ユーザ認証の盗聴

2002/9/10

峯 肇史

背景

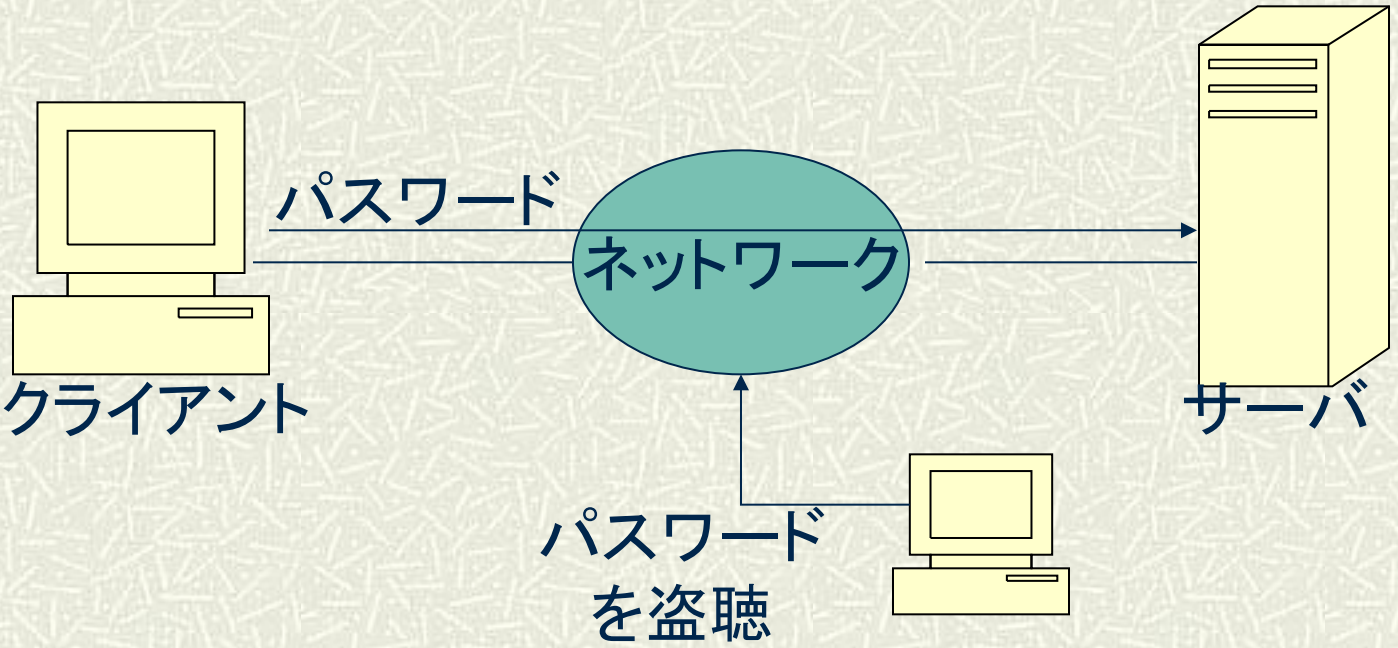
- インターネットの世界的普及
  - 世界中のコンピューターにアクセス可能
  - あらゆる場所の人々とコミュニケーション可能

この反面

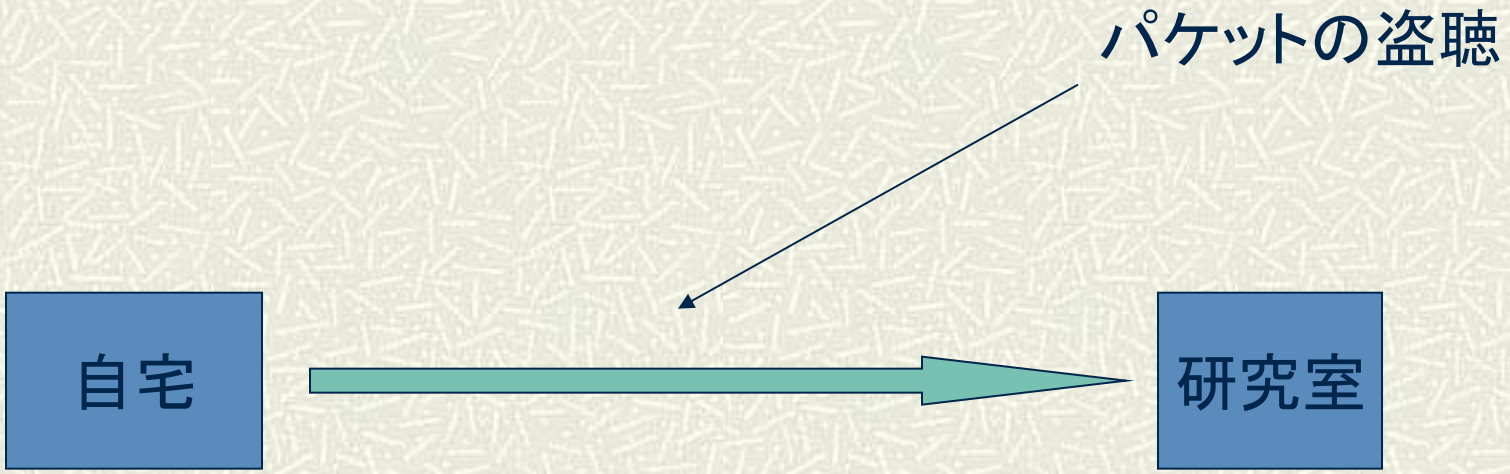
- 悪意のあるユーザがこの技術を利用
  - コンピュータに不正にアクセスしてデータを破壊
  - 個人情報にアクセスし悪用

ユーザ認証の盗聴

- ユーザ認証の際のパスワードをネットワーク上で盗み見る
  - 正規ユーザになりすましてアクセス可能



盗聴の例



盗聴

一番単純で効果的です。自宅の計算機から研究室の計算機までのネットワークの経路のどこかで、パケットを採集するプログラムを仕込み、全てのパケットのダンプを得ます。

Telnetにしろrloginにしろ、必ずパスワードを入力しますので、丹念に盗聴を行なえば、アカウントとパスワードの組を得ることができます。さらに、研究室の計算機から別の計算機にtelnetを行なえば、通信路にアカウントとパスワードのパケットが流れますからそれらを知ることが出来ます。

また、通常IPは暗号化されていません。ですから、リモートログインしてメイルを読んだ場合、盗聴者はメイルの内容を全て読むことができます。

パケットの盗聴には、特別なハードウェアは必要ありません。ネットワークの経路のどこかで専用のプログラムを動かせば良いだけです。つまりクラッカーが既に足場を築き上げている計算機が経路上に存在すれば良いのです。そのような状態になっているかは、リモートログインしようとしているユーザーには判断できません。

パケットスニファリング (Packet Sniffering)実習

スニファリング（パケット盗聴）

- ネットワーク上を流れるパケットを取り出す（盗み見る）行為

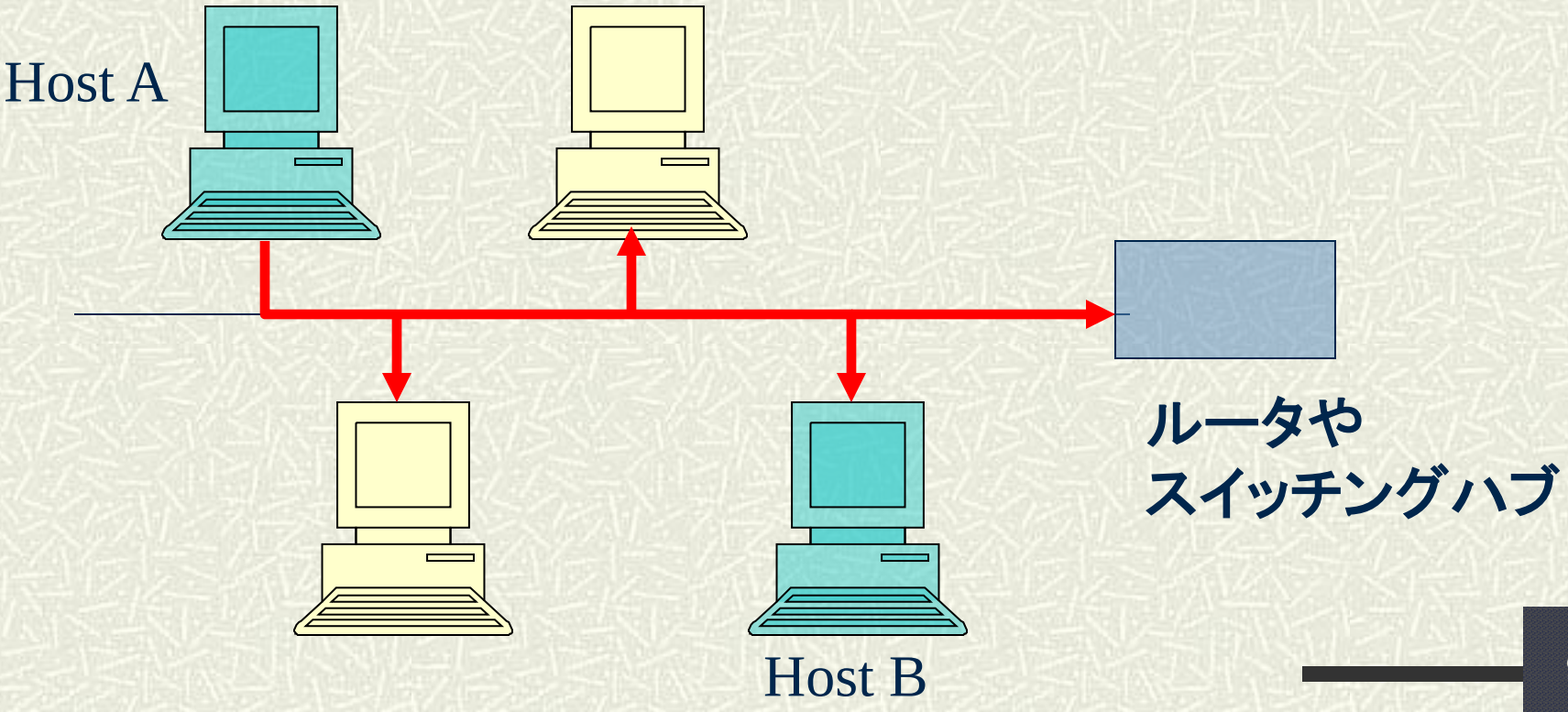
  暗号化されていないデータ（平文）はすべて盗聴可能

- パケット盗聴は比較的簡単

  - rootの権限
  - ツール（OSによっては標準で付属）

パケットの送信

- ネットワークセグメント（区画）内の相手に対し、パケットをばらまく



tcpdumpコマンド

ネットワーク管理ツール

コンピュータが接続しているネットワークを流れて
いるパケットを取り出す。

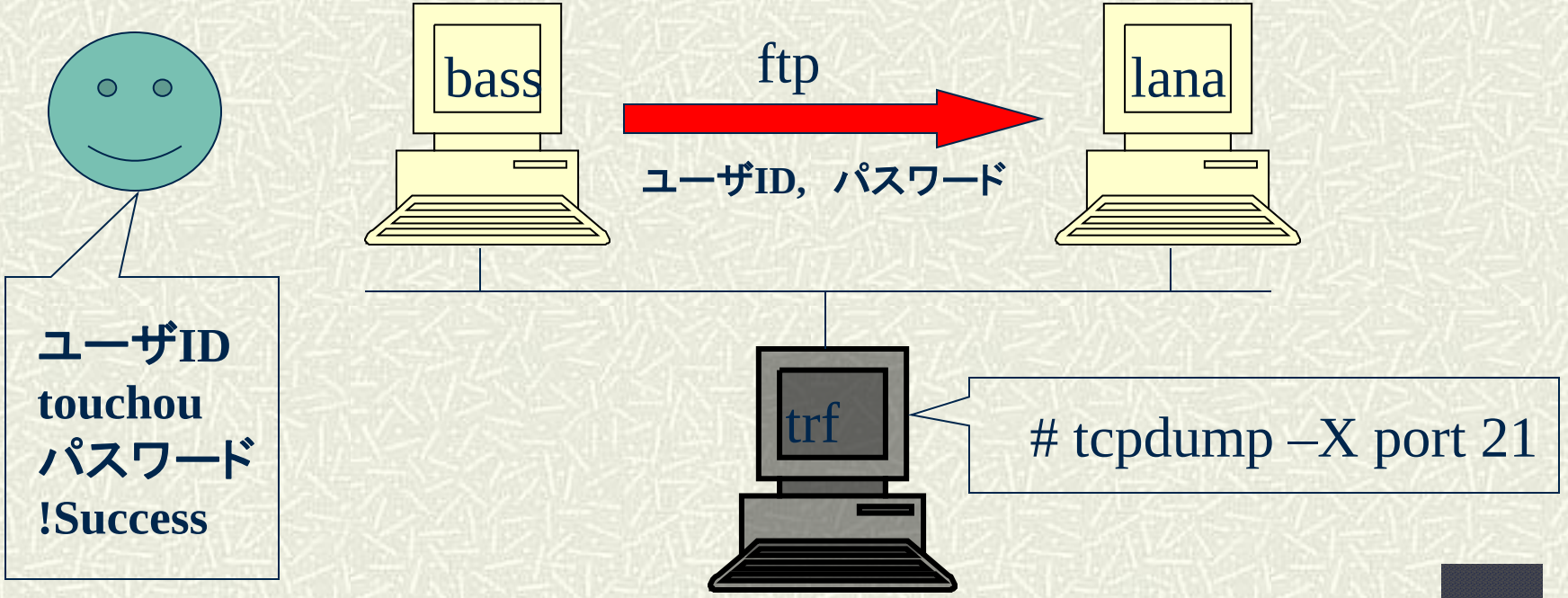
コマンド使用法

tcpdump [option]

option	**-X** 取り出したパケットの内容を表示 **host ホスト名** 指定したホスト名に関するパケットのみ取り出す **port ポート名** 指定したポート番号に関するパケットのみ取り出す
ポート番号	ssh：22 ftp(制御用):21 telnet：23 ftp(データ用):20

tcpdumpによる盗聴

- ftpを対象に、ユーザ認証情報であるユーザIDとパスワードの盗聴



tcpdump –X port 21

実際の結果

bassからlanaに送られたパケットであることを示す

```
09:31:13.453016 bass.4f.db.is.kyushu-u.ac.jp.1966 > lana.4f.db.is.kyushu-u.ac.jp.ftp:
P 15:30(15) ack 77 win 57920
<nop,nop,timestamp 26295216 22651681> (DF) [tos 0x10]
0x0000   4510 0043 5698 4000 4006 2062 c0a8 2139    E..CV.@.@..b..!9
0x0010   c0a8 2121 07ae 0015 f809 436b e0c4 0452    ..!!......Ck...R
0x0020   8018 e240 69a0 0000 0101 080a 0191 3bb0    ...@i.........;.
0x0030   0159 a321 5041 5353 2021 5375 6363 6573    .Y.!PASS.!Succes
0x0040   730d 0a                                    s..
```

実際のパケットのデータ

左の16進表記をASCIIコードで表したもの

パスワードが読み取れる

tcpdump出力例

tcpdump –X port 21

ftpに関するパケットが送信されるたび以下のような表示が出る。

bass.4f.db.is.kyushu-u.ac.jp > lana.4f.db.is.kyushu-u.ac.jp

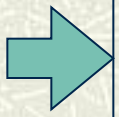
4510 0087 2bfb c036 5016 740c

:

:

0000 5555 4552 5353 c09c 5061

パケット内容の16進表示



16進をアスキーコードに変換

:

USER touchou

:

:

PASS !Success

出力

送信元 ＞ 送信先

パケット内容の16進表示、アスキーコード表示

実習

- マシンtrfでrootになり、

  trf# **tcpdump –X port 21**　　パケットを監視

- マシンbassからlanaへftpでログイン

  bass% **ftp lana**

- ユーザ名を聞かれるので入力

  bass% User: **touchou**

- パスワードを聞かれるので入力

  bass% Password: **!Success**