Second edition, 3rd revision, released 05/09/2000.

Written and Edited by
William H Stoner III

Some portions herein written by
Ge Weijers, Sam Napolitano, Diana Holmes, Michael Hullhorst
and Eric D. Osborne

Published by
Progressive Systems, Inc.
2000 West Henderson Road, suite 400
Columbus, Ohio 43220-2453

+1 614 326 4600 (voice)
+1 800 558 7827 (voice)
+1 800 330 7127 opt 3 (voice, support)
+1 614 326 4601 (FAX)
support@Progressive-Systems.Com (technical e-mail)
sales@Progressive-Systems.Com (sales and pre-sales e-mail)
http://www.Progressive-Systems.Com (World-Wide Web)
ftp://ftp.Progressive-Systems.Com (Web-based FTP)
ftp.Progressive-Systems.Com (anonymous FTP)

Comments and corrections concerning material in this User Manual are welcomed and can be forwarded to: **documentation@progressive-systems.com** or **docs@progressive-systems.com.**

目次

1. はじめに

Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) は、MIPS およびインテル・プロセッサ・ファミリを使用するさまざまなハードウェア・プラットフォーム上で稼動します。このユーザー・ガイドは、Phoenix Adaptive Firewall version 1.5.3 のすべてのインプリメンテーションをカバーします。特定のインプリメンテーションごとの相違点については本文中の適切な場所で随時記述されています。

1.1. Phoenix Adaptive Firewall の機能

Progressive Systems 社の Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) は、最も機密なデータをも保護できる高性能な機能を提供します。ネットワーク・セキュリティを保証するために Phoenix が提供している必須機能はつぎのとおりです：

1.1.1 アクセスのロギングおよびモニタ

多くのネットワーク・デバイスでロギング機能が提供されていますが、Phoenix ではアクセス試行を追跡するだけだけでなく、ネットワークが経験している内向きおよび外向きの両方のトラフィックを示すリアルタイムの状態情報も提供されます。

1.1.2 認証

社内ネットワークがインターネットのような公開されたネットワークに接続されているとき、社外のすべてのシステムが自分自身を正しく表現していると考えるのは間違っています。なぜなら、社内ネットワーク内にある信頼できるシステムのネットワーク・アドレスを調べ、その信頼できるホストから送られているように見せるパケットを偽造することが、クラッカーの典型的なテクニックだからです。Phoenix はこの種のアタックの検出および防止が可能です。

1.1.3 安全なリモート管理

Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) では、100% ピュアな Java のグラフィカル・ユーザー・インターフェースが使用されています。Progressive Systems 社は、 Phoenix GUI クライアント (Netscape 4.0.6 またはそれ以降のバージョンなど AWT をサポートしているすべてのブラウザ) と Phoenix サーバの間のトランザクションを外部の介入から保護されるようにデザインしました。これは Web が有効な場所ならどこからでもお客様のファイアウォールを制御できることを意味しています。

1.1.4 パケット・ファイアウォール

一般的に従来のスタティックなパケット・フィルタリングは、ある特定のソース (出発地) ネットワーク・アドレスとデスティネーション (目的地) ネットワーク・アドレスの間のトラフィックを制限するため、またはネットワークの通過を許可する特定のアプリケーションを定義するために使用されます。スタティックなフィルタリングは、長い間ルータおよびブリッジ製品で利用されてきました。このフィルタリング・ルールは定義された限りにおいて柔軟性があるのですが、しかし同時に、ファイアウォール・ルールが不測の事態に対応しきれないという重要な弱点を課題として残しました。 Phoenix はアダプティブ・ファイアウォール技術 (Adaptive Firewall Technology) を使用してこの問題を解決しています。Phoenix はネットワーク上のある特定のトラフィックに適応することが可能です。すなわち、 Phoenix は許可されたアプリケーション間のために許可されたホスト間の接続を必要に応じてオープン、ロックし、さらにはその接続に時間制限をセットすることができます。これは決して誇張しているわけではありませんが、 **Phoenix はお客様がファイアウォールをオープンしたいときにのみ、オープンしたい時間だけ、そして許可されたソース (出発地) とデスティネーション (目的地) の間でのみオープンします。**

1.2 本マニュアルのご利用について

上述のとおり、本マニュアルは Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) のソフトウェアおよびアプライアンスの両バージョンを対象としています。各章の内容は以下に説明してあります。お客様が使用されるバージョンによってはお読みいただかなくても良い章もあります。

第 1 章は本ファイアウォールの機能に関する簡単な紹介、このマニュアルのご利用方法および内容、修正済みエラーの検索方法、およびネットワーク、ファイアウォール、ネットワーク・セキュリティに関する推奨文献を紹介しています。

第 2 章は Phoenix ファイアウォールのアプライアンス・バージョンに焦点を当てています。ハードウェア本体、構成パネル・インターフェース、構成方法、アップグレード情報、トラブル発生時のリカバリ方法はこの章で説明されています。

第 3 章はソフトウェア・バージョンの x86 ベース PC でのインストレーション、アップグレード、および削除について説明しています。アプライアンス・バージョンをご利用のお客様は、この章をお読みいただく必要はありません。

第 4 章は各コンポーネントとその機能および相互作用を論じながら本ファイアウォールのインプリメンテーションについて解説しています。コンポーネントにはサーバ・コンポー

ネントおよび一般のユーザーが頻繁にアクセスするものも含まれます。この章は主にソフトウェア・バージョンに関して解説してあり、アプライアンスとの相違点は随時記述しています。

第 5 章はネットワーク・セキュリティの概念および基本的なファイアウォール・デザインの原理を含みます。パケット・フィルタリングについての簡単な解説もあります。

第 6 章はお客様の現在のネットワーク・トポロジーと Phoenix の統合について解説しています。この章は、”典型的な”ネットワークへのインストレーションの例をあげています。

第 7 章はお客様のネットワークおよびユーザーのニーズにお応えするためのファイアウォール構成を目的として、Secure Management System (SMS グラフィカル・ユーザー・インターフェース) を使用するうえでの詳細な手順を解説しています。また、Phoenix がデフォルトでサポートしているプロトコルおよびアプリケーションも説明しています。

第 8 章は Phoenix の拡張機能について詳しく説明しています。拡張機能にはカスタム・プロトコル（デフォルトでサポートされていないプロトコルなど）の使用と構成、およびネットワーク・アドレス変換機能の利用可能なモードが含まれます。

第 9 章は Phoenix の潜在的または疑わしい問題に対するトラブル・シューティングについて、ログおよびシステム・データの収集とそのデータの解釈に関するヒントに触れながら考えます。また、この章はヘルプを必要とする際の他のリソースについても紹介しています。

第 10 章は Phoenix の手動での構成方法を解説しています。手動構成は大変な作業ですが、お客様のネットワークを出入りするアクセスを制御するうえで、より高い柔軟性を持たせることが可能です。

第 11 章はファイアウォール・ファイルの例を紹介しています。

1.3 正誤表

本マニュアルのアップデートおよび修正に関しては、 Progressive Systems 社のサポート Web サイト http://www.progressive-systems.com をご覧ください。

1.4 推奨する文献

ネットワークおよび TCP/IP プロトコル

Computer Networks
By Andrew S. Tanenbaum
(March 1996) Prentice Hall; ISBN; 0133499456

Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture
By Douglas E. Corner
(March 1995) Prentice Hall; ISBN; 0132169878

TCP/IP Illustrated, Volume I: The Protocols (Addison-Wesley Professional Computing Series)
By Richard Stevens
(January 1994) Addison-Wesley Pub Co.: ISBN; 0201633469

ネットワーク・セキュリティ

Firewalls and Internet Security: Repelling the Wily Hacker
By Willian R. Cheswick, Steven M. Bellowin
(June 1994) Addison-Wesley Pub Co.: ISBN; 0201633574

Building Internet Firewalls
By D. Brent Chapman, Elizabeth D. Zwicky, Deborah Russell (Editor)
(September 1995) O'Reilly & Associates; ISBN; 1565921240

Computer Communications Security: Principles, Standard Protocols and Techniques (Addison-
Wesley Professional Computing Series)
By Warwick Ford
(January 1994) Prentice Hall; ISBN; 0137994532

Linux 管理

Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation
(October 1999) Sams; ISBN; 0672316706

Running Linux
By Matt Welsh, Matthias Kalle Dalheimer, Lar Kaufman, Matthew Welsh
(August 1999) O'Reilly & Associates; ISBN; 156592469X

Linux Install and Configuration Little Black Book: Little Black Book
By Dee-Ann Leblanc, Isaac Hajime-Yates
(November 1999) The Coriolis Group; ISBN; 1576104893

Unix 管理全般

UNIX System Adiministration Handbook
By Evi Nemeth, Garth Snyder, Scott Seebass, Trent R. Hein
(January 1995) Prentice Hall; ISBN; 0131510517

World Wide Web

CERT: Carnegie Mellon University's Computer Security Task Force
http://www.cert.org

Bruce Schneider: Counterpane; General tips on computer security and encryption
http://www.counterpane.com

Packetstorm: Secure archive site of exploits
http://packetstorm.secutiry.com

Risks Digest: News group on computer risks
http://www.catless.ncl.ac.uk/Risks

Antionline: General security news site
http://www.antionline.com

Slashdot: News group on Linux and related topics
http://www.slashdot.org

2 Phoenix ファイアウォール・アプライアンス

2.1 概要

Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) のアプライアンスは、1 スペースのラックマウント・ユニットまたは 8" x 8" マイクロサーバとして提供されています。3 イーサネット・ラックマウント・ユニットは、300MHz の x86 ベースのプロセッサ上の Linux 2.2 カーネルで稼動し、マイクロサーバは MIPS ベースのプロセッサの Linux 2.0 カーネルで稼動します。これらはつぎの標準機能を持ちます：

構成済みセキュア OS　　カーネルとオペレーティング・システムは、ファイアウォール・ルータとして適切に運用されるように最小限の機能で構成済みです。

3 イーサネット・インターフェース　　2 つの内部ネットワークまたは 1 つの内部ネットワークと境界/DMZ ネットワークに対応可能です。

透過イーサネット　　ARP スプーフィングを使用し、同じネットワーク上に外部および内部ネットワーク・インターフェースを共存させることが可能です。この機能により、追加ネットワークをお客様のサービス/アクセス・プロバイダから取得する必要がなくなり、既存のネットワークへのインストールは極めて簡単になります。

SmartGate VPN　　フルバージョンの V-One 社製バーチャル・プライベート・ネットワーク・ソリューションが 2 ユーザー分のライセンスとともに提供されます。現在、Windows、Macintosh、各種 UNIX/Linux 用のクライアントが利用可能です。追加ライセンスは、Progressive Systems 社およびその代理店から直接ご購入いただけます。

2.1.1 フロント・パネル (2 および 3 イーサネット・ポート・ラックマウント・アプライアンス)

図 1 ラックマウント・アプライアンス、フロント

フロント・パネル(図 1)は左から右へ、つぎの項目を含みます：

1. **LED** は以下の機能の状態を表示します：
   Tx/Rx いずれかのネットワークで送信または受信されたトラフィックを表示します
   Link 内部および外部ネットワーク・インターフェース上に存在するイーサネット・リンクを示します
   Col いずれかのネットワークでのパケットのコリジョン(衝突)を表示します
   100M 100M ビットのネットワークの存在を示します
   Disk すべてのディスク・アクティビティを表示します
   Firewall アクティブなファイアウォールのすべての動作を表示します
2. **液晶画面ディスプレイ (LCD Screen)** はさまざまな構成およびシステム状態メッセージを表示します
3. **キーホール・ボタン (Keyhole Button)** はファイアウォールのメニューの追加機能へアクセスすることを許可します
4. **構成パネル (Configuration Panel)** によりネットワーク・インターフェースとファイアウォールおよび VPN 機能の一部が構成可能です

2.1.2 リア・パネル (3 ポート・ラックマウント・アプライアンス)

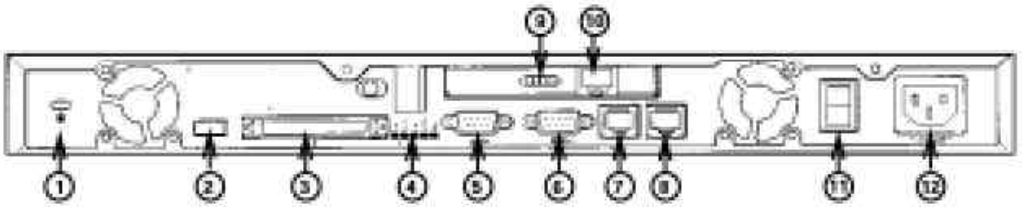


図 2 ラックマウント・アプライアンス、リア – 3 イーサネット

x86 ベースの 3 ポート・ユニットのリア・パネルは左から右へ、つぎの項目を含みます：

1. **セキュリティ・ロック・ホール(Security Lock Hole)** は安全な場所にユニットを固定するために使用されます
2. **USB ポート** は使用されません
3. **SCSI ポート** は使用されません
4. **外部/内部ネットワークおよび電源切断可能(OK to Power Off)の状態インジケータ** マザーボード・ネットワーク・コネクタの tx/rx およびリンク状態インジケータです。”OK to Power Off” インジケータは、ユニットの電源を安全に切れるときに点滅します
5. **シリアル・コンソール・ポート #1 (Serial Console Port #1)** はコンソール端末の接続用です。このポートは 115200 のボーレート(パリティ：8N1) で構成されており、

/dev/cua0 です

6. **シリアル・コンソール・ポート #2 (Serial Console Port #2)** はコンソール端末の接続用です。このポートは 9600 のボーレート(パリティ：8N1) で構成されており、/dev/cua1 です
7. **外部イーサネット・ポート (External Ethernet Port)** RJ-45 コネクタは、外部ネットワーク/サービス・プロバイダへの 10/100 Base T イーサネット接続を可能にします。システムでは eth1 です
8. **内部イーサネット・ポート (External Ethernet Port)** RJ-45 コネクタは、内部ネットワークへの 10/100 Base T イーサネット接続を可能にします。システムでは eth0 です
9. **3 番目のイーサネット/境界ネットワーク・ポートの状態インジケータ** PCI カード・ネットワーク・コネクタの tx/rx およびリンク状態インジケータです
10. **3 番目のイーサネット/境界ネットワーク・ポート (3rd Ethernet/Perimeter Network Port)** RJ-45 コネクタは、境界/DMZ ネットワークまたは 2 つ目の内部ネットワークへの 10/100 Base T イーサネット接続を可能にします。システムでは eth2 です
11. **電源スイッチ (Power Switch)** は電源のオン/オフを切り替えます
12. **電源ソケット (Power Socket)** は AC 電源コードのコンセントです。定格 100 – 240V AC、50/60Hz、1.6A、60W(最大)です

2.1.3 リア・パネル (2 ポート・ラックマウント・アプライアンス)

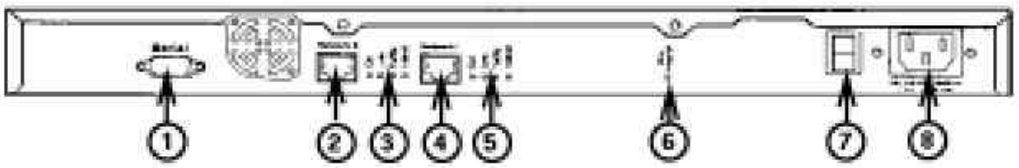


図 3 ラックマウント・アプライアンス、リア – 2 イーサネット

MIPS ベースの 2 ポート・ユニットのリア・パネルは左から右へ、つぎの項目を含みます：

1. **シリアル・ポート (Serial Port)** によりコンソール端末をアプライアンスに接続することができます。このポートは 9600 のボーレート(パリティ：8N1) で構成されており、/dev/cua0 です
2. **外部ネットワーク・コネクタ (External Network Connector)** RJ-45 コネクタは、外部ネットワーク/サービス・プロバイダへの 10/100 Base T イーサネット接続を可能にします。システムでは eth1 です
3. **外部ネットワーク状態インジケータ** 外部ネットワークのためのコリジョン、リンク、tx/rx および 100M モードのインジケータです

4. **内部ネットワーク・コネクタ (Internal Network Connector)** RJ-45 コネクタは、内部ネットワークへの 10/100 Base T イーサネット接続を可能にします。システムでは eth0 です
5. **内部ネットワーク状態インジケータ** 内部ネットワークのためのコリジョン、リンク、tx/rx および 100M モードのインジケータです
6. **電源切断可能インジケータ(OK to Power Off)** は Phoenix Firewall アプライアンスの電源を安全に落とせることを示します
7. **電源スイッチ (Power Switch)** は電源のオン/オフを切り替えます
8. **電源ソケット (Power Socket)** は AC 電源コードのコンセントです。定格 100 – 240V AC、50/60Hz、1.0A、40W(最大)です

2.1.4 リア・パネル (3 ポート・マイクロサーバ・アプライアンス)

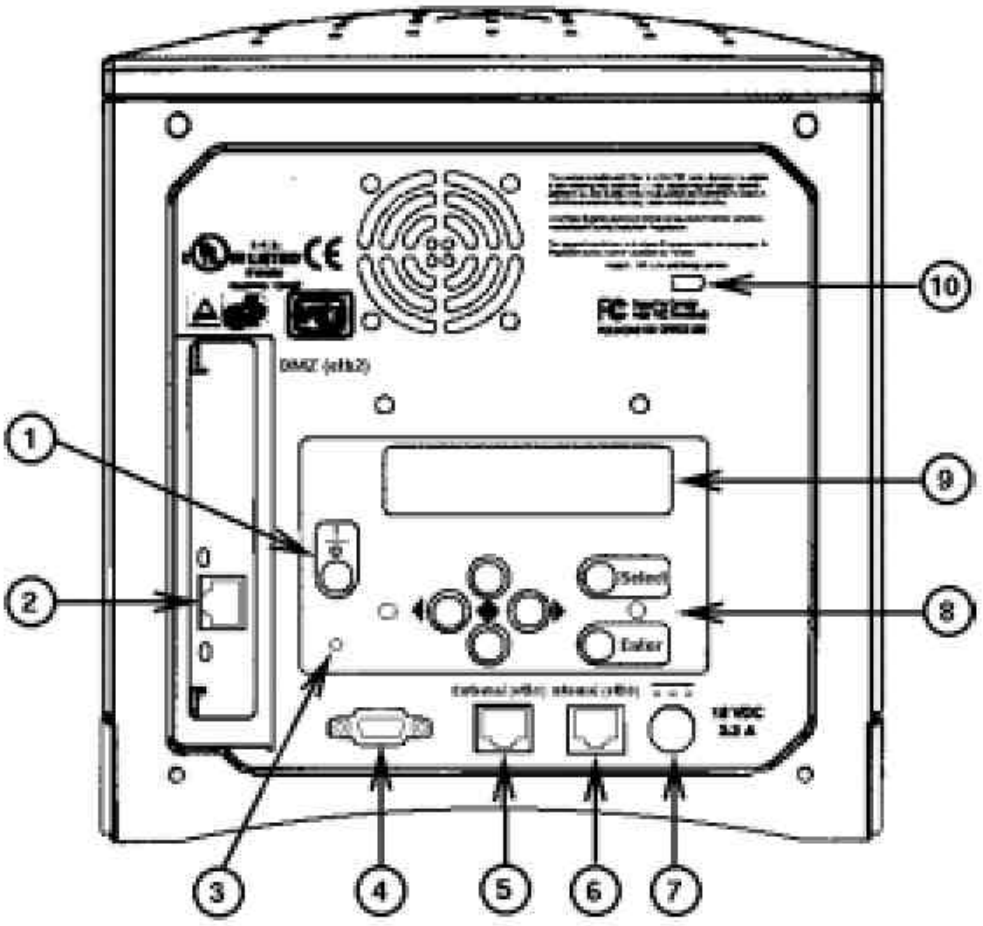


図 4 マイクロサーバ・アプライアンス、リア – 3 イーサネット

MIPS ベースの 3 ポート・ユニットのリア・パネルは左から右へ、つぎの項目を含みます：

1. **電源スイッチ (Power Switch)** は電源のオン/オフを切り替えます
2. **3 番目のイーサネット/境界ネットワーク・ポートの状態インジケータ** PCI カード・ネットワーク・コネクタの tx/rx およびリンク状態インジケータです
3. **キーホール・ボタン (Keyhole Button)** はファイアウォールのメニューの追加機能へアクセスすることを許可します
4. **シリアル・コンソール・ポート (Serial Console Port)** はコンソール端末の接続用です。このポートは 9600 のボーレート(パリティ：8N1) で構成されており、/dev/cua0 です
5. **外部イーサネット・ポート (External Ethernet Port)** RJ-45 コネクタは、外部ネットワーク/サービス・プロバイダへの 10/100 Base T イーサネット接続を可能にします。システムでは eth1 です。状態ライトがポートの上部の左側と右側の角にあります。黄色(左側)は送受信を、緑色(右側)はリンクの状態を示します
6. **内部イーサネット・ポート (External Ethernet Port)** RJ-45 コネクタは、内部ネットワークへの 10/100 Base T イーサネット接続を可能にします。システムでは eth0 です。状態ライトがポートの上部の左側と右側の角にあります。黄色(左側)は送受信を、緑色(右側)はリンクの状態を示します
7. **電源ソケット (Power Socket)** は DC 電源のプラグを差し込みます。定格 12V DC、3.3A です。外部 AC アダプタは、定格 100-240V AC、50/60Hz、1.2A、45W(常時) です
8. **構成パネル (Configuration Panel)** によりネットワーク・インターフェースとファイアウォールおよび VPN 機能の一部が構成可能です
9. **液晶画面ディスプレイ (LCD Screen)** はさまざまな構成およびシステム状態メッセージを表示します
10. **セキュリティ・ロック・ホール(Security Lock Hole)** は安全な場所にユニットを固定するために使用されます

2.2 構成パネル・インターフェース

多くの管理機能は、ファイアウォール・アプライアンスのフロント・パネル・インターフェースからアクセスできます。利用可能なメニューのナビゲーションは S (Select)、E (Enter)、および矢印ボタンを使用すれば可能です。 S ボタンを押すと個別のメニューをスクロールでき、E ボタンを押すと現在表示されているメニューに入れます。

表示されたメニュー内のデータの操作は、通常矢印ボタンを使用します。あるアクションまたは構成の変更に対する確認が必要な場合、上の矢印は変更の確定に、下の矢印は変更のキャンセルに使用してください。例えば、ネットワークの初期設定を入力した後、確認は液晶画面に表示されるつぎの 3 つのメッセージのうちいずれかを選択する際に上下の矢印ボタンを使用します：

Save Network
Configuration?

Use UP Arrow
to Confirm

Down Arrow
to abort

確認を必要とするすべての項目は類似したメッセージを表示します。もちろん、 Save Network Configuration は当該項目に置き換えられます。矢印ボタンの他の機能については、それぞれの機能が有効になる特定のメニューのセクションで詳しく説明されています。

2.2.1 基本機能

Network Configuration (ネットワークの構成)

ネットワークの構成はファイアウォールの内部、外部、ゲートウェイのアドレスおよび内部、外部のネットマスクの構成を許可します。デフォルトのメニューがロードされている場合、この機能へは S ボタンを 1 回押してアクセスします。機能は、選択されるとメニュー名のネットワークの構成 (Network Configuration) を表示します。メニューに入るには E ボタンを 1 回押してください。ユーザーは内部インターフェースの IP アドレスの入力を要求されます。液晶画面にはつぎのように表示されます：

Internal Address
000.000.000.000

点滅するカーソルは初めの数字入力欄に現れます。ユーザーは上または下の矢印ボタンを押して、選択されている入力位置の数字を増減することができます。 4 組の数字の初め（一番左側） にカーソルがある場合、下の矢印ボタンを押すと値は 000 から 255 に変わります。現在の入力位置に正しい数字を入力できたら、右の矢印ボタンを押して次の入力位置へ移動してください。ご想像されるとおり、入力位置の移動は左右の矢印ボタンを押して行ってください。完全なアドレスを入力できたら、E を押します。次は、内部インターフェースのネットマスクの入力を要求されます。

Internal Netmask
255.255.255.000

ネットマスクの入力は内部アドレスの入力と同様に行ってください。上下の矢印ボタンは、128.000.000.000 から 255.255.255.252 の有効なネットマスク値の範囲のスクロールに使用します。左右の矢印ボタンは使用しません。正しいネットマスクが入力でしたら E を押します。

外部アドレスおよびネットマスクも上と同様に設定します。ゲートウェイ・アドレスはネットマスクなしで、他のアドレスと同様に設定してください。

すべての入力欄の構成後、変更を保存するかどうかを確認するように要求されます。画面にはつぎの 3 つのメッセージが表示されます：

Save Network
Configuration?

Use UP Arrow
to Confirm

Down Arrow
to abort

変更を保存し適用するには上の矢印ボタンを押してください。ネットワーク構成の保存は、変更を有効にするためにシステムのリブートを必要とします。確認後、画面はしばらくつぎのメッセージを表示します：

Net Config Saved
Rebooting System

変更をキャンセルするには下の矢印を押してください。画面はキャンセルの確認をした後、デフォルトのメニューにリセットされます：

Procedure has
been ABORTED!!

このメニューで表示されるどのメッセージにも応答しない場合は、5 分でタイムアウトするので、再度開始する必要があります。すべての入力欄が構成されているにもかかわらず上の矢印ボタンで確認していない場合も、すべてのデータは失われ、やり直さなければなりません。

内部および外部インターフェースの両方が同一のクラス C ネットワークに構成される場合は、つぎのように確認されます：

Enable Transprnt
Ethernet?

他の機能と同様に上の矢印ボタンを押すと、このアクションを確認しマシンのリブート後にアプライアンスを透過イーサネット・モードに設定することになります。これは前述したように、より簡単なネットワーク・インストレーションを可能にする ARP スプーフをセットアップします。このモードを使用するインストレーションの詳細については、5.1.1 節をご覧ください。

Message Que (メッセージ・キュー)

アプライアンスの運用中に液晶画面に出力されたシステム・メッセージは、メッセージ・キューを選択して表示します。デフォルトのメニューがロードされている場合、 S ボタンを 2 回押してこの機能にアクセスしてください。

この機能は選択するとメニュー名の Message Queue (**メッセージ・キュー**) **を表示します。** E **ボタンを** 1 **回押してメニューにお入りください。液晶画面はつぎのメッセージを表示します：**

-> to Exit

<- for Date

この時点で左の矢印ボタンを押します。メッセージに対し 5 **秒間何のアクションも取らない場合、キューは最も新しいものから自動的に表示されます：**

M:>>>>System<<

06>>>>Ready<<

各行の初めの 2 **文字 （上の例は** M: **および** 06） **はメッセージ番号を示しています。元のメッセージは** 2 **文字分右に移動させる必要があり、したがって** 4 **文字分失われます。しかし、どのメッセージが表示されたかを判別することには影響しないでしょう。**

表示メッセージの日付および時刻はメッセージ表示中に左の矢印ボタンを押してご覧ください。タイム・スタンプは 60 **秒間、またはいずれかのキーが押されるまで画面に表示されます。例えば、上の例のメッセージのタイム・スタンプはつぎのとおりです：**

Recv'd 10/26/99

11:27:30 GMT

キューは 50 **メッセージまでループ型の配列で保存されています。前述のように、キューの最も新しいメッセージが最初に表示されます。表示された最初のメッセージ(**00**)に移動するには下の矢印ボタンを押してください。上の矢印ボタンを押すと次に最も新しいメッセージに移動します。上の例では、次の最も新しいメッセージは** 05 **です。いずれかのボタンを使用してキュー内をスクロールしてください。スクロールが完了しデフォルトのメニューに戻るには、右の矢印ボタンを押し終了してください。**

Disable External Interface (外部インターフェースを無効にする)
この機能は外部インターフェースを無効にします。デフォルトのメニューがロードされている場合、 S ボタンを 3 回押してこの機能にアクセスしてください。
この機能は選択するとメニュー名の Disable External Interface **(外部インターフェースを無効にする)を表示します。このまま続行する場合、**E **ボタンを** 1 **回押してください。**
前述のように、液晶画面はつぎの 3 **つのメッセージを表示します：**

Disable External
Interface?

Use UP Arrow
To Confirm

Down Arrow
To abort

上の矢印ボタンを押しアクションを確認すると、外部インターフェース、つまりお客様のネットワークへのすべてのトラフィックはシャットダウンされます。この機能は、ファイアウォールの侵害、またはメンテナンスのためにインターネットからアプライアンスを移動させたいけれども完全にシャットダウンはしたくない場合などに便利です。画面はつぎのメッセージを表示します：

External Interface
Disabled

上述のメッセージどおり、下の矢印ボタンを押すとアクションを中止します。画面はキャンセルを確認後、デフォルトのメニューにリセットされます：

Procedure has
been ABORTED!!

お客様の状況に応じたアクションを選択してください。いったんインターフェースが無効にされると、再度有効およびアクティブにするにはアプライアンスをリブートするしか方法はありません。

Drop External Firewall (外部ファイアウォールを落とす)
アプライアンスのリモート管理を行うため、この機能はアクティブなファイアウォールをシャットダウンさせます。一部のリモートのファイアウォールは、アクティブなファイアウォールによって SMS GUI をブロックされているかもしれません。この機能は、インストレーションのロケーションにいる人間がファイアウォールを無効にし、SMS へ管理者のリモート・アクセスを許可するために提供されています。ファイアウォールを非アクティブにすることに加え、この機能はアプライアンスの IP フォワード機能も無効にします。IP フォワードが無効にされると、トラフィックはネットワークの内部と外部インターフェースの間で通行できなくなります。これによりリモートの管理者が SMS を使用中でも、ネットワークのセキュリティは侵されていないものと保証されます。デフォルトのメニューがロードされている場合、S ボタンを 4 回押してください。
この機能は選択するとメニュー名の Drop External Firewall (外部ファイアウォールを落とす) を表示します。このまま続行する場合、E ボタンを 1 回押してください。前述のように、液晶画面はつぎの 3 つのメッセージを表示します：

Drop the External
Firewall?

上下の矢印ボタンを使用して、アクションの確認または中止を行ってください。

Reboot Appliance (アプライアンスのリブート)
これによりアプライアンスのリブートを行います。デフォルトのメニューがロードされている場合、S ボタンを 5 回押してこの機能にアクセスしてください。
この機能は選択するとメニュー名の Reboot Appliance (アプライアンスのリブート) を表示します。このまま続行する場合、E ボタンを 1 回押してください。液晶画面はつぎのメッセージを表示します：

Reboot the
System?

上下の矢印ボタンを使用して、アクションの確認または中止を行ってください。

Shutdown Appliance (アプライアンスのシャットダウン)
これによりアプライアンスのシャットダウンを行います。デフォルトのメニューがロードされている場合、S ボタンを 6 回押してこの機能にアクセスしてください。
この機能は選択するとメニュー名の Shutdown Appliance (アプライアンスのシャットダ

ウン) を表示します。このまま続行する場合、 E ボタンを 1 回押してください。液晶画面はつぎのメッセージを表示します：

Shutdown the
System

上下の矢印ボタンを使用して、アクションの確認または中止を行ってください。
アプライアンスの電源を切る前には必ずシャットダウンを行ってください。アプライアンスの電源を切る準備ができると、リア・パネルの“OK to Power Off(電源切断可能)”ライトが点滅します。

Exit (終了)
これによりメニューを終了します。デフォルトのメニューがロードされている場合、S ボタンを 7 回押してこの機能にアクセスしてください。この機能は選択するとメニュー名の Exit (終了)を表示します。デフォルトの実行画面に戻るには E ボタンを 1 回押してください。

2.2.2 キーホール機能

液晶画面とコントロール・ボタンの間に小さな穴があります。クリップのようなものを穴に挿し押すと、さらにいくつかの機能へのアクセスが可能になります。このメニューがアクティブにされると､サブ・メニューが前述の標準メニューと同様にアクセスが可能です。初めのサブ・メニューは自動的にロードされます。これらの機能は以下に説明されています。

Reset GUI Passphrase (GUI パスフレーズのリセット) この機能は、 GUI パスフレーズを忘れてしまった、あるいは変造された場合、それをリセットすることを許可します。このメニューはキーホール・ボタンを押したときに最初に表示されます。
この機能は選択するとメニュー名の Reset GUI Passphrase (GUI パスフレーズのリセット) を表示します。このまま続行する場合、E ボタンを 1 回押してください。標準メニュー同様、液晶画面はつぎの 3 つのメッセージを表示します：

Reset GUI
Passphrase?

Use UP Arrow
to Confirm

Down Arrow
to abort

上の矢印ボタンを押しアクションを確認すると、 GUI パスフレーズはリセットされ、液晶画面に表示されます。この機能は、パスフレーズを忘れてしまった、あるいは変造された場合などに便利です。

Pass Phrase:
code buff tidy

このように生成されるパスフレーズは､GUI への入力の際にはスペースを含めて使用してください。

Enable Telnet (Telnet を有効にする) これによりメンテナンスのために telnet を使用してアプライアンスに接続することを許可します。キーホール・メニューがロードされている場合、 S ボタンを 1 回押してこの機能にアクセスしてください。
この機能は選択するとメニュー名の Enable Telnet (Telnet を有効にする) を表示します。このまま続行する場合、 E ボタンを 1 回押してください。前述同様、画面は確認または中止オプションを表示します。
上の矢印ボタンを押しアクションを確認すると、アプライアンスへの telnet アクセスは許可され、新しく生成されたルート・パスワードを液晶画面に表示します。

Root Password:
dutycern

アクティブにされた telnet daemon はポート 2323 で 5 分間接続のため待機します。接続が確立されない場合、 telnet daemon は非アクティブになります。また、お客様は上述の手順を各 telnet セッションについて毎回繰り返す必要があります。

Disable Telnet (Telnet を無効にする) これによりアクティブな telnet daemon または接続をシャットダウンすることを許可します。キーホール・メニューがロードされている場合、 S ボタンを 2 回押してこの機能にアクセスしてください。
この機能は選択するとメニュー名の Disable Telnet (Telnet を無効にする) を表示します。このまま続行する場合、 E ボタンを 1 回押してください。前述同様、画面は確認または中止オプションを表示します。

SmartGate Administrator Enable (SmartGate の管理者を有効にする) これにより SmartGate の管理ユーザーを有効にすることができます。キーホール・メニューがロードされている場合、 S ボタンを 3 回押してこの機能にアクセスしてください。
この機能は選択するとメニュー名の SmartGate Admin Enable (SmartGate の管理者を有効にする) を表示します。このまま続行する場合、 E ボタンを 1 回押してください。前述同様、画面は確認または中止オプションを表示します。

Display MAC Address (MAC アドレスの表示) これによりアプライアンスのハードウェア・アドレスを表示させることができます。キーホール・メニューがロードされている場合、 S ボタンを 4 回押してこの機能にアクセスしてください。
この機能は選択するとメニュー名の Display MAC Address (MAC アドレスの表示) を表示します。 E ボタンを 1 回押すと、ハードウェア/MAC アドレスは液晶画面に表示されます。

Mac Address:
0010e0003779

この機能は、Progressive Systems 社から追加ライセンスを取得する場合に、アドレスへの容易なアクセスを提供します。

Reset to Factory Defaults (出荷時の状態にリセット) この機能はアプライアンスを出荷時のオリジナルの構成状態にリセットすることを許可します。キーホール・メニューがロードされている場合に、S ボタンを 5 回押してこの機能にアクセスしてください。
この機能は選択するとメニュー名の Reset to Factory Defaults (出荷時の状態にリセット) を表示します。このまま続行する場合、E ボタンを 1 回押してください。標準メニュー同様、液晶画面はつぎの 3 つのメッセージを表示します：

Reset to Factory
Defaults?

Use UP Arrow
to Confirm

Down Arrow
to abort

上の矢印ボタンを押しアクションを確認すると、すべての設定は出荷時の状態にリセットされ、マシンはリブートされます。いったんリセットを行うと、アクティブなファイアウォールは存在しなくなり、ネットワーク・インターフェースは再度構成される必要があります。

Exit (終了)
これによりメニューを終了します。キーホール・メニューがロードされている場合は、S ボタンを 5 回押してこの機能にアクセスしてください。この機能は選択するとメニュー名の Exit (終了) を表示します。デフォルトの実行画面に戻るには E ボタンを 1 回押してください。

2.2.3 トラブル時のリカバリ方法

Phoenix ファイアウォール・アプライアンスのハード・ドライブは 2 つのパーティションに分割されています。 1 つ目はコア・パーティションであり、オペレーティング・システムと Phoenix ファイアウォール・ソフトウェア・コンポーネントの両方のアーカイヴを含んでいます。 2 つ目はアクティブ・パーティションであり、 OS およびソフトウェアが実行/構成される部分です。すべてのユーザー・ファイルはここで変更されます。
ほとんどのディスク不良時においては、システム全体をアクティブ・システム・パーティションにリロードすることが可能です。アクティブ・パーティションを復帰させた後、ファイアウォールは再度構成される必要があります。次の手順はアクティブ・パーティションを再構築する方法を説明しています。これによりユニットは元の工場出荷時の状態に構成されます。
ユニットを工場出荷初期状態に戻すために使用される方法は、ご利用になっているハードウェアのタイプによって異なります。この節を注意深くお読みになり、確実に正しい方法を使用するようにご確認ください。

3イーサネット・ラックマウント・アプライアンスの場合

1. アプライアンスの構成パネルに移動し、S ボタンを 5 回押すことによりリブート・アプライアンス・メニュー・オプションにアクセスしてください。選択するとメニュー名、Reboot Appliance が表示されます。アプライアンスのリブートを進めるためには E を 1 回押します。ディスプレイにはつぎのメッセージが表示されます：

Reboot the
System?

上の矢印ボタンを押すことにより、リブートを確認するか中止してください。
液晶ディスプレイは、System Rebooting を表示します。そして画面は空白になります。

2. Cobalt Networks が表示されたら、S ボタンを押してください。プロンプトが表示されます：

Select Option:
Boot from disk

3. 液晶ディスプレイに Config boot disk オプションが現れるまで、右の矢印ボタンを 4 回押してください：

Select Option:
Config boot disk

4. E ボタンを押してください。つぎのプロンプトが表示されます：

Select boot disk
hda1

5. 再度 E ボタンを押してください。つぎのメッセージが表示されます：

Select boot disk
done

液晶ディスプレイは自動的に表示を戻します：

Select Option:
Config boot disk

6. 再度 E ボタンを押してください。Loading Kernel に続き、Booting が表示され、最後に Phoenix CORE boot が表示されます

7. Phoenix CORE boot が表示されているときに、下の矢印ボタンを押してください。つぎのメッセージが表示されます：

Factory
Reinstall

8. この後、標準的な確認または中止メッセージが表示されます。上の矢印ボタンを押して工場出荷状態への再インストールを行ってください

マイクロサーバおよび 2 イーサネット・ラックマウント・アプライアンスの場合

6.1 アプライアンスの構成パネルに移動し、S ボタンを 5 回押すことによりリブート・アプライアンス・メニュー・オプションにアクセスしてください。選択するとメニュー名、Reboot Appliance が表示されます。アプライアンスのリブートを進めるためには E を 1 回押します。ディスプレイにはつぎのメッセージが表示されます：

Reboot the
System?

上の矢印ボタンを押すことにより、リブートを確認するか中止してください。
液晶ディスプレイは、System Rebooting を表示します。そして画面は空白になります。

6.1 Starting Up メッセージが表示されたら、構成パネル上の上の矢印ボタンを 5 秒押し続けてください。つぎのメッセージが表示されます：

Phoenix
CORE boot…

6.1 つぎに下の矢印ボタンを押すとつぎのメッセージが表示されます：

Factory
Reinstall

6.1 上の矢印ボタンを押して工場出荷状態への再インストールを行ってください

再インストールが完了したらアプライアンスを再度構成する必要があります。液晶ディスプレイの要求に従い、適切な IP アドレスを入力してください。詳しくは後述するアプライアンスの初期構成の節をご覧ください。お客様が SMS GUI のバックアップおよび復帰機能を使用された場合、作業は簡単です。ファイアウォールがバックアップされたマシン

からアプライアンスに接続し、GUI のファイル・メニューから構成の復帰(Restore Configuration)を選択してください。構成およびファイアウォール・ファイルが戻されるとアプライアンスを一度リブートする必要があります。これにより復帰された情報は読み込まれ、アクティブなファイアウォールがインストールされます。
この手続を行ってもアプライアンスが利用可能な状態に戻らない場合、 Progressive Systems 社の販売代理店にお問い合わせいただき、ユニットの修理または交換の手配をしてください。

2.3 アプライアンスの初期構成

箱から取出した直後の Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) はネットワーク、ファイアウォールおよび VPN の何れも構成/構築されていません。まず行うべきことは、ネットワーク・パラメータをフロント・パネルに入力することです。それが完了すれば、アプライアンスのファイアウォールおよび VPN 部分の構成/構築が可能になります。

2.3.1 ネットワークの構成

アプライアンスの電源を入れると、フロント・パネルの液晶画面はつぎのメッセージを表示します： ” The Network is NOT Configured (ネットワークは構成されていません” および “Press S and then E to Start... (S の次に E を押して開始...)” 。このとき、アクティブなファイアウォールはまだインストールされていません。アクティブなファイアウォールはネットワークの構成が完了した後に構成し、有効にしてください。アプライアンスのネットワーク部分の構成はつぎの手順に従って行ってください。

1. アプライアンスの電源を入れます
2. フロント・パネルに ” The Network is NOT Configured (ネットワークは構成されていません)” メッセージが表示されたら、 S の次に E のボタンを押します。これでネットワーク構成のメニュー・アイテムに入ることができます。
3. お客様の内部 IP アドレスを尋ねられたら、矢印ボタンを使用して内部イーサネット・インターフェースの IP アドレスを入力します。入力後、 E ボタンを押します。
4. 内部ネットマスクを尋ねられるとき、デフォルトの 255.255.255.0 が表示されます。デフォルトの値は上下の矢印ボタンを使用して変更できます。これにより有効なネットマスク・アドレスの範囲をトグルします。入力後、 E ボタンを押します。
5. 外部 IP アドレスには矢印ボタンを使用して外部イーサネット・インターフェースの IP アドレスを入力します。入力後、 E ボタンを押します。
6. 次に、外部ネットマスクを尋ねられます。繰り返しになりますが、デフォルトの外部ネットマスクは 255.255.255.0 です。内部ネットマスク同様、値は上下の矢印ボタン

を使用して変更できます。入力後、 E ボタンを押します。両方のインターフェースが同じサブネットにあるように構成される場合は、透過イーサネット・モードを有効にするかどうか尋ねられます。詳しくは 2.1 節をご覧ください。

7. ゲートウェイの入力を要求されたら、矢印ボタンを使用してゲートウェイの IP アドレスを入力します。入力後、 E ボタンを押します。
8. アプライアンスはお客様がネットワーク構成で行った変更を保存するかどうかを尋ねます。変更の確認は上の矢印、変更のキャンセルはしたの矢印ボタンを押します。
9. 変更を確認した場合、アプライアンスは次のメッセージを表示します： ” Net Config Saved Gen’g Passphrase (ネットワークの構成は保存されました。パスフレーズの生成中)” 。これ以外のメッセージが表示される場合、ネットワーク構成のセットアップは再度開始します。
10. ネットワークの構成を保存した後、フロント・パネル・ディスプレイは SMS を通じてファイアウォールにアクセスするときに必要な Secure Management System (SMS) GUI のパスフレーズを表示します。このパスフレーズを（スペースも含め）控えてください。フロント・パネル・ディスプレイからパスフレーズを消去するには E ボタンを押します。次にアプライアンスはリブートをします。
11. リブート後、アプライアンスのフロント・パネル・ディスプレイはアプライアンスのホスト名 （デフォルトで Phoenix） およびファイアウォールの内部 IP アドレスを表示し、 Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) のバージョン情報の表示に変わります。

この時点でお客様は Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) アプライアンスの設定を、SMS を通じて変更したいかもしれません。その場合、Java AWT 1.1.5 (現在は Netscape 4.07 またはそれ以降のバージョン) をサポートする Web ブラウザが必要になります。

1. Web ブラウザを開き、アプライアンスの IP アドレス(内部または外部の何れか)にポート 8181 を付けてアクセスしてください（例：http://137.175.48.107:8181）。Java SMS は自動的に開始します。
2. SMS に尋ねられたら、アプライアンスによって生成されたパスフレーズ （スペースや特殊記号も含め） を入力します。
3. 初めて SMS を使用する場合、アプライアンスによって割り当てられたパスフレーズを変更するように要求されます。 OK をクリックしパスフレーズを変更してください。
4. 新しいパスフレーズを設定した後、 SMS へのアクセスは許可されます。

2.3.2 初期ファイアウォールの構成

初期ファイアウォールの構成については第 7 章をご覧ください。

2.4 Phoenix アプライアンスのアップグレード

各機能のバグおよび修正が Phoenix に加えられた場合、現在保守契約をいただいているお客様はアップデートされたバージョンをご利用いただけます。これらのアップグレードは署名付きの tar 形式のファイルで提供されています。*ご注意ください：アップグレードの手続はネットワークの構成を再度初期化してしまい、すべての既存のファイアウォールは削除されます。*

2.4.1 Phoenix アプライアンスにアップグレードを適用する

1 SMS GUI を実行するホストに適切なアップグレード・ファイルをダウンロードします。アップグレードを失敗なく完了するには、ダウンロードするホストはアプライアンス以外のマシンである必要があります。

2 SMS を通じてアプライアンスに接続します。詳細に関しては 7.1 節をご覧ください。

3 アプライアンスに接続したら、 File (ファイル) メニューを開き、 Backup Configuration (構成のバックアップ) を選択します。この機能により、アプライアンスの全般的な構成および作成したすべてのファイアウォール・ファイルは保存されます。**ご注意ください：アップグレードの手続はネットワークの構成を再初期化してしまい、すべての既存のファイアウォールは削除されます。構成のバックアップおよび構成の復帰機能はベータ版のソフトウェアでは動作しません。ベータ版をご利用のお客様はアップグレードを行う前に必ずこの事実を認識しておいてください。**

4 File (ファイル) メニューを開き、 Upgrade (アップグレード) を選択します。表示されるダイアログ・ボックスはつぎのメッセージを示します：

You are about to perform an Upgrade. Selecting ok will cause a browser window to open and initiate a file upload operation. Click on OK.（アップグレードを始めます。 OK を選択するとブラウザ・ウィンドウが開き、ファイルのアップロードを開始します。 OK をクリックしてください）

5 つぎのタイトルの新しいブラウザ・ウィンドウが開きます： Upload upgrade package to Phoenix Appliance. （Phoenix アプライアンスにアップグレード・パッケージをアップロードします。） ウィンドウは “Please enter the filename of your upgrade package or click Browse.”（アップグレード・パッケージのファイル名を入力するか、参照をクリックしてください。） というメッセージを表示します。お客様はシステムの既存のファイル名を入力 （または参照ボタンでファイルを指定） してください。参照 (Browse) ボタンはデフォルトで *.html に一致するファイルを探します。適切なパラメータに変更し、アップグレード・ファイルを探してください。

お客様のシステムからアプライアンスへのファイルのアップロードは、 Upload package (パッケージのアップロード) ボタンをクリックして行ってください。この手続が完了すると、ブラウザ・ウィンドウは更新され、 File upload successful (ファイルのアップロードに成功しました) というタイトルで、ウィンドウ内のメッセージは Upload successful (アップロードに成功しました) に変更されます。

6 つぎの手続きは、アプライアンスのリブートです。コア・パーティションからブートします。このパーティションはこれまでの手順でアップロードされたアップグレード・パッケージを含んでいます。コアからブートするとアップグレードが、ユニットが通常のブートを行うアクティブ・パーティションにインストールされます。

コア・ブートを行うために使用される方法は、ご利用になっているハードウェアのタイプによって異なります。この節を注意深くお読みになり、確実に正しい方法を使用するようにご確認ください。

3イーサネット・ラックマウント・アプライアンスの場合

6.1 アプライアンスの構成パネルに移動し、S ボタンを 5 回押すことによりリブート・アプライアンス・メニュー・オプションにアクセスしてください。選択するとメニュー名、Reboot Appliance が表示されます。アプライアンスのリブートを進めるためには E を 1 回押します。ディスプレイにはつぎのメッセージが表示されます：

Reboot the
System?

上の矢印ボタンを押すことにより、リブートを確認するか中止してください。
液晶ディスプレイは、System Rebooting を表示します。そして画面は空白になります。

6.2 Cobalt Networks が表示されたら、S ボタンを押してください。プロンプトが表示されます：

Select Option:
Boot from disk

6.3 液晶ディスプレイに Config boot disk オプションが現れるまで、右の矢印ボタンを 4 回押してください：

Select Option:
Config boot disk

6.4 E ボタンを押してください。つぎのプロンプトが表示されます：

Select boot disk
hda1

6.5 再度 E ボタンを押してください。つぎのメッセージが表示されます：

Select boot disk
done

液晶ディスプレイは自動的に表示を戻します：

Select Option:
Config boot disk

6.6 再度 E ボタンを押してください。Loading Kernel に続き、Booting が表示され、最後に Phoenix CORE boot が表示されます

6.7 Phoenix CORE boot が表示されているときに、S ボタンと上の矢印ボタンを同時に押してアップグレードを確認してください

6.8 ボタンを放すと、
To confirm upgrade, push up and down
arrows at the same time or E key to abort upgrade.
(アップグレードの確認は上下の矢印ボタンを同時に押し、アップグレードの中止は E ボタンを押してください)と表示されますので、上下の矢印ボタンを同時に押し、アップグレードを開始してください

アプライアンスはアップグレード処理の間に自動的に 2 回リブートします。

マイクロサーバおよび 2 イーサネット・ラックマウント・アプライアンスの場合

6.1 アプライアンスの構成パネルに移動し、S ボタンを 5 回押すことによりリブート・アプライアンス・メニュー・オプションにアクセスしてください。選択するとメニュー名、Reboot Appliance が表示されます。アプライアンスのリブートを進めるためには E を 1 回押します。ディスプレイにはつぎのメッセージが表示されます：

Reboot the
System?

上の矢印ボタンを押すことにより、リブートを確認するか中止してください。
液晶ディスプレイは、System Rebooting を表示します。そして画面は空白になります。

6.2 Starting Up メッセージが表示されたら、構成パネル上の上の矢印ボタンを 5 秒押し続けてください。これによりコア・ブートが開始します(Phoenix CORE boot... が画面に表示されます)

6.3 Phoenix core init が画面に表示されたら、上の矢印ボタンと S ボタンを同時に 5 秒間押しつづけてください

6.4 ボタンを放すと、
To confirm upgrade, push up and down
arrows at the same time or E key to abort upgrade.
(アップグレードの確認は上下の矢印ボタンを同時に押し、アップグレードの中止は E ボタンを押してください)と表示されますので、上下の矢印ボタンを同時に押し、アップグレードを実行/開始してください

アプライアンスはアップグレード処理の間に自動的に 2 回リブートします。

7 アップグレードが完了したら、ネットワークを再度構成してください。SMS を通じてアプライアンスへ再接続し、File(ファイル)メニューを開き Backup Configuration(構成のバックアップ)を選択します。これによりアプライアンスの全般的な構成および作成したファイアウォール・ファイルは復帰します。

8 構成および作成したファイアウォール・ファイルを復帰したので、最後にアプライアンスをリブートします。リブートは元に戻された情報をロードしアクティブなファイアウォールをインストールします。

3 Phoenix ソフトウェアのインストール

このセクションは Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) のソフトウェア・バージョンの準備およびインストレーションの詳細について説明します。ファイアウォールのアプライアンスをご利用のお客様は、本マニュアル第 8 章にハードウェアに関する記載がありますので、そちらをご覧ください。お客様のローカル・ネットワークにファイアウォール・ハードウェアをインストールする手順につきましては第 5 章をご覧ください。

3.1 ハードウェアの推奨動作環境

Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) は、486-DX2 から最新の Pentium のシステムまで、x86 ベースのハードウェアでご利用いただけます。一般的には Pentium {Pro, II, III} がほとんどのネットワークに適しています。ファイアウォールを通過すると予測されるトラフィック量によって使用する基本システムを決めるべきです。T1/E1 のスピード （2Mbps） の場合、初期の Pentium で充分でしょう。

イーサネット・カードは少なくとも 2 枚、最大で 8 枚、インストールしてください。バスのスピードはパフォーマンスを制限する要因となりますので、PCI ネットワーク・カードのみを使用するようにしてください。さらに、バス・マスタリングをサポートするカードは高いパフォーマンスを持ちます。私どもは 3Com 社の 3C90x カードを長く使用しております。

ファイアウォールのみのマシンにおいて、 RAM は大きな問題ではありません。大規模なネットワークでも 32MB で充分でしょう。

3.2 オペレーティング・システムの要件

Phoenix は、2.0 または 2.2 カーネル(OS によって異なります)の RedHat、S.u.S.E. および Turbolinux など最も一般的なバージョンの Linux オペレーティング・システムで実行します。ご利用の詳細に関しては表 1 をご覧ください。

オペレーティング・システム	カーネルのバージョン	Phoenix のバージョン
LASER5 6.2	2.2.14	1.5.3
Red Hat 6.0 および 6.1	2.2.14 まで	1.5.3
Red Hat 5.2	2.0.34, 2.0.35, および 2.0.36	1.5.3
SuSE 6.3	2.2.14 まで	1.5.3
Turbolinux 6.0	2.2.14 まで	1.5.3

表 1：サポートするオペレーティング・システム

3.3 オペレーティング・システムの準備

Phoenix を利用するために必要なオペレーティング・システムの構成手順は以下に説明しています。私どもは、そのマシンを、最小限のカーネル構成で動作させるファイアウォール専用マシンとしてご利用されることを推奨致します。

3.3.1 カーネルの構成

お客様がご利用になるカーネルが Phoenix がサポートしている Linux カーネルの最新バージョンであることをご確認ください。 RedHat Linux の標準の "サーバ" および "ワークステーション" のインストールは、 Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) のインストールおよび実行に必要なすべてのカーネル・サポートを含んでいます。

インストールが完了したら、すべての OS パッチが最新のものかを確認してください。ネットワークの弱点に関連するパッチは特に注意してください。

私どもはカーネルを必要最小限の機能に縮小することを推奨します。必要最小限の機能には以下のものが含まれている必要があります：

- ローダブル・モジュール
- ネットワーク・ファイアウォール
- IP ファイアウォール

カーネルを再度生成する際は **make menuconfig** というコマンドを使用することを強くお奨めします。このコマンドはカーネルが作成される前にすべての依存関係を解決します。

さらに、ファイアウォール・マシンで使用しないすべてのサービスは完全に削除することも提案します。一般的にはこれらはつぎのサービスを含みます： telnet、すべての r-exec コマンド（rlogin、rsh など)、ftp、http などです。使用しないサービスを削除することにより、ファイアウォールを誤って構成してしまった場合のマシンの持つリスクは減ります。

3.3.2 ネットワークの構成

どのようなファイアウォールであっても、インターフェースは少なくとも 2 つ必要です。1 つは LAN 外のネットワークに、もう 1 つは LAN そのものにつながるインターフェースです。したがって、お客様はネットワーク・インターフェース・カード （NIC） を、ファイアウォールが実行されるマシンがつながる各ネットワークにインストールする必要があります。

お客様のマシンに NIC を追加インストールする場合のインストール手順はハードウェア同梱のマニュアルを参照してください。

NIC のインストールが完了したら、カーネルにロードされる NIC に最適なドライバがあるかどうかを確認してください。確認する最も簡単な方法は、ローダブル・モジュールを

使用する方法です。利用可能な Linux NIC/ ネットワーク・ドライバ・モジュールのほとんどは **http://cesdis.gsfc.nasa.gov/linux/drivers** で入手可能です。

3.3.3 Phoenix ソフトウェアを基本システムにインストールする

1. 弊社の ftp または web サイトからお客様のシステムのための正しい RPM を取得してください。
2. RPM ファイルを任意の RPM またはソース・ディレクトリに置き、 **rpm -i <phoenix.rpm>** コマンドを実行してください。 RPM の初期インストールで問題がある場合、つぎのコマンドを使用してパッケージのリロードを試みてください：

   rpm –ivvh <phoenix.rpm> > /tmp/phoenix.install/log

   このコマンドにより **/tmp/phoenix.install/log** というファイルが作成されます。このログを検証後まだ問題が解明または修正されない場合、ファイルを Progressive Systems 社の販売代理店までお送りください。インストール・ログとともに、必ずお客様が行った RPM のインストール手順についての記述を添付してください。
3. ライセンス・キーをお持ちでなければソフトウェアは動作しません。まだライセンス・キーを取得されていないお客様は、すみやかに取得してください。 **ifconfig eth0** というコマンドの出力を弊社の販売代理店までお送りくだされば、ライセンスを取得できます。
4. Secure Management System GUI を開始し、初期ファイアウォールを構成してください。

3.3.4 Phoenix ソフトウェアのアップグレード

Phoenix RPM は、**rpm -U** のアップグレード・オプションで使用するできるようにデザインされていません。既存のインストレーションをアップグレードするには、現在の Phoenix インストレーションは削除する必要があります。既存の RPM を削除しても、Phoenix のホーム・ディレクトリ、 **/etc/phoenix** 、その他既存のファイアウォール構成ファイルは削除されないことにご注意ください。

1. 弊社の ftp または Web サイトからお客様のシステムのための正しい RPM を取得してください。 RPM ファイルを任意の RPM またはソース・ディレクトリに置きます。新しい RPM が正しくロードされ、新規にインストールされたファイアウォールが機能することを確認するまで、古い RPM はどこかに保存しておくとよいでしょう。
2. **rpm -e phoenix** で Phoenix の旧バージョンを削除してください。
3. 新しい RPM の保存場所へ行き、つぎのコマンドを実行してください：

   rpm -i <phoenix.rpm>

   必ず新しい RPM の名前を使用してください。新しい RPM の初期インストールで問

題がある場合、つぎのコマンドを使用してパッケージのリロードを試みてください：
rpm –ivvh <phoenix.rpm> > /tmp/phoenix.install/log
このコマンドにより **/tmp/phoenix.install/log** というファイルが作成されます。このログを検証後まだ問題が解明または修正しない場合、ファイルを Progressive Systems 社の販売代理店までお送りください。インストール・ログとともに、必ずお客様が行った RPM のインストール手順についての記述を添付してください。

4. Secure Management System GUI を開始し、元のファイアウォールをロードするか、新規のファイアウォールを作成してください。アップグレードされたソフトウェアで元のファイアウォール・ファイルをロードする前に、サポートされるファイアウォール・プロトコルやアプリケーションのセットに対する追加点や変更点を必ず確認してください。ある種の変更は特定のプロトコルに関して手作業による再構成を要求するかもしれません

3.3.5 Phoenix ソフトウェアのアンインストール

お客様が現在のシステムから Phoenix ソフトウェアを完全に削除したい場合：

1. **rpm -e phoenix** コマンドを実行してください。
2. **rm –rf /etc/phoenix** コマンドを実行してください。このコマンドには極めて注意が必要です。削除するディレクトリを正しく指定したかどうかを確認してください。誤ったディレクトリ指定は、予定外のファイルを削除してしまうことになりかねません。Progressive-Systems 社はこのようなコマンドの操作ミスに関しては、責任を負いかねます。

3.3.6 Phoenix Adaptive Firewall のライセンスの取得

最初に触れましたように、 Progressive-Systems 社からライセンスを取得されていないお客様のソフトウェアの標準インストールは、 ”Personal Edition” モードで実行されます。これは Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) の制限されたバージョンです。 Phoenix PE は、通過可能な接続数が制限されていること以外、あらゆる意味で完全な機能を持っています。このバージョンはシングル・ユーザー・ネットワークを対象にデザインされています。 Phoenix PE はホーム・ネットワーク、ワークステーション、または低容量サーバの保護に役立ちます。
接続数があらかじめ設定された上限 （2 つの IP アドレス/ 30 の同時 TCP セッション）を超える場合、それらの接続は切断され、タイムアウト時間が経過するまでは接続できなくなります。
お客様のネットワークが追加 TCP セッションおよび/または複数の IP アドレスを必要とする場合、 Progressive Systems 社の販売代理店にお問い合わせいただき、適切なライセンスの取得をお奨めします。大規模なネットワークでファイアウォールのテストを行

うためのデモ版もご利用いただけます。これらのライセンスは期限が設けられているので、ソフトウェアはあらかじめ設定された日数のみ動作します。
どのような追加ライセンスを取得される場合でも、お問い合わせいただく際は以下の情報をご確認ください：

- ご連絡先：お客様のお名前、会社名、住所、電話番号、電子メール・アドレスなど
- ご利用のオペレーティング・システム
- eth0 のハードウェア/MAC アドレス

マシンの eth0 の MAC アドレスを得るには、つぎのコマンドを実行してください：

```
/sbin/ifconfig eth0
```

コマンド出力の最初の行はこのようになるはずです：

```
eth0 Link encap:Ethernet Hwaddr 00:A0:CC:58:39:A1
```

Hwaddr は MAC アドレスです。このアドレスは 6 組のアルファベットおよび数字の組み合わせで構成され、それぞれコロンで区切られています。この番号は、ファイアウォールを実行するシステム固有のライセンス・キーを生成するために使用されます。
ライセンス・キーは生成後、電子メール、またはご希望の場合は FAX にてサポート・ナンバーとともにお客様に通知されます。サポート・ナンバーは電話または電子メールにて弊社のサポート・スタッフにお問い合わせいただく際に必要となります。

4 Phoenix Adaptive Firewall

Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) は、実際にはネットワークを保護するために互いに依存しながら機能するプログラムの集まりです。ファイアウォールの各コンポーネントは以下に詳しく紹介され、それぞれがどのように機能するかを簡単に説明してあります。

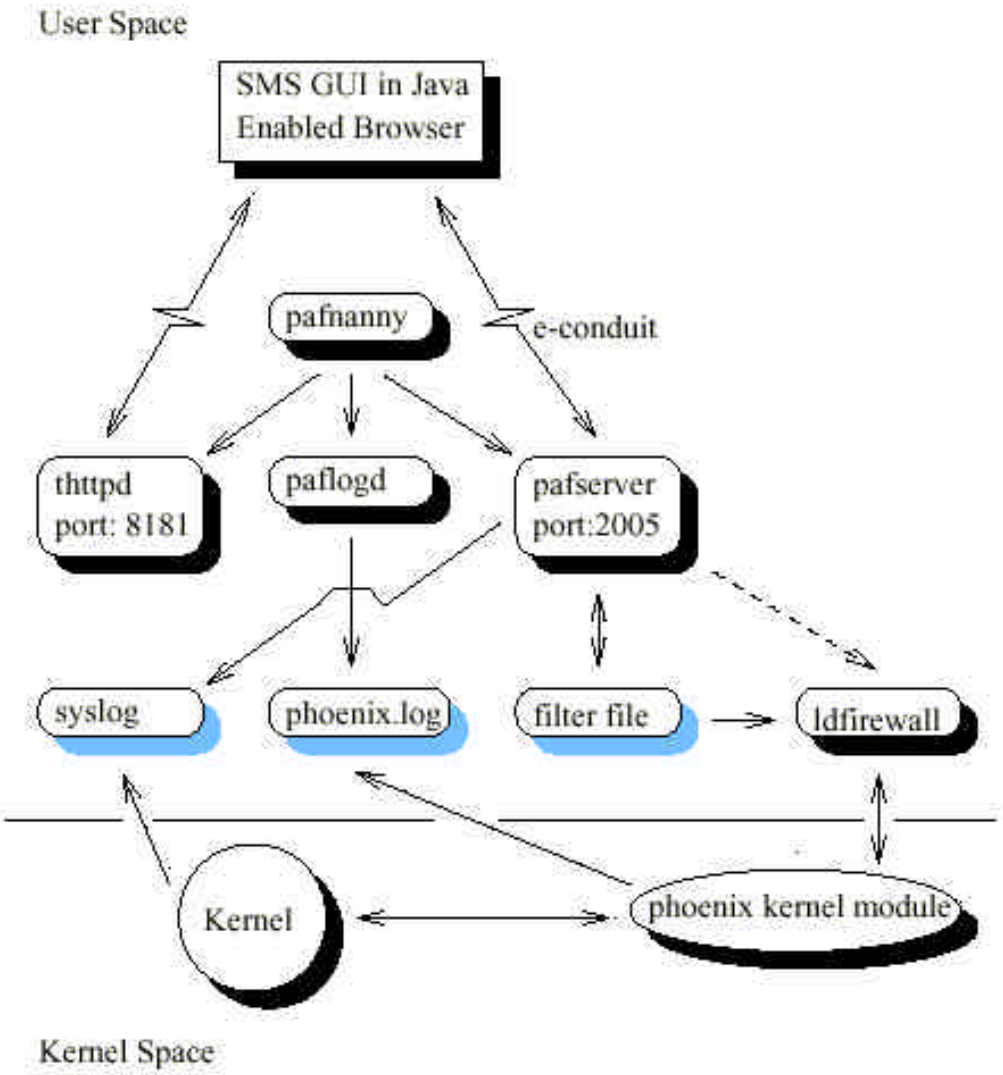


図 5 Phoenix Adaptive Firewall のコンポーネント

4.1 バックエンド／サーバ・コンポーネント

4.1.1 pafserver

pafserver は暗号化されたトンネルを利用して、Security Management System (4.2.1 節参照) の Web ブラウザによるリモート制御を可能にします。pafserver は ldfirewall (4.2.2 節参照)を呼び出し、SMS インターフェースからのリクエストに応答、つまりユーザーに代わってコマンドを実行します。デフォルトで pafserver はポート 2005 で受信待ちします。 Phoenix アプライアンス・バージョンの pafserver はフロント・パネル・ディスプレイから ldfirewall へ向けて発行されたコマンドを渡す役目も果たします。

4.1.2 paflogd

アクティブなファイアウォールからのメッセージは、paflogd を通して /var/log/phoenix.log にロギングされます。ディスクが満杯にならないように、ログ・ファイルが大きくなりすぎると paflogd はそれを循環させます。paflogd が負荷に耐えられなくなった場合も、引き続きファイアウォールを正しく機能させるための措置が取られます。負荷が集中しすぎた場合、カーネル・モジュールは失われたメッセージについてユーザーに報告するためのエントリを /var/log/phoenix.log に出力します。paflogd はデフォルトではすべての拒否されたパケットをロギングします。

4.1.3 thttpd-phoenix

thttpd-phoenix は、 Secure Management System （管理者用 GUI） からの接続の受信待ちを専門とする Web サーバです。デフォルトで thttpd-phoenix はポート 8181 で受信待ちし、 GUI への応答はポート 2005 を通じて行います。

4.1.4 pafnanny

プログラミング・ミスまたは他の問題は、pafserver、paflogd、あるいは thttpd-phoenix のクラッシュを引き起こしてしまう原因になりかねません。これらの 3 つのプログラムは、SMS インターフェースが機能するために必要なものです。pafnanny はそれらのプロセスを絶えず監視し、クラッシュの状況からガードします。いずれかのプログラムがクラッシュまたは不意に終了した場合、pafnanny はそれをただちに復帰させます。復帰後の SMS コンポーネントの状態にかかわらず、アクティブなファイアウォールは機能し続けます。SMS の何れかのセグメント(構成要素)がクラッシュした場合、ファイアウォールのリモート管理は不可能になります。

4.1.5 e-conduit

e-conduit 層は、 SMS が pafserver と通信するトンネルを提供します。この相互作用を

促進する個別の暗号化および認証キーは、データ・ストリーム内で既知のシークレット・トークンが使用されないように生成されます。トンネルは 56-bit DES で暗号化され、認証は SHA1 90bits で行われます。したがって e-conduit 層は、強力な暗号化機能、および極めて厳重な認証機能によって完璧な機密転送を可能にします。

4.1.6 phoenix のカーネル・モジュール

phoenix のカーネル・モジュールは、システムを起動する際オペレーティング・システムのカーネルに統合される実際のファイアウォールを含むユーザー・ローダブル・モジュールです。このモジュールは個別のプログラムとして実行されるものではありません。このモジュールの仕事はファイアウォール・システムを通過するトラフィックを把握することです。そして、そのトラフィックの通過が許可されているかどうかを、ファイアウォール・フィルタ・ファイルで定義されているルールに従って判断します。この部分さえ機能していれば、ファイアウォールはお客様のネットワークを保護する役目を果たすことができます。

4.1.7 ファイアウォール・フィルタ・ファイル

このファイルは、Phoenix カーネル・モジュールで実行されるアクティブ・ファイアウォールを構築するために使用されるファイアウォール・ルールを含みます。このファイルは SMS のファイアウォール・テンプレート・ファイルの選択に基づき生成されます。

4.1.8 ファイアウォール・テンプレート・ファイル

Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) で認識するアプリケーション・タイプは、アプリケーションによって提供されるテンプレート・ファイルで決定されます。サポートしている各アプリケーションは SMS GUI の最左列に表示されます。インターネットのような IP ベースのネット上で動作する一般的なアプリケーションのほとんどには、類似したパラメータのセットがあります。本ファイアウォールは、あらかじめ定義されているつぎのようなアプリケーションを認識します：

- クラッキング防止 (Cracking prevention) ： *SATAN* プログラム、アンチ・スプーフィングによる侵入から保護し、ソース・ルーティングをロックアウトします。
- 制限されるサイトのリスト (A restricted site list) ：リストにあるサイトとの通信は一切禁止されます。このリストにサイトを登録すると、プロトコルまたはアプリケーションごとの選択欄の同一サイトへの参照がすべて上書きされます。
- 信頼されるサイトのリスト (A trusted site list) ：トラフィックは、もう一方の完全に信頼されるサイトへ通過することが可能です。
- File Transfer Protocol
- Telnet

- World Wide Web (mosaic、Netscape、gopher、WAIS)
- News (*nntp*)
- SMTP メール (Simple Mail Transfer Protocol)
- Pop メール (Post Office Protocol)
- IMAP メール (Internet Mail Access Protocol)
- ドメイン・ネーム・サービス (Domain Name Service、すなわち DNS)
- UUCP (UNIX to UNIX Copy)
- Whois
- Finger
- Talk/チャット
- Archie
- UNIX ユーティリティの "r" コマンド (*rsh, rlogin, rcp*)
- マルチメディア
- Secure Shell
- X11
- Lan Manager (NetBIOS)
- タイム・サービス (Network Time Protocol 、または NTP)
- TFTP (Trivial File Transfer Protocol)
- IPsec (IP Security)
- PPP トンネル
- Ident
- ルーティング情報 (RIP, OSPF, BGP, EGP)
- Syslog
- SNMP (Simple Network Management Protocol)
- Ping/Traceroute
- ICMP (Internet Control Message Protocol)
- ログ

4.2 フロントエンド／ユーザー・コンポーネント

4.2.1 Secure Management System (GUI)

ファイアウォールの構成は、主に Java ベースのグラフィカル・ユーザー・インターフェースを介して行われます。この節は利用可能なメニュー・コマンドの概要を紹介します。GUI をご利用になるときの各コマンドの詳細に関しては 7.1 節をご覧ください。また、ファイアウォールは、ファイアウォール・ファイルを直接編集することによって手動で構成することも可能です。直接の編集は、ファイアウォール・ルールに関してのより高い柔軟性や制御を実現可能ですが、編集エラーを犯しやすいことに極めて注意する必要があり

ます。手動構成に関する詳細は第 10 章で解説しています。
ファイアウォールの管理は、この GUI またはいくつかのコマンド・ライン・インターフェースのツールにより行うことができます。

Phoenix GUI メニュー・バー・オプション Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール)のウィンドウの上部のメニュー・バーにはつぎのオプションがあります：

- **File (ファイル)**
  File (ファイル) オプションでは、ユーザーのログオン・ログオフ、新規ファイアウォールの作成、既存のファイアウォールのファイルを開く、新規または更新したファイアウォール定義をファイルに保存、編集したファイアウォール定義を新しいファイル名で保存、ファイアウォールの削除、Phoenix GUI からのログオフが可能です。***太字のメニュー・オプションは Phoenix アプライアンスでのみ利用可能です。***

- **Firewall (ファイアウォール)**
  Firewall (ファイアウォール) オプションでは、現在のファイアウォールを保存および有効にする、ファイアウォールを有効/無効にする、およびスタートアップのファイアウォールのセットおよび削除が可能です。

- **Admin (管理)**
  Admin (管理) オプションでは、パスフレーズの変更、ライセンス情報のインストール/削除および確認を行うことができます。ファイアウォール・ファイルを作成する際、オプションによりホスト名を IP アドレスへ自動変換する機能を有効にすることも可能です。***太字のメニュー・オプションは Phoenix アプライアンスでのみ利用可能です。***

- **About (バージョン情報)**
  About (バージョン情報) オプションでは、現在稼動しているオペレーティング・システムのバージョンと Phoenix クライアント、サーバ、およびファイアウォールのバージョンが表示されます。

メニュー	キー操作	説明
New Firewall (ファイアウォールの新規作成)	Ctrl+N	ブランクのテンプレートから新規のファイアウォールを作成します。"制限された"モデルのファイアウォールを維持するために、ブランクのテンプレートは、それがインストールされているインターフェースのトラフィックの通過を禁止します。
Open Firewall File... (ファイアウォール・ファイルを開く)	Ctrl+O	既存のファイアウォール・ファイルを開きます。
Save Firewall File... (ファイアウォール・ファイルの保存)	Ctrl+S	現在ロードされているファイアウォール・ファイルを保存します。現在のファイアウォールがすでに存在する場合、そのオリジナル・ファイルのバックアップ・コピーがオリジナルのファイル名の接尾辞 .bak を付けたかたちで保存されます。
Save Firewall File As... (ファイアウォール・ファイルを名前をつけて保存)	なし	現在ロードされているファイアウォール・ファイルを別の名前で保存します。
Delete Firewall File... (ファイアウォール・ファイルの削除)	Ctrl+D	ファイアウォール・ファイルを削除します。
Backup Configuration ... (構成情報のバックアップ)	なし	ファイアウォール・ファイルおよびその他の構成情報を、GUI を実行中のマシンの指定ディレクトリに保存します。
Restore Configuration ... (構成情報の復帰)	なし	ファイアウォール・ファイルおよびその他の構成情報を、GUI を実行中のマシンの指定ディレクトリから戻します。
Upgrade... (アップグレード)	なし	ファイアウォール・アプライアンスをアップグレードします。
Logoff (ログオフ)	Ctrl+Q	ファイアウォールの管理セッションを終了し、GUI を閉じます。

表 2：SMS File (ファイル)・メニュー

メニュー	キー操作	説明
Firewall Status (ファイアウォールの状態)	なし	バージョン情報、システム起動時にインストールされた現在アクティブなファイアウォール、およびライセンス情報を表示します。ldfirewall もご覧ください。
Save and Activate Current... (現在のファイアウォール・ファイルを保存および有効にする)	Ctrl+C	現在 GUI にロードされているファイアウォール・ファイルを保存し、ネットワークの特定のインターフェースにインストールします。
Activate Current Firewall... (現在のファイアウォール・ファイルを有効にする)	Ctrl+F	ネットワークの特定のインターフェースにインストールするファイアウォール・ファイルを選択します。
Deactivate Active Firewall... (アクティブなファイアウォール・ファイルを無効にする)	Ctrl+X	特定のインターフェースから現在のファイアウォール・ファイルをアンインストールします。
Set Startup Firewall... (スタートアップ・ファイアウォール・ファイルの設定)	Ctrl+T	選択されたファイアウォール・ファイルをシステム起動時に開始するファイアウォール・ファイルとしてネットワーク・インターフェースにインストールします。
Remove Startup Firewall (スタートアップ・ファイアウォール・ファイルの削除)	Ctrl+R	インストール済みのスタートアップ・ファイアウォール・ファイルを削除します。
Custom Protocols... (カスタム・プロトコル)	なし	ファイアウォールの標準テンプレートに含まれていないポート/プロトコルのルールを追加します。

表 3：SMS Firewall (ファイアウォール) ・メニュー

メニュー	キー操作	説明
Change Passphrase... (パスフレーズの変更)	なし	GUI にログインするパスフレーズを変更またはリセットします。
Licenses (ライセンス)	なし	
Phoenix License (Phoenix ライセンス)	なし	Phoenix ファイアウォールのライセンス・ファイルを表示または追加します。
SmartGate VPN License (SmartGate VPN ライセンス)	なし	SmartGate のライセンス・ファイルを表示または追加します。
Telnet...	なし	アプライアンスの telnet 接続を開始します。
Options... (オプション)	なし	日付、時刻、およびシステムのデバッグ・レベルを構成します。
Host Configuration ... (ホスト構成)	なし	ホスト名、ドメイン名、インターフェースの構成およびルートの追加などを行います。アプライアンスのリブートもできます。
IP Masquerading Configuration ... (IP マスカレードの構成)	なし	IP マスカレードを開始および構成します。
Port Forwarding Configuration ... (ポート・フォワードの構成)	なし	ポート・フォワードを開始および構成します。
Logging (ロギング)	なし	
View Log (ログの表示)	なし	ポップアップ・ウィンドウにファイアウォールのログを表示します。
Download Log (ログのダウンロード)	なし	ファイアウォールのログをテキスト・ファイルとしてダウンロードします。

表 4：SMS Admin (管理)メニュー

4.2.2 コマンド・ライン・インターフェース

これらのコマンドを利用するには、Phoenix を実行しているマシンにログインする必要があります。ログインには、Phoenix を実行中のマシンへのシェル・ アクセスをアクティブなファイアウォールが許可する構成であることが要求されます。ファイアウォールの外側からのアクセスは危険なため許可するべきではありません。お客様がアプライアンス・バージョンをご利用の場合は、 SMS またはフロント・パネル・コントロールから telnet を有効にする必要があります。これは SMS の Admin（管理）メニューの Telnet オプションから行います。それが完了すれば、アプライアンスのポート 2323 へ telnet することで telnet アクセスを取得できます。その際のコマンドは： telnet <myfirewall> 2323 であり、<myfirewall> はお客様のファイアウォールのホスト名または IP アドレスに置き換わります。

Phoenix init スクリプト

これは Phoenix を開始させる起動用のスクリプトです。このスクリプトは /etc/rc.d/init.d/phoenix においてあります。スクリプトに有効な命令は以下に説明してあります。

用法：

/etc/rc.d/init.d/phoenix {start | stop | shutdown | status | masq-config | portfw-config}

start（開始）	Phoenix のカーネル・モジュールをロードします。管理セグメントをつぎの順序で開始します： pafserver 、paflogd 、 thttpd-phoenix 、および構成されている場合は、デフォルトのファイアウォールをロードします。
stop（停止）	ファイアウォールの管理セグメントをつぎの順序でシャットダウンします： pafserver、paflogd、thttpd-phoenix。アクティブなファイアウォールおよびカーネル・モジュールは、ネットワークがそのまま保護されるように残されます。
shutdown（シャットダウン）	pafserver のシャットダウン、アクティブなファイアウォールの削除、paflogd および thttpd-phoenix のシャットダウン、カーネル・モジュールの削除を行います。アクティブなファイアウォールは存在しなくなるので、ネットワークはもはや保護されません。
status（状態）	ファイアウォールのつぎの各管理セグメントの実行時状態とプロセス ID をリストします： pafserver、paflogd、thttpd-phoenix。現在インストールされているいずれかのアクティブなファイアウォールの状態を確認するには、ldfirewall をご利用ください。
masq-config（マスカレード機能の構成）	IP マスカレード機能の構成に使用します。
portfw-config（ポート・フォワード機能の構成）	ポート・フォワード機能の構成に使用します。

ldfirewall

ldfirewall は、ファイアウォールのカーネル・モジュールと他の Phoenix コンポーネントの間のプライマリなインターフェースです。これはファイアウォール・ルールのセットをインストール/削除したり、ファイアウォールの状態をチェックしたり、その他の雑用をこなします。オプションなしで実行すると、ldfirewall は利用方法とともにバージョン情報を返します。

/usr/sbin/ldfirewall interface firewall-file

与えられたフィルタ・ファイルに記述されているルールセットを使用して、指定のインターフェースにアクティブなファイアウォールを作成します。

/usr/sbin/ldfirewall –r interface

アクティブなファイアウォールを指定のインターフェースから削除します。これにより、すべてのトラフィックはインターフェースを通行することができます。

/usr/sbin/ldfirewall –q [interface…]

インターフェースが指定されていない場合、すべてのインターフェースのすべてのアクティブなファイアウォールをリストします。

/usr/sbin/ldfirewall -v

ファイアウォール・ソフトウェアのバージョン情報を表示します。与えられた Phoenix のインストレーションが正しいライセンスのものかを確認するために、通常は –p オプションとともに使用されます。

/usr/sbin/ldfirewall -p

ファイアウォールのライセンス情報を表示します。与えられた Phoenix のインストレーションが正しいライセンスのものかを確認するために、通常は –v オプションとともに使用されます。

/usr/sbin/ldfirewall -I ホスト ID を表示します。

pafphrase

SMS GUI の現在のパスフレーズを忘れた場合、パスフレーズをリセットします。ご注意ください： pafphrase 実行後に GUI を利用すると、 GUI は再度パスフレーズを変更するよう要求してきます。コマンドは **/user/sbin/pafphrase** においてあります。

telnet

ある特定の状況下では、お客様はアプライアンスへの直接の シェル・ アクセスを必要とするかもしれません。そのために、私どもはオン・デマンドの telnet daemon **をセットアップしました。これは** SMS（Admin **メニュー）またはフロント・パネル・コントロールのキーホール・ボタンからのみ有効にすることができます。**

有効にすると、お客様は 8 **文字のパスワードをフロント液晶パネルまたは** SMS GUI **のポップアップ・ウィンドウから受け取ります。**telnetd **は接続のために** 5 **分間待機し、接続が確立できなければ自分自身をシャットダウンします。毎回、**telnetd **は生成された** 1 **回限りのパスワードで** 1 **接続を受け入れます。必要な各シェルに対して、お客様は** 1 **回ずつ** telnet **を有効にする必要があります。また、**telnetd **はポート** 2323 **で実行されています。したがって接続のコマンドはつぎのようになります：** **telnet <myfirewall> 2323** **。**<myfirewall> **はお客様のファイアウォールのホスト名または** IP **アドレスに置き換えてください。**

5 Phoenix を既存のネットワークにインストールする

ベース・マシンのセットアップ(ハードウェア、OS、Phoenix ソフトウェアのインストールおよび構成)が完了すれば、お客様はそれをネットワークに設置することができます。以下は一般的なネットワーク環境についての説明およびユニットをインストールするうえでの注意点を記述しています。この節はそれぞれの環境でのインストレーションの全般的なガイドラインを含んでいます。お客様がネットワークに関する知識を持ち、どのように機能するかを理解されていることを前提としています。

5.1 標準的なネットワークのインストレーション

標準的なネットワーク上でのインターネット接続は、インターネット・サービス・プロバイダ (ISP) を通じて実現されています。ISP から入ってくる接続は CSU/DSU 、ルータ、または何らかの形式のモデムに向けられます。そしてその後内部ネットワークに進みます。Phoenix ファイアウォールは既存のネットワークに挿入された場合、ゲートウェイ・ルータの代わりを務めます。 LAN 上のすべてのマシンはファイアウォールに向け、ファイアウォールは CSU/DSU に向け、その先は ISP に向ける必要があります。もちろんこれは逆方向についても同様です：したがって、CSU/DSU はパケットがファイアウォールにルーティングされるようにあらためて構成してください。しかし、ファイアウォールを正しく動作させるには、外部および内部のインターフェースはそれぞれ異なるネットワーク上に存在しなくてはなりません。すなわち、新しいネットワークを CSU/DSU とファイアウォールの間に設置する必要があります。

新しいネットワークを設置する際に選択可能な方法はいくつかあります。ファイアウォール・マシンの各インターフェースは別のネットワーク上に存在しなければならないということを覚えておいてください。場合によっては、お客様の ISP との連携アクションを必要とする可能性もあります(例えば、追加ネットワークの取得が必要かもしれません)。

5.1.1 透過イーサネット・モード

既存のネットワークへのファイアウォールのインストレーションを容易にするために、透過イーサネットが開発されました。これによりファイアウォールをインストールする際に、お客様の既存のネットワークの IP アドレスを変更する必要がなくなります。このモードの制限は内部および外部の両方のインターフェースが 24 ビット以下のネットマスク(標準的なクラス C)の同一ネットワーク上に構成されなければならないことです。また、ゲートウェイとなるルータは外部イーサネット・ポートに接続されなければなりません。ゲートウェイ・ルータの IP アドレスは、初期ネットワーク構成でセットされた External Gateway です。

透過イーサネット・モードでは、ファイアウォール・アプライアンスの内部および外部の

アドレスは、既存のネットワークのように同じクラス C に存在するユニーク(唯一)な IP アドレスとなります。通常のネットワーク構成では、ルーティング・ルールがパケットを送信すべきインターフェースを判断できないため、これはうまく動作しません。つぎのダイアグラムはこのタイプのインストレーションを示しています。ファイアウォール・アプライアンスをインストールする前のネットワークの例は図 6 に示されています。

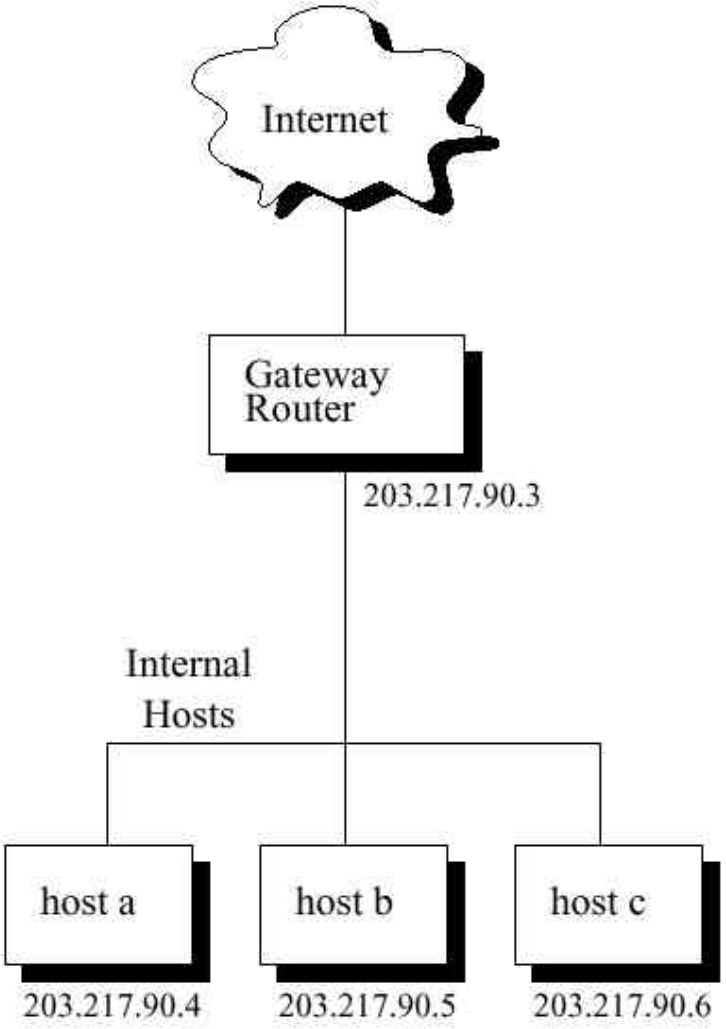


図 6 ファイアウォールなしの元のネットワーク

ファイアウォールが適切に設置され、上述したように構成されると、ファイアウォールは外部インターフェースのデフォルト・ルートの IP アドレス(203.217.90.3)を知り、また、すべての 203.217.90.x/24 パケットを内部インターフェースにルーティングします。各 PC が 203.217.90.3 のイーサネット・アドレスを問い合わせると、ファイアウォールは偽って内部インターフェースのイーサネット・アドレスを各 PC に返します。ルータが何れかの PC のイーサネット・アドレスを問い合わせるときには、ファイアウォールは再び偽

って外部インターフェースのイーサネット・アドレスをルータに返します。
透過イーサネットが有効になっているネットワークは図 7 のようになります。

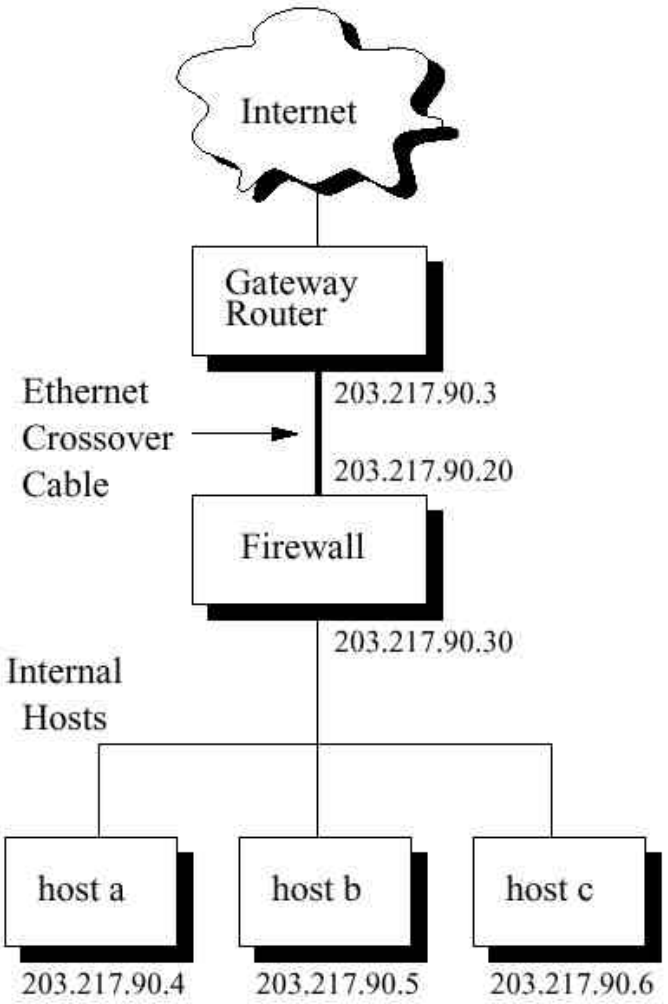


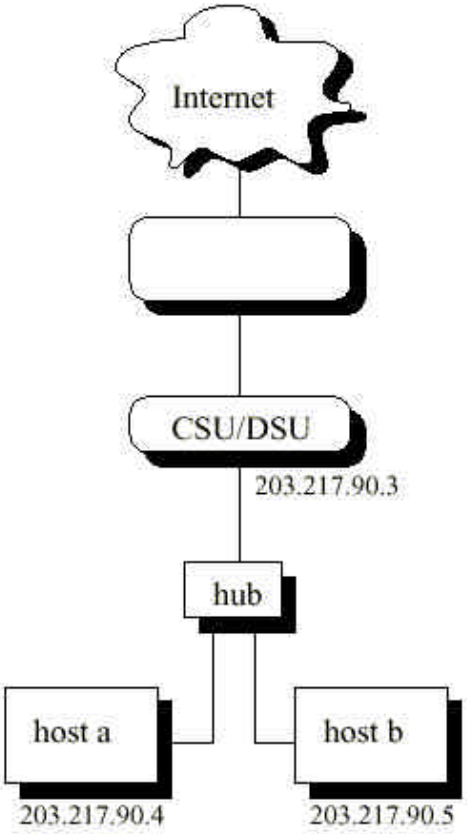
図 7 透過イーサネット・モードでインストールされた
ファイアウォールを持つネットワーク

5.1.2 30 ビットのネットワーク

これはネットマスク 255.255.255.252 を持つ、別名 /30 で知られるネットワークです。このネットワークは利用可能な 4 つの IP アドレスを与えます：ネットワーク・アドレス、ブロードキャスト・アドレス、および 2 つのホスト・アドレスです。1 つ目のホスト・アドレスは CSU/DSU に、2 つ目はファイアウォール・マシンの外部インターフェースに使用されます。ファイアウォール・マシンの内部インターフェースには、元のルータの外部インターフェースのアドレスが割り当てられます。LAN に到達するには設置された /30 ネットワークを通過する必要があるということに基づき、ISP は CSU/DSU の適切な構成を行います。これが完了すれば LAN 上のすべてのマシンは、ファイアウォールのイン

ストール前と同様に機能するはずです。図 8 はネットワークのインストール前とインストール後を示しています。

ファイアウォールをインストール前のネットワーク



ファイアウォールをインストール後のネットワーク(/30 net)

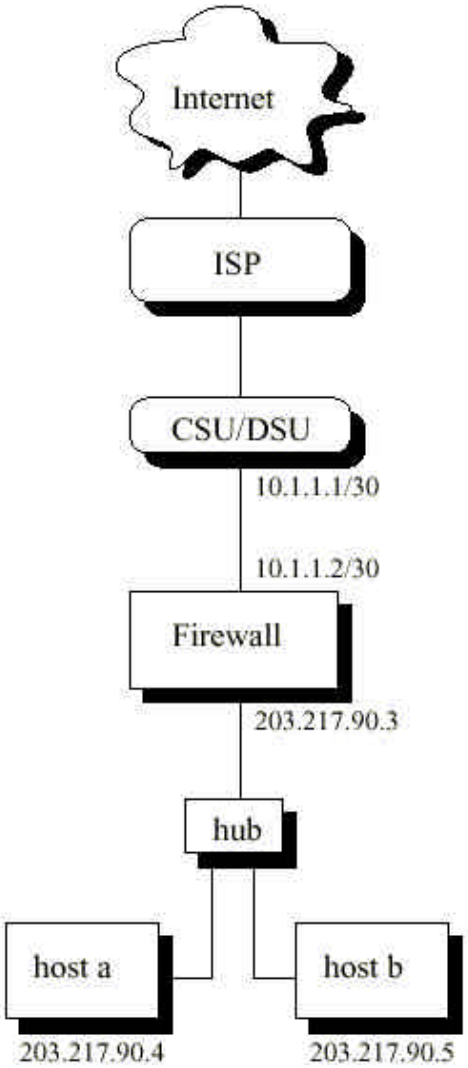


図 8：30 ビットのネットワークの利用

5.1.3 非公式な IP ネットワーク

非公式な IP ネットワークとは、ルーティングが不可能な特別な IP アドレスのセットを内部で使用するネットワークを指します。一般的に定義される標準的なアドレスは 10.X.X.X および 192.168.0.X です。非公式な IP ネットワークはファイアウォールと

CSU/DSU の間に設置可能です。これは 30 ビットのネットワークと似ていますが、お客様が CSU/DSU を制御できるという前提があります。その構成は ISP に問い合わせすることなく行うことができます。

5.1.4 24 ビットのネットワーク

1 台の(または複数の)マシンをファイアウォールの外に設置したい場合､最も良いソリューションは中型の 24 ビットのネットワークを使用する方法です。このネットワークはネットマスク 255.255.255.0 を持ち、スタンダードなクラス C のネットワークです。これはネットワーク・アドレス、ブロードキャスト・アドレス、および 254 のホスト・アドレスを与えます。セットアップは上述の 2 つと似ていますが、利点はファイアウォールの外にも追加アドレスを持つことができるということです。Progressive Systems 社はこのタイプの構成を推奨しません。ファイアウォールの外にさらされたマシンを正しく見せるルーティング技術は非常に複雑で難しいからです。

5.2 境界ネットワークのインストレーション

DMZ(De-Militarized Zone/非武装緩衝地帯)とも呼ばれる境界ネットワークは、メール・サーバまたは Web サーバのように、ファイアウォール外のホストマシンで特定のサービスを提供したい場合に便利です。このようにさらされたネットワーク上のホストは、一般的には提供する特定のサービスのみにアクセスできるように構成します。

内部ホストは一般的に境界ネットワーク上のホストに知られない別のネットワーク上に存在します。ほとんどの場合、アプライアンスの外部インターフェースのみにファイアウォールがインストールされます。このファイアウォールは、内部ホストからインターネット全般への外向きトラフィックを許可するように構成されるでしょう。内向きトラフィックは DMZ 上のホストへのみ許可されます。

DMZ 上のあるホストが内部ネットワーク上のホストにアクセスしなければならない場合は、ファイアウォールは DMZ インターフェースにもインストールされるかもしれません。このファイアウォールは､DMZ と内部マシンとの間のトラフィックを厳重に制限します。接続は、内部ネットワーク上の必要とされるホストとサービスのみへ許可されます。このタイプのセットアップでは、ファイアウォール・ルールが悪化していると思われることにご注意ください。このアクティブなファイアウォールは常にこのインターフェースと関連して実施されており、ファイアウォールされた他のどのインターフェースのものとも独立しています。従って、DMZ からのトラフィックでこのインターフェース(および内部マシン)に向けられたものは内向きトラフィックと考えられます。図 9 をご覧ください。

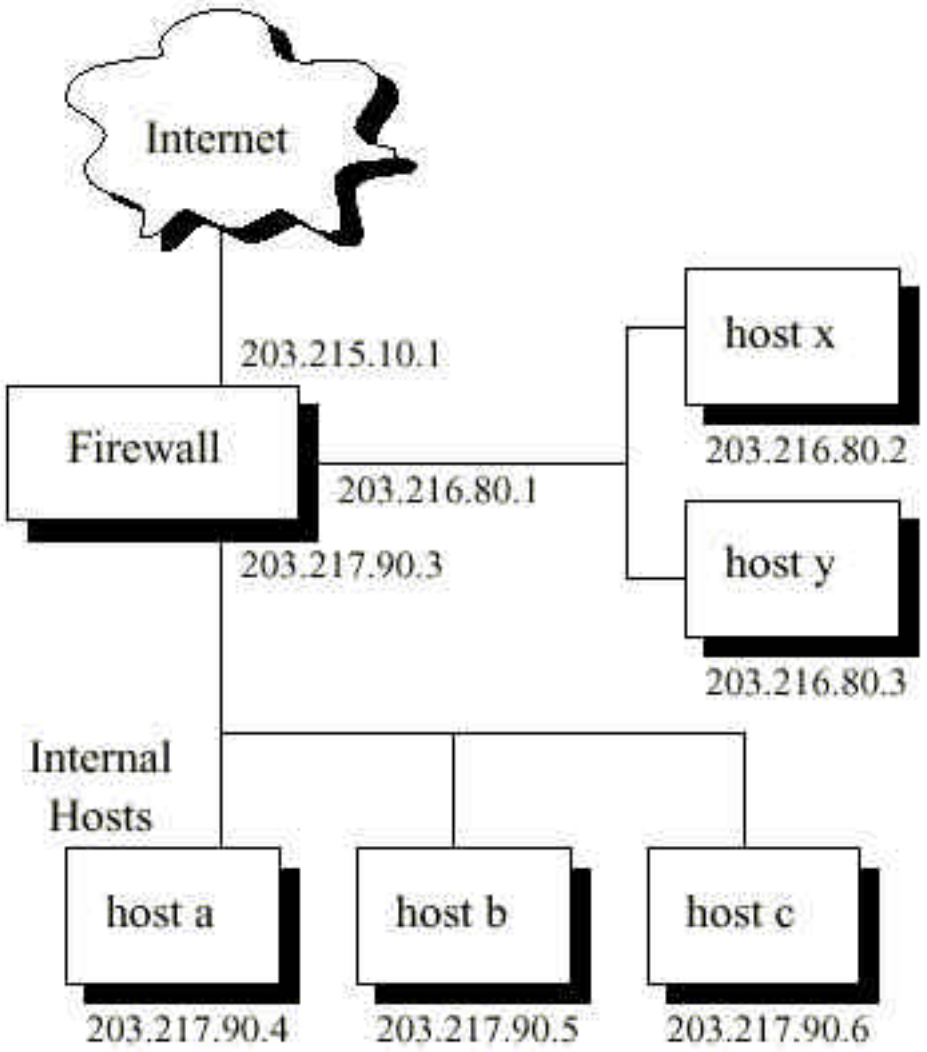


図 9：境界ネットワークの利用

6 ネットワーク・セキュリティの一般的な懸念

Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) のそのユニークでパワフルな機能を完全に利用するためには、ネットワーク・セキュリティの重要性およびネットワーク管理者が直面する問題点を理解する必要があります。これらの点を理解することは、ネットワーク・セキュリティの諸問題に対して独自のソリューションを導入する助けとなります。

インターネットの爆発的な発展により、従来には見られなかったような情報技術を利用する機会がビジネスに与えられました。しかしながら、今日のビジネスを繁栄させている最先端のネットワーク技術は、ネットワークでつながれたグローバルなコミュニティにとって残念ながら深刻な脅威でもあります。

インターネットの発展に影響している最も重要な点は、 World Wide Web の普及に隠されているのかもしれません。インターネットの広大な情報を一般ユーザーに公開したのは、World Wide Web が初めてだからです。 World Wide Web の普及が大勢の新しいユーザーをインターネットに動員し、その数は毎日増え続けています。企業はこの新しいテクノロジーに対応し、製品情報、宣伝資料、およびオンラインの製品販売を提供してきました。しかし、この爆発的な発展にともない、新種のクラッカー (破壊・解読行為を行う者) が出現し始めています。また、所有する情報を盗んだり、無防備にインターネットに接続されたシステム内にある重要なデータを破壊したりするような、悪意に満ちたビジネスも出現しています。それらの対応策として、ユーザーはネットワークの潜在的な弱点を分析するグラフィカル・ユーザー・インターフェース (GUI) が提供されているツールを使用するかもしれません。しかし、例えば Dan Farmer 社の SATAN (System Administrator's Tool for Analyzing Networks) (ネットワーク分析のシステム管理者用ツール) のようなソフトウェアは、ネットワークおよびシステム管理者が使用することを意図してはいるものの、その使いやすさはハッカーにとっても理想的なツールとなります。ネットワークおよびコンピュータ・セキュリティのエキスパートの多くが、簡単に使用できるウィルス・ビルダ、パスワード・デコーダ、およびネットワーク・セキュリティの信頼性を傷つけるようにデザインされた他のツールの出現はやむを得ないものと予測しています。これらのツールが使い易くなるにつれ、潜在的なシステム・クラッカーは増加し、同時にネットワークにつながれたシステムが侵される頻度も急激に増加するでしょう。

6.0.1 セキュリティ・ポリシーの確立

ネットワークまたはネットワークにつながれたホストに対する脅威の可能性があるとともに、既存のシステムから派生した数多くの技術や法的な細分化が進んでおり、セキュリティ・ポリシーの確立は今日の世の中で必須なものとなっています。

適切なセキュリティ・ポリシーは、ネットワークの日々の運用においてあらゆる局面を処

理するものでなくてはなりません。ネットワークのユーザーは誰か、ネットワークの正しい利用方法、決められた利用方法に違反した場合のレスポンスなどの定義は、適切なセキュリティ・ポリシーに含まれます。どのリソースおよびデータが保護されるべきかという意思決定がされる必要があります。お客様はそれらのリソースへアクセス可能なレベルや容易さも定義し、実施しなければなりません。さらに、ネットワークの物理的なセキュリティおよびアクセスについても考慮することが必要です。組織によってそのニーズおよび詳細は異なりますが、それぞれの組織は独自のセキュリティ・ポリシーを持つべきです。優れたセキュリティ・ポリシーの主な要素は、権利のない一般ユーザーをお客様のネットワークから排除するということです。ネットワーク上に存在を認めるトラフィックのみを許可し、然るべきデスティネーション (目的地) に到着させることは、ファイアウォールを使用することで促されます。しかしファイアウォール単独では、組織のセキュリティ要件に対する包括的なポリシー確立の代替にはならないことをご理解ください。

6.0.2 ファイアウォール・デザインの基本的な原理

ファイアウォールを定義する際､ネットワーク・ベンダは 2 つの一般的な原理を用います。1 番目は、ユーザーが、ファイアウォールの通過を明確に拒否されるサービスのリストを定義する "寛容" の原理です。このリストに記載のないすべてのサービスの通過は許可されます。 Progressive Systems 社ではこの原理を推奨していません。

2 番目は、特定の認証済みサービスをユーザーが定義する、"制限" の原理です。明確にリストされていないすべてのサービスは除外され、それらはファイアウォールの通過を許可されません。この原理は設定時に注意を必要としますが、前者よりも安全な選択と思われます。なぜなら、"寛容" の原理が用いられているファイアウォールは、設定漏れのエラーによるセキュリティの穴を作ってしまうからです。すなわち、"寛容" ファイアウォールでの入力漏れは、漏れたサービスでも本質的にはファイアウォールの通過を許可することを意味します。これに対し、"制限" の原理での漏れは、漏れたサービスが制限される結果に終わります。しかし、漏れたサービスの事実はただちにネットワーク管理者の目にとまるので、通常の漏れはさほどサービスに影響を及ぼすこともなく、ネットワーク・セキュリティが脅かされることはないでしょう。

6.1 パケット・フィルタリングについての簡単な解説

ネットワークに適用される "フィルタリング" という用語は、パケット・フィルタと物理的な処理で利用されるフィルタが類似していることに由来しています。例えば養魚用の水槽では、水は絶え間なくフィルタを通って流れています。水中にはときどき泥や瓦礫の形で汚れが含まれています。フィルタがそれらの不要な物質を抽出し、必要である水のみを通過させています。

パケット・フィルタリング・ルール (パケット・フィルタの運用指示) は、内向きおよび

外向きパケットを制御する方法を提供します。これらのルールはネットワーク・プロトコルの外側で働き、ユーザーにはトランスペアレント (透過的) です。一般的には、パケットを LAN から LAN へ、または LAN と外部ネットワークとの間で受渡しする際、フィルタがネットワーク間のゲートウェイとなります。したがって、これらのルールはフィルタによって生成されます。
パケット・フィルタのルールは、ネットワーク・トラフィックに対するシステム管理者のポリシーを実施します。ポリシーはつぎの両極端ないずれかから展開します：

A．明確に禁止されていないものは許可される
B．明確に許可されていないものは禁止される

明らかに、 B の前提は A の前提よりも寛容ではありません。パケットがあるルールに合わない場合にそれらを許可するよりも、パケットがルールに合わない場合はそれらをブロックする方がより安全です。さらに、 A のアプローチは絶えず注意が必要と言えます。フィルタリングでブロックするべきすべてのパケットをうまく認識させるような場合、新しいサービスがネットワークに追加される際にルールの追加を前もって計画する必要があります。
セキュリティ・ポリシーの基本的な前提がアクセスを許可することであっても禁止することであっても、パケット・フィルタリング・ルールには適応性がなく、常にスタティック (静的) です。つまり、パケット・フィルタリング・ルールは実行中ではなく実行前に決定されています。また、スタティックなパケット・フィルタは A の前提に従って働きます。
アダプティブ・ファイアウォール技術 (Adaptive Firewall Technology) は、ファイアウォール・サーバを通過するパケット中の情報に基づいて各ルールを適応させるため、どのようなパケット・フィルタリングよりも優れています。各パケットおよびそのヘッダをモニタし、トリガを探し出し、そしてネットワーク・アクセスを一時的に許可するようにあらかじめ用意されているテンプレートを編集します。

アダプティブ・ファイアウォール技術 (Adaptive Firewall Technology) は、パケット・フィルタリングにもう 1 つの選択肢を提供しています：

すなわち、パケット・データ中の情報を特別なトリガとして認識します。このトリガを使用して、ある一定時間だけファイアウォール・プロセスに挿入される新しいファイアウォール・ルールのセットを生成します。
ファイアウォールの各ステップは、 "入力" ストリームの各データグラムに対しつぎの 5 つのうちいずれかのアクションをとることができます：

1. データグラムが現在のファイアウォール・ルールの要件と一致した場合、次のステップへ進む
2. データグラムが現在のファイアウォール・ルールの要件と一致しない場合、ファイアウォールの後のポイントへスキップして進む
3. データグラムの通過を許可し、そのデータグラムに関するそれ以上の処理は行わない
4. データグラムを拒否 (破棄) し、そのデータグラムに関するそれ以上の処理は行わない。ただし、オプションで ICMP 配信不能メッセージを送信元に返すことができる。拒否されたパケットのロギングもオプションで可能
5. そのデータグラムを特別なトリガ・データグラムとして認識する。このトリガ・データグラムを出力ストリームへ単に通過させたりブロックしたりするのではなく、ある一定時間だけファイアウォール・プロセスに挿入される新しいファイアウォール・ルールのセットも生成する

上記のリストの最初の 4 つのオプションは、従来のスタティックなパケット・ファイアウォールを提供します。5 つ目のオプションが Phoenix をユニークなものにしています。なぜなら、アダプティブ・ファイアウォールは、従来のパケット・ファイアウォールとは異なり、状態検査技術を使用してデータグラム入力ストリームを処理します。すなわち、随時変更を伴った入力ストリームに対しても対応することが可能です。

Progressive Systems 社の Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) は、特定の 2 つのエンドポイントに対する制限されたセッションを設定することにより、各パケットに対応することができます。このセッションは特定の時間内に特定のアプリケーション・パケットのみを通過させます。 Phoenix Firewall により、ユーザーは、初めてインターネットのような公開ネットワークを越えたコミュニケーションで今日のビジネスが必要とする柔軟性を保ちながらデータ通信に関する完全なセキュリティを維持することが可能となりました。

7 Phoenix Adaptive Firewall の構成

Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) の構造および機能はご理解いただけましたでしょうか？これからは Phoenix を実際に構成してみましょう。本マニュアルのこの章では、Secure Management System GUI を詳しく紹介しています。

7.1 Secure Management System への接続

SMS GUI に接続するには、バージョン 4.07 以降の Java 対応の Netscape ブラウザを起動する必要があります。Windows プラットフォームは、最新のバージョンならば適切でしょう。Linux ではこれまで Netscape、Java、さまざまなウィンドウ・マネージャ、および SMS との相互作用についていくつか問題がありました。KDE ウィンドウ・マネージャのもとで動作する Netscape バージョン 4.07 以降は最も安定したブラウザであることがさまざまな Linux の構成でもわかっています。現在人気のある Netscape のバージョン、互換性に関する既知の課題、すべてのワーク・アラウンドまたは解決方法は、弊社のサポート Web サイト（**http://www.progressive-systems.com/support/**）でご覧いただけます。お客様は必ず最新の情報を確認してください。上述以外のブラウザによる SMS の利用はサポートしておらず、充分に動作しない可能性があることにご注意ください。また、SMS はマッキントッシュ・プラットフォームからは信頼性のあるアクセスができないことをご承知ください。

ブラウザ起動後、 **http://myfirewall:8181** を開いてください。 “myfirewall” は、ファイアウォールを実行しているホスト名または IP アドレスです。 Phoenix アプライアンスに接続すると、図 10 のようなスプラッシュ画面が表示されます。この画面から SMS の開始または SmartGate VPN 関連ファイルのダウンロードが可能です。

“Start Secure Management System(SMS を開始)”のリンクをクリックすると SMS の起動画面が現れ、続いてログイン・ウィンドウが表示されます（図 11 参照)。インストール時に生成された GUI パスフレーズを入力してください。SMS に初めてログインする場合、お客様はパスフレーズを変更するように要求されます（図 12 参照)。この後パスフレーズを変更するウィンドウが表示されます（図 13 参照)。これでアクティブなファイアウォールのパラメータを構成することが可能になります。

図 10 Phoenix **ファイアウォール・アプライアンス・スプラッシュ画面**

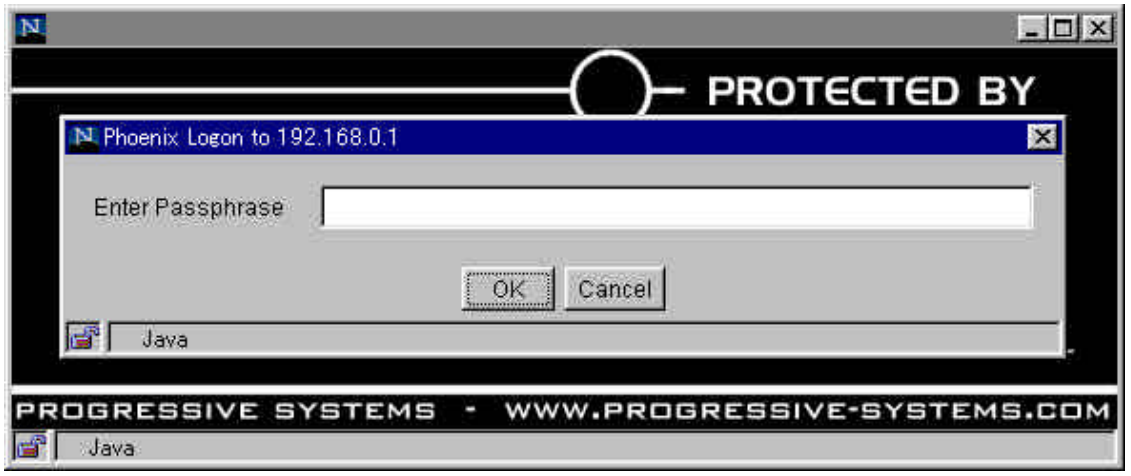


図 11：SMS ログイン・ウィンドウ

図 12：SMS パスフレーズ変更通知

図 13：SMS パスフレーズの変更

7.1.1 さまざまな機能を持つ Secure Management System

SMS GUI の初期画面を説明します。ウィンドウ上部はつぎのアイテムを含むメニューがあります：File (ファイル)、Firewall (ファイアウォール)、Admin (管理)、および About (バージョン情報)です。これらに含まれる機能に関しては 4.2.1 節をご覧ください。メニューの下の左側には、フィルタ・テンプレートに含まれるアプリケーションの一覧（4.1.8 節参照）があります。初期画面では、右側に Progressive-Systems 社への問い合わせ先と "Select an item from the list to the left (左側の一覧からアイテムを選択)" という案内が表示されます。(図 14 参照)

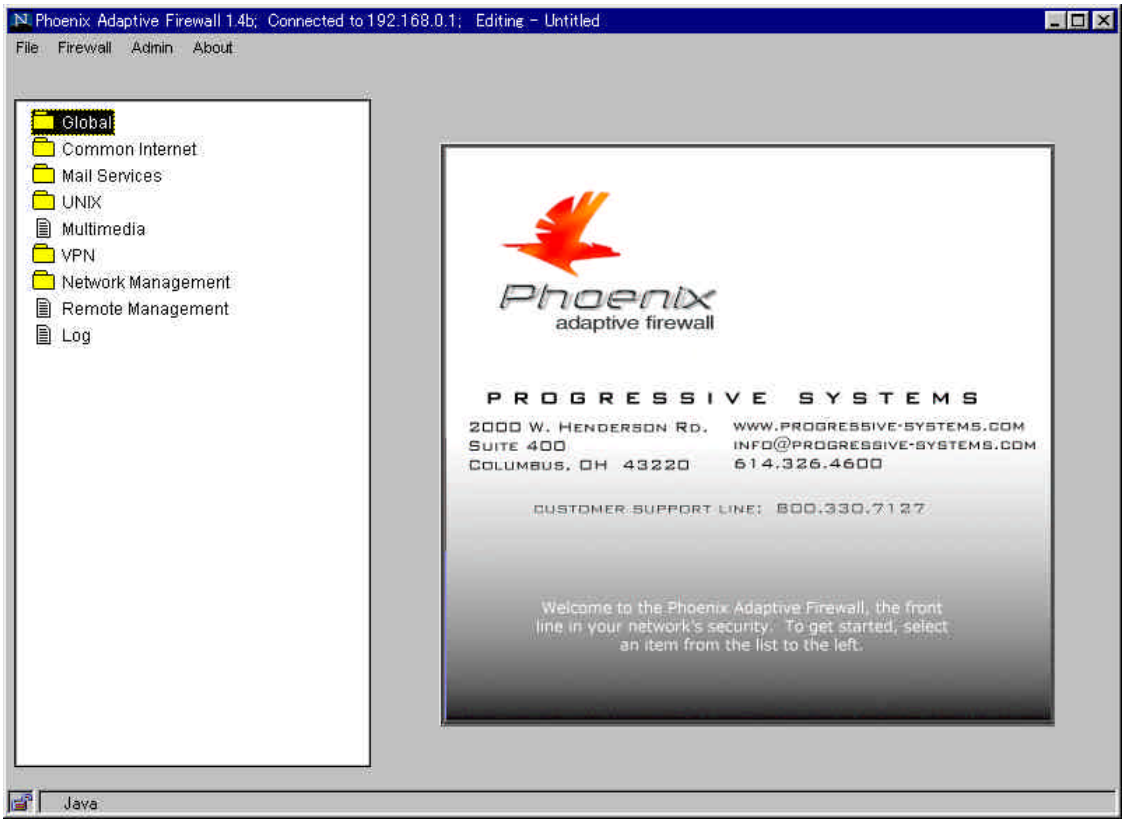


図 14：SMS 初期構成ウィンドウ

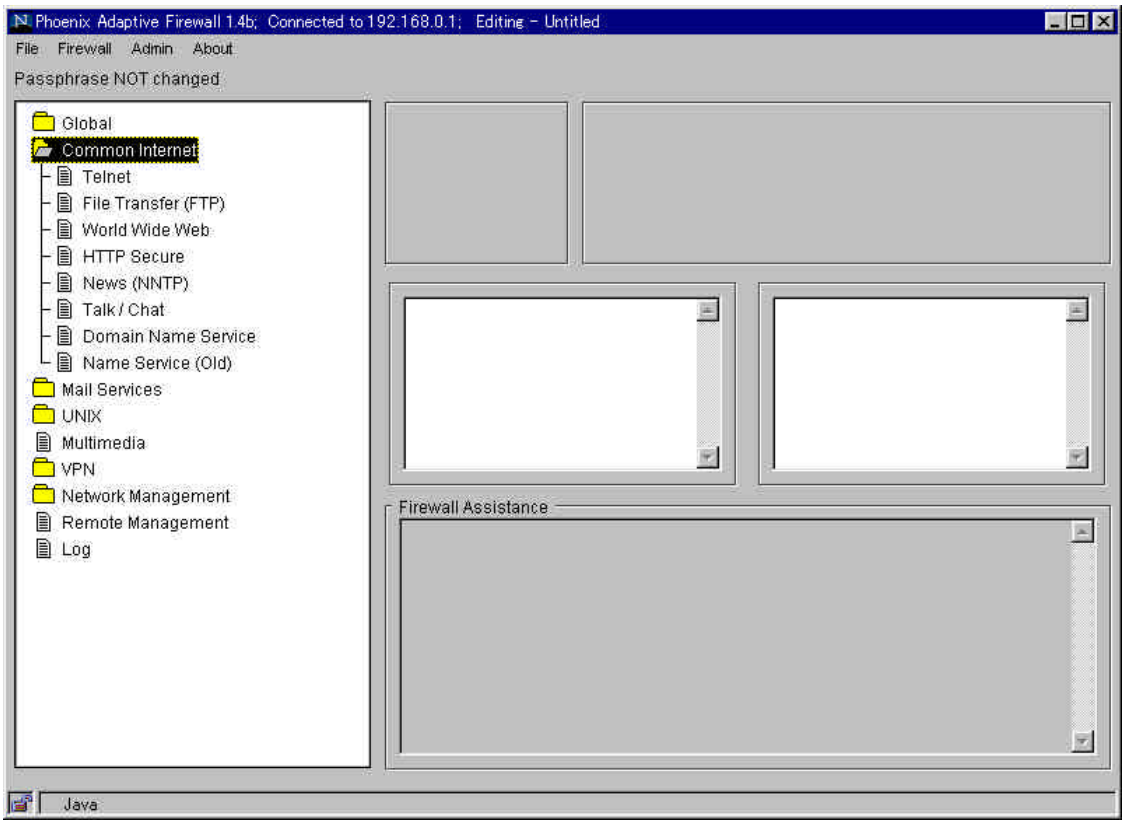


図 15：SMS Common Internet（一般的なインターネットの）アプリケーションおよびプロトコル

“Common Internet （一般的なインターネットの）” というフォルダをダブルクリックしてください。フィルタ・テンプレートで定義されている利用可能なアプリケーションおよびプロトコルが続いて表示されます。右側の初期画面は追加ウィンドウを含む 3 つの段に切り替わっていることに気づくでしょう。1 段目には 2 つのウィンドウ、2 段目には（スクロールバーつきの）2 つの入力欄、そして最後の段には“ファイアウォール・アシスタント” という名前の 1 つのウィンドウがあります。アプリケーション/プロトコルの構成エリアはこれらから成ります。（図 15 参照）

“World Wide Web” というファイルをシングルクリックしてください。構成エリアが完全にロードされます。アプリケーション/プロトコルが左の列から選択された場合、その選択に関する構成の初期画面がロードされます。デフォルトでは、そのアプリケーション/プロトコルで許可される内向きトラフィックの構成のための画面が表示されます。これは上部左側の “Incomming (内向き)” チェックボックスにより示されます。その隣の右側の欄は、ロードされているアプリケーション/プロトコル名の名前、すなわちこのケースでは “World Wide Web” とラベルされます。この欄には有効なプロトコルが表示されます。

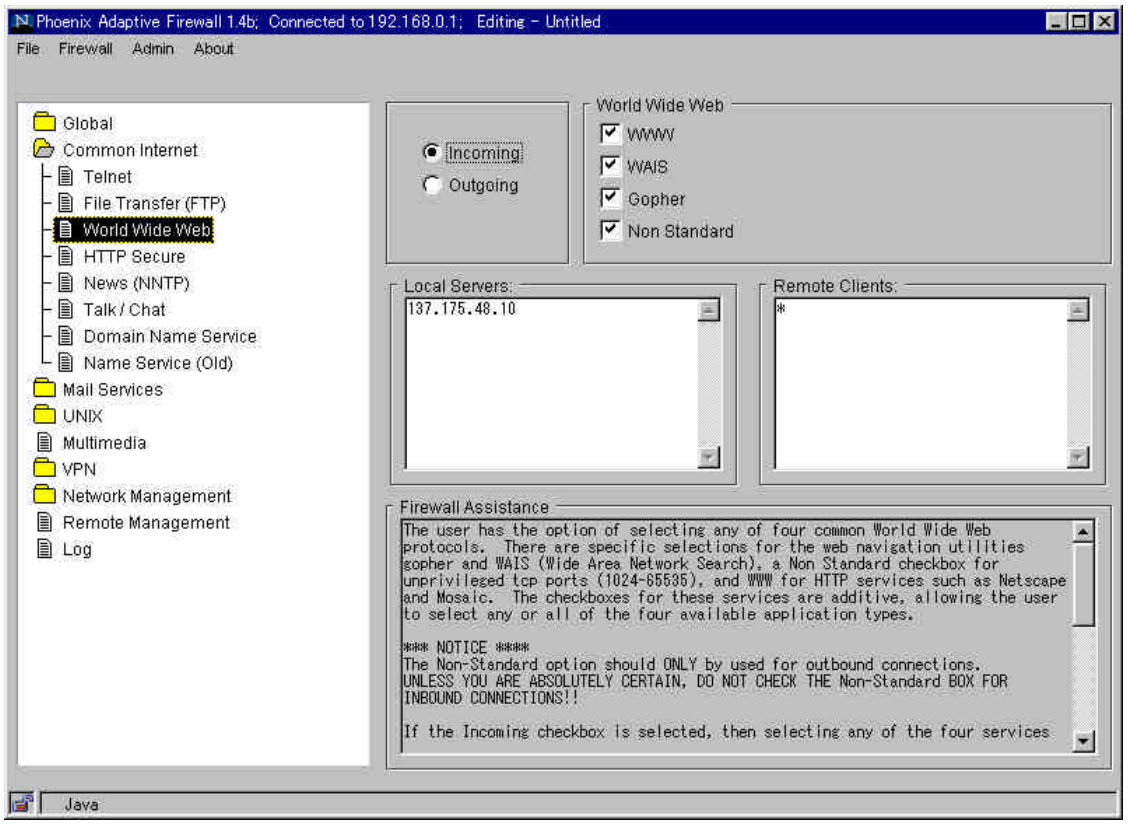


図 16：SMS 内向きサービスの構成 (WWW)

ここで“WWW”チェックボックスをクリックすると、お客様の Web **サーバへの接続を許可する適切なホスト情報が入力可能になります。Local Servers (ローカル・サーバ)** および **Remote Clients (リモート・クライアント)** 入力欄にホスト・アドレスが入力されるまでは、トラフィックはファイアウォールを通過しないことをご理解ください。すなわち、プロトコルを有効にするだけでは不充分であり、お客様は接続のエンドポイントがどこになるかを指定する必要があります。**Local Servers (ローカル・サーバ)** の入力欄(2 段目左側)には、お客様の Web サーバのアドレスを入力してください。**Remote Clients (リモート・クライアント)** の入力欄(2 段目右側)は必ず **Local Servers (ローカル・サーバ)** の入力欄で指定された Web サーバへのアクセスを必要とするホストの IP アドレスを含んでいる必要があります。外部ネットワーク上(通常はインターネット上)のすべてのホストから Web サーバが見えると仮定した場合、考えられるすべての IP アドレスをどのようにしてすべてリストすればいいのか疑問に思われることでしょう。これは **Remote Clients (リモート・クライアント)** の入力欄にアスタリスク (*) を入力すれば可能です。上の例では、ファイアウォールの内側の Web サーバである **Local Servers (ローカル・サーバ)** のアドレスが 137.175.48.10 であることを示しています。 **Remote Clients (リモート・クライアント)** の入力欄は * を表示しています。したがって、これはファイアウォール外のすべてのホストが 137.175.48.10 にアクセスできるということを意味します。(図 16 参照)

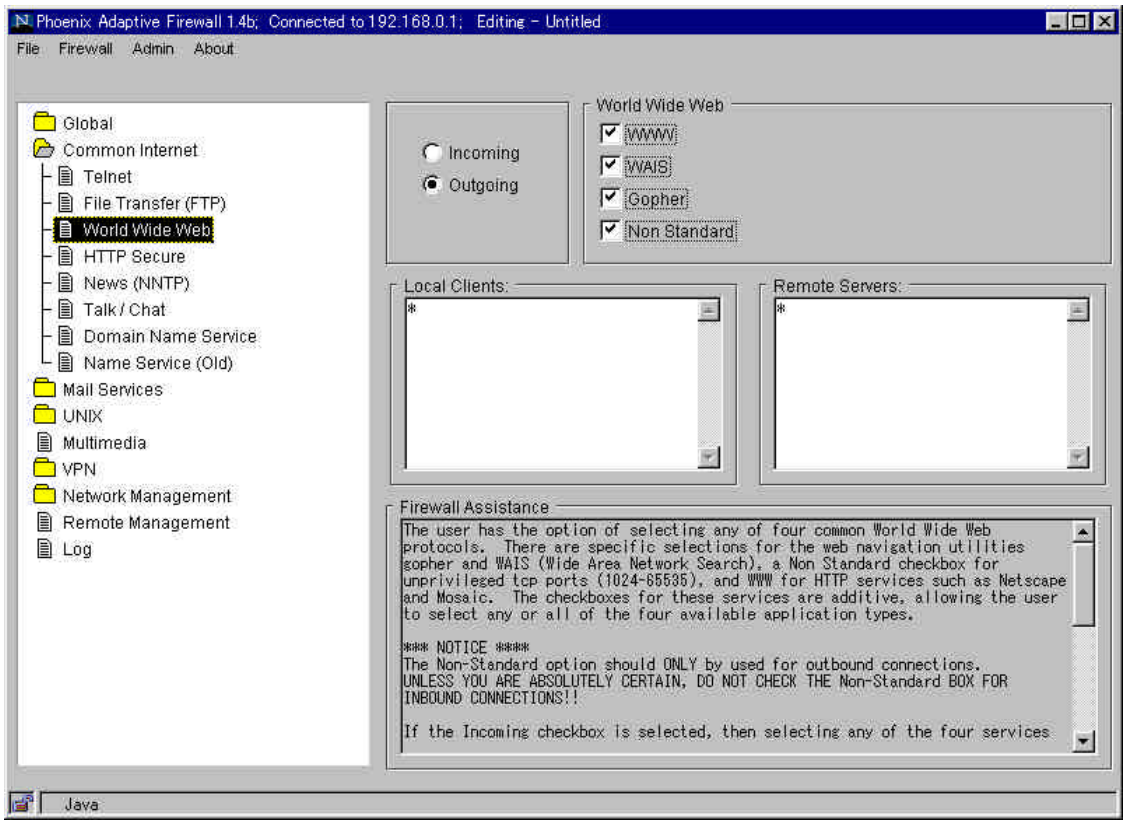


図 17：SMS 外向きサービスの構成 (WWW)

つぎに **Outgoing (外向き)** チェックボックスをクリックしてください。入力欄が空白の **Local Clients (ローカル・クライアント)** および **Remote Servers (リモート・サーバ)** に変更されたことにお気づきでしょう。加えて、いずれのプロトコル・オプションも選択されていません。ほとんどの場合、ファイアウォール内のすべてのマシンから、ファイアウォール外のすべての Web サーバへの外向き Web トラフィックを許可したいはずです。そのためには、 **Local Clients (ローカル・クライアント)** および **Remote Servers (リモート・サーバ)** の両方の入力欄にアスタリスク (*) を入力します。さらに、ファイアウォール内の誰かが必要とするときにアクセスができるように、**WAIS** および **Gopher** のチェックボックスもチェックします。(図 17 参照)

Firewall Assistance (ファイアウォール・アシスタント) ウィンドウにお気づきになられましたか？ この画面は、構成に関する一般的な情報やヒントとロードされたアプリケーション/プロトコルに関する詳細情報を表示します。図 16 の例では、**Non Standard (非スタンダード)** オプションの利用について、外向きの接続に限定するべきとの注意書きが表示されています。プロトコル・オプションを構成する前に、必ず **Firewall Assistance (ファイアウォール・アシスタント)** に表示される情報をお読みください。ここでの例と同様に、プロトコルの誤解や誤った構成がもたらす結果を警告または注意する文章が表示されます。

7.2 構成の全般的なヒント

7.2.1 ファイアウォール・ファイルのシンボリック・アドレス

フィルタ・ファイルはホスト名ではなく IP アドレスを使用して構成するように特に注意することが必要です。なぜなら、フィルタ・ファイルは名前の解決には Domain Name System (DNS) または NIS (Network Information Service) などのプロトコルを必要とする場合があるからです。また、 DNS が動作するためにファイアウォールされている接続が必要な場合は、ホスト名を含むファイアウォール定義は絶対に正しく解決できません。なぜなら、 (DNS クエリを含む) あらゆる情報がインターフェースを通過できる以前に、ファイアウォールは、完全にコンパイルおよびインストールされていなければならないというセキュリティ上の理由からです。ファイアウォールのルールセットを定義する際は、ホスト名よりもアドレスを使用する方が安全です。

7.2.2 ホスト・アドレス対ネットワーク・アドレス

お客様は場合によって、単独のホストからのものではなく、ある特定のネットワークを出入りするトラフィックを制限したいときがあるかもしれません。**Client (クライアント)** または **Server (サーバ)** の適切な入力欄にネットワーク・アドレスに続きネットマスクを追加すれば、そのような制限も可能です。入力形式は <network_address;netmask> です。利用可能なクラス C のネットマスクは表 5 をご覧ください。

略称	ネットマスク	ネットワーク数	ネットワークあたりのホスト数
24	255.255.255.0	1	254
25	255.255.255.128	2	126
26	255.255.255.192	4	62
27	255.255.255.224	8	30
28	255.255.255.240	16	14
29	255.255.255.248	32	6

表 5：クラス C ネットマスクの例

例えば、クラス C のネットワーク 137.175.48.0 のマシンからファイアウォール外のすべてのマシンへ telnet アクセスを許可したいとします。その場合、**Outgoing (外向き)** の Telnet 構成の画面で、**Local Clients(ローカル・クライアント)** の入力欄には 137.175.48.0;24 と入力し、**Remote Servers(リモート・サーバ)** の入力欄には * を入力してください。

7.2.3 ワイルドカードの使用

あるプロトコルの適切な欄に * 記号を入力すれば、お客様はその特定のアプリケーションまたはプロトコルの使用あるいはそれらへの接続をすべてのホストまたはネットワークに許可することができます。* の使用が危険または禁止される場合については、SMS のフ

ァイアウォール・アシスタント・ウィンドウまたはワイルドカードに関連する節に記述されています。

7.3 初期ファイアウォールの作成

SMS に接続したときに、outgoingonly という名前のファイアウォール/フィルタ・ファイルに気が付くかもしれません。これはお客様の最初のファイアウォールを生成するための良いベースとなります。このファイルは、ほとんどの標準的なインターネット・プロトコルおよびサービスに関しての外向き接続を許可します。お客様のネットワークが必要とする内向きサービスを有効にしたり、新たに必要な外向きサービスを追加したりするように編集できます。

このファイルをベースとして使用する場合は、外向きルールのみが構成されているオリジナルのファイルを残すために、お客様の変更は異なるファイルに保存するようにしてください。

7.4 プロトコルとアプリケーションのウィンドウ

これ以降の各図とその解説は、Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) がファイアウォール・ファイルを生成可能な、現在サポートしているアプリケーションおよびプロトコルのタイプを詳しく解説しています。各ウィンドウでの利用可能なオプションについても説明しています。プロトコルまたはアプリケーションのタイプを選択するには、希望する名称の横のチェックボックスをクリックします。

7.4.1 Global (グローバル)

Cracking Prevention (クラッキング防止) クラッキング防止は、ネットワークまたはシステムへの望ましくない侵入を防止するために提供されています。つぎの 4 つのオプションが利用可能です：

- **Port Scanning (ポート・スキャン)** は、ネットワークの外部から何者かがアドレス・スペースの自動スキャンを行うことを防ぎます。これらのスキャンは、ネットワーク内のシステムの位置を特定し調査するために、SATAN およびその他のツールで使用されます。
- **Anti-Spoofing (アンチ・スプーフィング)** は、信頼される内部のシステムのふりをしてリソースへアクセスしようとするクラッカーの一般的な技術を阻止するために使用されます。偽ホストのソース・アドレスがネットワーク外部から発しているものでありながらネットワーク内部に見えるアドレスを持っていることから、これらのタイプのアタックを認識することは可能です。アンチ・スプーフィング (Anti-Spoofing) オプションが選択されると、生成されたファイアウォール・ファイルは、内部ネットワーク内のソース・アドレスを持ついかなるパケットもファイアウォールされている接続を通過しな

いように防止し、偽パケットを阻止します。しかし、保護されているコンピュータ・システムのいずれかがファイアウォール外部のマシンを信頼している場合は、スプーフィングは防止できません。

Local Networks(ローカル・ネットワーク)ボックスはこの機能を有効にすると入力可能になります。このボックスは、ユーザー・サイトにとって内部となるネットワーク・アドレスのリストを定義するために使用されます。これらのネットワーク・アドレスは、信頼される内部ネットワークを特定するために、ファイアウォールのアンチ・スプーフィングで使用されます。このボックスはスクロール可能な領域なので、長いネットワークのリストも入力可能です。

・ソース・ルーティング (Source Routing) は、ルーティング情報が外部ホストによって提供されるクラッキング技術のことをいいます。このルーティング情報は、内部システムおよびルータの通常のルーティング・パスを上書きするためのものであり、パケットを不適切な目的地へリダイレクトしてしまう可能性があります。 Cracking Prevention (クラッキング防止) 画面の Source Routing (ソース・ルーティング) オプションを有効にすると、ソース・ルーティングされたパケットのローカル・ネットワークへ出入りは防止されます。

・Allow Estab (接続をアクティブなままにする) は有効にすると、編集されたファイアウォール保存時に確立された接続をアクティブなままにしておくことができる機能です。この機能が有効にされていない場合、すべての接続はアクティブなファイアウォールを保存する際にリセットされます。リセットされた接続は再度開始しなければなりません。

Local Networks/Hosts(ローカル・ネットワーク/ホスト) および Remote Networks/Hosts (リモート・ネットワーク/ ホスト) のいずれの入力欄でのアスタリスク (*) の使用は、ファイアウォールを通行する**すべての**トラフィックをブロックしてしまいます。このプロトコル/アプリケーションでは、アスタリスクは使用しないでください。

Restricted Sites (制限されるサイト) のリストは、ある特定の内部ホストが外部と通信すること、およびある特定の外部ホストが内部と通信することを完全に遮断する方法を提供します。あるホストが制限されると、そのホストは通信リンクの向こう側のどのホストとも通信できず、また、通信リンクの向こう側の各ホストもそのホストと通信できません。このリストを有効にするには、Enforce (有効にする) チェックボックスが選択される必要があります。Enforce (有効にする) チェックボックスが選択されると、 Undesirable Outsiders (望ましくない外部ホスト) および Grounded Locals (外部アクセス禁止のローカル・ホスト) ボックスが有効になり、サイト名、またはアドレスの追加、変更、削除が可能になります。これらの入力欄ははスクロール可能な領域なので、長いサイトのリストも入力可能です。

Trusted Sites (信頼されるサイト) のオプション・ボックスは、そのサイトともう一方の完全に信頼されるサイトの間のすべてのトラフィックの通行を許可します。一般的にはこれはあまりお奨めしない構成ですが、イントラネットでは便利です。

7.4.2 Common Internet (一般的なインターネット)

Telnet telnet 接続の構成が可能です。telnet の潜在的なセキュリティの問題から、お客様の内部ネットワーク上のマシンへの内向き telnet 接続を許可することはお勧めできません。telnet はポート 23 の tcp 接続をオープンします。

File Transfer Protocol (ファイル・トランスファー・プロトコル) オプションは、ローカル・ネットワークへの、またはローカル・ネットワークからのファイルの転送についてのユーザーの作業可能範囲を制御するために使用されます。Enable (有効にする)チェックボックスとともに Incoming (内向き) チェックボックスを選択すると、外部クライアントのローカルの FTP サーバへの接続が可能になります。入力欄は、Local Servers (ローカル・サーバ) と Remote Clients (リモート・クライアント) を指定するためのものが提供されます。IP アドレスのみが入力可能です。ネットワーク・アドレスを入力すると、そのネットワークからのすべてのホストが許可されます(7.2.2 節参照)。 * の記号はワイルドカードなので、リモート・クライアント部分に * を入力すると**すべての**リモート・クライアントが許可されます。
Outgoing (外向き) チェックボックスを選択し、内部サイトの外部ホストに対する FTP 接続を許可するように設定することもできます。 Outgoing (外向き) チェックボックスおよび Enable (有効にする) チェックボックスを選択すると、右側にあるスクロール可能なボックスの名前が Local Servers (ローカル・サーバ) から Local Clients (ローカル・クライアント) へ、そして Remote Clients (リモート・クライアント) から Remote Servers (リモート・サーバ) へと変更されます。
繰り返しになりますが、ここには IP アドレスのみが入力可能です。
FTP は ftp-data と ftp コマンド・チャネル用にポート 20/tcp と 21/tcp を開きます。

World Wide Web ユーザーは World Wide Web プロトコルに関して 4 つの一般的な選択オプションを持っています。すなわち、Web ナビゲーション・ユーティリティである gopher および WAIS (Wide Area Index Search) のための各選択肢、カスタム・プロトコルのための Non Standard (非スタンダード) チェックボックス、 *Netscape* や *Mosaic* のような HTTP サービスのための WWW があります。これらのサービスの各チェックボックスは同時に選択可能であり、ユーザーは 4 つの選択可能なアプリケーション・タイプのいずれかまたはすべてを選ぶことができます。

4 つのオプションのうちどれを選択しても Local Clients (ローカル・クライアント) および Remote Servers (リモート・サーバ) の入力欄が有効になり、内部クライアントによってアクセスできる利用可能なサーバまたはネットワークのリストを指定することが可能です。すべてのオプションは外向きの選択に対して制限ないアクセスを許すことが可能です。Restricted Sites (制限されるサイト)機能が、管理者にとって望ましくないと思われる外部 Web サイトへローカル・ユーザーがアクセスすることを防止するのに適しています。Web の他のエリアへのアクセスは許可されたままです。

Non Standard (非スタンダード) オプションは、内向きの接続の構成で選択された場合、tcp ベースのすべてのトラフィックに対して 1024 から 65535 のポートを開いてしまうので注意が必要です。これはお客様のファイアウォールに大きな穴をあけてしまうため、非スタンダードの内向きポートが使用される場合に、カスタム・プロトコルを利用するように強くお奨めします。詳しくは 8.1 節をご覧ください。

つぎのポート/プロトコルは World Wide Web で利用可能です：

・標準的な http/web トラフィックのための 80/tcp (WWW)

・wais

・gopher

・non standard (非スタンダード)

HTTP Secure は安全な HyperText Transmission Protocol を意味します。これは、安全なトランザクションの処理を目的として Netscape が開発した HTTP の別バージョンです。このサービスを有効にすると、 "https://" の方法のアクセスをサポートするブラウザなら、 Secure Socket Layer (SSL) を使用するサーバへアクセス可能です。

HTTP Secure は tcp 接続用にポート 443 を開きます。

News (NNTP) ユーザーは、技術情報からアートにわたる多様なトピックについての広範囲な情報にアクセスするために、*rn* のようなニュース・アプリケーションを使用します。多くのニュース・グループでは、ディスカッション・グループの形式がとられ、ユーザーは政治に関する記事や性などのデリケートな話題を投稿しています。ニュースはリレー方式で配布されます。あるサイトがニュースを受信するとそれをさらに他のサイト(複数のサイト)へ回します。ニュースはその繰り返しで流れていきます。ネットワーク管理者は News オプションにより、どのサイトからのニュースを内部ネットワークへ許可するか、およびどのサイトが内部ネットワークからのニュースの受信を許可されるかを制御することが可能です。内向きおよび外向きトラフィックの両方にそれぞれ制御機能が提供されています。

Enable (有効にする)チェックボックスとともに Outgoing (外向き) チェックボックスが選択されると、ユーザーは Local Clients (ローカル・クライアント) および Remote

Servers (リモート・サーバ) のリストを指定可能です。Enable (有効にする) チェックボックスとともに Outgoing (内向き) チェックボックスが選択されると、Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント) のリストが入力可能になります。他のオプションと同様に、各入力欄には IP アドレスが入力可能であり、* 記号がワイルドカードとして使用できます。
NNTP は tcp 接続用にポート 119 を開きます。

Talk and Chat (トーク / チャット) トーク (talk) およびチャット (chat) のプロトコルは、ネットワークを介してインタラクティブに通信する機能を提供します。ユーザーは、ほとんどリアルタイムに相手の画面に表示されるメッセージをタイプ入力することができます。この目的のために利用可能なアプリケーションおよびプロトコルはいくつか存在します。 *Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール)* のトーク / チャット(Talk/Chat)ウィンドウのオプションにより、 talk 、 ntalk (”New “ Talk) 、および irc (Internet Relay Chat) のいずれかまたはすべてのアプリケーションのパケットをファイアウォールすることが可能です。パケットは Incoming (内向き) または Outgoing (外向き) のいずれかの方向でファイアウォールすることが可能です。各アプリケーションのチェックボックスと組み合わせて Incoming (内向き) または Outgoing (外向き) が選択されると、それぞれ、 Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント) 、または Local Clients (ローカル・クライアント) および Remote Servers (リモート・サーバ) のボックスが有効になります。 talk および ntalk サービスでは、 ”クライアント” とはトーク・セッションを開始するホストのことで、”サーバ” は応答するホストのことです。セッションが進行していくと、両ホストともに事実上クライアントとなります。
つぎのポート/プロトコルがトークおよびチャットで利用可能です：
・Talk のための 517/udp
・Ntalk のための 518/udp
・IRC のための 197/tcp

Domain Name Service Domain Name Service、別名 DNS は、TCP/IP システムで名前をアドレスに変換する機能です。 DNS は階層のサービスです。 IP のネーミング協定により各ホスト名は "." の記号で区切られています。したがって、ftp.progressive-systems.com は、 ftp というホストが Com という大区分のドメインの Progressive-Systems のドメインにあることを示しています。また、ネーム・サーバは各ドメイン内に 1 つ以上存在します。ドメインのネーム・サーバは、ホスト名検索を解決するためのマップを管理しています。ネーム・サーバはこれらのマップを使用し、ドメイン内のホスト名を IP アドレス に変換します。ネーム・サーバは、ドメイン範囲外の名前

またはアドレスを尋ねられた場合、適切な情報を持つネーム・サーバを探すためにコンタクト情報のリストを使用します。
ほとんどのネーム・サーバは、ローカル・クライアントのために外部エンティティの名前およびアドレスを解決し、リモート・クライアントのために内部エンティティの名前およびアドレスを解決する必要があります。すなわち、一般的にネーム・サーバはクライアントとサーバの両方として動作します。したがってユーザーは Outgoing (外向き) および Queries (クエリ) のチェックボックスを選択し、両ボックスにアスタリスク (*) を入力します。 Local Servers (ローカル・サーバ)ボックスにそのアドレスを入力すれば、外向きクエリをお客様のローカル・ネーム・サーバからのみにできます。
お客様のネーム・サーバを外部ホストに照会させることを許可するには、 Incoming (内向き) チェックボックスおよび Queries (クエリ) のチェックボックスを選択してください。つぎに、 Local Servers (ローカル・サーバ) ボックスにネーム・サーバ・アドレスを入力し、 Remote Clients (リモート・クライアント) ボックスにアスタリスク (*) を入力します。 TCP Queries (TCP クエリ) チェックボックスを選択する前に、もう少し読み進んでください。
TCP Queries (TCP クエリ) を内向きパケットに対して選択する場合は 2 つあります。1 つ目の場合は、極めてまれですが、 DNS レコードが 512 バイトを超えるときです。この場合、超過分は返信にセットされ、お客様のネーム・サーバからは別のクエリが TCP を使用して送信されます。これらの TCP クエリはファイアウォールを通行する必要があります。
2 つ目の場合は、お客様のドメインのゾーン転送を外部のセカンダリ・サーバが行うときです。 Remote Clients (リモート・クライアント) ボックスにアスタリスク (*) がある場合、セカンダリ・サーバおよび他の誰もが、お客様のゾーン転送を行うことが可能です。セカンダリ・サーバからのみの内向きゾーン転送に制限したい場合、お客様の DNS ソフトウェアの方でそのように構成しなければなりません。 BIND 8 は特定のサイトからのゾーン転送を制限する "転送の許可" オプションが利用可能です。
お客様の DNS ソフトウェアがゾーン転送を制限する機能を持たない場合、 TCP Queries (TCP クエリ) チェックボックスは選択しないでください。その代わりに、セカンダリ・サーバからお客様の DNS サーバへゾーン転送 (内向き) を許可するカスタム・ポートを作成してください。
つぎのポート/プロトコルが DNS で利用可能です：
・クエリのための 53/udp
・TCP クエリ(ゾーン転送)のための 53/tcp

Name Service (旧) 警告－このサービスはご利用なさらないでください。
このサービスは旧バージョンとの互換性を持たせる目的にのみ提供されています。このサ

ービスは今後のリリースで削除されますので、上述の Domain Name Service のエントリに置き換えてください。

Domain Name Service、別名 DNS は、TCP/IP システムで名前をアドレスに変換する機能です。 DNS は階層のサービスです。 IP のネーミング協定により各ホスト名は "." の記号で区切られています。したがって、 ftp.progressive-systems.com は、ftp というホストが Com という大区分のドメインの Progressive-Systems のドメインにあることを示しています。また、ネーム・サーバは各ドメイン内に 1 つ以上存在します。ドメインのネーム・サーバは、ホスト名検索を解決するためのマップを管理しています。ネーム・サーバはこれらのマップを使用し、ドメイン内のホスト名を IP アドレス に変換します。ネーム・サーバは、ドメイン範囲外の名前またはアドレスを尋ねられた場合、適切な情報を持つネーム・サーバを探すためにコンタクト情報のリストを使用します。

ほとんどのネーム・サーバは、ローカル・クライアントのために外部エンティティの名前およびアドレスを解決し、リモート・クライアントのために内部エンティティの名前およびアドレスを解決する必要があります。

すなわち、一般的にネーム・サーバはクライアントとサーバの両方として動作します。内部ホストに外部ネーム・サーバをクエリさせるには、 Outgoing (外向き) および Queries (クエリ) のチェックボックスを選択します。さらに、 TCP Queries (TCP クエリ) チェックボックスも選択し、Local Servers (ローカル・サーバ) ボックスにアスタリスク (*) 、またはより制限を設けたい場合はローカル・ネーム・サーバのアドレスを入力します。外部ホストに内部ネーム・サーバをクエリさせるには、 Incoming (内向き) および Queries (クエリ) のチェックボックスを選択します。 Local Servers (ローカル・サーバ) ボックスにはお客様のネーム・サーバを入力してください。さらに、TCP Queries (TCP クエリ) チェックボックスも選択し、 Remote Clients (リモート・クライアント) ボックスにアスタリスク (*) を入力するべきです。これにより、リモート・サイトは TCP および UDP を使用してお客様の DNS サーバをクエリすることができます。

特にご注意ください： Phoenix の以前のバージョン（1.04 以前）は、TCP Queries (TCP クエリ)チェックボックスを “Sec. Dump”、Remote Clients (リモート・クライアント) ボックスを“Remote（for dump）”と表示していました。これらのバージョンでは、Phoenix ファイアウォールは特定のサイトへの DNS セカンダリ・ダンプを制限することを許可しています。しかしこの機能は BIND 8 などいくつかの DNS 機能のインプリメンテーションにより、ファイアウォール・レベルではもはや不要となりました。さらに、過去の Phoenix のバージョンは、TCP クエリの機能をゾーン転送を行うサイトにのみ制限していました。したがって通常の TCP クエリもファイアウォールによってブロックされていた可能性があり、結果特定のクエリが完了することを妨害していました。現在ではインターネット・ネーム・サーバが返すデータ量が増え TCP クエリの利用頻度も増加したことから、過去にはまれにしか発生しなかったこの問題は最近頻繁に起きています。お客様の

ネーム・サーバから、またはネーム・サーバへの TCP クエリを利用可能にするために、Progressive-Systems 社は上述の手順を推奨しています。特定のサイトへのゾーン転送を制限する追加セキュリティ機能をご希望される場合、私どもは BIND 8 および"転送の許可"オプションの構成を推奨します。セカンダリ・ダンプ機能は今後のバージョンで削除されるので、アップグレードされたお客様も同様にこれらの手順に従ってください。

7.4.3 Mail Services (メール・サービス)

SMTP Mail (SMTP メール) ネットワーク管理者は、メールの最も一般的な形式の 1 つである SMTP の、ネットワークへのまたはネットワークからの流れを制御することができます。 SMTP すなわち Simple Mail Transfer Protocol は、 sendmail およびその他多くの一般的なメール・ソフトに使用されている基本プロトコルです。内向きと外向きメールのために別々の制御が提供されています。制御機能は前述の節などで説明したのと同様に動作します。ネットワーク管理者は、 Enable (有効にする) チェックボックスを選択し、ローカルおよびリモートのクライアントとサーバを目的に合うように入力することができます。一般的に内向きメールの Local Clients (ローカル・クライアント) 入力欄はメール・サーバを実行しているマシンの IP アドレスを含みます。Remote Servers (リモート・サーバ) 入力欄はお客様のサイトにメールを送信するマシンの IP アドレスを含みます。
SMTP は tcp 接続用にポート 25 を開きます。

POP Mail (POP メール) POP(Post Office Protocol) とは、クライアント・サーバ型のメールプロトコルです。内向きおよび外向き POP トラフィックのための別々な制御が提供されています。また、 POP-2 および POP-3 プロトコルが選択できる別々なチェックボックスもあります。Incoming (内向き) および Enable (有効にする) チェックボックスが選択されると、指定された Local Servers (ローカル・サーバ) と Remote Clients (リモート・クライアント) の間の内向き POP メッセージが許可されます。 Outgoing (外向き) および Enable (有効にする) チェックボックスが選択されると、指定された Local Clients (ローカル・クライアント) と Remote Servers (リモート・サーバ) の間の外向き POP メッセージが許可されます。
つぎのポート/プロトコルが POP メールで利用可能です：
・Pop-3 のための 110/tcp
・Pop-2 のための 109/tcp

IMAP Mail (IMAP メール) IMAP (Internet Mail Access Protocol) メールは、メールボックスのすべてをダウンロードする前にユーザーにリモート・サーバ上でのメール操作が提供される、クライアント・サーバ型のメール・プロトコルです。内向きおよび外向き

IMAP トラフィックのために別々の制御が提供されています。また、プロトコルのバージョン 2/4 またはバージョン 3 を選択するためのチェックボックスも別々にあります。Incoming (内向き) チェックボックスが選択されると、指定された Local Servers (ローカル・サーバ) に内向きの IMAP Remote Clients (リモート・クライアント) がアクセスすることが許可されます。 Outgoing (外向き) チェックボックスが選択されると、指定された L ocal Clients (ローカル・クライアント) と Remote Servers (リモート・サーバ) の間の外向き IMAP メッセージが許可されます。
つぎのポート/プロトコルが IMAP メールで利用可能です：
・v2/v4 のための 143/tcp
・v3 のための 220/tcp

CCMail P.O. ccMail はファイル・ベースのマルチ・プロトコル・メール・システムです。ワークステーションがローカルのハードディスクに見せかけて cc:Mail サーバのディレクトリを持つことを許可するネットワークは、 ccMail をインストールすることができます。
ccMail は tcp 接続用にポート 3264 を開きます。

CCSO Phonebook CCSO Phonebook は個人およびアカウントの情報を把握するために配布されるデータベース・プロトコルです。
CCSO Phonebook は tcp 接続用にポート 105 を開きます。

7.4.4 Unix

Archie Archie は、ftp を使用しインターネット上のファイルを探すサービスです。Incoming (内向き) および Enable (有効にする) チェックボックスが選択されると、指定された Local Servers (ローカル・サーバ) と Remote Clients (リモート・クライアント) の間の内向き Archie パケットが許可されます。 Outgoing (外向き) および Enable (有効にする) チェックボックスが選択されると、指定された Local Clients (ローカル・クライアント) と Remote Servers (リモート・サーバ) の間の外向き Archie パケットが許可されます。
Archie は udp 接続用にポート 1525 を開きます。

Finger Finger アプリケーションは、システムの任意のユーザーに関する情報を提供するために使用されています。 Whois とは異なり、 finger は登録情報を含むスタティックなデータベースには依存しません。 Finger は特定のユーザーに関する情報を特定のホストに照会します。返される情報には、ユーザーがログインしてからの時間、および現在のユーザーのアイドリング時間のデータが含まれます。*Phoenix Adaptive Firewall (フェニ*

ックス・アダプティブ・ファイアウォール) の finger のオプションでは、 Incoming (内向き) または Outgoing (外向き) finger トラフィックのいずれかが許可または拒否されるファイアウォールの構築が可能です。任意の方向を選択し Enable (有効にする) チェックボックスをクリックしてください。 Incoming (内向き) トラフィックでは、 Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント) の任意のリストを入力します。 Outgoing (外向き) トラフィックでは、 Local Clients (ローカル・クライアント) および Remote Servers (リモート・サーバ) の任意のリストを入力します。 Finger は tcp 接続用にポート 79 を開きます。

Whois Whois アプリケーションにより、ユーザーはユーザー ID およびホスト ID 情報のデータベースを照会することが可能です。国防省を含む多くの米政府団体は whois サーバを管理しています。また、Whois はユーザーおよびホスト情報を特定するために、rs.internic.net にある Internet Registry の照会にも使用されます。
Whois は tcp 接続用にポート 43 を開きます。

UNIX R-コマンド UNIX R-コマンドは、他のホストでのリモート操作を許可するコマンドのセットです。これらは極めて強力ですが、極めて危険でもあり、 UNIX システムの潜在的なセキュリティ障害の 1 つとなっています。特に rexec コマンドは非常に危険です。 rlogin コマンドではユーザーがリモートからマシンにログインすることが許可されています。 rexec および rsh 機能はいずれも、インタラクティブなログイン・セッションを確立しないリモート・システムでのコマンド実行に使用されます。 UNIX R-コマンドを介した未認証の侵入から保護するようにデザインされたシステム・レベルでのセキュリティ対策があっても、誤って構築されているシステムは外部アタックのリスクにさらされることになります。 Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール) のこれらのコマンドのためのオプションでは、ネットワークに入ってくるまたはネットワークを出ていく、あるいは両方のすべての R-コマンド パケットをブロックまたは通過させるファイアウォールを構築できます。rlogin、rsh、または rexec のいずれかとともに Incoming (内向き) チェックボックスが選択されると、 Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント)の入力欄が有効になります。これらの入力欄には IP アドレスを入力することが可能です。 * 記号もワイルドカードとして使用できます。内向き接続については、これらのプロトコルを使用できるサイトが信頼できる場合にのみに限定することを推奨します。
つぎのポート/プロトコルが UNIX R-コマンド で利用可能です：

・rsh のための 512-1023/tcp
・rexec のための 512/tcp
・512-1023/tcp rlogin

・515/tcp printer (lpr)

X11 X11 は、ユーザーにリモート・グラフィック・アクセスを提供するウィンドウ・システムです。不幸にも X11 はリモート・ユーザーにターミナルにいるユーザーと同じ機能を与えてしまいます。 X11 の異なるバージョンのためのオプションは、各チェックボックスをクリックすることにより選択可能です。ユーザーはパケットを内向きまたは外向きのいずれかの方向でフィルタできます。いずれかのアプリケーションのチェックボックスとともに Incoming (内向き) または Outgoing (外向き) が選択されると、関連する Local Programs On(ローカル・プログラムを実行するホスト) および Remote Displays On (リモート・ディスプレイ機能を提供するホスト)、または Local Displays On (ローカル・ディスプレイ機能を提供するホスト) および Remote Programs On (リモート・プログラムを実行するホスト) が有効になります。
つぎのポート/プロトコルが X11 で利用可能です：
・:0.0
・:0.1
・:0.2
・XDM

UUCP UUCP は、 UNIX から UNIX へのコピー・プログラムです。 UUCP プロトコルでは TCP/IP 接続またはダイアルアップ・モデム接続を通じて、ファイル転送、メール転送、およびリモートからのプログラム実行が可能です。制御は News および FTP の節での説明と同様に動作します。 Enable (有効にする) チェックボックスとともに Incoming (内向き) が選択されると、指定された Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント) の間の内向き UUCP トラフィックが許可されます。Enable (有効にする) チェックボックスとともに Outgoing (外向き) が選択されると、指定された Local Clients (ローカル・クライアント) および Remote Servers (リモート・サーバ) の間の外向き UUCP トラフィックが許可されます。
UUCP は tcp 接続用にポート 540 を開きます。

TFTP Trivial File Transfer Protocol は、認証をサポートしない FTP の簡易バージョンです。そのため、TFTP をお客様のネットワーク外で使用することはお奨めできません。しかし TFTP オプションにより、内向きおよび外向き TFTP 接続を安全にすることができます。Incoming (内向き) および Enable (有効にする) チェックボックスが選択されると、指定された Local Servers (ローカル・サーバ) と Remote Clients (リモート・クライアント) の間の内向き TFTP トラフィックが許可されます。Enable (有効にする) チェックボックスとともに Outgoing (外向き) が選択されると、指定された Local Clients (ロー

カル・クライアント) と Remote Servers (リモート・サーバ) の間の外向き TFTP トラフィックが許可されます。
TFTP は udp 接続用にポート 69 を開きます。

Rsync Rsync はネットワークを経由してファイルを送受信するために使用されるプログラムです。
Rsync は tcp 接続用にポート 873 を開きます。

SOCKS SOCKS は TCP アプリケーション・データをプロキシします。ファイアウォール内のホストで SOCKS ベースのサーバを実行しているか、リモートの SOCKS サーバに接続する場合は、このサービスを有効にしてください。
SOCKS は tcp 接続用にポート 1080 を開きます。

CVS CVS (Concurrent Versions Systems) はバージョン管理システムです。
CVS は tcp 接続用にポート 2401 を開きます。

7.4.5 Multimedia (マルチメディア)

Multimedia (マルチメディア) のオプション・ボックスにより、ユーザーは RealAudio および Streamworks からのマルチメディア・パケットを通過またはブロックすることができます。つぎのポート/プロトコルがマルチメディアで利用可能です：
・RealAudio のための 7070/tcp

7.4.6 VPN

Secure Shell Secure Shell は、 UNIX R-コマンドの機能を、より安全なアプリケーションに置き換えるためのインターネット・プロトコルです。 SSH では暗号化および認証などのセキュリティ対策が提供され、ユーザーによる Virtual Private Network (VPN) の構築を支援します。Secure Shell のオプションでは、Incoming (内向き) または Outgoing (外向き) いずれかの SSH トラフィックが許可あるいは拒否されるフィルタの構築が可能です。任意の方向を選択し、Enable (有効にする) チェックボックスをクリックしてください。Incoming (内向き)トラフィックでは、Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント) の任意のリストを入力します。Outgoing (外向き)トラフィックでは、Local Clients (ローカル・クライアント) および Remote Servers (リモート・サーバ)の任意のリストを入力します。
Secure Shell は tcp 接続用にポート 22 を開きます。

IPSec IP Security (IPSec) は、ネットワーク越しのデータ認証および暗号化を提供する

スタンダードです。 IPSec のオプションにより、ユーザーはセキュリティ要件を満たすための ESP (Encrypted Security Payload) および / または AH (Authentication Header) を選択することが可能です。いずれか、または両方のチェックボックスがチェックされると、Local Gateways (ローカル・ゲートウェイ) および Remote Gateways (リモート・ゲートウェイ)と呼ばれるアドレス・ボックスが有効になります。

IKE IKE は Internet Key Exchange を意味します。IP で利用するセキュリティ関係のネゴシエーションのために、このサービスは IPSec と連動して使用されます。
IKE は udp 接続用にポート 500 を開きます。

PPP トンネル PPP トンネルのオプション・ボックスにより、ユーザーはソースおよびデスティネーションのアドレスの間に PPP トンネルを作成することが可能です。tcp および udp パケットはカプセル化され作成されたトンネルを通じて送られます。 PPP トンネルは、 Progressive Systems 社の Morning Star を使用した VPN (Virtual Private Network) を構築する際の追加ステップです。いずれかのアプリケーションのチェックボックスとともに Incoming (内向き) または Outgoing (外向き) が選択されると、関連する Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント) 、または Local Clients (ローカル・クライアント) および Remote Servers (リモート・サーバ) が有効になります。
PPP トンネル は udp 接続用にポート 57 を開きます。

V-One SmartPass V-ONE Smartpass は V-ONE 社の SmartGate VPN 製品のコンポーネントです。このサービスを有効にすると、 SmartPass クライアントは V-ONE SmartGate サーバへの接続が許可され、バーチャル・プライベート・ネットワーク (VPN) を構築できます。

L2TP L2TP は Level-Two Transport Protocol です。
L2TP は tcp 接続用にポート 1701 を開きます。

PPTP PPTP は Point-To-Point Tunneling Protocol を意味します。このサービスは現在実験中の段階にあります！
PPTP は tcp 接続用にポート 1723 を開きます。

7.4.7 Network Management (ネットワーク管理)

LAN Manager (NetBIOS) NetBIOS (Network Basic Input/Output System) は、Microsoft Networking を管理するサービスです。 Lan Management (NetBIOS) のオプ

ション・ボックスでは、ファイル/プリンタ情報およびネーム・サービスを NetBIOS が実行されているマシンから送ることができます。
LAN Manager は udp 接続用にポート 137 を開きます。

Time Services (タイム・サービス) タイム・サービスは NTP (Network Time Protocol)、rdate 、および daytime を含んでいます。ユーザーは NTP により、内部および外部の両方のソースを使用してマシンの時間を設定することが可能です。
つぎのポート/プロトコルがタイム・サービスで利用可能です：
・NTP のための 123/udp
・rdate
・daytime
・timed のための 525/udp
ご注意ください: この注意書きは 1.4 以前のバージョンで生成された古いファイアウォールを使用するユーザーに適用します。NTP は Outgoing (外向き) のメニューに追加され、他のタイム・サービスの位置を 1 つずつ下にずらすことになりました。例えば、以前に rdate を選択していた場合、今は NTP が選択され rdate は選択されません。また、以前のファイアウォールで daytime が選択されていても、現行バージョンは rdate を選択します。外向きの時間選択を必ず見なおし、正確に修正してください。

Ident Ident は、受信ホスト宛てにメールを送信するユーザーのログイン名を送信ホストに照会するプロトコルです。
Ident は tcp 接続用にポート 113 を開きます。

Routing Information (ルーティング情報) 独立したルータおよび IP ルータとして動作しているシステムは、ネットワークとホストの間の利用可能なルートを特定する目的でルーティング情報プロトコルを使用しています。複数のルートが利用可能な場合、ルータは常に変化するネットワークの状態にダイナミックに適応することができます。また、ルーティング情報プロトコルは、ネットワークのトポロジーの様相を特定したり、ホストを誤ったルートのパケットに導いたりしてしまうこともあります。 *Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール)* は、 4 つの一般的なルーティング情報プロトコルのいずれの通過もブロックできるファイアウォールの構築が可能です。つぎのポート/プロトコルがルーティング情報で利用可能です：
・BGP のための 179/tcp

Syslog ユーザーはネットワーク上のマシンおよびデバイスによって生成されたメッセージを Syslog でロギングすることができます。しかし、 Syslog をメッセージで溢れさせ

ることは、侵入者のアタックの一般的な方法として知られています。メッセージでいったん満杯になると Syslog サーバのディスク・スペースにはそれ以上記録されません。つまり、侵入者にアタックされても証拠は残らないのです。

SNMP SNMP (Simple Network Management Protocol) により、ユーザーはルータ、ハブ、サーバその他の機器を管理することが可能です。 Enable (有効にする) チェックボックスとともに Incoming (内向き) が選択されると、指定された Local Servers (ローカル・サーバ) と Remote Clients (リモート・クライアント) の間の内向き SNMP トラフィックが許可されます。 Enable (有効にする) チェックボックスとともに Outgoing (外向き) が選択されると、指定された Local Clients (ローカル・クライアント) と Remote Servers (リモート・サーバ) の間の外向き SNMP トラフィックが許可されます。
SNMP は udp 接続用にポート 161 を開きます。

LDAP LDAP は Lightweight Directory Access Protocol です。
LDAP は tcp 接続用にポート 389 を開きます。

RADIUS RADIUS (Remote Authentication Dial In User Service) サーバはユーザー認証および認可サービスを提供します。また、 RADIUS はクライアントへアカウンティング情報を送信できます。 RADIUS プロトコルはポート 1812 の UDP パケットを使用し、 RADIUS アカウンティングはポート 1813 の UDP パケットを使用します。

TACACS TACACS は Terminal Access Controller Access Control System を意味します。 TACACS はルータまたはアクセス・サーバへアクセスしようとするユーザーにユーザー認証機能を提供します。
TACACS は udp 接続用にポート 49 を開きます。

Ping and Traceroute (Ping および Traceroute) Ping および Traceroute は、 ICMP (Internet Control Message Protocol) を使用するアプリケーションです。 Ping はホストが到達可能であるかどうか、またはパケットがそのホストへ到達するまでにかかる時間の情報をユーザーに与えます。 Traceroute はホストが到達不可能かどうかをテストし、さらにホストに到達するために使用するルートの情報も与えます。

ICMP ICMP (Internet Control Message Protocol) メッセージは、サービスの可用性や、データの送信レートをホストマシンに落としてほしいという受信側マシンのリクエストや、ルートを変更してほしいというリクエストなどのネットワーク状態情報をユーザーに提供します。 ICMP のオプション・ボックスでは、これらの ICMP メッセージは 3 つのカテ

ゴリに分割されています；エラー、情報リクエスト、およびリダイレクトです。いずれかのアプリケーションのチェックボックスとともに Incoming (内向き) または Outgoing (外向き) が選択されると、関連する Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント) 、または Local Clients (ローカル・クライアント) および Remote Servers (リモート・サーバ) が有効になります。

7.4.8 Remote Management (リモート管理)

リモートの、およびリモートで Phoenix ファイアウォールを管理するには Secure Management System を有効にしてください。ファイアウォールがインストールされているインターフェースを経由してファイアウォールを管理する場合、このサービスの構成は必須です。そうでなければ、アクティブなファイアウォールは Phoenix の管理を禁止します。

ファイアウォールを経由して Secure Management System を利用したい場合、ファイアウォールがインストールされているホストへの内向きパケットを有効にします。Phoenix ファイアウォールをリモートから構成する場合で現在のサイトからリモートの Secure Management System を使用したいときは、ファイアウォールがインストールされているホストへの外向きパケットを有効にしてください。

Secure Management System が使用するポートは 8181 および 2005 の 2 つです。

7.4.9 Log (ログ)

Log (ログ)・オプション・ボックスは、システム・ログにどのログを記録するかをユーザーに選択させることを許可します。ユーザーはログに記録する内向きまたは外向きパケットを選択できます。デフォルトの動作はすべての拒否されたパケットを記録しますが、No Reject (拒否パケットをロギングしない)チェックボックスをクリックすればオフにできます。 Start (開始) チェックボックスがチェックされると、ユーザーはパケット・ストリームの初めのパケットのみをロギングします。End (終了)チェックボックスがチェックされると、ユーザーはパケット・ストリームの終わりのパケットをロギングします。これらは “Log Sessions(セッションをログ)”ボックス内の IP アドレスに一致するパケットに関して行われます。 ”All Packets (すべてのパケット)” を選択すると、 ”Log Packets (パケットをログ)”ボックスにリストされているすべての IP アドレスに一致するすべてのパケットをロギングします。アスタリスク (*) を ”Log Packet(パケットをログ)” ボックスに入力すると、すべてのパケットをロギングします。

8 拡張機能

8.1 Custom Protocols (カスタム・プロトコル)

テンプレートのリストに含まれない特定のポートまたはプロトコルのファイアウォール通過を許可したい場合は、カスタム・プロトコルがこれを可能にします。ダイナミックな TCP および UDP ルールの組み合せを用いる複雑なプロトコルを取扱うことはできませんが、カスタム・プロトコルは大半のケースを取扱うことができます。

カスタム・プロトコルはポート番号およびプロトコルのタイプに基いています。つぎのリストは、最も一般的なプロトコル・タイプを紹介しています。

・TCP Session (TCP セッション)
・UDP Session (UDP セッション)
・UDP Query/Response (UDP クエリ/応答)
・UDP Packet Dst Spec (UDP パケット・デスティネーション指定)
・UDP Packet Src Spec (UDP パケット・ソース指定)
・Raw IP Packet (Raw IP パケット)

TCP Session (TCP セッション) Local (ローカル)および Remote(リモート)ボックスで入力されたロケーション間をパケットが伝送される場合、ファイアウォールは指定されたデスティネーション・ポートを含む TCP パケットを通過させます。

UDP Session (UDP セッション) Local(ローカル)および Remote(リモート)ボックスで入力されたロケーション間をパケットが伝送される場合、ファイアウォールは指定されたデスティネーション・ポートを含む UDP パケットを通過させます。ソース・ポートはどのポートでもかまいません。 UDP セッション中、クライアント側のポートが元のソース・ポートでありサーバ側のポートが最初の UDP 応答パケットのソース・ポートである場合に、最初のパケットを通過させた後に続く UDP パケットも通過させます。

UDP Query/Response (UDP クエリ/応答) これは UDP セッションによく似ていますが、ソース・パケットを受信するデスティネーション・ポートは通常 1 つか 2 つのパケットで応答した後、セッションを終了します。

UDP Packet Dst Spec (UDP パケット・デスティネーション指定) ファイアウォールが Local(ローカル)および Remote(リモート)ボックスに指定されたロケーション間で UDP パケットを一方向に通過させることを許可します。デスティネーション・ポートは指定されたものと一致する必要があります。

UDP Packet Src Spec (UDP パケット・ソース指定) ソース・ポートが Port/Protocol (ポート/プロトコル) 入力欄で指定されたものと一致する必要がある以外は上と同じです。

Raw IP Packet (Raw IP パケット) TCP、UDP、または ICMP プロトコルによって定義されていない IP パケットを許可します。このオプションを選択すると、Port/Protcol (ポート/プロトコル) 入力欄はプロトコルが入力されることを期待します。
その他のオプションでは、Port/Protcol (ポート/プロトコル) 入力欄はポートが入力されることを期待しています。

8.1.1 カスタム・プロトコルの構成

Secure Shell は既にテンプレートに存在しますが、お客様はカスタム・プロトコルを使用して SSH を追加したいとします。SSH は TCP を使用し、ポート 22 で実行されます。

1. Add (追加) を押します
2. Incoming (内向き) をチェックします
3. Enable (有効にする) をチェックします
4. プルダウン・リストの TCP Session (TCP セッション) を選択します
5. Port/Protocol (ポート/プロトコル) の入力欄に 22 を入力します
6. Name (名前) の入力欄に SSH を入力します
7. ボックスに Local Servers (ローカル・サーバ) および Remote Clients (リモート・クライアント) のアドレスを入力します
8. OK をクリックします

8.2 Network Address (Port) Translation (ネットワーク・アドレス/ポート変換機能)

お客様のネットワーク上のすべてのマシンにグローバルでユニーク(唯一)な IP アドレスを割り当てることは、特定の状況下では不可能です。その理由はいくつか考えられます：ISP が追加の IP アドレスに対し高額な費用を課す、あるいは、お客様の使用するインターネット接続方法が IP アドレスを 1 つしか割り当てない、などです。ネットワーク・アドレス変換機能 (NAT) を使用すれば、複数のマシンでもインターネット接続は可能になります。
その概念は簡単です：内部ネットワークのマシンには “非公認” の IP アドレスを割り当てます。そして、ISP に接続するファイアウォールまたはルータは、内部マシンの IP アドレスを ISP がお客様に割り当てた IP アドレスに変換します。アドレス変換機能は 2 つの異なるケースに区別されます：

・ネットワーク・アドレス変換機能 (NAT) ： NAT 機能はお客様のネットワークからインターネットへ向けられるパケットの IP アドレスを変換します。お客様は、インターネットに 1 度に接続しなければならないマシンの台数分だけ“正式”な IP アドレスを ISP から取得してください。“正式”な IP アドレスを取得しないと NAT 機能はインターネットから入ってくるパケットをどこに送ればいいのかを判断できません。

・ネットワーク・アドレス/ポート変換機能 (NAPT) ： NAPT 機能はパケットがお客様のネットワークから出る際、IP アドレスおよび TCP/UDP ポート番号の両方を変換します。NAPT 機能は、複数のマシンのトラフィックの処理に複数の “正式” な IP アドレスを必要としません。

Linux オペレーティング・システムは、 *Masquerading (マスカレード)*と呼ばれる制限された形の NAPT 機能をはじめからサポートしています。 Phoenix ファイアウォールのユーザー・インターフェースはマスカレード機能のリモートからの構成をサポートします。

8.2.1 NAT/NAPT 機能の一般的な利用目的

NAT/NAPT 機能の最も一般的な利用目的は、お客様の IP アドレス数を増やさないようにすることです。 NAPT 機能は低コストの ISP からの単独 IP アカウントでホーム・ネットワーク上のすべてのマシンにインターネット接続をさせることができます。 DSL やケーブル・モデムなどの高速なインターネット接続が多くの地域で導入されている現在、NAT/NAPT 機能は非常に魅力的です。

Progressive Systems 社は、 ISP の変更にともなう移行を容易にするマスカレード機能を利用したことがあります。古い (すなわち現在は非公認の) IP アドレスを正式なアドレスに変換する作業に Linux マシンが使用されました。こうすれば余裕を持ってネットワークを移行することが可能であったからです。

お客様が内部ネットワークに“非公認”なアドレスを永続的に割り当てる予定である場合は、IANA がその目的のために確保している IP アドレスを使用することを、私どもは強く推奨します。その範囲については表 6 をご覧ください。

IP アドレス範囲	ネットマスク
10.0.0.0	255.0.0.0
172.16.0.0	255.240.0.0
192.168.0.0	255.255.0.0

表 6：インターネットのプライベート IP アドレス範囲

8.2.2 マスカレード機能

複数のマシンを 1 台に ‘マスカレード(見せかける)’ することが可能という理由から、Linux の NAPT インプリメントは’マスカレード’として知られています。この機能によ

り小規模なホーム・ネットワークは安価なダイアルアップ・アカウントでインターネットに接続することもできます。
マスカレード機能は、変換を行う IP アドレスを 1 つのみ使用します。それは ISP に接続しているインターフェースの IP アドレスです。すなわち、すべてのトラフィックはお客様のルータまたはファイアウォールから来ているように見えます。この機能は中小規模のネットワークを充分に満足させるものです。

ある例を見ていきましょう。著者の 1 人は常に 1Mbit でインターネットに接続するホーム・ネットワークをもっています。内部マシンは 192.168.200.1 から 192.168.200.254 の範囲で IP アドレスが割り当てられます。 ISP によって割り当てられた IP アドレスは 209.33.44.55 です。2 つのイーサネット・インターフェースを持つ Linux マシンは図 17 および表 7 のようにセットアップされました。

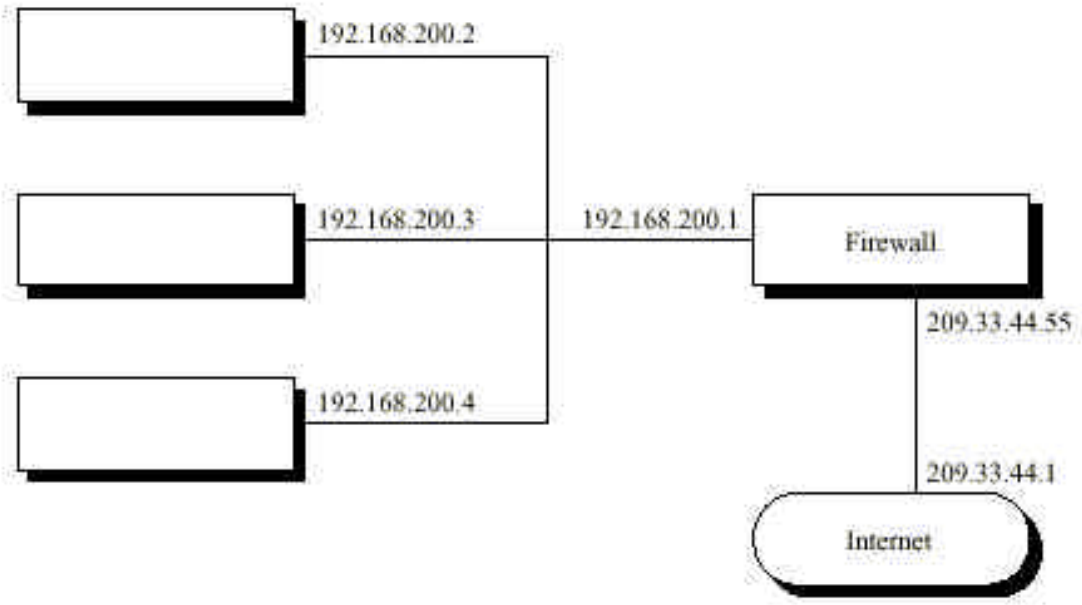


図 18：ネットワーク・ダイアグラム

	IP アドレス	ネットマスク
外部インターフェース (eth1)	209.33.44.55	255.255.255.0
内部インターフェース (eth2)	192.168.200.1	255.255.255.0
ゲートウェイ・アドレス	209.33.44.1	-

表 7：ネットワーク構成

マスカレード機能のルールは、 *eth1* を出て行くすべてのトラフィックがマスカレードさ

れる必要があると指定しています。各内部マシンから来るすべてのトラフィックは 209.33.44.55 という IP アドレスから来ているように見えます。

8.2.3 IP マスカレード機能 (NAPT 機能) の構成

構成前の注意点

Inbound(内向き) パケットはイーサネット・ケーブルから読み込まれマシンに渡されます。**Inbound(内向き)** インターフェースは*パケットを受け入れる*インターフェースです。

Outbound(外向き) パケットはカーネルからイーサネット・ケーブルへ送られるパケットです。**Outbound(外向き)** インターフェースは*パケットを送り出す*インターフェースです。

あるインターフェースで受け入れられ、別のインターフェースで送り出されるパケットは "フォワードされたパケット" と呼ばれます。マスカレード機能はフォワードされたパケットのみに適用します。マスカレードされたパケットとは、ソース・アドレスおよびソース・ポートが書き換えられた **Outbound (外向き)** パケットを指します。

Internal interface(内部インターフェース) は一般的に、内部 LAN につながるインターフェースと考えられています。

External Interface (外部インターフェース) は一般的に、通常 ISP を通じてインターネットにつながるインターフェースと考えられています。

シンタックス

- エントリ・リスト内の名前はアルファベットおよび数字の文字列にしてください
- IP アドレスには 2 つの形式があります：ネットワーク・アドレスまたはホスト・アドレスです。いずれの場合もネットマスクを指定してください
- ホスト名の入力は許可されていません；有効な点区切りの 4 組の数字アドレスのみが受け入れられます
- ホスト・アドレスは個別ホストの IP アドレスです

ホスト・アドレス	ネットマスク	備考
209.41.220.100	255.255.255.255	あるホスト
192.168.212.45	255.255.255.255	別のホスト

表 8 ホスト・アドレスの例

ネットワーク・アドレスは IP アドレスを集めたグループと考えてください

ネットワーク・アドレス	ネットマスク	備考
209.41.220.0	255.255.255.0	クラス C ネットワーク
172.24.0.0	255.255.0.0	クラス B ネットワーク

表 9 ネットワーク・アドレスの例

以下の特別なアドレスには注意が必要です。これはすべてのパケットを指定する際に使用されます。

デフォルトのアドレス	デフォルトのネットマスク	備考
0.0.0.0	0.0.0.0	すべてのパケットを表示

表 10 デフォルトのアドレス

定義

OK/Cancel (OK/キャンセル) "OK" が選択されるまで変更は保存または実行されません。変更をキャンセルするには、 Cancel (キャンセル)を選択してください。

Entries (エントリ) マスカレードするエントリのリストです。エントリはいつでも追加または削除することができます。これらのエントリは他のメニューにあるすべてのエントリから完全に独立しています。

Enable (有効にする) マスカレードするエントリが有効にされると、そのときに選択されたインターフェースに適用されます。無効にされたエントリは適用されませんが、マスカレード機能の構成ファイルに保存されます。

Masquerade/Don't Masquerade (マスカレード機能を実行する/しない) リストされた IP アドレスと一致するすべてのパケットはマスカレードされます （されません)。

Interface (インターフェース) これはマスカレード機能を適用する外向きインターフェースを指定します。Phoenix アプライアンスでは、インターフェースはほとんどの場合、必ず外部インターフェースである eth1 です。ご注意ください：マスカレード機能を動作させるには、選択したインターフェースは外向きパケットが送り出されるインターフェースであるべきです。

Source IP (ソース IP) このアドレスはパケットのソース・アドレスに対して比較され、パケットをマスカレードするかどうかを判断します。

Destination IP (デスティネーション IP) このアドレスはパケットのデスティネーション・アドレスに対して比較され、パケットをマスカレードするかどうかを判断します。

基本的な構成 IP マスカレード機能を構成するダイアログ・ウィンドウは極めて強力です。1 つの画面に多くの情報を詰め込むことで、思いつくほとんどすべての方法でマスカレード機能を構成することができます。初めは複雑に思えますが、時間をかけて本マニュアルをお読みいただければ理解も簡単になるでしょう。
ほとんどの場合、すべての **Outgoing (外向き)** パケットをマスカレードしたいと思われるでしょう。つまり、 LAN から発生しファイアウォールを通じてインターネットへ送り出されるすべてのパケットは、外部インターフェースの IP アドレスによってマスカレードされるべきだということです。その方法は以下のとおりです：

1. 新規エントリを Add (追加) します:
2. “masqall” などの任意の名前をつけてください
3. Enabled (有効にする) を選択します
4. Masquerade (マスカレード機能を実行する) を選択します
5. 外部インターフェース (アプライアンスをご利用の方は eth1) を選択します
6. OK を選択します

ある特定のネットワークをマスカレードしたいと思うときがあるとします。例えば、ファイアウォールの内側に 2 つの内部ネットワークがあるときです： 1 つのネットワークは有効なインターネット・アドレスを使用し、もう一方はプライベート・ネットワーク・アドレスを使用しています （RFC1918)。このうち、プライベートなネットワーク、例えば 192.168.212.0 のアドレスでネットマスクが 255.255.255.0 のネットワークのみをマスカレードしたい場合：

1. 新規エントリを追加します
2. “private_lan” または任意の名前をつけてください
3. Enable (有効にする) を選択します
4. Masquerade (マスカレード機能を実行する) を選択します。
5. Source IP (ソース IP) 入力欄にネットワーク・アドレスを入力します（192.168.212.0 など）
6. 外部インターフェース (アプライアンスをご利用の方は eth1) を選択します
7. OK を選択します

この例ではパケットをそれらのソース・アドレスに基づいてマスカレードしました。パケットはデスティネーション・アドレスに基づいてもマスカレード可能ですし、ソースおよびデスティネーションの両アドレスに基づいてもマスカレードすることができます。

ソース IP およびデスティネーション IP の入力欄は両方埋める必要がないということだけ覚えておいてください。これらの入力欄は、カーネルがパケットをマスカレードするべきかどうかを判断する際に使用する選択条件です。パケットが条件に合った場合、マスカレード機能を実行する/しないの選択に応じて、そのパケットはマスカレードされます(されません)。

構成時にさらに注意する点

先行性　マスカレードおよび非マスカレードの両方のエントリは簡単に多数作成できますのでパケットがマスカレードされるかどうか、ときどき不明瞭な場合があります。
非マスカレードのエントリはマスカレードするエントリよりも*前に*インストールされます。カーネルは最後にインストールされたエントリを使用するので、マスカレードするエントリは非マスカレードのエントリよりも高い優先度を持ちます。
また、非マスカレードおよびマスカレードするエントリのそれぞれのセットの中ではリストは ABC 順にソートされ、エントリは上から下へとインストールされます。

例　すべてのパケットをマスカレードする “masqall” というエントリを作成したとします。そしてさらに、すべてのパケットをマスカレードしない “masqall_not” というエントリも作成したとします。両エントリはまったく同一のパケットに一致するので、カーネルはどうするのでしょう：パケットをマスカレードするのでしょうか、それともしないのでしょうか？
上述の優先順位に従うと、非マスカレードのエントリは先にインストールされ、マスカレードするエントリはその後にインストールされます。マスカレードするエントリが最後にインストールされたので、この例の場合すべてのパケットはマスカレードされます。

簡単な FAQ　Q1) パケットはどのような IP アドレスに書き換えられるのですか？
A1) パケットがマスカレードされない場合は、そのソース・アドレスは変更されません。パケットがマスカレードされる場合は、そのパケットのソース・アドレスはマスカレード・ルールがインストールされたインターフェースの IP アドレスに書き換えられます。
Q2) インターフェースから送り出すパケットに、インターフェースの IP アドレス以外のアドレスを持たせたいのですが、その方法は？
A2) それは不可能です。

8.2.4 ポート・フォワード機能 (NAT 機能)

NAPT 機能(IP マスカレード機能)は、インターネットから内部ネットワーク上のマシンを隠すのに効果的ですが、あるケースでは、インターネットあるいは DMZ ネットワークからの何らの制限されたアクセスを許可したいこともあるかもしれません。**私どもはこれを推奨しません。**インターネットへ向けて利用可能にするサービスが妥協されたものであるならば、Pheonix ファイアウォールがお客様に利益を提供しないことに気が付くでしょう。しかし、私どもはある種の内向きアクセスをセットアップすることに対する良い理由がときどきあることも認めています。Linux の NAT インプリメンテーションは、これらを解決するためのポート・フォワード機能を提供します。

ポート・フォワード機能は、ファイアウォール/ルータを経由して、あるサービスを内部マシンにフォワード(転送)します。例えば、8.2.2 節のホーム・ネットワーク上の内部マシンに対する telnet アクセスを提供したいとしましょう。内部マシンの IP アドレスは 192.168.200.2 です。telnet アクセスを許すには、ファイアウォールに、ファイアウォールの外部インターフェース(すなわち、アドレス 209.33.44.55、ポート 23)から来るすべての TCP 接続を内部マシン(アドレス 192.196.200.2、ポート 23)へフォワードするように指示する必要があります。表 11 に構成例を示します。

ソース IP	ソース・ポート	デスティネーション IP	デスティネーション・ポート
209.33.44.55	23 telnet	192.168.200.2	23 telnet
209.33.44.55	25 smtp	192.168.200.8	25 smtp

表 11：ポート・フォワード構成の例

8.2.5 ポート・フォワード機能 (NAT 機能) の構成

上述のとおり、ポート・フォワード機能はパケットのデスティネーション・アドレスおよびデスティネーション・ポートを新しいアドレスおよびポートに書き換え、パケットを新しいデスティネーションにルーティングします。

シンタックス エントリ・リストの名前はアルファベットおよび数字の文字列にしてください。 IP アドレスは有効な点区切りの 4 組の数字アドレスのみが受け入れられます。

定義

OK/Cancel (OK/キャンセル) “OK” が選択されるまで変更は保存または実行されません。変更をキャンセルするには、Cancel(キャンセル)を選択してください。

Entries (エントリ) ポート・フォワードを行うエントリのリストです。エントリはいつでも追加または削除することができます。これらのエントリは他のメニューにあるすべてのエントリから完全に独立しています。

Enable (有効にする) ポート・フォワードを行うエントリが有効にされると、そのときに選択されたインターフェースに適用されます。無効にされたエントリは適用されませんが、ポート・フォワード機能の構成ファイルに保存されます。

Forward TCP (TCP のフォワード) TCP パケットをフォワードします。

Forward UDP (UDP のフォワード) UDP パケットをフォワードします。

Interface IP (インターフェース IP) 内向きパケットの元のデスティネーション・アドレスおよびポートです。ポート・フォワード機能を動作させるには、選択されるインターフェースは外向きパケットが送り出されるインターフェースであるべきです。

Destination IP (デスティネーション IP) パケットの新しいデスティネーション・アドレスおよびポートです。これはパケットが転送されるアドレスおよびポートです。

例 2 つのイーサネット・ポートを持つ Phoenix アプライアンスをご利用されているとします。そして、内向きトラフィックをネットワーク内の別のホストへフォワードしたいとします。つぎの IP アドレスがあると仮定する場合：

Phoenix – eth1：209.41.220.1
Phoenix – eth0：192.168.212.1
メール・ホスト：192.168.212.55

1. 新規エントリを Add (追加) します
2. “SMTP” または任意の名前をつけてください
3. Enable (有効にする) をチェックします
4. Forward TCP (TCP のフォワード) をチェックします (SMTP トラフィックは TCP のみです)
5. Interface IP (インターフェース IP) の入力欄に 209.41.220.1 を入力します
6. Port (ポート) 入力欄に 25 を入力します
7. Destination IP(デスティネーション IP)の入力欄に 192.168.212.55 を入力します
8. Port (ポート) 入力欄に 25 を入力します
9. OK をクリックします

フォワードされるパケットを異なるポートに送りたい場合、そのデスティネーション・ポートを指定してください。

8.2.6 問題と制限

不幸にも、 NAT および NAPT はいくつかの問題を抱えています。最も重要な問題は、いくつかのプロトコルが NAT 機能を通じて動作するためには補助が必要だということです。この問題の最も一般的な原因は、これらのプロトコルがデータとして IP アドレスおよび TCP/UDP ポート番号を送ることです。この問題を持つ最も一般的なプロトコルは FTP です。 Linux マスカレード機能が提供する、一般的に使用されているプロトコルに対してのヘルプ・モジュールは多いとは言えません。他のプロトコルに至っては、状況はさらに深刻です。独自のプロトコルは特にサポートが困難です。また、電話会議に使用されるプロトコル (Microsoft Net Meeting で使用されるプロトコルなど) にも問題は発生しています。

8.2.7 構成のチェック

構成は SMS の Firewall メニューにある Firewall Status 機能によりダブルチェックできます。IP マスカレードまたは IP ポート・フォワードに何らかの問題があれば、この Firewall Status 機能により警告されます。

ファイアウォール・アプライアンスでは、IP マスカレードまたは IP ポート・フォワード・オプションが SMS の Restore(復帰) 機能を使用してリストアされた場合、その構成を有効にするためにマシンをリブートする必要があります。

8.3 V-One SmartGate の VPN

すべてのアプライアンスは Linux 用 SmartGate サーバがプリ・インストールされ出荷されています。 SmartGate サーバは V-One 社のバーチャル・プライベート・ネットワーク(VPN)・ソリューションです。これは、ローカル・ネットワーク・ファイアウォール内のサービスへの安全な暗号化による接続をリモート・ユーザーに提供します。

出荷時の VPN は管理者を含み 2 ユーザーにライセンス登録されています。追加ライセンスに関するお問い合わせは、Progressive Systems 社の販売代理店までお願いいたします。

8.3.1 SmartGate の各コンポーネント

SmartGate サーバは VPN ユーザーを認証し、ローカル・ネットワークへのリモート・アクセスを管理します。アクセス制御データベースは、指定されたアプリケーション・サービスにどのユーザーがアクセスを許可されるかを定義します。また、アクセス権はグループ・レベルでも定義が可能です。これにより、あるアプリケーションへのアクセスを包括的に制御することができます。

SmartAdmin クライアントはクライアント・マシンで実行されます。管理者はユーザーあるいはグループ、およびそれらに関連するアプリケーションに対する許可/権利を追加、削除、および編集することができます。

SmartPass クライアントはクライアント・マシンで実行され、サーバとの接続を管理します。ユーザー認証およびセッション中に渡されるすべてのデータの暗号化を行います。

8.3.2 V-One SmartGate サーバの構成

SmartGate サーバはアプライアンスには完全にロード済みであり、基本的には自動構成されます。アプライアンスにファイアウォールをインストールしている場合は、VPN フィルタ・テンプレートの SmartPass トラフィックを有効にして動作させます。
Progressive Systems 社から出荷される際、VPN は管理者のほかに追加の 1 ユーザーをサポートする、2 ユーザー・ライセンスがインストールされています。ユーザーおよびクライアント・ソフトウェアの構成手順はつぎの節で詳しく解説しています。

8.3.3 SmartPass および SmartAdmin クライアントのインストールと構成

SmartPass および SmartAdmin クライアントをダウンロードしてください。
ftp://ftp.progressive-systems.com/pub/vpn/
SmartAdmin および SmartPass のすべてのファイルが上記のロケーションにあります。お客様のオペレーティング・システムに適切な各ファイルをダウンロードしてください。

SmartPass クライアントのインストール

1. SmartPass クライアントのインストーラ・ファイルをダウンロードしてください。ファイルは圧縮された zip ファイルです。ファイルの解凍後、セットアップを実行してください。
2. 画面のインストール指示に従って進んでください。後に必要となるので、SmartPass クライアント・ソフトウェアのインストール先のパスを控えておきます。
3. 新しいアクセス・コードを要求されたら、個人のアクセス・コードを入力してください。コードはインストールを完了するために必要となるので控えておきます。
4. マシンの再起動が要求されたら OK をクリックします。
5. リブート後、インストール先の場所から SmartPass クライアントを開始してください。このソフトウェアを初めて開始するときは、ダイアログ・ボックス上でマウスを動かしランダムなデータを作成することを要求されます。これが完了したら手順 3 のアクセス・コードを尋ねられます。
6. つぎに、SmartGate サーバでクライアント・ソフトウェアを登録してください。

SmartGate サーバで SmartPass クライアントを登録する

1. Web ブラウザを開始し、つぎの URL シンタックスを使用して SmartGate サーバのロケーションを入力します：

http://your.smartgate.domain:3845/OLR
この作業はアプライアンスの外部インターフェースから行ってください。SmartGate **サーバは内部ネットワークのクライアントを登録することはありません。**

2. SmartPass **を実行してください**
3. **初めてユーザーを追加する場合は、そのユーザーを管理ユーザーにしてください。フォームを入力し、**First Name(**名前**)**を** SG **、**Last Name(**姓**)**を** ADMIN **にします。これでお客様の** SamrtPass **クライアントは** SmartGate **サーバによって** "SG ADMIN" **として登録されました。クライアントおよびサーバは認証キーのネゴシエーションおよび交換ができるようになります。**
4. **フォームの送信後、お客様は** SmartPass **クライアントの登録が成功したことを通知されます**

管理ユーザーを有効にする

1. SmartGate/Phoenix **アプライアンスのフロント・パネルのボタンを押し、登録したユーザーを有効にします**
2. SmartPass **クライアントを実行してください。生成されるユーザー名は、タスクバー・トレイの** SmartPass **アイコンをダブルクリックすれば表示されます。お客様の** IP **アドレスおよび割り当てられたユーザー名は、左側の** "Network Outbound (**ネットワーク外向き**)" **というウィンドウの下にあります。**
3. SmartAdmin **構成ソフトウェアをインストールするには、まず** SmartAdmin **のインストーラ・ファイルをダウンロードします。このファイルは圧縮された** zip **ファイルです。ファイルを解凍後、セットアップを実行してください。**
4. **画面のインストール指示に従って進んでください。** SmartAdmin **ソフトウェアのインストール先のディレクトリは控えておいてください。インストールが完了したら次の手順に進んでください。**
5. **この時点で、お客様のユーザー名は** SmartGate **の管理者としてセットアップされました。** SmartAdmin **ソフトウェアを開始してください。**
6. SmartAdmin **ソフトウェアの開始後、** SmartAdmin **サーバの選択を要求されます。サーバ名、サーバ・ポート**(3900)**、およびローカル・ポート**(2080) **を入力してください。**

2 人目以降のユーザーを有効にする

1. **最初の管理者が登録されたクライアントと同じマシンから** 2 **人目以降のユーザーも登録することはお奨めしません。** SmartGate **サーバは** 1 **つのクライアントから** 1 **人のユーザー登録のみを受け付けます。同じクライアントからの** 2 **人目以降のユーザー登録が前の登録を上書きしてしまうことを認識していただくことは重要です。ここでは、**

2 人目以降のユーザーは異なるクライアントから登録するものと仮定しています。

2. SmartPass クライアントを実行してください。生成されるユーザー名は、タスクバー・トレイの SmartPass アイコンをダブルクリックすれば表示されます。お客様の IP アドレスおよび割り当てられたユーザー名は、左側の“Network Outbound (ネットワーク外向き)”というウィンドウの下にあります。ユーザーは、手順 6 で使用する自分のユーザー名を管理者に通知します。
3. SmartAdmin 構成ソフトウェアをインストールするには、まず SmartAdmin のインストーラ・ファイルをダウンロードします。このファイルは圧縮された zip ファイルです。ファイルを解凍後、セットアップを実行します。
4. 画面のインストール指示に従って進んでください。 SmartAdmin ソフトウェアのインストール先のディレクトリは控えておいてください。インストールが完了したら次の手順に進んでください。
5. 手順 5 から 7 は管理者によって行われます。したがって管理者のマシンで SmartPass および SmartAdmin を開始してください。
6. “Users (ユーザー)” を選択し、その人の ID をダブルクリックして有効にしてください (または “Edit(編集)…” をクリックします)
7. 有効にする (Enable) の横のボックスをチェックし、 OK をクリックします
8. 有効にするユーザーのマシンで、 SmartPass のファイル・メニューの下の 1 番目のアイコンをクリックし、すべてのアクセス権を更新してください。以前のユーザーは SmartPass のリストへ移されているのではなく、無効にされているだけです。
9. SmartAdmin ソフトウェアの開始後、 SmartAdmin サーバの選択を要求されます。サーバ名、サーバ・ポート(3900)、およびローカル・ポート(2080) を入力してください。

SmartGate の構成での注意

すでに（管理者を含む）他のクライアントを登録済みで、クライアントを管理者として有効にしたい場合、フロント・パネルをつぎのように操作してください：

1. 新しい管理者を追加する前に、利用可能な未登録ライセンスが充分にあるかどうかを確認します。
2. 未登録ライセンスがある場合は新しい管理者は追加されます。
3. 未登録ライセンスがない場合は、新しい管理者を追加するためにすべてのユーザーは無効にされます。その場合、”SG ADMIN” などの同じ名前で管理者を登録する必要があります。また、Last Name(姓)の入力欄で Last Name(姓)の後に大きな値の数字を付け加えてください。これは、追加された管理者を有効にする作業は、ユーザーの “SG ADM” という名前に基いて行われ、大きな数値は他のすべての “SG ADMIN” という登録者(もしいれば)に対し、フロント・パネルから有効にするユーザーとしてリストされることを保証するためです。

4. **残りのユーザーの管理は SmartAdmin を使用して管理を行うべきです。新しいクライアントの追加および管理者の作成は SmartAdmin からできますし、初期の管理者のアカウントも削除できます。ご注意ください：初期の管理者アカウントを登録したクライアントからは、そのアカウントの削除を行うことはできません。**

9 トラブル・シューティング

9.1 アクティブなファイアウォールのデバッグ

あるアプリケーションまたはプロトコルがファイアウォールを通過できるか否か定かでない場合、本章に記述されている情報はファイアウォールが予想どおりに動作しているかどうかの判断に役立つはずです。

9.1.1 デバッグ情報の収集

アクティブなファイアウォールのログ・セクションで定義された設定は、ファイアウォールによってロギングされるパケットのタイプを決定します。デフォルトでは、ファイアウォールにブロックされたすべてのパケットがロギングされます。また、パケットはセッション単位でロギングできます。さらに、パケットはすべてロギングする、またはすべてロギングしないことも可能です。利用可能な設定の詳細に関しては、ログ・アプリケーションのウィンドウをご覧ください。

お客様は拒否されたパケットがロギングされていることを確認したいことでしょう。それが確認できないかぎり、ファイアウォール・ファイルの有効性を保証するデータはどこにもありません。これらの情報は /var/log/phoenix.log にロギングされます。これは GUI からも表示可能です。また、つぎのコマンドを使用すれば情報をキャプチャすることができます：

```
cat /proc/net/phoenix_log | tee <filename>
```

<filename> はロギングを保存したいファイルへの完全なパスです。ロギング・データを収集中に表示したくない場合、コマンドの末尾に "> /dev/null" を付け加えてください。これにより cat の出力データはお客様の端末のウィンドウではなく、/dev/null に送られます。

9.1.2 Phoenix ログ・ファイルの解説

以下は /var/log/phoenix.log からの一般的なエントリの例です。

1/2-15:55:36 eth1::tcp 209.41.220.250/13223<-209.186.246.198/3765 48 syn !pass (769)

上の例のログは、エントリの各フィールドを分割するとつぎのようになります：

1/2-15:55:36	エントリが作成された日次を示すタイムスタンプ
eth1::	フィルタされているインターフェースを示します
tcp	使用されたプロトコルを示します
209.41.220.250/13223	ローカル・マシンの IP アドレスおよびポート番号を示します
<-	トラフィックの方向を示します
209.186.246.198/3765	リモート・ホストの IP アドレスおよびポート番号を示します
48	伝送されたパケットのサイズをバイトで示します
syn	パケットのビット設定を示します。この例では ”syn” ビットは tcp セッションのリクエストを示します
!pass	パケットのアクセスが拒否され、ファイアウォールでブロックされた (通過がブロックされた) ことを示します
(769)	トリガされたルールがあるファイアウォール・ファイルの位置を行数で示します

以上をふまえると、次の 2 つのエントリ例はホスト 209.243.40.33 からローカル・ホスト 209.41.220.250 に向けられた ping のリクエスト (8/0/icmp) であるということがわかります。これらは現在のファイアウォールの 748 行目のルール ((748)) によってファイアウォールの通過を拒否 (!pass) されました。パケットは 1500 バイトの長さでした。

1/2-15:20:25 eth1:: 8/0/icmp 209.41.220.250<-207.243.40.32 1500 !pass (748)
1/2-15:20:26 eth1:: 8/0/icmp 209.41.220.250<-207.243.40.32 1500 !pass (748)

以下は最初に見た行です。この行は、ホスト 209.186.246.198 がポート 3765 からファイアウォール内のホスト 209.41.220.250 （リクエストは受信側のポート番号 13223 に向けられています）に tcp セッションをリクエストしたことを示しています。このリクエストはファイアウォール・ファイルの 769 行目 ((769)) にあるルールセットによって拒否 (!pass) されています。

1/2-15:55:36 eth1:: tcp 209.41.220.250/13223<-209.186.246.198/3765 48 syn !pass (769)

最後に、ファイアウォールを通過可能な接続の成功例を紹介します。これらの例は、ローカル・ホスト 209.41.220.250 がローカル・ポート 51435 からリモート・ホスト 152.163.210.84 のポート 80 へ tcp セッションのリクエスト (syn) を送っていることを示しています。このセッションはファイアウォール・ファイル 385 行目 (385) のルールセットによって許可されています。受信ポートが 80 なので、これは Web リクエストだということが予想できます。

1/2-15:55:37 eth1:: tcp 209.41.220.250/61435->137.175.48.16/80 40 syn (385)
1/2-15:55:37 eth1:: tcp 209.41.220.250/61436->137.175.48.16/80 40 syn (385)
1/2-15:55:38 eth1:: tcp 209.41.220.250/61437->137.175.48.16/80 40 syn (385)

10 ファイアウォールの手動構成

10.0.1 ファイアウォール・ファイルの手動管理

ファイアウォールを定義する際、ネットワーク・ベンダは 2 つの一般的な原理を用います。 1 番目は、ファイアウォールの通過を明確に拒否されるサービスのリストをユーザーが定義する "寛容" の原理です。このリストに記載のないすべてのサービスの通過は許可されます。 **Progressive Systems 社ではこの原理を推奨していません。**

2 番目は、特定の認証済みサービスをユーザーが定義する"制限"の原理です。明確にリストされていないすべてのサービスは排除され、それらはファイアウォールの通過を許可されません。この原理は設定時に注意が必要ですが、前者よりも安全な選択と思われます。なぜなら、"寛容"の原理が用いられているファイアウォールは、設定漏れのエラーによるセキュリティの穴を作ってしまうからです。すなわち、"寛容"ファイアウォールでの入力漏れは、漏れたサービスでも本質的にはファイアウォールの通過を許可することを意味します。これに対し、"制限"の原理での漏れは、漏れたサービスが制限される結果に終わります。しかし、漏れたサービスの事実はただちにネットワーク管理者の目にとまるので、通常の漏れはさほどサービスに影響を及ぼすこともなく、ネットワーク・セキュリティが脅かされることはないでしょう。

ファイアウォールを構築する際、ユーザーは内向きパケットがどこで発生したものかを理解することが重要です。パケットはイーサネット接続を通ります。ファイアウォールを説明する際、"送信済み"パケットは Phoenix Firewall サーバによって転送されたものを指します。"受信済み"パケットは Phoenix Firewall サーバによって受信されたものを指します。

10.0.2 ファイアウォール・ファイルで使用される用語

つぎの用語はファイアウォール・ファイルを解説する際に使用されています：

・ルールセット

ルールセットは、ネットワーク・インターフェースを通過するデータ・ストリームのすべてのパケットに適用されるファイアウォール条件のリストです。インターフェースがイーサネットの LAN または Frame Relay ネットワーク上にある場合、ルールセットはそのネットワーク上にあるこのルータのインターフェースの IP アドレスまたはホスト名で前置きする必要があります。さらに、ピアまたはローカル・インターフェースのアドレスにかかわらず、すべてのインターフェースにルールセットを適用するための特別な **default** キーワードが使用可能です。このキーワードがあれば、ユーザーは各インターフェースおよびピア・アドレスに対するユニーク(唯一)なルールセットを作成する必要がなくなります。

・ファイアウォール

ルールセットでルールを構築する際、2 つのファイアウォールのキーワードがあります。それは **pass （通過させる）**と **log （ロギングする）** です。ユーザーは、1 つのルールセット内に複数のファイアウォールのキーワードを指定することができます。例えば、あるファイアウォールは、条件に合うパケットを **pass** し、なおかつ **log** することができます。

・スタンザ

ルールセットがファイアウォールの関連グループとして取り扱われる場合、スタンザはファイアウォール内の個別のルールとなります。各スタンザはキーワード、アドレス、またはスラッシュ区切りの番号のグループによって構成されています。スタンザはそれぞれ新しい行、タブ、またはスペースによって区切られています。以下に明記されている場所以外、スタンザ中の構成要素の順序は重要ではありません。スタンザのシンタックスおよび構築に関しては後に詳しく述べられています。

・キーワード

キーワードは、特別な意味を持つ予約されている用語です。利用可能なキーワードおよびその用法は後に表で解説されています。

10.1 ファイアウォール・ファイルのシンタックスの解説

ファイアウォール・ファイルの構成要素は階層形式で定義されています。つぎの定義の中では、変化するデータを*イタリック*表示で示しています。**太字**はキーワードとして使用される用語で、括弧 [ ] 内の値はオプションのパラメータを示しています。ファイアウォール・ファイルのシンタックスはつぎのとおりです：

<ruleset> = <ruleset-name> <firewall> <firewall> ...

において *<ruleset-name>* **はホスト名、IP アドレス、または default キーワードです。**

ルールセットの 1 行目はファイル内で左揃えにする必要があります (行頭のタブまたはスペースを持たない)。 2 行目以降はルールセットが続くことを示すために字下げ (インデント) します。ルールセットの *<firewall>* 要素のシンタックスはつぎのとおりです：

<firewall> = <firewall-name> <stanza> <stanza> ...

において *<firewall-name>* は **pass** または **log** のいずれかのキーワードです。

ファイアウォール・キーワードの用法に関しては、**10.2** 節をご覧ください。ファイアウォール定義の *<stanza>* の要素のシンタックスは：

<stanza> = <keyword>/<keyword>/...

スタンザで利用可能な多くのキーワードは、後に詳しく述べられています。キーワードの順序は、キーワード定義表に明確に記されていない限りは重要ではありません。

パケットはスタンザと一致するまで、インターフェースのファイアウォールの各スタンザ

と比較されます。一致するスタンザに述べられているアクションがパケットに適用された後、パケットの処理を中断します。したがって、前述のようにファイアウォール内のスタンザの順序は極めて重要です。最も具体的なまたは強制的なスタンザは初めに、そして最も総括的なスタンザは終わりにくるべきです。
各ルールセットはつぎのいずれかで始まります：

- IP アドレス　ルールセットのアクションは、物理的なネットワーク・インターフェースよりも、接続しているホストまたはネットワークにもとづいて定義されます。必要な IP アドレスは点区切りの 4 組の数字で表記されます (192.0.2.1 など)。
- ホスト名
- 特別な **default** キーワード

イーサネット・インターフェースは **ifconfig** コマンドラインで指定されている IP アドレスを使用します。
ファイアウォール・ファイルをある特定のインターフェースにインストールする処理の際、ファイアウォール・コンパイラは順番にルールセット名 (IP アドレス、ホスト名、または **default**) を審査します。そのインターフェースのアドレスと等しくない名前を発見した場合、そのルールセットを無視して処理を続行します。 **default** ルールセットを発見した場合、コンテンツをコンパイルして処理を続行します。そのインターフェース・アドレスと等しいルールセット名を発見した場合、そのルールセットのコンテンツをコンパイルし、ファイアウォール・ファイルの残りは無視され処理を中断します。ルールセットがコンパイルされる際、既存のファイアウォールは新しくコンパイルされたルールセットに含まれるファイアウォールに置き換えられます。したがって、複数の **default** ルールセットを含む各ファイアウォール・ファイルは、後続のルールセットのデフォルト動作を指定しています。処理中にエラーが発生しなかったファイアウォールはインターフェースにインストールされます。

10.2　2 つのファイアウォール

ルールセット内のファイアウォールは、ファイアウォール・サーバによる個々のパケットの取り扱いをつぎのように規制しています：
・**pass** ファイアウォールはすべてのパケットに用いられ、どのパケットにインターフェースの通過を許可するかを定義します。
・**log** ファイアウォールも **pass** ファイアウォールと同様に、すべてのパケットに用いられます。サーバは **log** ファイアウォールの条件を満たす各パケットについては、システム・ログにメッセージを記録します。
サーバはルールセットから除外されたファイアウォールに､デフォルト設定を適用します。ルールセット内の無指定のままになっているファイアウォールは、 **default** ルールセット

の最も新しい定義により設定されます。あらかじめ明確な定義が設定されていないファイアウォールは、すべてへのデフォルトを設定します (内向きおよび外向き両方の**すべての**パケットに合う)。この例外は、もともとすべてのパケットに合わないとデフォルト設定されている `log` ファイアウォールであり、この設定で一致するパケットはありません。
ルールセット内で明確に定義されているファイアウォールはデフォルトの定義を置き換えます。

10.3 ファイアウォール・スタンザのシンタックス

ファイアウォール名の後に続くいくつかのキーワードは*スタンザ*と呼ばれます。スタンザは 1 つ以上の数字、アドレス、またはキーワードで構成され、スラッシュで区切られています。以下に述べられている場合以外、スタンザ内の構成要素の順序は重要ではありません。
スタンザ内の各数字、アドレス、またはキーワードは、そのスタンザに他の修飾子を追加しています。パケットに述べられたアクションを適用するには、スタンザ内のすべての修飾子はパケットと等しい必要があります。すなわちファイアウォールは、パケットと等しいスタンザが見つかるまで各スタンザに対してチェックを行います。ファイアウォールのアクションは、パケットとスタンザが一致した時点で実行され、そのファイアウォールはパケットに対する他のスタンザのチェックを中止します。したがって明らかに、**ルールセット内のスタンザの順序は極めて重要**です。
つぎの特殊文字はファイアウォール構成要素を限定します。パケットが受信される際、または伝送される直前に、そのパケットと等しいものが見つかるまで順番に各スタンザに対して比較されます。そして、ファイアウォール・プロセッサはスタンザで示されているアクションをとります (`pass!stanza` のアクションならば、そのスタンザと等しいパケットをすべて通過させない、など)。つぎに述べられているのは、一般的なパケットを形容するいくつかのキーワードです。

10.3.1 スタンザのシンタックス構成要素

ファイアウォール構成要素はこれらの特殊文字により限定されます：

オペレータ	目的	備考
!	否定	スタンザの初めに使用します。スタンザと等しいパケットはファイアウォールを通過しません。
{	テンプレート開始位置	スタンザの末尾の { } 内に置かれたスタンザはテンプレート定義です。テンプレートのコピーは、パケットが前述のルールと等しい際に挿入されます。各 { } は空白でスタンザと区切る必要があります。
}	テンプレート終了位置	上記参照
/	セパレータ	キーワードを区切ります。
#	コメント	# より右の文字はすべて無視されます。

10.3.2 パケット選択キーワード

パケットが受信される際、または伝送される直前に、そのパケットは等しいものが見つかるまで各スタンザに対して順番に比較されます。つぎにファイアウォール・プロセッサは、スタンザで示されているアクションをとります (**pass!stanza** のアクションなら、そのスタンザと等しいパケットはすべて通過させない、など) 。つぎのいくつかのキーワードは、一般的なパケットを形容するものです：

キーワード	目的	備考
all		すべてのパケットに適用されます。
src	パケットのソース	スタンザ内のすべてのアドレスおよびポートに適用されます。
dst	パケットのデスティネーション	スタンザ内のすべてのアドレスおよびポートに適用されます。
recv	パケットの進行方向	サーバが受け取るパケット。 ”send” とは併用できません。
send	パケットの進行方向	サーバが送り出すパケット。”recv” とは併用できません。
recv	進行方向制御	サーバが受け取った外部ソースからのパケットをマッチングします。
syn	TCP ヘッダ・ビット	SYN ビットがセットされているパケットと ACK ビットがセットされていないパケットとをマッチングします。
estab established	TCP ヘッダ・ビット	SYN ビットがセットされているパケット以外のすべてのパケットと ACK ビットがセットされていないパケットとをマッチングします - 確立済みの接続を示します。
ack	TCP ヘッダ・ビット	TCP ACK ビットがセットされているパケットをマッチングします。
rst	TCP ヘッダ・ビット	TCP ReSeT ビットがセットされているパケットをマッチングします。
fin	TCP ヘッダ・ビット	TCP FIN ビットがセットされているパケットをマッチングします。
frag	フラグメンテーション制御	元々データグラムの一部ではないパケットをマッチングします。
srcport=*value*	ソース・システムの IP ポート	*Value* はポート番号または文字表記のポート名です。
dstport= *value*	デスティネーション・システムの IP ポート	*Value* はポート番号または文字表記のポート名です。
srcaddr= *value*	ソース・システム/ネットワークの IP アドレス	*Value* はホスト名またはアドレスです。アドレスは十六進、点区切りの 4 組の数字、または文字で表記可能です。
dstaddr=*value*	デスティネーション・システム/ネットワークの IP アドレス	*Value* はホスト名またはアドレスです。アドレスは十六進、点区切りの 4 組の数字、または文字で表記可能です。
srcmask=*value*	ソース・ネットワークのネットマスク	*Value* は 有効なネットマスクを十六進、点区切りの 4 組の数字、または文字で表記可能です。
dstmask=*value*	デスティネーション・ネットワークのネットマスク	*Value* は 有効なネットマスクを十六進、点区切りの 4 組の数字、または文字で表記可能です。
ip-opt=*value*	IP オプション	*Value* は IP オプション名または番号です。

10.3.3 IP プロトコル名

キーワード	目的	備考
udp	パケットのプロトコル指定	tcp または icmp のキーワードとは併用できません。
tcp	パケットのプロトコル指定	udp または icmp のキーワードとは併用できません。
icmp	パケットのプロトコル指定	udp または tcp のキーワードとは併用できません。

10.3.4 *ip-opt* の値

キーワード	目的	備考
rr	ルート追跡	ルートを記録します。
ts	タイム・スタンプ	
security		DoD 要件と互換性のある制限コードを取扱う際、およびセキュリティ、コンパートメンテーション、ユーザー・グループを保持するのに使用されます。
lsrr	ルーティング	ソースがルーティング情報を提供します。
satid		
ssrr		
srcrt		
any	ワイルドカード	現在は使用していません。

10.3.5 TCP 特有のキーワード

キーワード	目的	備考
syn	ヘッダ・ビットの組合わせ	SYN がセットされ、ACK がクリアされています。接続リクエストを示します。
ack	ヘッダ・ビット	TCP ACK ヘッダ・ビットがセットされています。
estab		接続リクエスト以外のパケットに使用される仮の値です。syn の逆を示します。
rst	ヘッダ・ビット	TCP RESET ヘッダ・ビットがセットされています。
fin		TCP FIN (接続の終了) ヘッダ・ビットがセットされています。

これらのキーワードは、 TCP セッションのある特定の段階でパケットを選択するのに役立ちます – セットアップ、ストリーム中、および終了時です。 **send** および **recv** のキーワードと組合わせた場合、ファイアウォールの通過が許可されているセッション全体の方向を制御する目的に使用できます。

10.3.6 応答キーワード

pass ファイアウォールの否定スタンザの後に /unreach=*code* が続く場合、サーバはコードのフィールドに *code* が埋め込まれた ICMP デスティネーション到達不能メッセージを、ブロックされたパケットのソース IP アドレスへ送ります。 *code* は文字および数字の両方で指定可能です。 *code* が何も指定されない場合、サーバは最も新しく指定された *code* を送ります。

ブロックされたパケットが TCP セグメントだった場合、指定 *code* にかかわらず、ICMP デスティネーション到達不能メッセージの代わりに TCP RST をソース・アドレスに送ります。これは送信者に、セッションが 1 つだけブロックされたけれども、デスティネーション・ホストとのすべての通信が中断されるのではないことを通知します。

キーワード	目的	備考
net	ICMP コード	デスティネーションのネットワークが到達不能です。
host	ICMP コード	デスティネーションのホストが到達不能です。
prot	ICMP コード	指定のプロトコルがサポートされていません。
protocol	ICMP コード	指定のプロトコルがサポートされていません。
port	ICMP コード	指定のプロトコル (UDP など) でデータグラムを分割できず、送信者に通知可能なプロトコルのメカニズムも持ち合わせていません。
needfrag	ICMP コード	分割が必要なのに分割しないフラグが設定されています。
net-unknown	ICMP コード	デスティネーションのネットワークが不明です。
host-unknown	ICMP コード	デスティネーションのホストが不明です。
net-tos	ICMP コード	指定されたサービス・タイプのデスティネーションのネットワークが到達不能です。
host-tos	ICMP コード	指定されたサービス・タイプのデスティネーションのホストが到達不能です。
prohibited	ICMP コード	管理者によって通信が禁止されています。
precedence	ICMP コード	ホスト順序の違反です。
precedence-cutoff	ICMP コード	結果としてホスト順序が無効になりました。
rst		TCP RST を送ります。

10.3.7 ファイアウォール・アクションのキーワード

キーワード	目的	備考
log		**pass** ファイアウォールのすべてのパケットに適用可能です。1 行のパケット・サマリがログされます。
trace	デバッグ	**pass** または **log** ファイアウォールのすべてのパケットに適用可能です。パケットの十六進表記をロギングします。
rejected		通過を許可されなかったすべてのパケットを指します。 **log** ファイアウォールでのみ指定可能であり、他のキーワードおよび資格との併用はできません。
ftpport	ICMP コード	FTP コマンド・ストリームで PORT コマンドを含む TCP パケットをマッチングします；ネゴシエーションされたポートの値を **save-port** キーワードに保存します。
ftppasv	ICMP コード	FTP コマンド・ストリームで PASV コマンドを含む TCP パケットをマッチングします。

10.3.8 ダイナミックな特殊キーワード

これらのキーワードはダイナミックなトリガ・ルールを構築する際、またはテンプレートがトリガから値を継承する際に特殊な意味を持ちます。

キーワード	目的	備考
ftp227	通過パラメータ	FTP コマンド・ストリームで “227” レスポンスを含む TCP パケットをマッチングします；ネゴシエーションされたポートの値を **saveport** キーワードに保存します。
ntalkport	通過パラメータ	ntalk ランデヴー・ネゴシエーションで UDP パケットをマッチングします；ネゴシエーションされたポートの値を **saveport** キーワードに保存します。
label=*name*	ダイナミック・ルールの特定	後でトリガから、または認証成功時に参照できるように、ダイナミック・ルールに名前をつけます。 10 文字まで設定可能です。
timeout=*value* timeout	ダイナミック・ルールの制御	(TCP ルールで) このダイナミック・ルールの残存秒数
keepalive=*value* keepalive	ダイナミック・ルールの制御	(UDP ルールで) このダイナミック・ルールの残存秒数
max=number	ダイナミック・ルールの制御	ある時間に有効にできるこのタイプのダイナミック・ルールの最大数
trigger=*name*	ダイナミック・ルールの呼出	ファイアウォール・ファイル内の名前付けされたルールを呼び出す際に使用します。
dstport=*parm* dstport=*value*	通過パラメータ	パケットのデスティネーション・ポートがダイナミック・ルール内の srcport 、 dstport 、または saveport のいずれかと等しい。定数を与えることも可能です。
Srcport=*parm* srcport=*value*	通過パラメータ	パケットのソース・ポートがダイナミック・ルール内の srcport 、dstport 、または saveport のいずれかと等しい。定数を与えることも可能です。

10.3.9 スタンザのシンタックス

一般的なスタンザのフォームはつぎのとおりです：

[!]*address|hostname/[netmask|;number_of_bits][/keyword][/keyword]*

{ template_specification }

正確なシンタックスは、特定のオプションによって異なります。シンタックスはつぎのルールに従う必要があります：

- スタンザ内の構成要素の順序は、上述のキーワード定義に記述されていない限り重要ではありません。
- スタンザ内の値および/またはキーワードはスラッシュ記号 / で区切る必要があります。
- ネットマスクにネットワーク・アドレスがついている際、ネットマスクはネットワーク・アドレスに従う必要があります。
- 空白はスタンザを区切ります。したがって、1 つのスタンザ内での空白の使用は許可されません。
- スタンザ内では 1 つのプロトコルのみ (tcp、udp、icmp) が指定可能です。
- 0-225 の範囲内のすべての番号は、ポート定義の場合以外は IP プロトコル番号として見なされます。その際、プロトコルおよびポートは両方指定されている必要があります。
- IP アドレスおよびネットマスクは前述のとおり、十六進、点区切りの 4 組の数字、または文字表記のいずれかで表示可能です。
- ほとんどのキーワードはその位置に依存しません。ただ 1 つの例外は、ポート番号を使用するときです。ポート番号は、 **tcp** または **udp** のキーワードと一緒に使用される必要があります。同様に、ICMP タイプおよびコード値は、 **icmp** キーワードとの組合わせでのみ使用可能です。
- **syn** 、 **fin** 、 **rst** 、 **ack** 、および **estab** のキーワードは、 **tcp** のキーワードとの組合せでのみ使用可能です。 **tcp** のキーワードは TCP のある特定サービスのキーワードの使用により暗示される場合があります。**Syn** 、**fin** 、**rst** 、**ack** 、または **estab** のキーワードは、いずれか 1 つのみが 1 つのルールに使用可能です。

10.3.10 スタンザの例

```
# 簡単なスタンザです。指定されたホストをブロックします。
!192.168.199.1
# 特定のネットワークを許可します。指定にネットマスクを含めてください。
# 10.7.123.0 から 10.7.123.255 のホストは指定のネットマスクで許可されます。
10.7.123.0/255.255.255.0
# ビット数シンタックスの使用で同じネットワークを指定します。
10.7.123.0;24
# ポート/プロトコルの組合せを指定します。
25/tcp          # SMTP メールを許可
!0-1023/udp     # 特権を持つ UDP ポートをブロック
# icmp キーワードの後の 1 つ目の数字は、 ICMP メッセージ・タイプを示します。
#  icmp キーワードのあとの 2 つ目の数字は、コードの組合せを示します。
!icmp/5         # リダイレクトされた ICMP メッセージをブロック
!icmp/3/0       # 到達不能 ICMP メッセージをブロック
                # "bad net" メッセージ
# 特定のポートおよびアドレスの組合せを定義します。つぎの例は、 10.7.127 と
# 192.168.5 のネットワーク上にあるすべてのホストの間のパケットをブロックする
# ことを示しています。
!srcaddr=10.7.127.0/srcmask=255.255.255.0/dstaddr=192.168.5.0
# 内部ネットワークが 192.168.12.0 であると仮定します。その内部ネットワークから
# であると主張する、外部から受信したすべてのパケットはブロックされます。
!recv/src/192.168.12.0
# 同様に、ネットワークを出ていこうとするすべての内部パケットで、外部のもので
# あってはならないソース・アドレスを持つパケットはブロックされます。
!send/dst/192.168.12.0
```

10.3.11 スタンザの一般的な誤り

インデントには十分注意してください。よくあるエラーは、初めのルールセットの識別子 (ホスト名、 IP アドレス、または **default** キーワード) をインデントしてしまうことです。ファイルでルールセットの識別子が左寄せでない場合、そのルールセットは別のルールセットのスタンザとして見なされます。

同様に、ファイアウォール指定およびルールセット内のすべてのスタンザは必ずインデントしてください。インデントしない場合、それらはアドレスまたはホスト名として解釈されます。

tcp または **udp** のいずれかのプロトコルを使用していると思われるサービスを参照する

場合、 tcp または udp のキーワードの指定には注意してください。例えば、ドメイン・ネーム・サービス (DNS) は通常のクエリでは UDP を使用し、ゾーン転送には TCP を使用します。内向きクエリをブロックしたい場合は、サービス名に必ず tcp キーワードを追加する必要があります。

ファイアウォール定義の中で、ローカルで解決できないホスト名は*絶対に*使用しないでください。

もう 1 つの一般的な間違いは、 FTP パケットをファイアウォールしようとする際に発生します。 FTP は実際に 2 つのチャンネルを使用します。 1 つはコマンドに、そして (ftp-data と呼ばれる) 2 つ目のチャンネルはデータ伝送に使用します。ポートは 1 つ目のチャンネルに 1 つダイナミックに割り当てられています。

最後に、外部ネットワークに対してのネットワーク接続を維持するのに必要となるパケットは必ず許可するようにしてください。一部のインターネット・サービス・プロバイダ (ISP) はルーティング・プロトコルの使用を必要とし、ルーティング・パケットが 1 つも見えない場合、 ISP はお客様のリンクを非アクティブとマークします。

11 Phoenix Adaptive Firewall のファイアウォール・ファイルの例

つぎのファイアウォール・ファイルは *Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール)* により構築されたものです。ファイルは読みやすくするために一部のコメントのフィールドを再フォーマットしてあります。また、印刷されるページの制限の関係上、一部の長い行は途中で改行されていますが、ルールは実際に *Phoenix Adaptive Firewall (フェニックス・アダプティブ・ファイアウォール)* から出力したものです。改行された箇所はバック・スラッシュによって示しています。

ファイアウォールに使用されている IP アドレスは、クラス C のプライベート・アドレス 192.168.210.0 からのものです。パブリックのホストである 192.168.210.10 は、4 つのサービスを実行しています： ftp、www、smtp、および DNS です。ファイアウォールはこのホストに接続するため、これらのサービスに内向きトラフィック、ping、および traceroute を許可しています。さらに、ファイアウォールは内向き ICMP エラーでもファイアウォールの通過を許可しています。他のすべての内向きトラフィックは拒否されます。ファイアウォールは、パブリックのホストへまたはホストから、 smtp および DNS トラフィックのみを許可しています。内部ホスト (ホスト A およびホスト B など) は、つぎのいずれかのサービスを利用して、インターネット上のホストに接続することが可能です： ftp、www、telnet、ping、または traceroute です。

このファイアウォールは、インターネットへまたはインターネットからのすべてのトラフィックが通過するマシンのイーサネットのインターフェースにインストールされます。このマシンには最低でも 2 つのインターフェースが存在するため、ファイアウォールはインターネットに “最も近い” インターフェースにインストールされる必要があります。内向きトラフィックはインターネットから受信され、外向きトラフィックはインターネットへ送信されます。

```
## Parseable filter file information for rereading into
## Filter Utilities.
## DO NOT MODIFY THIS FILE BY HAND!
### Generated by MST Filter Builder version 1.0.2a
### Using Template: Easy Mode Template 1.0.12a
###~~~~(Main)
### "Cracking Prevention", 1, 1, 1, 1
### 192.168.210.0;24, 127.0.0.0;8
###~~~
### "Telnet", 0
###~~
### 1
### *
### *
###~~~
### "File Transfer (FTP)", 1
### 192.168.210.10
### *
###~~
### 1
### *
### *
###~~~
### "World Wide Web", 1, 0, 0, 0
### 192.168.210.10
### *
###~~
### 1, 0, 0, 0
### *
### *
###~~~
### "SMTP Mail", 1
### 192.168.210.10
### *
###~~
### 1
```

```
### 192.168.210.10
### *
###~~~
### "Name Service (DNS)", 1, 0
### 192.168.210.10
###~~~
### "Ping / Traceroute", 1, 1
### 192.168.210.10
### *
###~~
### 1, 1
### *
### *
###~~~
### "ICMP", 1, 0, 0
### *
### *
###~~
### 1, 0, 0
###~~~
## End of parseable section ----------——----------
default
pass
#############################################################
# Generic `shut down this host' label
#
label=shutdown
{
timeout=300
!recv/srcaddr
}
#
#############################################################
### Block source-routed packets
!recv/ip-opt=srcrt/unreach=srcfail
### Allow external sites to access and configure
```

```
### phoenix firewall
# Web Connection
recv/tcp/dstport=81
send/tcp/srcport=81
# Server connection
recv/tcp/dstport=2005
send/tcp/srcport=2005
####### the generic tcp session rule ###################
label=tcp-estab
{
keepalive=3600
tcp/estab/srcport/srcaddr/dstport/dstaddr
}
label=rsh-in2
{
send/tcp/syn/dstport=saveport/srcaddr/dstaddr/ ¥
trigger=tcp-estab # /dstport=512-1023
}
label=rsh-in
{
recv/tcp/estab/srcport/dstport/srcaddr/dstaddr/ ¥
rshport/trigger=rsh-in2
tcp/estab/srcport/dstport/srcaddr/dstaddr
}
label=rsh-out2
{
recv/tcp/syn/dstport=saveport/srcaddr/dstaddr/ ¥
trigger=tcp-estab # /dstport=512-1023
}
label=rsh-out
{ send/tcp/estab/srcport/dstport/srcaddr/dstaddr/ ¥
rshport/trigger=rsh-out2
tcp/estab/srcport/dstport/srcaddr/dstaddr
}
### Block Incoming IP-spoofed packets
!recv/srcaddr=192.168.210.0;24
```

```
!recv/srcaddr=127.0.0.0;8
### Block Outgoing IP-spoofed packets
!send/dstaddr=192.168.210.0;24
!send/dstaddr=127.0.0.0;8
# outbound requests to RealAudio(tm) servers
label=realaudio-out
{
keepalive=3600
send/tcp/estab/srcport/srcaddr/dstport/dstaddr/ ¥
realaudioport
{
keepalive
recv/udp/dstport=saveport/srcaddr/dstaddr
}
tcp/estab/srcport/srcaddr/dstport/dstaddr
}
# inbound requests to RealAudio(tm) servers
label=realaudio-in
{
keepalive=3600
recv/tcp/estab/srcport/srcaddr/dstport/dstaddr/ ¥
realaudioport
{
keepalive
send/udp/dstport=saveport/srcaddr/dstaddr
}
tcp/estab/srcport/srcaddr/dstport/dstaddr
}
# an inbound ftp session
label=ftp-in
{
# Allow outbound ftp-data sessions
recv/tcp/estab/srcport/srcaddr/dstport/dstaddr/ftpport
{
## NOTE: this rule requires incoming, non-passive
## ftp's to come from the ftp-data port on your
```

```
## internal ftp server. To remove this restriction,
## remove the "/srcport=ftp-data" from the following
## line:
send/tcp/syn/srcport=20/srcaddr/dstport=ftpport/ ¥
dstaddr/trigger=tcp-estab
}
# Allow inbound PASV data sessions
send/tcp/estab/srcport/srcaddr/dstport/dstaddr/ftp227
{
timeout=30
recv/tcp/syn/srcaddr/dstport=ftpport/dstaddr/ ¥
trigger=tcp-estab
}
tcp/estab/srcport/srcaddr/dstport/dstaddr
} # end of ftp-in
# an outbound ftp session
label=ftp-ps
{
timeout=30
recv/tcp/estab/srcport/srcaddr/dstport/dstaddr/ftp227
{
send/tcp/syn/srcaddr/dstport=ftpport/dstaddr/ ¥
trigger=tcp-estab
}
}
label=ftp-out
{
# Allow inbound ftp-data sessions
send/tcp/estab/srcport/srcaddr/dstport/dstaddr/ftpport
{
recv/tcp/syn/srcaddr/dstport=ftpport/dstaddr/ ¥
trigger=tcp-estab
}
# Allow outbound PASV data sessions
send/tcp/estab/srcport/srcaddr/dstport/dstaddr/ ¥
ftppasv/trigger=ftp-ps
```

```
tcp/estab/srcport/srcaddr/dstport/dstaddr
}
### Inbound FTP
# * -> 192.168.210.10
recv/tcp/syn/dstport=21/dstaddr=192.168.210.10/ ¥
trigger=ftp-in
### Inbound WWW
# * -> 192.168.210.10
recv/tcp/syn/dstport=80/dstaddr=192.168.210.10/ ¥
trigger=tcp-estab
### Inbound SMTP
# * -> 192.168.210.10
recv/tcp/syn/dstport=25/dstaddr=192.168.210.10/ ¥
trigger=tcp-estab
# dynamic rule for Inbound talk and ntalk tcp sessions
label=talk-ou3
{
recv/tcp/syn/dstport=saveport/srcaddr/dstaddr/ ¥
trigger=tcp-estab
}
### Outbound TELNET
# * -> *
send/tcp/syn/dstport=23/trigger=tcp-estab
### Outbound FTP
# * -> *
send/tcp/syn/dstport=21/trigger=ftp-out
### Outbound WWW
# * -> *
send/tcp/syn/dstport=80/trigger=tcp-estab
### Outbound SMTP
# 192.168.210.10 -> *
send/tcp/syn/dstport=25/srcaddr=192.168.210.10/ ¥
trigger=tcp-estab
# dynamic rule for Outbound talk and ntalk tcp sessions
label=talk-in3
{
```

```
send/tcp/syn/dstport=saveport/srcaddr/dstaddr/ ¥
trigger=tcp-estab
}
label=ping-in
{ # allow response to inbound ping
keepalive=10
send/0/icmp/srcaddr/dstaddr
recv/8/icmp/srcaddr/dstaddr
}
label=ping-out
{
keepalive=10
recv/0/icmp/srcaddr/dstaddr
send/8/icmp/srcaddr/dstaddr
}
label=trrt-in
{
timeout=60
send/11/icmp/dstaddr
send/3/icmp/srcaddr/dstaddr
}
label=trrt-out
{
timeout=60
recv/11/icmp/dstaddr
recv/3/icmp/srcaddr/dstaddr
}
### Inbound PING
# * -> 192.168.210.10
recv/8/icmp/dstaddr=192.168.210.10/trigger=ping-in
### Outbound PING
# * -> *
send/8/icmp/trigger=ping-out
### Inbound ICMP Errors
recv/3/icmp# * -> *
recv/4/icmp# * -> *
```

```
recv/11/icmp# * -> *
recv/12/icmp# * -> *
### Outbound ICMP Errors
# a generic UDP session
label=udp-sess
{
keepalive=60
udp/srcport/dstport/srcaddr/dstaddr
}
# a generic high-to-high UDP session
label=udp-inhi
{
timeout=30
send/udp/dstport/srcaddr/dstaddr/trigger=udp-sess
}
label=udp-ouhi
{
timeout=30
recv/udp/dstport/srcaddr/dstaddr/trigger=udp-sess
}
# a UDP session Useful for stateless UDP like SNMP
label=udp-shrt
{
keepalive=10
udp/srcport/dstport/srcaddr/dstaddr
}
# handle outgoing *requests* for StreamWorks streams
# (actual stream comes *in*)
label=strm-out
{
keepalive=30
udp/srcport/dstport/srcaddr/dstaddr # control stuff
recv/udp/dstport/srcaddr/dstaddr # data stream
}
# handle incoming *requests* for StreamWorks streams
# (actual stream goes *out*)
```

```
label=strm-in
{
keepalive=30
udp/srcport/dstport/srcaddr/dstaddr # control stuff
send/udp/dstport/srcaddr/dstaddr # data stream
}
# dynamic rule for Archie "sessions"
label=archie
{
keepalive=600
udp/srcport/dstport/srcaddr/dstaddr
}
# dynamic rule for replies to DNS requests
label=dns-resp
{
timeout=120
recv/udp/srcport/dstport/srcaddr/dstaddr
}
label=talk-in
{
timeout=120
send/udp/srcport/dstport/srcaddr/dstaddr/talkport/ ¥
trigger=talk-ou3
send/udp/dstport=517/srcaddr/dstaddr/trigger=talk-out
udp/srcport/dstport/srcaddr/dstaddr
}
label=talk-out
{
timeout=120
recv/udp/srcport/dstport/srcaddr/dstaddr/talkport/ ¥
trigger=talk-in3
recv/udp/dstport=517/srcaddr/dstaddr/trigger=talk-in
udp/srcport/dstport/srcaddr/dstaddr
}
label=ntalk-in
{
```

```
timeout=120
send/udp/srcport/dstport/srcaddr/dstaddr/talkport/ ¥
trigger=talk-ou3
send/udp/dstport=518/srcaddr/dstaddr/trigger=ntalk-ou
udp/srcport/dstport/srcaddr/dstaddr
}
label=ntalk-ou
{
timeout=120
recv/udp/srcport/dstport/srcaddr/dstaddr/talkport/ ¥
trigger=talk-in3
recv/udp/dstport=518/srcaddr/dstaddr/trigger=ntalk-in
udp/srcport/dstport/srcaddr/dstaddr
}
############################################################
### Inbound DNS Queries
# anywhere -> 192.168.210.10
recv/udp/dstport=53/dstaddr=192.168.210.10
### Inbound TRACEROUTE
# * -> 192.168.210.10
recv/udp/dstport=33410-33524/dstaddr=192.168.210.10/ ¥
trigger=trrt-in
### Outbound DNS replies
# 192.168.210.10 -> anywhere
send/udp/srcport=53/srcaddr=192.168.210.10
### Outbound TRACEROUTE
# * -> *
send/udp/dstport=33410-33524/trigger=trrt-out
frag
tcp/estab # So that reloading the filter doesn't
# break all current sessions
############################################################
#
# Block automated scans of our address space
#
# RPC
```

```
!recv/sunrpc/trigger=shutdown/log
# Subnet scan
label=ping-3
{
timeout=2
!recv/8/icmp/srcaddr/dstaddr
!recv/8/icmp/srcaddr/trigger=shutdown/log
}
label=ping-2
{
timeout=2
!recv/8/icmp/srcaddr/dstaddr
!recv/8/icmp/srcaddr/trigger=ping-3
}
label=ping-1
{
timeout=2
!recv/8/icmp/srcaddr/dstaddr
!recv/8/icmp/srcaddr/trigger=ping-2
}
!recv/8/icmp/trigger=ping-1
#
# Block automated scans of TCP ports
#
label=tcp-3
{
timeout=65
!recv/tcp/syn/srcaddr/dstaddr/dstport/ ¥
unreach=prohibited
!recv/tcp/syn/srcaddr/dstaddr/trigger=shutdown/log
}
label=tcp-2
{
timeout=65
!recv/tcp/syn/srcaddr/dstaddr/dstport/ ¥
unreach=prohibited
```

```
!recv/tcp/syn/srcaddr/dstaddr/trigger=tcp-3/ ¥
unreach=prohibited/log
}
label=tcp-1
{
timeout=65
!recv/tcp/syn/srcaddr/dstaddr/dstport/ ¥
unreach=prohibited
!recv/tcp/syn/srcaddr/dstaddr/trigger=tcp-2/ ¥
unreach=prohibited/log
}
!recv/tcp/syn/trigger=tcp-1/unreach=prohibited/log
#
# Block automated scans of UDP ports
#
label=udp-3
{
timeout=65
!recv/udp/srcaddr/dstaddr/dstport/unreach=prohibited
!recv/udp/srcaddr/dstaddr/trigger=shutdown/log
}
label=udp-2
{
timeout=65
!recv/udp/srcaddr/dstaddr/dstport/unreach=prohibited
!recv/udp/srcaddr/dstaddr/trigger=udp-3/ ¥
unreach=prohibited/log
}
label=udp-1
{
timeout=65
!recv/udp/srcaddr/dstaddr/dstport/unreach=prohibited
!recv/udp/srcaddr/dstaddr/trigger=udp-2/ ¥
unreach=prohibited/log
}
# traceroute
```

```
!recv/udp/dstport=33410-33524/unreach=prohibited
# anything else
!recv/udp/trigger=udp-1/unreach=prohibited/log
#############################################################
tcp/rst
!all/unreach=prohibited
log
rejected
```

Phoenix Firewall Appliance/SmartGate に関するお問合わせ

KDD ネットワークシステムズ株式会社
TEL　　03-3347-8383
E-MAIL　security@kdd-ns.co.jp

テクノブレスト株式会社 製品販売部
TEL　　046-259-1458
FAX　　046-259-1459
E-MAIL　sales@technoblest.com

翻訳・編集：　八巻 卓、内山 久子（テクノブレスト株式会社）
発行　　：　中西 俊夫（プログレッシブ・システムズ　日本代表）