WWW システム構築におけるネットワーク セキュリティに関しての検証

解析事業部　電力システム部　システム開発課

牧　　正　樹

はじめに

今日フレッツ･ISDN、xDSL サービス、CATV インターネット接続サービス等の常時接続サービスの普及により個人でサーバを立てて WWW サイトを構築しようと考える人が増えてきています。しかし常時接続における WWW サイト構築は設定に注意しないとクラッカー[1]などの標的になるおそれがあります。クラッカーによる被害がサーバ管理者のみの問題ですむ場合は少なく、クラッカーによりサーバに混入されたプログラムが他のサーバに対してのクラッキングの足がかりとして利用される場合がほとんどです。もし運営しているサーバがそのようなクラッカーに侵入された場合、社会的信用を損なうばかりでなく、足がかりにされたことにより被害を受けた他サーバの被害も補償しなければいけない事態になる可能性が十分あります。このような事態にならないように、WWW サイト構築における最低限のセキュリティ対策方法について考えていきたいと思います。

1．WWWシステムの選定

まず WWW システムの選択を行いたいと考えます。現在 WWW システムとして代表的なものとして Apache と IIS の 2 種類があります。

Netcraft[2]が 2001 年 9 月に行った調査によると Apache は全世界で稼動している WWW システムの約 60%と、2 位の IIS の約 27%の約 2 倍となるシェアを占めています。同調査機関の WWW システムの OS の調査では Windows が 50%占めているにもかかわらず、これだけ Apache が使用されていることは Apache のソフトの質が高いことが世界で証明されていることを示していると考えます。それ故、このレポートにおいては Apache を WWW システムに使用した場合におけるセキュリティ対策について考えていきたいと思います。

次に WWW システムを動作させる OS を選定したいと思います。Netscraft が行った調査結果によると WWW システムとして使用されている OS としては Windows が50%で 1 位、次に Linux が30%で 2 位です。それ以降は Solaris が7%で3位、ＢＳＤが６％の４位となっています。今回は Apache を WWW システムとして選択しましたので OS は 1 位の Window ではなく 2 位の Linux または4位のＢＳＤに代表される PC-UNIX を推薦したいと思います。なぜなら PC-UNIX は Apache

1 他人のパソコンに侵入してパソコンを乗っ取ったり、不正行為の足がかりに使用したりする人々の総称

2 Netcraft : http://www.netcraft.com/survery/

の主要稼働環境である UNIX の一派であるため Apache との親和性が高く、なおかつ UNIX 文化にて培われた豊富なフリーソフト(セキュリティ対策ツールを含む)が利用可能であるからです。また PC-UNIX は基本的に無料であるため Apache を用いて WWW システムを構築する場合、PC-UNIX は安定面・セキュリティ面・価格面に関して最適な OS の一つであると言えます。[3]

これらのことより以下では Apache & PC-UNIX を用いての WWW システム構築に関してのセキュリティ対策に対して考えていきたいと思います。

2．安全なWWWシステム構築方法

PC-UNIX を用いての WWW システム構築にあたり、必要最低限のセキュリティ・ポリシーには大別して以下の 5 つが存在します。

(1) 他人にはわからないパスワードを利用
(2) 不要なサービスを立ち上げない。できればそのサービスの元になるアプリケーションはインストールしない。
(3) 特定のコンピュータからのみ接続可能にする。必要なポートだけを開ける。
(4) OS やアプリケーションに関してのセキュリティ情報の収集を欠かさず行う。セキュリティ・パッチは欠かさず当てるようにする。
(5) 定期的なメンテナンス

この 5 点に関する対策方法について順次説明していきたいと思います。

3．パスワードの設定方法

まず(1)のパスワード設定について考えたいと思います。

WWW システムのセキュリティ対策として最も基本的な対策は他人にわからないパスワードを使用することです。このパスワードが安易に解読できるものであるとすぐにクラッカーにより解読されてシステムを乗っ取られてしまう可能性があります。そこでパスワード決定時は最低限以下の点に考慮したものを使用することを心がけてください。

① 辞書に載っている単語を使用しない。
② 身近な単語を使用しない。
(誕生日、電話番号、名前 etc)
③ パスワードの文字数は8文字以上にする。

まず①ですが、クラッカーはパスワードを調べる時、多数の電子辞書を用いて調べます。それ故、辞書に載っている単語を使用することはすぐにクラッカーに調べられてしまいます。

次に②ですが、このような身近な情報はクラッカーにとって調べあげることは困難ではないため使用することは避けるべきです。

最後に③についてですが①や②の条件をクリアーしたパスワードでもパスワードの文字数が 6 文字程度であれば現在の高性能なパソコンを使用すれば数時間もあれば解析することが可能です。しかし 8 文字以上になるとどんなに高性能なパソコンを使用しようと解析に数日を有します。それ故、①、②の条件をクリアし、なおかつ文字数が 8 文字以上であればそう簡単にクラッカーに調べあげられる心配がなくなるのです。[4]

3 もちろん価格の面で可能であれば商用 UNIX でのサーバ構築も選択項目に含まれます。

4 ユーザ名もこの規則にしたがって作成することにより更なる安全性が保障されます。

4．不要なサービスの停止

次に(2)の不要サービス削除について考えていきたいと思います。今回 WWW システムのサーバとして選択した PC-UNIX は通常インストール直後の状態のまま使用すると WWW システムでは使う必要のないサービスまでが稼動している状態になります。サーバは機能が多いほど優れているという考えの方が多いですが、こと WWW システムのように固有の機能に対してのサーバを構築する場合は使用しないサービスはセキュリティホールになるばかりでなく、パフォーマンスの低下につながるので停止すべきです。

4.1. 最低限必要なサービスは？

通常、最低限必要なサービスのみ起動した状態にすると、外部と接続しているポートが少なくなるため進入される危険性が減少します。

WWW システムとして最低限必要なサービスは HTTP(80/TCP)を制御する httpd サービスです。しかし実際問題として httpd サービスだけではサーバ設定作業等で大変不便です。[5]それ故、少しずつ起動サービスを追加(セキュリティ面で妥協)していくことで、サーバ運営を快適にする必要があります。次に httpd サービス以外に起動するサービスを限定する方法について検討したいと思います。

4.2. 起動サービスの限定方法

起動しているサービスを減らすことは、セキュリティのリスクを減らすことに直結致します。マイナーなサービスほどセキュリティホールの対策が十分されていないため、起動しているだけでリスクを背負うことになります。できるだけ不要なサービスは停止しておくことがWWWシステムを安全に運営するためには不可欠です。では、これらのサービスの起動･停止を制御するためにはどうしたらよいのでしょう？一度起動して毎回不必要なサービスを停止していたのではきりがありません。

ですので不要なサービスは起動しないようにすべきです。PC-UNIX は起動プロセス毎に起動用スクリプトが存在します。それ故、その起動用スクリプトを編集･削除することによって、起動サービスを制限することが可能です。RedHat 系 Linux であば/etc/rc.d/rc3.d 以下、Debina 系

表1 代表的なサービス

サービス名		ポート
WWW システムとして最低限必要なサービス	http	80/TCP
他の用途で必要なサービス	ftp	21/TCP
	ssh	22/TCP
	telnet	23/TCP
	syslogd	514/UDP
必ずしも必要ではないサービス	X11	6000/TCP
	cannna	5680/TCP
	wnn	22273/TCP
	smtp	25/TCP
	lpr	515/TCP
	linuxconf	98/TCP
	time	37/TCP
	finger	79/TCP
	auth	113/TCP
	portmap	111/TCP
		111/UDP

5 リモートログイン、FTP などが使えないため直接サーバにて作業を行う必要があり作業効率が大変悪い状態になります。

Linux では/etc/rc2.d 以下、FreeBSD であれば /etc/rc.conf 又は/usr/local/etc/rc.d 以下にあるスクリプトファイルを編集・削除することにより、サービスの起動制限を行うことが可能です。[6] 表1は主なサービスと使用ポートの一覧です。

4.3. リモートログインの安全性強化

通常 WWW システムは、実際にサーバの画面[7]で作業を行うよりはリモートログインにて作業を行うことが多いと思います。現在リモートログインサービスとして最もよく使用されているサービスは telnet サービスです。しかしこの telnet サービスは、リモートコンソールから入力したコマンドを平文のまま送受信を行うため、通信データが第三者によって盗聴される危険性が高いサービスとして知られています。したがって、telnet サービスと同一のリモートログインサービスであるが公開鍵認証等による暗号通信を行うことによりセキュリティ機能を強化した ssh サービス[8]を使用することを推奨します。

この ssh サービスはユーザ認証用に使用する個人鍵、公開鍵の作成などの作業を行う必要があるため導入にはそれなりの技術力が必要です。それ故すぐに導入する事は困難ですが、WWWシステムの最も弱い部分をがっちりガードしてくれる頼もしいツールであることも事実です。したがって、WWW システムをインターネット公開するならば是非とも導入すべきツールです。

5．接続可能コンピュータの制限

次に(3)の接続可能コンピュータの制限について考えてみたいと思います。これまでの作業により不必要なサービスが起動しない状態になりましたのでかなりセキュリティホールが減少しました。しかし現在の状況では起動しているサービスに対してはどのパソコンからも使用することが可能です。これでは起動しているサービスにセキュリティホールがあった場合に不安です。それ故、現在起動しているサービスに対して接続可能なパソコンを制限することはさらなる安全性が保証されることになります。この接続ユーザの制限方法はPC-UNIX の各種ＯＳまたは起動サービスにより異なりますので一概に説明することは困難ですが、Linux の inetd に関する制限は/etc/hosts.allow に

許可するサービスの実行ファイル名:許可するIPアドレス

を記載し/etc/hosts.deny に、

ALL ： ALL

と記述しておけば/etc/hosts.allow に記載されている IP アドレスから同ファイルに記載されているサービスに対してのみ接続可能な状態になります。

たとえば FTP サーバの wu-ftpd なら、/etc/hosts.allow に

in.ftpd: 172.16.1.1 , 172.20.41.1 (例)

といった感じで記載し、

これに加えて、/etc/hosts.deny に

---

6 起動ランレベル等によっては編集するファイル構成が異なります。

7 X サーバにもセキュリティホールが存在します。それ故サーバには可能であれば X のインストールをしないことを推奨します。

8 PC-UNIX ではフリーの SSH として OpenSSH が広く使用されています。

ALL : ALL

と記載すれば「172.16.1.1」,「172.20.41.1」以外の IP からの FTP 接続はできない状態になります。OS･起動サービスによっては設定方法が多少異なりますが同じように設定を行うことにより安全性を高めることが可能です。

つぎに接続可能ポートの制限ですが、一般的な方法として/etc/services ファイルを編集する方法があります。それ以外にもカーネルバージョン 2.4 を採用した Linux であればほとんどのディストリビューション[9]においてインストール時に接続可能ポートの制御が可能です。たとえば RedHatLinux7.0 以降をベースにしたディストリビューションではインストール時に ipchains と呼ばれる Linux カーネルに実装されているファイアウォール機能を用いて必要なポートのみを開くように設定することが可能です。[10] このほかにも、ごく基本的な対策としてルータ(ダイヤルアップルータ他)などの機能を用いて接続可能なポートを制御する方法があります。ネットワーク環境、使用 OS により設定方法は異なりますがこのように接続可能ポートを制限することはクラッカーによる被害の可能性を減少させるためには有効な手段ですので、設定されるべき項目です。

6．セキュリティ情報の収集

次に(4)のセキュリティ情報の収集について考えていきたいと思います。WWW システム構築などを行う場合、セキュリティ情報の収集は欠かさず行う必要があります。いくら(1)～(3)の方法を用いてセキュリティを固めたとしてもどこかにセキュリティホールがあった場合、そこからクラッカーに侵入される可能性があります。それ故、WWW システムを構築している PC-UNIX のセキュリティ情報や最新パッチを提供しているサイトは日常的にアクセスすることをお勧めします。それ以外にも JPCERT[11]のように最新のセキュリティ情報を提供しているメーリングリストに加入して最新情報を入手するなどの方法もあります。

最新のセキュリティ情報を公開しているサイトは多数存在いたしますが代表的なサイトとして

●Securityfocus
http://www.securityfocus.com

●CERT/CC
http://www.cert.org

などがあります。

これ以外にも

●セキュリティ memo
http://www.st.ryukoku.ac.jp/~kjm/security/memo/

●日本の Linux 情報
http://www.linux.or.jp

など多数存在しますので、ご自分の環境に合った情報源を見つけていただき、安全な WWW システムの構築･運営していただきたいと思います。

9 Linux における各種類の総称。RedHatLinux、Debina などが存在する。

10 インストール後も/etc/sbin/setup を実行することにより設定が可能です。

11 JPCERT : http://www.jpcert.or.jp

7．定期メンテナンス

これまでいろいろな WWW システムのセキュリティ対策に関して述べてまいりましたがセキュリティ対策はこれだけではありません。

これ以外にも

①定期的なデータバックアップ

②各種ログの管理及び解析

などに代表される定期メンテナンスがセキュリティ対策に欠かせない作業であります。

①の定期バックアップはデータ更新頻度が少ないサイトにおいては忘れがちですができる限りバックアップするように心がけてください。

②のログ管理･解析にはアクセス解析ツールが欠かせません。アクセス解析ツールには、商用、フリーの物があります。ここでは、使いやすくなおかつフリーである Analog を紹介いたします。

Analog は、http//www.analog.cx/が公式サイトのフリーソフトウェアです。日本語対応は日本 Analog ユーザ会(http://www.jp.analog.cx/) が行っていますので日本語で使用したい場合は、そこからパッケージをダウンロードして使用することにより可能です。またインストール方法･設定方法等は日本 Analog ユーザ会のサイトに詳しく紹介されていますのでここでは控えさせていただきます。

8．最後に

ここまでいろいろと述べてきましたセキュリティ対策は膨大な課題であるためどうしても概論的な説明になってしまいました。ですから WWW システムの構成においてはこれだけでは不十分な場合も多々あると思います。それ故、今回記載いたしました情報を参考にいたしまして個々の WWW システムにおいて最適な方法を皆様の方で改良していただければと考えております。

参考文献

1) 日経 Linux 2001 10月号
特集:カーネル 2.4 時代のセキュリティ対策入門
日経 DP 2001.11

2) UNIX ネットワークセキュリティ導入･運用ガイド
高町 健一郎 著
秀和システム 2001.4

3) OpenSSH セキュリティ管理ガイド
新山 祐介/春山 征吾 著
秀和システム 2001.6

4) SoftwareDesign 2001 10月号
特集:Apache でゼロから作る Web サイト
技術評論社 2001.10

5) Linuxmagazine 2001 5月号
特集:ネットワークセキュリティを固める
ASCII 2001.5

6) Linuxmagazine 2001 7月号
特集:インターネットサーバらくらく公開術
ASCII 2001.7