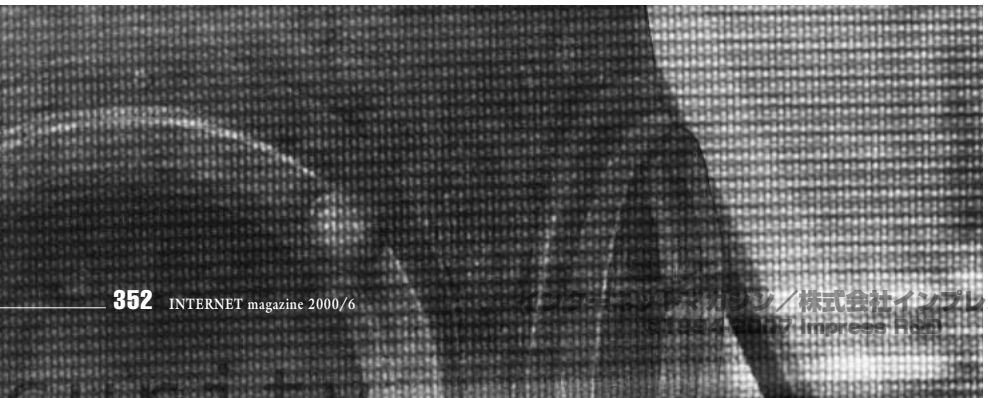
実践 Linux セキュリティー講座

今回は外部に接続するIPルーターの設定についての解説です。これが済めば外部へ接続するための一通りのセキュリティーは完了したことになります。このIPルーターでのフィルタリングは基本中の基本であり、少ない労力で効果的なセキュリティーを確保することができます。

最終回 外部に接続するIPルーター

ソフトウェアコンサルタント　すずきひろのぶ



使用するルーターについて

SOHOレベルでの常時接続用IPルーターとしては、ISDN用のダイアルアップルーターがOCNエコノミーなどの常時接続でも利用できます。現在、常時接続といっても転送速度は128kbps程度ですから、あまり高価な機材は必要ありません。実売価格で2～3万円程度のもので十分です。こうした製品は、多くの場合IPルーター（以下文中では単にルーターと呼びます）としての機能よりも、ハブの機能やプロバイダーとの接続に関するオプション機能などに主眼がおかれているようです。これは、常時IP接続ユーザーよりも、ダイアルアップで接続するユーザーの方がはるかに多いため、そのユーザーに対してより便利な機能を提供する形で開発が進んでいるからです。

まず、これから話を進めるルーターには以下の機能が備わっているものとします。

・IPフィルタリングができる
・IPマスカレードができる
・リモートのsyslogへの出力ができる

ルーターの設定方法に関しては各社各様なので、ここでは設定方針の枠組みについてだけ説明します。

ルーターは防御の最前線

ルーターはインターネット側とサイト側を接続する最前線にあるネットワーク装置で、IPパケットの経路を制御します。ルーターによるIPパケットのフィルタリングが、まず最初に行うセキュリティー対策であり、そしてもっとも効果のあるセキュリティー対策といえるでしょう。本章では、ルーターは次の2つのセキュリティーの重要な役割を果たします。

・IPフィルタリングにより外部からのIPパケットを排除する
・IPマスカレードによりIPアドレスとポート番号を変換する

ルーターによるフィルタリングだけでは十分とはいえませんが、それでも立派なファイアーウォールの機能を果たします。また整合性のあ

るフィルタリングのルールを設定し、サーバー側の利用環境と上手に組み合わせれば、最近話題になった省庁アタック程度の技術レベルしか持たない攻撃者ぐらいは防げます。無駄なお金を使わず、既存のもので効果的なセキュリティーを確保できるのです。

CATVの場合の注意点

本連載ではOCNエコノミーのようなネットワーク接続での運用を前提としていますが、CATVインターネットやインターネットマンションといったほかの常時接続の場合でも、IPフィルタリングは同様に必要となります。「CATVにケーブルモデムで接続すると、他の家庭から接続しているパソコンの共有ディレクトリーが全部丸見えの状態だった」という、笑うに笑えない話もよく聞かれます。ケーブルモデムにはフィルタリングの制御が含まれていないので、CATV全体が1つの巨大なLANのような状態になってしまうためです。

現在では、CATVでも利用可能なホームIPルーターと呼ばれる、小型で安価なルーターが製品として出てきています。本章で解説しているIPフィルタリングなどの手法は、ホームIPルーターにも適用できます。CATV接続でのセキュリティー対策を考えるならば、こうした製品の導入を検討してみてください。

ルーターには必ずパスワードを

ルーターの設定を行う前には、必ずルーターにパスワードを設定し、第三者に勝手に設定を変更されるようなことがないようにしてください。これは外部からの侵入者よりも、むしろ内部のユーザーに変更されてしまう危険性への対策です。別に悪意があって変更するわけではなく、自分の使っているツールが外部へネットワーク接続できないため、勝手にルーターに接続して変更してしまうという話を何度か聞いたことがあります。典型的な例がリアルオーディオで、リアルオーディオのサーバーはクライアントに対して6970/UDPから7170/UDPまでの範囲でUDPパケットを送る一種のプッシュ型の機能を実装しています。このポートに関してはIANAにも申請していない様子で、ポート番号表にも載っていません。クライアント（リアルオーディオのプレーヤー）はこのUDPポートを受け取る必要がありますが、UDPポートは一見しただけではランダムなものを使用しているように見えます。まったく何も知らない人が見たら、とにかくUDPパケットなら全部通したくなるのも人情というものでしょう。

本格的なルーターとは違い、ダイアルアップルーターは操作方法も簡単で誰でも操作できるという部分が一因でもあるようです。勝手に設定を変更され、せっかく設定したフィルタリングを台無しにされてしまうことがないようくれぐれも注意しましょう。

いずれにしろルーターはセキュリティーに重要な役割を果たすシステムですので、きちんとパスワードを設定し、安全な状態にしておくというのは基本中の基本です。

フィルタリングの方針を決める

ルーターのIPフィルタリングについては、本連載第5回の「パケットフィルタリングを設定する」と考え方は基本的には同じです。まず、どのようなサービスを利用するかという、サイトのセキュリティーポリシーを決めます。それにしたがって、外部からのアクセスを許可するマシンとプロトコルや、内部のマシンからアクセスを禁止するプロトコルは何かといった、フィルタリングの方針を決めます。この際に重要となるのは、方向（外部→内側、内側→外部）、プロトコル（TCP、UDP、ICMP）、ポート番号の3点です。

どのプロトコルを利用するかは個々のサイトによって異なりますが、ここではそうした点に左右されない、どのサイトでも設定すべき基本事項を説明します。

偽造IPアドレスの破棄

まず、自分のサイト内のアドレスをもったIPパケットが外部から来たら無条件に破棄します。こうしたパケットは何かの設定ミスによる事故である可能性も否定はできませんが、無意味なパケットを大量に送りつけるサービス不能攻撃（Denial of Service Attack）の可能性もあります。いずれにせよ、内部で利用しているアドレスのパケットが外部から送られてくること自体、故意であれ事故であれ正常ではありません。

これはSOHOレベルでは関係ありませんが、大学やプロバイダーのような内部で誰が利用しているかわからないようなサイトは、自分のサイトから発信されるIPパケットの送付元が自分のサイト以外であるような正しくないIPパケットは、その場で破棄して外部に出さないようにしましょう。それは事故か、あるいは悪質な攻撃のどちらかだからです。

❶ フィルタリングの管理ノートの例

処置	方向	プロトコル	外側アドレス	外側ポート	内側アドレス	内側ポート	理由
破棄	外→内	すべて	内部のアドレス	すべて	（なし）	（なし）	アドレス不正
通過	外→内	TCP	すべて	すべて	ウェブサーバーのアドレス	80（httpd）	ウェブサーバーへのアクセス
通過	外→内	TCP	すべて	すべて	メールサーバーのアドレス	25（smtp）	メールサーバーへのアクセス
通過	外→内	UDP	すべて	53（domain）	すべて	1024以上	DNSからの応答

※デフォルトではすべてのパケットを通さない設定になっていることが前提です。

IANA（アイアナ／Internet Assigned Numbers Authority）：南カリフォルニア大学内に置かれた組織で、ドメイン名の管理およびIPアドレスやプロトコルについての管理を行っていた。実際には、故ジョン・ポステルの献身的な努力による活動であった。現在は、IANAの役割はICANNへと受け継がれている。 www.iana.org

サービスへの許可

内部でサービスしているサーバーへのアクセス許可です。たとえばウェブサーバーやメールサーバーへのアクセスがあります。この場合、外部からのアクセスはウェブならばウェブサーバーのhttpd（80番ポート）のみに、メールならばメールサーバーのsmtp（25番ポート）のみにといったように、接続する先のマシンと利用するポートの組み合わせだけを通過させます。内部のすべてのマシンに対してのsmtpポートの解除などといった、接続先を限定しない許可はできる限り避けるべきです。また、内部にサーバーを持たない小規模な接続を開始するようなIPパケットについては、「すべてを許可しない」という1行だけの設定で済みます。

これらの許可に関しては、思いつきでいきあたりばったりに行うのではなく、きちんと管理ノートを作って、何を許可するのかを整理してから行うと間違いが少なくなります（❶）。こうした形できちんと記録を残しておくと、あとで変更を行う際にも作業が楽になります。

ここではセキュリティーに関して述べていますが、これ以外にも実際のルーター設定では、「RIPのパケットを外部に出さない」とか「netbiosを通過させない」といったものが必要になります。詳しくはルーターの運用マニュアルに書かれていると思いますので、その記述に従ってください。

内部から外部へのフィルタリング

内部のネットワークから外部へ接続を試みるようなトロイの木馬の危険性は常に存在していますが、内部から外部への接続を厳しく制限しすぎると自由度の少ないサイトになります。これはリスクと簡便のバランスをどう取るかを、個々のサイトで判断する必要があります。

1つは、内部から外部への制限を厳しくしてしまい、内部から外部へ接続する時は、socksやhttpd proxyなどを用いることで直接個々のクライアントが外部に接続しないような方法があります。しかし、だからといってトロイの木馬を必ず防げるということでもありません。

もう1つは、セキュリティー目的での内部から外部への制限を設けず素通ししてしまう方法です。ただし、内部から外部にそのまま通信できるのは境界ネットにあるサーバーのみで、一般ユーザーが使うマシンについては、境界ネットと内側ネット間にあるPCルーターのフィルタリングで通信を制限します。これは、一般ユーザーの利用がサーバー上ではほとんどないという前提に立っています。

IPマスカレードの活用

IPマスカレードはIPアドレスとポート番号を変換する機能です。これをたとえばウェブサーバーのポート番号の変更と組み合わせて利用すると、さらにシステムが安全になります。

ウェブサーバーを例に取るとApache（httpd）は、通常ではルート権限で80番ポートでサーバーが起動します。一般ユーザーの権限で起動するには、一般ユーザーが使えるようなポート番号、たとえば10080番で起動することになります。ただし、このウェブサーバーにアクセスするためには、http://h2np.net:10080/という具合に、URLでポート番号を明示的に指定しなければいけません。ウェブサーバーを一般ユーザー権限で動かせば、ウェブサーバーにバッファーオーバーフローのような致命的な脆弱性があった場合でも、直接はルート権限を詐取できないので少しは安心できます（しかし、満足できるほど十分に安全ではありません）。

そこで、このためにIPマスカレードを活用します。まず、Apacheを10080ポートで立ち上げます。これはApacheのhttpd.confファイル中のPort設定の値を変更することで可能になります。ルーター側の設定は、外部からの80ポートを10080ポートへ変更します（❷）。

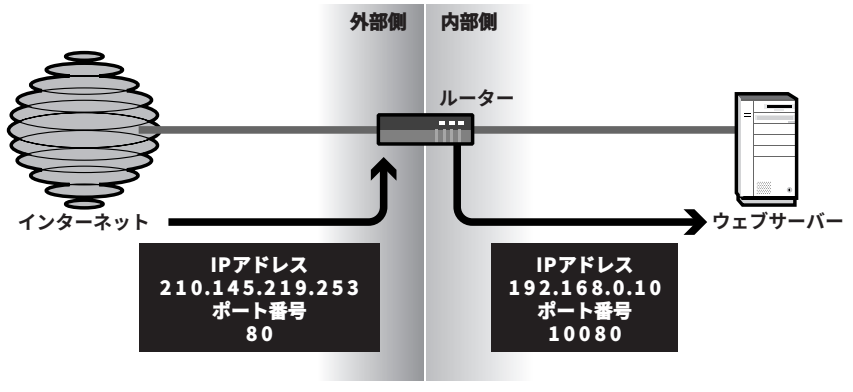
この設定は、外部と内部のIPアドレスの変換を指定する際に、ポート番号変換の指定を追加するだけで済みます。実質的にはルーター設定に費やす労力を考える必要もありませんし、最初からウェブサーバーのポート番号を決めておけば、何1つ追加作業を必要とせずに設定ができます。

リモートのsyslogへの出力

ルーターのフィルタリングの動作状況については、ルーターのsyslog機能を使って確認できます。ほとんどのルーターには、システムログをネットワーク経由で送信する機能があるので、このログをLinuxマシンで受け取る方法を使います（❸）。syslogのしくみや詳しい設定方法については、本連載の第10回（1999年11月号）で説明していますので参照してください。

ルーター側の設定としては、ログを記録するマシンのIPアドレスを指定します。また、ファシリティー値が指定できるルーターであれば、Linuxマシンの側でルーターのログだけを別の

❷ IPマスカレードの使用例



外部からのウェブサーバーへのリクエストを、内部のIPアドレスとポート番号に変更する。

socks（ソックス）：ファイアーウォールを超えて通信するためのプロトコル。socks対応のクライアントであれば、ファイアーウォール上のsocksサーバーを通じて外部との通信が可能となる。ウェブブラウザーでは、インターネットエクスプローラとネットスケープナビゲーターは両方ともsocksに対応している。

ファイルに記録できます。Linuxではlocal0（ファシリティー値16）からlocal7（ファシリティー値23）までローカルに使えるので、適当なファシリティーを使うといいでしょう。設定はLinuxマシンの/etc/syslog.confで行います（❹）。新規ログを作ったらログのローテーションなども忘れずに行いましょう。

実際のログを見てみると、外部から数多くのスキャンが行われていることがわかると思います。もし、一度もこのようなログを見たことがなければ、その数の多さに驚かれることと思います。よく知られた攻撃をするための事前の調査であろうスキャン、あるいは、まったく何のためにやっているかわからないスキャンなど多種多彩です。この情報を観察することによって、どのような攻撃が現在流行しているか大体想像がつくようになります。

ログの管理方法

システムログは1週間も経つとかなりの量になりますが、人間が読むには面倒なフォーマットで大量に出力されていますので、きちんとチェックするには苦痛が伴います。筆者は、ログ中のデータでセキュリティーに関連するものを抜きだし、綺麗に出力するプログラムを自作して利用しています。ログを読み込み、定義ファイル中で定義された危険度にしたがって分類し、HTMLフォーマットで記述された見やすい表を出力します（❺）。またこれは親切な協力者の方々のおかげでSOHOレベルで利用される主なダイアルアップルーターをサポートすることができました。利用条件をGNU Public Licenseとして公開しているので自由にコピーしてご利用ください。場所は下記のURLにあります。

CLSCANのページ
Jump h2np.net/clscan/

最終回のおしらせ

一通りではありますが、外部に接続するルーターの設定まで説明しましたので、連載はここで終了させて頂きます。誌面の関係上、補足する部分やもう少し細かい部分を省略せざる得なかった部分が多々ありました。また、1年半以上も長く連載を行っていた関係で、前半部分では内容的に古くなってしまっているところもあります。

昨今、世の中では情報セキュリティーのニーズが高まっています。セキュリティーの解説本といいつつ、実際には「クラックの手口教えます」というレベルの本も世に溢れています。反対に全体のシステムを捉え、具体的に安全なサイトを構築するような本は残念ながらわずかです。こうした点を踏まえ、この連載をベースにして、さらに加筆して1冊の本にすることを決心しました。観念論や包括論ではなく、SOHOレベルでも安価で安全なシステムが構築できるのだということを具体的に提示したいと思います。単行本では、「激安マシンの作り方」、「秋葉原で機材を調達する方法」など、非常に具体的な、かつ、現実に即した内容も組み入れたいと思います。

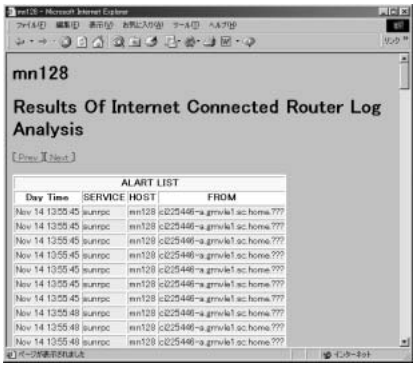
では、また会う日まで。

❹ /etc/syslog.confの設定

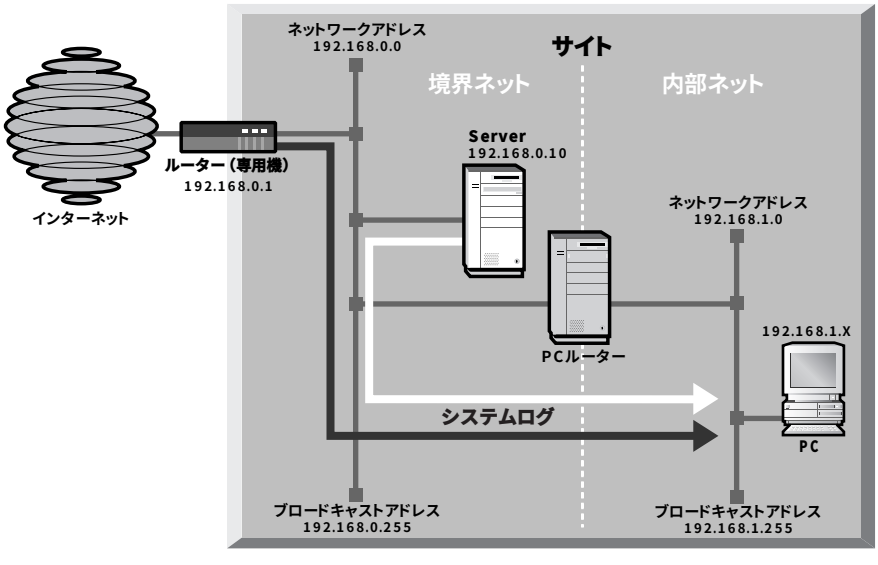
```
....
#
# ROUTER LOG （Facility Val = 16）
   local0.*          /var/log/router
   ファシリティー番号     ログファイル名

local0 = 16
local1 = 17
      :
      :
local7 = 23
```

❺ CLSCANの出力画面（例）



❸ サイトのネットワーク構成図



GNU（グヌー／Gnu is Not Unix）：1983年にリチャード・ストールマンが提唱した、フリーソフトウェアで構成されたUNIX互換のソフトウェア・システム、およびそのプロジェクトの名称。GNU Public Licenseは、ソフトウェアの複製や配布を自由に行うことを保証するためにGNUによって立案された使用許諾条件。Jump www.gnu.org

［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