# 戸じまりは大丈夫ですか?

## ネットワークの安全性のために

TAINS 利用研究会
tains-riyou@tohoku.ac.jp

TAINS は，コンピュータ間の通信という枠を超えて，東北大学の活動に欠かせない基盤の役割を果たしています。しかし，コンピュータネットワークの利用によって研究活動への強力な支援が得られる一方で，新しい危険性がもたらされるかもしれないことを見落としてはいけません。よく言われる，ネットワークを利用したいたずらや犯罪的行為を防ぐよう，利用者の一人一人が気を付けなければなりません。

コンピュータは，不正利用やデータ破壊などから守るために，たくさんのガードがかけられています。しかし人間が設計し，利用している機械ですから，考慮漏れを防ぎきれず，安全性 (セキュリティ) に関る抜け穴もあります。抜け穴を利用して悪さをするのは，そのコンピュータの利用者かもしれないし，部外者かもしれません。ネットワークに接続している状況では，ネットワークを通ってどこか遠くから見知らぬ人が近づいてきて，いたずらされる可能性があります。 TAINS のようにインターネットに接続されていると，世界中からねらわれているとも言えます。

たとえ貴重な情報を置いていないコンピュータであっても，ねらわれ，侵入されたときに被害が無いとは言い切れません。例えば，よそのコンピュータを攻撃する足場として利用されることが考えられます。これは，駐車していて盗まれた車を強盗に使われたり交通事故を起こすようなケースに似ています。本来は被害者なのに責任を問われることがあり得ます。このような間接的被害を防ぐためにも，コンピュータの戸じまりは大切です。

コンピュータのガードをくぐって裏口から侵入して来るような抜け穴には，広く知られているものがたくさんあります。もしも抜け穴が放置されていたら，それを利用すると，たとえば，システム管理者になりすまして何でもできたり，よそのコンピュータからファイルを自由に読み書きすることもできます。明らかになっている抜け穴は公的な場で公表されていますから，それをふさぐ戸じまりを急がなければなりません。もうひとつ，パスワードの管理が悪ければ，それは玄関に鍵を掛けていないようなもので，玄関からやすやすと侵入される可能性があります。パスワードを設定していない利用者がいるとか，誰でも root 権限で作業できる設定は，もっとも初歩的な管理上のミスです。

たくさんある抜け穴のすべてを，1 台ごとに検査するには手間とかなりの専門的知識が必要です。この検査を自動化したプログラムが何種類か作られていて，あるアドレス範囲

のコンピュータを次々に検査するものはISS (Internet Security Scanner) と呼ばれます。ISSは，システムの管理者が利用する限りは戸じまりを点検する強力な支援ツールですが，その半面で，外部の者が同じプログラムを悪意をもって使えば，侵入口を探す便利な道具にもなります。すなわち，インターネットに接続されたTAINSでは，1台も残さずに戸じまりを徹底させなければ，学外からでも容易に抜け穴を見つけられてしまいます。

コンピュータの戸じまりはけっして管理者だけの仕事ではなく，一人一人の利用者が気を付けなければなりません。もし，あなたの使っているコンピュータで，パスワードを設定しないで使っている人がいたら，設定するように勧めましょう。パスワードを解読するプログラムも出回っていて，簡単すぎるものではわかってしまいますから，分かりにくいものをつけましょう。パスワードに利用ID (ログイン名) や名前を使っていたら，すぐに見破られてしまいます。英単語や人名の綴りを使うのも悪い例です。

コンピュータの管理を任されている方々は，公表された抜け穴をふさいであるか，もう一度確認してください。また，まわりの方も，戸じまりが大丈夫で安全性が確保されているのか，管理担当者に尋ねておきましょう。

TAINSの安全性に関する情報は，ネットワークニュースの `tains.net` やTAINS BBMSの `network` カテゴリーに流れます。安全性に関する情報が流れたら，まわりの人にも教えてください。また，安全性に関する問題に気付いたときや疑問を感じたときには，遠慮なく，同様に流してください。**SuperTAINS**ニュースの記事にも注意してください。 TAINS世話部局 (大型計算機センター，電話3659) に連絡するのも良い方法です。