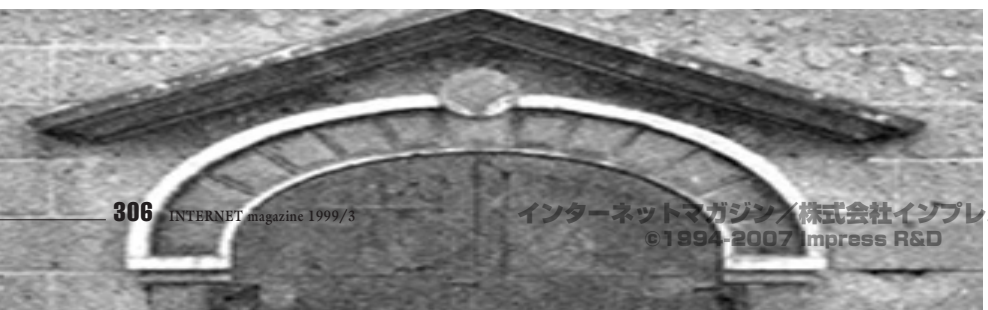
実践 Linux セキュリティー講座

今回はファイアーウォールの基本的な部分を考えてみましょう。まだLinuxに触らないので、がっかりされる方もいらっしゃると思いますが、このような基礎的な技術や知識の蓄積は重要なのです。もし基礎的な知識がないままLinuxの設定を参考に書いてある設定例どおりに行ったとしても、何が正しくて、何が正しくないかの判断ができません。「急がば回れ」のことわざどおり、まずはじっくり足元を固めましょう。

第2回 ファイアーウォールを知る

ソフトウェアコンサルタント　すずきひろのぶ



すでに身近なファイアーウォール

ファイアーウォールという言葉を聞くと、どうしても規模の大きなサイトが行うことであり、小規模サイトには関係がないように聞こえてしまいます。しかし、セキュリティーの本質的な部分においては、サイトの規模は関係ありません。

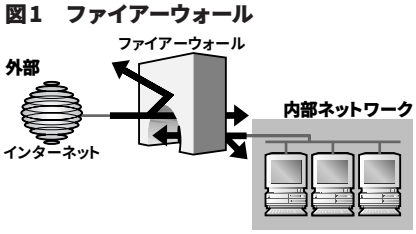
確かに今までファイアーウォールを作るとなると、高価なハードウェアや専用のソフトウェアを購入せざるを得ないという状況にありました。小規模サイトでは金銭的な負担がかかることは大変な問題です。しかし、現在ではこういった問題は過去のことだといえるでしょう。128Kbps～256Kbps程度の回線速度を対象としたファイアーウォールの構築ならば、旧式のPCを再利用することで十分に対応できます。たぶん486DX2程度のCPUでも賄えると思います。

もちろん、そのオペレーティングシステムにはファイアーウォール専用にチューニングしたLinuxを使います。これもわざわざ買い求める必要はありません。本誌1999年1月号付録CD-ROMに入っているRedhat 5.2を用いればいいでしょう。

ファイアーウォールとは何か

今まではファイアーウォールも高嶺の花だったので、「ファイアーウォールという言葉を聞いたことはあるが、その中身についてはよくは知らない」という人も多いのではないでしょうか。そこで確認の意味も含めてファイ

図1　ファイアーウォール



ファイアーウォールは外部から不必要な通信を遮断し、内部から漏れてはいけない情報を遮断する。これによって、外部からの不正な侵入を防ぐ。

アーウォールとは何かを説明します。

ファイアーウォールとは内部の保護されたネットワークとインターネットのような外部のネットワークとの間のアクセスを制御するシステムです。システムといっても1つのルーターだけで構成されている場合もありますし、複数のネットワーク機材やホストから構成されている場合もあります（図1）。

ファイアーウォールの構造

ファイアーウォールと一口にいっても、いろいろな構造が存在します。ここでは典型的な3つの構造を紹介します（図2、図3、図4）。ここから各構造の違いを検討し、どの構造を採用するかという話になるのですが、先に結論から申し上げますと、本連載ではより本格的なスクリーンドサブネット構造を導入します。

残念なことに、以前は機材コスト負担の問題があり、小規模サイトではあまり使われませんでした。

デュアルホームホスト構造

デュアルホームホスト構造の特徴は、デュアルホームホストとなるコンピュータを経由して、内部と外部のパケットの往来を完全に一度は遮断する方法です。

多くの場合、コンピュータに2枚のNIC（ネットワークインターフェイスカード）をインストールし、一方を外部に接続しているIPルーターに、もう一方を内部のネットワークセグメントに接続します。

このほかにもコンピュータのシリアルI/OにISDN TAをつないでPPPでネットワーク接続を行い、NICを内部ネットワーク側に接続する方法は、必要な機材も少なくて済みますし、小規模サイトでは割と一般的な方法だと思います。

もちろん、どちらもLinuxで構築することが可能です。本連載でも2枚のNICを使うことになりますが、この詳細に関しては今後の連載の中で説明していきます。

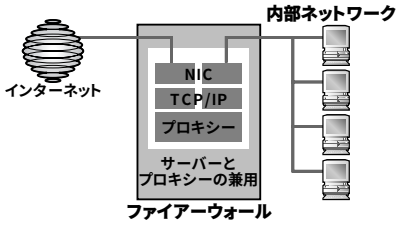
さて、一般的な考え方としてこのホストが置かれたポジションは、インターネット側と内側ネットワークのセグメントを接続させるために（ルーターのように機能させて）ルーティングを行うべき場所です。しかし、このデュアルホームホスト構造では直接は橋渡しをしません。つまりルーティングの機能はありません。

したがって、インターネット側（外部）からのIPパケットは、直接は内部に入ることはありません。しかし、内部からはホストと通信でき、外部からもホストと通信できる状態にする必要があります。

そこで、ホスト上で特定の通信に対してのみフォワードするサービスを提供します。このサービスの典型的なのがHTTPプロキシー（WWWプロキシー）です。内部からホスト上のHTTPプロキシーを経由することによって、外部からは内部のネットワークがどのようになっているかの情報を消すことができます（図5）。

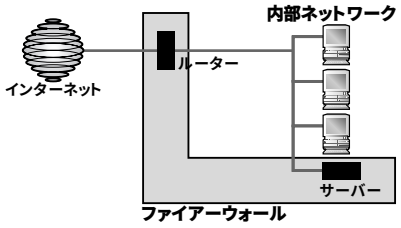
もちろん、このようなプロキシーはHTTPだ

図2　デュアルホームホスト



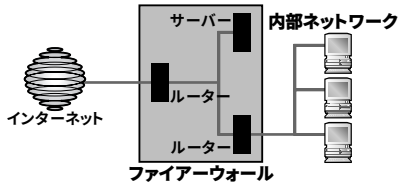
デュアルホームホストは1台のホストコンピュータでプロキシー機能と各種サーバー（WWWや電子メールサーバー）を稼動させる。外部ネットワークと内部ネットワークのルーティングは行わず、プロキシーを経由させて外部と内部のネットワーク通信を可能にする。

図3　スクリーンドホスト



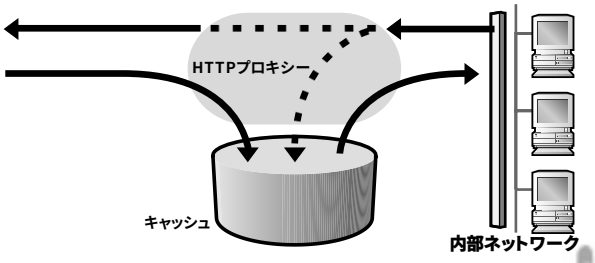
スクリーンドホストはルーター機能とサーバー（WWWや電子メールサーバー）を異なるホストコンピュータ上で稼動させる。ルーターでパケットフィルタリングをすることで、外部から通信できるのはサーバーのみで、内部ネットワークには到達できない。

図4　スクリーンドサブネット



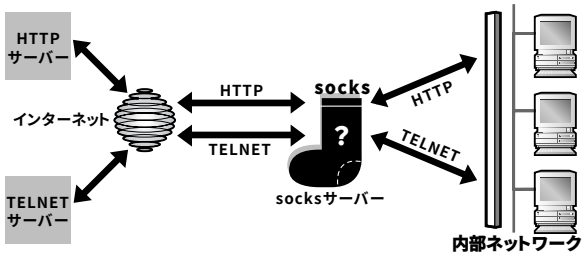
スクリーンドサブネットはスクリーンドホストを拡張したもので、内部ネットワークの直前にルーターを置いて、パケットフィルタリングをしている。つまり、外部ネットワーク用のルーターと内部ネットワーク用のルーターの2つのルーターを用意する。この2つのルーターにはさまれた境界ネットワークをDMZ（非武装地帯）と呼び、外部と通信する各種サーバー（WWWや電子メールサーバー）を置く。

図5　HTTPプロキシーの役割



内部からのアクセスは直接外部に出ることはない。また、すでにHTTPプロキシーがキャッシュしているページであれば外部にすらアクセスしない。

図6　socksのしくみ



socksは単一の通信だけを代理アクセスするものではなく、さまざまな通信の代理をするものだ。たとえば、HTTPやTELNETといった通信ができる。

けではありません。FTPやほかの通信専用のものもあります。特定の通信用プロキシーに対して、通信は限定せずにTCPの接続に対して汎用的にサービスを行うSOCKSのようなプロキシーもあります（図6）。ただし、すべての通信に対してプロキシーの機能が実行できるとは限りません。プロキシーも万能ではない点に注意してください。なお、プロキシーの標準化に関しての情報は次のURLが参考になるでしょう。

URL http://web.ansi.org/public/iisp/std_need/need145.html

このように単純な構造で効果的に見えるデュアルホームホスト構造ですが、最大の難点は何でしょうか？

デュアルホームホスト構造では、少なくともマルチユーザーモードでLinuxを動作させなければなりません。万が一、ホスト上で動かしている各種のサービスにぜい弱性（セキュリティー上のバグ）があったり、設定に問題があったりして、外部からホストをクラックされてrootアカウントの乗っ取りが行われたとしましょう。デュアルホームホスト構造は、このホストだけがセキュリティーの関所として機能します。rootアカウントが乗っ取られるのは、関所が陥落したと同じことですから、ネットワークの防御がまったくできなくなってしまいます。デュアルホームホスト構造にはこのような問題があります。

スクリーンドホスト構造

スクリーンドホスト構造では、まずルーターによりパケットのフィルタリングを行い、外部に公開するのは専用のサーバーだけに限り、それ以外の外部からのIPパケットは一切遮断するという方法です。一方、内部から外部へ接続できる通信は、ごく限られたものにするという方法を採ります。これは小規模サイトにおいて最も一般的なファイアーウォールの構造として用いられているものです。

現在ではダイアルアップルーターやIPルーターのほとんどは、プライベートIPアドレスとグローバルIPアドレスを変換するNAT（IP Network Address Translator）やIPマスカレード（Masquerade：仮装や変装という意味）の機能を持っています。これもまた1つのフィルタリングの役目を果たすことができ、内部のネットワークが直接外部にさらされることを回避できます。このように、始めから用意されている機能を使い、効果的にフィルタリングを行うことができます。

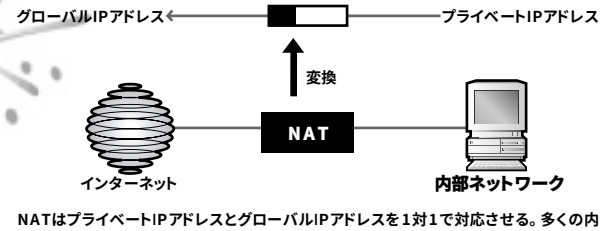
ここで少しNATとIPマスカレードの話をしましょう。NATやIPマスカレードの機能は、枯渇するインターネット上のIPアドレス空間を有効に使おうという視点から、グローバルIPアドレス（インターネット側に割り当てられた、世界で唯一のIPアドレス）とプライベートIPアドレス（閉じたネットワークで自由に付けられるIPアドレス）を変換するというものです。内部のネットワークと外部のネットワークとでやりとりする際に、パケットのIPアドレスなどが変換されるため、副作用として内部のネットワークの状態をおおい隠すことになります。まさにマスカレード（仮面で仮装する）状態になります。

NATは、プライベートIPアドレスとグローバルIPアドレスが「一対一」に対応しています（図7）。一方、プライベートIPアドレスとグローバルIPアドレスが「多対一」に対応しているのが、IPマスカレードです（図8）。ほとんどのサービスの場合、IPマスカレードで十分ですが、ストリーミングコンテンツやネットワークゲームなど今までのTCP/IPネットワークでできていたすべてのサービスに対して、必ずしも有効ではないという問題があります。実際のルーター製品では、NATとIPマスカレードの両方の特徴を備えるハイブリッド化した機能を持たせて解決しています。

このように、すいぶん便利で効果的なスクリーンドホスト構造ですが、欠点があります。それは、外部に公開しているサーバーが万が一クラックされてしまったら、内部ネットワークに自由にアクセスできてしまうことです。サーバーのホストマシン上で、ネットワーク盗聴を行うプログラムを仕掛けられてしまった場合、内部ネットワークのセキュリティーはズタズタになってしまいます。

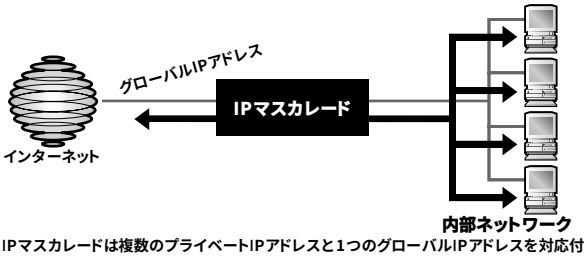
外部からサーバーにログインアクセスを一切させないように、パケットをフィルタリングしてアクセスできるサービスを制限する、また、サーバーから外部へもパケットを送出しないといった制限を加えることによって、かなり強力なサイトセキュリティーを確保できま

図7　NATのしくみ



NATはプライベートIPアドレスとグローバルIPアドレスを1対1で対応させる。多くの内部ネットワークのコンピュータが同時に外部のコンピュータと通信するには、複数のグローバルIPアドレスが必要となる。

図8　IPマスカレードのしくみ



IPマスカレードは複数のプライベートIPアドレスと1つのグローバルIPアドレスを対応付ける。実際には、ポート番号というサブアドレスのようなものを変換して、1対多の通信ができるようにしている。

すが、構造的にはまだ改善の余地があります。

スクリーンドサブネット構造

スクリーンドホスト構造をさらに発展させたものがスクリーンドサブネット構造だといえるでしょう。

先ほど説明したように、外部に公開しているサーバーは当然ながら攻撃を受ける最前線に位置するわけです。これらのホストは徹底してセキュリティーを強化しなければなりません。セキュリティーの専門家はこのようなホストを要塞ホスト（Bastion Host）と呼びます。しかし、物事に完全はありません、常に万が一を考えて二重三重の防御を行います。

スクリーンドサブネット構造では、外部と内部の間にサブネットをはさみ、そこに要塞ホストを用意します。このサブネットをDMZ（De-Militarized Zone：直訳すると非武装地帯）あるいは境界ネットワーク（perimeter network）と呼びます。最悪の場合、要塞ホストが陥落しても、被害が内部ネットワークまで及ぶことを阻止します。

パケットのフィルタリングに関しては、基本的にスクリーンドホストと同じです。ただし、それが外側と内側の二重になります。スクリーンドホストでは、内部からの攻撃はほとんど無防備でしたが、今度はサブネットで区切られますので、内部から境界ネットワーク上にある要塞ホストへのパケットに対してもフィルタリングができます。

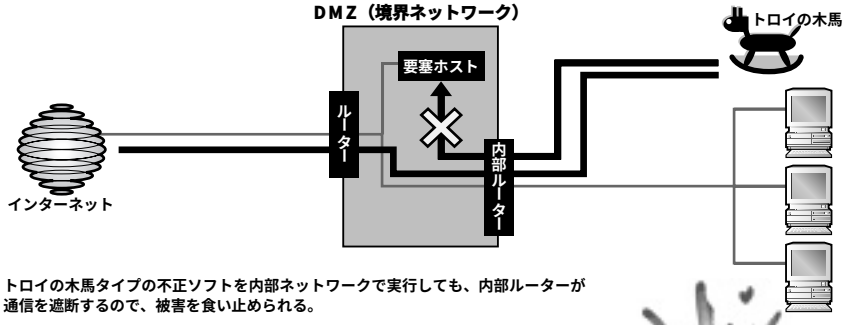
これは内部にあるクライアントのマシンに、トロイの木馬タイプの悪意のあるプログラムが送り込まれた場合などに対して防御できるようにするためです。トロイの木馬は非常に厄介です。たとえばWWWブラウザーなどでソフトウェアをダウンロードして、それが自動的に自己解凍を始めるようなことは、多くのみなさんが日頃目にしていると思います。

しかし、このような便利なメカニズム自体が、潜在的にトロイの木馬を取り入れてしまう危険性を持っています。電子メールに添付されているプログラムを自動的に実行してしまい、PCがコンピュータウイルスに感染してしまうような場合がありますが、これもトロイの木馬タイプの攻撃が可能であるということを示唆しています。

スクリーンドサブネット構造を使えば、要塞ホストが知らぬ間に乗っ取られたり、トロイの木馬タイプの攻撃が仕掛けられていたりしても、内部のネットワーク上に流れる情報に対してネットワークの盗聴をするようなことは非常に困難です。このように、たとえ1つの穴を見つけても、多重の防御線を張って守れば十分に防御することができます（図9）。

たしかに、スクリーンドサブネット構造を構築するには少々手間はかかりますが、その手間に見合うだけの効果はあります。出費という面でいえば、本連載では、外部に接続するルーターは広く使われているダイアルアップルーターやIPルーターを前提としていますし、内部に接続するルーターは古いPCを再利用してLinuxをインストールし、ルーターの役目を果たすための設定を行います。もちろん要塞ホストもLinuxを用いて構築します。新たな高額出費は必要なく、本格的なファイアーウォールを作ることができます。

図9　スクリーンドサブネットならトロイの木馬も防げる



トロイの木馬タイプの不正ソフトを内部ネットワークで実行しても、内部ルーターが通信を遮断するので、被害を食い止められる。

複数の要塞ホスト

スクリーンドホスト構造とスクリーンドサブネット構造の話の中では暗黙のうちに要塞ホストは1台であることを想定していました。本連載でも1台で進めます。マシンが複数台用意できるようであれば、境界ネットワーク上に複数の要塞ホストを用意して、サービス別に割り当てるというのもよい方法です。

たとえば、WWWのサービスとFTPのサービスを1つのホストとし、別のホストでは電子メール（SMTP、POP3、IMAP4）のサービスを提供するというのもよい選択です。こうすれば、設定ミスやセキュリティーホールを持ったcgi-binを使ったためにWWWサーバーが攻撃や侵入を受けても、ユーザーの電子メールはその時点ではまだ安全です。

また、WWWのサービスでも外部からアクセス可能なWWWサーバーを動かすホストと、WWWのコンテンツをWWWサーバーのホストからの読み取りだけができるNFSで提供するホストに分割してしまうのも1つの案です。もちろん、NATやIPマスカレードを使ってフィルタリングしているので、外部からはコンテンツを保持するサーバーは直接アクセスすることはできません。この方法を使えば、セキュリティーバグのあるcgi-binコマンドを経由してコンテンツを書き換えようとしても書き換えられません（ただし、当然、WWWサーバー自体が危険な状況にある点は理解してください）。

このようにいろいろな応用が考えられます。

おわりに

次回は、使っていない古いPCにLinuxをインストールし、2枚のNICを装着してIPフィルタリングの設定ができるまでを解説する予定です。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp