IBM Firewall Windows NT 版

使用者の手引き

バージョン 3 リリース 2.1.1

GD88-7845-01
英文原典：GC31-8658-01

IBM Firewall Windows NT 版

使用者の手引き

バージョン 3 リリース 2.1.1

英文原典：GC31-8658-01
GD88-7845-01

ご注意

本書および本書がサポートする製品をご使用になる前に、131ページの『付録. 特記事項』にある一般情報を必ずお読みください。

本書は、IBM Firewall Windows 版 (プロダクト番号 5765-C16) のバージョン 3 リリース 2.1.1 に適用されます。本書は、GD88-7845-00 の改訂版です。

原　典： GC31-8658-01
IBM eNetwork Firewall for Windows NT
User's Guide
Version 3 Release 2.1.1

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 1998.6

この文書では、平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

目次

本書について

本書は、セキュア・ネットワークとの間の好ましくない無許可の通信を防止できるように、Windows NT** システム上で IBM Firewall を構成および管理する方法について説明します。

本書は、IBM Firewall をインストールし、管理し、使用するネットワークまたはシステム・セキュリティー管理者を対象として書かれています。クライアント・プログラムを使用してファイアウォールにアクセスする方法も説明していますが、本書はクライアント・プログラムの使用者の手引きではありません。 Telnet または FTP のようなクライアント・プログラムを使用するには、 TCP/IP クライアント・プログラム用の使用者の手引きを参照してください。

製品をインストールするには、本書を読む前に、CDROM のケースに入っているインストールの手引きを使用してください。

構成クライアントを開始した後は、構成クライアント・フィールドに入力したり、ダイアログ・ボックスからダイアログ・ボックスに移動するのに、オンライン・ヘルプ情報が役立ちます。

予備知識

IBM Firewall をインストールおよび構成する前に、TCP/IP アドレス指定、マスクおよびネットワーク管理についての正しい知識を身につけることが大切です。ネットワークの内外へのアクセスを制御するファイアウォールの設定と構成を行うためには、まず、ネットワークがどのように動作するかについて理解しておかなければなりません。特に、IP アドレス、省略しない完全な名前、サブネット・マスクの基本について理解しておく必要があります。

netstat、arp、ifconfig、ping、nslookup、DNS、sendmail、経路指定、等々を扱う TCP/IP に関する優れた資料としては、 *TCP/IP Network Administration* があります。詳細については、*参考文献* を参照してください。

また、TCP/IP および経路指定、ネットワーク・ハードウェア、DNS、および sendmail についての概要がよくまとまっており、UNIX 管理を行うユーザーにとっての優れた資料としては、 *UNIX System Administration Handbook* があります。詳細については、参考文献を参照してください。

本リリースの機能

IBM Firewall Windows NT 版は、豊富な機能を提供し、 3 つのファイアウォール・アーキテクチャーのすべてを組み込んでいます。

1. アプリケーション・プロキシー
   - FTP
   - HTTP (Gopher および WAIS を含む)
   - Telnet
   - SafeMail

HTTP、Telnet、および FTP には、認証機能があります。

2. Socks プロトコル バージョン 5 (インターネット標準) を使用した、サーキット・レベルのゲートウェイ
3. フィルター処理--トラフィックの可否を決定する膨大かつ強固な基準の集合。基準には、TCP/IP アドレス、ポート、方向、プロトコル、アダプター (セキュア/非セキュア) 、等々があります。

   多くの事前定義サービスによってセットアップが迅速に行われます。

Socks プロトコル バージョン 5

Socks プロトコル バージョン 5 は、簡単で、かつ柔軟性をもつようになったのに加えて以下の利点があります。

- 認証および暗号化方式の使い方が簡単
- UDP 関連。UDP を基本とするプロキシー回線を探すための仮想プロキシー回線を作成します。
- Socks V5 ウォッチャー。リアルタイムの Socks パフォーマンス情報を表示します。

ネットワーク・アドレス変換

インターネットの急速な発達に伴い、IP アドレスの不足が重要な問題となっています。ネットワーク・アドレス変換 (NAT) を使用すると、アドレスの再利用に基づいて、IP アドレスの不足の問題を解決することができます。

NAT の利点は、ネットワークが、専用のまたは無許可のアドレスを使用してインターネット上のホストと通信できることで、専用ネットワークに広いアドレス空間をもつことができます。さらに、NAT を使用することによって、セキュリティーの追加レベルを提供する外部から、専用ネットワーク内のアドレスを隠すことができます。

簡単な管理

リモート・マシンから管理できる Java** アプリケーションを使用して、ファイアウォール構成を簡単に更新することができます。そして、さまざまな管理者に、ファイアウォールに対するアクセスの制御を強めるさまざまなレベルの権限を割り当てることができます。この理解しやすい単一のグラフィカル・ユーザー・インターフェース (GUI) を用いて、 Windows NT 版と AIX 版の両方のファイアウォールを管理することができます。

NT の強化

ファイアウォールがインストールされると、TCP/IP でないプロトコルも、不要なシステム・サービスも、管理者以外のアカウントからのローカル・ログインも使用不可になります。

強力な認証

SecurID、SecureNet キー、その他、一般的なトークンを基本としたすべての認証メカニズムに対するサポートは提供されます。

レポート・ユーティリティー

レポート・ユーティリティーを使用すると、システム・ログが一度データベース・エンジンに報告されれば、システム・ログに対して SQL 照会を実行することができます。

アラート、モニター、およびロギング

大量かつ詳細なログ記録には、TCP/IP アドレス、ユーザー ID、TOD、ファイル名、ポート番号、等々と一緒に、すべてのファイアウォール活動記録が含まれます。ログ・モニターには、疑いのある活動を監視し、しきい値が超えたときにアラートを出す活動が含まれます。

複数ネットワークの分離

ファイアウォールに複数のネットワーク・インターフェース・カード (NIC) を使用すると、複数のサブネットワークを分離することができます。

各国語サポート

英語、日本語、韓国語、フランス語、中国語 (簡体字)、中国語 (繁体字)、イタリア語、スペイン語、およびブラジル・ポルトガル語には、各国語サポートが提供されます。

IP アドレスの入力

ファイアウォールを構成する場合、IP アドレスの入力を要求されます。 完全な小数点付き 10 進数 IP アドレスを、オクテットを 4 つ全部という次のような形式で、入力する必要があります。

```
nnn.nnn.nnn.nnn
```

ここで、各 nnn は 000 から 255 の範囲の 3 桁の数値です。

サービスのための IBM への連絡方法

IBM サポート・センターは、ユーザーの問題診断と解決のためのご相談を電話によって行っております。いつでも IBM サポート・センターにお電話いただければ、営業時間内に（月曜から金曜の午前 8 時から午後 5 時）ご返事をさしあげます。電話番号は 1-800-237-5511 です。

米国以外またはプエルトリコの場合には、弊社営業担当員または貴社担当 IBM 特約店に連絡をお取りください。¢

第1章 IBM Firewall の紹介

IBM Firewall は、AIX および Windows NT** 用のネットワーク・セキュリティー・プログラムです。 本質的には、ファイアウォールは、社内 (セキュア) ネットワークと別の (非セキュア) ネットワークかインターネットとの間を遮断するものです。ファイアウォールの目的は、セキュア・ネットワークの中への、またはセキュア・ネットワークの外部の、望ましくない通信または無許可の通信を防ぐことです。ファイアウォールには、次の 3 つの役割があります。

- インターネットのセキュリティー・ポリシーを強化する。
- ネットワーク内のユーザーが、ネットワークのデータおよび資源を危険にさらすことなく、ネットワークの外部から許可された資源を使用できるようにする。
- 無許可ユーザーがネットワーク内に入れないようにする。

ファイアウォールの概念

インターネットではいかなる接続の可能性もあるので、セキュリティーのリスクも多くなりがちです。独自のプライベート・データを保護し、また専用ネットワーク内部のマシンへのアクセスを保護して、外部からの不正な使用を防ぐ必要があります。以上を行う最初のステップは、専用ネットワークがインターネットと接続するポイントの数を制限することです。専用ネットワークが 1 つのゲートウェイだけによってインターネットに接続される構成であれば、インターネットに出入りするトラフィックを十分に制御することができます。このゲートウェイをファイアウォールを呼びます。

ファイアウォールの働きを理解するため、次の例を考えます。アクセスを制限し、人の入館を制御したいビルディングを想定します。このビルディングの唯一のロビーは、唯一の入り口です。このロビーには、ビルディングに入ってくる人に応対する受付が数人、それを監視するガードマンが数人、そして人々の行動を記録するビデオカメラが数台とその ID を認証するバッジ読取装置が数台あります。

以上は、プライベートなビルディングへの入館を制御するのに大変うまく働きます。しかし、いったん無許可の人がロビーの通過に成功したら、この人がどのような行動に出ようがビルディングを守る手だてはありません。しかし、この人の動きを監視していたら、どのような怪しい動作も検出することができるでしょう。

ファイアウォールの戦略を定義するとき、組織にとって危険となるすべてを禁止し、それ以外を認めることで、十分と考えるかもしれません。しかし、攻撃方式も新しくなるため、このような攻撃を防ぐ方法を先取りすることが必要ですし、ビルディングの場合のように、防御が破られそうな兆候をモニターする必要があります。一般に、侵入を最初の場所で防ぐよりは、侵入されてから回復する方が、損害は大きく費用もかかります。

IBM Firewall ツール

IBM Firewall は、異なるファイアウォール・アーキテクチャーをインプリメントするのに使用するツール・ボックスのようなものです。アーキテクチャーとセキュリティー戦略を選択したら、必要な IBM Firewall ツールを選択します。 IBM Firewall 構成クライアントは、管理用にユーザー・フレンドリーなグラフィカル・ユーザー・インターフェースを備えています。IBM Firewall は、管理の変更や、セキュリティー違反の試みなどの、すべての重要事象を広範囲にロギング記録します。

IBM Firewall は、本来は IP ゲートウェイであるため、全体を複数のネットワーク (1 つまたは複数の非セキュア・ネットワークと 1 つまたは複数のセキュア・ネットワーク) に分割します。非セキュア・ネットワークは、たとえばインターネットです。セキュア・ネットワークは、通常はそれぞれの企業の IP ネットワークです。 IBM Firewall が提供するツールのいくつかを、次に示します。

- エキスパート・フィルター
- プロキシー・サーバー
- Socks サーバー
- ドメイン・ネーム・サービス (DNS) や SafeMail のような特定のサービス

エキスパート・フィルター

エキスパート・フィルターは、時刻、IP アドレス、およびサブネットなどの複数の基準に基づいて、セッション・レベルでパケットを検査するツールです。 フィルター規則は IP ゲートウェイ機能とともに働くので、マシンは、複数のネットワーク・インターフェース (それぞれ個別の IP ネットワークとサブネットワーク内に) を持つ必要があります。一方のインターフェースのセットは非セキュアであると宣言され、他方のセットはセキュアであると宣言されます。フィルターは、2ページの図 1 の説明のように、この 2 つのインターフェースの間で行動します。

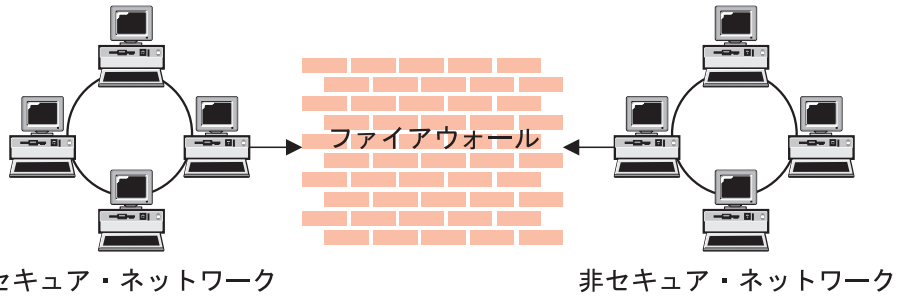

図 1. エキスパート・フィルター付きファイアウォール

エキスパート・フィルターの目的

エキスパート・フィルターは、ファイアウォール用の基本的な保護メカニズムを備えています。フィルターを用いると、IP セッションの詳細情報に基づいてそのメカニズムを通過したトラフィックを判別することができるため、セキュア・サーバーに関するスキャンや IP アドレスのスプーフィングのような外部の脅威から、セキュア・ネットワークを保護することができます。フィルター機能は、ほかのツールの構成の基本と考えてください。

プロキシー・サーバー

通過するパケットをただ検査するだけのフィルター処理とは異なり、プロキシー・サーバーは、ファイアウォールの一部としてのアプリケーションであり、ネットワーク・ユーザーに代わって特定の TCP/IP 機能を実行します。ユーザーは、いずれかの TCP/IP アプリケーション (Telnet または FTP) を用いてプロキシー・サーバーに接続します。プロキシー・サーバーは、ユーザーに代わってリモート・ホストに接続します。このように、ネットワーク構造を外部ユーザーに隠すことによってアクセスを制御します。 3ページの図 2 は、外部ユーザーからの要求を代行受信するプロキシー Telnet サーバーを示しています。

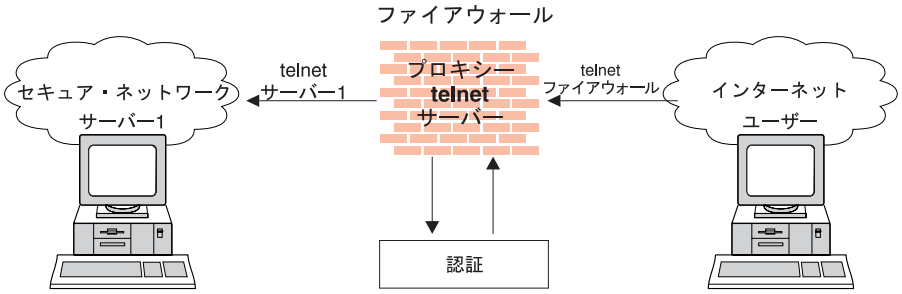

図 2. プロキシー・サーバー付きファイアウォール

プロキシー・サービスが、Telnet、FTP、HTTP、WAIS、GOPHER、および HTTPS、ならびに SafeMail で使用可能です。

IBM Firewall プロキシー・サーバーは、さまざまな認証方式によってユーザーを認証することができます。ユーザーは、内部ネットワークのセキュリティーを損なうことなく、インターネット上の有益な情報にアクセスすることができます。

プロキシー・サーバーの目的

プロキシー・サーバーを介して接続すると、ファイアウォールで TCP/IP 接続が中断されるため、セキュア・ネットワークが危険にさらされる可能性は減少します。ユーザーは、多数の認証方式のいずれかを用いて本人確認を行わなければならない場合があります。

プロキシー・サーバーの大きな利点の 1 つは、アドレスの隠蔽です。プロキシーからのアウトバウンド接続では、すべてファイアウォールのアドレスを使用します。プロキシー・サーバーのもう一つの大きな利点は、セキュリティーです。 IBM の専門家は、クライアント・マシンに存在する可能性があるセキュリティー上の弱点を保護するために、これらのプロキシー・サーバーを開発しました。

プロキシー・サーバーのもう一つの利点は、クライアント・マシン上で特別のクライアント・プログラムは必要がないということです。したがって、ファイアウォールをインストールすれば、ファイアウォールに記録されているすべてのユーザーが、追加ソフトウェアをインストールせずに、非セキュア・ネットワークへのアクセス権を持つことができます。

Socks サーバー

Socks は、アドレスの隠蔽を行う、サーキット・レベルのゲートウェイの標準です。従来のプロキシー・サーバーのようなオーバーヘッドはありません。

Socks サーバーは、セッションがファイアウォールで中断される点では、プロキシー・サーバーに類似しています。相違点は、Socks が、アプリケーションごとに固有のプロキシーを必要とせずに、すべてのアプリケーションをサポートできることです。透過的に、Socks クライアントは IBM Firewall ホストの Windows NT socks サービスを使用してセッションを開始し、送信元アドレスとユーザー ID が非セキュア・ネットワークへの前方向接続を確立する許可を得ているかを妥当性検査してから、2 番目のセッションを作成します。 4ページの図 3 で、Socks サーバー付きファイアウォールを説明します。

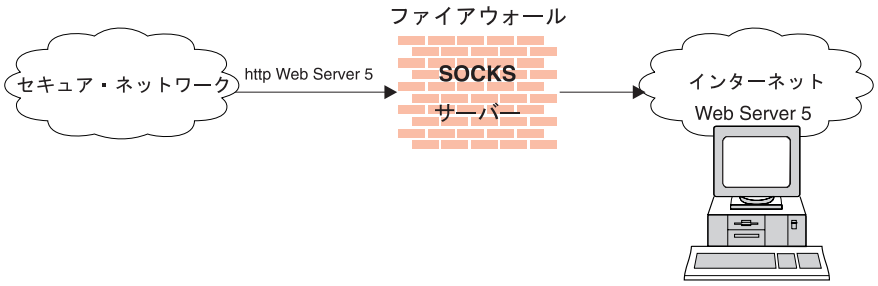

図 3. Socks サーバー付きファイアウォール

Socksified クライアント (Socks-aware) は、 Netscape Navigator** または Microsoft** Internet Explorer などの多くのアプリケーションで使用したり、Aventail** AutoSocks** などの TCP/IP ソフトウェアを介して使用することができます。

Socks サーバーの目的

アウトバウンド・セッション (セキュア・クライアントから非セキュア・サーバーへの) の場合、Socks サーバーにはプロキシー・サーバーと同じ目的があります。すなわち、セッションをファイアウォールで中断し、ユーザーが通過するのに身元確認をしなければならない、セキュア・ドアを用意することです。 これにより、ユーザーは管理作業を少し行うだけでよく、簡素化の利点を得ることができます。

ドメイン・ネーム・サービス

セキュア・ネットワークのドメイン・ネーム・レコードへのアクセスは、侵入者にとっては大変な助けになります。それには、攻撃対象のホストがリストされているからです。ドメイン・ネーム・サービス・サーバーが破壊されると、これも侵入者にとってはアクセス経路となります。外部ネットワークからは、ファイアウォール上のネーム・サーバーは自らを識別するだけで、内部 IP ネットワークに関する情報を公開することはありません。内部ネットワークからは、このネーム・サーバーはインターネット・ネットワークを識別しており、インターネット上の任意のマシンにその名前でアクセスするのに非常に便利です。

DNS サーバーの目的

ファイアウォールで DNS サーバーを実行することには、ネーム・レゾリューション要求がファイアウォール全体に流れるのを防ぐことと、セキュア・ネットワークのホストを非セキュアの世界から隠すことの、二重の利点があります。

SafeMail

メールは、組織がインターネットにアクセスしたい主な理由の 1 つです。 SafeMail は、内部ネットワークのドメイン名を隠すようにように設計された、 IBM のメール・ゲートウェイです。 SafeMail 機能は、メールをゲートウェイ上に保管したり、あるいはルート・ユーザー ID のもとで実行したりしません。発信メール上のファイアウォール・ゲートウェイのプライベート・ドメイン名に代わってパブリック・ドメイン名が使用されるので、メールはユーザーのアドレスからきたのではなく、ファイアウォールのアドレスからきたように見えます。 SafeMail は、Simple Mail Transfer Protocol (SMTP) および Multipurpose Internet Mail Extensions (MIME) をサポートします。

ネットワーク・セキュリティー・スキャナー (Network Security Auditor) の使用

ネットワーク・セキュリティー・スキャナーは、ネットワークをスキャンして、セキュリティー・ホールまたは構成エラーの有無を調べます。ネットワーク・セキュリティー・スキャナーは、サーバーおよびファイアウォールをスキャンして、オープン・ポートやその他のエクスポージャーなどの問題点や弱点のリストを作成し、問題解決のためのリストを編集します。ネットワーク・セキュリティー・スキャナーは、重要なホストの定期的なスキャナーとして使用することもできるし、一度だけの情報収集ツールとして使用することもできます。ネットワーク・セキュリティー・スキャナーの管理は、使いやすいコマンド行インターフェースを用いて行われます。ネットワーク・セキュリティー・スキャナーにより、ファイアウォールを自衛します。

ネットワーク・セキュリティー・スキャナーの機能は、次のとおりです。

- TCP および UDP ポートのスキャン
- 標準外ポートのサーバーの認識
- 危険なサービス、既知の脆弱点、無効になったサーバー・バージョン、およびカスタマイズされたサイト・ポリシーに違反したサーバーやサービスのレポート
- ブラウズが容易な HTML によるレポートの生成

第2章 計画

IBM Firewall を構成する前に、チェックリストと計画ワークシートを用いてネットワーク構成の理解に役立ててください。

計画チェックリスト

1. 目的を決めます。 以下のことを行いますか。
   - インターネット（Telnet、名前なし FTP、など）へのアクセス ?
   - 内部ネットワークを分割したいのか?
   - お客様のネットワークへの外部からのアクセスを規定したいのか?
2. IP サブネットワークのレベルで、ネットワークのトポロジーを評価します。
   - 1 つのセキュア・ネットワークのインターフェースおよび 1 つの非セキュア・インターフェースの構成は正しいか。
   - ご使用のアドレスはサブネット・マスクを規則どおりにサポートできますか ?
3. DNS の使い方を決定します。 31ページの『第6章 ドメイン・ネーム・サービスのハンドリング』 を参照してください。
4. SafeMail の使い方を決定します。 39ページの『第7章 SafeMail』 を参照してください。
5. Socks を使用したい場合は、Netscape Navigator または Microsoft browser などの Socksified クライアントがインストールされていることを確認します。 Socks の使用法については、71ページの『第11章 Socks サーバーの構成』 を参照してください。
6. 必要な認証のタイプは何か。
   - ユーザーの認証に Security Dynamics** ACE/Server** を使用する場合は、ファイアウォール・ホストに ACE/Serverのクライアント・コードをインストールします。セキュア・ネットワークの内部にある他のホストに、ACE/Server のサーバー・コードをインストールすることをお勧めします。

     Security Dynamics ACE/Server および SecurID** カードをインストールして使用するための情報については、Security Dynamics Technologies Inc. が提供する情報をご覧ください。
   - AssureNet Pathways** SecureNetKey** カードを使用する場合は、 IBM Firewall とは別にカードを購入してください。
   - 独自の認証方式を使用する場合は、*IBM Firewall 解説書* の「独自の認証方式の提供」の章を参照してください。
   - NETBIOS の代わりに TCP を使用するには、認証の目的の承認された Windows NT ドメインを検索する機能をインプリメントする、Windows クライアント・コードを構成しなければなりません。 NETBIOS は使用不可になります。承認された Windows NT サーバーには、TCP/IP ホスト名とアドレス、およびそれらとファイアウォール間の TCP/IP 接続性がなければなりません。ファイアウォールと承認された NT サーバーとの間でトラフィックが流れるようにするために、ファイアウォール管理者は、この 2 つの間に接続を作成する必要があります。

この接続は、以下の事前定義のサービスを用いて設定します。

a. ドメイン・コントローラー認証 - これによって、ドメイン・コントローラーをユーザーの認証に使用できる
b. NetBT ネーム・サービス同報通信 - これによって、 TCP/IP ネーム・サービス同報通信で NetBT を使用できる

そして、信頼関連を定義するには、NT 構成ユーティリティーを使用します。

7. フィルター処理を使用するには、簡単なフィルター規則から始め、その制限を強めるようにします。 必要なサービスで使用するポートとプロトコルについては、よく理解しておいてください。
8. 保存ログ・ファイル用のメソッドを決定します。アーカイブは、Windows NT スケジューラー・サービスでのスケジュールされたジョブの理想的な対象となります。 113ページの『第15章 ログ・ファイルとアーカイブ・ファイルの管理』 を参照してください。

ネットワーク構成計画ワークシート

次の情報を、IBM Firewall 構成の計画の一部として記入してください。

ファイアウォールのホスト名

_____

セキュア・ネットワーク・インターフェース（1つまたは複数）（内部セキュア・ネットワークへ接続されているもの）

IP アドレス _____ サブネット・マスク _____

IP アドレス _____ サブネット・マスク _____

IP アドレス _____ サブネット・マスク _____

IP アドレス _____ サブネット・マスク _____

非セキュア・ネットワーク・インターフェース（1つまたは複数）（信頼できない非セキュア・ネットワークへ接続されているもの）

IP アドレス _____ サブネット・マスク _____

IP アドレス _____ サブネット・マスク _____

IP アドレス _____ サブネット・マスク _____

IP アドレス _____ サブネット・マスク _____

ルーターの名前 _____

ルーターのアドレス _____

セキュア・ドメイン・ネーム
_____

セキュア・ドメイン・ネーム・サーバー (DNS) の IP アドレス
_____

非セキュア・ドメイン・ネーム・サーバー (DNS)（1 つまたは複数）の IP アドレス _____

セキュア・メール・サーバー
_____

パブリック・ドメイン・ネーム
_____

構成クライアントの IP アドレス _____

リモート・クライアント（1 つまたは複数）の IP アドレス
_____

Windows NT Firewall のルート・ディレクトリー
_____
(文書全体にわたる ROOTDIR)

c:¥winnt (このディレクトリーに Windows NT がインストールされていると想定します。)

第3章 構成サーバーおよび構成クライアントの設定

本章では、IBM Firewall 用のグラフィカル・ユーザー・インターフェース (GUI) である、構成サーバーと構成クライアントの設定方法について説明します。

構成サーバーの設定

構成サーバーは、ファイアウォールへの構成クライアントのインターフェースです。 構成サーバーは、構成クライアントからの要求を処理します。ファイアウォール・マシン上で実行し、ローカル・マシンもしくはリモート・マシンの構成クライアントからの要求を処理することができます。構成サーバーは、一度設定したら、ファイアウォール・マシンの一部と考えてください。

構成サーバーのポート番号は、Windows オペレーティング・システムをインストールしたディレクトリーにある NT サービス・ファイル、
`c:¥winnt¥system32¥drivers¥etc¥services` で指定されます。ポート番号のデフォルトは 1014 ですが、構成サーバー・サービスを停止し、サービス・ファイルを変更し、そして構成サーバー・サービスを再始動することで、追加したセキュリティーについて、これを変更することができます。

構成サーバーは、最初は、ローカル・マシン上の構成クライアントからの要求を受け入れるためだけに設定されます。最初の要求は暗号化されていません。 これらのオプションを変更するには、コマンド行から `fwcfgsrv cmd=change` を使用します。

localonly=
ファイアウォールがローカル・マシンからのみ管理できるかどうかを示します。

localonly=yes
構成を要求できるのは、ローカル・マシンからのみです。これはデフォルトです。

localonly=no
構成はすべてのマシンから要求できます。

encryption
構成サーバーへの、着信データがセキュア・ソケット・レイヤー (ssl) によって暗号化されているかどうかを示します。

暗号化オプションまたは sslfile を変更する場合は、構成サーバー・サービスを停止して、再始動しなければなりません。

encryption=none
暗号化は発生しません。これはデフォルトです。

encryption=ssl
SSL 暗号化が発生します。

sslfile=
SSL 暗号化に使用する SSL キー・ファイルの名前を示します。デフォルトは `ROOTDIR¥config¥fwkey.kyr` です。 *ROOTDIR* は、インストールの際に IBM

Firewall の宛先ロケーションとして選択したディレクトリーです。キー・ファイルの作成方法については、*IBM Firewall 解説書* を参照してください。

構成クライアントがファイアウォール・マシンに接続できず、かつ別のマシン上にある場合は、`fwcfgsrv cmd=list` を用いて `localonly=no` が設定されているか検査してください。また、クライアントとサーバーが使用する言語は一致していなければなりません。最後に、サービス・パネルを立ち上げて、その状況を検査して、構成サーバー・サービスが必ず実行するようにしてください。こうするには、制御パネルへ進み、サービス・アイコンをダブルクリックして、サービスごとの状況を検査します。実行していない場合は、サービスを再始動しなければなりません。

構成クライアント (GUI) の設定

IBM Firewall のインストール時に、構成クライアントは自動的にインストールされます。構成クライアントは Firewall を使わなくとも個別に Windows NT マシンにインストールすることもできます。これにより、リモート管理が可能になります。 構成クライアントを開始するには、IBM Firewall プログラム・グループの構成クライアント・アイコンをダブルクリックします。構成クライアントが開始したら、 Windows NT 管理者アカウントを用いて、まずファイアウォールにログオンしなければなりません。

構成クライアントを用いてファイアウォールにログオンできるのは、適切な管理認証を持つ Windows NT 管理者とファイアウォール管理者のみです。

Firewall をインストールすると、Windows NT 管理者は、1 次ファイアウォール管理者として指定されます。構成クライアントを使用して、1 次ファイアウォール管理者を用いて構成サーバーにログオンし、必要に応じて、追加のファイアウォール管理者ユーザー名を定義します。構成クライアントを用いてファイアウォール管理者を定義する方法については、 77ページの『第12章 ファイアウォールにおけるユーザーの管理』 を参照してください。

速度が異なるマシンのログオン・タイムアウト値を設定するには IBM Firewall 構成クライアントのアイコンをクリックして以下の変更を行い、「**プロパティー**」をクリックしてください。プロパティーは、**ショートカット・タブ**を用いて変更してください。 「**タイムアウト**」パラメーターを *20* に変更します。ここで 20 は、接続の発生を待機する時間 (秒) です。高速マシンは 10 に設定でき、遅いマシンはデフォルト値を受け入れなければなりません。

JAVA コンソールのデバッグ情報のレベルを上げるには、構成クライアントのアイコンを使用する代わりに、 `ROOTDIR¥cfgcli¥gui` 内の `ibmfw.bat` を実行します。しかし、コンソール・ログが使用可能になるとパフォーマンスが落ちることがありますので注意してください。

構成クライアントへのログオン

構成クライアント (ローカル・マシンまたはリモート・マシン上の) にログオンするには、以下の条件があります。

- ユーザーはファイアウォール管理者でなければならない。

- ファイアウォール管理者は、認証スキームを定義済みにしていなければならない。 82ページの『ユーザーの認証方式』 を参照してください。
- ユーザーには特定の構成機能を行う権限がなければならない。

構成クライアントによるリモート構成の使用可能化

構成クライアントによってリモート構成を使用可能にするには、ログオンする管理者に、ファイアウォール・マシンで定義された以下の属性があることを確認します。

- 管理者がネットワークのセキュア・ネットワーク側にいて、ファイアウォール・マシンのセキュア・インターフェースを使用するのであれば、セキュア管理についての適切な認証方式で定義されていなければなりません。(これはすべて拒否に設定することはできません。) これは、ローカルでのファイアウォールへのログオンにも当てはまります。
- 同様に、管理者が非セキュア側にいて、ファイアウォール・マシンの非セキュア・インターフェースを使用するのであれば、非セキュア管理についての適切な認証方式で定義されていなければなりません。(これはすべて拒否に設定することはできません。)

ユーザー属性はすべて、構成クライアントの「ユーザー変更」ダイアログ・ボックスによるか、 `fwuser` コマンドを使用して設定することができます。すべてのファイアウォール管理者には、上記フィールドのすべてが、 Firewall のインストールが完了すると、適切に設定されます。詳細については、77ページの『第12章 ファイアウォールにおけるユーザーの管理』 を参照してください。

リモート構成サーバーのロギング出力のサンプル

リモート構成サーバーのロギング出力サンプルを、以下に示します。

```
Feb 03 13:52:15 1998 mr16n18: ICA9005i: Starting remote configuration server.

Feb 03 13:52:21 1998 mr16n18: ICA2024i: User administrator successfully
authenticated using NT authentication from secure network:127.0.0.
Feb 03 13:52:21 1998 mr16n18: ICA2169i: User administrator successfully
authenticated for Remote Administration Server using NT from secure network:127.0.0.1.
```

第4章 構成クライアントの使用

構成クライアントは、グラフィカル・ユーザー・インターフェースであり、 IBM Firewall の構成と管理に使用します。

はじめて IBM Firewall をインストールした時点では、ローカル・マシンの構成クライアントからの要求だけを受け入れるように初期設定されます。ただし、別のマシンに構成クライアントをインストールすれば、ファイアウォールをリモートで管理することができます。これについては、11ページの『構成サーバーの設定』を参照してください。

構成クライアントを特定ロケールの言語で開始するように設定するには、「IBM Firewall 構成クライアント」のアイコンをクリックしてから、「**プロパティー**」をクリックします。プロパティーは、**ショートカット・タブ**を用いて変更してください。デフォルトでは、ホスト・マシンのロケールが使用されます。 IBM Firewall では、以下の言語がサポートされます。

- en_US - US 英語
- ja_JP - 日本の PC
- ko_KR - 韓国語
- zh_CN - 中国の EUC
- zh_TW - 中国語 (Big 5)
- fr_FR - フランス語
- it_IT - イタリア語
- pt_BR - ブラジル・ポルトガル語
- es_ES - スペインの PC

構成クライアントを使用するには、マウスは必須です。

「**ヘルプ**」ボタンは、構成クライアントのメイン・パネルの最上部近くにあります。機能については、「**ヘルプ**」をクリックします。

構成クライアントにログオンする方法

1. ファイアウォールと同じマシンであれば、ログオン・タイプに対して「ローカル」を選択します。「ローカル」はデフォルトです。リモートで別のファイアウォールにアクセスしたい場合は、「リモート」を選択します。「リモート」の場合は、ホスト名の入力が必要です。
2. 「リモート」ログオンを選択した場合は、ホスト名か、ログオンするファイアウォール・マシンの IP アドレスを入力する必要があります。
3. ファイアウォールに使用される暗号化によって、「SSL」か「なし」を選択します。クライアントの場合、「ローカル」のデフォルトは「なし」であり、「リモート」のデフォルトは「SSL」です。
4. ファイアウォール管理者か Windows NT 管理者のユーザー名を入力します。
5. サーバーが listen するポート番号を入力します。デフォルトは 1014 です。
6. 「モード」では、ログオンする Windows NT ファイアウォール・マシンを構成する場合「ホスト」を選択します。ホスト管理では、管理者はローカルもしくはリ

モートから、同時に 1 つのファイアウォールを更新することができます。 AIX ファイアウォールのエンタープライズ・ファイアウォール管理 (EFM) の管理には、「エンタープライズ」を選択します。

7. ログオンすると認証メッセージが表示され、パスワードがユーザー名に対して設定された認証方式であれば、パスワードの入力が要求されます。パスワードを要求されたら、「ユーザー応答」フィールドにパスワードを入力し、 Enter キーを押すか、「送信」をクリックします。パスワードの入力が間違っていると、メッセージが表示されます。「クローズ」をクリックして、ログオン・プロセスを再始動します。パスワードをプロンプトされない場合は、ユーザー認証方式がすべて許可されている可能性があります。この場合は、直ちに IBM Firewall 構成クライアント・パネルが表示されます。
8. 認証が正常に行われると、メイン構成パネルが表示されます。

図 4. 構成クライアントの「ログオン」パネル

ナビゲーション・ツリー

構成クライアントには、17ページの図 5 が示すような、左側に沿って折りたたみ式のツリー状ナビゲーションがあります。

ノードまたは機能の下に項目がある場合は、ファイル・フォルダー・アイコンがノードの左に表示されます。副次機能を調べる場合は、アイコンをダブルクリックしてビューを拡大することができます。アイコンをもう一度ダブルクリックすると、このノードのビューは縮小して、元のビューに戻ります。

機能をクリックすると選択され、強調表示されます。ノードの拡大、縮小は、右側のウィンドウ・ビューを変更しないで行うことができます。ツリーが拡大して、使用できる垂直方向の空間を越えると、ナビゲーション・ツリーの右にスクロール・バーが表示されます。ナビゲーション・ツリーに入りきれない機能名があると、水平スクロール・バーが表示されます。

図5. 構成クライアントのナビゲーション・ツリー

メイン・パネルの一般機能

17ページの図 5 に示す「**アラート表示**」上には、次の 3 つの ボタンがあります。

ヘルプ 「**ヘルプ**」ボタンは、構成クライアントのメイン・パネルの最上部近くにあります。「**ヘルプ**」をクリックすると、IBM Firewall を立ち上げて、実行させるために必要なことが表示されます。

使用者の手引き
「**使用者の手引き...**」ボタンは、構成クライアントのメイン・パネルの最上部近くにあります。「**使用者の手引き...**」をクリックすると、そのソフトコピー版が表示されます。

解説書 「**解説書...**」ボタンは、構成クライアントのメイン・パネルの最上部近くにあります。「**解説書...**」をクリックすると、そのソフトコピー版が表示されます。

以下に、メイン・パネルで見られるその他のボタンを示します。

最新　「**最新**」ボタンは、構成クライアントのメイン・パネルの最下部にあります。「**最新**」をクリックすると、最新のアラートが表示されます。

ログオフ/ログオン

「**ログオフ/ログオン...**」ボタンは、構成クライアントの右上隅にあります。これは再接続ボタンです。ログオン順序を再始動すると、別のファイアウォールに接続することも、別の管理者としてログオンすることもできます。

ログオフするには、「ログオフ」をクリック、ログオン・パネルの 「取消」をクリック、あるいはアプリケーションをクローズします。

ログ・ビューアー

「**ログ・ビューアー**」ボタンは、構成クライアントの右下隅にあります。これを使用すると、ファイアウォール・ログをブラウズすることができます。

前ページ

「**前ページ**」ボタンは、構成クライアントのメイン・パネルの最下部にあります。「**前ページ**」をクリックすると、前のアラートが表示されます。

アラート表示

19ページの図 6 に見られるように、システム・ログ・モニターによって生成されたアラート・レコードを、構成クライアントのメイン・ウィンドウの右下部分に表示することができます。

表示されるアラート・レコードは、ROOTDIR¥config¥syslog.conf で定義された最初のアラート・ログ機能によって識別されるファイルから入手されます。 アラート・ログ機能が定義されていなければ、何も表示されません。 アラート・ログ機能を定義する際のヘルプについては、 114ページの『ログ機能の追加』 を参照してください。

パネルは、アラート・ファイルの名前とそのファイルから現在表示されている行番号を示しています。「**最新**」をクリックすると、最新のアラートを表示することができます。「**前ページ**」をクリックすると、前のアラートを見ることができます。

表示される行ごとに、アラートの日時、アラートが発生したファイアウォールのホスト名、アラート・メッセージ・タグ、およびアラート・メッセージ・テキストが表示されます。タグは、アラートのタイプを示します。

図 6. アラート表示

ログ・ビューアー

「**ログ・ビューアー**」をクリックすると、 20ページの図 7 が示すような「ログ・ビューアー」ウィンドウが表示されます。 ログ・ビューアーでは、ファイアウォール・ログ・レコードを表示することができます。ログ・ファイルおよびレコード・カウント (デフォルトは 25) を指定することができます。

デフォルト・ログは、ROOTDIR¥config¥syslog.conf で定義された最初の **ファイアウォール・ログ**機能によって識別されたファイルです。 「ファイル名」フィールドのプルダウン・メニューから他のターゲット・ログ・ファイルを選択することも、表示するファイルの名前を入力することもできます。

特定の開始行を要求する場合は、「開始行:」の隣のフィールドに行番号を入力した後に、「**開始行:**」をクリックします。最後の複数行を要求する場合は、「**下端**」をクリックすると、ファイルの下部が表示されます。「**次へ**」をクリックすると、ファイル内の次の数行に進みます。「**前ページ**」をクリックすると、ファイル内の前の数行に戻ります。「**上端**」では、ファイルの最上部に移動します。「**はい**」にチェックを入れると、任意選択でファイアウォール・ログを読み取り可能なテキストに拡大することができます。

ログ・ファイル、機能、モニターおよびアラートの詳細については、 113ページの『構成クライアントの使用によるログ・ファイル作成およびアーカイブ操作』 および 101ページの『第14章 ファイアウォール・ログのモニター』 を参照してください。

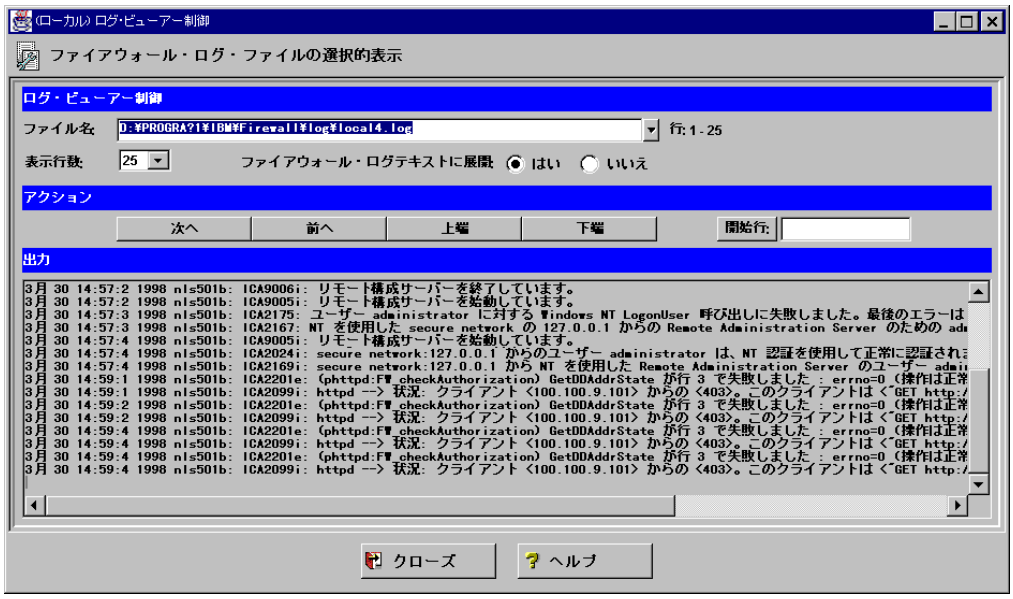

図 7. ログ・ビューアー

その他の機能

パネルの一部には、最上部左隅近くに「**検索**」フィールドがあります。検索文字列を入力して、「**検索**」をクリックすることができます。

構成クライアントのダイアログ・ボックスの多くで表示されるその他のボタンを以下に示します。

適用 「**適用**」をクリックすると、現在の選択に前のパネルのフィールドを取り込むか、パネルで行った変更を保管します。「**適用**」ボタンを押しても、ウィンドウは消えません。

下端 「**下端**」をクリックすると、パネルの最下部に進みます。

取消 「**取消**」をクリックすると、変更を保管せずにウィンドウをクローズします。

クローズ
「**クローズ**」をクリックすると、画面からウィンドウを消します。

コピー 「**コピー**」ボタンを使用すると、新規項目をリストに加える場合に時間を節約できます。リストの項目を選択した後、「**コピー**」をクリックして、選択した項目に類似した項目を作成します。「**コピー**」をクリックして、選択した項目に類似した項目を作成すると、リストの選択した項目からフィールド値をコピーする新しい項目がオープンされます。これで、必要に応じて新しい項目のフィールド値を変更することができます。

削除 「**削除**」をクリックすると、選択した項目をリストから削除します。

下方移動
リストの項目を選択して、「**下方移動**」をクリックすると、リスト中での項目の相対的位置が下がります。クリックするごとに、項目の位置は 1 つずつ下がります。

上方移動
リストの項目を選択して、「**上方移動**」をクリックすると、リスト中での項目の相対的位置が上がります。クリックするごとに、項目の位置は 1 つずつ上がります。

了解 「**了解**」をクリックすると、変更を保管して、ウィンドウをクローズします。

オープン
リストの項目を選択した後「**オープン**」をクリックすると、その項目を表示もしくは変更できます。新規項目を追加するには、リストの「**新規**」項目をクリックし、「**オープン**」をクリックします。

最新表示
「**最新表示**」をクリックすると、ファイアウォールからデータに再アクセスし、パネルにデータを再表示します。

除去 「**除去**」をクリックすると、選択された項目をリストから除去します。このアクションは、リストから項目を除去するだけです。このアクションは、項目が定義付けられている他の場所には影響しません。

選択 「**選択**」をクリックすると、この機能に有効な候補項目のリストにアクセスします。

上端 「**上端**」をクリックすると、パネルの最上部に移動します。

共通フィールド

構成クライアントのダイアログ・ボックスの多くで表示される共通フィールドを以下に示します。

出力 開始したコマンドが処理されると、進行情報はここに表示されます。

名前 この項目の名前を指定します。この項目名は、ファイアウォールのこの特定の機能に固有でなければなりません。この名前には、パイプ記号 (|)、単一引用符(またはアポストロフィ)、もしくは二重引用符 (") を含めてはなりません。なぜなら、これらは SMIT およびファイルの区切り文字として使用されるためです。これらの文字を使用すると、信頼できないデータを生ずることがあります。

説明 このフィールドは任意選択で、この項目に関する共通情報または追加情報を提供したい場合に入力します。

固有の機能

構成クライアントには、知っておくべき固有の機能がいくつかあります。

Windows 95 または Windows NT の構成クライアントを使用する場合、画面の解像度は、1024 ピクセル x 768 ピクセル以上にしたほうが見やすくなります。

左マウス・ボタンを押さえてスピン制御を行っているときに、マウス・ボタンをリリースせずに他の場所にドラッグすると、スピン制御は継続します。これを停止するには、左マウス・ボタンで、スピン制御の方向矢印のいずれかをクリックします。

SSL を使用してファイアウォールに 2 回以上即時に連続してログオンすると、接続が拒否されます。終了して、構成クライアントを再起動してください。

第5章 IBM Firewall の開始

本章では、IBM Firewall の初期の設定に必要な、基本構成ステップについて説明します。 本章では、セキュア・インターフェースの定義方法、セキュリティー・ポリシーの判別方法、およびネットワーク・オブジェクトの定義方法について説明します。

基本構成ステップ

IBM Firewall の基本設定では、以下のステップを行います。

1. IBM Firewall の設定を計画します。使用したいファイアウォールの機能およびその使い方を、前もって決めておきます。以下の節を参考にしてください。
   - 1ページの『第1章 IBM Firewall の紹介』
   - 7ページの『第2章 計画』
   - 53ページの『計画に関する考慮事項』
2. セキュア・ネットワークに接続するインターフェースを、ファイアウォールに教えます。ファイアウォールを正しく働かせるには、セキュア・インターフェースと非セキュア・インターフェースを持たなければなりません。構成クライアントのナビゲーション・ツリーから「システム管理」フォルダーをオープンして、「**インターフェース**」をクリックします。ファイアウォールのネットワーク・インターフェースのリストが表示されます。インターフェースのセキュリティー状況を変更するには、インターフェースを選択して、「**変更**」をクリックします。詳細については、25ページの『ネットワーク・インターフェースの指定』 を参照してください。

   インターネットに接続しようとする場合は、ISP に接続して、ファイアウォールの非セキュア・インターフェースの登録済み IP アドレスを取得します。
3. 「システム管理」フォルダーの「**セキュリティー・ポリシー**」ダイアログにアクセスして、一般セキュリティー・ポリシーを選択します。一般的なファイアウォール構成の例を以下に示します。
   - DNS 照会許可
   - 非セキュア・インターフェースへの同報通信メッセージの送付禁止
   - 非セキュア・インターフェースへの Socks の禁止

   詳細については、25ページの『構成クライアントを用いたセキュリティー・ポリシーの定義』 を参照してください。
4. ドメイン・ネーム・サービスおよびメール・サービスを設定します。これらの機能には、構成クライアントのナビゲーション・ツリーの「システム管理」フォルダーからアクセスします。まず、31ページの『第6章 ドメイン・ネーム・サービスのハンドリング』 をお読みください。
5. 構成クライアントのナビゲーション・ツリーの**ネットワーク・オブジェクト**の機能を用いて、ファイアウォールへのネットワーク (1 つまたは複数) の主要要素を定義します。ネットワーク・オブジェクトは、ファイアウォールを通過するトラフィックを制御します。ネットワーク・オブジェクトとして、以下の主要要素を定義してください。

- ファイアウォールのセキュア・インターフェース
- ファイアウォールの非セキュア・インターフェース
- セキュア・ネットワーク
- セキュア・ネットワーク上の各サブネット
- SDI サーバーおよび NT ドメイン・サーバーのホスト・ネットワーク・オブジェクト (該当する場合)

詳細については、27ページの『ネットワーク・オブジェクト』 を参照してください。

6. ファイアウォールのサービスを使用可能にします。セキュア・ネットワークのユーザーはこれらのメソッドを用いて、非セキュア・ネットワーク (Socks もしくはプロキシーなどの) にアクセスできます。インプリメントされるサービスは、計画段階での決定によって決まります。サービスのインプリメントには、特定のタイプのトラフィックを通過させる接続構成の設定が必要になります。たとえば、セキュア・ユーザーに、HTTP プロキシーを用いてインターネットの Web をサーフィンさせる場合は、ファイアウォール上で HTTP プロキシー・デーモンを構成するだけでなく、HTTP トラフィックを通過させる接続を設定することも必要です。特定のサービスをサポートする接続の設定方法については、 53ページの『第9章 サービスの例』を参照してください。
7. ファイアウォール・ユーザーを設定します。アウトバウンド Web アクセスのような機能やファイアウォール管理者に認証が必要になる場合は、これらのユーザーをファイアウォールに定義する必要があります。詳細については、77ページの『第12章 ファイアウォールにおけるユーザーの管理』 を参照してください。
8. Windows NT ドメイン・パスワードを認証に使用したい場合は、認証目的で承認された Windows NT ドメインを検索する機能をインプリメントする、 Windows クライアント・コードを構成しなければなりません。 NETBIOS は使用不可になります。承認された Windows NT サーバーには、TCP/IP ホスト名とアドレス、およびそれらとファイアウォール間の TCP/IP 接続性がなければなりません。ファイアウォールと承認された Windows NT サーバーとの間でトラフィックが流れるようにするために、ファイアウォール管理者は、この 2 つの間に接続を作成する必要があります。
9. 将来ネットワーク・アドレス変換を使用する場合は、まず ISP に接続して、複数対 1 変換で使用する登録済みインターネット・アドレスを取得します。次に、「*NAT Configuration (NAT 構成の追加)*」パネルに進み、「*Many-to-One IP Address (複数対 1 IP アドレス)*」フィールドを追加します。詳しくは、121ページの『第16章 ネットワーク・アドレスの変換』 を参照してください。

これらのステップに従えば、基本的なファイアウォール構成の設定と実行に役立つはずです。 IBM Firewall は、ネットワークのセキュリティーを確保するのに役立つシステム・ログのような、その他の機能を備えています。詳細については、113ページの『第15章 ログ・ファイルとアーカイブ・ファイルの管理』 を参照してください。

ネットワーク・インターフェースの指定

本書では、セキュア・インターフェースと非セキュア・インターフェース、ネットワーク、およびホストを区別しています。セキュア・インターフェースは、IBM Firewall ホストをユーザーの内部ネットワーク (保護する必要があるネットワーク) 内のホストのネットワークに接続します。 **ファイアウォールを稼働させるには、最低 1 つのセキュア・インターフェースが必要です。** 非セキュア・インターフェースは、IBM Firewall を外部のネットワーク (1 つまたは複数) もしくはインターネットに接続します。 IBM Firewall には、少なくとも 1 つの非セキュア・インターフェースがなければなりません。

セキュア・インターフェースを通じて接続されたネットワークはすべて、セキュア・ネットワークと見なされます。セキュア・インターフェースに接続されたさまざまなサブネットを識別するために、同じインターフェース上のいくつかのサブネット間のアクセスを、 IP アドレスまたはアドレス・マスクに基づいて許可または拒否するエキスパート・フィルター規則を使用します。

セキュア・インターフェースおよび非セキュア・インターフェースを指定する場合は、構成クライアントのナビゲーション・ツリーの「システム管理」フォルダーを使用します。 認識されているすべてのインターフェース (アダプター) が表示され、セキュア・ネットワーク用か非セキュア・ネットワーク用かが識別されます。

特定インターフェースのフィルター処理を実行する際には、各インターフェース名を提供する必要があります。

ネットワーク・インターフェースをセキュアまたは非セキュアとして示すには、次のようにします。

1. インターフェースを選択し、「**変更**」をクリックします。
2. 必要に応じて繰り返します。
3. 「**クローズ**」を選択します。

インターフェースをセキュアまたは非セキュアとして示し、そのインターフェースに意味のある名前を指定するには、「**オープン**」をクリックします。この名前は、フィルターが特定インターフェースのフィルター処理に使用します。

構成クライアントを用いたセキュリティー・ポリシーの定義

IBM Firewall の構成時に最初に考慮すべきことの 1 つは、インストール・システムの一般的セキュリティー・ポリシーです。

IBM Firewall には、26ページの図 8 が示すように、セキュリティー・ポリシーの設定に役立つダイアログ・ボックスがあります。

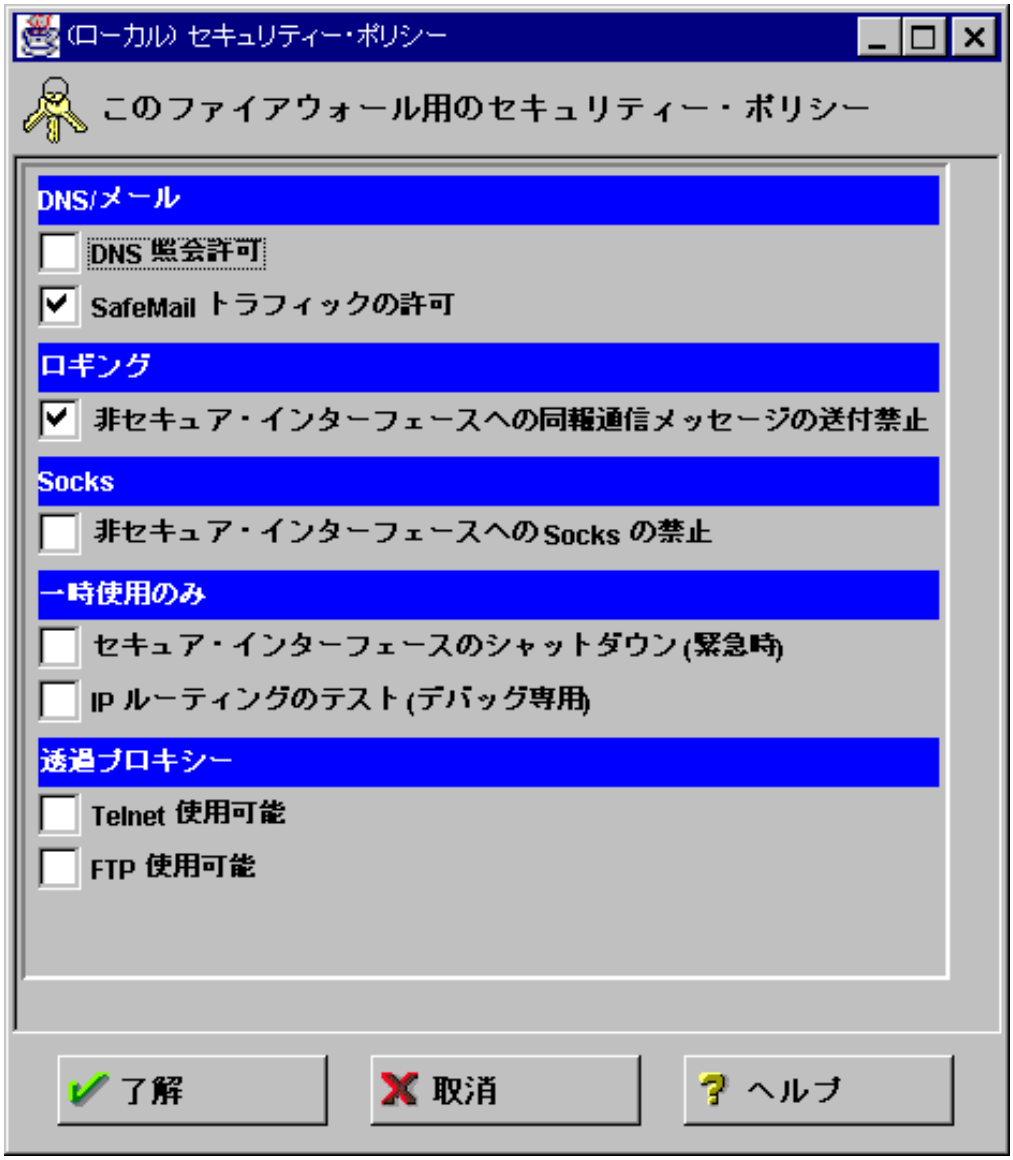

図 8. セキュリティー・ポリシー

「ヘルプ」をクリックすると、「セキュリティー・ポリシー」パネルについての追加情報が得られます。

「セキュリティー・ポリシー」パネルでは、管理者は迅速かつ簡単にファイアウォールのブランケット・ポリシーを設定することができます。 「セキュリティー・ポリシー」ウィンドウで表示されるチェックボックスの大部分は、ファイアウォールが受信したすべてのネットワーク・トラフィックに当てはまる特定の事前定義サービスを選択する、簡略操作を備えています。例外は「透過プロキシー」の選択項目です。そこで指定できるのは、単に透過 Telnet と透過 FTP を使用可能もしくは使用不可にすることだけです。

セキュリティー・ポリシーを選択すると、ファイアウォールはフィルター規則を作成します。次に、これを活動化する必要があります。ファイアウォールによって、選択したサービスが使用可能になり、一般使用できるようになります。

事前定義サービスに関係するチェックボックスを選択して「**了解**」をクリックしたときは、常に「接続の活動化」ウィンドウによってこれらの変更を活動化する必要があることに注意してください。「透過プロキシー」の選択は、事前定義サービスとは関係がないので、活動化する必要はありません。事前定義サービスについては、64ページの『事前定義サービス』 にリストが記載されています。

以下のチェックボックスのリストが表示され、そこから、それぞれのサイトのセキュリティー・ポリシーを反映した属性を選択することができます。選択された属性は、IBM Firewall の両サイドのすべてのアドレスに適用します。

- 「**DNS 照会許可**」を選択して、ドメイン・ネーム・サービス・レゾリューションの要求と応答を可能にします。
- 「**SafeMail**」を選択し、メール・トラフィックがファイアウォール内をフローできるようにします。
- 「**非セキュア・インターフェースへの同報通信メッセージに送付禁止**」を選択して、ブロードキャスト・メッセージが非セキュア・ポートで受信されないようにします。ファイアウォールの非セキュア・インターフェースがインターネットに接続されている場合、このサービスは、ファイアウォールへのログの量を減らすのに役立ちます。
- 「**非セキュア・インターフェースへの Socks の禁止**」 を選択して、 Socks トラフィックが非セキュア・ネットワークからファイアウォールに入るのを禁止します。
- 「**セキュア・インターフェースのシャットダウン (緊急時)**」を選択して、ファイアウォールとの間のすべてのトラフィックがセキュア・インターフェースを通過するのを禁止します。これは、緊急目的でのみ使用されます。
- 「**IP ルーティングのテスト(デバッグ専用)**」を選択して、ファイアウォールとの間のすべてのトラフィックが任意のインターフェースを通過するのを許可します。このチェックボックスの値を変更した場合は、「**了解**」をクリックしてそれを保管し、「接続の活動化」ウィンドウによってそれを活動化しなければならないことに注意してください。**このサービスを使用すると、ファイアウォールのセキュリティーが危険にさらされる恐れがあります。この使用には十分な注意が必要です。**
- 「**Telnet 使用可能**」を選択して、透過プロキシー Telnets を許可します。
- 「**FTP 使用可能**」を選択して、透過プロキシー FTP を許可します。

ネットワーク・オブジェクト

ネットワーク・オブジェクトとは、ホスト、ネットワーク、ルーター、仮想的な専用ネットワーク、およびユーザーのような、ネットワークにすでに存在するコンポーネントのことです。 ネットワーク・オブジェクトは、接続を作成する際に、サービスの送信元や宛先のアドレスを指定します。

オブジェクトは、名前、アイコン表示、タイプ、および説明によって識別することができます。ネットワーク・オブジェクトにはいくつかのタイプがありますが、ホストとファイアウォールがもっとも一般的です。 IBM Firewall のデフォルトのネットワーク・オブジェクトは、″The World″ です。 これは、可能なあらゆる IP アドレ

スを包み込んだグローバル・オブジェクトです。ネットワーク構成のワークシートへの記入が終われば (8ページの『ネットワーク構成計画ワークシート』を参照)、オブジェクトの作成準備は完了です。

オブジェクトは単一でもグループでも作成することができます。ネットワーク・オブジェクトはすべて、IP アドレスおよびアドレス・マスク (サブネット・マスク) によって定義されます。したがって、1 つのオブジェクトで特定範囲のネットワーク・アドレスを表すことができます。

構成クライアントを用いたネットワーク・オブジェクトの定義

単一のネットワーク・オブジェクトを定義する場合は、構成クライアントのナビゲーション・ツリーから「**ネットワーク・オブジェクト**」を選択します。「ネットワーク・オブジェクト」ダイアログ・ボックスが表示されます。「**新規**」をダブルクリックします。 28ページの図 9 のような、「**ネットワーク・オブジェクトの追加**」ダイアログ・ボックスが表示されます。

図 9. ネットワーク・オブジェクトの追加

1. オブジェクト・タイプを入力します。「**オブジェクト・タイプ**」の矢印記号をクリックし、作成可能なオブジェクト・タイプを表示します。パフォーマンスの点からは、「ホスト」タイプのオブジェクトではなく、「ネットワーク」タイプのオブジェクトを作成する方が有利です。作成できるオブジェクト・タイプを、次に示します。
   - ホスト - ネットワーク上の特定のノード (マスクは、255.255.255.255)。
   - ネットワーク - アドレス範囲と特定のサブネット・マスクで特徴づけられたネットワーク・アドレスの集合範囲。

- ファイアウォール - ファイアウォールをインストールした単一のマシン (マスクは、255.255.255.255)。 IBM または手動トンネルのターゲットにすることができるのは、ファイアウォール・ネットワーク・オブジェクトのみです。
- ルーター - トラフィックを複数のネットワーク間でルーティングするホスト (マスクは、255.255.255.255)。
- インターフェース - マシン上のネットワーク・アダプター (マスクは、255.255.255.255)。ファイアウォール上のアダプターである必要はありません。

2. オブジェクト名を入力します。
3. 説明を入力します。このフィールドは任意選択です。
4. このオブジェクトの IP アドレスを、小数点付き 10 進数で入力します。
5. アドレスのビットを指定するサブネット・マスクを入力して、 IP パケットのアドレスと比較します。
6. 「**了解**」をクリックします。

ネットワーク・オブジェクト・グループ

グループは、ネットワーク・オブジェクトの集合です。グループは、接続設定の便宜上使用され、繰り返し作業を排除することができます。ネットワーク・オブジェクトによって個々に表されるいくつかのアドレスを、1 つのネットワーク・オブジェクト・グループにまとめて部門を表すなどは、その例です。この部門は、接続の送信元か宛先アドレスのいずれかとして使用できます。

ネットワーク・オブジェクト・グループを定義する場合は、構成クライアントのナビゲーション・ツリーから「ネットワーク・オブジェクト」を選択します。 「**ネットワーク・オブジェクト**」ダイアログ・ボックスが表示されます。「**新規グループ**」をダブルクリックします。「**ネットワーク・オブジェクトの追加**」ダイアログ・ボックスが表示されます。

1. グループ名を入力します。
2. 説明を入力します。このフィールドは任意選択です。
3. 「**選択**」をクリックして、グループのオブジェクトを選択します。
4. 「**了解**」をクリックします。

ヒント: 隣接するアドレス範囲を、可能な限り単一のネットワーク・オブジェクトに包括することをお勧めします。 これは、接続規則処理のパフォーマンスを改善します。以下の例が、このことを説明しています。

```
ACCOUNTING DEPARTMENT
  Kevin's machine  191.1.10.1
  Susan's machine  191.1.10.3
  Helen's machine  191.1.10.5
  Peter's machine  191.1.10.7
  Bob's machine    191.1.10.9
```

この ACCOUNTING DEPARTMENT のネットワーク・オブジェクトを作成するには、このグループの IP アドレス情報を、サブネット・マスク を 255.255.255.0 として、191.1.10.0 と入力します。このネットワーク・オブジェクト、つまり ACCOUNTING DEPARTMENT は、接続の送信元か宛先アドレスのいずれかとして使用できます。

ファイアウォール構成のバックアップ

ファイアウォールは、すべての構成ファイルを、ROOTDIR¥config に格納します。ファイアウォール・ファイルのすべてをバックアップせずに個人のファイアウォール構成をバックアップしたい場合は、 ROOTDIR¥config ディレクトリーの全内容のバックアップをとってください。

バックアップ・ファイアウォール構成を復元するには、 ROOTDIR¥config ディレクトリーのすべての既存ファイルを削除して、バックアップ・バージョンのファイルを復元してください。復元した構成を有効にするには、フィルター規則を再生成し活動化させてください。

キー・ファイアウォール構成ファイルは、以下にリストされています。ファイアウォール上の ¥config ディレクトリーには、ここにリストされるすべてのファイルが含まれるわけではありません。ほとんどのファイアウォール構成ファイルが、テキスト・エディターで表示可能な簡単なテキスト・ファイルですが、**これらのファイルの手動編集はサポートされていない**ことに注意してください。

- carriers.cfg - ポケット・ベル通信業者定義
- cfgfilt.output
- explode.cfg
- filters.active - フィルター処理が活動状態かどうかを示す
- fwadpt.cfg - ネットワーク・インターフェースの定義
- fwconfig.map - 構成ファイル名を含む
- fwconns.cfg - フィルター接続定義
- fwfilters.cfg - 現行活動状態フィルター
- fwhttp.cfg - HTTP プロキシー構成
- fwmail.conf - SafMail 構成
- fwobjects.cfg - ネットワーク・オブジェクト定義
- fwpolicy.cfg - セキュリティー・ポリシー・オプション
- fwrules.cfg - フィルター規則テンプレート定義
- fwservices.cfg - サービス定義
- fwsocks.cfg - 構成クライアントからの Socks 5 規則
- fwtdefn.conf - アラート定義
- fwtpproxy.cfg - 透過的プロキシー定義
- fwusrdb.cfg - ファイアウォール・ユーザー・データベース
- logmgmt.cfg - アーカイブ定義
- modems.cfg - モデム定義
- pager.cfg - ポケット・ベル定義
- rcsfile.cfg - 構成サービス・パラメーター
- Socks5.conf - Socks 5 構成ファイル生成
- Socks5.header.cfg - 生成済み Socks5.conf のユーザー提供部分
- syslog.conf - ログ機能定義

第6章 ドメイン・ネーム・サービスのハンドリング

この章では、ドメイン・ネーム・サービス (DNS) の構成方法について、 IBM Firewall との関係で説明します。 DNS の目的は、セキュア・ネットワーク外部のホストに情報を提供しないようにしながら、セキュア・ネットワーク内部のホストに完全なドメイン・ネーム・サービスを提供することです。 DNS を使用すれば、セキュア・ネットワーク内部のユーザーは、インターネットが提供するすべてのサービスにアクセスすることができます。しかし、セキュア・ネットワークの情報は、外部からは知ることができないようにしてあるため、侵入者が特定のコンピューター見つけて攻撃することは困難です。

これを行うには、次の 3 つのドメイン・ネーム・サーバーが必要です。

1. IBM Firewall 上に 1 つ
2. セキュア・ネットワーク内に 1 つ
3. セキュア・ネットワーク外に 1 つ

DNS が IBM Firewall をどのように処理するかを理解するには、 31ページの図 10を参照してください。

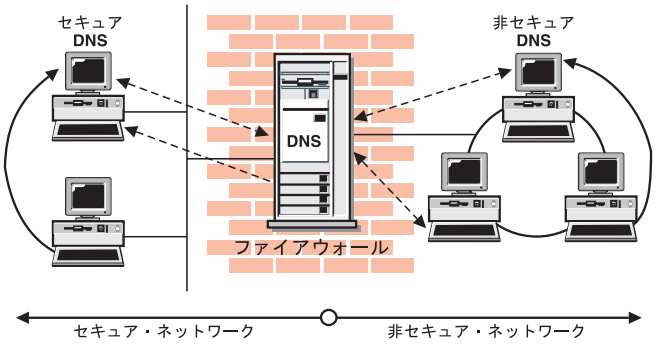

図 10. DNS

ファイアウォールは、セキュア・ネットワークおよび非セキュア・ネットワークのネーム・サーバー間のゲートウェイとして機能します。ファイアウォールの働きを正式に表現すれば、キャッシュ*専用*ネーム・サーバーです。ファイアウォールの DNS 自体には、データベース・ファイルが含まれていないからです。

31ページの図 10 に、ファイアウォールの役割を示します。 ファイアウォールが自分で行う処理を目的として名前を解決しなければならないときは、セキュア側のネーム・サーバーに問い合わせます。照会がファイアウォールに送られると、ファイアウォールは、この照会を非セキュア・ネーム・サーバーに順番に送ります。

セキュア・ネットワーク上のクライアントがセキュア側の情報を要求すると、ファイアウォールはその要求をセキュア側の DNS に送り、応答してもらいます。 このクライアントが非セキュア側の情報を要求しても、ファイアウォールはその要求を同じセキュア側の DNS に送ります。照会が非セキュア情報に対するものであれば、セキュア側の DNS は回答できません。したがって、DNS はその照会をファイアウォー

ルに送ります。 非セキュアの DNS が要求をファイアウォールに送る場合、この要求は非セキュアの DNS ドメインに送られます。したがってここでも機密情報が漏えいすることはありません。

構成クライアントを用いた DNS の構成

DNS を構成するには、構成クライアントのナビゲーション・ツリーから、「システム管理」を選択します。 ファイル・フォルダー・アイコンをダブルクリックして、表示を拡大します。「**ドメイン・ネーム・サービス**」を選択します。 IBM Firewall は、現行 DNS 構成を表示します。これは変更することができます。

図 11. ドメイン・ネーム・サービス

注: DNS を追加すると、ファイアウォールは既存のドメイン・ネーム・サービス構成ファイルの保管と名前変更を行います。

1. 「**セキュア・ドメイン・ネーム**」フィールドに指定するのは、ファイアウォールが非修飾名ホスト名に付けるドメイン名です。
2. 「**セキュア・ドメイン・ネーム・サーバー**」フィールドには、 IBM Firewall によってインターネットから保護されているホストの名前および IP アドレスを解決するサーバーを指定します。小数点付き 10 進数形式の IP アドレスを入力します。スペースで区切れば複数入力することができます。
3. 「**非セキュア・ドメイン・ネーム・サーバー**」フィールドには、非セキュア・ネットワークに関する情報を解決するサーバーを指定します。このサーバーは、ご利用のサービス・プロバイダーが提供するものです。小数点付き 10 進数形式の IP アドレスを入力します。スペースで区切れば複数入力することができます。

注: 初期設定されるとネーム・サーバーは照会を出し、root ネーム・サーバーのリストを取得します。ほとんどのサーバーの設定では、このリストがメモリーに保持されますが、 Mircosoft の設定の場合は、構成ファイルに書き込まれます。この操作により、ネーム・サーバーの動作が変わることはありませんが、「**非セ**

キュア・ネーム・サーバー」フィールドに表示される値は変化します。 ただし、これは問題となることではありません。

セキュア・ネーム・サーバーの構成

セキュア・ネーム・サーバーの設定では、未解決の照会がファイアウォールに送られるように指定する必要があります。 標準の BIND インプリメンテーションを行う場合は、以下のように *forwarders* 文、および *cache* 文をセキュア・ネーム・サーバーの *boot* ファイルに追加します。

```
forwarders      aaa.bbb.ccc.ddd
cache           .               named.cache
```

次に、ファイアウォールを指定するキャッシュ・ファイル、*named.cache* を作成します。

```
. 99999999 IN NS firewall.private.com
firewall.private.com   99999999 IN A aaa.bbb.ccc.ddd
```

ここで *private.com* は、セキュア側から使用されるドメイン・ネームであり、*aaa.bbb.ccc.ddd* は、ファイアウォールの IP アドレスです。

さらに、ファイアウォール・ホスト名を DNS データベースに追加することもできます。 こうすればユーザーは、IP アドレスの代わりにファイアウォールのホスト名を使用することで、ファイアウォールの Socks サーバー、HTTP プロキシー、Telnet プロキシー、および FTP プロキシーにアクセスすることができます。ただし、そのためには、*DNS および BIND の第 4 章*の説明にある、2 つの追加ステップが必要です。この資料の詳細については、*参照文献* を参照してください。

まず、A レコードをドメイン・データベース・ファイルに追加します。

```
firewall.private.com     IN A aaa.bbb.ccc.ddd
```

PTR レコードを reverse-lookup ファイルに追加します。

```
ddd.ccc.bbb.aaa.in-addr.arpa.     IN PTR   firewall.private.com.
```

セキュア・ネットワークに DNS を用いない場合、ファイアウォールは自分の情報を自分で解決しなければなりません。このときは、ファイアウォールを標準設定し、「**セキュア・ネーム・サーバー**」フィールドにファイアウォールのセキュア・インターフェースを指定します。次に、以下の行を `c:¥winnt¥system32¥dns¥boot` に追加します。

```
primary ccc.bbb.aaa.in-addr.arpa c:¥winnt¥system32¥dns¥fwnamed.rev
```

以下のような *fwnamed.rev* を作成します。

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9       ; Serial
                          86400   ; Refresh after 1 day
                          300     ; Retry after 5 minutes
                          654000  ; Expire after 1 week
                          3600  ) ; Minimum TTL of 1 day
ccc.bbb.aaa.in-addr.arpa.         IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.     IN PTR   firewall.private.com.
```

セキュア・クライアントの構成

セキュア・ネットワークのクライアントの構成は、送信する照会がファイアウォールではなく、セキュア・ネーム・サーバーに送られるように設定しなければなりません。 この設定は、セキュア側の情報をファイアウォールの内部メモリー・キャッシュに保管しないようにするためですので、重要です。また、このことは、ファイアウォールの作業負荷を軽くします。なぜなら、照会がセキュア側から非セキュア側への照会の送信を必要としない限り、ファイアウォールにはかかわりが生じないからです。

セキュア・ネットワークに DNS を用いない場合、クライアントはファイアウォールをネーム・サーバーとして指定しなければなりません。

サービスの公開

多くの組織がインターネット上に特定のサービスを公開することを望んでいます。 どのようなタイプの TCP/IP サーバーが使われていても、サービスには、電子メールや Web サーバーが含まれています。このようなサービスを利用してもらうためには、サーバーをネットワーク上のアクセス可能な場所に配置するだけではなく、公用 DNS にサーバーを登録し、ユーザーが正しい情報を入手できるようにしなければなりません。

そのためには、2 つの方法があります。1 つは、サービス・プロバイダーにユーザーのサーバーをドメインの一部として登録してもらう方法 (つまり、ネーム・サーバー上にも)、もう 1 つは、自分でネーム・サーバーを用意して、それをインターネットに登録することです。インターネット・サービス・プロバイダー (ISP) にとってメール・サーバーを用意することは、たやすいことです。 この場合は、登録したいホスト名および IP アドレスをプロバイダーに伝える必要があります。たとえば、web サーバーを *www.public.com*、 IP アドレス *50.100.150.200* で運用する場合は、*www.public.com (IP アドレス 50.100.150.200)* という情報を ISP に登録してもらう必要があります。

さらに、電子メールを受信したい場合は、ユーザーのファイアウォールを公用電子メール・ドメインの*メール交換機* として ISP に登録してもらう必要があります。 ISP に伝える必要のある項目は、ホスト名 *(gateway.public.com)* とその IP アドレス *(50.100.150.201)*、およびメール *(public.com)* を受信するドメイン・ネームです。

ISP がこれらのサービスを提供できない場合は、自分の手で以上の事柄を行う必要があります。 ここでまた、2 つの選択肢があります。 1 つは、DNS サーバーを DMZ 内に配置すること、もう 1 つは、ファイアウォールをネーム・サーバーとして使用することです。ファイアウォールを使うことでセキュリティーの危険性が増大することはありません。ファイアウォールに置かれるデータベース・ファイルには、セキュア・ネットワークに関する情報が含まれていないからです。ファイアウォールに置かれる情報は、提供したい公のサービスに関する情報だけです。

DNS サーバーの設定に関する詳細は、*DNS および BIND* (*参照文献*にリストされています) の第 4 章に記載されています。必要な場合、この項目は必ず読んでおいてください。DNS サーバーの設定は平凡な作業ではありません。専門家に行ってもらうことが最善の策です。専門家がいる場合は、その方に作業を依頼してください。

詳細については、35ページの『構成サンプル』 を参照してください。

Microsoft の DNS サーバーの導入

Microsoft の DNS サーバーをインストールする場合は、「コントロール パネル」をオープンし、「**ネットワーク**」、「**サービス タブ**」、「**追加**」の順にクリックし、「**Mircosoft DNS サーバー**」を選択します。インストール用の CD-ROM が必要になります。

DNS 問題追及

IBM Firewall 解説書 には、ファイアウォールの問題追及について説明した章が含まれています。その章の中に、 DNS 問題を詳しく説明している個所があります。ここには、 *nslookup* コマンドを使用して、DNS システムの障害個所を特定するヒントが記載されています。

構成サンプル

本セクションでは、ファイアウォールを配置する構成のサンプルをいくつか図示します。ほとんどの例が、DNS 操作で必要な構成に焦点を置いています。これらの例のいずれかにユーザーのネットワークが図示されているとは限りません。おのおのの例を理解し、個人のインストールに合った適切な概念を適用するようにしてください。

例 1: 非セキュア・インターフェースの DMZ 内に DNS サーバーがある

最初の例として、非セキュア・ネットワーク内において DMZ 内のネーム・サーバーを操作するための必須ファイルを 35ページの図 12 に示します。

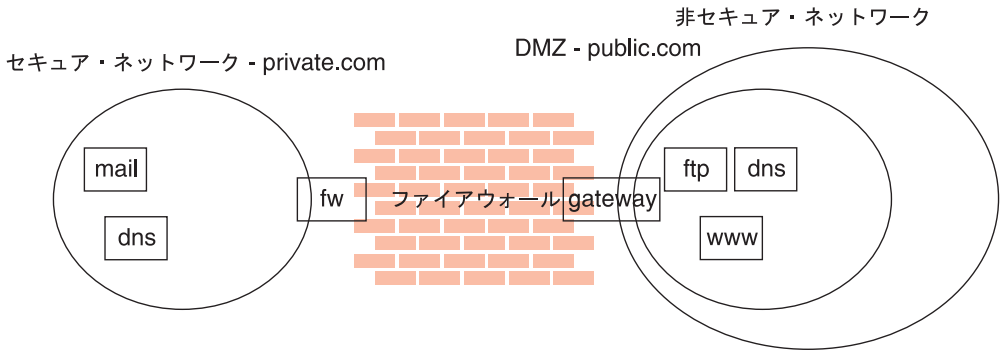

図 12. 非セキュア・ネットワークにおける DMZ 内のネーム・サーバー

この図は、専用ネットワーク *private.com* を図示しています。このネットワークは、セキュア・インターフェース名が *fw.private.com* で、非セキュア・インターフェース名が *gateway.public.com* である IBM Firewall の背後に位置しています。この企業の DMZ は、非セキュア・インターフェースに付加され、ネーム・サーバー

dns.public.com、 FTP サーバー *ftp.public.com*、および Web サーバー *www.public.com* を含んでいます。このシナリオを実行するための *dns.public.com* にあるファイルは以下のとおりです。

db.public

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                  3600        ; retry after 1 hour
                  604800      ; expire after 1 week
                  86400 )     ; minimum TTL 1 day
;
; Nameservers
;
public.com           IN NS  dns.public.com.
;
; Hosts in the DMZ
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; Mail-related entries
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

db.50.100.150

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                  604800      ; expire after 1 week
                  86400 )     ; minimum TTL 1 day
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

db.127.0.0

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                  604800      ; expire after 1 week
                  86400 )     ; minimum TTL 1 day
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

db.cache

このファイルの選択に関しては、以下のサイトにある FTP への現在のルート・ネーム・サーバーのリストを参照してください。 *ftp://ftp.rs.internic.net/domain/named.root*

boot

```
primary public.com                  db.public
primary 150.100.50.in-addr.arpa     db.50.100.150
primary 0.0.127.in-addr.arpa        db.127.0.0
cache   .                           db.cache
```

トラフィック・フィルターに適切な DNS トラフィックを許可するよう設定するには、「**セキュリティー・ポリシー**」パネルの「*DNS 照会許可*」を使用可能にします。

例 2: 専用インターフェースの DMZ 内に DNS がある

この例では、依然として DMZ の DNS は専用ネーム・サーバー上にありますが、DMZ は非セキュア・ネットワークと同じインターフェースではなく異なるインターフェースに付加されています。

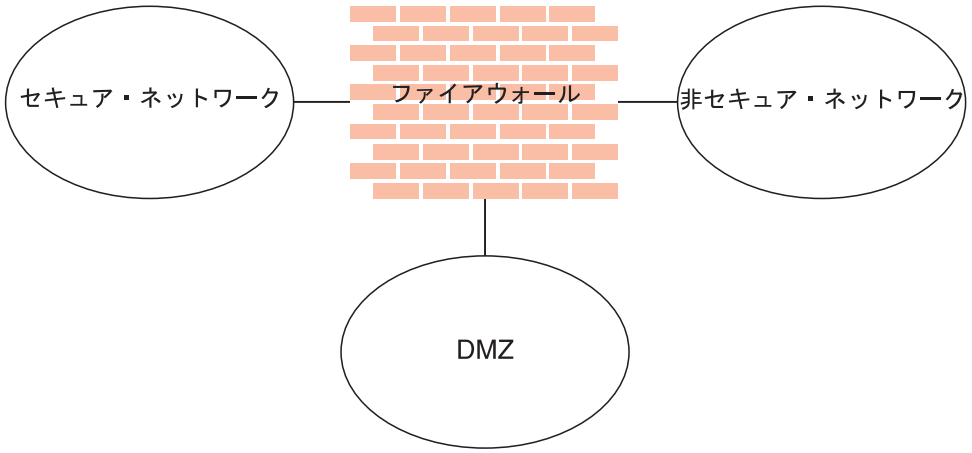

図 13. 専用インターフェース上の DMZ 内の DNS

dns.public.com 上の DNS データ・ファイルは、直前の例と同じです。このネーム・サーバーをパブリック・サーバーにアクセス可能にするためには、トラフィック・フィルターをオープンするか、ゾーン転送を実行してファイアウォールへデータ・ファイルをコピーしなければなりません。

トラフィック・フィルターをオープンするには、 *DNS サーバー照会*、*DNS 応答*、および *DNS クライアント照会* の 3 つの規則テンプレートをコピーしてください。それぞれの規則の経路指定設定を、 *local* から *routed* に変更してください。次に 3 つの新規の規則テンプレートをサービスに含め、フロー標識を以下のように設定してください。

- DNS クライアント照会: --->
- DNS 応答: <---
- DNS サーバー照会: --->
- DNS サーバー照会: <---

ソース・オブジェクトとして *The World* を、宛先オブジェクトとして *dns.public.com* を使用する接続内にこのサービスを含めます。

ゾーン転送を行うには、トラフィック・フィルターを設定し、かつ、ネーム・サーバーに対して適切なファイルをコピーするよう指示することが必要です。トラフィック・フィルターを設定するには、以下を行います。

1. 「**セキュリティー・ポリシー**」で、「*DNS 照会許可*」を使用可能にします。

2. *dns.public.com* (ソース・オブジェクト) からファイアウォールの DMZ インターフェース (宛先オブジェクト) へ接続を追加します。これには、*DNS 転送* のサービスが含まれます。

ゾーン転送を活動化するには、以下の行を、ファイアウォールの c:¥winnt¥system32¥dns 内の *boot* ファイルに追加してください。

```
secondary public.com     50.100.150.202 db.public
secondary 150.100.50.in-addr.arpa  50.100.150.202 db.50.100.150
```

次に、サービス制御マネージャーへ進み、 DNS サーバーのサービスを停止させ、再始動してください。

例 3: ファイアウォールをセキュア・ネーム・サーバーとして使用する

ファイアウォールを個人のセキュア・ネーム・サーバーとして使用するには、通常セキュア・サーバー上にあるデータベース・ファイルをファイアウォール上に配置します。こうすることでクライアントは、ファイアウォールを個人の DNS サーバーとして指し示すことができます。この方法に関係するリスクは、DNS サーバーが、セキュア側からの要求か非セキュア側からの要求かを区別できないことにあります。したがって、要望があればどのクライアントにも、このセキュア側の情報が提供されます。ユーザーは個人のセキュア DNS 情報を隠すことができなくなりました。

この方法を実行するには、構成クライアントを使用してファイアウォール DNS 機能を構成することから始めます。「セキュア・ドメイン・ネーム」フィールドに、セキュア・ネットワークで使用するドメイン・ネームをリストします。「セキュア・ネーム・サーバー」 フィールドに、ファイアウォールのセキュア・インターフェースをリストします。「*非*セキュア・ネーム・サーバー」フィールドに、個人の ISP から提供されたネーム・サーバーをリストします。次に、この構成を補足するために、ファイアウォール上で reverse-lookup ファイルを作成します。

以下の例に似たファイル c:¥winnt¥system32¥dns¥fwnamed.rev を作成します。

この例では、ファイアウォールのセキュア・インターフェース名は *fw.private.com* で、IP アドレスは *10.100.100.1* です。

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                  604800      ; expire after 1 week
                  86400 )     ; minimum TTL 1 day
1.100.100.10.in-addr.arpa.        IN NS fw.private.com.
1.100.100.10.in-addr.arpa.        IN A  fw.private.com.
```

次に、以下の行を c:¥winnt¥system32¥dns¥boot に追加します。

```
primary 100.100.10.in-addr.arpa     fwnamed.rev
```

このシナリオでは、ユーザーのクライアントは、独自の DNS サーバーとしてファイアウォール (10.100.100.1) を指示するよう構成されなければなりません。ファイアウォールは外部情報の解決とともに援助しますが、セキュア側情報の解決はありません。つまり、ファイアウォール上の構成サーバーまたはプロキシー・サーバーに接続するどのセキュア側クライアントも、ファイアウォールを、ホスト名ではなく IP アドレスで参照しなければなりません。

第7章 SafeMail

IBM Firewall SafeMail ゲートウェイには、SMTP トラフィック用のゲートウェイ機能を備えています。 IBM Firewall SafeMail ゲートウェイは、セキュア・メール・サーバーから非セキュア側へのメッセージ転送を、重要なドメインの名前を隠しながら中継します。非セキュア側からセキュア・メール・ドメインへの転送も中継しますが、その際、セキュア・ネットワークを外部の攻撃から保護します。

SafeMail は、コンテンツ・スクリーニングを実行しませんが、コンテンツ・スクリーニングを実行するユーザー出口を提供します。詳細については、41ページの『SafeMail ユーザー出口』 を参照してください。

SafeMail は、送信側から受信側へ、リアルタイムでメッセージを中継します。これにより、さまざまなリスクや、ファイアウォール上のメッセージ待ち行列の保守に関する複雑さを回避することができます。ただし、隣接するメール・ドメインに関しては、特定の構成要件が必要になります。場合によってこの要件は、特定のインストレーションに対しては有効ではないことがあります。そのような場合は、適当な SMTP サーバーを購入し、SafeMail の代わりにインストールします。 SMTP サーバーの全機能をインストールする場合は、セキュリティーが機能するように構成してください。 詳しくは、42ページの『SafeMail の代わりに SMTP を使用する』 を参照してください。

構成クライアントを用いた SafeMail の構成

SafeMail を構成するには、構成クライアント・ナビゲーション・ツリーから、「システム管理」を選択します。 「ファイル・フォルダー」アイコンをダブルクリックして、表示を拡張します。「**SafeMail**」を選択します。IBM Firewall は、構成済みのメール・サーバーおよびドメインのリストを表示します。プライベート側の構成済み各メール・ドメインごとに、 1 つの項目を構成しなければなりません。

1. ドメインを追加するには、「**新規**」を選択し、「**オープン**」をクリックします。「**メール・サーバーの追加**」ダイアログ・ボックスが表示されます。
2. 「**セキュア・ドメイン・ネーム**」フィールドには、ファイアウォールのセキュア・サイドのユーザーが、記述されるメール・ドメインを認識する際に用いる名前が入ります。
3. 「**セキュア・メール・サーバー・ネーム**」フィールドには、この項目が適用されるメール・サーバーのホスト名または小数点付き 10 進数形式の IP アドレスが入ります。このサーバーは、いずれかのセキュア・ネットワークになければなりません。 指定したドメイン 1 つにつき、1 つのメール・サーバーを記入することができます。
4. 「**パブリック・ドメイン・ネーム**」フィールドには、ファイアウォールの非セキュア・サイドのユーザーが、記述されるメール・ドメインを認識する際に用いる名前が入ります。 セキュア・ネットワークの地形を隠蔽するために、セキュア・ドメイン・ネームの代わりにこの名前が使用されます。
5. 「**了解**」をクリックします。

メール構成項目の変更

メール構成項目を変更するには、リスト内の項目を選択して、「**オープン**」をクリックします。「**メール・サーバー構成の変更**」ダイアログ・ボックスが表示されます。

「**セキュア・ドメイン・ネーム**」フィールドは使用できませんが、 39ページの『構成クライアントを用いた SafeMail の構成』 での説明のように、他のフィールドは変更することができます。

注:

1. 以前に SafeMail を構成していて、ここでセキュア・メール・サーバーを指定すると、前に構成したメール・サーバーはこのメール・サーバーによって置換されます。
2. 以前にセキュア・メール・サーバーを構成していない 場合に、ここでセキュア・メール・サーバーを指定すると、このメール・サーバーは構成に追加されます。

メール構成項目の削除

SafeMail 構成項目を削除するには、リスト内の項目を選択して、「**削除**」をクリックします。 削除の警告が表示されます。 「**了解**」をクリックして削除するか、削除をやめる場合は「**取消**」をクリックします。

セキュア・サーバーの構成

セキュア・メール・サーバーの構成では、ファイアウォールを未知のドメインに対するゲートウェイとして指定しなければなりません。こうすることで、非セキュア・ネットワーク宛てのメールがファイアウォールに送られます。また、各サーバーは、プライベート・ドメイン・ネームだけではなく公用ドメイン・ネームにアドレス指定されたメッセージも受け入れるように構成しなければなりません。ファイアウォールが非セキュア・ネットワークからの情報を転送するときは、すべての宛先が公用側のドメイン・ネームとともにリストされます。

セキュア・ネットワーク内に 2 つ以上の別個のメール・ドメインがある場合は、他のセキュア側ドメインへのメールを、ファイアウォールではなくそのサーバーに転送されるように構成しなければなりません。そうすれば、ファイアウォールの不必要な作業負荷が低減され、ファイアウォールのリアルタイムの送達機構が正常に機能します。

公用ドメインの構成

非セキュア・ネットワークに必要な構成は、ファイアウォールをネットワークのメール交換機として指定することだけです。サービス・プロバイダーに依頼して、必要な情報を DNS サーバーに追加してもらってください。関連するこれ以外の詳細なメカニズムについては31ページの『第6章 ドメイン・ネーム・サービスのハンドリング』を参照してください。

この目的は、メールを受け入れたい各パブリック・ドメイン・ネームのメール交換機 としてファイアウォールをリストすることです。たとえば、ドメイン・ネームに、セキュア・ネットワーク内では *private.com* を、セキュア・ネットワーク外では *public.com* を使用する場合、ファイアウォールは *gateway.public.com* と指定することができます。その場合は、ファイアウォールのホスト名および IP アドレスを、通常 ″A″ レコードおよび ″PTR″ レコードとともにリストされるホストとして、プロバイダーに指定してもらいます。次に、 *user@public.com* 宛てのメールを受け入れたいので、そのドメインのメール交換機として *gateway.public.com* をリストするドメイン *public.com* の MX レコードを追加するように、プロバイダーに依頼します。*user@somethingelse.com* 宛てのメールも受信する場合は、ファイアウォールも指す MX レコードを追加してリストしてください。

SafeMail ユーザー出口

SafeMail は、起きる可能性のある、処理が困難なトラフィックを拒否するためのユーザー出口を提供します。これは、インストレーション時に SafeMail を調整することで提供されます。この目的で提供される Software Developers Kit の詳細については、*IBM Firewall 解説書* を参照してください。

この機能により、*UsrCheck()* 機能を生成することができます。これは、SafeMail が送信側からパケットを受信するたびに呼び出されるものです。この機能には、システムの状態に関するいくつかのフィールドを含む構造体が渡されます。この構造体に含まれるのは、固有のセッション ID、送信および受信サーバーの IP アドレス、前に受信したコマンドの標識、および分析済みパケットを含む平文バッファーです。

この機能にインプリメントされる検査のタイプのいくつかを以下に示します。

- *禁止*されたホスト・リスト
- 許可されていない文字順序、たとえば、不適当な言語またはプロジェクト・コード・ネームなどのスキャン
- 組み込み引用符付き文字列の試験
- メッセージ長制限

必要な場合、サード・パーティー製のコンテンツ・スクリーニング・プロダクトへのインターフェースをインプリメントするために、ユーザー出口を使用することもできます。

ユーザー出口機能でメッセージを処理しないようにすると、ユーザー出口機能は SafeMail に理由コードを戻します。 SafeMail は、すぐに、送信 SMTP サーバーへの接続を拒否します。同時に、ファイアウォール・ログにはユーザー出口が戻した理由コードを含むメッセージが書き込まれます。

ユーザー出口を作成する際、この機能はパケットを受信するごとに呼び出されるということに気を付けてください。また、システムのパフォーマンスへ悪影響を及ぼさないように、できるだけ効率的に作成するように注意してください。この機能はマルチスレッド環境で実行されるので、スレッドに悪影響を与えないように作成しなければなりません。このユーザー出口は、マルチ・スレッド操作が可能で、かつ *_cdecl* 連係規則を使用できるコンパイラーで作成できます。IBM Visual Age C++ および Microsoft Visual C++ 用の Make ファイルのサンプルが用意されています。

SafeMail の代わりに SMTP を使用する

SafeMail の使用不能化

他の SMTP サーバー・プロダクトとの衝突を避けるために SafeMail を使用不能にするには、**サービス コントロール マネージャー**から SafeMail サービスを使用不能にします。 Windows の「**スタート**」メニューから、「**設定、コントロール パネル、サービス**」と選択します。スクロールして、「*IBM Firewall SafeMail* サーバー」を選択します。「**スタートアップ**」をクリックします。「**スタートアップ タイプ**」フィールドから「**使用不能**」を選択します。「**了解**」をクリックします。

SMTP サーバーの構成

SafeMail の代わりに SMTP サーバーの全機能をインストールするには、いくつかの点を考慮しなくてはなりません。このセクションでは、SafeMail と同様の機能が実行されるように SMTP を構成するために、 SafeMail のセキュリティー機能について説明します。SMTP サーバー・プロダクトによっては、 SafeMail のタスクの一部を実行できないものがあります。したがって、プロダクトの購入の際には、使用できる機能や必要とする機能をよく調べてから、購入するようにしてください。

メール待ち行列をオーバーフローさせたり破壊したりする外因がいくつかあります。メール待ち行列を使用しないで動作するフル装備のサーバーはありませんが、メール処理専用のディスク・ボリュームを使用すれば、メール待ち行列に関する危険を低減することができます。こうすることで、オーバーフローした待ち行列がファイアウォールの他の動作に影響を与える可能性を最小限に抑えることができます。

メール・サーバーにセキュア・ネットワークに関する情報を隠してもらうことも重要です。ある大きさのメールを転送する各サーバーは、SMTP の規則に従って、*Received:* というヘッダー行を挿入しなければなりません。このヘッダー行は、侵入者がセキュア・ネットワークをマップするために使用する可能性があります。 SafeMail では注釈を処理する際、このヘッダー行をすべて取り除きます。SMTP サーバーでもこれと同じ動作をするように構成してください。また、SafeMail では、プライベート側のホスト名をすべて公用ドメイン名に書き直します。これにより、ネットワークをマップするために使用される可能性のある情報がさらに除去されます。

SafeMail のサンプル・ロギング出力

SafeMail のロギング出力のサンプルを以下に示します。

```
Feb 03 13:46:11 1998 mr16n18: ICA2163i: safemaild started.

Feb 03 13:41:14 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e7a19
received from RACK3BD.
Feb 03 13:41:21 1998 mr16n18: ICA2179i: SafeMail has forwarded 215575
bytes for connection 0xd71e6118 from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:21 1998 mr16n18: ICA2178i: SafeMail session 0xd71e7a19
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:23 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e831a
received from RACK3BD.
Feb 03 13:41:36 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e901b
received from RACK3BD.
```

```
Feb 03 13:41:56 1998 mr16n18: ICA2179i: SafeMail has forwarded 215567
bytes for connection 0xd71e7a19 from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: SafeMail session 0xd71e831a
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: SafeMail session 0xd71e901b
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail has forwarded 346
bytes for connection 0xd71e901b from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail has forwarded 358
bytes for connection 0xd71e831a from 9.67.144.52 to 9.67.131.250.
```

ログ・メッセージは、以下を示します。

- ICA2177 - 新規接続の開始
- ICA2179 - 正常な終了
- ICA2178 - 受信 SMTP サーバーとの接触
- ICA2181 - SafeMail によるセッション拒否理由コードの詳細については、 *IBM Firewall 解説書* を参照してください。
- ICA2180 - セッションの終了
- ICA2182 - ユーザー出口によるセッション拒否

第8章 ファイアウォールによるトラフィックの制御

本章では、構成クライアントを用いて、ファイアウォール内でのネットワーク・トラフィックを制御する方法について説明します。 ファイアウォールは、エキスパート・フィルターを用いて、時刻、IP アドレス、およびサブネットなどの複数の基準に基づいて、セッション・レベルでパケットをフィルター処理します。フィルターは、セキュア・ネットワーク・インターフェースと非セキュア・ネットワーク・インターフェースの間で働きます。フィルターは、ファイアウォールの経路指定テーブルには影響を与えません。

デフォルトの場合は、ファイアウォールではどのトラフィックもセキュア・ネットワークと非セキュア・ネットワーク間を流れることはできません。特定のタイプのトラフィックがセキュア・ネットワークと非セキュア・ネットワーク間を流れるようにするには、接続を作成しなければなりません。

構成クライアントを用いた接続の作成

ネットワーク・オブジェクト、規則テンプレート、サービスおよび接続を作成するには、46ページの図 14 に示す構成クライアントの構成要素を使用します。

接続 ネットワーク・オブジェクトを、サービスまたは Socks テンプレート (あるいはその両方) に関連付けて、端点間で許可される通信のタイプを定義します。各接続は、送信元ネットワーク・オブジェクトと宛先ネットワーク・オブジェクト間で許可もしくは拒否される、特定のタイプの IP トラフィックを定義します。

サービス

1 つまたは複数の規則テンプレートから作成されます。送信元ネットワーク・オブジェクトと宛先ネットワーク・オブジェクト間で許可もしくは拒否される IP トラフィックのタイプを定義します。たとえば、Telnet を許可し、PING は拒否するサービスを構成することもあります。 (FTP サービスの 1 つは、8 つの規則テンプレートで構成します)。 IBM Firewall には、デフォルト・サービスのセットが付いています。 これらのプリロード・デフォルト・サービスは削除できませんが、特定のフィールドを変更することができます。しかし、これらの事前定義サービスが要件に合わない場合は、規則テンプレートを用いて新しい規則を作成して、サービスに追加することができます。詳細については、67ページの『サービスの定義』 を参照してください。

規則テンプレート

ファイアウォールに指示して、IP パケットのさまざまな属性に基づいてその可否を行わせます。

Socks テンプレート

ファイアウォール Socks デーモンに指示して、IP パケットのさまざまな属性に基づいてその可否を行わせます。

ネットワーク・オブジェクト

ファイアウォールと対話するホスト、ユーザー、サブネットなどのさまざまなネットワーク構成要素を表します。これらは IP アドレスおよびアドレス・マスクによって定義されます。したがって、 1 つのオブジェクトでネットワ

ーク・アドレスの範囲全体を表すことが可能です。ネットワーク・オブジェクトは、グループ化することができます。

ネットワーク・オブジェクト・グループ

1 つまたは複数のネットワーク・オブジェクトを表します。これらは、接続設定の便宜上使用され、繰り返し作業を排除することができます。いくつかのアドレスを 1 つのネットワーク・オブジェクト・グループにまとめて、部門を表すなどは、その例です。これで、このネットワーク・オブジェクト・グループは、接続の送信元か宛先のいずれかとして使用することができます。

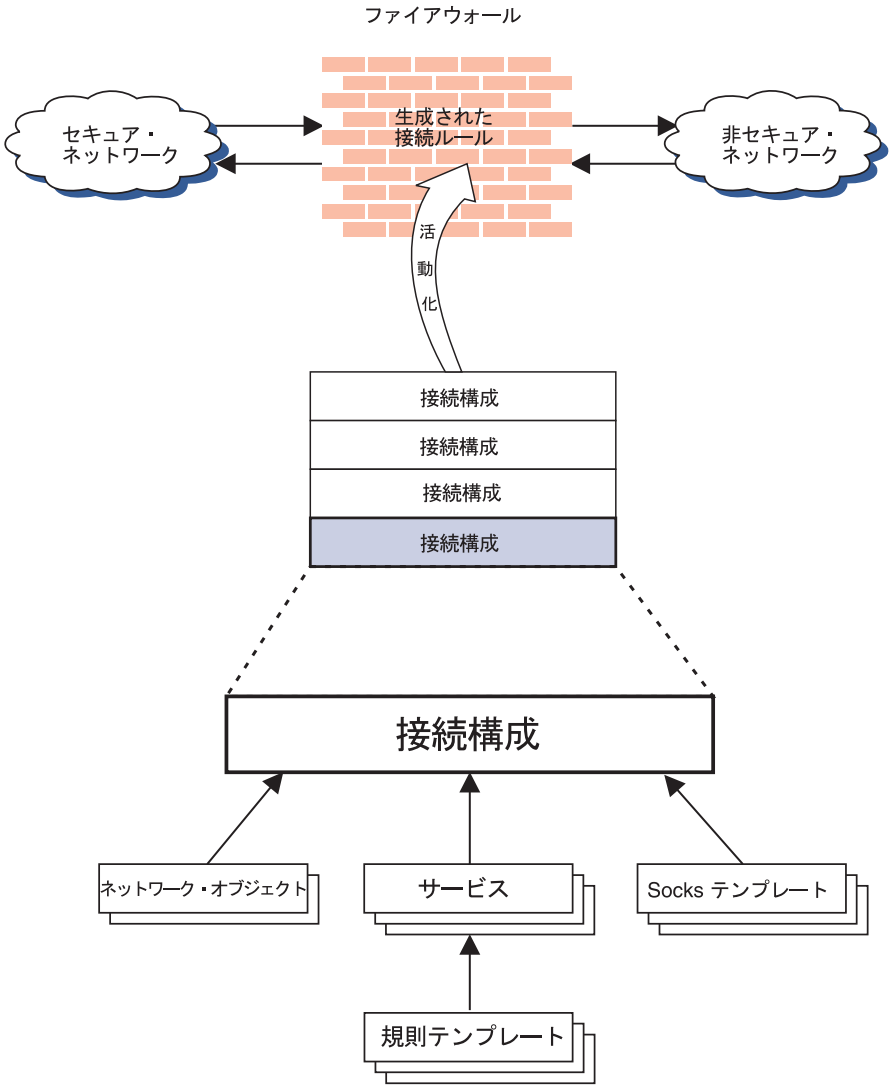

図 14. 接続の作成

事前定義サービスを用いた接続の作成

端点として利用する 2 つの名前付けされたネットワーク・オブジェクトまたはネットワーク・オブジェクト・グループ間の特定のタイプの通信を、許可もしくは拒否するためには、接続を作成する必要があります。

ネットワーク・オブジェクトを定義した後に、接続を作成します。一方のネットワーク・オブジェクトまたはグループを、ファイアウォールを通過するトラフィックの流れの送信元として選択し、他方のネットワーク・オブジェクトまたはグループを宛先として選択します。

接続を作成するには、構成クライアントのナビゲーション・ツリーから「トラフィック制御」を選択し、ファイル・フォルダー・アイコンをダブルクリックして表示を拡大します。 「**接続設定**」を選択します。「**接続リスト**」ダイアログ・ボックスが表示されます。「**新規**」を選択して、「**オープン**」をクリックします。 48ページの図 15 に示す「**接続の追加**」ダイアログ・ボックスが表示されます。

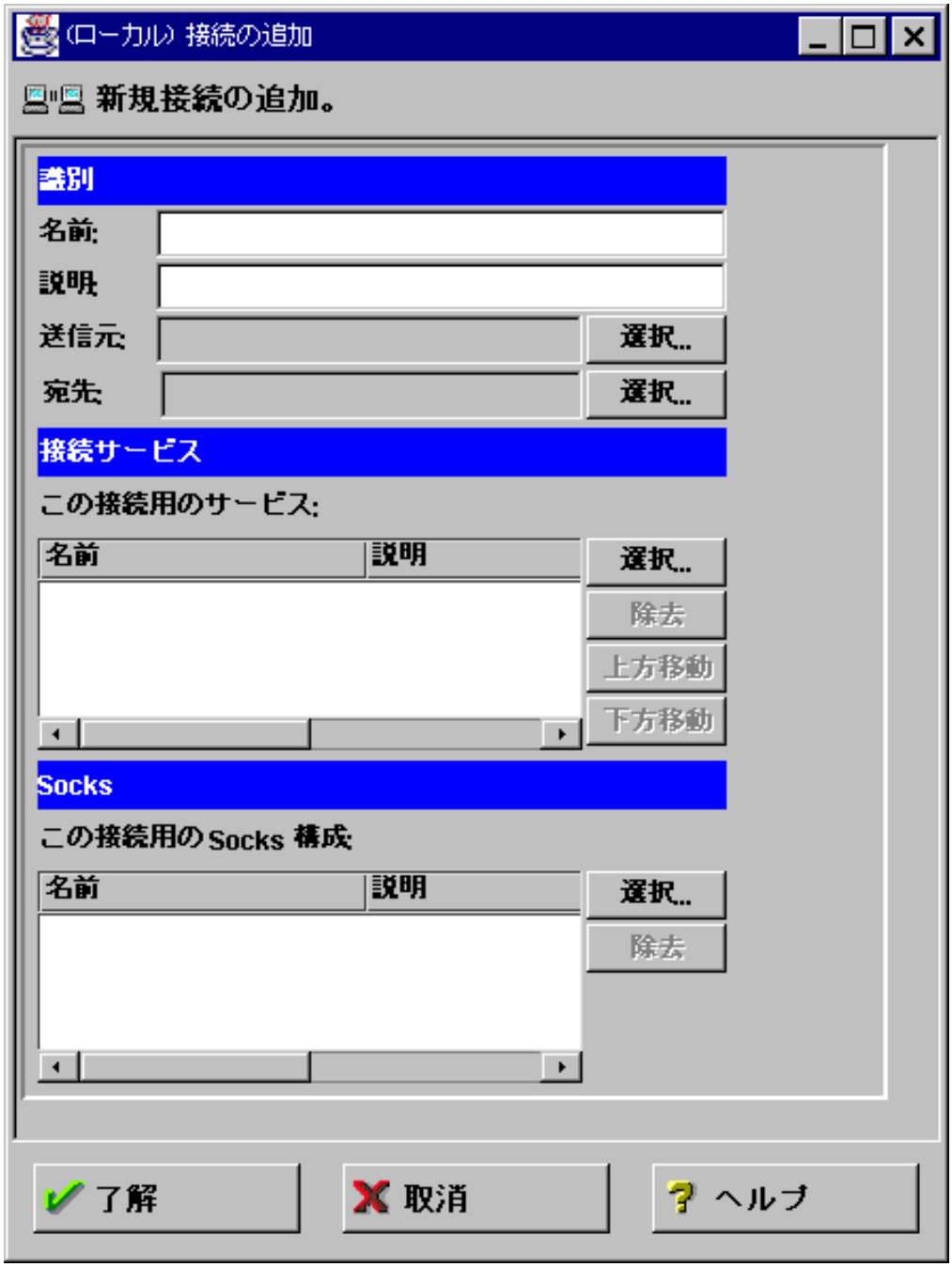

図 15. 接続の追加

1. 接続の名前を入力します。
2. 接続の記述を入力します。
3. 「送信元」フィールドでは、「**選択**」をクリックして、「**ネットワーク・オブジェクト**」ダイアログ・リストからネットワーク・オブジェクトを選びます。
4. 「宛先」フィールドでは、「**選択**」をクリックして、「**ネットワーク・オブジェクト**」ダイアログ・リストからネットワーク・オブジェクトを選びます。
5. この接続のサービスを変更するには、「**選択**」をクリックし、端点間で制御するトラフィックのタイプを選択します。

6. リストから 1 つまたは複数のサービスを選んで、接続に追加します。
7. サービスを選択し、「**上方移動**」または「**下方移動**」をクリックして、リストを並べ替えることができます。 49ページの『接続の順序付け』 を参照してください。
8. サービスは、選択して「**除去**」をクリックすると除去することができます。
9. 「**この接続用の Socks 構成**」を使用します。 Socks の接続を行うには、ステップ 5 から 7 を実行してください。
10. すべて定義した後に、「**了解**」をクリックします。
11. 接続のすべてを活動化します。 49ページの『接続の活動化』 を参照してください。

接続の順序付け

ほとんどの IBM Firewall ユーザーが持つ規則の数は、1000 未満です。規則の数が多いほど、パフォーマンスに与える影響は大きくなります。

ネットワーク・インターフェースでパケットを受信すると、ファイアウォール・ホストに入るもの、出ていくものに関係なく、生成された接続規則の先頭から規則が適用されます。パケットからの情報が正確に規則内の情報と一致する場合は、そのアクション (許可または拒否) が取られます。ファイル全体を検索しても一致が見つからない場合は、要求は拒否されます。

ヒント: 特定の接続は最上部に、特に特殊ではない接続は最下部に置いてください。たとえば、アドレスが (1.1.10.X) の部門 ABC と、部門 ABC の内部のサーバーとして使用する、アドレスが (1.1.10.7) のマシンを持つ場合があります。マシン (1.1.10.7) を Telnet トラフィックに使用してはならないサーバーであるために除外したい場合は、接続:`Deny telnet for Dept ABC server` を接続:`Permit telnet for Dept ABC` の前に置かなければなりません。接続の順序を逆にすると、接続の拒否が検出されることはありません。

接続の活動化

注: 接続を活動化する前に、セキュア・インターフェースが定義されているか確認してください。

次のどれを行う場合も、構成クライアントのナビゲーション・ツリーから、「**接続の活動化**」を選択してください。

接続規則の再生成と活動化
ファイアウォールは、生成された接続規則を接続構成から作成して、その規則セットを活動化します。

接続規則の活動停止
ファイアウォールは、以後デフォルトの規則によって保護されます。

現行接続規則のリスト
最新の接続規則セットが表示されます。これらの規則を事前に活動停止すると、使用されなくなります。

規則生成の検査
作成した規則は、有効か無効のどちらかです。

接続規則ロギングの使用可能
ファイアウォールは、選択されたトラフィックをファイアウォール・ログ機能に記録します。

接続規則ロギングの使用不可
ファイアウォールのロギングを停止します。

50ページの図 16 に示す、「**接続の活動化**」ダイアログ・ボックスが表示されます。

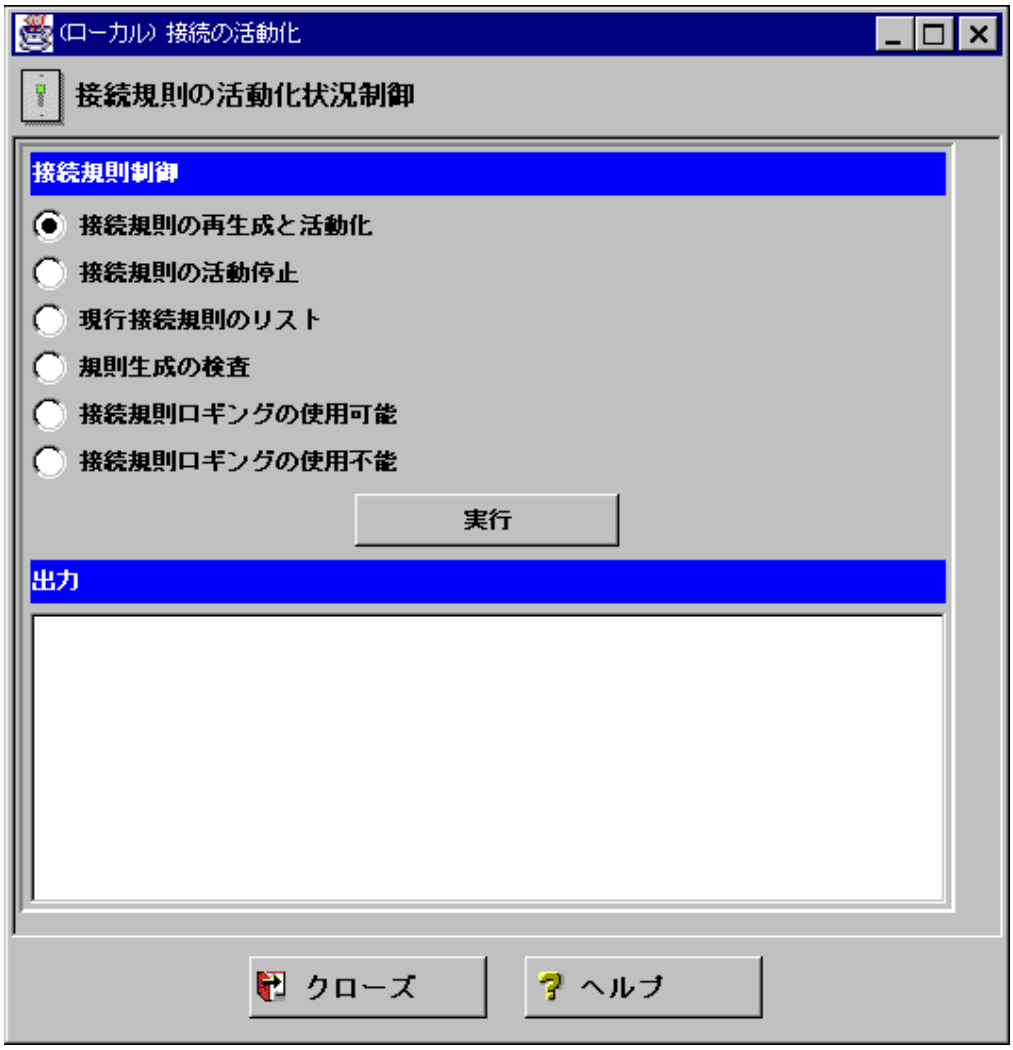

図 16. 接続の活動化

選択を行ったら、「**実行**」をクリックします。

接続規則の再生成および活動化を行ったときのロギング出力のサンプル

接続規則を再生成して活動化したときのロギング出力のサンプルを以下に示します。

```
Feb 03 13:46:53 1998 mr16n18: ICA9037i: Firewall interfaces being updated
automatically on Tue Feb  3 13:46:53 1998.

Feb 03 13:46:55 1998 mr16n18: ICA1032i: Filter rules updated at
13:46:55 on Feb-03-1998

Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp gt  1023 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 gt  1023 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:4 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp     gt  1023 eq 25 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:5 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp/ack eq  25 gt 1023 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:6 permit 9.67.144.49 255.255.255.240
9.67.130.154 255.255.248.0 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:7 permit 9.67.130.154 255.255.248.
0 9.67.144.49 255.255.255.240 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:8 permit 9.67.144.49 255.255.255.240
9.67.131.250 255.255.255.255 tcp     gt  1023 eq  21 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:9 permit 9.67.131.250 255.255.255.255
9.67.144.49 255.255.255.240 tcp/ack eq  21 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:10 permit 9.67.131.250 255.255.255.
255 9.67.144.49 255.255.255.240 tcp     eq  20 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:11 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp/ack gt  1023 eq  20 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:12 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp     gt  1023 gt  1023 secure local inbound
l=n f=y t=0 e=none a=none
.
.
.
Feb 03 13:46:58 1998 mr16n18: ICA1037i: #:100 deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
all any 0 any 0 both both both l=y f=y t=0 e=none a=none
```

規則状態の判別

IBM Firewall の規則は、次のいずれかの状態になります。

1. 構成がアクティブではありません。

   構成クライアントを用いて構成を活動化していないか、構成を活動停止しています。これは、最初に IBM Firewall をインストールし、システムをブートするか、フィルター規則を活動停止したときの構成の状態です。ファイアウォールを最初にインストールしたとき、デフォルト・フィルターがネットワークを侵入から保護するのに適した状態にあります。

   ファイアウォール・アクセス:

   - デフォルト・フィルター構成では、すべてのローカル・インバウンド・トラフィックおよびすべてのアウトバウンド・トラフィックが許可されます。

2. 構成はアクティブですが、エラーがあります。

   構成を活動化しました。構成にエラーがあるか (無効な規則)、何も構成されていません。活動化の「出力」ウィンドウで、エラーおよび警告が表示されます。

   ファイアウォール・アクセス:

- すべてのローカル・インバウンド・トラフィックを許可します。
- すべてのアウトバウンド・トラフィックを許可します。

3. 構成はアクティブで、かつ有効です。警告にはいくつかあり、最も顕著なのは、フィルター規則の重複であることに注意してください。

   構成クライアントのトラフィック制御セクションを用いて定義した構成が活動化しました。

   注: 構成ファイルは有効でも、まだ規則が入っていないことがあります。この場合は、暗黙の「すべてのアクセスを禁止」規則が効力を持ちます。

   ファイアウォール・アクセス:

   - 構成ファイルによって判別されるアクセス。

     あらゆるネットワーク・インターフェースにより受信されるか、これから送信される各パケットは検査され、その内容は生成された接続規則内の各規則と比較されます。一致が検出された場合、その規則上のアクション (アクセスの許可または拒否) が実行されます。
   - パケットと一致する規則がない場合でも、アクセスを拒否する暗黙の「すべてを禁止」規則が実行されます。

第9章 サービスの例

本章では、ファイアウォールを構成して、所定の共通作業を行う方法について説明します。リストされているタスクは、単なる例に過ぎませんが、これらを理解すれば、ファイアウォールを構成して、提供されたサービスをすべて使用することができるはずです。

計画に関する考慮事項

ファイアウォールのトラフィック制御は、端点の対の間で許可または禁止される通信のタイプを定義する、接続の観点から編成されます。したがって、接続の計画を、これらの端点の観点から行うことが重要です。

45ページの『第8章 ファイアウォールによるトラフィックの制御』 での説明のように、端点はネットワーク・オブジェクトによってファイアウォールに対して表されます。7ページの『第2章 計画』のネットワーク計画ワークシートにまだ記入していない場合はそれを記入し、ネットワークを表すのに必要なネットワーク・オブジェクトを作成します。

本章の例では、以下のネットワーク・オブジェクトを使用しています。

セキュア・インターフェース
ファイアウォールのセキュア・インターフェース

非セキュア・インターフェース
ファイアウォールの非セキュア・インターフェース

セキュア・ネットワーク

ファイアウォールのセキュア・インターフェースを介してアクセス可能なアドレスの範囲。これは、いくつかの個別のドメイン (それぞれはその独自のネットワーク・オブジェクトによって表される) を含む、ネットワーク・オブジェクト・グループであっても構いません。

The World
非セキュア・ネットワーク。

それぞれ望まれるタイプの通信は、関係する端点間通信の観点から描かれなければなりません。この段階では、ファイアウォールがこれらの通信の代理をするのかどうか、あるいはこれらの通信の経路指定をするのかについて考えます。

ファイアウォールがプロキシーとして作動する場合、ファイアウォールはセキュア・ユーザーに代わって必要な作業を行い、非セキュア・ホストはセキュア・ホストが存在するのを知ることはありません。ファイアウォールがトラフィックを経路指定する場合、セキュア・ホストと非セキュア・ホストは相互に直接通信します。

ファイアウォールをプロキシーとして使用する場合は、54ページの図 17 が示すように、通信の端点にはファイアウォールが組み込まれます。

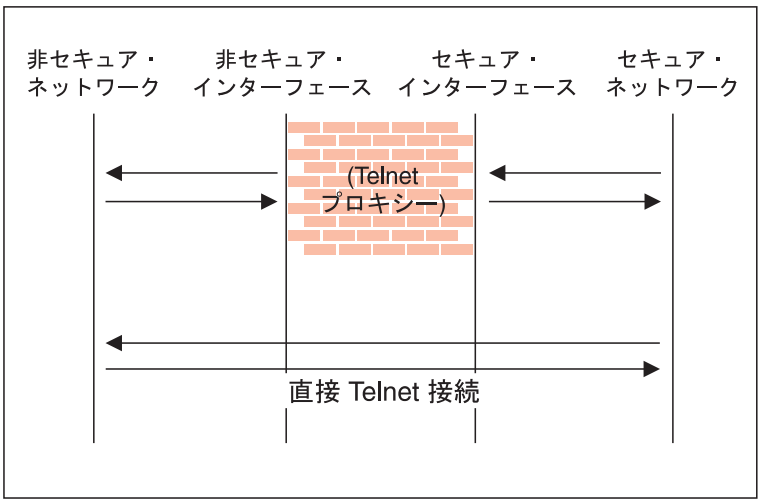

図 17. Telnet プロキシーおよび直接の Telnet 接続

Telnet プロキシーの例

この最初の例は、直接のアウトバウンド Telnet プロキシー接続の例です。この例で、セキュア・ネットワークのユーザーは、ファイアウォールの Telnet プロキシーを用いて、非セキュア・ネットワーク内のホスト上の Telnet サービスにアクセスすることができます。

54ページの図 17 に示すように、2 つの接続が発生します。

1. セキュア・ネットワーク内部のクライアントは、ファイアウォールの Telnet プロキシーに接続されています。
2. ファイアウォールの Telnet プロキシーは、セキュア・ユーザーに代わって、非セキュア・ネットワーク内のホストに接続されています。

この通信用にファイアウォールのトラフィック制御を構成するには、2 つの接続を設定する必要があります。

表 1. Telnet プロキシー

セキュア・オブジェクト	宛先オブジェクト	必要なサービス
セキュア・ネットワーク	セキュア・インターフェース	Telnet Proxy out 1/2
非セキュア・インターフェース	The World	Telnet Proxy out 2/2

フィルター処理された Telnet の例

上記の例と簡易フィルター処理された Telnet 接続を対比します。この場合、セキュア側のクライアントは、非セキュア側のホストに直接接続します。

表 2. フィルター処理された Telnet

セキュア・オブジェクト	宛先オブジェクト	必要なサービス
セキュア・ネットワーク	The World	Telnet direct out

前述したとおり、この構成では、非セキュア・ホストに接続する際、セキュア・クライアントのアドレスは公開されることになります。

プロキシー HTTP の例

大部分のインストール先では、そのセキュア・クライアントのいくつかで Web サーフィンができるようにしたいことでしょう。 IBM Firewall には、事前定義の HTTP アウトバウンド・ダイレクト・サービスがあり、経路指定 HTTP が可能です。これは、フィルター処理された Telnet の例と全く同じように機能します。さらに、Firewall は HTTP プロキシーを備えています。

HTTP プロトコルは、他のプロトコルをカプセル化する点で、Telnet と異なります。簡単なサーフィンの場合でさえ、ほとんどのユーザーは、HTTP だけでなく、 FTP サービスも必要です。 Gopher および WAIS は使用頻度が低いといえども、HTTP の全機能を提供するために許可されるべきです。

しかし、これらの追加プロトコルは、使用される際に、クライアントとプロキシー間の HTTP で循環するので注意してください。したがって、通信は、55ページの図 18 のダイアグラムのようになります。

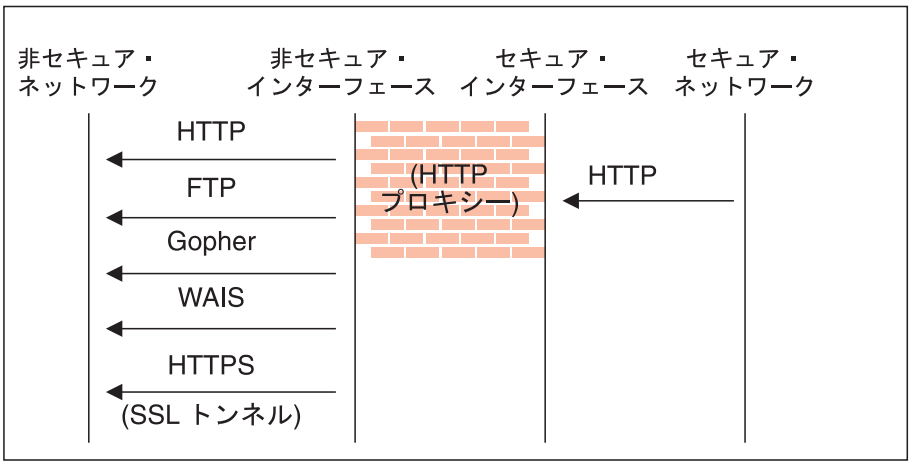

図 18. プロキシー HTTP

関係する端点は 2 組あるので、2 つの接続をコード化しなければなりません。

表 3. プロキシー HTTP

セキュア・オブジェクト	宛先オブジェクト	必要なサービス
セキュア・ネットワーク	セキュア・インターフェース	HTTP proxy outbound 1/2

表 3. プロキシー HTTP (続き)

セキュア・オブジェクト	宛先オブジェクト	必要なサービス
非セキュア・インターフェース	The World	以下から選択... • HTTP proxy out 2/2 • FTP proxy out 2/2 • Gopher proxy out 2/2 • WAIS proxy out 2/2 • HTTPS proxy out 2/2

HTTP プロキシーの詳細については、91ページの『第13章 プロキシー・サーバーの構成』 を参照してください。

Socks の例

Socks デーモンが多様なプロトコルを処理し、プロトコルをファイアウォールとクライアント間の単一のデータ・ストリームにカプセル化するという点で、Socks は、HTTP プロキシーの場合と同様の課題があります。 Socks が HTTP プロキシーより柔軟性がある理由は、どのような TCP または UDP ベースのプロトコルにも対応できる点と、ファイアウォールをフィルターとは別個に構成し、通信の制御性を高めることができる点です。

この柔軟性が加わったことにより、Socks の構成には、 HTTP プロキシーで説明した接続に加えて 3 番目の接続が必要になります。 2 つの基本接続によってパケットはファイアウォールとの間を流れることができます。3 番目の接続は、Socks デーモンに、パケットを受け取ったら、リクエストのプロキシーを務めるよう指示するために必要です。

表 4. Socks

セキュア・オブジェクト	宛先オブジェクト	必要なサービス
セキュア・ネットワーク	セキュア・インターフェース	Socks 1/2
非セキュア・インターフェース	The World	以下から選択... • HTTP proxy out 2/2 • FTP proxy out 2/2 • Telnet proxy out 2/2 (サポートする任意のプロキシー・サービス 1/2)
セキュア・ネットワーク	The World	「Socks 構成」ウィンドウでは、以下から選択... • permit socksified HTTP • permit socksified FTP • permit sockisfied Telnet

もちろん、セキュア・ネットワーク内部のクライアントは、Socks 化し、ファイアウォールを Socks サーバーとして使用するように構成しなければなりません。

Socks の詳細については、71ページの『第11章 Socks サーバーの構成』 を参照してください。

DNS についてのヒント

DNS 解決を指定しないと、効率的な通信はほとんどできません。 DNS の構成については、31ページの『第6章 ドメイン・ネーム・サービスのハンドリング』 を参照してください。セキュリティー・ポリシーの「DNS 照会許可」を必ず使用可能にしてください。

非セキュア Socks クライアントについてのヒント

「セキュリティー・ポリシー」パネルには、「**非セキュア・インターフェースへの Socks の禁止**」のチェックボックスが入っています。このサービスにより、すべての非セキュア・インターフェースから Socks デーモンに宛てられるパケットをすべて拒否し、ファイアウォールをより安全なものにします。

クライアントに、非セキュア・ネットワークから自分のネットワークに入ることを許可したい場合、 このチェックボックスをオンにしてはいけません。

第10章 トラフィック制御のカスタマイズ

本章は、フィルター規則およびサービスの定義に役立ちます。 サービスとは、たとえば Telnet セッションのように、ファイアウォールを介して特定のタイプのトラフィックを許可したり、拒否したりする規則の集合もしくは、命令のセットのことです。規則テンプレートを用いて新規規則を作成して、サービスに追加することができます。サービスは、削除することもできます。 Socks サービスは、Socks 化した接続に適合します。

IBM Firewall には、サービスのデフォルト・セットがプリロードされています。事前定義サービスを特定の要求に合わせて変更することも、新規サービスを作成することもできます。

構成クライアントを用いた規則テンプレートの作成

この手順は、新規規則を使用可能な規則テンプレートのリストに追加するのに使用します。

1. 構成クライアントのナビゲーション・ツリーから、「トラフィック制御」を選択して、ファイル・フォルダー・アイコンをダブルクリックします。「**接続テンプレート**」を選択してから、「**規則**」を選択します。
2. 「**規則リスト**」ダイアログ・ボックスで、「**新規**」をダブルクリックします。

   IBM Firewall が、60ページの図 19 に示す「**IP 規則の追加**」ダイアログ・ボックスを表示するので、規則を定義することができます。

図 19. IP 規則の追加

3. 規則名を入力します。
4. 規則の説明を入力します。このフィールドは任意選択です。
5. 「処置」の矢印をクリックし、ファイアウォールへのアクセスの可否を選びます。
6. 「プロトコル」の矢印をクリックし、以下のリストから項目を選択します。

   すべて すべてのプロトコルがこの規則に一致します。

   tcp この規則に一致するためには、パケット・プロトコルは TCP でなければなりません。

   tcp/ack
   この規則に一致するためには、パケット・プロトコルは肯定応答を指定した TCP でなければなりません。

   udp この規則に一致するためには、パケット・プロトコルは UDP でなければなりません。

icmp この規則に一致するためには、パケット・プロトコルは ICMP でなければなりません。

ospf この規則に一致するためには、パケット・プロトコルは OSPF (Open Shortest Path First) プロトコルでなければなりません。 OSPF をプロトコルとして指定すると、発信元ポート演算と発信元ポート値が OSPF レコード・タイプ値に使用されます。フィルター処理は、OSPF タイプに対しても実行できます。値のタイプは「**any**」と指定することができます。「宛先ポート」フィールドは、「**any 0**」と指定しなければなりません。それ以外はすべて無視されます。

ipip この規則に一致するためには、パケット・プロトコルは IPIP プロトコル (IP-in-IP) でなければなりません。 IPIP を指定すると、「ポート」フィールドは「**any 0**」と指定する必要があります。

esp この規則を満たすためには、パケット・プロトコルはカプセル化 IP パケットを送信するための仮想的な専用ネットワークが使用する、カプセル化セキュリティー・プロトコルでなければなりません。

ah 認証ヘッダー・プロトコルは、関連する認証トークンを持つ IP パケットを送信するための、仮想的な専用ネットワークが使用するパケット・プロトコルです。

7. 数値プロトコルにより、その10 進値 (RFC-1700 による) を用いてプロトコルを指定する ことができます。有効値は、1 から252 の範囲です。このオプションを使用する場合は、この規則の「ポート」フィールドを「0」 (任意のポートの指定) と指定する必要があることに注意してください。全プロトコルのリストについては、RFC-1700 を参照してください。あるいは、ブラウザーによって IANA (Internet Assigned Numbers Authority) に直接アクセスして参照することもできます。
8. 演算とポート番号オペランドは、一緒に使用されます。パケットのポート番号 (宛先または送信元) と、送信元ポート番号オペランドおよび宛先ポート番号オペランドの間の関係を記述する送信元および論理演算です。たとえば、パケット宛先ポートがポート 20 で、宛先演算子と宛先ポート番号が 『ge 15』 ならば、パケットは一致します。(20 は 15 以上であるため)。

   送信元または宛先オペレーションに「**any**」を指定すると、フィルターはポート番号を調べません。どのポートも一致するからです。この場合、ポート番号は変更することができません。

   ICMP プロトコルの場合は、送信元ポートを指定するのではなく、 ICMP タイプを指定し、また、宛先ポートの代わりに ICMP コードを指定します。指定された論理演算子は、タイプまたはコードに適用されます。また、ポート用に指定された演算子「any」はタイプまたはコード、またはその両方の値が規則と一致することを意味しています。この場合、ポート番号は変更することができません。

   オペレーションの値を以下に示します

   - Any
   - Equal to (等しい)
   - Not equal to (等しくない)
   - Less than (〜より小さい)

- Greater than (～より大きい)
- Less than or equal to (～より小さいか、または等しい)
- Greater than or equal to (～より大きいか、または等しい)

次に、保護すべき、さらに重要なポートをいくつか示します。ポート番号の値は、1 から 65535 までの範囲内でなければなりません。

ポート 使用対象

20 FTP データ

21 FTP 制御

23 Telnet

25 メール

53 ドメイン・ネーム・サーバー

70 Gopher

80 HTTP

111 RPC

161 SNMP

1080 Socks

次に ICMP のタイプとコードをいくつか示します。

タイプ コードおよび説明

0 0 - PING 応答

8 0 - PING 要求

3 1 - 到達不能ホスト

3 3 - 到達不能ポート

5 1 - ホストへのリダイレクト

9. 「**インターフェース**」の矢印をクリックし、インターフェース (アダプター) のタイプを選択します。

   両方 セキュア・インターフェースか非セキュア・インターフェース上で送受信するパケット用

   セキュア
   セキュア・インターフェース上で送受信するパケット用

   非セキュア
   非セキュア・インターフェース上で送受信するパケット用

   特有 インターフェースに名前を割り当てている場合は、インターフェースの選択時にインターフェース名フィールドで使用

10. インターフェース・タイプで「特有」を選ぶと、「名前」フィールドに特定インターフェースのタイプが表示されます。
11. 希望する経路指定をクリックします。

    両方 すべてのトラフィックに適用します。

ローカル

パケットがファイアウォール・ホストに対してローカルであることを暗黙指定します。つまり、

- 着信ローカル・パケットとは、インターフェースで受信され、宛先はこのファイアウォール・ホストになっているパケットです。このパケットは、別のホストに経路指定されることはありません。宛先はローカルです。
- 出力パケットは、インターフェースから送信されますが、ファイアウォール・ホストが発信元です。このパケットの発信元はローカルです。

経路指定

パケットがファイアウォール・ホストによって経路指定されることを暗黙指定します。つまり、

- 着信ローカル・パケットとは、インターフェースで受信され、宛先はその他のホストになっているパケットです。このパケットは、ファイアウォール上にとどまりません。このパケットの宛先はリモートです。
- 出力パケットは、インターフェースから送信され、その他のホストが発信元です。このパケットの発信元はリモートです。

12. 希望する方向をクリックします。

両方 選択されたインターフェースとの間で送受信するパケット用

インバウンド

ネットワークから選択したインターフェースに入ってくるパケット用

アウトバウンド

選択したインターフェースからネットワークに出ていくパケット用

13. 「ログ制御」フィールドに「はい」を選ぶと、その規則に一致するあらゆるパケットが、優先順位「**エラー**」で**ファイアウォール・ログ**に記録されます。このパラメーターを指定しないと、デフォルトは「いいえ」になります。

14. 「**断片化制御**」の矢印をクリックし、希望する断片化制御を選択します。断片化制御の指定規則と一致する IP パケット情報の場合、制御は次のように解釈されます。

はい 規則は断片化ヘッダー、断片および非断片と一致します。断片の場合、ポート情報は無視され、一致とみなされます。

専用 断片と断片化ヘッダーだけが一致します。断片化ヘッダーの場合、ポート情報も一致する必要があります。断片の場合は、ポート情報は無視されます。

いいえ 非断片だけが一致します。断片化ヘッダーと断片はこのパラメーターにより除外されます。

ヘッダー

非断片と断片化ヘッダーだけが一致します。断片はこのパラメーターにより除外されます。

このパラメーターを指定しないと、″許可″ 規則および ″禁止″ 規則の両方のデフォルトは、「はい」になります。

注: この制御の設定に関係なく、オフセットが 1 に指定された IP 断片は廃棄されます。この処置により、一般的に知られているパケット断片化を使用した攻撃で TCP ヘッダー・フラグが上書きされるのを防ぎます。

パケット・ヘッダーが、定義された IP 規則と一致するためには、パケット情報が、コード化された規則で指定されたパラメーターのすべてと一致しなければなりません。たとえばパケット断片の場合、ポート情報を除くすべてのパラメーターが一致を判別するために使用されます。

「はい」または「専用」を指定している前の規則によって断片化が許可されなかった場合は、常に規則ファイルの最下部に追加される最後の規則によって、パケット断片が拒否されます。

IP 規則構成項目の変更

作成した IP 規則を変更するには、次のようにします。

1. 「**規則リスト**」の既存の規則をダブルクリックします。「**IP 規則構成の変更**」ダイアログ・ボックスが表示されます。
2. 59ページの『第10章 トラフィック制御のカスタマイズ』 での説明のように該当するフィールドを変更し、「**了解**」をクリックして、変更を行います。

規則構成項目の削除

規則を削除するには、「**規則リスト**」から規則を選択して、「**削除**」をクリックします。

事前定義サービス

IBM Firewall には、サービスのデフォルト・セットがプリロードされています。 サービスとは、たとえば Telnet セッションのように、ファイアウォールを介して特定のタイプのトラフィックを許可したり、拒否したりする規則の集合もしくは、命令のセットのことです。規則テンプレートを用いて新規規則を作成して、サービスに追加することができます。

プリロードされているデフォルト・サービスを、以下に示します。

All non-secure
: 非セキュア・インターフェースを通過するすべてのトラフィックを拒否します

All permit
: すべてのトラフィックを許可します (デバッグ目的に限定)

All permit, in one direction
: すべてのトラフィックを許可します (デバッグ目的に限定)

All secure
: セキュア・インターフェースを通過するすべてのトラフィック拒否します (セキュリティー違反の場合)

All shutdown
すべてのパケットを拒否します (シャットダウンまたはデバッグ)

Anti Spoofing
セキュア送信元アドレスのインバウンド非セキュア・パケットを拒否します

Broadcasts
非セキュア・インターフェースへのブロードキャスト・メッセージを拒否します

Config Client non-secure
非セキュア・ネットワークからの構成クライアントの使用を許可します

Config Client secure
セキュア・ネットワークからの構成クライアントの使用を許可します

CU-SeeMe
デフォルト・ポート 7649 および 7648 上の CU-SeeMe Video

DNS queries
(セキュリティー・ポリシー) が DNS 照会を許可します

DNS transfers
DNS ゾーン転送を許可します (2 次ネーム・サーバーの場合)

Domain Controller Authentication
ユーザー認証用のドメイン制御装置に使用を許可します

FTP proxy in 1/2
非セキュア・ネットワークからファイアウォールへの FTP インバウンドを許可します

FTP proxy in 2/2
ファイアウォールからセキュア・ネットワークへの FTP インバウンドを許可します

FTP proxy out 1/2
セキュア・ネットワークからファイアウォールへの FTP アウトバウンドを許可します

FTP proxy out 2/2
ファイアウォールから非セキュア・ネットワークへの FTP アウトバウンドを許可します

Gopher proxy in 2/2
ファイアウォールからセキュア・ネットワークへの gopher を許可します

Gopher proxy out 2/2
ファイアウォールから非セキュア・ネットワークへの gopher を許可します

HTTP deny non-secure
非セキュア・インターフェースへの HTTP を拒否します

HTTP direct out
セキュア・ネットワークから非セキュア・ネットワークへの直接の HTTP を許可します

HTTP proxy in 2/2
ファイアウォールからセキュア・ネットワークへの HTTP を許可します

HTTP proxy out 1/2
セキュア・ネットワークからファイアウォールへの HTTP (ポート 8080) を許可します

HTTP proxy out 2/2
ファイアウォールから非セキュア・ネットワークへの HTTP を許可します

HTTPS direct out
セキュア・ネットワークから非セキュア・ネットワークへの HTTPS (SSL) を許可します

HTTPS proxy out 2/2
ファイアウォールから非セキュア・ネットワークへの HTTPS (SSL トンネル) を許可します

IDENTD
Socks プロトコルのユーザー ID を許可します

Mail (セキュリティー・ポリシー) がファイアウォールを介したメール・トラフィックを許可します

NetBT Name Services broadcasts
NetBIOS over TCP/IP ネーム・サービス同報通信を許可します

Ping セキュア・ネットワークからの任意の場所へのアウトバウンド PING を許可します

SDI authentication
セキュア・ネットワークの SecurID ACE サーバーへの接続を許可します

Socks 1/2
セキュア・ネットワークからファイアウォールへの Socks の使用を許可します

Socks deny non-secure
非セキュア・アダプターからの Socks を拒否します

Socks in 1/2
非セキュア・ネットワークからファイアウォールへの Socks の使用を許可します

Telnet direct out
セキュア・ネットワークから非セキュア・ネットワークへのアウトバウンド Telnet を許可します

Telnet proxy in 1/2
非セキュア・ネットワークからファイアウォールへのインバウンド Telnet を許可します

Telnet proxy in 2/2
ファイアウォールからセキュア・ネットワークへのインバウンド Telnet を許可します

Telnet proxy out 1/2
セキュア・ネットワークからファイアウォールへのアウトバウンド Telnet を許可します

Telnet proxy out 2/2
ファイアウォールから非セキュア・ネットワークへのアウトバウンド Telnet を許可します

VDOLIVE Direct In
セキュア・サーバーへ向かう非セキュア・クライアントを許可します

注意:個別のプレーヤーの特性は、UDP ポート 7001 だけが使用されるように構成しなければなりません。

VDOLIVE Direct Out
非セキュア・サーバーに向かうセキュア・クライアントを許可します

WAIS proxy in 2/2
ファイアウォールからセキュア・ネットワークへの WAIS (z39.50) を許可します

WAIS proxy out 2/2
ファイアウォールから非セキュア・ネットワークへの WAIS (z39.50) を許可します

サービスの定義

規則 (1 つまたは複数) を定義した後は、サービスに規則 (1 つまたは複数) を追加する必要があります。構成クライアントのナビゲーション・ツリーから「トラフィック制御」を選択し、「接続テンプレート」をダブルクリックしてから、「サービス」を選択します。「サービス・リスト」ダイアログ・ボックスが表示されます。「新規」をダブルクリックすると、68ページの図 20 に示すような「サービスの追加」ダイアログ・ボックスが表示されます。

図 20. サービスの追加

構成クライアントを用いたサービスの作成

1. サービス名を入力します。
2. 説明を入力します。

3. 「**ログ制御の上書き**」フィールドでは、このサービス用に選択された規則テンプレートのログ制御設定値を指定変更することができます。たとえば、ログ制御を通常は「いいえ」に設定している規則テンプレートのセットを組み込む場合は、このサービスのために、この設定値を「はい」に指定変更することができます。この設定値の指定変更は、このサービスの規則全体に働きます。「**ログ制御の上書き**」フィールドでは、次のいずれかの選択項目を入力します。
   - 上書きなし - 指定変更は無効になり、規則自体の設定値をそのまま適用する。
   - はい - このサービスのすべての規則が一致したときに、ログ・レコードを書き込む。
   - いいえ - このサービスのすべての規則が一致したときに、ログ・レコードを書き込まない。

   ログ・レコードがフィルター規則用に書き込まれる場合は、ログ・レコードに示されている値が IP パケットからの実際の値になります。一致したフィルター規則をログに記録すると、たとえば、実際のプロトコルやポート番号などの、ファイアウォールが調べる、IP パケットの内容に関する貴重な情報を得ることができます。
4. 「**断片化制御の上書き**」フィールドでは、このサービス用に選択された規則テンプレートの断片化制御の設定値を指定変更することができます。たとえば、断片化制御を通常は「いいえ」に設定している規則テンプレートのセットを組み込む場合は、このサービスのためにこの設定値を「はい」に指定変更することができます。この設定値の指定変更は、このサービスの規則全体に働きます。「断片化制御の上書き」フィールドでは、次のいずれかを入力します。
   - 上書きなし - 指定変更は無効になり、規則自体の設定値をそのまま適用する。
   - はい - 任意の IP パケット、たとえば、非断片、断片化ヘッダーおよびヘッダーなしの断片と一致する。
   - いいえ - 非断片・パケットのみと一致。断片化ヘッダーまたはヘッダーなし断片とは一致しない。
   - 専用 - 断片化ヘッダーおよびヘッダーなし断片のみと一致する。非断片とは一致しない。
   - ヘッダー - 非断片および断片化ヘッダーのみと一致する。ヘッダーなし断片とは一致しない。
5. 時刻制御によって、時刻範囲を各サービスに関連付けることができます。したがって、このサービスは、指定した時間枠でのみ有効です。サービスに時刻の指定がない場合、そのサービスは常に有効です。

   Control by Time of Day (時刻による制御)

   一日の開始時刻と終了時刻によってこのサービスを活動化または活動停止させたい場合に選択します。 24 時間形式を使用します。このフィールドを使用可能にしなければ、Time of Day フィールドは 1 日 24 時間有効です。

   Control by Days (日による制御)

   週またはカレンダー日に基づくスケジュールによってこのサービスを活動化または活動停止させる場合に選択します。このサービスを活動化するか、活動停止するかは、「時間制御処理」フィールドの値により異なるので注意してください。

Time Control Action (時間制御処理)

このサービスを指定した時間の間活動化する場合は、「**指定した時間の間、サービスを活動化**」を選びます。このサービスは、指定した時間以外の間は活動停止になります。

このサービスを指定した時間の間活動停止する場合は、「**指定した時間の間、サービスを活動停止**」を選びます。このサービスは、指定した時間以外の間は活動停止されます。

6. 「**選択**」をクリックして、このサービスを構成する規則を選びます。
7. 「フロー」トグルを用いて、接続の送信元と宛先の値を規則ベース・ファイルに書き込む際に、それらをフィルターに割り当てる方法を決めます。

```
---> Left to Right indicates that the Source and Destination of the
     Connection gets written directly to the rule as it is written
     to the Rule Base File.

<--- Right to Left indicates that the Source and Destination of the
     Connection gets reversed when it is written to the Rule Base
     File.
```

8. パケットを受信すると、IBM Firewall はパケット内の情報と規則構成ファイル内の規則との比較を、ファイルの先頭から開始します。最初の一致が検出された時点で比較は終了し、規則内に組み込まれたアクションが実行されます。

   一連の規則をサービスに追加すれば、規則の順序を変更することができます。「**サービス・オブジェクト**」リストから規則を選択し、「**上方移動**」または「**方向移動**」ボタンをクリックして、規則の位置を変更します。あるいは、「**除去**」をクリックして、規則を除去することもできます。構成クライアントは、規則の最新表示リストを表示します。「**了解**」をクリックして、変更を保管します。

第11章 Socks サーバーの構成

Socks は、サーキット・レベル・ゲートウェイ用のインターネット標準です。 アプリケーションが、Web ブラウザー、FTP、または Telnet などの TCP を使用する場合は、アドレス変換に Socks サーバーを使用します。 Socks は、内部 IP アドレスを隠蔽しながらインターネットにアクセスする場合に役立ちます。

アウトバウンド要求 (セキュア・クライアントから非セキュア・サーバーへの) の場合、Socks サーバーにはプロキシー・サーバーと同じ目的があります。すなわち、セッションをファイアウォールで中断し、内部ネットワークのアドレス指定や構造を保護しながら、ユーザーが外部の非セキュア・ネットワークへのアクセスを許可される場所に、セキュア・ドアを設けます。 Socks サーバーには、ユーザーにとって簡素化の利点があり、追加の管理作業はあまりありません。

Socks サーバーは、ネットワークとインターネット間を通過するすべてのアウトバウンド TCP 要求を代行受信することができます。 Socks サーバーにはリモート・アプリケーション・プログラム・インターフェースがあるため、セキュア・ドメインのクライアント・プログラムが実行する機能は、ファイアウォール・ワークステーションのセキュア・サーバーによってパイプ処理され、クライアントの IP アドレスは隠蔽されます。アクセスは、Socks 規則に関連付けられたフィルターによって制御されます。

Socks サーバーは、プロキシー・サーバーに類似しています。しかし、プロキシー・サーバーがファイアウォールで実際に TCP/IP 機能を実行するのに対し、Socks サーバーはユーザーを識別し、機能をファイアウォールを介してリダイレクトするだけです。実際の TCP/IP 機能は、ファイアウォールではなく、クライアント・ワークステーションで実行されます。この結果、ファイアウォールでの処理が省かれます。セキュア・ネットワークのユーザーは、Socks 標準をサポートする多数の TCP/IP 製品を使用することができます。 図 21 で、セキュア・ネットワーク内のクライアントからの HTTP 要求を代行受信する Socks サーバーを説明します。

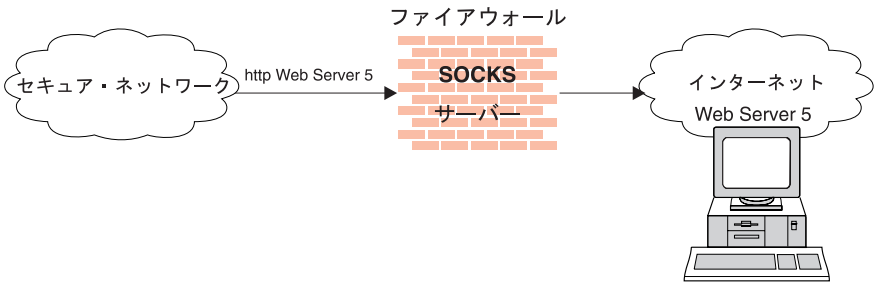

図 21. Socks サーバー

Socks サーバーは、内部 IP アドレスを効果的に外界から隠蔽します。

IBM Firewall には Socks プロトコル バージョン 5 があります。これにより、セキュア・ネットワーク内のクライアントは、非セキュア・ネットワークのアプリケーションにアクセスする前の認証段階をパスすることができます。また、IBM Firewall は、認証された総称プロキシー、およびいくつかのストリーミング・オーディオおよびビデオ・プロトコルのプロキシーをも考慮に入れています。

Socks デーモンは、Windows NT サービスとして稼働し、そのシステムが開始すると、自動的に開始します。さらに、監視エージェントを備えており、サーバーをモニターすることができます。監視エージェントは、手動で開始することができます。

IBM Firewall には、3 つの認証プロファイルの形式でのスムーズな移行パスがあり、Socks プロトコル バージョン 5 クライアントを紹介しながら、インストール済みの Socks プロトコル バージョン 4 クライアントを引き続き使用することができます。

1. 最も自由なプロファイルの場合は、アウトバウンド認証は使用可能にならず、Socks プロトコル バージョン 4 クライアントを使用するか、 Socks プロトコル バージョン 5 クライアントを使用するかに関係なく、どのユーザーも接続することができます。このシナリオでは、インバウンド接続は拒否されます。
2. 移行プロファイルの場合、Socks プロトコル バージョン 4 ユーザーは無認証でのパスが許されますが、 Socks プロトコル バージョン 5 ユーザーは認証が必要です。インバウンド Socks プロトコル バージョン 4 接続は拒否され、インバウンド Socks プロトコル バージョン 5 接続は認証を求められます。これは、省略時プロファイルです。
3. 最も安全なプロファイルの場合は、すべてのユーザーが Socks プロトコル バージョン 5 クライアントを使用し、有効な認証を備えています。

Firewall をインストールすると、Socks サーバーは使用可能ですが、 Socks 構成ファイルには規則は入っていません。Socks クライアントが Socks サーバーを使用するには、構成クライアントを用いて Socks を構成しなければなりません。 Socks サービスの設定方法の例については、 56ページの『Socks の例』 を参照してください。

Socks プロトコル バージョン 5 サーバーがサポートするプロトコル

Socks プロトコル バージョン 5 サーバーは、以下の TCP および UDP プロトコルなど、数多くのプロトコルをサポートします。

- Archie
- Finger
- FTP
- Gopher
- HTTP
- HTTP Proxy
- News
- SNMP
- Telnet
- TFTP
- RealAudio
- RealPlayer
- Whois
- X-Windows

加えて、大部分の電子メール・クライアントもサポートされます。これらのプロトコルのサポートは、その実際のインプリメンテーションによって異なります。

構成クライアントを用いた Socks サーバーの構成

Socks テンプレートとは、 Socks サーバーによってセキュリティーを制御する規則です。 Socks テンプレートを用いると、既存の Socks テンプレートの、カスタマイズ、追加、コピー、もしくは削除を行うことができます。次に、これらの Socks テンプレートは、規則テンプレートを使用する場合と同じ方法で、ファイアウォール上の接続の定義で使用することができます。

新しい Socks 規則の追加

構成クライアントが備えている Socks テンプレートを用いて、規則を Socks 構成ファイルに追加するには、構成クライアントのナビゲーション・ツリーから、「トラフィック制御」を選択します。ファイル・フォルダー・アイコンをダブルクリックして、表示を拡大します。「接続テンプレート」を選択します。ファイル・フォルダー・アイコンをダブルクリックして、表示を拡大します。「**Socks**」を選択します。「**Socks**」ダイアログ・ボックスが表示されます。

1. 「**新規**」をダブルクリックして、新しい Socks テンプレートを追加します。

   73ページの図 22 に示すような、「**Socks 規則の追加**」ダイアログ・ボックスが表示されます。

図 22. Socks 規則の追加

2. 「**テンプレート名**」フィールドで、 Socks 項目の名前を入力します。この名前は固有でなければなりません。またパイプ記号 (|)、単一引用符 (またはアポストロフィ (’))、もしくは二重引用符 (") が入っていてはなりません。なぜなら、これらは

ファイル区切り文字として使用されるためです。これらの文字を使用すると、信頼できないデータを生ずることがあります。

3. 説明を入力します。
4. 「処置」オプション・メニューをクリックして、送信元から宛先へのアクセスの「許可」もしくは「拒否」を選択します。

   データグラムが Socks サーバーに入ると、サーバーは、データグラム仕様と構成ファイル内の各規則を、最初の規則から始めて完全一致の規則を検出するまで比較します。完全一致の規則を検出すると検索を終了して、その規則に対する関連処置 (アクセスの可否) を実行します。一致が検出されなければ、アクセスは自動的に拒否されます。
5. 「**ユーザー・リスト**」フィールドでは、ユーザー ID またはユーザー ID のリストを入力することができます。リストに入力する場合は、項目をコンマで分離してください。ユーザー・リストでは、スペース、タブ、パイプ記号 (|)、または二重引用符 (″) は使用しないでください。
   - ユーザー・リストは、396 文字に制限されます。
   - ユーザー ID は、宛先ホストまたは Socks サーバー・ホストの ID ではなく、リクエスト側ホストのユーザーの ID でなければなりません。
   - ユーザー ID は、1 から 8 文字で構成され、次のような文字を含むことができます。
     - a から z
     - A から Z
     - 0 から 9
     - _ (下線)
6. ユーザー ID には、パイプ記号 (|) や二重引用符 (″) を入れてはなりません。
7. ファイル名を使用する場合は、完全修飾しなければなりません (先に ″/″ を付けて、ユーザー ID と解釈されないようにします)。各ファイルには、1 行に 1 つまたは複数の、コンマで分離されたユーザー ID のリストを含めることができ、さらに任意選択で # 文字で区切られたコメントも含むことができます。 # 文字で始まる全注釈行もサポートされています。ファイルの各行とも、最長 1023 文字で、″改行文字″ で終了しなければなりません。
8. 「**操作**」フィールドで、ポート番号について実行される以下の論理演算子を入力します。

   eq 等しい

   neq 等しくない

   lt ～より小さい

   gt ～より大きい

   le ～より小さいか、または等しい

   ge ～より大きいか、または等しい

   論理演算子は、ポート番号とともに使用されると、一致しなければならない関係を確立します。たとえば、演算子 gt とポート番号 23 を入力した場合、規則を呼び出すには、ポート番号は 23 より大きくなければなりません。

9. 「**ポート番号**」フィールドで、ポートの番号を入力します。 ポート番号は「操作」フィールドと一緒に使用され、一致しなければならない関係を確立します。たとえば、演算子 gt とポート番号 23 を入力した場合、規則を呼び出すには、ポート番号は 23 より大きくなければなりません。演算子とポート番号を省略すると、規則はすべての宛先ポート番号に適用されます。

この「**Socks 規則の追加**」ダイアログ・ボックスを用いて、IP アドレスに基づいてネットワーク・ホストへのファイアウォール・アクセスを許可または拒否します。

Socks 規則の変更

1. 「**Socks**」ダイアログ・ボックスの項目をダブルクリックします。

   「**Socks 規則の変更**」ダイアログ・ボックスが表示されます。
2. 73ページの『新しい Socks 規則の追加』 の説明のように、該当するフィールドを変更して、「**了解**」をクリックします。

Socks 規則の削除

「**Socks**」ダイアログ・ボックスから項目を選択し、「**削除**」をクリックします。この Socks 規則を確実に削除するかどうかを確認されます。「**了解**」をクリックして、規則を削除します。

接続規則の活動化

フィルター規則の場合のように、Socks 規則を活動化する必要があります。 構成クライアントのナビゲーション・ツリーの「**接続の活動化**」をクリックし、「**接続規則の再生成と活動化**」を選択してから、「**実行**」をクリックします。

ファイアウォールは、規則を Socks 構成ファイルからファイアウォール規則にコピーし、その規則を活動化します。規則が活動化すると、新しい規則がファイアウォール・ログ・ファイルに記録されます。

Socks のサンプル・ロギング出力

Socks のロギング出力のサンプルを以下に示します。

```
Feb 03 13:46:20 1998 mr16n18: ICA3123i: Sockd サーバーを始動しています。
Feb 03 13:47:31 1998 mr16n18: ICA3010i: 接続しました。
Feb 03 13:47:31 1998 mr16n18: ICA3011i: 接続しました。
Feb 03 13:49:15 1998 mr16n18: ICA3007i: 最大接続回数を超えたため接続は拒否されました。
Feb 03 13:58:31 1998 mr16n18: ICA3015i: 終了しました。
```

Socks サーバーを使用するためのクライアントに関する考慮事項

大多数の Web ブラウザーは Socks 化されていて、大部分のプラットフォーム用の Socks 化されたスタックを入手できます。その他の TCP/IP アプリケーション用の Socksified クライアントは、多くの供給元から手に入ります。 Socks を実装している特定のクライアントについては、そのクライアントの関連文書を参照してください。詳細については、次の URL を参照してください。

http://www.raleigh.ibm.com/sng/sng-socks.html

http://www.socks.nec.com

Socks サーバー連鎖

Socks サーバー連鎖とは、一方の Socks サーバーが他方の Socks サーバーの背後に常駐でき、なおかつ、最外部の Socks サーバーを越えたネットワークへのアクセスを許可するという機能です (これは、Socks サーバーを Socks 化する考えだといえます)。これは、非常に役に立つイントラネット・シナリオです。

Socks サーバーを使用して Socks サーバー連鎖を設定するには、 `socks5.header.cfg` ファイルを編集します。このファイルは、ファイアウォールの `config` サブディレクトリーにあります。以下を追加してください。

- *no proxy* 指示 - ユーザーのファイアウォールが直接アクセスをもつサブネットを示します。
- *socks4* 指示 - Socks プロトコル バージョン 4 サーバーを通じてアクセス可能なサブネットを示します。
- *socks5* 指示 - Socks プロトコル バージョン 5 サーバーを通じてアクセス可能なサブネットを示します。

たとえば、次のネットワークを考えてみましょう。統計部門は、独自のファイアウォールの背後に、小規模な専用ネットワーク *q.private.com* をもちます。統計部門のサブネットは、10.007.007.0/255.255.255.0 です。企業の専用ネットワーク *private.com* には、10.0.0.0/255.0.0.0 ネットワークの全体が含まれています。企業の Socks プロトコル バージョン 4 サーバー *socks.private.com* は、インターネットへのアクセスを提供します。

統計部門の Socks サーバー *socks.q.private.com* で、以下の 2 行を `socks5.header.cfg` に追加します。

```
no proxy 10.0.0.0/255.0.0.0 - - -
socks4      0/0   - socks.private.com 1080
```

最後に、*socks.q.private.com* が *socks.private.com* と通信できるように、「トラフィック制御」接続を追加します。より一般的なサービスによって、このプロセスはすでに終了している場合があります。送信元が *q.private.com* ファイアウォールの非セキュア・インターフェースで、宛先が *socks.private.com* である接続を追加し、 *Socks プロキシー連鎖*サービスを組み込んでください。次に、トラフィック制御規則を再活動化してください。

第12章 ファイアウォールにおけるユーザーの管理

本章では、以下のような IBM Firewall に関する日常の管理用タスクを行う方法について説明します。

- ユーザーを IBM Firewall に追加して、セキュア・ネットワーク外のホストにアクセスできるようにします。
- ファイアウォールにアクセスするユーザーの属性を変更します。
- ネットワークの外部にアクセスする必要がなくなったユーザーを削除します。

構成ファイルは直接編集しないでください。直接編集すると、IBM Firewall ユーザー属性が正しく設定されません。 IBM Firewall 管理は、すべて構成クライアントのダイアログまたはコマンド行を用いて行ってください。

IBM Firewall へのユーザーの追加

IBM Firewall は 3 つのタイプのユーザーを定義して、それらに関する情報を 2 つの異なるユーザー・データベースに保管します。

ユーザーのタイプ

IBM Firewall では、ユーザーを次の 3 つのカテゴリーに分けます。

プロキシー・ユーザー

会社のネットワーク内からインターネットの Web サイトにアクセスする HTTP プロキシー・サービスなどの、ファイアウォール・サービスを使用します。プロキシー・ユーザーは、ファイアウォール・マシンを通じてサービスを使用することができますが、ファイアウォール・マシンへのアクセス権はなく、ファイアウォール・マシンへのローカル・ログインを行うことはできません。

ファイアウォール管理者

ファイアウォール・プロキシー・サービスを使用することができますが、構成クライアントを使用し、かつリモート・ホストからファイアウォールにログオンすることで、ファイアウォールを構成することもできます。プロキシー・ユーザー同様、ファイアウォール管理者もファイアウォール・マシンへのローカル・ログインを行うことはできません。

ファイアウォール管理者は、プロキシー・ユーザー用の定義を作成、かつ変更することができますが、他のファイアウォール管理者の定義を作成し、変更することはできません。

1 次ファイアウォール管理者

ファイアウォール管理者と同じ機能を持っています。ファイアウォール・マシンへのローカル・ログインを行うこともできます。 1 次ファイアウォール管理者は、他のファイアウォール管理者の定義を作成し、変更することができます。

データベースのタイプ

ユーザー・データベースには、以下の 2 つのタイプがあります。

ファイアウォール・ユーザー・データベース
プロキシー・ユーザーおよび管理者ごとのファイアウォール関連の属性が含まれます。ユーザーのファイアウォール・パスワードとパスワード規則、およびサービスごとにユーザーの認証に使用すべき認証方式などの、属性が組み込まれます。

プロキシー・ユーザーがファイアウォール・ユーザー・データベースで定義されずに、そのユーザーがファイアウォール・プロキシー・サービスを使用しようとすると、デフォルト・ユーザー・レコードの `fwdfusr` が、ユーザーの妥当性検査に使用する属性と認証スキームの定義に使用されます。

1 次ファイアウォール管理者は、ファイアウォール・ユーザー・データベースで定義することはできません。管理者に属性を割り当てる場合は、デフォルトのファイアウォール管理者レコード、 `fwdfadm` を使用してください。

プロキシー・ユーザー同様、ファイアウォール管理者も Windows NT ユーザー・データベースで定義される場合は、 NT ログオン・パスワードを用いて認証しなければならないサービスを、ユーザーが要求したとき、その管理者の NT ログオン・パスワードが使用されます。

Windows NT ユーザー・データベース
ユーザー用の NT ログオン・パスワードを収めます。通常、NT ログオン・パスワードを用いて認証されるのでなければ、プロキシー・ユーザーは NT ユーザー・データベースで定義される必要はありません。

プロキシー・ユーザーの認証に他の認証方式を使用する場合、そのユーザーは Windows NT ユーザー・データベースで定義する必要はありません。

1 次ファイアウォール管理者は、 NT 管理者グループのメンバーである Windows NT ユーザーと同義であり、 Windows NT ユーザー・データベースで定義されなければなりません。

構成クライアントを用いたユーザーの追加

ユーザーを IBM Firewall に追加すると、ユーザーは外部ネットワークにアクセスすることができます。

1. 構成クライアントのナビゲーション・ツリーから、「ユーザー」を選択します。「**ユーザー管理**」ダイアログ・ボックスが表示されます。
2. 「**ユーザー管理**」ダイアログ・ボックスから「**新規**」を選択し、「**オープン**」をクリックします。79ページの図 23 に示すような、「**ユーザーの追加**」ダイアログ・ボックスが表示されます。

図 23. ユーザーの追加

3. 次の情報を入力してください。

権限レベル

このユーザーの権限レベルを指定します。「**権限レベル**」の矢印をクリックし、ユーザー・タイプを選択します。

Socks/Proxy ユーザー

定義されているユーザーは、Socks サーバー・アクセス用およびプロキシー・アクセス用のユーザーです。ユーザーには、管理権限はありません。これはデフォルトです。

ファイアウォール管理者

ユーザーの属性のすべてを持っていますが、管理者は、ファイアウォールにログインし、管理用タスクを実行することもできます。管理者は、実行することができる管理機能を定義する追加の属性を持っています。ファイアウォール管理者はファイアウォール・ユーザーを作成することができますが、他のファイアウォール管理者を作成することはできません。ファイアウォール管理者は、ローカルにファイアウォール・マシンにログインすることはできません。リモート・マシンから構成サーバーにアクセスしなければなりません。

1 次ファイアウォール管理者

1 次ファイアウォール管理者は、ローカルに ファイアウォール・マシンにログインすることができます。 1 次ファイアウォール管理者には、アクセス管理機能全体に対するアクセス権があります。また、1 次ファイアウォール管理者を除く他のファイアウォール管理者を作成することもできます。

1 次ファイアウォール管理者は、ユーザーを NT データベースに作成し、そのユーザーを NT 管理者グループのメンバーにすることで、定義されます。 1 次ファイアウォール管理者の属性を定義する場合は、 `fwdfadm` レコードを変更します。

ユーザー名

このユーザーの名前を指定します。これは、このユーザーが、IBM Firewall の Telnet または FTP サーバーにログインする際のユーザー名です。これは、必ずしもユーザーの TCP/IP ユーザー名またはホスト名とは限りませんが、両者は同じであっても構いません。

ユーザー名は、1 から 8 文字で構成され、次のような文字を含むことができます。

a から z

A から Z

0 から 9

_ (下線)

ユーザー名は、大文字小文字を区別しません。

ファイアウォールには、次の 2 つのユーザーが事前定義されています。

a. デフォルトのユーザーまたは `fwdfuser`。ユーザーがファイアウォール・データベースで定義されない場合は、ユーザーの認証時に使用する認証方式のような、ユーザーのファイアウォール属性の判別に、`fwdfuser` が使用されます。

   インストール時、`fwdfuser` の作成時はすべての認証方式がすべて拒否に設定されています。 `fwdfuser` に対する許可によって、ファイアウォールが未定義ユーザー名を処理する方法が制御されます。

管理者は、構成クライアントまたはコマンド行を用いて、fwdfuser を表示することも、割り当てられた認証方式を変更することもできます。しかし、fwdfuser は削除することはできず、常にファイアウォールに存在していなければなりません。加えて、ファイアウォール・パスワードと SNK は、 fwdfuser の認証タイプとしては無効です。詳細については、*IBM Firewall 解説書* を参照してください。

b. デフォルトの 1 次ファイアウォール管理者、fwdfadm は、すべての 1 次ファイアウォール管理者のファイアウォール属性を定義します。 1 次ファイアウォール管理者は、その独自のユーザー・レコードをファイアウォール・データベース内に持たないため、このレコードは、 1 次ファイアウォール管理者の認証に用いる認証方式の定義に使用されます。

インストール時、fwdfadm のすべての認証方式は、NT ログオン・パスワードに設定されるセキュアおよび非セキュア管理認証方式を除き、「すべて*拒否*」に設定されています。1 次ファイアウォール管理者は、このレコードを表示し、変更することはできますが、削除することはできません。加えて、ファイアウォール・パスワードと SNK は、fwdfadm の認証タイプとしては無効です。

ユーザーの姓名
ユーザーの記述を指定します。

次のフィールドは、認証方式に関係します。矢印をクリックし、認証方式のリストから項目を選択します。選択項目については、82ページの『ユーザーの認証方式』 に説明があります。

セキュア Telnet
セキュア・ネットワークからログインする場合、このユーザーのアイデンティティー (身分証明) をいずれかの方法で認証する必要があるかどうかを指定します。

非セキュア Telnet
非セキュア・ネットワークからログインする場合、このユーザーのアイデンティティー (身分証明) をいずれかの方法で認証する必要があるかどうかを指定します。

セキュア FTP
このユーザーが、FTP を用いてセキュア・ネットワークからファイアウォールにアクセスするときに必要とする認証のレベルを指定します。

非セキュア FTP
このユーザーが、FTP を用いて非セキュア・ネットワークからファイアウォールにアクセスするときに必要とする認証のレベルを指定します。

セキュア Socks
ファイアウォールのセキュア・サイドから着信する Socks クライアント接続の、Socks V5 認証方式を指定します。矢印をクリックし、選択項目のリストから選択します。選択項目については、82ページの『ユーザーの認証方式』 に説明があります。

非セキュア Socks
ファイアウォールの非セキュア・サイドから着信する Socks クライアント

接続の、Socks V5 認証方式を指定します。矢印をクリックし、選択項目のリストから選択します。選択項目については、82ページの『ユーザーの認証方式』 に説明があります。

セキュア HTTP
アウトバウンド HTTP プロキシー要求に関する認証のユーザー ID/パスワードのタイプを指定します。矢印をクリックし、選択項目のリストから選択します。選択項目については、82ページの『ユーザーの認証方式』 に説明があります。

ブラウザーからユーザー ID とパスワードがプロンプトが出されるので、SDI を使用する場合は、パスワード・プロンプトにパスコードを入力してください。

指定されたユーザーは、Socks/パスワードは対話式のダイアログはサポートできず、それに応じて行動することを認識していなければなりません。

セキュア管理
セキュア・インターフェースを介して、構成クライアントからログオンするのに使用する認証方式を指定します。ローカルにログオンする (ログオン・パネルでローカルを選んで) ときは、常にセキュアの環境にいるため、これが、使用する認証方式であることに注意してください。

非セキュア管理
非セキュア・インターフェースを介して、構成クライアントからログオンするのに使用する認証方式を指定します。

SecureNet キー
AssureNet Pathways SecureNet キー・カードを持つリモート・ユーザーが入力する文字順序を指定します。キー・カードにも入れるキー・コードを入力します。キー・コードの選択およびインストールの指示については、SecureNet キーの説明を参照してください。

注:

a. このフィールドは、SecurID カードには使用しません。
b. 各ユーザーごとに、固有のランダム・キーを作成する必要があります。
c. キーを SecureNet キー・カードにインストールするときは、 AssureNet Pathways インストール手順を使用し、「**モード 5**」を選択します。

詳細については、87ページの『認証方式』 を参照してください。

ユーザーの認証方式

ユーザー認証の選択項目を、以下に示します。

すべてを禁止
ユーザーは、アクセスを拒否されます。

すべてを許可
認証は必要ありません。

NT ログオン・パスワード

NT ログオン・パスワードは、ファイアウォール・パスワードに比べて、安全度が劣ります。しかし、ユーザーがすでに Windows NT ドメインで定義されていれば、Windows NT ログオン・パスワードを使用できるため、ユーザーは複数のパスワードを必要としません。

この認証の方式を選択すると、ユーザー ID とパスワードは、ローカル Windows NT ユーザー・データベースに照らして妥当性検査されます。ファイアウォールが他の Windows NT サーバーを承認するように構成されていれば、これらの承認されたサーバーは、ユーザー定義について検索されます。

Windows NT ファイアウォールと承認された Windows NT サーバー間で信頼関係を設定するには、2 つのマシン間に接続を設定して TCP/IP 通信のトラフィックを可能にしておかなければなりません。

この接続は、以下の事前定義サービスを用いて設定します。

1. ドメイン・コントローラー認証 - これによって、ドメイン・コントローラーをユーザーの認証に使用できる
2. NetBT ネーム・サービス同報通信 - これによって、 TCP/IP ネーム・サービス同報通信で NetBT を使用できる

Windows NT 構成ユーティリティーを用いて、信頼関係を定義します。

SecureNet キー

認証は、AssureNet Pathways SecureNet キーを用いて行われます。

「SecureNet Key」フィールドでは、SecureNet キー・カードにも入れるキー・コードを入力します。

注:

1. 各ユーザーごとに、固有のランダム・キーを作成する必要があります。
2. ランダム・キーは、8 つの 8 進数ごとに、1 から 377 の範囲になければなりません。
3. キーを SecureNet キー・カードにインストールするときは、 AssureNet Pathways インストール手順を使用し、「**モード 5**」を選択します。

詳細については、87ページの『認証方式』 を参照してください。

SecurID カード

認証は、Security Dynamics SecurID セキュリティー・カードまたは pinpad (暗証番号入力機構) カードを使用して行われます。「SecureNet Key」フィールドは使用しない でください。 PIN は、この認証方式を IBM Firewall に使用する前に設定しなければなりません。

FTP の場合は、SDI 新規 PIN モードと次トークン・モードはサポートされません。

詳細については、87ページの『認証方式』 を参照してください。

ユーザー提供の認証 1、2、および 3

認証はお客様の提供によるものです。ユーザー提供の認証方式は、3 つまでファイアウォールにインストールすることができます。 ユーザー提供の認証のサブルーチンを作成し、コンパイルする方法については、 *IBM Firewall 解説書* を参照してください。

ファイアウォール・パスワード

ユーザーに、有効なパスワードを要求するプロンプトが出され、それを入力しなければなりません。このパネルを完了すると、IBM Firewall から、この新規ユーザーのパスワードを指定するように要求されます。

ファイアウォール・パスワードの場合は、Windows NT ログオン・パスワードより使用できるセキュア・パスワードやパスワード規則が多いので、パスワードにはこれを選択するようお勧めします。

変更するユーザーが必要です

「はい」または「いいえ」をクリックして、次の認証の際にパスワードの変更が必要かどうかを示します。

パスワードのロック

「はい」または「いいえ」をクリックして、パスワードをロックするかどうかを示します。ログインの失敗数が最大を超えたり、「ロックアウトまでの最大時間」で指定した週の数にパスワードが使用されていないときは、これは「はい」に設定されます。

管理者は、このフィールドを「はい」に設定して、ユーザーがパスワード認証を使用できないようにすることができます。

注:

1. パスワードは、大文字と小文字が区別されます。管理担当者が大文字と小文字を混ぜてユーザーのパスワードを入力した場合、そのユーザーは同様にパスワードを入力しなければなりません。大文字のみで動作するワークステーションがある場合は、それらのユーザーに対するパスワードは大文字で入力してください。
2. オペレーティング・システムを使用することで、パスワード規則を定義できます。以下のパスワード規則は、ユーザーが自分のパスワードを変更した場合に適用されます。管理者がパスワードを変更した場合は、適用されません。パスワード規則を、次に示します。

   期限切れまでの警告日数 (日)

   パスワードが失効するまでの日数。ファイアウォールではこの間にパスワードを変更するオプションがユーザーに与えられています。

   期限切れまでの最大週数

   ユーザーによるパスワードの変更が必要になるまでの週数。

   ロックアウトまでの最大週数

   パスワードを使用しないでロックアウトされるまでの週数。

   許可される最大ログイン試行回数

   パスワードがロックされるまで、ログインを試みで失敗する最大回数。

   再利用までのパスワード

   パスワード活動記録リストに格納されるパスワード数。パスワードは、現在活動記録リストに入っているパスワードに変更することはできません。このパラメーターが有効なのは、パスワード再利用までの週数がゼロの場合のみです。

パスワード再利用までの週数
パスワードがパスワード活動記録リストに保持される週数。パスワードは、現在活動記録リストに入っているパスワードに変更することはできません。

最小文字数
パスワード内の最小文字数。

英字の最小文字数
パスワード内の最小英字数。

その他の文字の最小数
パスワードの英字以外の最小文字数。

繰り返し文字の最大数
パスワード内で単一の文字を繰り返すことができる最大回数。

異なる文字の最小数
パスワード内の異なる文字の最小数。

86ページの図 24 に示すように、**ファイアウォール・パスワード・**タブをクリックし、ユーザーごとにこれらの値をクリックします。

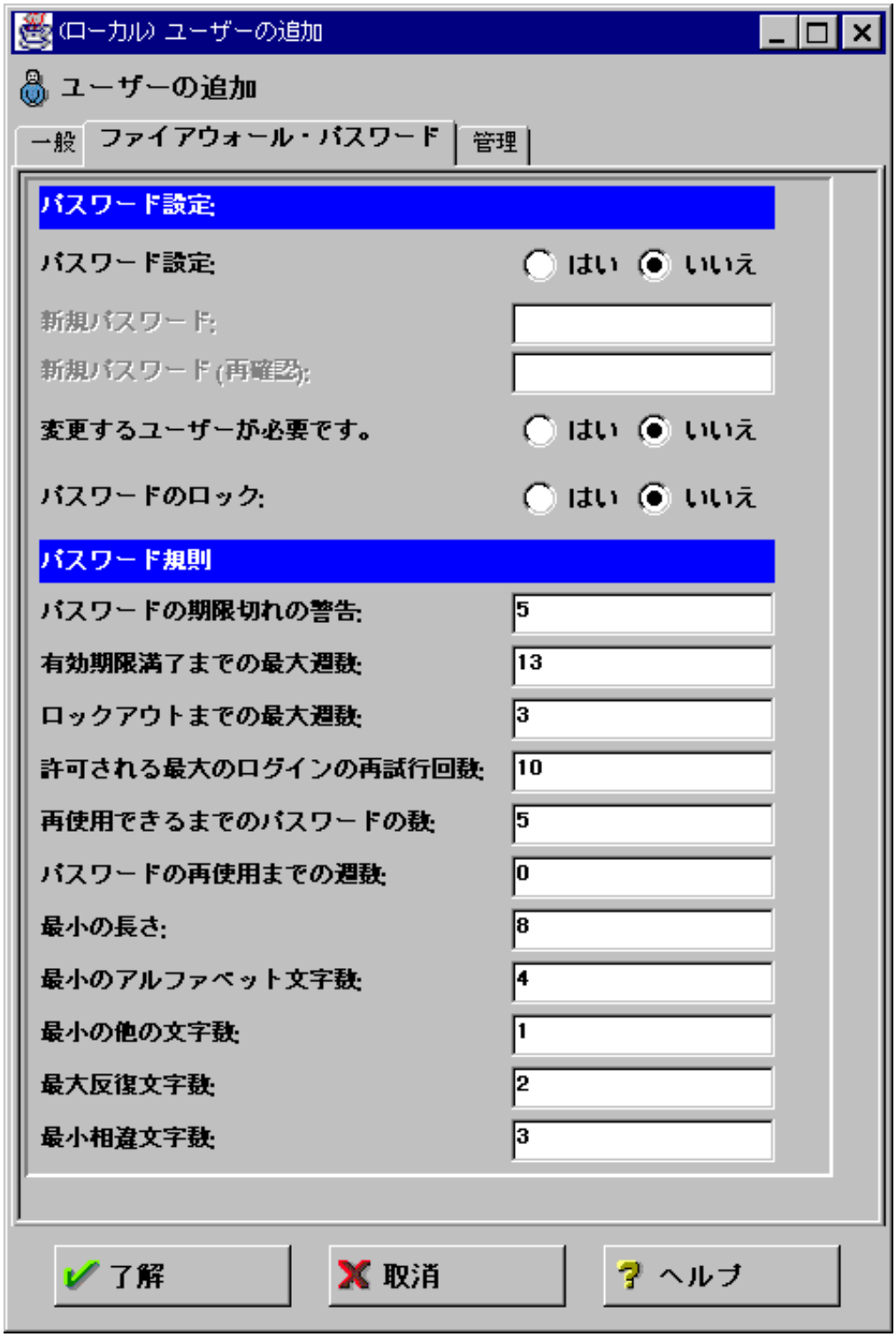

図 24. ファイアウォール・パスワード・タブ

ユーザーのアクセスの変更

ユーザーをファイアウォールに追加してから、「**ユーザーの変更**」ダイアログ・ボックスから、そのユーザーのセキュリティー属性を変更することができます。

1. 変更したいユーザーを「**ユーザー**」ダイアログ・ボックスから選択し、「**オープン**」をクリックします。
2. 「**ユーザーの変更**」ダイアログ・ボックスが表示されたら、該当するフィールドを変更します。変更可能なユーザー属性のリストについては、77ページの『IBM Firewall へのユーザーの追加』 をご覧ください。
3. 変更を行ったら、「**了解**」をクリックします。

IBM Firewall からのユーザーの削除

注: `fwdfuser` または `fwdfadm` ユーザーは削除しないでください。

ユーザーを削除するには、「**ユーザー・リスト**」パネルの「**削除**」をクリックします。

機能による管理者権限レベル

管理者を作成かつ変更し、管理者が使用する権限を持つファイアウォールの機能を決めることができるのは、*1 次ファイアウォール管理者*のみです。たとえば、特定の管理者の権限を、単に「ユーザー」および「ログ・モニター」機能の実行に限定することができます。

「**ユーザーの追加**」ダイアログ・ボックスで、「**権限レベル**」フィールドの「ファイアウォール管理者」を選択します。「**ユーザーの追加**」ダイアログ・ボックスを完了するための詳細については、 77ページの『IBM Firewall へのユーザーの追加』を参照してください。

次に、「**ユーザーの追加**」ダイアログ・ボックスの最上部で「**管理者**」タブを選択します。管理者に使用を許可する機能を選択します。

認証方式

以下に、各種ユーザー認証方式を示します。

すべてを禁止

IBM Firewall は、サーバーへのアクセスを拒否します。

すべてを許可

認証は必要ありません。サーバーは、ユーザーの認証を行いませんが、コマンド・プロンプトは続行するので、外部ホストにアクセスすることができます。

ファイアウォール・パスワード

先に進む前に、サーバーからファイアウォール・パスワードを求められます (表示されない)。

```
Password:
```

ファイアウォール・パスワードを入力してください。このパスワードは、ユーザー名をファイアウォールに追加するときに使用したパスワードと同じものです。

SecurID カードの認証

この方式は、お客様が SecurID カードを持っている場合、およびお客様のネットワークが Security Dynamics ACE/Server を使用している場合に使用します。

プロキシー・サーバーは、先に進む前に、PASSCODE を要求します (画面には表示されません)。

```
Enter PASSCODE:
```

この時点で、4 桁の SecurID PIN コードに続いてコンマ、その後に SecurID カードのコードを入力します。たとえば、SecurID カードにコード 179091 が表示されている時に、ユーザー NEWUSER として 1234 が割り当てられた PIN を使用してログインするには、次のように入力します。

```
login: NEWUSER
Enter PASSCODE: 1234,179091
```

FTP を最初に使用すると、SecurID カード認証が失敗します。FTP にはパスワード変更を許可するオプションがないためです。 PIN を作成するために、初めて SecurID カード認証を行うときは、telnet を使用しなければなりません。作成した PIN は、以後の FTP、HTTP などの認証のために、続けて使用することができます。

SecurID カードが新規の PIN モードになっている場合は、この認証方式を IBM Firewall で使用する前に、PIN を設定しておく必要があります。

SecureNet キーの認証

この方式は、ユーザーが Assurenet Pathways SecureNet キー・カードを持っている場合に使用します。 SNK カードを初期設定するときは、以下を使用してください。

- 表示形式 (16 進数)
- 消去機能 (オン/オフ)
- 単一桁のチャレンジ機能 (オフ)

プロキシー・サーバーは、先に進む前に SecureNet キー・カードによる応答を要求してきます。

```
Use SNK for challenge
######## for user user_id
Ed:
```

チャレンジ ######## は、ユーザーが SecureNet キー・カードに入力する 8 桁の数字です。

1. このプロンプトを受け取ったら、SecureNet キー・カードを活動化し、ユーザーの PIN コードを入力します。この PIN コードは、カードと一緒に与えられたものです。
2. サーバーによって提供されたチャレンジを入力します。

   たとえば、サーバーにログインすると、サーバーは次のプロンプトを出します。

```
Use SNK for challenge
   78987648 for user NEWUSER
Ed:
```

値 78987648 を SecureNet キー・カードに入力します。次に、このカードは応答を表示し、ユーザーはそれをプロキシー・サーバーに提供します。

3. この応答をサーバーに入力します。

   SecureNet キー・カードが、ユーザーのチャレンジに対する応答を 8AE222A9 と表示したら、サーバーに 8AE222A9 と入力してください。

```
logon: NEWUSER
   Use SNK for challenge 78987648 for user NEWUSER
Ed:8AE222A9
```

AXENT** 技術により、SecurNetKey (SNK) は Defender Handheld Token** (DHT) と名前変更されました。

NT ログオン・パスワード

この認証方式を選択すると、ユーザー ID とパスワードは、ローカル Windows NT ユーザー・データベースと照合して妥当性検査されます。ファイアウォールが他の Windows NT サーバーを承認するように構成されていれば、これらの承認されたサーバーは、ユーザー定義について検索されます。

ユーザー提供認証 1、2、および 3

ユーザー提供の認証方式を、FTP と Telnet に使用することができます。 詳細については、*IBM Firewall 解説書* を参照してください。

第13章 プロキシー・サーバーの構成

この章では、セキュア・ネットワークの内部と外部の両方のワークステーションからプロキシー・サーバーを設定および使用する方法についての一般的な情報を記載しています。

HTTP プロキシー

HTTP プロキシーは IBM Firewall を介してブラウザー要求を効率的に処理するので、Web ブラウズを行うための socks サーバーを必要としません。 ユーザーは、自分の内部ネットワークのセキュリティーを危険にさらすことなく、また HTTP プロキシーをインプリメントするために自分のクライアント環境を変更することなく、インターネット上の有用な情報をアクセスすることができます。

HTTP プロキシーは、サーバーではありません。エンド・ユーザーは、プロキシーからファイルを取り出すこともできませんし、プロキシーにファイルを入れることもできません。また、HTTP プロキシーは、キャッシュ・プロキシーでもありません。HTTP 要求があっても、ファイアウォールには何も保管されません。

持続セッション

持続接続により、クライアントとサーバーは TCP 接続のクローズをシグナルすることができます。このシグナル方式は、接続ヘッダー・フィールドを使用します。

IBM Firewall プロキシーは、クライアントとプロキシー間の持続接続をサポートします。*最大持続要求*条件および*持続接続*タイムアウト条件により、その接続の存続時間が制御されます。これらの条件のいずれかが生じると、プロキシーとクライアント間の socket 接続はクローズします。*最大持続要求*条件および*持続接続*タイムアウト条件が生じない場合、接続は開かれたままで、要求が完了する時間を決定するのはクライアントの義務です。

これが不適切に決定されると、接続上でトラフィックがないときに、ディスプレイにトラフィックが示されます。この例としては、ページが完全にロードされた後でも引き続いて稼働している、ブラウザーの動画アイコンがあります。アニメーションを停止するには、「**停止**」をクリックします。これらのパラメーターについての詳細は、94ページの『最大持続要求』 および 94ページの『持続接続タイムアウト』を参照してください。

構成クライアントを使用した HTTP プロキシーの構成

HTTP プロキシーを構成するには、以下のようにします。

1. DNS 照会を使用可能にして、HTTP プロキシーを正しく動作させます。これを簡単に行うには、構成クライアントのナビゲーション・ツリー上にある「システム管理」フォルダーの中の「セキュリティー・ポリシー」をクリックし、「DNS 照会許可」をクリックします。
2. フィルターを活動化します。

3. 接続を追加します。ネットワークの外部ネットワーク側に接続を設定する方法の例については、 55ページの『プロキシー HTTP の例』 を参照してください。

4. HTTP プロキシーを構成するには、構成クライアントのナビゲーション・ツリーから「HTTP」を選択します。 IBM Firewall は、92ページの図 25 に示すような **HTTP プロキシー** ダイアログ・ボックスを表示します。

図 25. HTTP

5. プロキシーを停止するには、「マイ コンピュータ/コントロール パネル/サービス」を選択します。「IBM Firewall HTTP プロキシー」を選択してから、*停止* をクリックします。

   実行可能な phttpd は、システムが開始するときに自動的に開始されるシステム・サービスです。

HTTP プロキシー ダイアログ・ボックス上で、パラメーターを設定します。パラメーターを変更すると、Firewall HTTP プロキシー・サービスは停止し再び開始します。活動中のプロキシー・ユーザーは、プロキシーが再開するまでに要求を終了させます (数秒間)。

プロキシー・ポート番号

このパラメーターは、プロキシーが要求を listen するポート番号を指定するために使用します。ポート番号を変更する場合は、フローがポートを通ることを許可するか許可しないかをフィルターに設定する必要があります。 1024 より小さいポート番号は、TCP/IP アプリケーション用に予約されています。プロキシー Web サーバーに使用される共通のポートは、8080 と 8088 です。

デフォルトのフィルター規則は、ポート 8080 のインバウンドの非セキュア・トラフィックを許可しないように設定されていますが、そのポートでのセキュア・トラフィックは許可されます。プロキシーが拒否するのは、非セキュア・プロキシー要求だけです。 デフォルトは 8080 です。この設定を変更する場合は、この構成について設定されている「サービス」のポート番号も変更しなければなりません。これらのいずれかの設定を変更した場合は、phttpd プロセスを再始動する必要があります。

コンテンツの最大バッファー長

このパラメーターは、サーバーによって生成される動的データ用バッファーのサイズを設定するために使用します。動的データは、CGI プログラム、サーバー・サイド・インクルード、および API プログラムによって出力されます。動的データは、プロキシーからは出力されないデータです。

K バイト (K) 単位で値を指定します。デフォルトは、 50K です。

スレッド・プール・サイズ

このパラメーターは、同時に活動状態にするスレッド数を設定するために使用します。プロキシーは、別の要求が終了してスレッドが使用可能になるまで、新しい要求を保留します。 一般に、マシンの能力が高くなるほど、このパラメーターに使用する値も大きくなります。 オーバーヘッド・タスク (たとえば、メモリー・スワッピング) のためにマシンが過度の時間を費やすようになった場合は、この値を減らしてみてください。 たとえば、総数を 60 と指定します。 デフォルトは、200 です。

ユーザーのレベル

認証するユーザーのレベルをプロキシーに指示します。「すべて」、「新規」、または「なし」のいずれかの値を指定します。デフォルトは、「なし」です。それぞれの値の意味は、次のとおりです。

すべて ユーザー ID およびパスワードの入力をユーザーにプロンプト指示するためのプロキシー認証応答がすべてのブラウザーに送られます。ブラウザーがプロキシー認証応答をサポートしていない場合は、その旨を伝えるエラー・ページが表示されます。ブラウザーがプロキシー認証応答をサポートしている場合は、ユーザー ID およびパスワード・プロンプトが表示されます。

新規 移行援助プログラムとして使用します。ユーザー ID およびパスワード・プロンプトを出すことをブラウザーに指示するための 407 プロキシー認証応答のみが、クライアント・ブラウザー (HTTP/1.1 ブラウザーであるもの) に送り返されます。 Internet Explorer 4.0 でスイッチを設定すれば、HTTP/1.1 識別子を付けた要求が同報通信されます。 Netscape およびその他のブラウザーは、それ自身が HTTP/1.0 要求として識別されます。

なし ブラウザー要求を検査しません。ユーザー ID およびパスワードのプロンプト指示はありません。

タイムアウト

ユーザー認証を再要求するまでの、クライアント要求の待ち時間をプロキシーに指示します。ユーザーは、アイドル時間中の最初の認証のときに指定された特定の IP アドレスおよびユーザー ID から認証されます。時間は分単位で指定します。デフォルトは、60 分です。

ユーザーが活動的にブラウズしている間、このときのウィンドウは満了しません。

最大持続要求

プロキシーが HTTP/1.1 の永続的な接続で受け取ることのできる要求の最大数を指定します。これは、認証タイムアウトに直接影響を与えるパフォーマンス・ツールです。永続的セッションの場合、永続的セッションが終了するまで、ユーザー認証のテストは行われません。総数で値を指定します。たとえば、25 と指定します。デフォルトは、5 です。

持続接続タイムアウト

このパラメーターは、HTTP/1.1 互換ブラウザーがプロキシーとともにセッションを開始したときに、クライアント・ブラウザーとの HTTP/1.1 の永続的な接続を維持する時間を秒単位で指定します。これは、認証タイムアウトに直接影響を与えるパフォーマンス・ツールです。永続的セッションの場合、永続的セッションが終了するまで、ユーザー認証のテストは行われません。時間は秒単位で指定します。デフォルトは、60 です。

HTTP ログ管理

このパラメーターは、始動/シャットダウンのほか、firewall log に対するすべてのプロキシー要求をログに記録するようにプロキシーに指示するために使用します。プロキシーは、LOG_NOTICE レベルのログ記録を使用します。HTTP 要求活動をモニターしたい場合は、これをオンに設定します。 イベントは、ファイアウォール・ログ機能に記録されます。

ブラウザーの設定

クライアント・ブラウザーは、HTTP プロキシーが listen しているポートへ接続されるように設定する必要があります。

HTTPS を使用する場合は、IBM Firewall の HTTP プロキシーをセキュリティー・プロキシーとして指定することも必要です。

Internet Explorer ブラウザーを、プロキシーへの HTTP/1.1 ブラウザーとして使用する場合は、以下を行います。

- 「*View (表示)*」プルダウンをオープンします。
- 「*Internet Options (オプション)*」を選択します。
- 「*Advance Tab (詳細設定)*」を選択します。

- HTTP 1.1 設定までスクロールダウンし、オンに切り替えます。

SSL 接続

他のサーバーへの HTTP セキュア接続の SSL トンネル伝送がサポートされます。IBM Firewall は、この場合のゲートウェイとして動作します。トンネルは、クライアントからファイアウォールを経由してサーバーへつながっています。次の例に示されているような、HTTP セキュア接続用の標準ポート 443 を使用します。

```
https://www.ibm.com:443
```

また、事前定義サービス `HTTPS proxy out 2/2` も使用します。

HTTPS を使用する場合は、IBM Firewall の HTTP プロキシーをセキュリティー・プロキシーとして指定することも必要です。

詳しくは、55ページの『プロキシー HTTP の例』 を参照してください。

サポートされているメソッド

HTTP プロキシーは、次の方式をサポートします。これらの方式は、インターネットをそれぞれ別の観点から見たものです。

- FTP
- Gopher
- HTTP
- HTTPS
- WAIS

HTTP プロキシーのロギング出力例

以下は、get 要求を承認した HTTP プロキシーのロギング出力の例です。

```
Mar 06 14:04:50 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication UNSUCCESSFUL
for user <Unknown>, on 9.67.140.162, thru secure network ... RC:30.
Mar 06 14:04:50 1998 fire3: ICA2099i: httpd --> Status: 407 from client
9.67.140.162, who requested "GET http://9.67.128.69/ HTTP/1.1" for 0 bytes.
Mar 06 14:05:05 1998 fire3: ICA2024i: User fred successfully authenticated
using NT authentication from secure network:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2169i: User fred successfully authenticated
for HTTP Server using NT from secure network:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user (fred), on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:05 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/HTTP/1.1" for 2693 bytes.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user (fred), on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:06 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/Admin/lgsplash.gif HTTP/1.1"
for 211 bytes.
Mar 06 14:05:10 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user fred, on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:10 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/Admin/lgmast.gif HTTP/1.1"
for 211 bytes.
```

ロギング・アクティビティーは、以下のように説明されます。

- ICA2099i - 戻りコード 407 を示し、get 要求に対して認証が失敗したことを意味します。

  次に、ブラウザーはユーザーに認証を要求し、ユーザー ID およびパスワードを求めます。
- ICA2140i - 認証がユーザー fred に対して成功しました。

認証は、Web ページ上のすべての要素に対する get 要求ごとに生じます。

FTP

1. ファイアウォール・ホストにアクセスするには、FTP プロキシーを使用します。(ファイアウォールのホスト名には、ftp_gw.domain.net.com を使用します)。

   ```
   ftp ftp_gw.domain.net.com
   ```

   プロキシー・サーバーは、ユーザー名を要求してきます。

   ```
   login:
   ```
2. ファイアウォールの使用を許可されているユーザー名を入力します。

   ```
   login: jane_doe
   ```

サーバーは、ユーザー名をファイアウォールに追加する時に選択された認証方式に従ってユーザー ID を妥当性検査します (77ページの『IBM Firewall へのユーザーの追加』 を参照)。ユーザーがプロキシー・サーバーによってどのように認証されるかについては、 87ページの『認証方式』 を参照してください。

ユーザーが認証されると、プロキシー・サーバーは FTP コマンド・プロンプトを表示します。

```
ftp>
```

次のように、FTP コマンドの quote と site を使用して外部ホストに接続します。

```
ftp> quote site forhost.network.outside.com
```

ここで外部ホストは、接続するためのユーザー名とパスワードを要求します。このユーザー名とパスワードは、Firewall への FTP を行うために使用したものと異なっている可能性があることに注意してください。

ログインのデフォルト・タイムアウト値は 60 秒で、アイドル・プロキシーのデフォルト・タイムアウト値は 7200 秒です。デフォルト・タイムアウト値を変更するには、98ページの『FTP および Telnet プロキシーのタイムアウト値の上書き』を参照してください。

透過的 FTP

ファイアウォールを通して透過的に ftp することができます。 透過的プロキシーにはファイアウォール認証は必要ありません。したがって、透過的プロキシーのユーザーを、ファイアウォール・プロキシー・ユーザーとして定義する必要はありません。 透過プロキシーは、ファイアウォールの内部ネットワーク側からファイアウォー

ルの外部ネットワーク側への送信の場合にのみ許可されます。 透過プロキシーを機能させるには、構成クライアントの「セキュリティー・ポリシー」パネルでそれを選択する必要があります。

1. ftp を使用してファイアウォール・ホストをアクセスします。(ファイアウォールのホスト名には、 ftp_gw.domain.net.com を使用します。)

   ```
   ftp ftp_gw.domain.net.com
   ```

2. プロキシー・サーバーは、ユーザー名を要求してきます。

   ```
   USER:
   ```

3. 非セキュア・ネットワークで次のユーザー名を入力します。

   ```
   USER: username@remote_site_host_name
   ```

4. 前のステップで入力したユーザー名のパスワードを入力するように、ターゲット・ホストから要求されます。

   ```
   password:
   ```

5. パスワードを入力してください。

ログインのデフォルト・タイムアウト値は 60 秒で、アイドル・プロキシーのデフォルト・タイムアウト値は 7200 秒 (2 時間) です。デフォルト・タイムアウト値を変更するには、98ページの『FTP および Telnet プロキシーのタイムアウト値の上書き』を参照してください。

Telnet

ファイアウォール・プロキシー・サーバーにログインするには、telnet プロキシーを使用します。 ホスト名またはインターネット・アドレスのいずれかを使用することができます。 次に、身分証明が認証されてから、ファイアウォール で Telnet コマンドを使用して希望のホストにログインします。 たとえば、セキュア・ネットワークの内部から Telnet を使用して、ホスト名 telnet_gw でファイアウォールを通過し、最終的な宛先 forhost.network.outside.com をアクセスしてみましょう。

1. 処理を開始するには、Telnet を使用して、ファイアウォール・ホストにアクセスします。 (ファイアウォールのホスト名には、telnet_gw.domain.net.com を使用します。)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. プロキシー・サーバーは、ユーザー名を要求してきます。

   ```
   login:
   ```

3. ファイアウォールの使用を許可されているユーザー名を入力します。

   ```
   login: jane_doe
   ```

サーバーは、ユーザー名をファイアウォールに追加する時に選択された認証方式に従ってユーザー ID を妥当性検査します (77ページの『IBM Firewall へのユーザーの追加』 を参照)。ユーザーがプロキシー・サーバーによってどのように認証されるかについては、 87ページの『認証方式』 を参照してください。

ワン・アクト・シェルを使用してください。 IBM Firewall プロキシー telnet デーモンを使用すれば、すべての通信がファイアウォールを通過します。

ワン・アクト・シェルを使用している場合は、ユーザーが認証された後、プロキシー・サーバーは次を表示します。

```
ENTER DESIRED HOST:
```

次のように入力します。

```
telnet forhost.network.outside.com
```

外部ホストは、そのホストで認識されているユーザー名およびパスワードを尋ねます。このユーザー名とパスワードは、ファイアウォール・プロキシー・サーバーで使用したものと異なっている可能性があります。

ログインのデフォルト・タイムアウト値は 60 秒で、アイドル・プロキシーのデフォルト・タイムアウト値は 7200 秒です。デフォルト・タイムアウト値を変更するには、98ページの『FTP および Telnet プロキシーのタイムアウト値の上書き』を参照してください。

透過的 Telnet

ファイアウォールを通して透過的に telnet することができます。 透過的プロキシーにはファイアウォール認証は必要ありません。したがって、透過的プロキシーのユーザーを、ファイアウォール・プロキシー・ユーザーとして定義する必要はありません。 透過プロキシーは、ファイアウォールの内部ネットワーク側からファイアウォールの外部ネットワーク側への送信の場合にのみ許可されます。 透過プロキシーを機能させるには、構成クライアントの「セキュリティー・ポリシー」パネルでそれを選択する必要があります。

1. Telnet を使用してファイアウォール・ホストをアクセスします。 （ここでは、ホスト名として `ftp_gw.domain.net.com` を使用します。）

   ```
   telnet telnet_gw.domain.net.com
   ```

2. プロキシー・サーバーは、ユーザー名を要求してきます。

   ```
   Login:
   ```

3. 非セキュア・ネットワークで次のユーザー名を入力します。

   ```
   Login@remote_host
   ```

外部ホストは、そのホストで認識されているユーザー名およびパスワードを尋ねます。このユーザー名とパスワードは、ファイアウォール・プロキシー・サーバーで使用したものと異なっている可能性があります。

ログインのデフォルト・タイムアウト値は 60 秒で、アイドル・プロキシーのデフォルト・タイムアウト値は 7200 秒です。デフォルト・タイムアウト値を変更するには、98ページの『FTP および Telnet プロキシーのタイムアウト値の上書き』を参照してください。

FTP および Telnet プロキシーのタイムアウト値の上書き

FTP および Telnet は、ログインおよびアイドル状態での待機についてのタイムアウト値を持っています。デフォルトでは、ログインおよびユーザー認証の最中は、少なくとも 60 秒に 1 回はセッション活動があるものとしています。これをログイン・タイムアウトとしています。

ログインが正常に完了した場合は、少なくとも 7200 秒、またはセッションが切断されるまでに 1 度はセッション活動があるものとしています。

これらのデフォルト値をオーバーライドするには、 fwTimeout.cfg ファイルを ROOTDIR¥config ディレクトリーに作成し、新しいタイムアウト値を秒単位で指定します。 fwTimeout.cfg ファイルは、以下の形式で作成します。

```
telnet
proxyTimeout=7200
loginTimeout=60

ftp
proxyTimeout=7200
loginTimeout=60
```

第14章 ファイアウォール・ログのモニター

この章では、アラートのログをリアルタイムでモニターする方法について説明します。構成されたしきい値に違反すると、アラートが生成されます。

IBM Firewall は、起こりうる危険な状況に備えるために、ユーザー定義のしきい値に基づいてファイアウォール・ログに送られるメッセージを監視します。しきい値違反の場合は、ファイアウォール管理者が指定した方法でファイアウォールからアラートが出されます。

しきい値定義

しきい値は、カウントおよび時間のパラメーターで構成されています。カウント (特定のイベントの発生件数) が指定時間内 (分単位) で超過すると、しきい値に違反が生じ、アラート・メッセージが生成されます。ログ・モニターは、次の 4 つのタイプのしきい値を認識します。

1. 認証失敗全体
2. 特定のユーザー ID に対する認証失敗
3. 特定のホストで生じた認証失敗
4. ログ内でのメッセージ・タグのオカレンス

すべてのしきい値は、構成クライアントまたはコマンド行インターフェースを使用して構成されます。しきい値定義が変更されると、すべての変更内容が IBM Firewall によって自動的に保存されます。

アラート・メッセージ

しきい値に達すると、IBM Firewall がアラート・メッセージを生成します。 アラート・メッセージは、次のいずれかの形式で出すことができます。

1. ログ・ファイルへの入力
   - 構成クライアントまたはコマンド行を介して構成できる、 **アラート・ログ**機能を使用して。
   - **ファイアウォール・ログ**に。
2. 電子メールによる、ユーザー・リストへのメール
3. 構成されたページャー (ポケット・ベル)。103ページの『ポケット・ベル通知サポート』 を参照してください。ただし、現在日本国内においては、TAP プロトコルはサポートされていないため、ページャー (ポケット・ベル) へアラート・メッセージを送信できません。
4. アラート・メッセージを先頭パラメーターにした、ユーザー定義コマンドの実行

アラート・メッセージには、特定のしきい値違反に関係のある情報が含まれています。たとえば、以下のようなものがあります。

```
ICA0001e: アラート -- 20 の認証に失敗
ICA0002e: アラート -- ユーザー root の 10 の認証に失敗
ICA0003e: アラート -- ホスト 56.67.78.89 の 15 の認証に失敗
ICA0004e: アラート -- 3 ログ項目のタグ ICA1234e。
```

ログ・モニターにより出されたアラート・メッセージおよびその他のメッセージは、監視されません。

構成クライアントの使用によるログ・モニターの構成

ここでは、構成クライアントを使用してリアルタイム・ログ・モニターを構成する方法について説明します。 構成クライアントのナビゲーション・ツリーから「システム・ログ」を選択します。ファイル・フォルダー・アイコンをダブルクリックして、表示を拡大します。 「**ログ・モニターしきい値**」をクリックします。

「**ログ・モニターしきい値管理**」ダイアログ・ボックスから、しきい値定義の追加、変更、または削除を行うことができます。

ログ・モニターの追加

しきい値定義を追加するには、「**ログ・モニターしきい値管理**」ダイアログ・ボックスから「**新規**」を選択し、「**オープン**」をクリックします。「**ログ・モニターの追加**」ダイアログ・ボックスが表示されます。次のフィールドに入力します。

1. 「**クラス・タイプ**」の矢印をクリックして、クラス・タイプのリストからタイプを選択します。「クラス・タイプ」は、次のとおりです。
   - メール通知
   - 実行コマンド
   - ユーザー別の認証失敗しきい値
   - 認証失敗全体のしきい値
   - ホスト別の認証失敗しきい値
   - メッセージしきい値
2. クラス・タイプに「メール通知」を選択した場合は、電子メール・アドレスを入力します。複数の「メール通知」クラスを定義することができます。

   すべてのしきい値違反メッセージが、指定された電子メール・アドレスに送信されます。
3. クラス・タイプに「実行コマンド」を選択した場合は、コマンド・ファイル名を入力します。

   ログ・モニターは、アラート・メッセージをこのコマンドの最初のパラメーターとしてコマンドを実行します。 1 つの実行コマンド・クラスのみを定義することができます。
4. クラス・タイプに「メッセージしきい値」を選択した場合は、モニターする IBM Firewall ログ・メッセージからの標準タグであるメッセージ・タグを入力します。
5. いずれかのしきい値クラスを選択した場合は、「しきい値カウント」フィールドに入力します。

   「しきい値カウント」は、指定時間内における失敗イベントの最大許容数です。
6. いずれかのしきい値クラスを選択した場合は、「しきい値時間」フィールドに入力します。

   「しきい値時間」とは、イベントの最初のオカレンスから経過した時間 (分単位) です。

7. いずれかのしきい値クラスを選択した場合は、「はい」または「いいえ」をクリックして、ポケット・ベル通知を活動状態にするかしないかを示します。
8. コメントへの入力は任意です。
9. 「**了解**」をクリックします。

しきい値定義の変更

しきい値定義を変更するには、「**ログ・モニターしきい値管理**」ダイアログ・ボックスから変更対象の項目を選択し、「**オープン**」をクリックします。「**ログ・モニターの変更**」ダイアログ・ボックスが表示されます。

1. 「しきい値カウント」フィールドと「しきい値時間」フィールドについて変更したい内容を入力します。

   「しきい値カウント」とは、指定時間枠内に検出される認証失敗メッセージの最大数です。「しきい値時間」とは、メッセージの最初のオカレンスから経過した時間 (分単位) です。
2. 「**了解**」をクリックします。

しきい値定義の削除

しきい値定義を削除するには、「**ログ・モニターしきい値管理**」ダイアログ・ボックスから削除対象の項目を選択し、「**削除**」をクリックします。削除の確認をするよう要求されます。「**はい**」をクリックして確認します。「削除」は、ログ・ファイルからの削除ではないことに注意してください。「削除」は定義の削除を意味しています。

ポケット・ベル通知サポート

ファイアウォール上で割り込みアラートが発生したときに、管理者のポケット・ベルにメッセージが送られます。この原理で、ファイアウォールがシステム管理者を呼び出します。ポケット・ベル通知サポートを設定するには、以下の 3 つのポケット・ベル構成要素を設定する必要があります。

1. コマンド・カスタマイズ - この構成要素は、構成クライアントを使用して作成および変更しなければなりません。ポケット・ベル・コマンドに対してはデフォルトが設定され、ログ・モニターがこれを使用しますが、コマンド行から使用することもできます。この構成要素には、ポケット・ベル環境を定義する固有の項目が含まれます。この構成要素の定義およびカスタマイズについての詳細は、105 ページの『コマンド・カスタマイズ』 を参照してください。
2. 通信事業者の管理 - モデムを接続する前に、適切な通信事業者を定義する必要があります。この構成要素には、米国で使用されるデフォルトの通信事業者のリストが含まれています。使用する通信事業者がこのいずれでもない場合は、使用する通信事業者をこの構成要素に追加してください。詳細については、106ページの『通信事業者の管理』 を参照してください。

   通信事業者から電話番号を入手して、通信事業者の既存の電話番号を検査します。通信事業者に問い合わせるときは、必ず、通信事業者のモデム電話番号と購入した特定のサービスに対して有効な他の設定を記録するようにしてください。

3. モデム管理 - モデムを接続する前に、適切なモデム定義を作成する必要があります。これらの定義には、ポケット・ベル通知サポートが使用するすべての関連モデム情報が含まれます。この構成要素には、選択できるモデムのリストが含まれます。このリストに追加することもできますが、モデムによっては、通信事業者のサポートする機器と互換性のないものがあります。モデム定義の保守については、108ページの『モデム管理』 を参照してください。

注: IBM Firewall は、ポケット・ベル通知サポート用にトレース分析プログラム (TAP) 通信プロトコルをサポートします。

サポートされる通信事業者およびモデム

この通信事業者データベース・ファイルには、すべての通信事業者とそれに関連した伝送パラメーターが含まれています。 他の通信事業者を追加することもできます。通信事業者名とモデム電話番号以外のパラメーターとしては、次のものがあります。

- 文字対応型ポケット・ベルには最大メッセージ長、数字対応型ポケット・ベルには最大桁
- ボー・レート、パリティー・ビット、データ・ビット、およびストップ・ビット長

通信事業者を利用する前に、その通信事業者が TAP プロトコルを使用していることを確認してください。

ポケット・ベル・コードには、デフォルト・モデム定義が付いています。それは次のとおりです。

- IBM MOD 448 14400 bps
- IBM 5853 2400 bps
- IBM 7852 28800 bps
- IBM 7855 2400 bps
- 一般 Hayes 互換
- US Robotics Courier 9600 bps
- Zoom V.34

ポケット・ベル通知サポートの構成

「ポケット・ベルの設定」は、コマンド・カスタマイズ・ファイルの構成および通信事業者とモデムの保守のために使用します。ポケット・ベルを使用する場合は、「ポケット・ベルの設定」を使用し、ポケット・ベル環境を設定してから、ログ・モニターを使用します。

構成を始める前に、通信事業者から正確なモデム電話番号、ポケット・ベル ID、およびモデム・パラメーターを入手する必要があります。

ポケット・ベル通知サポートを構成するには、構成クライアントのナビゲーション・ツリーから「システム管理」を選択します。 ファイル・フォルダー・アイコンを

ダブルクリックして、表示を拡大します。「**システム・ログ**」を選択します。ファイル・フォルダー・アイコンをダブルクリックして、表示を拡大します。「**ポケット・ベルの設定**」を選択します。

コマンド・カスタマイズ

「**ポケット・ベルの設定**」を選択すると、使用する通信事業者と、ポケット・ベル・メッセージを書き込むモデムを選択することができます。

コマンド・カスタマイズ設定値

ナビゲーション・ツリーから「**ポケット・ベルの設定**」を選択すると、 105ページの図 26 に示すダイアログ・ボックスとほぼ同じ、コマンド・カスタマイズ設定ができる「**ポケット・ベルの設定**」ダイアログ・ボックスが表示されます。

図 26. ポケット・ベルの設定

入力フィールドへ追加する値を、入力するか選択します。

1. ポケット・ベル ID を入力します。これは通常、通信事業者がポケット・ベルに割り当てる固有の PIN です。
2. ポケット・ベル・メッセージを入力します。これは、ユーザーが送りたいデフォルト・メッセージを含む文字列です。数字対応型ポケット・ベルの場合は、メッセージは数字しか使用できません。文字対応型ポケット・ベルの場合は、テキスト・メッセージを使用することができます。通信事業者の設定で指定された最大メッセージ長を超えないようにしてください。そうしないと、メッセージが切り捨てられることがあります。コロン (:) を使用しないでください。使用すると、それはブランクのスペース文字で置き換えられます。

3. 通信事業者名が定義されていない場合は、「**選択**」をクリックして通信事業者を定義します。「**ポケット・ベル通信事業者の管理**」ダイアログ・ボックスが表示されます。このパネルへの入力方法については、106ページの『通信事業者の管理』 を参照してください。
4. モデム名が定義されていない場合は、「**選択**」をクリックしてモデムを定義します。「**ポケット・ベル・モデムの管理**」ダイアログ・ボックスが表示されます。このパネルへの入力方法については、108ページの『モデム管理』 を参照してください。
5. 「**了解**」をクリックします。

コマンド・カスタマイズの変更

ナビゲーション・ツリーから「**ポケット・ベルの設定**」を選択すると、コマンド・カスタマイズの設定ができる「ポケット・ベルの設定」ダイアログ・ボックスが表示されます。

1. 入力フィールドへの値を入力するか選択して、既存のカスタマイズ入力フィールドの値を変更します。
2. 「**了解**」をクリックします。

コマンド・カスタマイズの削除

1. 「**ポケット・ベル通信事業者の管理**」ダイアログ・ボックスまたは「**ポケット・ベル・モデムの管理**」ダイアログ・ボックスの項目を削除するには、リストから項目を選択して、「**削除**」をダブルクリックします。

   削除の確認をするよう要求されます。
2. 「**はい**」をクリックして削除を確認するか、または「**いいえ**」をクリックして「**ポケット・ベルの設定**」ダイアログ・ボックスへ戻ります。

カスタマイズ項目が存在しない場合は、ポケット・ベル通知サポートはページを送信できません。

通信事業者の管理

「ポケット・ベルの設定」ダイアログ・ボックスの「**通信事業者名**」フィールドから、「**選択**」をクリックします。 107ページの図 27 に示すダイアログ・ボックスとほぼ同じ「**ポケット・ベル通信事業者の管理**」ダイアログ・ボックスが表示されます。

図 27. ポケット・ベル通信事業者の管理

通信事業者の追加

新しい通信事業者を追加するには、「**ポケット・ベル通信事業者の管理**」ダイアログ・ボックスから「**新規**」を選択し、「**オープン**」をクリックします。該当する入力フィールドに値を入力するか、選択します。

1. 通信事業者名を入力します。この名前は、固有で、かつ通信事業者を十分識別できるだけの情報が含まれていれば、何でも構いません。
2. 通信事業者の電話番号を入力します。これは通信事業者のモデム用の電話番号であり、ボイス・ページングやその他のサービスの番号とは異なります。これは、契約したページング装置およびサービスに必要な、数字対応型または文字対応型ポケット・ベル用の地域または全国をカバーするモデム電話番号でなければなりません。
3. ページング方式には TAP を入力します (これ以外は指定できません)。
4. 通信事業者が許可するか、または必要としているときは、パスワードを入力します。
5. 文字対応型ポケット・ベルの場合は最大メッセージ長を、数字対応型ポケット・ベルの場合は最大桁を入力します。
6. ボー・レートを入力します。矢印をクリックして、リストから値を選択します。
7. パリティー・フィールドの「**偶数**」、「**奇数**」、または「**使用しない**」をクリックします。
8. デフォルトのデータ・ビットを選択します。つまり、**7**または **8**のいずれかをクリックします。
9. **1**または **2**のいずれかをクリックし、デフォルトのストップ・ビットを選択します。
10. 「**了解**」をクリックします。

通信事業者の変更

1. 「**ポケット・ベル通信事業者の管理**」ダイアログ・ボックスから変更したい通信事業者を選択し、「**オープン**」をクリックします。
2. 変更可能なこれらのフィールドの詳細については、 107ページの『通信事業者の追加』 を参照してください。通信事業者名それ自体を変更することはできません。変更しようとすると、このフィールドは使用禁止になります。
3. 希望の変更を行います。
4. 「**了解**」をクリックします。

通信事業者の削除

1. 「**ポケット・ベル通信事業者の管理**」ダイアログ・ボックスから削除したい通信事業者を選択し、「**削除**」をクリックします。
2. 削除の確認をするよう要求されます。「**はい**」をクリックして確認します。

注: 通信事業者データベースには、常に、少なくとも 1 つの通信事業者が入っていなければなりません。通信事業者が定義されていないと、ポケット・ベル通知サポートは失敗します。

モデム管理

ご使用のモデムのマニュアルには、モデムの初期設定方法についての関連情報が含まれているはずです。通信事業者に合わせてモデムの設定を調整する必要がある場合があります。通常は、標準モデム・コマンドを使用する Hayes 互換モデムのみがサポートされます。

「**ポケット・ベルの設定**」ダイアログ・ボックスのモデム名フィールドで、「**選択**」をクリックします。 109ページの図 28 に示すダイアログ・ボックスとほぼ同じ「**ポケット・ベル・モデムの管理**」ダイアログ・ボックスが表示されます。

図 28. ポケット・ベル・モデムの管理

このダイアログ・ボックスを使用して、さまざまなモデムを追加、変更、または削除することができます。

モデムの追加

新しいモデム定義ファイルを追加するには、「**ポケット・ベル・モデムの管理**」ダイアログ・ボックスで「**新規**」を選択し、「**オープン**」をクリックします。「**モデムの追加**」ダイアログ・ボックスで、入力フィールドへの値を入力するか、選択します。

1. モデム名を入力します。この名前は、他のモデム定義に対して固有で、かつモデムを十分識別できるだけの情報が含まれていれば、何でも構いません。
2. COM ポート番号を入力します。これにより、モデムを接続するシリアル COM ポートが定義されます。 10 より小さい番号を入力します。モデムをこのポートへハードウェア的に構成しなければなりませんが、 Windows NT へ定義してはいけません。定義すると、ポケット・ベル機能のそのポートへのアクセスが禁止されます。モデムのハードウェア設定が適切でないと、ポケット・ベル・コードが何度も再試行を繰り返し、ついには失敗します。
3. 初期設定ストリングを入力します。このストリングでモデムを、X レベル 4 のエコーを持ち、ローカル・サイトで定義された固定ボー・レートを持つデータ・モデムとして定義します。 AT コマンドは含めないでください。ポケット・ベル機能は初期設定ストリングの先頭にこれを付けます。
4. 外線接頭部を入力します。これは、社外に電話するための番号です。
5. 「**了解**」をクリックします。

モデムの変更

1. モデム定義ファイルを変更するには、「**ポケット・ベル・モデムの管理**」ダイアログ・ボックスでモデム名を選択し、「**オープン**」をクリックします。

「**モデムの変更**」ダイアログ・ボックスに、変更できるモデム定義のフィールドのリストが示されます。これらのフィールドの説明については、 109ページの『モデムの追加』 を参照してください。

2. 「**了解**」をクリックします。

モデムの削除

1. モデム定義ファイルを削除するには、「**ポケット・ベル・モデムの管理**」ダイアログ・ボックスでモデム名を選択し、「**削除**」をクリックします。
2. 削除の確認をするよう要求されます。「**はい**」をクリックして確認します。

ポケット・ベル通知ロギング

ポケット・ベル通知プロセスは、ファイアウォール・ログ・ユーティリティーを使用して出力ログを作成します。すべてのポケット・ベル・メッセージおよびエラーは、ファイアウォールの一般的なシステム・ログ機能に書き込まれます。 ファイアウォール・ログ・ファイルの設定方法および使い方については、 113ページの『第15章 ログ・ファイルとアーカイブ・ファイルの管理』 を参照してください。

ポケット・ベル設定のテスト

ポケット・ベルの設定を検査するには、ポケット・ベル・コマンドを使用します。詳しくは、*IBM Firewall 解説書* を参照してください。ポケット・ベルの設定を定義または変更したときは、システム、モデム、通信事業者、およびページング装置が互いに正常に通信し、ページが実際に送受されることを、ポケット・ベル・コマンドを使用して確認するよう強くお勧めします。

実行コマンド

アラートしきい値が到着する度に呼び出すプログラムを指定することができます。以下のようにして、プログラムを指定します。

1. 「**ログ・モニター管理**」をクリックし、「**新規**」をダブルクリックします。

   「**ログ・モニターの追加**」ダイアログ・ボックスが表示されます。

2. 「**クラス・タイプ**」ドロップダウン・ボックスで、「**実行コマンド**」を選択します。これにより、パネルの「**コマンド・ファイル名**」フィールドが可能になります。
3. 「**コマンド・ファイル名**」フィールドに、アラートしきい値が到着するときに呼び出すプログラムの完全修飾のパス名を入力します。

   ログ・モニターにより実行されるコマンドの作業ディレクトリーは、`¥winnt¥system32` です。コマンド・シェルは、システム・プロセスから立ち上がるため、システム環境変数だけが設定されます。ユーザー環境変数は設定されません。一般に、立ち上がったプログラムは、絶対パスによるファイル名を使用し、パスファイル名変数に依存しません。

   ファイアウォールは、以下のように、完全なアラート・メッセージを、プログラムの最初のパラメーターとして渡します。

認証障害アラート全体: ICA0001e
ユーザーごとの認証障害アラート: ICA0002e
ホストごとの認証障害アラート: ICA0003e
メッセージしきい値アラート: ICA0004e

これらのメッセージの完全な説明については、*IBM Firewall 解説書* を参照してください。

第15章 ログ・ファイルとアーカイブ・ファイルの管理

この章では、構成クライアントを用いてログ機能を使用する方法を説明します。 ユーザーが各種の IBM Firewall サーバーを介してホストにアクセスしようとすると、 IBM Firewall は、IBM Firewall ロギング・サービス によって保守されているログ・ファイルに項目を書き込みます。

IBM Firewall は、ファイアウォールの構成方法に従って、大量のログ情報を生成します。ログ項目は、socks やエキスパート・フィルターなどのさまざまな場所で発生します。さらに、ログ・ファイルは、デバッグ、情報、またはエラーなどのさまざまな重大度レベルで書き込まれます。この章では、ログ管理機能とログ・アーカイブ管理機能を使用してログ・ファイルとアーカイブ・ファイルを管理する方法についても説明します。

構成クライアントの使用によるログ・ファイル作成およびアーカイブ操作

構成クライアントは、ログ管理とログ・アーカイブ管理に使用することができます。 すべてのログ情報を収容できるほどの十分な大きさをもつディスク・スペースが使用可能であると想定しています。ファイアウォールは、 ファイアウォール・ログ機能に対してルーチン・デバッグおよびエラー情報を生成します。 ファイアウォール・ログ機能にアクセスできるのは、1 次ファイアウォール管理者だけです。アラート・メッセージは、アラート・ログ機能に送られます。 管理監査ログ情報は、監査ログ機能に送られます。

レポート機能を正常に動作させるために大切なことは、ファイアウォール・ログ・メッセージだけを入力ファイルに記述することです。 ファイアウォール・ログと同じファイルに他の機能が送信されないようにしなければなりません。それを考慮に入れてシステム・ログを設定してください。

構成クライアントのメイン・パネルにアラートを表示したい場合は、 アラート・ログ機能として指定されたファイルにアラートを送信する必要があります。その他のものをこのファイルに指定してはなりません。

次の優先順位は下にいくほど大きくなります。「デバッグ」は大抵の情報を取り込みます。「重要」は、最も重大なファイアウォール・イベントのみを取り込みます。

- デバッグ
- 情報
- 警告
- エラー
- 重要

ファイアウォール・プロシージャーが安定するまで、「情報」レベルから始めることをお勧めします。その後で、「警告」または「エラー」に変更すれば、ログ活動とシステム ・ログ・サイズを減らすことができます。

優先順位レベルは、メッセージ・タグの接尾部 *(i,e,w,s..)* に*正確に対応しません*。. 特定のメッセージをシャットオフする方法を判別しておく必要があるかもしれません。

ログ機能の追加

構成クライアントのナビゲーション・ツリーの「システム管理」ファイル・フォルダー・アイコンをダブルクリックして、表示を拡大します。「システム・ログ」ファイル・フォルダー・アイコンをダブルクリックして表示を拡大します。「ログ機能」を選択します。「**ログ機能**」ダイアログ・ボックスが表示され、現在使用可能になっているログ機能のセットが示されます。

1. 現在使用可能になっているこれらのログ機能にシステム・ログ項目を追加するには、「**ログ機能**」ダイアログ・ボックスから「**新規**」を選択し、「**オープン**」をクリックします。

   114ページの図 29 に示す、「**ログ機能の追加**」ダイアログ・ボックスが表示されます。

図 29. ログ機能の追加

2. 「**タイプ**」の矢印をクリックしてタイプを選択します。ファイル名を入力します。
3. ログ機能は、ログに記録する情報のタイプと送信元を判別します。「**機能**」の矢印をクリックして次のログ機能のいずれかを選択します。

- ファイアウォール・ログ - 一般的なファイアウォール・ログ。フィルター・ロギングも含みます。
- アラート・ログ - アラート表示を取り込むために使用されたログ・モニター・デーモン状況およびしきい値違反警告。
- メール・ログ

4. 「**優先度**」の矢印をクリックして、優先度を選択します。重大度が大きくなっていくように、ロギングの優先度がリストされます。選択した優先度は、最低レベルでログに記録されます。
5. ログ・ファイル名を入力します。ログ・ファイル名が絶対パス (ドライブ名と円記号 ¥ で始まる) を持っていて、そのファイルへのパスが存在していなければなりません。
6. アーカイブ管理は、*ファイル名タイプ・ログ*機能を用いてしか使用できません。ログ・ファイル・サイズが使用可能になると、定期的にそれを削減することができます。アーカイブ管理を使用可能にすることは、`fwlogmgmt` コマンドが依存するパラメーターを設定することを意味します。詳しくは、116ページの『ログのアーカイブ』を参照してください。アーカイブ管理パラメーターを使用可能にしたり、使用不可にしたりできます。
7. アクティブ・ログ内のレコードがアーカイブされるまでの全日数を選択します。この値は、ゼロまたはそれ以上でなければなりません。 `fwlogmgmt -l` コマンドが、この基準を満たすアクティブ・ログ・レコードを検出すると、アーカイブが生じます。ログ管理では、ログ・レコードを保持する日数を計算する時に、当日は含めません。
8. アーカイブ・ファイル名および完全なパスを入力します。 IBM Firewall は、ディレクトリーを使ったデフォルトのアーカイブ機能を提供します。ただし、必要な場合は、プラグイン・アーカイブ機能を使用することもできます。
9. アーカイブ済みログ・ファイルがアーカイブから削除されるまでの全日数を選択します。この値は、ゼロまたはそれ以上でなければなりません。 `fwlogmgmt -a` コマンドが、この基準を満たすアーカイブ済みファイルを検出すると、除去が行われます。ログ管理では、アーカイブ済みファイルを保持する日数を計算する時に、当日は含めません。
10. 「**了解**」をクリックします。

ログ機能の変更

1. 「**ログ機能**」ダイアログ・ボックスから変更したいファイアウォール・ログ項目を選択し、「**オープン**」をクリックします。

   「**ログ機能の変更**」ダイアログ・ボックスが表示されます。
2. 希望のフィールドを変更します。これらのフィールドの説明については、114ページの『ログ機能の追加』 を参照してください。
3. 「**了解**」をクリックします。

ログ機能の削除

1. 「**ログ機能**」ダイアログ・ボックス上の現在使用可能になっている項目からファイアウォール・ログ項目選択し、「**削除**」をクリックします。

   「**削除の警告**」パネルが表示されます。

2. 削除を続行したい場合は、「**了解**」をクリックします。停止する場合は、「**取消**」をクリックします。「取消」をクリックすると、実際のログ・ファイルは削除されません。

ログのアーカイブ

アーカイブ・プロセスでは、以下のことを行います。

- アクティブ・ログから該当のレコードを除去します。
- これらのレコードを別々のファイルに置きます。
- 結果ファイルを圧縮します。
- 新規ファイルをアーカイブ・ディレクトリーに入れます。

蓄積されたログ・レコードをアーカイブするためのログ管理プログラムを開始するには、次の 2 つの方法があります。

1. コマンド行から `fwlogmgmt -l` コマンドを実行する。
2. NT スケジュール・サービスとして `fwlogmgmt -l` コマンドを設定する。

ログ・アーカイブを除去すると、該当のアーカイブ・ファイルがアーカイブ・ディレクトリーから削除されます。

アーカイブ・ファイルを除去するには、次の 2 つの方法があります。

1. コマンド行から `fwlogmgmt -a` コマンドを実行する。
2. NT スケジュール・サービスとして `fwlogmgmt -a` コマンドを設定する。

該当のレコードおよびファイルは、ログ機能定義で指定された値によって判別されます。詳しくは、114ページの『ログ機能の追加』 を参照してください。

ログ管理プロセスを実行する最も効率的、または便利な方法は、ログ管理プロセスを NT スケジュール・サービスとして設定することです。「コントロール パネル」の「サービス オブジェクト」を使用して、プロセスを開始してください。

たとえば、ログ管理アーカイブ・プロセスを毎日午前 3:00 に実行するように設定するには次のように入力します。

```
at 3:00 /every:M,T,W,Th,F,S,Su fwlogmgmt -l
```

プラグイン DLL

IBM Firewall のデフォルト DLL を置換するために使用できるファイアウォール・アーカイバーのプラグイン DLL の詳細については、 *IBM Firewall 解説書* を参照してください。

ログ管理出力

ログ管理機能は、ログ管理アクティビティーを行う前に、いくつかの予備的な保全性検査を行います。コマンド行から `fwlogmgmt` コマンドを実行すると、問題発生時に診断結果がファイアウォール・ログ機能に送られます。

メール・ログ機能または管理監査 (local0) ログ機能は、他の機能とは異なるアーカイブ規則を条件とします。すべてのログ機能は、アーカイブがアーカイブ用に使用可

能になるよう要求します。ただし、ファイアウォール (local4) およびアラート (local1) の各ログ・レコードは、これらの日付が、アーカイブ処理の実行時に、機能定義で指定した基準を超えたときにのみアーカイブされます。その一方、すべてのメール用または監査用のログ・ファイルはそのたびにアーカイブされます。また、メール・ログの情報はデバッグ目的に考慮され、通常この情報をアーカイブする価値はあまりありません。他方で、一般的により有益なメール情報は、ファイアウォール (local4) ログ内に記録されます。

レポート・ユーティリティー

レポート・ユーティリティー機能を使用して、最新の、またはアーカイブされたログ・ファイルからレポートを作成すると便利です。 レポート・ユーティリティーは、編成および形式設定された管理情報を表形式のファイルで生成するため、リレーショナル・データベース・テーブルへのマッピングが容易です。 これらのテーブルは、ファイアウォール管理者が以下の分析をする際、役に立ちます。

- ファイアウォールの一般的な使用法
- ファイアウォール処理でのエラー
- セキュア・ネットワークへの無許可アクセス

管理者は、これらのユーティリティーとファイアウォール・ログを使用して、系統づけられたメッセージ・テキスト・ファイルを作成することができます。さらに、表形式のファイルを作成して、DB2 ファミリー製品などのリレーショナル・データベース・システムへインポートすることができます。管理者は、構造化照会言語 (SQL) を使用してデータを照会し、レポートを生成することができます。

レポート・ユーティリティーは、ファイアウォール・インストールの一部としてインストールされています。レポート・ユーティリティーを別々にインストールして、非ファイアウォール・ホスト上で実行することもできます。構成クライアントを使用して、これらのユーティリティーをファイアウォールで実行することができます。非ファイアウォール・マシンの場合は、コマンド行を使用します。

レポート機能を正常に動作させるために大切なことは、**ファイアウォール・ログ・メッセージ**だけを入力ファイルに記述することです。 **ファイアウォール・ログ**と同じファイルに他の機能が送信されないようにしなければなりません。それを考慮に入れてファイアウォール・ロギングを設定してください。

IBM Firewall AIX 版 バージョン 3.1 より以前のログ・ファイルに対して、レポート機能を使用しないでください。ただし、IBM Firewall AIX 版 バージョン 3.1 以降のログ・ファイルを処理するためにレポート機能を使用することはできます。これらの機能を使用して AIX su ログを処理することもできます。レポート・ユーティリティーの詳細については、 *IBM Firewall 解説書* を参照してください。

構成クライアントの使用によるレポート・ユーティリティーの実行

構成クライアントのナビゲーション・ツリーの「システム管理」ファイル・フォルダー・アイコンをダブルクリックして、表示を拡大します。「システム・ログ」ファイル・フォルダー・アイコンをダブルクリックして表示を拡大します。「**レポート・ユーティリティー**」を選択します。 118ページの図 30 に示す、「**レポート・ユーティリティー**」ダイアログ・ボックスが表示されます。

図 30. レポート・ユーティリティー

1. IBM Firewall に備え付けのデフォルトのアーカイバーの場合、ログ・アーカイブ・パス名には、圧縮ログ・ファイルが入っているディレクトリーを指定します。「**ログ機能**」ダイアログ・ボックスの「アーカイブ・ディレクトリー」フィールドに指定したディレクトリーを「ログ・アーカイブ・パス名」フィールドへ入力します。アーカイブ・ファイルへの絶対パス名を入力します。アーカイブされていないログ・ファイルを表示したい場合は、このフィールドをブランクにしておきます。
2. 「**レポート・タイプ**」を選択します。拡張されたログ・メッセージ・テキストを作成するには、「**テキスト・ログ**」を選択します。 DB2 用の表形式ファイルを作成するには、「**テーブル・ログ**」を選択します。こうして作成されたファイルを DB2 にインポートする場合は、ログ・データについて SQL 照会を行うことができます。詳しくは、*IBM Firewall 解説書* を参照してください。
3. ログ・ファイル名に指定するのは、圧縮されたアーカイブ・ログ・ファイルのいずれか 1 つ、他の有効な**ファイアウォール・ログ**、または AIX su ログ・ファイル名です。「ログ・アーカイブ・ディレクトリー」フィールドにデータを入力した場合は、「**ログ・ファイル名**」の矢印をクリックして、処理対象のログを選択することができます。ステップ 1 で「ログ・アーカイブ」を入力しない場合は、

ここで入力する「ログ・ファイル名」を、有効な圧縮ファイアウォール・ログ・ファイルまたは su ファイル・ログの名前にしなければなりません。全パスを指定する必要があります。

4. **Firewall** または **AIX su** のいずれかの**ログ・タイプ**を選択します。
5. **出力テキスト用のパスおよびファイル名**を入力します。
6. 「**はい**」を選択して、テーブル・ログ要求の結果を既存の表形式ファイルに追加するか、または「**いいえ**」を選択して既存のファイルを置き換えます。
7. このフィールドにより、出力テキスト・ファイルに置かれるメッセージの特定のタイプを選択できます。このフィールドのコンテンツは、標準 Windows NT の Find コマンドへ配置されるパラメーターとして処理されます。たとえば、フィールドに ″ICA0″ と入力すると (引用符必須)、以下のコマンドを実行している場合でも、このコンテンツはパラメーターとして処理されます。

   ```
   fwlogtxt < my.log | find "ICA0"
   ```

   以下は、このフィールドへ配置できるいくつかの例とその結果です。

フィルター	結果
"ICA0"	ログ・モニターしきい値のアラート・メッセージをリスト
"ICA3"	Socks 関連のメッセージ (#ICA3000 - 3999) をリスト
"ICA2010"	ICA2010 メッセージのオカレンスのみをリスト
/V "ICA3"	Socks メッセージ以外のメッセージをすべてリスト
/C "ICA001"	ICA0001 メッセージ数をカウント

8. 「**了解**」をクリックすると、要求したファイルが指定の出力ディレクトリーに作成されます。
9. 「レポート・ユーティリティーの結果」領域には、実行されたレポート・ユーティリティーからのエラー・メッセージが表示されます。「テキスト・ログ」レポート・タイプからの結果ログ・テキストを表示するには、ファイアウォールの「構成クライアント」のメイン・パネル上の「**ログ・ビューアー**」をクリックして、完全修飾の出力ファイル名を入力します。「テーブル・ログ」レポート・タイプの結果の .tbl ファイルをデータベースにロードする方法については、 *IBM Firewall 解説書* を参照してください。

第16章 ネットワーク・アドレスの変換

インターネットの急速な発達に伴い、IP アドレスの不足が重要な問題となっています。ネットワーク・アドレス変換 (NAT) を使用すると、アドレスの再利用に基づいて、IP アドレスの不足の問題を解決することができます。

専用ネットワーク内のアドレスには、非常に広いアドレス空間 (一般的に 1 アドレス空間当たり 10.0.0.0. クラス) を割り当てることができます。これらは専用のアドレスで、インターネットで公開することはできません。したがって、これらのアドレスを別の IP ネットワークが再利用することができます。単一の登録済み IP アドレスを使用すると、たくさんの専用ネットワーク・アドレスが隠されます。 NAT は未登録のアドレスとポート番号を有効な登録済みインターネット・アドレスとポート番号に変換します。インバウンド指示では、NAT は登録済みのインターネット・アドレスとポート番号を未登録のアドレスとポート番号に変換し直します 。 NAT の利点は、ネットワークが、専用のまたは無許可のアドレスを使用してインターネット上のホストと通信できることであり、これによって、専用ネットワークに広いアドレス空間をもつことができます。さらに、NAT を使用することによって、セキュリティーの追加レベルを提供する外部から、専用ネットワーク内のアドレスを隠すこともできます。

121ページの図 31 は、IBM Firewall 環境での基本 NAT 操作を示しています。

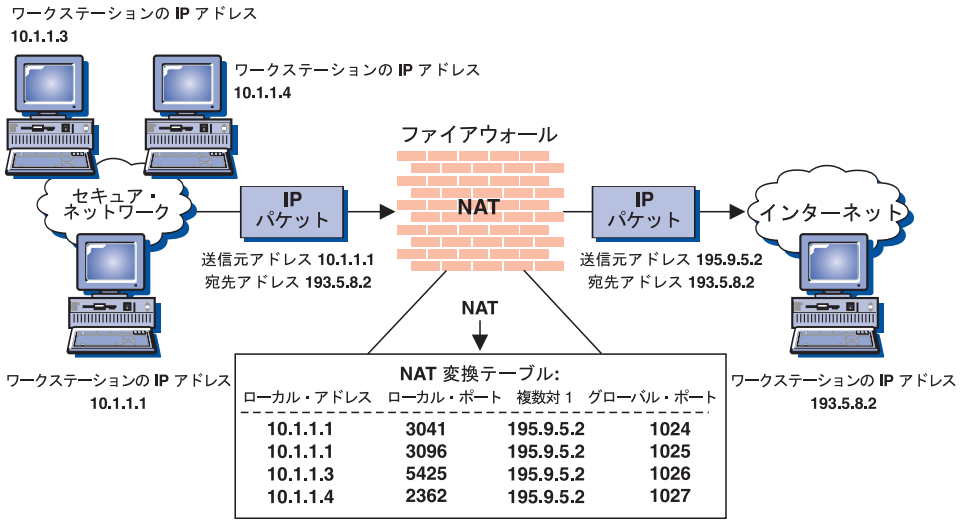

図 31. ネットワーク・アドレス変換

セキュア・ホストで生成した TCP/UDP パケットには、登録済みのインターネット・アドレスと置き換えた送信元アドレスがあります。セキュア・ホストのポートは、固有のポート番号に変換されます。すべてのアウトバウンド・パケットの送信元アドレスは同じですが、ポート番号は固有です。複数対 1 の変換と呼ばれるこの変換形式によって、多くのセキュア・ホストを単一のアドレスに隠すことができます。 IP ヘッダと TCP/UDP 疑似ヘッダ内におけるパケットの検査概要は更新されます。同時に接続できる最大数は、64536 に制限されます。(実際は64512) これはポート 0 から 1023 は予約済みだからです。インバウンド接続は、(動的というより) 静的変換テーブル入力でサポートされます。たとえば、195.9.5.2 を 10.1.1.1 にマップする NAT 変

換テーブルに静的記入項目がある場合のみ、ホスト 193.5.8.2 は、ホスト 10.1.1.1 で TCP 接続を開始することができます (グローバル・アドレス 195.9.5.2 を使用して)。

TCP/UDP アプリケーションで生成するすべてのパケットを変換します。 IP パケットに含まれるアプリケーション・データに IP アドレスが含まれていると、障害が発生します。アドレス変換にとって特に厄介なアプリケーションは、FTP です。 FTP コントロール接続は、メッセージに ascii コード化した IP アドレスを含む ″PORT″ コマンドまたは ″PASV″ 返信を発行します。この場合、NAT は、IP ヘッダのアドレスだけでなく、ペイロード内の ascii アドレスとポート番号も変更する必要があります。

やがて公開される APAR のリリースによって、 NAT の 複数対 1 と MAP 変換のオプションは、インバウンドとアウトバウンドの ICMP パケットを変換することができるようになります。転送のほかに既存の変換テーブル記入項目がある場合のみ、インバウンドの ICMP 返信パケット (ping、タイムスタンプ、アドレス・マスク) とすべてのエラー・パケット (未着の出力先、ソース消滅、転送、時間超過、および不正なパケット・メッセージ) を変換します。 ICMP 転送は、未変換の NAT の中を移動します。これはフィルター規則に精通していて、ICMP 転送を許可するか、あるいは拒否します。

アウトバウンドの照会・応答 ICMP パケット (ping 要求/応答、タイムスタンプ要求・応答、アドレス・マスク要求応答) は、別のセキュア・ホストからの ICMP パケットが単一の登録済みアドレスを共用できるような、パケットのセキュア・アドレスと ICMP 照会識別子を変換することによって、サポートすることができます。

管理者は、特定の ICMP パケット、特にアドレスのマスク・応答および転送がセキュア・ネットワークと非セキュア・ネットワーク間を流れることができるように注意する必要があります。ファイアウォールを介した ICMP トラフィックに許可される機密保護障害に関する情報については、次のレッドブックを参照してください。このレッドブックは参考文献にリストされ、表題は次のとおりです: *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2* 。

IBM eNetwork Firewall NAT インプリメンテーション

IBM Firewall NAT インプリメンテーションでは、上記で説明したような基本アドレス変換をサポートしていますが、次のような注意事項があります。

- ペイロード内に IP アドレス情報を含む TCP/UDP アプリケーション (下記で説明する FTP を除く) には、上記の通りに変換されたパケット・ヘッダ・フィールドがあるだけです。これは、DNS または SNMP のような UDP アプリケーションには、変換されたペイロード内に含まれるアドレス情報がないことを暗黙指定しています。
- FTP PORT コマンドは完全に変換されます。しかし、 PASV 応答パケットに組み込まれたアドレスは変換されません。
- ICMP 要求・応答と暗号化メッセージは変換されます。これによって、たとえば、アウトバウンド ping が、 TCP パス MTU ディスカバリーと同様に正しく作動できるようにします。

- 動的変換テーブル記入項目を削除し、登録済みの IP アドレスを使用可能なアドレスのプールに戻す前に、NAT はTCP 切断を検出しないどころか、構成可能なアイドル・タイムアウトに応答します。

NAT、フィルターおよびトンネル間の対話の例

123ページの図 32 は、NAT、フィルターおよびトンネル間の対話の例を示しています。

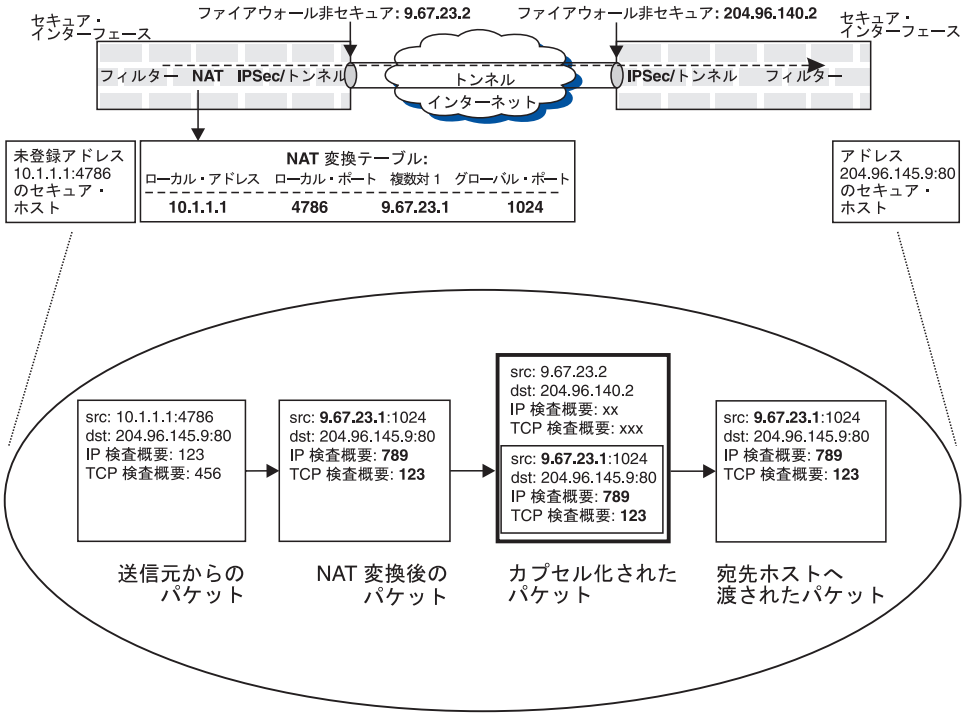

図 32. NAT、フィルターおよびトンネル間の対話の例

IPSec ESP トンネルが、ファイアウォール 9.67.23.2 と 204.96.140.2 の間に設定されていると想定します。 NAT は 9.67.23.2 ファイアウォールでのみアクティブになります。これは、このセキュア・ネットワークは専用アドレスを使用するからです。トンネルのもう一方の端のセキュア・ネットワークは NAT を使用していません。基本 NAT 変換を示すほかに (左から 2 番目のパケット内にある太字のフィールドは、アウトバウンドのアドレス変換中に変更されるパケット内のフィールドを示します)、 123ページの図 32 は、ホストから変換されたパケットが、変換されていない IP パケットにカプセル化されていることも示しています。

一般的に、フィルター処理は、NAT と NAT 変換後のインバウンド・パケットより前のアウトバウンド・パケットに適用されます。したがって、フィルター規則は未変換のアドレスを基本とします。 NAT とトンネルが含まれると、アクティブな NAT をもつファイアウォールのフィルター規則も、未変換のアドレスを基本とします。トンネルのもう一方の端では (NAT がこのファイアウォールではアクティブでないと仮定して)、インバウンド・パケットのフィルター規則は変換済みのソースと宛先アドレスを基本とします (インバウンドとアウトバウンドそれぞれに対し)。 NAT がトンネルの両端でアクティブである場合は、上記の説明は両方向に適用されます。

例として 123ページの図 32 で示したシナリオを使用して、そして、セキュア・ホスト 10.1.1.1 がトンネルの向こう側のセキュア・ホストと通信できるようにすることを目的と想定し、 10.1.1.1 に付加されたファイアウォールには、10.1.1.1 がトンネルの向こう側の 204.96.145 と通信できるようにするフィルター規則がなければなりません。出力先ホストに接続されたほかのファイアウォールでは、フィルター規則は、トンネルを介した 9.67.23.1 と 204.96.145.9 の間の通信が許可されなければなりません。

NAT に関する詳細

次の許可が必要な場合は、NAT を使用します。

- セキュア・マシンのアドレスが保護されている場合に、ファイアウォールの後ろのマシンに直接アクセスする。
- 登録済みのアドレスをもたない複数のマシンが、インターネット上のサイトに達することができるように登録済みのアドレスを共用できるようにする。
- 非セキュア位置以外の位置からほかのマシンが、ファイアウォールの後ろのサーバーにアクセスする。

NAT のために登録済みのアドレスを ISP から獲得します。 NAT のために使用したすべてのアドレスを、ほかの目的に使用することはできません。

NAT には次の 4 つのオプションがあります。

複数対 1 (Many-to-One)
: たくさんの (65536 まで) 内部アドレスが 1 つの登録済み IP アドレスを共用できるように、パケットのセキュア・アドレスとポート番号を変換することを含んでいます。登録済みの IP アドレスを共用した内部アドレスはローカル・アドレスを隠しますが、さらに、ファイアウォールの非セキュア・アドレスに対して、ほかの登録済みのインターネット・アドレスが必要です。NAT 構成は、複数対 1 の記入項目を使用するポート変換に使う登録済みのインターネット・アドレスを識別します。

変換 (Translate)
: 変換するセキュア・アドレスのリストを作成するために使用します。

除外 (Exclude)
: 変換しないセキュア・アドレスのリストを作成するために使用します。

マップ (Map)
: 特定のセキュア・アドレス用に、特定の登録済みアドレスを予約するために使用します。

構成クライアントを使用した、ネットワーク・アドレス変換の構成

1. 構成クライアント・ナビゲーション・ツリーで、アドレス変換ファイル・フォルダー・アイコンをダブルクリックして、表示を拡張します。 NAT ファイル・フォルダー・アイコンをダブルクリックして、表示を拡張します。
2. 「**NAT Setup (NAT セットアップ)**」を選択して、ネットワーク・アドレス変換モジュールを構成します。

125ページの図 33 に示す「**Network Address Translation List (ネットワーク・アドレス変換リスト)**」が表示されます。

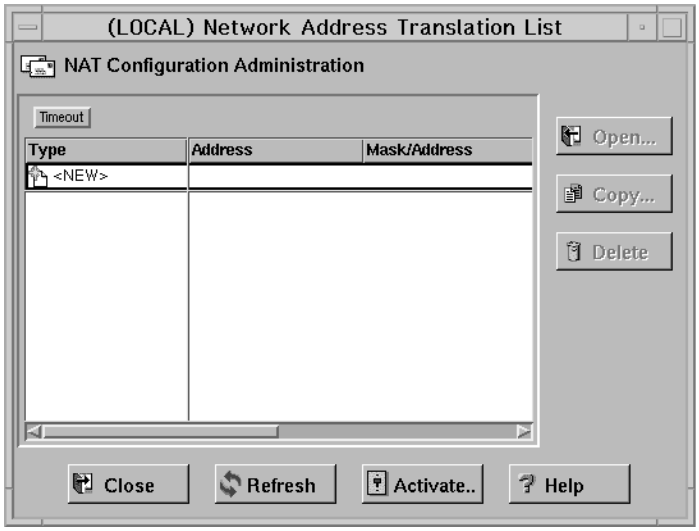

図 33. ネットワーク・アドレス変換リスト

3. NAT 構成ファイルに含まれるネットワーク・アドレス変換記入項目は、このダイアログ・ボックスに表示されます。 NAT 記入項目の追加、変更、または削除を行うこともできます。

NAT 記入項目の追加

1. 「**Network Address Translation List (ネットワーク・アドレス変換リスト)**」から「**New (新規)** 」を選択し、「**Open (開く)**」をクリックして NAT 構成ファイルに新規の記入項目を追加します。

   125ページの図 34 に示すような「**Add NAT (NAT の追加)**」ダイアログ・ボックスが表示されます。

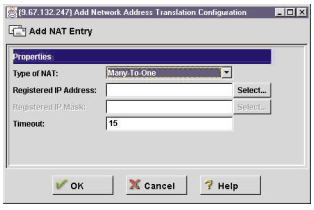

図 34. NAT 構成の追加

2. 「**Add NAT (NAT の追加)**」ダイアログ・ボックスから、「Type of NAT (NAT の型)」フィールドの矢印をクリックして、次の中から選択します。
   - Many-to-One Registered Network Address (複数対 1 の登録済みネットワーク・アドレス): 予約済みの IP アドレスに指定した IP アドレスを追加します。パラメータは、変換テーブルに関連する予約済みの IP アドレスとタイムアウトです。

- Translate Secured Network Address (保護したネットワーク・アドレスの変換): ネットワーク・アドレス変換を必要とするセキュア IP アドレスの範囲を指定します。
- Exclude Secured Network Address (保護されたネットワーク・アドレスの除外): ネットワーク・アドレス変換から除外するべきセキュア IP アドレスの範囲を指定します。
- Map Secured Network Address (保護されたネットワーク・アドレスのマップ): 1 対 1 の保護対登録済みの IP アドレス静的変換を定義します。

複数対 1 の登録済みのネットワーク・アドレス

複数対 1 の登録済みアドレス記入項目がパケットのセキュア・アドレスとポート番号を変換して、たくさんの (65536 まで) 内部アドレスが 1 つの登録済み IP アドレスを共用できるようにします。 これで、1 つの登録済みの IP アドレスで、たくさんのローカル・アドレスを隠すことができます。 (ファイアウォールの非セキュア・アドレスには、追加の登録済みインターネット・アドレスが必要です。)

セキュア・ホストがパケットを非セキュア・ネットワークに送信すると、 1 つの登録済み IP アドレスが割り振られます。この固有の IP アドレスは、 IBM Firewall とセキュア・ネットワークの外のマシンの間で IP フレームをトランスポートするために使用します。

「Add NAT (NAT の追加)」画面から「Many-to-One (複数対 1)」を選択した場合は、次の値を入力します。

Registered IP Address (登録済み IP アドレス)
ISP から獲得します。このアドレスは、すべてのセキュア・アドレスが隠す小数点付き 10 進数の IP アドレスになります。

「**Select (選択)**」をクリックしてネットワーク・オブジェクトを選択し、「**Select Network Object (ネットワーク・オブジェクトの選択)**」ダイアログ・ボックスを入手します。ネットワーク・オブジェクトを選択して、「**了解**」をクリックします。ネットワーク・オブジェクトが、「**Add NAT Configuration (NAT 構成の追加)**」ダイアログ・ボックスの「Network Object (ネットワーク・オブジェクト)」フィールドに追加されます。 あるいは、あらかじめネットワーク・オブジェクトを作成しなかった場合は、フィールドに直接値を入力します。

タイムアウト値
NAT が登録済み IP アドレスを解放できる前に、アドレス変換がアイドル状態でいられる分数を入力します。このタイムアウト値は、この記入項目で指定する IP アドレスの範囲内の登録済み IP アドレスにだけ適用されます。

デフォルトは 15 分です。値の範囲は 5 から 45 です。

保護されたネットワーク・アドレスの変換

保護された IP アドレスの変換の記入項目は、IP アドレス変換を実行するために必要なセキュア・ネットワーク・アドレスのセットを定義します。 デフォルトでは、保護された IP アドレスの変換セット内のすべてのセキュア IP アドレスに対するアドレス変換を実行します。

「Add NAT (NAT の追加)」画面から「Translate (変換)」を選択した場合は、次の値を入力します。

Secured IP Address (保護された IP アドレス)
ネットワーク・アドレス変換に必要なセキュア IP アドレスの範囲を識別する小数点付き 10 進数の IP アドレスを指定します。

「**Select (選択)**」をクリックしてネットワーク・オブジェクトを選択し、「**Select Network Object (ネットワーク・オブジェクトの選択)**」ダイアログ・ボックスを入手します。ネットワーク・オブジェクトを選択して、「**了解**」をクリックします。ネットワーク・オブジェクトが、「**Add NAT Configuration (NAT 構成の追加)**」ダイアログ・ボックスの「Network Object (ネットワーク・オブジェクト)」フィールドに追加されます。 あるいは、あらかじめネットワーク・オブジェクトを作成しなかった場合は、フィールドに直接値を入力します。

Secured IP Address Mask (保護された IP アドレス・マスク)
IP アドレスの範囲を識別するために使用するセキュア IP アドレスでビットを指定するサブネット・マスクのような、マスクを指定します。 0 に設定されるこのマスクのビットは、 0 または 1 をもつビット位置が IP アドレスの範囲内に取り込まれていることを示しています。したがって、マスク内で 255.255.255.255 を指定することは、唯一のセキュア IP アドレスがこの変換記入項目に取り込まれているを示しています。この場合、 255.255.255.0 のマスクは、アドレス変換に必要なクラス C の IP アドレスを示しています。

保護されたネットワーク・アドレスの除外

セキュア IP アドレスの除外記入項目は、IP アドレス変換を実行するために NAT を必要としないセキュア・ネットワーク・アドレスのセットを定義します。 デフォルトでは、保護された IP アドレスの変換セット内のすべてのセキュア IP アドレスに対するアドレス変換を実行します。

「**Add NAT (NAT の追加)**」ダイアログ画面から「Exclude (除外)」を選択した場合は、次の値を入力します。

Secured IP Address (保護された IP アドレス)
ネットワーク・アドレス変換から除外すべきセキュア IP アドレスの範囲を識別する小数点付き 10 進数の IP アドレスを指定します。

「**Select (選択)**」をクリックしてネットワーク・オブジェクトを選択し、「**Select Network Object (ネットワーク・オブジェクトの選択)**」ダイアログ・ボックスを入手します。ネットワーク・オブジェクトを選択して、「**了解**」をクリックします。ネットワーク・オブジェクトが、「**Add NAT Configuration (NAT 構成の追加)**」ダイアログ・ボックスの「Network Object (ネットワーク・オブジェクト)」フィールドに追加されます。あるいは、あらかじめネットワーク・オブジェクトを作成しなかった場合は、フィールドに直接値を入力します。

Secured IP Address Mask (保護された IP アドレス・マスク)
IP アドレスの範囲を識別するために使用する保護された IP アドレスのビットを指定するサブネット・マスクのような、マスクを指定します。 0 に設定されるこのマスクのビットは、 0 または 1 をもつビット位置が IP アドレス

の範囲内に取り込まれていることを示しています。したがって、マスク内で 255.255.255.255 を指定することは、唯一の保護された IP アドレスがこの記入項目で指定されていることを示しています。この場合、 255.255.255.0 のマスクは、クラス C の IP アドレスがアドレス変換から除外されることを示しています。

保護されたネットワーク・アドレスのマップ

保護された IP アドレスのマップ記入項目は、セキュア IP アドレスから登録済みの IP アドレスへの 1 対 1 のマッピングを定義します。 この 1 対 1 のIP アドレスのマッピングは、FTP または Telnet クライアントのような外部アプリケーションのクライアントが、保護されたネットワーク内に常駐するサーバー・マシンを使用して TCP セッションをセットアップできるようにします。セキュア IP アドレスのマップ記入項目内の登録済み IP アドレスは、登録済み IP アドレスの予約記入項目で指定されるIP アドレス空間をオーバーラップすることができます。

「**Add NAT Configuration (NAT 構成の追加)**」ダイアログ・ボックスから「Map (マップ)」を選択した場合は、次の値を入力します。

Secured IP Address (保護された IP アドレス)
指定された登録済み IP アドレスに変換するべき小数点付き 10 進数の IP アドレス。

「**Select (選択)**」をクリックしてネットワーク・オブジェクトを選択し、「**Select Network Object (ネットワーク・オブジェクトの選択)**」ダイアログ・ボックスを入手します。ネットワーク・オブジェクトを選択して、「**了解**」をクリックします。ネットワーク・オブジェクトが、「**Add NAT Configuration (NAT 構成の追加)**」ダイアログ・ボックスの「Network Object (ネットワーク・オブジェクト)」フィールドに追加されます。 あるいは、あらかじめネットワーク・オブジェクトを作成しなかった場合は、フィールドに直接値を入力します。

Registered IP Address（登録済み IP アドレス) フィールド
指定したセキュア IP アドレスが変換される小数点付き 10 進数の IP アドレス。

「**Select (選択)**」をクリックしてネットワーク・オブジェクトを選択し、「**Select Network Object (ネットワーク・オブジェクトの選択)**」ダイアログ・ボックスを入手することができます。ネットワーク・オブジェクトを選択して、「**了解**」をクリックします。ネットワーク・オブジェクトが、「**Add NAT Configuration (NAT 構成の追加)**」ダイアログ・ボックスの「Network Object (ネットワーク・オブジェクト)」フィールドに追加されます。

NAT 記入項目の変更

「**NAT Configuration (NAT 構成)**」ダイアログ・ボックスから既存の NAT 記入項目を選択して、「**Open (開く)**」をクリックし、NAT 構成ファイルの「Network Translation (ネットワーク変換)」記入項目を変更します。

NAT 記入項目の削除

1. 「**NAT Configuration (NAT 構成)**」ダイアログ・ボックスから既存の NAT 記入項目を選択して、「**Delete (削除)**」をクリックし、NAT 構成ファイルの「Network Translation (ネットワーク変換)」記入項目を削除します。

   確認ダイアログボックスが表示されます。
2. 「はい」または「いいえ」を選択します。

NAT 起動

1. 構成クライアント・ナビゲーション・ツリーで、アドレス変換ファイル・フォルダー・アイコンをダブルクリックして、表示を拡張します。 NAT ファイル・フォルダー・アイコンをダブルクリックして、表示を拡張します。
2. 「**NAT Activation (NAT 起動)**」を選択すると、 129ページの図 35 に示すものとほぼ同じダイアログ・ボックスが表示されます。

図 35. NAT 起動

3. 次のいずれかを選択して、「**Execute (実行)**」をクリックすることができます。
   - 指定された NAT 構成ファイルに含まれるネットワーク・アドレス変換記入項目の妥当性検査を行います。
   - 構成を起動/更新し、現在 NAT モジュールが使用する「Network Address Translation (ネットワーク・アドレス変換)」記入項目を表示します。
   - NAT を非活動化し、ネットワーク・アドレス変換を使用不可にします。

- ロギングを使用可能にし、ネットワーク・アドレス変換ロギングを使用できるようにします。
- ロギングを使用不可にし、ネットワーク・アドレス変換ロギングを使用できないようにします。

ロギング

NAT は、NAT ロギングとフィルター・ロギングの両方が使用可能である場合に、エラー条件の種類をログします。 NAT ロギングは、「**NAT Activation (NAT 起動)**」パネルで、または **fwnat** コマンドを使用することによって、使用可能になります。フィルター・ロギングは、「**Log Facility (ログ機能)**」パネルで、または **fwlog** コマンドを使用することによって、使用可能になります。

次の活動は、ファイアウォール・ログ機能にログされます。

- 管理機能 (たとえば、静的または MAP 記入項目)から NAT テーブルへの更新
- NAT 変換テーブルへの動的更新
- エラー・メッセージ
- パケットが破棄される、変換の失敗
- 毎度の活動化および非活動化

NAT のフィルター規則の作成

NAT 構成を完了後、NAT を使用する接続のために、フィルター規則を作成する必要があります。 45ページの『第8章 ファイアウォールによるトラフィックの制御』 を検討し、直接接続のための定義済みサービスを利用します。直接接続のための定義済みサービスの例は、次のとおりです。

- HTTP direct out
- Telnet direct out

詳細については、46ページの『事前定義サービスを用いた接続の作成』 を参照してください。

ネットワークに直接入るサービスが必要な場合は、定義済みサービスを作成する必要があります。これについては、68ページの『構成クライアントを用いたサービスの作成』 を参照してください。

付録. 特記事項

本書において、日本では発表されていない IBM 製品（機械およびプログラム）、プログラミング、およびサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのような IBM 製品、プログラミング、またはサービスを、日本で発表する意図があることを必ずしも示すものではありません。本書で、IBM ライセンス・プログラムまたは他の IBM 製品に言及している部分があっても、このことは当該プログラム、または製品のみが使用可能であることを意味するものではありません。これらのプログラムまたは製品に代えて、IBM の知的所有権を侵害することのない機能的に同等のプログラムまたは製品を使用することができます。ただし、IBM によって明示的に指定されたものを除き、これらのプログラムまたは製品に関連する動作の評価および検査はお客様の責任で行っていただきます。

IBM は、本書で説明する主題に関する特許権（特許出願を含む）、商標権、または著作権を所有している場合があります。本書は、これらの特許権、商標権、および著作権について、本書で明示されている場合を除き、実施権、使用権等を許諾することを意味するものではありません。実施権、使用権等の許諾については、下記の宛先に、書面にてご照会ください。

〒106-0032 東京都港区六本木3丁目2-31
AP事業所
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム（本プログラムを含む）との間での情報交換、および（ii）交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
USA

本プログラムに関する上記の情報は、適切な条件の下で使用することができますが、有償の場合もあります。

本書において解説されているライセンス・プログラムまたはその他のライセンス資料は、 IBM 所定のプログラム計画の契約条項に基づいて、 IBM より提供されます。

本書は、生産的な使用を意図するものではなく、特定物として現存するままの状態で提供され、法律上の瑕疵担保責任を含めて、いかなる保証も適用されません。

この製品には、University of California, Berkeley とその貢献者により開発されたソフトウェアが含まれています。

商標

以下の用語は、IBM Corp. の米国またはその他の国における商標です。

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

Microsoft、Windows 、および Windows 95 のロゴは、 Microsoft Corporation の商標または登録商標です。

Java および HotJava は、Sun Microsystems, Inc. の商標です。

その他の会社、製品、およびサービス名（二重アスタリスク (**) で示されます）は、他社の商標です。

参照文献

インターネットのセキュリティーについて、さらに詳しくお知りになりたい場合は、次の IBM Firewall ホーム・ページをご覧ください。
http://www.software.ibm.com/enetwork/firewall

IBM 資料の情報

ファイアウォール、インターネット・セキュリティー、および一般的なセキュリティーに関する IBM のその他の資料を以下に示します。

ファイアウォール関連

以下の資料は、IBM Firewall の CD-ROM、および IBM Firewall のホーム・ページから入手できます。

- *IBM Firewall Windows NT 版 使用者の手引き*、GD88-7845
- *IBM Firewall Windows NT 版 解説書*、SD88-7846
- *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*, SG24-5209

インターネットおよび WWW 関連

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

一般的なセキュリティー関連

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor AIX 版 使用者の手引き*、SC88-7990
- *TCP/IP 入門*、N:GG24-3376

専門書の情報

以下に示すのは、TCP/IP および UNIX に関する専門書です。

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail*. O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration*. O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook*. Prentice Hall. (ISBN: 0-13-151051-7

以下に示すのは、ファイアウォール、およびインターネット・セキュリティーに関する専門書です。

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)
- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

用語集

IBM ソフトウェア用語集は、次のホーム・ページから入手することができます。 **http://www.networking.ibm.com/nsg/nsgmain.htm**

索引

日本語, 英字, 数字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

［ア行］

［カ行］

［サ行］

［タ行］

［ナ行］

［ハ行］

［マ行］

［ヤ行］

［ラ行］

［ワ行］

D

F

H

I

M

N

S

T

U

W

Printed in Japan

GD88-7845-01