ISSN 0917－3668
1993. 3. 31

KUINS ニュース No. 15

京都大学学術情報ネットワーク機構

犬山地区に設置されている IP ルータ（写真右側）とメール用ワークステーション（同左側）

目　　次

KUINS の対外接続について …… 126
ターミナル・サーバの運用について …… 127
TSS オンライン目録検索のマニュアル改訂について …… 129
ネットワークセキュリティについて（パスワード編） …… 130
ネットワークセキュリティについて（システム編） …… 132
KUINS 会議日誌 …… 136

KUINS の対外接続について

学術情報ネットワーク機構

KUINS は，インターネットに接続することによって国内外の IP ネットワークに対してアクセスできるようになっており，この接続は遠隔ログインやファイル転送，電子メールなど様々な形で利用されています。現在，KUINS は NCA 5，JAIN，WIDE，GENOME/TISN，SINET の 5 つの広域あるいは地域ネットワークに直接接続されており，他大学，他研究組織あるいは国外のいろいろな組織等に対して，適宜これらを経由してアクセスできるようになっています。（ネットワークとしての JAIN は発展的に解消し，地域ネット等に変貌しつつありますが，ネットワーク研究としての JAIN の活動は，大学ばかりでなく企業をも含んだ JAIN Consortium という形で継続されています。興味のある方は jc-request@jain.ad.jp までご連絡下さい。）

これまでは，これらの広域ネットワークに対する接続に用いるルータと呼ばれる装置がそれぞればらばらに設置されていたため，ネットワーク間の整合を取ることが難しい場合がありました。そこで，今回 KUINS の基幹ループ LAN 上に新たに論理的なセグメントを設け，このセグメントに

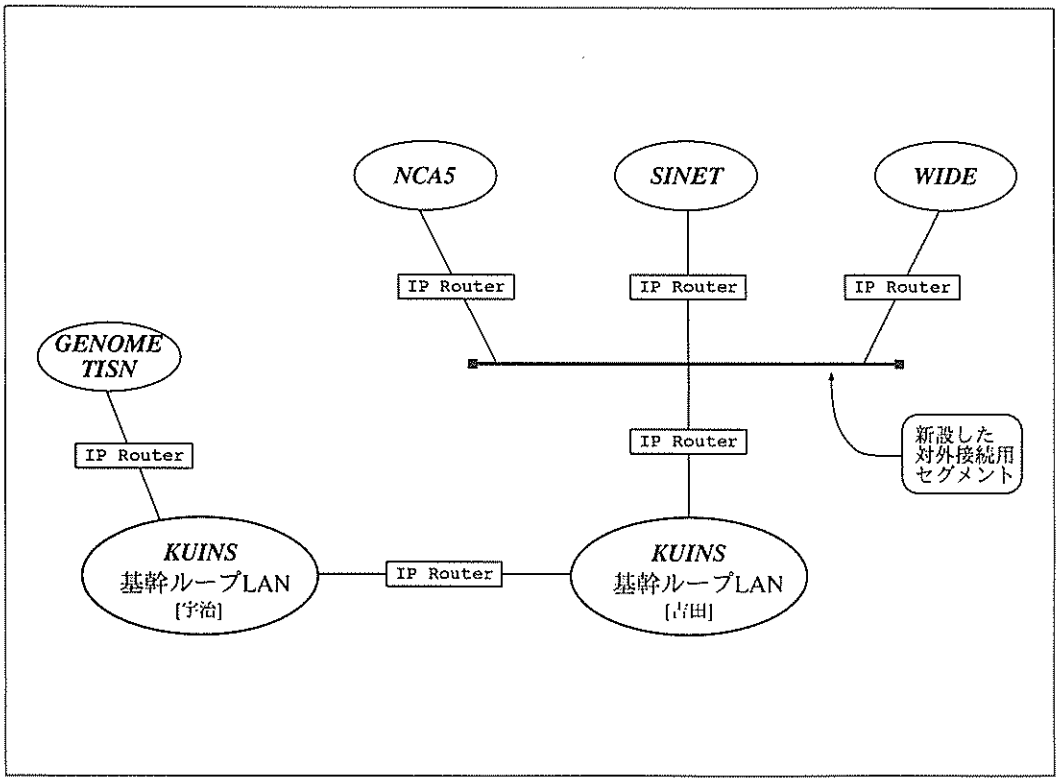

図 1　KUINS の IP 接続構成（一部）

すべてのルータを接続することによって統一的な学外へのアクセスを提供することになりました。今後は，KUINSにおけるすべての対外接続用ルータは，これまでの基幹ループLANではなく新設のセグメントに接続され，外部とのすべての通信はこれら2つの間をつなぐルータを経由して行なわれることになります。（ただし，GENOME/TISNとの接続については吉田地区と宇治地区を接続する学内接続用ルータを経由するため，当面例外的な扱いとなります）

対外接続用のセグメントにルータを移設した後も，一般ユーザの皆様のご利用にあたっては特に変化はありませんが，一部パソコン用イーサネットボード等においてルータを静的に設定しているような場合には変更が必要となることがあります。

我々は，この構成変更によって，直接目には見えないかも知れませんが，より信頼できる充実した通信サービスが提供できるものと考えています。

なお，学外とのIP接続を予定されている場合には，KUINS利用者に対する混乱を避けるため，あらかじめ学術情報ネットワーク機構までご相談下さいますよう改めてお願い申し上げます。

ターミナル・サーバの運用について

学術情報ネットワーク機構

学内のTTY端末等からKUINS-LANに接続する為のゲートウェイの運用を行っていましたが，今回，学外からもKUINS-LANに接続ができる様になりました。これによって，学外から電話回線を利用してKUINS-LANに接続されたワークステーション等にアクセスすることが可能となります。

(1) 必要な設備

ターミナル・サーバを利用するには，端末となるコンピュータと，コンピュータとターミナル・サーバを電話回線を経由して接続する為のモデムが必要です（図1参照）。

コンピュータは，RS232C等のシリアルポート

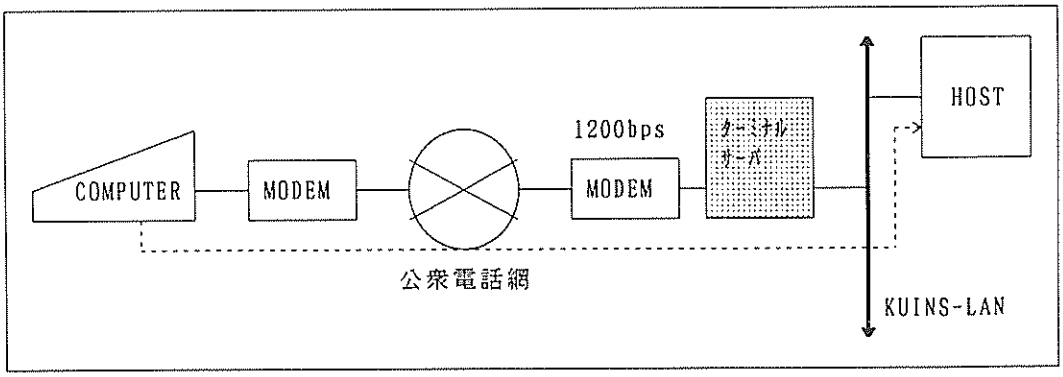

図1 接続例

を装備しているもので，シリアルポートを使用した通信ソフトを装備している機種が必要です。

モデムは，CCITT 勧告の V.22（非同期全二重 1200 bps）をサポートしているものが必要です。

(2) 端末の通信環境の設定

ターミナル・サーバに接続する時の，端末側の通信環境は表 1 の様にして下さい。設定の方法は各通信用ソフトによって異なりますのでマニュアルを参照して下さい。

(3) ターミナル・サーバへの接続

設定が終わったらターミナル・サーバに接続してみましょう。モデム及び通信ソフトにオートダイヤル機能があればそれを利用して，なければ電話機でターミナル・サーバにダイヤルします（表 2 参照）。

正常に接続できたら，一度リターンキーを叩いて下さい。すると，ターミナル・サーバと接続されログインプロンプトが表示されます。接続できない場合や，文字が化ける場合は設定を確認してみてください。

(4) ターミナル・サーバへのログイン

ログインプロンプトがでたらログイン名 telnet でログインして下さい。正常にログインできれば図 2 の様に表示して IP アドレスの入力プロンプトが表示されます。

表 1　通信環境

通信速度	1200 bps（全二重）
データ長	8 ビット
パリティ	なし
ストップビット	1 ビット
フロー制御	RS/CS（ハードウエア）

表 2　ターミナル・サーバのアクセス番号と回線数

CS のアクセス番号	075－753－7849
回線数	4 回線

```
login: telnet [CR]

################  Nice to meet you !!!  ################
I am yoshida-telephone-station sigma station (130.54.6.1).


##################################################
######          Executing TELNET command          ######
##################################################

Please input IP-NO. ?
```

図 2　ターミナル・サーバへのログイン

(5) ホストマシンへの接続

大型計算機センターのUXP（130.54.9.11）への接続例を図3に示します。

UXPと接続が完了して，ログインプロンプトが表示されました。接続完了後は各ホストマシンの利用方法に従って下さい。

(6) ターミナル・サーバの利用終了

ターミナル・サーバから接続したホストをログアウトするとターミナル・サーバと端末間の電話回線もターミナル・サーバ側から切断されます。

(7) 注意事項

ターミナル・サーバからは，本学のネットワークアドレス（130.54及び133.3）を持つホストにだけ接続することができます。

ターミナル・サーバには，電話回線から誰でもアクセスすることができる為，不正なアクセスをターミナル・サーバの上で防止することは不可能です。KUINS-LANに繋がれている各ホストマシンの管理にはこの事を充分に認識して不正アクセスの防止に努力するようにお願いします。

```
Please input IP-NO. ?  130.54.9.11 [CR]
Trying . . .
Connected to 130.54.9.11.
Escape character is ' ^]'.


UXP/M TELNET (sakura)

login :
```

図3　UXPへの接続例

TSSオンライン目録検索のマニュアル改訂について

附属図書館でTSSオンライン目録検索サービス（OPAC/TSS）を開始してから，2年が経過しました。長らく暫定版のマニュアルでご利用いただいておりましたが，このたびマニュアルを「TSSオンライン目録検索（OPAC/TSS）利用マニュアル　—研究室からの蔵書検索—」第1版として改訂，発行いたしました。全体として見やすいものとなるよう心がけて編集いたしました。

上記OPAC利用マニュアル（第1版）をご希望の方，およびOPAC/TSSをご利用になりたい方は附属図書館1階⑦番カウンター（参考調査）までお申し出ください。

附属図書館参考調査掛，システム管理掛

ネットワークセキュリティについて（パスワード編）

石 橋 勇 人

このニュースでお伝えしましたように，この度，モデム経由でKUINSにアクセスできる端末サーバを用意しました。これによって，外部からKUINS基幹ループLANに接続されたワークステーションなどのIP機器にアクセスできるようになりますが，このことは，裏を返せば外部からの侵入経路ともなり得ることを意味します。

もちろん，これまでにも研究室などでこのような装置を用意されているところは多いでしょうし，モデム以外の侵入経路もあるわけですから，これまでにも危険がなかったわけではありませんが，今度の場合には電話番号がこうしてかなりの範囲に広報されますので，ネットワークに接続された各マシンのセキュリティには今まで以上に配慮するように心がけて下さい。

特にパスワードには十分な心がけが必要です。パスワードなしのユーザ名や，ユーザ名と同じパスワードなどは絶対に避けなければなりません。一般に，侵入者はあるアカウントに侵入するとそれを隠れ蓑にして次々と別のマシンへの侵入を繰り返しますから，あなたのアカウントが破られることは，あなた1人だけの問題ではなく，全世界のネットワークに被害を広げるおそれがあるのです。

少し脅かしましたが，パスワードをきちんと管理しておけば，それだけでかなり安全性は高くなります（少なくとも端末サーバ経由で破られることはないでしょう）から，決してパニックする必要はありません。

"Practical UNIX Security"
Simon Garfinkel and Gene Spafford
O'Reilly & Associations, Inc.
1991

という本から，良いパスワード，悪いパスワードの例を翻訳・引用しておきます。（この本はUNIXシステムのセキュリティに関して大変参考になりますので，特にシステム管理者の方は一度御覧になると良いでしょう。）

良くないパスワード

あなた自身の名前
配偶者の名前
両親の名前
ペットの名前
子どもの名前
親友や同僚の名前
お気に入りのキャラクタの名前
上司の名前
とにかく誰かの名前
使っているOSの名前
あなたの計算機のホスト名
電話番号

車のナンバー
社会保険番号の一部
誰かの誕生日
その他あなたについて容易に得られる情報
wizard, guru, gandalf などの単語
その計算機に登録されている計算機のユーザ名（頭を大文字にしたり，２度繰り返したもの等も含む）
英語の辞書にある単語
外国語の辞書にある単語
地名
適当な名詞
同じ文字ばかりのパスワード
キーボード配列通りのもの（例　qwerty）
上のいずれかの逆順
上のいずれかの先頭あるいは最後に数字を付けたもの

良いパスワード

大文字と小文字を両方含むもの
数字や句読点を含むもの
憶えやすいもの——書き留めずにすむから
７～８文字の長さのもの
素早くタイプできて，誰かが後ろから見てもわからないもの

良いパスワードのためのヒント

２つの短い単語の間に記号や数字をはさむ
　　robot4my, eye-con

あなただけがわかる略号を使う
　　Notfsw (None of This Fancy Stuff Works)
　　AUPEGC (All UNIX programmers eat green cheese)

（もちろん，robot4my, eye-con, Notfsw, AUPEGC はここに書いてあるから悪いパスワードである）

いかがですか？　世の中にはパスワード破りのプログラムがすでに PDS として出回っていて，しかも，かなり強力です。とあるプログラムを使うと，特に何も考慮していない一般ユーザのパスワードを対象にした場合，その３～４割ほどは簡単に解読することができます。このプログラムにかかれば，辞書にのっている（プログラムが知っている）単語の前後に数字をつけたり，l(エル)を１(いち)に置き換えるというような小細工はほとんど無意味です。少しチューニングすれば，解読される割合はもっと高まることでしょう。今や，外国であっても日本語や日本人の名前を含んだ辞書は簡単に手にはいりますから，日本語の単語（ローマ字）だからといって安心してはいけません。

これを読んだらすぐにあなたのパスワードをもう一度チェックすることをお勧めします。それがあなたとすべてのネットワークユーザの平和のためなのです。

ネットワークセキュリティについて（システム編）

石橋勇人，櫻井恒正

ネットワークに接続された計算機のセキュリティについて，パスワードに関する注意を述べましたが，今度はUNIXシステムの設定に関する注意事項をとりあげておきます。以下に掲げるのは，CERT Coordination Centerが出している"Generic Security Information"（1992年9月18日付）のうち，関連する部分について翻訳・引用したものです。

CERT/CC 一般的なセキュリティについての情報

1992年9月18日

以下に述べる情報は，次のふたつの場合に役立つものである。

1） すでに侵入された経験がある，あるいは侵入された可能性があるサイトに対する手助け

2） まだ侵入された経験がないサイトが，セキュリティの評価をするときの手助け

セクションAでは，システムが傷つけられているか否かを決定する方法をいくつか列記する。セクションBとCは，それぞれ，UNIXとVMSの侵入者によって利用されたことのある弱点を列記する。セクションDは，システムの安全を保つために利用できるルーツについて記述する。

このドキュメントの情報は，いくつかの形の侵入を防ぐために利用できる。我々はシステム管理者にこのドキュメントの全セクションを再検討し，それに従って潜在的な弱点をなくすようシステムを変更することを推奨する。

A．システムが傷つけられたか否かを決める方法

1．lastログ，プロセスアカウント，syslog，C2セキュリティ用ログなどを調べ，変わった場所からのログインやおかしな活動がないかを調査せよ。これはそれほど簡単なことではないことに注意せよ。というのは，多くの侵入者は活動を隠そうと企てて，アカウンティングファイルを編集するからである。

2．おかしな，あるいは隠されたファイル（ピリオド(.)から始まっていて，通常lsコマンドでは表示されないファイル）がないかどうか，システムのあらゆるところを調べよ。これらは，パスワード破りのプログラムや他のシステムのパスワードファイルなどの情報を隠すために使われることがある。UNIXシステムでよく使われるトリックは，変な名前（'...'や'.. '(dot dot space space)や'..^G'(dot dot control-G)など）の隠されたディレクトリを利用者のアカウントのもとに作ることである。'.xx'や'.mail'などの名前が付けられたファイルが使われたこともある。

3．システムのあらゆる場所について，set-uidされたファイルを探しなさい。侵入者はしばしば，後からrootでアクセスできるように/bin/sh周辺のコピーにset-uidしたものを残しておく。UNIXのfindプログラムを使うと，rootにset-uidされたファイルを捜し出すことができる。次の例は，/(ルート)ディレクトリ以下のrootにset-uidされたファイルを捜し出そうとする例である（findコマンドは，シンボリックリンクはたどらないことに注意)。

```
find / -user root -perm -4000 -print
```

4．システムのバイナリーファイルが変更されていないことを確かめよ。これまでに我々は，侵

入者がUNIXシステムのloginやsu, telnetその他の危険なネットワークやシステムのプログラムを変更したのを見てきている。VMSシステムでは，侵入者によってloginout.exeやshow.exeのようなプログラムが変更されたことがある。システムのバージョンを，最初にインストールしたテープのように正しいと分かっているものと比較せよ。バックアップには用心しなさい。バックアップにもトロイの木馬が入っているかも知れない。

5．cronやatによって実行されるすべてのファイルを調べよ。侵入者がcronやatから実行されるファイルに裏口を残した例がある。これらのテクニックは，あなたが侵入者を追い払った後でさえも，彼らがシステムにもどってくることを可能にする。また，cronやatから実行されるジョブから（直接あるいは間接的に）参照されるすべてのファイルやプログラム，およびジョブファイル自身が誰にでも書き込めるようになっていないことを確認せよ。

6．/etc/inetd.confに不正な追加や変更がないか調査せよ。特に，シェルプログラム（例えば，bin/shや/bin/csh）を実行するすべてのエントリーを捜し出せ。また，/etc/inetd.confで指定されているすべてのプログラムが正しく，また，トロイの木馬によって置き換えられていないことを検証せよ。

7．システムやネットワークの定義ファイルに不当なエントリーがないか調べよ。特に，'+'や自分たちのものでない不適切なホスト名が/etc/hosts.equiv，/etc/hosts.lpdおよびすべての～/.rhostファイル（特に～rootや～uucp，～ftp，その他システム用アカウント）にないかどうか調べよ。これらのファイルは，誰にでも書き込み可能であってはならない。さらに，これらのファイルがいかなる侵入よりも以前から存在し，侵入者によって作られたものではないことを確かめよ。

8．侵入の兆候を捜索するときには，LAN上のすべてのマシンを調べよ。特に，NIS(YP)やNFSによる共有を行なったり，/etc/hosts.equivファイルから参照されているホストをチェックせよ。また，ユーザが.rhostで互いに参照しているすべてのホストもチェックせよ。

9．システムの/etc/passwdファイルを調べて，アカウントに何か追加や変更がないかチェックせよ。特に，不当に新しく作られたアカウント，パスワードのないアカウント，既存のアカウントのUIDの変更を調べよ。

B．過去に利用されたUNIXシステム設定上の問題

1．弱いパスワード

侵入者は，fingerやruserを使ってアカウント名を見つけ出し，単純なパスワードを試してみることが多い。利用者に対して，推測しにくいパスワード（たとえば，どんな言葉のどんな辞書にものっていない単語，有名な実在あるいは架空のキャラクタの名前も含めてちゃんとした名詞でないもの，計算機の専門家にとって常識的な略号でないもの，姓・名の単純なバリエーションでないもの）を選ぶよう勧めなさい。さらに，利用者に対して，ユーザ名/パスワードの情報をいかなるシステム上のファイルにも通常のテキストとして書き残さないように伝えなさい。

パスワードを選ぶためのよい方法の1つは，"By The Dawn's Early Light"のように憶えやすい文句を選び，最初の文字を取ってパスワードにすることである。句読点を入れたり，大文字小文字を混在させたりもしなさい。上の文句の場合は，たとえば，"bt}DeL{"のようにすればよい(決してこの例をそのままパスワードとして使わないように)。

侵入者は，パスワードファイルを手に入れたなら別の計算機へ持っていってパスワード推測プログラムを走らせることだろう。そのようなプログラムは，大きな辞書を探すことによって遅い計算

機であっても素早く実行することができる。多くのサイトの経験では，パスワードの形に何も制約をつけていないほとんどのシステムには簡単にわかるパスワードが少なくとも1つはある。

もし，パスワードファイルが取られたと思うなら，システム上のすべてのパスワードを変更しなさい。最小限，システム関係のパスワードはすべて変更しなければならない。なぜなら，十分適切と考えられるパスワードでも，侵入者はそれらを集めて推測できるかも知れないからである。

セクションDでは，ユーザが「良い」パスワードをつけていること，システムユーザにとってそれらが見えてしまわないこと，を確かめる手段について述べている（訳注：原文では，COPSというプログラムについて数行の紹介がある。COPSは主要なanonymous ftpサイトから入手できる）。

2．TFTPを使ってパスワードファイルを盗む

この弱点があなたのシステムにあるかどうかをテストするためには，自分のシステムに対してtftpで接続し，'get /etc/passwd'を試してみれば良い。これができたならば，ネットワーク上の誰か他の人がパスワードファイルを持っていった可能性がある。この問題を避けるためには，必要がなければtftpdを止めてしまうか，あるいはアクセス制限がかかっていることを確認すべきである。

パスワードファイルが取られたと思われる場合のもっとも安全な方法は，システムのすべてのパスワードを変更することである。

3．パスワードなし，あるいは既知のパスワードを持つアカウント（ベンダーのデフォールトのパスワードのままのアカウントが狙われる）

侵入者は，インストールしてから変更されていない，システムのデフォールトのパスワードを利用することが良くある。ソフトウェアをインストールしたら，必ずすべてのデフォールトパスワードを変更するようにせよ。また，製品をアップグレードした際に，パスワードが黙って新しいデフォールトに変更されることがあるので注意せよ。アップデートの後にデフォールトのパスワードを変更するのがもっとも良い。

パスワードファイルの中で，（root以外の）UIDが0であるようなアカウント，パスワードのないアカウント，新しいエントリをチェックせよ。パスワードなしのアカウントを一切許してはならない。使われていないアカウントはパスワードファイルから抹消しなさい。アカウントを停止するには，/etc/passwdファイルのパスワードフィールドをアスタリスク（*）に変更し，侵入者がネットワーク上のtrusted system（訳注：/etc/hosts.equivや.rhostsに書かれたシステム）からログインすることを確実に防ぐために，ログインシェルを/bin/falseにせよ。

4．sendmailのセキュリティホール

最新のsendmailを走らせていることを確認せよ。BSDのバージョン5.65はすべての既知の穴を塞いでいる（訳注：現在の最新は5.67である）。sendmailのバージョンを調べるには，次のようにtelnetを用いてSMTPポート（25）へ接続しなさい。

telnet 〈your hostname〉 25

5．古いバージョンのFTP；誤った設定のanonymous FTP

最新のftpd，つまりBerkeley version 5.60 of July 22, 1990を走らせていることを確認せよ。アップグレード情報については，ベンダーに確認せよ。anonymous ftpの設定も調べよ。anonymous FTPでアクセスできるファイルやディレクトリを適切に設定する（たとえば，ファイルやディレクトリのパーミッション，所有者，グループ）ためには，オペレーティングシステムについてくる説明書に従うことが重要である。FTP用のパスワードファイルやグループファイルにシステムの通常のものを使わないように注意すべきである。anonymous FTPのルートディレクトリと2つのサブディレクトリ（etcとbin）

はftpの持ち物であってはならない。

6．Morris Internet wormが使ったfingerdのセキュリティホール

fingerのバージョンが1988年11月より新しいことを確認せよ。多くのバークレー系システムにはこの弱点があった。

7．ネットワーク設定ファイルの不適切なエントリ

ベンダーの中には，/etc/hosts.equivに'+'記号のエントリを置いているところがある。＋エントリは，他のすべてのシステムを信用することを意味するので，取り除くべきである。/etc/hosts.lpdや全員の～/.rhostsファイルにも＋エントリを含めてはならない。これらのファイルは誰にでも書けるようになっていてはならない。特に必要がなければ，/etc/inetd.confの中の次のサービスは使わないことをお勧めする。

port 11 － systat
port 69 － tftp
port 87 － link

8．uucpの誤った設定

あなたのマシンがuucpをサポートしているなら，L.cmdsファイルをチェックし，必要なコマンドだけが含まれていることを確認せよ。このファイルは（uucpでなく!）rootが所有していて，誰でも読めるようになっているべきである。L.sysファイルは，uucpにsetuidされたプログラムだけがアクセスできるように，uucpが所有していてプロテクトされている（モードが600になっている）べきである。

9．不適切な/etc/ttysと/etc/ttytabの'secure'設定

/etc/ttysあるいはUNIXのリリースによっては/etc/ttytabとなっているファイルをチェックせよ。コンソール以外のすべての端末回線，仮想端末，ネットワーク端末のデフォールト設定をsecureにセットするべきではない。

10．/usr/lib/aliasesの不適切なエントリ

/usr/lib/aliases（mailのalias）ファイルに不適切なエントリがないか調べよ。aliasファイルには，'uudecode'あるいは単に'decode'という名前のaliasが含まれていることがある。このaliasがある場合は，特にそれを使っていない限り削除すべきである。

11．ファイルやディレクトリの不適切なプロテクション

システムファイルやディレクトリに正しいモードや所有者を設定するために，システムのドキュメントをチェックせよ。特に，'/'，'/etc'ディレクトリやすべてのシステム設定，ネットワーク設定のファイルをチェックせよ。ソフトウェアをインストールする前後にファイルとディレクトリのプロテクションを調べるか，検証ユーティリティを実行せよ。そのような場合，ファイルやディレクトリのプロテクションが変わることがあり得る。

12．古いバージョンのシステムソフト

古いバージョンのOSには，侵入者が良く知っているセキュリティ上の弱点が存在することが良くある。攻撃に対する弱点を最小にするためには，OSのバージョンを最新に保ち，セキュリティ関係のパッチはできるだけ早くあてることである。

KUINS 会議日誌

平成 4 年 9 月 10 日～平成 5 年 3 月 31 日

学術情報ネットワーク機構運営会議

5．3．9（第 4 回）

- 平成 4 年度歳出概算要求について
- 学術情報ネットワーク機構の活動状況について

学術情報システム整備委員会技術専門委員会

4．12．15

- 今後の KUINS の整備計画について —TV 講義・会議システム—
- KUINS の現状について
- 基幹ループ LAN ノード配置状況について
- KUINS パケット交換システム加入者一覧について

KUINS ネットグループ連絡会（第 22 回）

4．10．14

- IP ネットワークでの対外接続の整備に対するパケット交換機の変更について
- DPBX の ISDN 化について
- KUINS ニュースについて
- パケット交換機の障害について
- ISDN による IP 接続について

KUINS ネットグループ連絡会（第 23 回）

4．12．2

- パケット交換機の障害について
- DPBX の ISDN 化について
- KUINS における対外接続について
- ISDN による IP 接続について
- KUINS 講習会について
- 地域ネットワーク・コミュニティ（NCA 5）について

KUINS ネットグループ連絡会（第 24 回）

5．1．27

- KUINS における対外接続の概念図について
- ノードの障害について
- パケット交換回線の増設について
- 地域ネットワーク・コミュニティ（NCA 5）について
- KUINS ニュースについて

KUINS ネットグループ連絡会（第 25 回）

5．3．10

- 基幹ループ LAN のノードの停止について
- パケット交換機の障害について
- KUINS ニュースについて
- 学術情報ネットワーク機構運営会議の報告

ノード管理担当者の変更について

人事異動等によりノード管理担当者を交代される場合は，ノード番号と，新しい担当者の氏名・所属・職名・電話番号・電子メールアドレスを，学術情報ネットワーク機構情報システム管理掛（大型計算機センター内，☎ 753－7841）までご連絡下さい。