールを削除しました。 オリジナルのメールは、送信されませんでした。 ウイルスの感染被害の拡大を防止するためにも、送信メールに添付した感染ファイルを削除することをお勧めします。 誤って感染ファイルを開かないようご注意ください。
放置（送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXX_XXXX_VIRUS-C を添付ファイル「XXXX_XXX.COM 」（XXX@XXX.XXX 宛に2005/08/12 12:23 頃に送られたメール）から検出しました。 Web Caster X310は、このメールを削除しました。 オリジナルのメールは、送信されませんでした。 ウイルスの感染被害の拡大を防止するためにも、送信メールに添付した感染ファイルを削除することをお勧めします。 誤って感染ファイルを開かないようご注意ください。
駆除不可能・感染ファイル放置 （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXXX_XXXX_VIRUS を添付ファイル「XXXX_XXX_XXX.exe 」（XXX@XXX.XXX 宛に2005/08/12 12:24 頃に送られたメール）から検出しました。Web Caster X310は、このメールを削除しました。 オリジナルのメールは、送信されませんでした。 ウイルスの感染被害の拡大を防止するためにも、送信メールに添付した感染ファイルを削除することをお勧めします。 誤って感染ファイルを開かないようご注意ください。

メール通知内容一覧

項目	タイトル	本文
感染数が多い （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXXX_XXXX_VIRUS を添付ファイル「XXXX.doc 」（XXX@XXX.XXX 宛に2005/08/12 14:22 頃に送られたメール）から検出しました。 Web Caster X310は、このメールを削除しました。 Web Caster X310は、XXXX_XXXX_VIRUS を添付ファイル「XXXX.doc 」（XXX@XXX.XXX 宛に2005/08/12 14:22 頃に送られたメール）から検出しました。 Web Caster X310は、このメールを削除しました。 Web Caster X310は、XXXX_XXXX_VIRUS を添付ファイル「XXXX.doc 」（XXX@XXX.XXX 宛に2005/08/12 14:22 頃に送られたメール）から検出しました。 Web Caster X310では、感染しているウイルスの数が多いため、ファイル"XXXX.doc"からウイルスを駆除することができません。 いくつかのウイルスは駆除されましたが、まだウイルス感染している可能性があります。 誤って感染ファイルを開かないようご注意ください。 オリジナルのメールは、送信されませんでした。 ウイルスの感染被害の拡大を防止するためにも、送信メールに添付した感染ファイルを削除することをお勧めします。 誤って感染ファイルを開かないようご注意ください。
添付ファイルサイズ制限超え （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310 から自動的に送信されています。 Web Caster X310 は、XXX@XXX.XXX 宛に 2005/08/12 11:34 頃送信されたメールの添付ファイルのウイルス検索ができませんでした。 "4Madd1" 添付ファイルのファイルサイズが大きすぎるため、ウイルスチェックを行っておりません。 送信先にはウイルス検索を実施せずメールを送信しました。
リソース不足 （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXX@XXX.XXX 宛に2005/08/17 14:50 頃送信されたメールの添付ファイルのウイルス検索ができませんでした。 "XXXXXXX" これはシステムのリソースが不足しているためです。 送信先にはウイルス検索を実施せずメールを送信しました。
添付ファイルサイズ制限超え （ウイルス付き） （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、DOS_TEST_VIRUS-C を添付ファイル「XXXX_XXX.COM 」（XXX@XXX.XXX 宛に2005/08/18 11:24 頃に送られたメール）から検出しました。ファイルサイズが大きいため、ウイルス駆除できませんでした。 オリジナルのメールは、送信されませんでした。 ウイルスの感染被害の拡大を防止するためにも、送信メールに添付した感染ファイルを削除することをお勧めします。 誤って感染ファイルを開かないようご注意ください。
多重圧縮 （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXX@XXX.XXX 宛に2005/08/12 11:37 頃送信されたメールの添付ファイルのウイルス検索ができませんでした。 "XXXX_XXX.zip" 添付ファイルが複数回、圧縮されているためです。 送信先にはウイルス検索を実施せずメールを送信しました。
PWD保護 （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXX@XXX.XXX 宛に2005/08/12 11:40 頃送信されたメールの添付ファイルのウイルス検索ができませんでした。 "XXXX_XXX.COM" これは、ファイルがパスワード保護されているか、ファイルフォーマットがサポートされていないのが原因です。 送信先にはウイルス検索を実施せずメールを送信しました。
総メールサイズ制限超え （送信時）	Web Caster X310通知メール	このメールは、Web Caster X310から自動的に送信されています。 Web Caster X310は、XXX@XXX.XXX 宛に2005/08/12 13:59 頃送信されたメールの添付ファイルのウイルス検索ができませんでした。 これは、メールのファイルサイズがWeb Caster X310の制限サイズを超えているためです。 送信先にはウイルス検索を実施せずメールを送信しました。

索引

アルファベット

五十音

ア行

カ行

サ行

索引

仕様

項目		仕様
WAN ポート	回線形式	IEEE802.3(100/10BASE 自動認識)
	ポート数	1
	コネクタ形式	モジュラジャック(8 ピン)
	線路条件	カテゴリ 5 ／ UTP ケーブル、線路長≦ 100 m
LAN ポート	回線形式	IEEE802.3(100/10BASE 自動認識)
	ポート数	4
	コネクタ形式	モジュラジャック(8 ピン)
	線路条件	カテゴリ 5/UTP ケーブル、線路長≦ 100 m
使用電源		AC100 V ± 10 %(50/60 Hz)(専用電源アダプタ使用)
消費電力		最大 10 W
外形寸法（本体）		約 36.5 mm(W)×約 143 mm(D)×約 207.5 mm(H)
質量（本体）		約 0.4 kg
使用条件		温度： 0 ℃～ 40 ℃　湿度： 20 %～ 85 %　RH(結露しないこと)

保守サービスのご案内

●保証について

保証期間（1 年間）中の故障につきましては、「保証書」の記載にもとづき当社が無償で修理いたしますので、「保証書」は大切に保管してください。
（詳しくは「保証書」の無料修理規定をご覧ください。）

●保守サービスについて

保証期間後においても、引き続き安心してご利用いただける「定額保守サービス」と、故障修理のつど料金をいただく「実費保守サービス」があります。
当社では、安心して商品をご利用いただける定額保守サービスをお勧めしています。

保守サービスの種類は

定額保守サービス	●毎月一定の料金をお支払いいただき、故障時には当社が無料で修理を行うサービスです。
実費保守サービス	●修理に要した費用をいただきます。 （修理費として、お客様宅へお伺いするための費用および修理に要する技術的費用・部品代をいただきます。） （故障内容によっては高額になる場合もありますのでご了承ください。） ●当社のサービス取扱所まで商品をお持ちいただいた場合は、お客様宅へお伺いするための費用が不要になります。

●故障の場合は

■ 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

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。

■ 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

0120 − 248995（24 時間　年中無休）

●その他

定額保守サービスの料金については NTT 通信機器お取扱相談センタへお気軽にご相談ください。

NTT 通信機器お取扱相談センタ

■ 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

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。

■ 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

0120-109217（トークニイーナ）
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。

MEMO

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（トークニイーナ）
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。

この取扱説明書は、森林資源保護のため、再生紙を使用しています。
921839A3

本2667-2 (2005.11)
SEC-WBC4＜X310＞トリセツ