ファイアウォール

白崎 博生

((株)インターネットイニシアティブ)

1999 **年** 12 **月** 14 **日**

Internet Week 99 **パシフィコ横浜**

(社)日本ネットワークインフォメーションセンター編

目次

1 概要

この講演では、ファイアウォール登場の背景、役割、得失、およびその構成要素などを紹介します。そして、運用上の注意事項や選定のポイントなども説明します。WWW サーバ、FTP サーバの配置法、暗号技術の応用についても紹介します。ファイアウォールへの攻撃の防御、その限界などについても説明します。

2 ファイアウォール

2.1 なぜファイアウォール

表 1:なぜファイアウォール

- **インターネットの拡大、悪意あるユーザの増加、使用するソフトウェアの増加、多数のホストを守るのは不可能**
- **壁を設けよう → ファイアウォール**
  - **壁の外には数台のホスト**
  - **壁の中は低いセキュリティレベル**
  - **いくつかのサービスは壁を越えられる**

インターネットの拡大に伴いユーザ数が拡大しましたが、その結果、悪意あるユーザも増加しています。また、使用するソフトウェアも増加し、複雑なソフトには一般的にセキュリティホールがあり、設定ミスなども起こしやすいということがあります。さらに、ネットワークの拡大により、ホスト数も増大しましたが専任のコンピュータの管理者が少なく、多数のホストを防御することが不可能になってきています。このような事情から、ネットワークの外部と内部に「壁を設ける」、即ち、「ファイアウォール」を設ける必要性が発生しています。

壁の外にはセキュリティを厳しくした数台のホストを配置し、壁の内側はセキュリティレベルを低くします。そして、いくつかのサービスは壁を越えられるようにする、というものです。

2.2 ファイアウォールの得失

間に壁を設けるため、セキュリティはユーザの利便性を下げることになります。たとえば、メールなどは最低限として使用を許可しますが、ストリーミング系の Real Audio などは利用できない、サポートされないことがあります。しかし、メーカによってはストリーム系の使用を可能にするリリースを提供しています。

セキュリティ、安全はただでは実現できません。次のような関係があります。

セキュリティ × 使いやすさ ＝ 体力 ＋ 気力
セキュリティ × 使いやすさ ＝ お金

ファイアウォールによって安全を手に入れることはできます。しかし、万能のツールではありません。たとえば、内部のダイアルアップのモデムなども適切にガードしておかないと、外部からの攻撃にさらされ、破られることになります。

2.3 ファイアウォールの役割

- 境界防御を実現する

  外部組織からの悪意ある、不正なアクセスを防ぐ、即ち、アクセス制御を実現するものです。内部のユーザやデータが外に出ていくのを制御／監視するようにします。また、ファイアウォールがあると外部から直接アクセスできないので、IP アドレスや OS の種類、使用しているソフトのバージョンなど内部ネットワークの情報・構成を外部から隠蔽し漏洩を防止できます。

- 内部のホストに高いレベルのセキュリティ対策を施さなくてもよい

  すべてのホストに対策を施すのは大変ですが、ファイアウォールを設けると内部のホストでは低いレベルのセキュリティ対策で十分となります。即ち、ネットワークの内側と外側とで異なるセキュリティポリシーを設定できるため、最小限のコストでネットワークを防御することができます。

- ログの記録とレポーティング

  どんな通信がファイアウォールを通過したか、誰が誰にどんなメールを出したかなどを記録し、1 日に 1 回、1 週間に 1 回など、必要なときにレポートを得ることが可能になります。

- プライベートアドレスによるネットワーク運用を実現する

  ファイアウォールによる副次的な効果ですが、グローバル IP アドレスの代わりにプライベート IP アドレスを使用できるため、ネットワークのアドレス空間の有効利用が実現できます。

- ユーザには利用しやすい環境を提供する

  透過型プロキシなどを使用して、ユーザにはファイアウォールの存在を意識させないような利用環境を実現できます。ただし、ストリーム系などは必ずしもこのかぎりではありません。

2.4 ファイアウォールを構成する要素

ファイアウォールを構築するための技術には以下のようなものがあります。以下に簡単に説明します。

表 2:ファイアウォールを構成する要素

■要塞ホスト	**■サーキットゲートウェイ**
■デュアルホームホスト	**■アプリケーションゲートウェイ**
■パケットフィルタリング	**■透過型プロキシ**
■NAT	■IP masquerade

- 要塞ホスト(Bastion Host)

  インターネットから直接アクセスできるホストであり、余分なソフトウェアやサービスは削除します。そして、セキュリティパッチを実施するなどして、厳格なセキュリティを実現します。

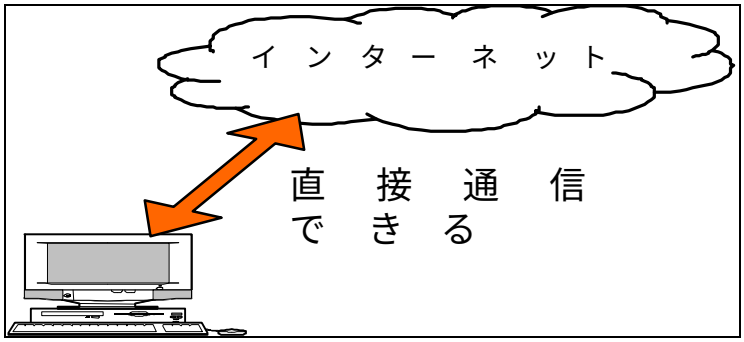

図 1:要塞ホスト

- デュアルホームホスト

  インターネットと内部ネットワークの 2 つのネットワークに接続したホストです(DMZ のように、3 つ以上のネットワークに接続する場合もあります)。IP フォワード機能を停止してファイアウォールにすることもあり、厳格なホストセキュリティが必要です。

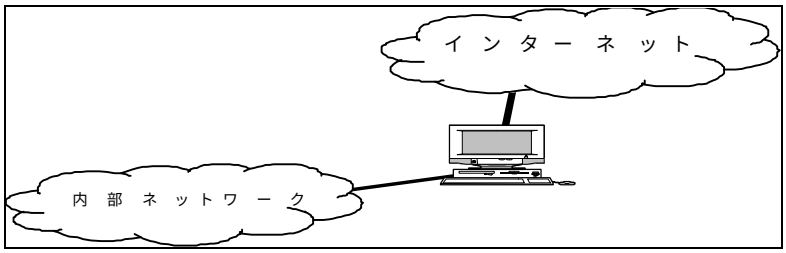

図 2:デュアルホームホスト

- パケットフィルタリング

  パケットレベルでのスクリーニングには、次のものがあります。

  ・アドレス、ポート番号、プロトコル（TCP、UDP、ICMP...）、インタフェース等のスクリーニング

  また、パケットフィルタリングには、以下の 2 つの原則があります

  ・許可したものだけを通す(デフォルトの拒否)

  ・拒否したもの以外を通す(デフォルトの許可)

  一般的には、前者がベターですが、ネットワークのトポロジなどでも異なるためどちらを採用するかはその都度検討が必要になります。

- NAT(Network Address Translation)

  RFC-1631 で定義されています。この背景は IP アドレスの枯渇であり、必要なグローバルアドレスを減少させようとするものです。機能的には、プライベートアドレス空間の発信元アドレスをグローバル空間にマッピングします。この特徴は、ポート番号は変わらず、一次パケットのホスト宛先アドレスだけが変わります。副次的効果として、外部からアクセスしようとしても変換テーブルがないと拒否されるため、内部ネットワークの構造を隠蔽でき、アクセス制御を実現できます。しかし、これはセキュリティ向上のための手段ではありません。また、コネクションの張り方として、内側から外側は可能ですが、外側から内側には張れないのでアプリケーションは制限されます。このようなアプリケーションの場合、FTP の passive モードのような機構が必要となります。

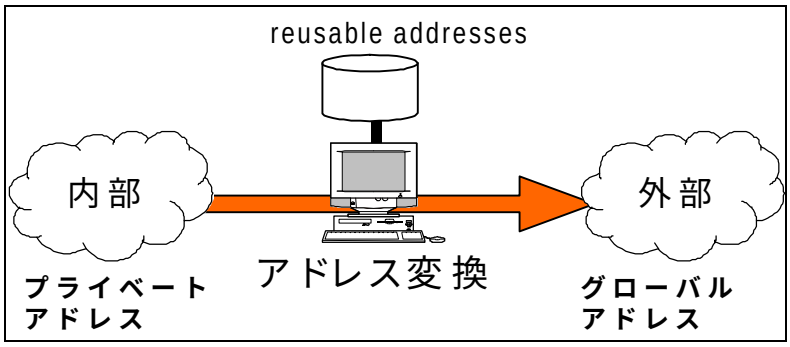

図３：NAT

- IP masquerade （NAPT）

  IP masquerade はポート番号も変換するので、ルータのアドレスだけで運用できます(IP アドレスを 1 つしか消費しません)。しかし、ソースポート番号が 1024 以下でなければならないコマンドやデータ中にポート番号が入っているようなプロトコルは、NAPT がポート番号を書き換えるため、使えなくなることがあります。このような場合は、「このプロトコルの通信はポート番号を変更しない」というルールを設定する必要があります。

- サーキットゲートウェイ

  アプリケーション層でデータを中継し、プロトコルの内容は理解しないプロキシです。socks などの汎用プロキシと呼ばれるものがこれに該当します。

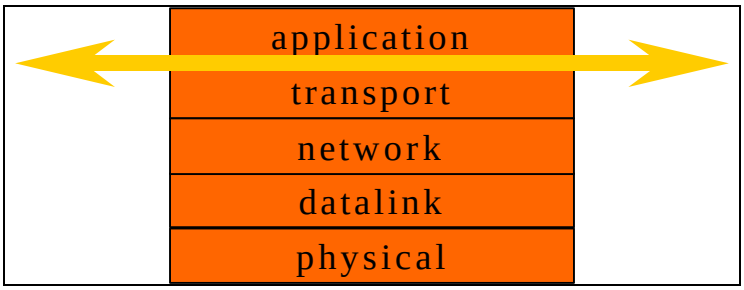

図 4:サーキットゲートウェイ

- アプリケーションゲートウェイ

  アプリケーション層でデータを中継する、プロトコルの内容を理解するプロキシです。通信内容を理解するため、プロトコル内のこのコマンドは中継しないといったアクセス制御が可能になります。また、あるコマンドが使用された場合やプロトコル内のデータのログを取るなどの、監視情報の記録が可能になります。たとえば、SMTP プロキシの場合、誰がどこに何バイト送信したかなどのログが取得できます。ユーザ認証を組み込むことも可能です。

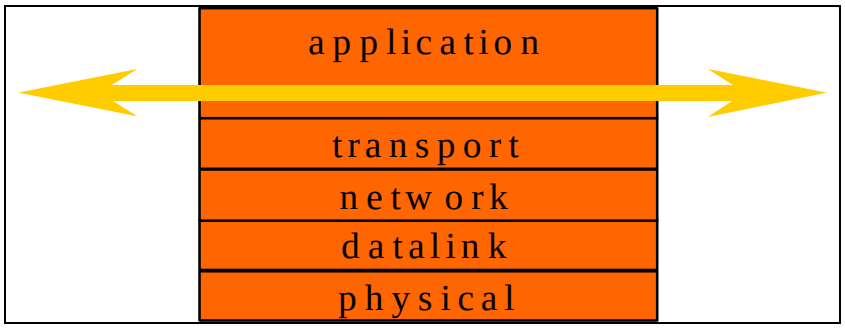

図 5:アプリケーションゲートウェイ

- 透過型プロキシ

  アプリケーションゲートウェイの発展型です。

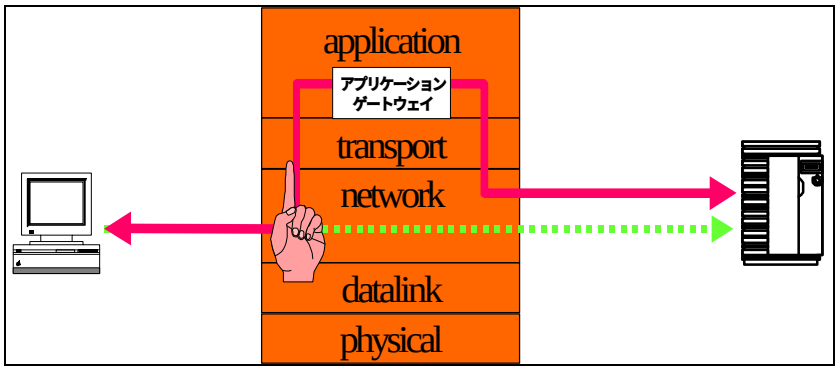

図 6:透過型プロキシ

本来は自分宛てではない宛先アドレスを横取りして、クライアントが相手と直接通信しているように見せるプロキシです。コネクション志向の TCP 接続でのみ対応できます。これは IP masquerade のような効果もありますが、中継しているレベルが異なります。しかし、TCP 接続の特殊状況ではトラブルの原因となることもあります。たとえば、以下の図 7 のように PmathMTU Discovery が動作しないことがあります。

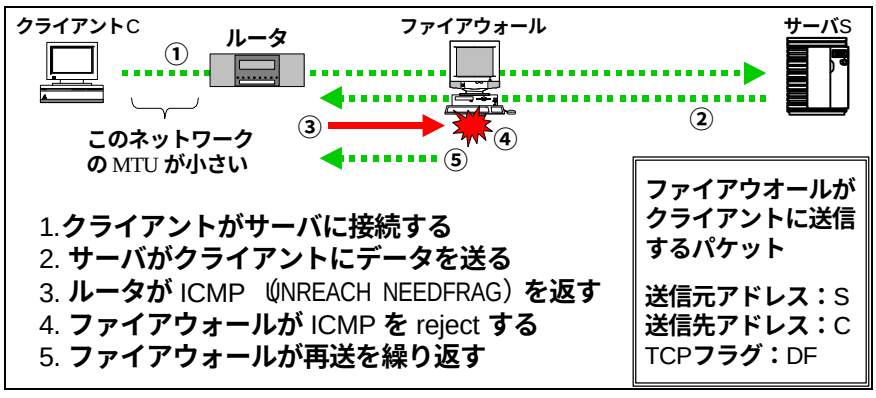

図 7: PmathMTU Discovery が動作しない例

3 ファイアウォールの導入

3.1 導入のポイント

以下の 3 つのポイントがあります。

- セキュリティポリシーを策定する ― ガイドライン
- 設置場所 ― 重要なポイントであり、ファイアウォールの障害時に運用に支障をきたさないように物理的、論理的な配置場所の検討が必要
- 選定 ― 機能要求を明確にする(商用またはフリーのファイアウォール)

3.2 ファイアウォールのセキュリティポリシー

まず、外部インターネットから内部ネットワークへのアクセスを許可するのかしないのかを決めます。そして、許可する場合には、どのように許可するのか、認証を使用するかなどを決めます。次に、内部から外部へ、外部から内部へ許可するサービス(Web、FTP、メールなど)を選定し、それらのサービスを全ユーザに共通に許可するのかまたはクラス分け、すなわち部署毎に許可するのかなどのアクセス制御を決めます。また、新しいサービスをユーザから要求された場合の審議方法を決めておく必要があります。デフォルトの「許可」なのか「拒否」なのかも決める必要があります。重要なことは、運用と監査に誰が責任を持つのかを決め、万一攻撃を受けたり進入された場合などの連絡体制も問題が起きないように決定しておく必要があります。

3.3 商用ファイアウォール

- 背景

  商用ファイアウォールが登場した背景は、以下のものです。

  - コンピュータが専門ではないユーザの増加
  - 攻撃手法の高度化
  - インターネット上のサービスの複雑化
  - 手作りファイアウォールはコストがかかりすぎ(構築、アップデート、安全性の検証のためのコスト)

通常は、トータルで売り物になっています。トータルとは、サービスの統合で、コンサルティング、構築、導入前後のトレーニング／セミナー、バージョンアップのアップデート、監視代行、運用代行（アウトソーシング）などが含まれています。今後は、管理しきれない、セキュリティアラートの増加傾向などから運用の代行が増えると思われます。また、低価格、低機能、低サポートのオールインワン型のファイアウォールも増えると思われます。

- 商用ファイアウォールの種類

  「ハイブリッド型ファイアウォール」と「オールインワン型ファイアウォール」があります。前者は、複数の技術を組み合わせた(パケットフィルタリングとアプリケーションゲートウェイなど)高度な高価なもので、後者は、低価格で低機能で、電源を入れるとすぐに使用できる手軽なものです。

- 商用ファイアウォールの例には、以下のものがあります：

  - UNIX ベース：Firewall-1、CyberGuard、Gauntlet、Raptor...
  - Windows NT ベース：Firewall-1、NetGuardian、Gauntlet、Raptor
  - Hardware：PIX、Firebox II、SonicWALL

3.4 フリーファイアウォール

商用ファイアウォールでは高く、セキュリティに予算をかけられるほどの余裕がなく自分で作るユーザ、大学の研究室など技術も時間も人材もあるが予算はないといったユーザに向いています。また、常時接続料金の低価格化(ISDN の IP 接続サービス、ASDL など）から家庭のインターネットの普及に伴い、今後家庭のファイアウォールとしての使用の増加が予想されます。

何故、家庭にファイアウォールが必要かということですが、インターネットに常時接続されるようになると、家庭のマシーンも他の大きなサイトと同様にインターネットから攻撃を受ける可能性が高くなります。その結果、自分のファイルが破壊されたりすることなどはまだしも、他を攻撃するための DoS アタックなどの踏み台にされたり、SPAM の中継に使用されたり、クラッカーのインターネットチャットサーバにされたりする可能性があるからです。これが、家庭の CPU と言えどもファイアウォールが必要な理由です。

フリーファイアウォールの例には、以下のものがあります：

- アプリケーションゲートウェイ

  TIS FWTK: ライセンスが厳しく(お金を取れない、コードを他人に

譲渡できない)、今後の中心ではなくなると思われます。現在は管理もよくありません。

DeleGate: 電総研の方が作成されたものです。日本でのユーザも多く日本語のドキュメントもあります。

SOCKS: NEC の製品です。

- パケットフィルタリング：

IP filter: フリーUNIX にはデフォルトで入っています。

screend、DrawBridge: 現在はあまり使用されていません。

4 ファイアウォールの選定

4.1 選定のポイント

ファイアウォールの選定には、以下のように 3 つのポイントがあります。

- ポイント －1

ユーザのニーズを調査し必要なアプリケーションは使えるか、新しいサービスに対して拡張性はあるか、処理能力は十分かを検討する必要があります。特に会社などの場合には、販売代理店などのサポート体制は大丈夫か、動作環境は PC/Workstation で動作するのか、故障には強いか、そして導入コスト/管理コストなどを考慮する必要があります。

- ポイント －2

同一価格帯の場合は、プロダクトよりサポートが重要です。機能よりもコンセプト、つまり自社のターゲット(大規模なファイアウォールなのか中規模なものかなど)に合っているか、などが重要です。また、新しい機能はうまく動作しないこともありますので、注意が必要です。

- ポイント －3

フリーファイアウォールを構築する場合は、ポリシーとコンセプトを具体的に、明確にする必要があります。ポリシーとは、パケットフィルタリングなのか透過型プロキシで行うなのかなどです。また、コンセプトとは、新しいサービスの導入法などです。ベースとなる OS の選定も重要です。TCP/IP にバグがあると、ここを攻撃されることがあるため OS の堅牢性と安定性が重要になります。また、バ

グのあるソトウェアから侵入されることもありますので、不要なソフトはインストールしないようにします。プログラムの入れ替えが必要な場合もあります。たとえば、named のバッファオーバーフローで多くのサーバが侵入されたケースがあります。たとえば、コンパイラはサーバのコンパイル後やカーネルの再構築後では不要ですので削除した方が無難です。ソフトウェアの調査も重要です。Web ページ、FAQ 、メーリングリストやセキュリティホールの通知なども確認します。

4.2 アプリケーションゲートウェイかパケットフィルタリングか

- 攻撃からの防御

  攻撃からの防御という点では、管理スキルがある場合はどちらでも問題はなく、効果は同じです。しかし、アプリケーションゲートウェイ(AG)、パケットフィルタリング(PF)では防ぎにくい攻撃があります。たとえば、PF では、アプリケーションレイヤのプロトコルのセキュリティは防御できません。SMTP にバグがあったり、これを通すようにしていると攻撃に対応できません。AG では、不正な IP パケットを使用した DoS(Denial-of-Service)サービス攻撃に対応できずサーバがダウンすることがあります。これは PF がないと防御できません。

- 通信のログ

  ログという点では、PF ではコネクションの情報はログに記録できますが、通信内容は記録できません。一方、AG では通信内容などの種々のログが取れます。

- 性能

  PF の方が有利です。

以上のように一長一短のため、予算が許せば、アプリケーションゲートウェイとパケットフィルタリングの両方を使用するのがベターです。

4.3 ファイアウォールと UDP アプリケーション

- UDP をファイアウォールを通すのは危険

  UDP はパケットの偽造が簡単です。かつ、フロー制御がないのでパケットを送り続けて相手の計算機をダウンさせるということがあります。たとえば、「トリノ (trinoo)」と「TFN」という攻撃ツールがあります。トリノは大量の UDP パケットを送り、TFN では様々な Dos パケットを送り続けて相手のコンピュータをダウンさせるツ

ールです。トリノでは、ある侵入先のサーバにマスタを立ち上げ、別の侵入先のサーバにその配下の多数のデーモンを立ちあげます。そして、攻撃者がマスタに telnet などで 1 回攻撃の指示を出します。そうすると、マスタが多数のデーモンに命令を出し、大量の UDP パケットを攻撃相手に送信して攻撃を行ないます。このような UDP を使用した DoS サービスが流行っています。

- マルチメディア系のアプリケーション

  マルチメディア系のアプリケーションが今後一般になってきます。これらのアプリケーションは UDP を使用しています。しかし、これらのアプリケーションの通信を中継する汎用的なプロキシの作成は難しいわけです。しかし、REAL AUDIO では自社のプロトコルに独自のプロキシを作成して対応しています。また、UDP を使用するオプションと TCP を使うオプションを別に設定できるアプリケーションもあります。

  RTSP (Real Time Streamining Protocol)の標準化の動きがあります。これが制定されるとこれに対応したプロキシが作成される可能性があります。

5 WWW、FTP サーバ

5.1 WWW、FTP サーバの配置

- バリアセグメント

  ファイアウォールの外と ISP と接続するルータとの間の部分をバリアセグメントといいます。ルータのパケットフィルタリングとファイアウォールを組み合わせ、FTP サーバであれば FTP パケットだけ通すといったことを行います。公開サーバなどサーバホストにはホストセキュリティ対策を実施し telnet などでファイアウォールと通信します。WWW と FTP は通常は異なるホストで運用します。これは、WWW などの公開サーバは攻撃のターゲットになり易く、WWW サーバが侵入されると FTP サーバの内容が変更され、FTP サーバが侵入されると WWW サーバの内容が書き換えられるといったことが発生する可能性があるからです。

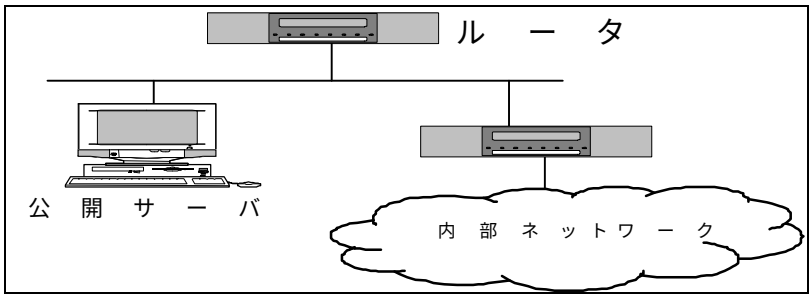

図 6:バリアセグメント

- 第三セグメント（DMZ）

  第三セグメントは、DeMilitarized Zone、または緩衝(非武装)地帯などとも呼ばれます。ここに公開サーバを配置します。しかし、「Redirection proxy の source address」の保存の問題があります。つまり、第三セグメントのサーバはファイアウォールからアクセスされたように見えるため、どこからアクセスされたかの実態が分からないというアクセスログ上の問題があります。DMZ を通すため性能の問題もあります。また、ファイアウォールがダウンすると内部ネットワークを含め公開サーバもすべてが止まるという問題もあります。

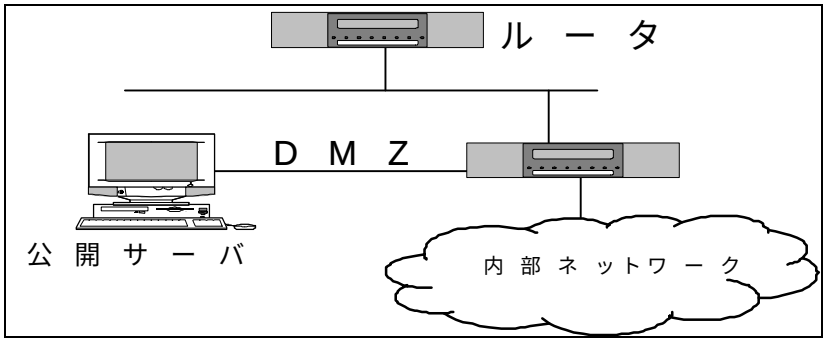

図 7:第三セグメント

さらに、すべての攻撃から防御できるわけではありません。しかし、DMZ を設定すると、ここに第三のセキュリティポリシーを実装できます。第一と第二のポリシーはネットワークの内側と外側のポリシーですが、DMZ には外部ポリシーよりは「緩く」、内部ポリシーよりは「厳しい」、第三のポリシーの実装が可能になり、要塞ホストをここに構築できます。

バリアセグメントと第三セグメントは、どちらも一長一短です。

- 内部セグメント

  ファイアウォールを通した内側のネットワークに公開サーバ、FTP サーバを置くのは避けるべきです。外部と内部という異なるセキュリティポリシーのサーバを 1 つのネットワーク内に混在させるのは危険です。

5.2 運用

- 各サーバは chroot (change root)環境内で稼働させます。
- サーバのコンテンツを管理する方法は以下のとおりです。
  - 内部から telnet や ftp する
  - 内部からシリアル経由でログインする
  - オリジナルを内部で管理し、ミラーする(一日に一回更新など)
  - リムーバブルメディアを利用(CDR、DVD など)
- 内部の DB にアクセスする場合は次のようにします。
  - 専用プロキシ(SQL*Net など）を動作させる。しかし、インターネット側から繰り返し攻撃し、サーバの DB を使用させないという攻撃も考えられる。この場合には、レスポンスを遅くするという仕組みなどを考慮する必要がある。

5.3 リモートアクセスサーバ

外出中の社員などが外部から組織の内部ネットワークにアクセスしたいという要求に答えるための内側のサーバです。この場合には、リモートアクセス用ネットワークは、ファイアウォールの外側に置くか DMZ に置くようにします。そうしないと、ここから侵入されることが多々あります。

war dialer というプログラムなどで、攻撃のターゲットとなるモデムを比較的簡単に探すことができますので、注意が必要です。

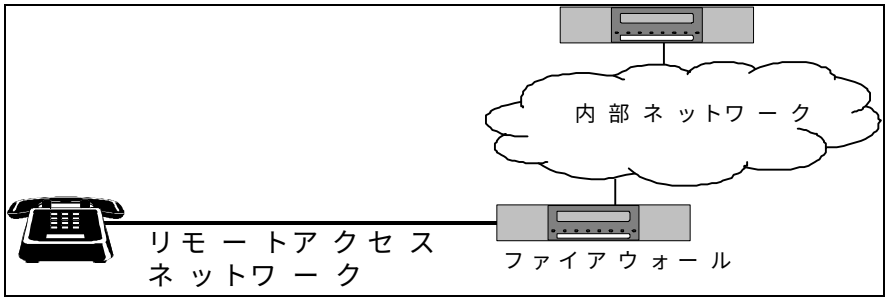

図 8:リモートアクセスサーバ

5.4 IP パケットのフィルタリング

ファイアウォールを構築する場合は、最低限以下のルールを設定してください。

表 3:パケットのフィルタリング

方向	始点アドレス	終点アドレス	プロトコル	始点ポート	終点ポート	アクション	参照
内	自サイトのアドレス	任意	任意	任意	任意	禁止	
両方	プライベートアドレス	任意	任意	任意	任意	禁止	RFC 1597
外	自サイト以外のアドレス	任意	任意	任意	任意	禁止	RFC 2267
内	任意	ブロードキャスト	ICMP	―	―	禁止	CA-98.01

しかし、これだけでは十分ではありません。各サイトで要求されるレベルのパケットフィルタリングも実施する必要があります。

6 バグ、攻撃などへの対応

6.1 Third party relay の対策

対策を実施せず放置していると、SPAM 中継サイトのブラックリストに載ってしまいます。ブラックリストの MAPS RBL、ORBS などに自社のサイトが載ると、これらのリストにあるサイトからのメールは受け付けないというサイトもあります。現在のファイアウォールでは問題ないと思いますが、FWTK の場合などでは対策が必要です。

6.2 アプリケーションのバグへの対応

ファイアウォールのアプリケーションにバグがある場合と公開サーバにバグがある場合の 2 種類があります。いずれもパッチをすぐ当てる必要があります。

- ファイアウォールアプリケーション

  セキュリティパッチをすぐ当てます

- 外部からアクセスされるサーバ(公開サーバ)

  セキュリティパッチをすぐ当てます

- 外部にアクセスするクライアント(IE ,Java、ActiveX など)

  これらのクライアントにより内部が危険にさらされることがあります。たとえば、以前 NCFTP クラインとのバッファオーバーフローでセキュリティが脅かされる可能性がありました(ミラーオプション使用)。

6.3 サービス妨害攻撃への対応

- TCP/IP スタックへの DoS 攻撃

  TCP/IP スタックにバグがあると防御は困難です。よいプロダクト、セキュリティサポートのしっかりしているプロダクトを買うしか方法はありません。

- ネットワーク資源への DoS 攻撃

  一般的に、ファイアウォールでは対応できません。ISP への協力の

依頼が必要です。即ち、あるパケットなどをフィルタリングするようにISPに依頼する方法です。しかし、ISPが個々の要求に対応してくれるかは不確かです。

- アプリケーションへのDoS攻撃

  一般的にファイアウォールで攻撃を防ぐのは困難です。しかし、被害の拡大は防げる可能性はあり、ファイアウォールが全く無意味というわけではありません。

6.4 コンテンツフィルタリング

コンテンツフィルタリングには、以下のものがあります。

- 中継データのコンテンツをフィルタリング

  データの内容を理解する必要があり、賢いアプリケーションゲートウェイ、性能上の問題があります。

- コンピュータウィルスのフィルタリング

  商用製品は実用的なレベルに達しています。

- Java/ActiveX

  現在は完璧ではなく、これからの技術革新に期待したいと思います。

- URLフィルタリング

  問題のホームページにアクセスしないように、FTPプロキシなどを書き換え、コンテンツフィルタリングに対応させるなどの方法です。

6.5 ファイアウォールのリモート管理と二重化

- ファイアウォールのリモート管理

  1台のファイアウォールでは組織を防御できないという事実が今後明らかになってくることから、重要性が今後高まると思われます。

  たとえば、以下のような背景があります。

  ■ 複数のファイアウォールを集中管理する

  ・1つの組織内に複数のファイアウォールを導入

  本社と支店組織内、部署毎のファイアウォール

  ・管理コストの増大

  一貫したセキュリティポリシーを実装、

セキュリティパッチ、アップグレード

■ リモート管理ツールを用いて集中管理

ファイアウォールの数の増加や、ISP、ファイアウォールベンダによるファイアウォールの運用代行の増加に伴いリモート管理の必要性が増加してきます。

製品例としては、Gauntlet Firewall Maganer があります。これで、複数のファイアウォールを管理できます。

- ファイアウォールの二重化には以下のようなものがあります

  - ファイアウォールが停止すると、「自動的に」予備のファイアウォールに切り替わるもの

    VRRP（Virtual Router Redundancy Protocol： RFC2338)を使用している製品には、Firewall-1、Sidewinder があります。

  - ファイアウォールの並列運用

    Alteon ACE Director がありますが、実績などの面で現在の時点では不安があります。

7 暗号技術の応用

- 通信経路の暗号化

インターネットを流れるデータを暗号化して、データの秘匿性、安全性を確保します。2 つのホスト間(ルータ間)でパケットを暗号化してあたかもローカルネットで接続されているように見せる、VPN (Virtual Private Network)があります。最近は、ファイアウォール内に VPN 機能を持つプロダクトが登場しています。

VPN とは、

- ネットワーク間のパケットをカプセル化する
- インターネットを使って、仮想的に専用線で接続したローカルネットワークと同等の環境を構築できる

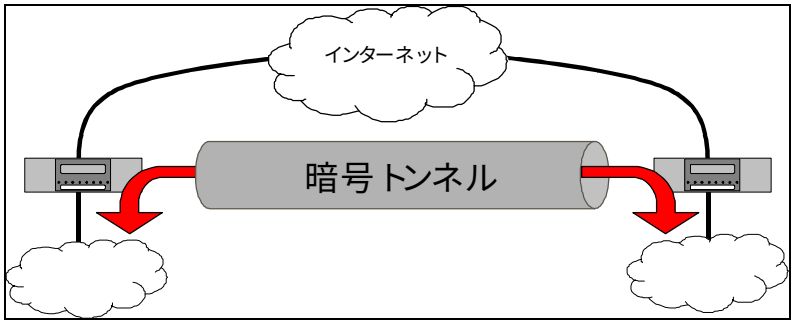

図 9:VPN

- ファイアウォールでの暗号化

  VPN 機能を持つファイアウォール製品には色々あります。

  次のような構成も可能です。この場合は、ファイアウォールをリプレースしても IPsec の VPN はそのまま使用できます。

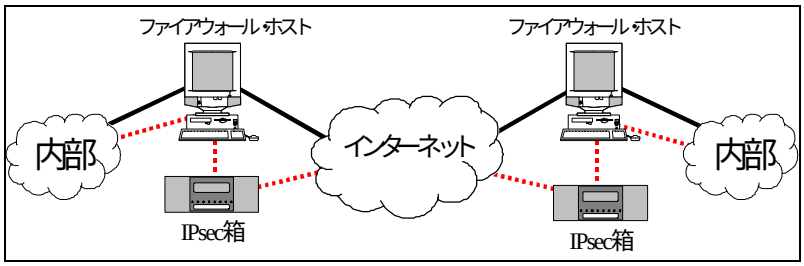

図 10:構成

8 攻撃の防御

8.1 ファイアウォールの限界

- 防げない攻撃もある
  - DoS （Denial of Service）
  - ウィルス
  - 悪意ある Java や ActiveX
  - 悪意あるメッセージ

    INN のコントロールメッセージ（JPCERT-E-INF-97-0002）

- クライアントプログラムのバグ

  Web ブラウザや FTP クライアント、特定の URL にアクセスするとバッファオーバーフローが起きます。

- 攻撃が成功したことを知らせてくれない

  失敗の検出はログなどを利用して容易に行えますが、攻撃成功の検出は難しく、また攻撃されていることを通知してくれるプロダクトはないと思います。このような場合には、IDS (Intrusion Detect System)との併用が必要になります。

- 重要なことは「限界を知る」こと

  ファイアウォールは完全な「解」ではなく、あくまでも 1 つのツールです。

8.2 ファイアウォールへの攻撃

- ファイアウォールのアプリケーションへの攻撃

  ISC の named に対するバッファオーバーフローの攻撃を受けると、被害を受ける可能性があるファイアウォールプロダクトもありました。

- TCP/IP スタックへの攻撃

  DoS や独自実装にバグがある場合もあり、カーネル内で無限ループというバグも発見されています。

- 他組織への攻撃の踏み台として利用

  バリアセグメント上のホストを Amplifier として利用したり、http proxy も狙われやすく、悪用される可能性があります。

8.3 それでもファイアウォール

ファイアウォールを適切に構築すると、攻撃者の行動は大きく制限されます。

このため、複数の異なるコンポーネントを組み合わて使用するとか、フェイルセーフな設計をすることが必要です。

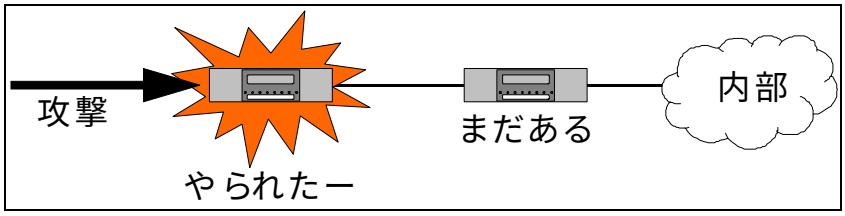

図 11:フェイルセーフな設計

8.4 ユーザ教育

セキュリティ対策の最も重要なポイントが「ユーザ教育」です。ユーザは最大のセキュリティホールです。

しかし、あまり厳しくするとユーザがこっそり穴を作ることがあります。

- ISP にダイアルアップしている内に、そのコネクションから侵入される
- ファイアウォールをすり抜けるツールを仕込む
- 自分のマシンにソフトウェアをインストールする

  ウイルスやトロイの木馬の危険性があります。

ソーシャルエンジニアリングは、海の向こうの話ではありません。