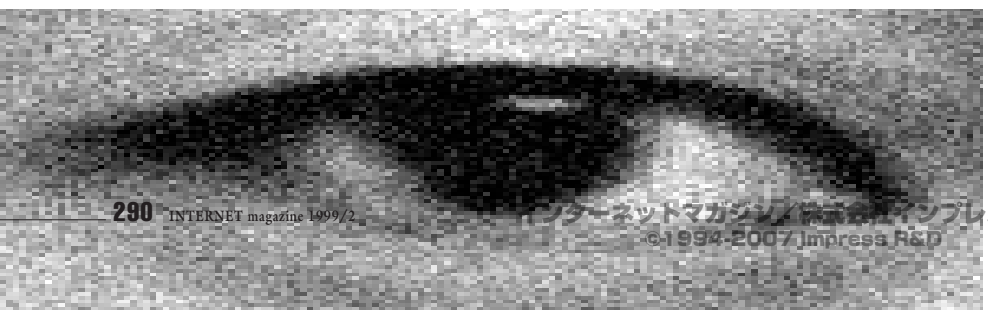
実践 Linux セキュリティー講座

自宅や小規模なオフィスなどで専用線を引くにあたって考えなければならないことは、サイトを守るためのセキュリティーです。そこでこの新連載では、Linuxをプラットフォームとするマシンを使い、不正アクセスに対するセキュリティー対策をどのように施せばいいのかを実際の設定を交えながら解説していきます。用意するのは、もう使わなくなった非力なPC/AT互換機だけです。連載を重ねるごとにサイトのセキュリティーは高まっていくでしょう。

新連載 第1回 セキュリティーについて理解する

ソフトウェアコンサルタント　すずきひろのぶ



本格的なセキュリティーに踏み出そう

インターネットはすでに一般のPCユーザーにまで利用の裾野が広がり、さらに本格的に自らサーバーを構築するユーザーが現れる状況になっています。以前は大企業や大学、研究所などが持っていた自前の独自サイトも、現在では小規模な組織や会社、あるいは個人でも持てる時代になりました。

しかし、現状では、サーバー構築に関するノウハウが必要であり、それ以上に不正アクセスを防ぐためのセキュリティーに対する十分な考慮が必要です。ここでいうセキュリティーとは、ネットワークに接続されているサイトを守るサイトセキュリティーを意味しています。

インターネットに接続している小規模サイトの場合、インターネットへの接続を可能にするという目的を達するレベルで終わってしまっていて、その先にある不正アクセスに対応すべきセキュリティーなどは対策がなされていないという傾向が見受けられます。

セキュリティーの意識に欠けるサイトがたくさんあるという部分もあるでしょうが、一方でセキュリティーを考慮しようと思っていても実際には対応できていない所もたくさんあると思います。

この理由を想像すると、十分なシステムを構築するための機材には高額な投資が必要となること、あるいはセキュリティーに関するノウハウを得るチャンスがないといったことがあるのではないでしょうか。インターネットに接続された大企業のサイトでは、外部業者にシステムのセキュリティー対策を発注するとか、高価なハードウェアの交換や増設をする、あるいはセキュリティーソフトウェアを購入することができるでしょう。

しかし、小規模で運営しているインターネット接続サイトでは、そうそうお金をかけるわけにはいきません。だからといって、問題を放置しておくわけにもいきません。これはジレンマです。

インターネットマガジン株式会社／インプレスR&D
©1994-2007 Impress R&D

このようなサイトがセキュリティーに対してどう対処していけばいいのかを解決していくのが本連載の目的です。

金銭的な負担は極力抑えるような工夫をしますが、セキュリティーに対して何もしないよりも費用はかかります。また、自分ですべて行うわけですから、それなりの手間もかかります。しかし、高価なツールや機材を使わずとも十分に効果のあるセキュリティーを実現できるように工夫していきたいと思います。

本連載では小規模サイトでのセキュリティーを対象にしていますが、極端にスケールの違う大きなサイトは別として、基本的なノウハウは多くのサイトで利用できるものだと思っています。また、個々の知識は、いろいろな場面でのヒントになるでしょう。

不正アクセスの種類を理解しよう

まずは不正アクセスが何かを考えてみます。アクセス方法から分類すると大きく3つのパターンがあります（図1）。

- 不正な侵入
- 情報への不正アクセス
- サービスの妨害

まず最初の「不正な侵入」とは、多くの人が認識しているとおり、システムに不正にログインして利用することです。ここで指摘したいのは、多くの人はこれだけが不正アクセスの問題だと思っている傾向が見られることです。

確かに不正にログインして情報にアクセスするというのは、わかりやすいモデルで危険です。しかし、次の「情報への不正アクセス」というのはシステムに直接的にアクセスしなくとも成立します。

たとえばサーバーアプリケーションのぜい弱性（セキュリティーバグ）を突くような形でシステムにログインすることなしに、システム内部の情報を取り出したり、あるいは改ざんしたり破壊したりするといったことも十分に考えられます。

また、一般にサービス不能攻撃と呼ばれる「サービスの妨害」も同様です。遠隔地から不正なコマンドや情報、あるいは大量のデータを送りつけられることによってシステムが麻痺し、サービスを提供できなくなることも考えられるのです。

これらの不正アクセスの特徴を踏まえたうえでセキュリティーについて考えなければなりません。

セキュリティーはバランスである

セキュリティーを計算する数式があるとするなら（そんな数式はありませんが）、たぶんこんな数式になるのではないでしょうか。

$$\text{セキュリティー} = \frac{\text{コスト}\times\text{ノウハウ}\times\text{運用}}{\text{ヒューマンエラー}}$$

予算（コスト）がたくさんあり、ノウハウもたくさんあり、日々の運用もきちんと行い、そしてヒューマンエラーが少なければセキュリティーは高まるでしょう。コストが少ないとしても、その分、ノウハウと運用の値を大きくすれば、セキュリティーの値は同じになります。また、どんなにコストやノウハウや運用を大きくしても、ヒューマンエラーが多いシステムでは、セキュリティーが低くなってしまいます。実際にはもっと小さな要素がありますから、セキュリティーはいろいろなバランスの上に成り立っているといえるでしょう。

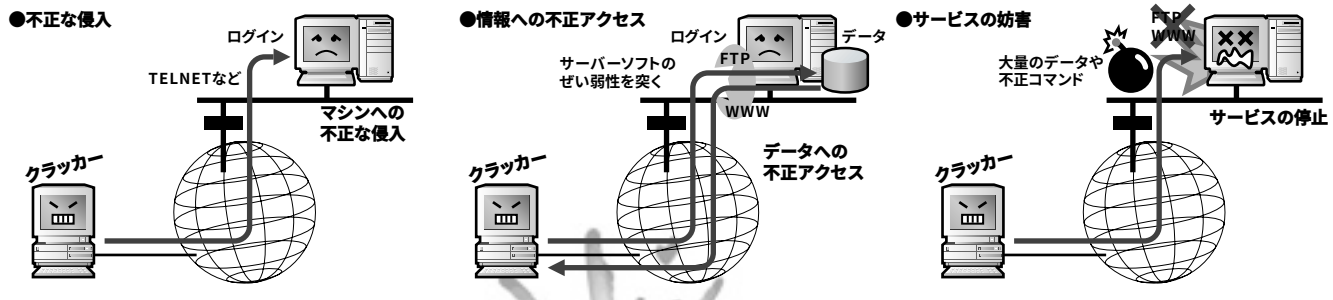
もしセキュリティーを考慮しないと……

もし、何もセキュリティーを考慮しないまま専用線で接続して自分で各種のサーバーを利用していた場合、次のようなトラブルが考えられます。

- スパムメールの不正中継
- FTPサーバーの不正利用（ポルノ画像や海賊ソフトの配布中継点）
- ウェブサーバーの乗っ取り（ページの改ざんや破壊）
- 不正なサーバーのサービス（ポルノサイトとして利用など）
- 証拠隠滅のためのサーバー情報破壊
- 踏台として利用（ほかのサイトの攻撃基地としての利用）

スパムの不正中継が行われた場合、あちらこちらのISPで、その中継に利用されたドメインから発信される電子メールを一切受け付けなくするような処置を取られる場合があり

図1　不正アクセスの種類



©1994-2007 Impress R&D

ます。もしそうなると、自分のドメインから発信された電子メールが届かなくなるという大きな問題が発生します。

サーバー類に対するセキュリティーの不備はいろいろな問題を引き起こします。FTPサーバーの設定が甘いと、そのサーバーはポルノ画像や海賊ソフトなどの中継基地に使われてしまう危険性があります。

ウェブサーバーの改ざんや破壊はよく聞く話ですが、これによって運用組織の信用を失墜させるだけではなく、FTPサーバーと同様の不正な情報の中継にも使われる危険性があります。

不正なサーバーのサービスとは侵入者が勝手にサーバーを立ち上げる、もしくはトロイの木馬のように直接侵入は行わずとも、命令あるいはプログラムを送りこんでサーバーを立ち上げるような方法です。不正なサーバーを立ち上げ、不正な情報の発信基地にしてしまう危険性があります。

見つかりそうになると、証拠隠滅のためにディスクの内容をすべて破壊して逃走するという事態も発生することが考えられます。そうなれば貴重なデータがすべて破壊される危険性があります。

もっとも大きなトラブルに発展する可能性があるのは、踏み台として利用される場合です。踏み台とは攻撃目標とするサイトから逆探知されないように利用する隠れ蓑となるマシンのことです（図2）。直接踏み台マシンに侵入して、そこから攻撃することもありますし、踏み台マシンに侵入せずとも、外部から踏み台マシンに不正な命令を与え、本来の目的としているサイトに攻撃する方法も考えられます。

自分のサイトがこのような踏み台として使われてしまった場合、攻撃を受けた側から踏み台サイトを提供してしまった管理責任を追及される可能性も十分に考えられます。最悪のケースとして、管理責任が不十分だったということで、損害賠償を求められて民事裁判に発展するような状況も十分に考えられるでしょう。

プロバイダーのサービスを利用する

現在、独自ドメインを取得して専用線でインターネットに接続している場合でも、必要なサーバー管理をプロバイダー側で行い、利用者は最小のリスクで専用線に接続できるプロバイダーによるサービスがあります。

IIJを例に取ると、IIJエコノミー（低価格専用線接続サービス）とIIJポストオフィスサービスを組み合わせることによって、独自ドメインを取得していても、DNSサーバーや電子メールサーバーをプロバイダー側で管理してもらえます。この場合、外部からサイト内へのアクセスをルーターで極端に制限してしまうという安全な運用も可能です。さらに、ウェブサーバーなどもレンタルすることによって、管理コストを下げるのと同時にセキュリティーを高められるでしょう。

このように、プロバイダーのサービスを上手に使ってサーバーを安全に運用する手段もあります。システム管理に自信がない場合は、そのようなサービスを利用するのを検討するのもいいでしょう。

Linuxを使えばコストが安くあがる

本連載ではこれからLinuxを使ってセキュリティーの能力の高いサイトを構築していきます。LinuxはPOSIX仕様（標準化されたUNIX）のOSですので、ネットワークシステム環境を構築するプラットフォームとして非常に有効に活用できます。現在のLinuxは十分に安定しており、かつ、動作に必要な資源が少なくて済むという利点があります。そしてなによりも導入のための金銭的負担が小さくて済むという利点があります。

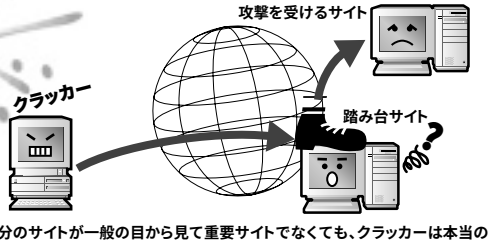
これらの理由を背景に、Linuxはインターネット上のプラットフォームとしてシェアを伸ばしています。そのシェアを伸ばしている現象自体が注目を浴び、さらに利用者が急速に伸びるという状況になっています。

この連載で使うソフトウェアプラットフォームはLinuxの最新版を利用しますが、筆者がハードウェアプラットフォームとして用意しているマシンは古いPC/AT互換機です。手元にはペンティアム75MHzと90MHzのマシンが2台があるので、これらを利用する予定です。

UNIXとネットワークの知識が必要

この連載を読めばコンピュータやインターネットに対してまったくの初心者が、すぐに

図2　踏み台サイトに使われる！



自分のサイトが一般の目から見て重要サイトでなくても、クラッカーは本当の目的サイトを攻撃するために踏み台サイトとして利用する場合がある。このとき自分に被害がなくても、自分のセキュリティーの甘さがほかのサイトに大きな被害をもたらす。

表1　守るべきものとアクセスを許可するもの

対象	守るべきもの	アクセスを許可するもの（人）
クライアント	ユーザーが利用するクライアント上のすべてのデータ	基本的になし
サーバー	サーバー上にある公開している情報以外のすべてのデータ	ウェブで公開している情報
		FTPで公開している情報
		クライアントからの個人のメールボックスへのアクセス
システム	使用権限を越えたシステムのリソース	正当なアカウント保持者

サイト内で守るべきものとアクセスを許可するものをはっきりと区別することで、セキュリティー対策が施しやすくなる。本連載では上記のようなポリシーの下で解説するが、自サイトの特殊なものについては、この中に加えて考えてほしい。

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

セキュリティーの高いサイトを構築できたり、スキルの高い管理者になれたりするということは残念ながらありません。エキスパートである必要はありませんが、ある程度のUNIXの知識、ネットワークの知識、インターネットの知識を持っていることを前提とします。

この連載はソフトウェアのインストールやシステムの設定、あるいは使い方を述べるだけの範囲にとどまらず、セキュリティーそのものを考える内容にしていきたいと考えています。システムをブラックボックスとして利用するようなアプローチは取りません。このため、先に挙げた分野での基本的な知識は持っていることが望ましいのです。

セキュリティーポリシーを考える

セキュリティーポリシーを一言で表現すれば「サイトのセキュリティー方針を決めること」です。セキュリティーポリシーを難しく考える必要はありません。自分の守るべきサイトに対して次のことを考えてみてください。また、文章として記録することをおすすめします。文章にすることによって明確にできますし、抜けがないかを確認する材料ともなります。

❶何を守るのか
❷誰から守るのか
❸どうやって守るのか
❹守っていることをどうやって確認するか
❺守ったことをどうやって周知させるか

❶何を守るのか

目標を決めないということは、何も守っていないのと同じことです。まずは目標を決めます。もし、マシン上のすべてのデータを安全に保持したいのなら、そのマシンはネットワークの接続をすべて遮断すべきでしょう。また、サーバーマシンとなるものは接続性を保つことが前提となりますので、これを考慮したうえで運用を考えなくてはなりません。サイトごとに構成が異なるので一概にどのような対策が正しいとは言えませんが、単純化して表1のように決めます。

❷誰から守るのか

ここでは非常にシンプルに考えます。まず、「外部からのアクセスは一切受け付けない」というのは非常に明確でわかりやすいと言えるでしょう。また、サーバーは基本的にはサーバー管理者以外はログインできないということにして、それ以外のユーザーはログインできないようにします。

❸どうやって守るのか
❹守っていることをどうやって確認するか

これは技術的な個々の話になるので、連載を通して考えましょう。

❺守ったことをどうやって周知させるか

サイトを守るためのセキュリティーをユーザーに理解して協力してもらわないと、せっかく努力してセキュリティーを施しても、サイト内のユーザーが内部からセキュリティーを崩していく危険性があります。

簡単な例でかつ怖いのは、ユーザーがどこかから得体の知れないソフトウェアを持ち込み、実はそのソフトウェアがトロイの木馬だったりする場合です。たとえばソフトウェアにほかのサイトを自動攻撃する機能が組み込まれていて、それが持ち込まれた場合、自分の守るサイトから外部へ攻撃していることになってしまいます。

しかし、この問題は小規模なサイトではあまり障害にはならないと思います。多くの場合、ユーザーが少ないので意思疎通が簡単だからです。

ところが大きなサイトではこれがかなりの問題になる場合があります。セキュリティーに関する意思疎通がうまくいかない場合、サイト内のユーザーはこのようなセキュリティーは邪魔なだけだと考えるかもしれません。中には自分のマシンにモデムを接続し、直接外部へアクセスするようなユーザーがいるかもしれません。このようにサイト管理者が知らない部分で外部に接続されてしまった場合、そこがセキュリティーホールとなり、せっかくのセキュリティーも内部から崩壊してしまう危険性すらあります（図3）。

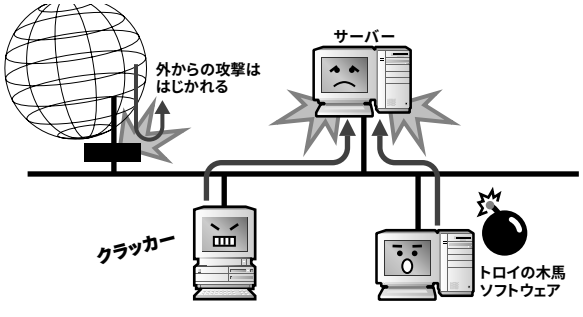
さらに、大企業や大学などの大きなサイトの場合、内部のユーザーが不正アクセスを行う張本人である危険性もあります。また、内部から情報を流して外部からの不正アクセスを手引きするような場合もあり得るでしょう。

内部からの不正アクセスの場合、同じネットワーク内にあるマシンを内部犯行から守るのは非常にコストのかかる問題であり、また技術的にも単純には解決できません。しかし、こういう問題があるにしてもインターネットとの接続の根幹をなすサーバーシステムは守らなければならないのは言うまでもありません。

次回取り上げるテーマは……

今回は、最初の導入部として全体の心構え的な部分で話が終わってしまいました。次回はファイアーウォールの構成について、具体的な設定を示しながら解説します。

図3　内部からの攻撃もある



内部にクラッカーまがいの人物がいれば、内部からサーバーへの攻撃があることも考慮しなければならない。大規模なサイトの場合は、内部からの攻撃のほうが多いこともある。また、エンドユーザーがトロイの木馬タイプのソフトウェアを知らぬ間にインストールして、これがサーバーを攻撃したり情報を持ち出したりする場合もあるので、細心の注意が必要だ。

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

［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

Copyright © 1994-2007 Impress R&D, an Impress Group company. All rights reserved.