—論文—

高岡短期大学紀要　第14巻　平成12年3月
Bull. Takaoka National College, Vol.14, March 2000

地域ボランティアが運営するインターネット・サーバのセキュリティ管理

近藤　潔[1]

(平成11年10月15日受理)

要　旨

大学開放活動の一環として，インターネット・サーバを地域に公開する試みを行なってきた。サーバを公開する際の主な問題は，システム運営に必要となる負荷の軽減と，境界ネットワークに置かれたサーバのセキュリティ管理である。大学のシステム管理者の負荷を軽減するために，地域のボランティア管理者を募集してシステム運営を分担する体制を整えるとともに，利用者にとって制約の少ないセキュリティ管理方法を模索して約1年間の試験運用を行なってきた。セキュリティ管理は，protect, detect, react のすべての段階で抜けのないセキュリティ対策が要求される。しかし，あまり厳格な管理は利用者に多くの制約を課し，利用意欲をそぐおそれがある。そこで，実運用の経験にもとづき，必要最小限のセキュリティ機能を確保しつつ利用者に最大限の自由を与えるセキュリティポリシーを適用した．このセキュリティポリシーと実現方法について述べる。

キーワード
セキュリティ管理，セキュリティポリシー，システム管理，インターネット・サーバ，
地域ボランティア，地域サービス，地域活性化

1 はじめに

高岡短期大学は,地域との密接な連携の推進を特色の一つとして掲げ[1]，大学開放活動を積極的に行なっている。その中で，大学のインターネット機能を地域に開放することを目的として，インターネット・サーバを地域に公開する試みを1998年11月から行なっている。

公開サーバを構築して地域に開放する際の主要な問題点を以下に挙げる：

1. サーバの運用管理体制
   新たに設置する公開サーバを運営する人手が不足する
2. セキュリティ管理方法
   大学外からアクセスして利用するのでセキュリティ管理を強化する必要がある

これらの2つの問題点のうち，本論文では

[1] 産業情報学科

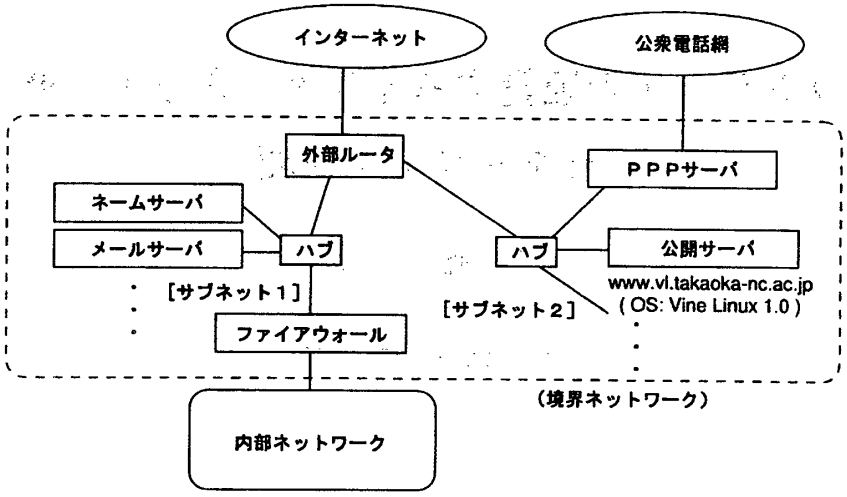

図1：公開サーバのネットワーク環境

主としてセキュリティ管理の問題をとりあげ，必要最小限のセキュリティ機能を確保しつつ利用者に最大限の自由を与えることを目的としたセキュリティポリシーとその実現方法について述べる。

2 セキュリティの前提条件

セキュリティの詳細に入る前に，その前提となる，公開サーバを接続するネットワーク環境とサーバの運用管理体制について述べる。

2.1 公開サーバのネットワーク環境

図1に示すように，高岡短期大学のネットワークはファイアウォールを境として内部ネットワークと境界ネットワークとに分かれ，境界ネットワークは外部ルータによりサブネット1とサブネット2に分割されており，公開サーバはサブネット2に属している。

境界ネットワークには，ネームサーバ，メールサーバ，WWWサーバ，PPPサーバ等が接続されている[2]。内部ネットワークはファイアウォールにより強固にセキュリティが守られているが，境界ネットワークは外部ルータを介して直接インターネットに接続している。このため，境界ネットワーク上のサーバはそれぞれ個別にインターネットからの侵入に対して備えなければならない構成となっている。

2.2 サーバの運用管理体制

ボランティアの管理者グループ

大学のシステム管理の人手はきわめて限られており，今後，数が増えていくことも予想される公開サーバの運用管理を大学だけで引受けることは非現実的である。そこで，システムの運用管理に興味を持つ地域のボランティアを募り，ボランティア管理者グループ(vladminグループ)を結成して運用管理を行なうことにした。

地域ボランティアのようなグループでシステム管理を行なう場合，

1．各メンバーの活動実施結果が不整合をおこすおそれがある
(例) 共通的なファイルを変更した場合には全体に影響を及ぼす
2．メンバーの技術レベルにばらつきがある
3．大学外からシステム管理を行なうのでセキュリティが緩くなるといった問題点がある。

これらの問題点を解決するために，

1．コミュニケーションの活性化
　グループのメーリングリストの活用，月例のミーティング
2．メンバー相互の技術的研鑽
　月例ミーティングでの学習活動
3．管理ツールやマニュアルの整備
4．セキュリティポリシーの作成

を行なってきた。

利用者の管理

大学の公共性の観点から，公開サーバの利用者を次のように設定した：

1．公共性が高く，地域と結びついた活動を行なうグループ及び個人
　(例)ボランティア活動のグループ
2．高岡短期大学の卒業生及び在校生(希望者)

日本ボーイスカウト富山県連盟がその一例である[3]。今後，利用者数が増大すれば公開サーバを分離・増設する計画をたてている。

利用者とvladminグループの対応は，1人のvladminメンバーにいくつかの利用者(グループを含む)を割当てるという方法を採用して利用者管理の負荷分散を計っている(図2参照)。

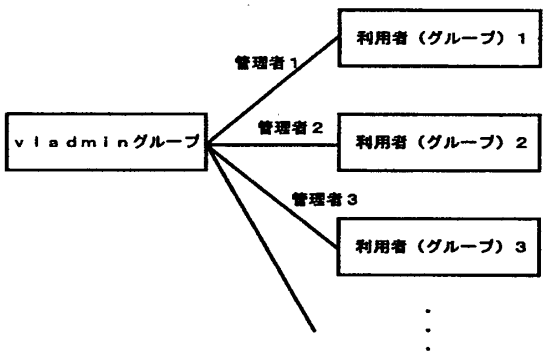

図2：ユーザの管理

3 セキュリティ計画

コンピュータ・セキュリティの問題は，第一にポリシーを設定することが重要である。なぜならば，どんなに時間やお金や人手をかけても，セキュリティ問題を完全に解決することはできないからである[4]。そのためには，セキュリティ問題を計画問題としてとらえ，目的と条件を明確にした上で，とるべき対策を明らかにして実装し，実行していく必要がある。これらの全体がセキュリティポリシーを形成する。

3.1 セキュリティ計画のステップ

セキュリティポリシーを作成するための指針であるRFC2196[5]によれば，セキュリティ計画のステップは次のようになる：

1. 守るべきものを明確にする
2. 何から守るかを決める
3. 可能性のある脅威を想定する
4. コストを抑えつつセキュリティ確保に必要な手段を実装する

以上のプロセスを常に見直し，弱点が見つかれば補強する

3.2 公開サーバのセキュリティ計画

守るべき対象

公開サーバで守るべき対象を以下のように設定した：

1. 利用者のWebドキュメント
　HTML文書，CGIプログラム等
2. 利用者の電子メール文書

想定される脅威

1. 外部からの侵入
　インターネットからの侵入を想定する。
　内部利用者による侵入には別途コミュニケー

ションの活性化のような人的な対策をとることで解決を図る。

2. システムの損傷
ハードやソフトのエラーによるシステムの損傷

目的と条件

RFC2196で述べられたアプローチを目的と条件の観点から整理すると，目的はコストの最小化であり，条件は守るべき安全の確保ということになる。公開サーバの場合は，はじめからコストを低く抑えることが前提となるため，コストは条件として扱う。この場合，コストに代って利用者の自由度を目的にする。つまり，次のような計画問題となる：

1. 目的
利用者の自由度を最大にする。また，利用者の使い方にできるだけ制限を設けない。
2. 条件
(a) インターネットからの侵入やシステムの損傷から，利用者のWebドキュメントやメール文書を守る。
(b) ボランティアの管理者グループがシステムを運営する。
(c) セキュリティ管理のための高価なソフトやハードを導入しない。

4 セキュリティ対策の実装

セキュリティ計画の実施段階として実装される種々の対策は，その機能によって，“protect”(防護)，“detect”(検知)，“react”(リアクション) の3つに分類できる[6]。公開サーバのセキュリティ対策として行なった，種々の設定やツールのインストール，及びツールの開発について述べる。

4.1 侵入に対する防護

インターネットからの侵入に対して防護するための対策は，現在最も盛んに取組まれている技術であり，防護を目的とした種々のツールの開発やソフトのバージョンアップが頻繁に行なわれている。

サービスの種類の制限

提供するサービスの種類を増やすと，セキュリティの複雑さが指数的に増大することが指摘されている[5]。そこでサービスの種類を表1のように限定した。

表1: サービスの種類

サービス	説明
TELNET	管理者グループが使用
FTP	Web データのアップロード用
SMTP, POP3	メールのサービス
WWW	Web のサービス

アクセス制御とユーザ認証

TELNET, FTP, POP3 に対するアクセス制御は TCP Wrapper [7]を用いて，表2のように行なった。

表2: TCP Wrapper によるアクセス制御

サービス	アクセスを許可するドメイン
TELNET	管理者グループのメンバーが使用するドメイン
FTP	全利用者が使用するドメイン
POP3	全利用者が使用するドメイン

SMTPとWWWについてのアクセス制御を表3に示す。SMTPではSPAMルール以外のアクセス制御を行なっていない。また，WWWの場合，特に厳密なセキュリティ・チ

表3: SMTP と WWW のアクセス制御

サービス	ソフト名称	説明
SMTP	sendmail-8.9.3	SPAM ルールの設定
WWW	Apache-1.3.6	システム管理ツール等へのアクセス

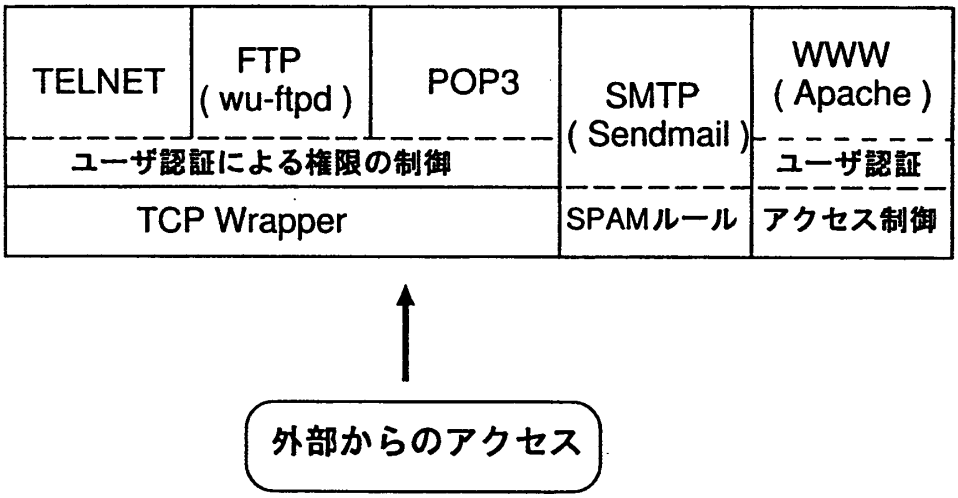

図３：アクセスと権限の制御

ェックが必要となるシステム管理ツール等へのアクセスに対しては，ユーザ名とパスワードによるユーザ認証とアクセス制御を併用してセキュリティのレベルを上げている。各サービスに対するアクセス制御とユーザ認証による権限の制御を図３にまとめて示す。

パスワード盗聴等の問題と対策

ユーザ名とパスワードによるユーザ認証では，パスワードがネットワークに流れ，盗聴されるという問題がある。また，パスワードが破られたり，パスワードの情報が洩れたりする可能性もある。パスワードがネットワークに流れても，暗号化すれば問題ないが，現状では，利用者が特別なソフトをインストールする必要があるなど，利用者に制限を課すことになる。そこで，利用者の便を優先して平文パスワードを採用することにした。

平文パスワードを用いる一方，セキュリティの弱さを補うために以下の対策をとることにした：

1．一般利用者が使用するFTPでは，自分のホームディレクトリの中だけしかアクセスできないようにする
2．一般利用者が自分でパスワード変更を行なうためのツールを開発する
3．公開サーバ以外の境界ネットワーク上のコンピュータについて，セキュリティ管理を厳しくする

一般利用者のパスワードが破られても，自分のホームディレクトリ以外にアクセスできなければシステム全体への影響は小さく抑えることができる。この機能は，wu-ftpd[9]を使い，利用者はguestgroupに登録することで実現した。

```
( /etc/passwd file )
user:*:200:500:: \
  /home/ftponly/./user:/etc/ftponly
( /etc/group file )
ftpgrp:*:500:
( /etc/ftpaccess file )
guestgroup ftpgrp
```

図４：ftpのアクセス制限

図4に wu-ftpd に関する設定例を示す。/etc/passwd 及び/etc/group ファイルでは，利用者のアカウントを“user”，グループを“ftpgrp”としている。/etc/ftpaccess ファイ

ルに, "guestgroup ftpgrp"と指定することで, 利用者は "/home/ftponly"ディレクトリより上にアクセスできなくなる。また, 利用者のシェルとして実在しない "/etc/ftponly"を指定することで, 利用者はTELNET を使えなくなる。しかし, TELNETを使えないと利用者が自分でパスワードを変更できなくなるので, Web上からパスワードを変更するツールを作成した(第5節参照)。図中, 紙面の制約から, 長い行には適宜改行を挿入し, 挿入位置は行末の "＼"で表わした。以後の図中の設定ファイルやスクリプトでも同様の表記法を用いる。

また, 境界ネットワーク上にセキュリティの弱いマシンがあって侵入を受けると, パスワードの盗聴が行なわれ易く, また, TCP Wrapperによるアクセス制御も効果がなくなるので, 同一ネットワーク上で1つでもセキュリティの弱いマシンを作らないことが重要である。

```
( access.conf file )

<Directory /home/httpd/html/adm>
Satisfy all
order deny,allow
allow from .domain1.ac.jp
allow from .domain2.co.jp
allow from .domein3.ne.jp

Authtype Basic
AuthName wwwadmin
AuthUserFile /etc/www/wwwadmin
require valid-user
</Directory>
```

図5：Web サーバの設定例

Webサーバのアクセス制御と認証

公開サーバで用いるWebサーバソフト(Apache-1.3.6)はアクセス制御とユーザ認証の機能を持つ。これらの機能を, パスワード変更やログ監視のようなシステム管理を行なうWebドキュメントへのアクセスに用いる。図5にApache で採用しているアクセス制御と認証の設定例を示す。

セキュリティホールの対策

新しいセキュリティホールが次々と発見されるので, JPCERT/CC(コンピュータ緊急対応センター)[9] のようなセキュリティ関連組織の情報に注意してセキュリティホールのないソフトへのバージョンアップを心掛ける。

セキュリティ関連ファイルの保護

パスワードファイルやTCP Wrapperの設定ファイル(/etc/hosts.allow, /etc/hosts.deny)のような, セキュリティ関連のファイルに関してはシャドウ・パスワードを採用したり, ファイルの許可モードを変更することにより, 一般ユーザ権限で読めないようにする。

管理者グループのメンバー数と地域の制限

ボランティアのシステム管理者グループ(vladmin) のメンバーは現在7名であり, 全員が高岡市近郊に在住している。インターネットの接続には大部分が地元のインターネットプロバイダーや企業を利用している。従って, メンバー数とメンバーの在住地域を制限すればメンバーがアクセスしてくるドメインの範囲も狭くなるので, アクセス制御で設定を許可する範囲を狭く設定できることになり,かなり強力な防護が可能となる。

対策のまとめ

侵入に対する防護の対策をまとめて図6に示す。

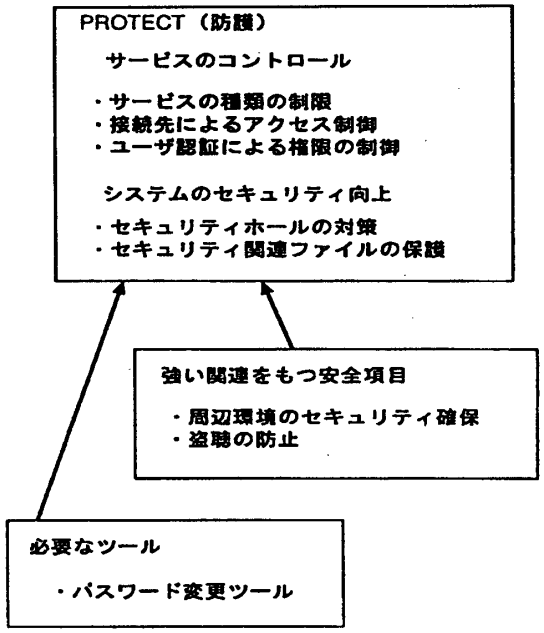

図6：防護対策のまとめ

4.2 侵入の検知

侵入に対する防護機能を補う意味で，侵入検知は重要である。検知の機能は以下のようにまとめられる：

1. ログの監視
2. 異常の監視
3. 不正アクセスの検知

ログの監視

監視すべき主なログには以下のものがある(ただし，Linuxの場合)：

1. lastコマンドの出力
2. /var/log/secure
3. /var/log/messages
4. /var/log/maillog
5. /var/log/xferlog
6. Webサーバのアクセスログ

/var/log ディレクトリのファイルは基本的にスーパーユーザのみがアクセスできるので，必要に応じてシステム管理者が TELNET でログインして中を見るにとどめた。lastコマンドは一般ユーザの権限で実行でき，ログインした情報が得られるので，Web上から実行できるようにした。ただし，アクセスできるのはシステム管理者のみとし，アクセス制御とユーザ認証を併用してセキュリティの確保を計った。

Webサーバのアクセスログは量が多いので，ログ解析ツール等を使った見易い表示を行なう予定である。

異常の監視

侵入されてしまった場合は，一刻も早く侵入の事実を知ることが大切である。CERT が提供している侵入検知するためのチェックリスト[10] には10のチェック項目が掲載されている。その中で，容易に定型的なチェックが可能な項目として以下を取り上げ，チェックを実行するシェルスクリプトを作成した。

1. root に setuid したファイル及び kmem に setgid したファイルの監視
2. 異常な名前を持つ隠しファイルの検出

侵入者はシステムを操作するために setuid や setgid を行なったファイルを作成したり，持ち込んだファイルを隠すために通常と異なった名前の隠しディレクトリを作成することがよくある。これらのファイルやディレク

```
#! /bin/bash
# init.sh
echo "Initializing Set UID & Set GID files ..."
find / -user root -perm -4000 -printf "%p %Cx\n" \
                              > /var/log/suid.txt
find / -group kmem -perm -2000 -printf "%p %Cx\n" \
                              > /var/log/sgid.txt
echo "done
```

```
#! /bin/bash
# check.sh
echo "Checking Set UID & Set GID files ..."
find / -user root -perm -4000 -printf "%p %Cx\n" \
                              | diff /var/log/suid.txt -
find / -group kmem -perm -2000 -printf "%p %Cx\n" \
                              | diff /var/log/sgid.txt -
echo "done"
echo "Checking Doubtful Names ..."
find / -name ".[^0-9a-zA-Z]*" -print | cat -v
echo "done"
```

図7：侵入検知用シェルスクリプト

トリを検出するために作成したシェルスクリプトを図7に掲げる。

図7には2つのスクリプトが載せてある。最初のスクリプト(init.sh)は, setuid や setgid されたファイルを探して /var/log/suid.txtと /var/log/sgid.txt に書き出す。2番目のスクリプト(check.sh)は, init.sh を実行した後で, setuid/setgid されたファイルが変更されたり, 追加・削除されていないかチェックする。また, 通常とは異なる名前の隠しディレクトリやファイルの存在を探索する。一度 init.sh を実行した後, 定期的に check.sh を実行することである程度の異常検知が可能となる。

不正アクセスの検知と通報

侵入者はシステムの弱点を探すために, 対象となるコンピュータに対してポートスキャンを行なうことが多い。従って, できるだけ早くポートスキャンを察知できれば警戒を強めるなどの対策をとりやすい。不正なポートスキャンの情報は, TCP Wrapperのアクセス拒否としてログに記録されるが, メールでポートスキャンの事実を連絡することができれば早期に知ることができる。

図8に不正なアクセスをメールで知らせるための, /etc/hosts.deny ファイルの設定例を示す。図中の name@domain が連絡先のメールアドレスを表わしている.

```
ALL: ALL: \
spawn (/usr/sbin/safe_finger -l @%h \
| /bin/mail -s %d-%h name@domain) &
```

図8：不正アクセスの通報

4.3 侵入に対するリアクション

侵入を発見した後の処置は次のようにまとめられる：

1. 緊急時の連絡先(Point of Contact)へ連絡
2. JPCERT/CCなどのセキュリティ対応組織へ報告
3. ネットワークとの接続解除
4. 侵入状況の分析とデータ収集
5. システムの初期化(ほとんどの場合)
6. システムの復帰

緊急時の連絡と報告

RFC2196には 特定の連絡先(Point of Contact)を設定しておき, 異常時にはそこへ連絡することが力説されている。公開サーバについては, vladminメーリングリストをこの連絡先として設定した。

次にセキュリティ対応組織へ報告する。JPCERT/ CCのホームページ[9]には詳細な連絡方法や報告様式が載っているので, これを参照して連絡をとる。

接続解除とデータ収集

侵入を検知した場合は, まずネットワークとの接続を解除することが重要である[11]。次に, JPCERT/ CC等と連絡をとりながらデータを収集して分析してもらう。

システムの復帰

システムを復帰する場合, まず全体を初期化して最初からインストールし直すのが最も安全な方法である。そのためには, 普段から必要なデータのバックアップを実行していなければならない。

システムのバックアップ

第3.2節で述べたように, 公開サーバで守るべき対象は, 利用者のWebドキュメントと電子メール文書である。これらは主に /home 及び /var/spool/ mail ディレクトリに含まれているので, これらのディレクトリを中心にしてバックアップを行なう。図9に GNU tar[12]によるテープバックアップ用スクリプトの例を示す。

図中, /etc/tar_exclude/root ファイルにバ

```
#!/bin/sh
cd /
tar --verify -cf /dev/st0 \
 -X /etc/tar_exclude/root . \
 > /var/log/bup_root
```

図9：バックアップスクリプトの例

ックアップから除外するディレクトリやファイル名を記載する。また，ベリファイされた結果は /var/log/bup_root ファイルに記録されるようになっている。このスクリプトは cron に登録し，定期的に実行される。

5 パスワード変更ツールの作成

5.1 作成の経緯

TELNETを利用できない一般利用者がパスワードを自分で変更するために，Web上からパスワードを変更するためのツールが必要となる。このようなツールとしては パスワードコマンドをCGI経由で実行するxpasswd [13] 等があるが，必ずしも十分に種々のOSやバージョンに対応し切れていない。passwdコマンドの出力はOSやバージョンによっても細かい差があるため，この出力結果を利用する汎用のソフトを維持していくのは大変手間がかかる。

一方，最近のLinux等のログイン認証には，PAM [14] に準拠した標準的な認証方法が用いられるようになってきた。そこで，パスワードコマンドではなく，Linux-PAM の関数 [15] を直接用いて，Web上からパスワードを変更するツールを作成した。PAMの関数を利用することでプログラムが簡潔になり，セキュリティに関して誤った処理が入り込む危険性が少ないと思われる。

5.2 プログラムの概要

図10にパスワード変更ツールで起動されるプログラムの流れを示す。

Webサーバとして用いた Apache-1.3.6 は，

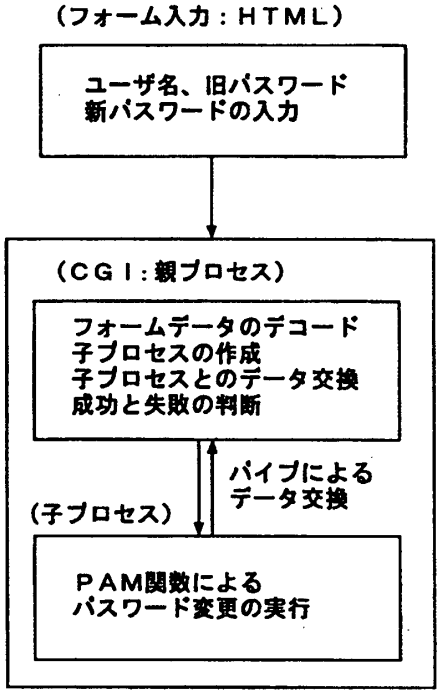

図10：プログラムの流れ

セキュリティ上の理由から root に setuid したプログラムをCGIとして実行することを許していない。一方，パスワードを変更するPAM関数である pam_chauthtok() は root権限がなければ実行できない。そこで，図10のように，一般ユーザ権限の親プロセスをCGIとして実行し，この親プロセスから root に setuid したプログラムをfork/exec して実行することにした。

セキュリティを向上させるため，親プロセスとなるCGIプログラムはC言語で記述した。

親プロセスと子プロセスの間で交換されるデータは以下の通りである：

1. 親プロセス → 子プロセス
   (a) ユーザ名
   (b) 旧パスワード
   (c) 新パスワード
2. 子プロセス → 親プロセス
   (a) ユーザ名のチェック結果
   (b) PAM関数が出力するメッセージ

なお, 子プロセスでは, 入力されたユーザ名をチェックして, 存在しないユーザ名及びスーパーユーザ名(root)は受けつけないようにしている。

実行例

1. 認証ダイアログ(図11)
   ユーザ名,旧パスワード,新パスワードの入力
2. 実行結果(図12)

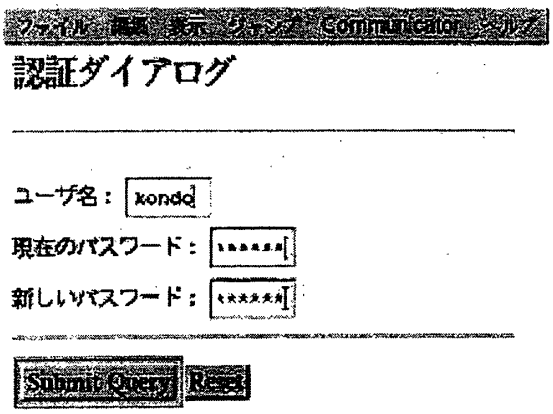

図11：認証ダイアログ

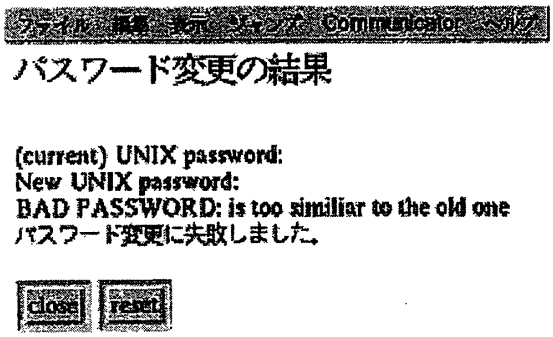

図12：実行結果の例

実行結果は,親と子のプロセス間でのデータのやりとりを含め,親プロセスが出力する。

6 ボランティアによる運営について

複数の地域ボランティアがグループで運営することによる得失や問題点について考察する。

6.1 セキュリティへの影響

マイナス面とその対策

セキュリティに対するマイナス面は, 次の要素が原因となっている：

1. 外部からのtelnet等によるアクセス
2. 複数の管理者
3. 管理者の技術レベルのばらつき

これらの要素により, セキュリティが低下する可能性のある項目を以下に示す：

1. 複数の管理者が外部からアクセスするでアクセス制御の対象が広くなり, チェックが緩くなる
2. 複数の管理者が非同期で管理作業を行なうので, 作業の結果が他の管理者にとってセキュリティの低下を招く恐れがある
3. スーパーユーザの権限で誤操作する可能性がある

項目 1 に対しては, TCP Wrapper等によるアクセス制御のデータを正しく管理する, ログ監視を強化する等の対策をとる必要がある。また, 1 つのサーバーを管理する管理者数を制限して, アクセス制御の記述があまりにも複雑化しないように配慮することが有効と思われる。

項目 2 及び 3 に対しては, グループの間でのコミュニケーションを活発にするとともに, 技術レベルを均一化するための学習活動が必要になる。

プラス面

セキュリティに対するプラス面は，頻繁に違った角度から監視が行なわれ得る点である。一人あるいは少数の同じような環境にある管理者の場合は，同じような思考形態であるため，監視の盲点が生まれやすい。実際にインターネットからの侵入があったときに，最初に異常に気づいたのは著者以外のボランティア管理者であった。このプラス面はかなり大きいと考えられる。

6.2 管理者の権限

ボランティア管理者を募った最大の目的はシステム運営の負荷分散である。ボランティア管理者間での権限に大小があると，大きな権限を持つ管理者に責任が集中することになり負荷の分散が実現されにくい。そこで，管理者間の権限は平等とし，メーリングリストと月1回のミーティングの中ですべてを決定する体制をとった。

今後，更に管理者グループの規模が増大した場合には，サーバーの数も増加することが予想されるので，分散的な管理形態を損なわずに大きな規模に対応できる体制を考えていく必要があると思われる。

7 結　言

地域活動の支援と地域の活性化促進を目標として，高岡短期大学の境界ネットワーク上に公開インターネットサーバを構築して約1年間運営してきた。

利用者ができるだけ自由に使用できることを旨としてセキュリティ管理を行なったが，開始後半年目にインターネットから侵入を受け，セキュリティ管理方法を全面的に見直して再出発した。

これらの経験を踏まえ，利用者に必要最小限度の制約を課しつつ，インターネットからの侵入を防ぐためのセキュリティポリシーをまとめ，必要なツール等も開発した。

現在，ネットワークを流れるパスワード等のデータの暗号化を検討している。すでに，Secure Shell[16] 等のシステムが開発されており，今後，広く使用されるようになると思われる。現状ではこれらのシステムに対応したソフトが一般的に広く使われるまでには至っていないが，折を見て導入したい。

今後の課題として，公開サーバが複数に増え，ボランティア管理者の数が増えた場合の，セキュリティ管理方法について取組んでいきたい。

謝　辞

最後に，本研究を進めるにあたって種々のアイデアを提供し，テストに協力していただいたボランティア管理者グループ vladmin の方々，及び，セキュリティに関して数々の助言をいただいた JPCERT/CC の方々に厚

引用文献

1）高岡短期大学ホームページ，
http://www.takaoka-nc.ac.jp/tnc/shomu/aims.HTM

2）近藤：内部情報の保護と外部への公開を 統合したネットワークの設計と構築，高岡 短期大学紀要，第10巻 (1997)

3）日本ボーイスカウト富山県連盟ホームページ，
http://www.vl.takaoka-nc.ac.jp/~bstoyama

4) S.Garfinkel, G.Spafford : Practical UNIX &Internet Security - 2nd Edition, Chap.2, O'Reilly & Associates, Inc. (1996)
5) B.Fraser et al.: Site Security Handbook, RFC2196 (1997)
6) B.Panda, J.Giordano: Defensive Information Warfare, Communications of the ACM,Vol.42 No.7, pp31-32 (1999)
7) CERT Coordination Center: List of Security Tools (1997)
ftp://info.cert.org/pub/tech/tech_tips/security_tools
8) wu-ftpd のホームページ,
http://www.wu-ftpd.org/
9) JPCERT/CC のホームページ,
http://www.jpcert.or.jp/
10) CERT Coordination Center: Intruder Detection Checklist (1997)
ftp://info.cert.org/pub/tech/tech_tips/intruder_detection_checklist
11) E.Guttman et al.: User's Security Handbook, RFC2504 (1999)
12) GNUプロジェクトのホームページ,
http://www.gnu.org/
13) xpasswd のホームページ,
http://www.bento.ad.jp/~fujiya/Lib/
14) V.Samar, R.Shemers: Unified Login with Plaggable Authentification Modules (PAM), RFC86.0 (1995)
15) A.G.Morgan: The Linux-PAM Application Developers' Guide, DRAFT-v0.63 (1998)
16) Secure Shellプログラム・ユーザグループのホームページ,
http://www.ssh.org/

A Security Policy of an Internet Server Managed by Local Volunteer Administrators

Kiyoshi KONDO

(Received October 15, 1999)

ABSTRACT

An attempt to keep an Internet server open to local peple has been carried out as a community service of Takaoka National College. The reduction of man power required for system administration and the security management of computers on the perimeter network are important problems. Volunteer administrators were invited to reduce the burden of administrators of our college. An Internet server was established and has been operated for about one year under the administration of the volunteers. As the security of entire system is determined by the weakest link, a certain level of security should be kept for every stage of security actions, that is, "protect", "detect" and "react." Too strong security often leads to too many limitations on users' operations, discouraging users from using the server. So a security policy which aims at allowing the largest freedom on users as well as keeping the minimum required security of system was introduced based on the experiences of actual operation. This paper describes the security policy and its implementation.

KEY WORDS

security management, security policy, system administration, internet server, local volunteer, community service, promotion of local society