情報実験 第 11 回

ネットワークコンピューティング

佐々木 洋平
地球流体力学(林・小高)研究室 博士課程 1 年
uwabami@ep.sci.hokudai.ac.jp

2004/01/09

始めに(1)リモートアクセスとは

- リモートアクセス:
  ネットワーク上で接続された計算機同士でのデータのやりとり.

  - ⋆ 例) 地球大気大循環モデルを開発した. さて動かそう.
    - ∗ 手元の計算機では遅くてやってられない
      →どっかのスパコンで計算したい
    - ∗ 遠くの計算機センタまで行くのは嫌.
      → スパコンの操作 & データの転送をここからやりたい

こんな時にリモートアクセス!!

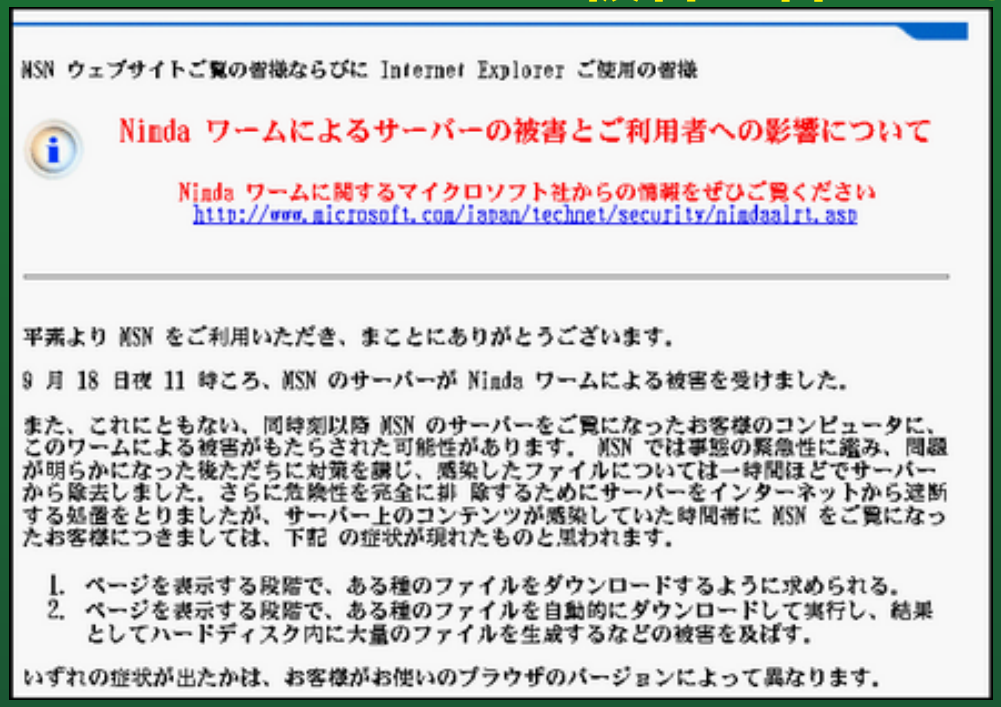
始めに(2)クラッカー，コンピュータウィルスの脅威

- 聞いたことがありますか?
  「セキュリティホール」，「コンピュータウィルス」，「クラッカー」

始めに(2)クラッカー，コンピュータウィルスの脅威

- 聞いたことがありますか?
  「セキュリティホール」，「コンピュータウィルス」，「クラッカー」

Microsoft のサーバも被害に合いました



MSN ウェブサイトご覧の皆様ならびに Internet Explorer ご使用の皆様

Nimda ワームによるサーバーの被害とご利用者への影響について

Nimda ワームに関するマイクロソフト社からの情報をぜひご覧ください
http://www.microsoft.com/japan/technet/security/nimdaalrt.asp

平素より MSN をご利用いただき、まことにありがとうございます。

9 月 18 日夜 11 時ころ、MSN のサーバーが Nimda ワームによる被害を受けました。

また、これにともない、同時刻以降 MSN のサーバーをご覧になったお客様のコンピュータに、このワームによる被害がもたらされた可能性があります。 MSN では事態の緊急性に鑑み、問題が明らかになった後ただちに対策を講じ、感染したファイルについては一時間ほどでサーバーから除去しました。さらに危険性を完全に排 除するためにサーバーをインターネットから遮断する処置をとりましたが、サーバー上のコンテンツが感染していた時間帯に MSN をご覧になったお客様につきましては、下記 の症状が現れたものと思われます。

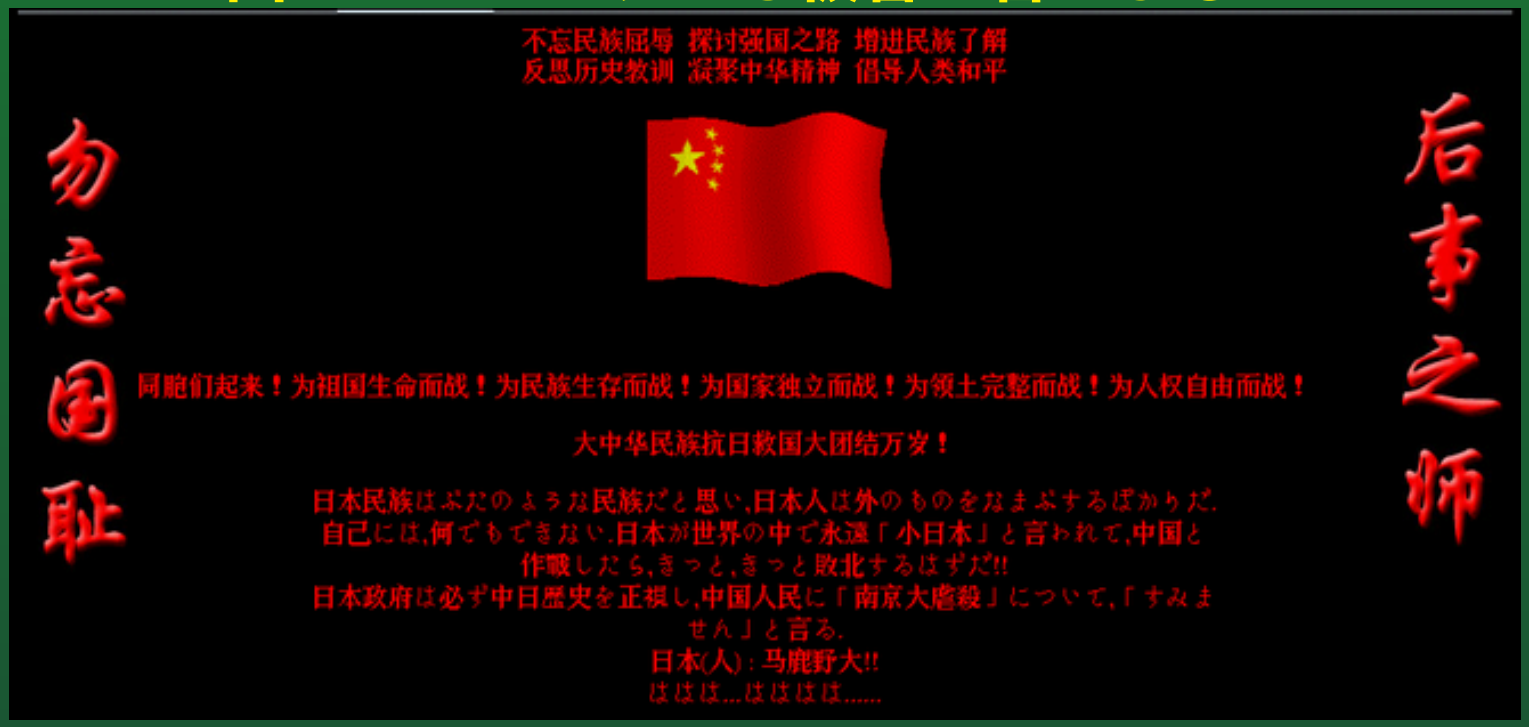
1. ページを表示する段階で、ある種のファイルをダウンロードするように求められる。
2. ページを表示する段階で、ある種のファイルを自動的にダウンロードして実行し、結果としてハードディスク内に大量のファイルを生成するなどの被害を及ぼす。

いずれの症状が出たかは、お客様がお使いのブラウザのバージョンによって異なります。

始めに(2)クラッカー，コンピュータウィルスの脅威

- 聞いたことがありますか?
  「セキュリティホール」，「コンピュータウィルス」，「クラッカー」

国立がんセンターも被害に合いました



始めに(2)クラッカー，コンピュータウィルスの脅威

- **聞いたことがありますか?**
  「セキュリティホール」，「コンピュータウィルス」，「クラッカー」

- **他人事じゃないんです!!**
  - ⋆ 2001/01/09 **報告，国立** H **大学** EE **研の計算機に不正侵入.**
    メールサーバのパスワードが盗られた痕跡あり.
  - ⋆ 2001/01/23 **報告，国立** H **大学** EO **センターの計算機に不正侵入.**
    コマンド置換，バックドア作成等，悪事の限りを尽くされた模様.
  - ⋆ 2001/01/29**報告，国立** H **大学** E **専攻某教授がメールよりウィルス感染.**
    ○○です.
    まちがって，開いちゃった(略).
    止める方法あったらおせーて!!
  - ⋆ 2001/02/04 **報告，国立** H **大学** E **専攻の計算機に不正侵入.**
    コマンド置換がなされた模様…該当 host**名は永久欠番に.**

始めに(3)本日の御品書き

- リモートアクセス系コマンド
  - ⋆ 概論
  - ⋆ リモートログイン
  - ⋆ リモートコマンド実行
  - ⋆ ファイル転送
  - ⋆ 注意すべき事
  - ⋆ 推奨コマンド=ssh, scp
- インターネットセキュリティの基礎
  - ⋆ クラッカーの手口
  - ⋆ 注意!!
  - ⋆ どうやって守るかの初歩

リモートアクセス系コマンド(1)概論

- TCP/IP 層では「アプリケーション層」に対応.
  → 情報実験 第五回 講義資料参照

- リモートアクセス系コマンドの分類
  - ⋆ リモートログイン:rlogin, telnet, ssh
    - ∗ 自分が現在使っている計算機(localhost) からネットワークを経由して他の計算機(remote host) にログインすること.
  - ⋆ リモートコマンド実行: rsh, ssh
    - ∗ remote host 上でコマンドを実行すること
      - ○ 「リモートログイン→コマンド実行→ログアウト」を一度に行う.
  - ⋆ ファイル転送: rcp, ftp, scp
    - ∗ ネットワーク経由でファイルを転送すること

リモートアクセス系コマンド(2)リモートログイン

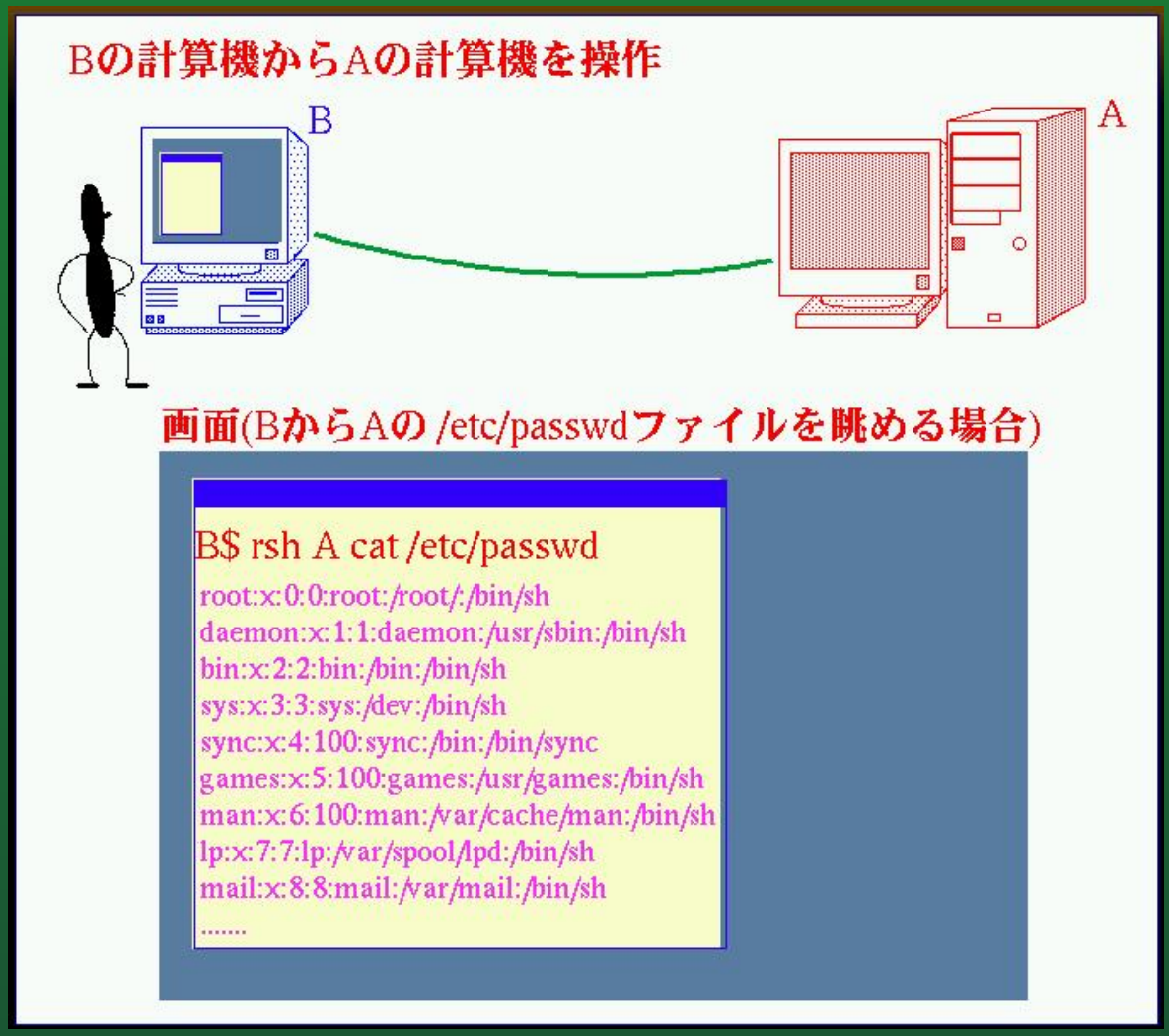
Bの計算機からAの計算機にログイン&操作

画面(BからAにtelnetでログイン)

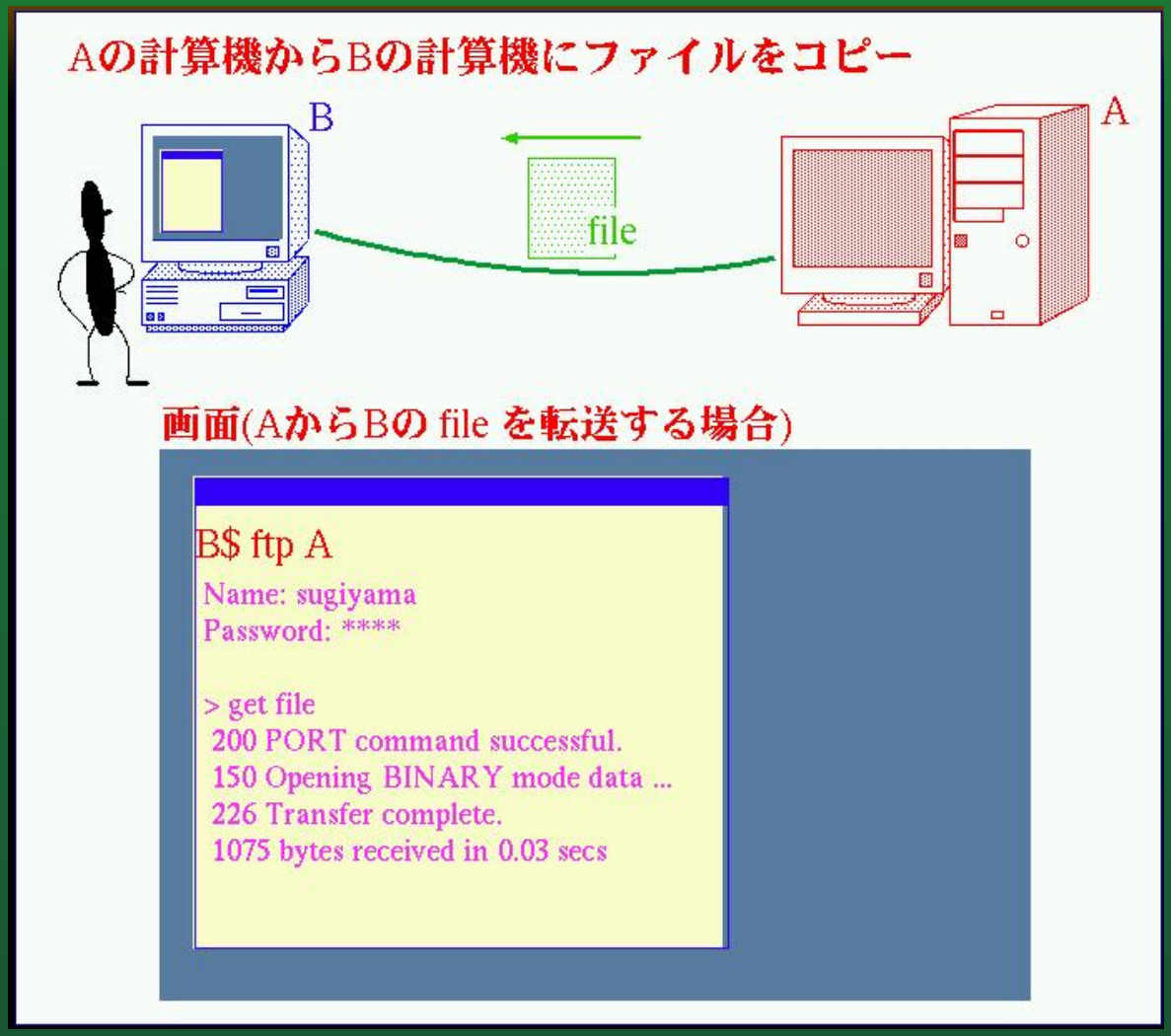
```
B$ telnet A
Debian GNU/Linux 3.0 A.hoge.jp
A login: sugiyama
Password: ****

A$ less /etc/passwd
root:x:0:0:root:/root/:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
.....
```

リモートアクセス系コマンド(3)リモートコマンド実行

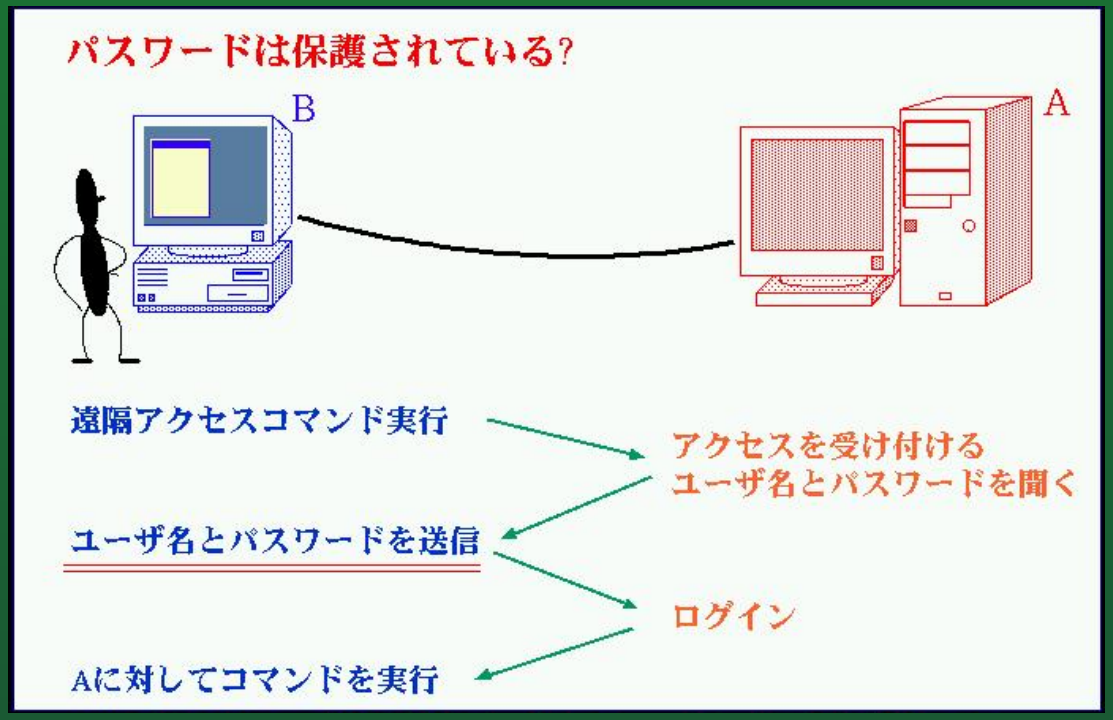


リモートアクセス系コマンド(4)ファイル転送



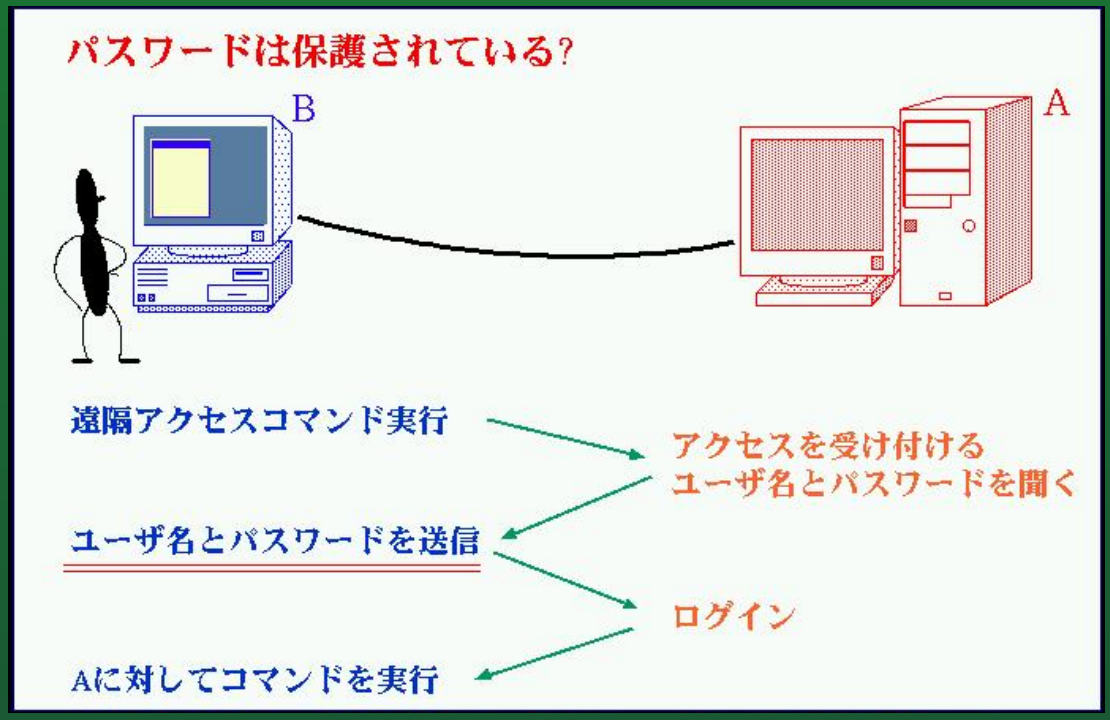
リモートアクセス系コマンド(5)注意すべき事

- 通信内容がどこまで保護されるのか?
  - ⋆ 例）リモートログインの際に…



リモートアクセス系コマンド(5)注意すべき事

- 通信内容がどこまで保護されるのか?
  - ⋆ 例）リモートログインの際に…



  - ⋆ スニフ(盗聴)されるとアウト!!⇒通信内容を暗号化しましょう.

リモートアクセス系コマンド(6)推奨コマンド

- **リモートログイン・コマンド実行**: ssh(Secure SHell)
- **ファイル転送**: scp(Secure CoPy)
  - **長所**:
    - **通信内容(含パスワード)が暗号化されている**
      - ftp や telnet **は平文のまま(そのまま)流れる!!**
  - **短所**:
    - **暗号化されるので処理に時間がかかる.**
    - **パケットも大きくなる.**
    - **サーバによっては対応していない.**
      - **情報基盤センターの端末とか…**

今日の実技ではこれらコマンドの使い方をやります

参考: Windows のssh, scp

リンクは専攻計算機ネットワークの手引き集へリンクされています

- ssh 編
  - TeraTerm + ssh = ttssh
    - ssh1 **にしか対応していないが, 結構便利. ⇒使い方**
  - putty
    - ssh2 **にも対応.⇒PuTTyで login**

- scp 編
  - WinSCP
    - **結構使える. 大量転送時はメモリを喰うので設定に注意**
      ⇒WinSCP1, WinSCP2

参考: Windows のssh, scp

リンクは専攻計算機ネットワークの手引き集へリンクされています

- ssh 編
  - TeraTerm + ssh = ttssh
    - ssh1 **にしか対応していないが, 結構便利. ⇒使い方**
  - putty
    - ssh2 **にも対応.⇒PuTTyで login**

- scp 編
  - WinSCP
    - **結構使える. 大量転送時はメモリを喰うので設定に注意**
      ⇒WinSCP1, WinSCP2

…情報基盤センターが対応してないので, ガッカリですけどね

インターネットセキュリティの基礎(1)クラッカーの手口

代表的なのは以下の三つ

- プログラムのバグを利用したシステムへの不正侵入(ログイン)
  - ⋆ データの盗難，破壊，下記攻撃の際の踏み台，信用失墜,…
- ネットワーク上の通信に対する攻撃
  - ⋆ 盗聴，改竄,…
- ネットワーク上の通信を利用した攻撃
  - ⋆ 発信者の詐称，ウィルスによるシステムの破壊，DoS 攻撃，…

攻撃を未然に防ぐには?

インターネットセキュリティの基礎(2)注意

攻撃を防ぐための第一歩＝相手の手を知る事

です.

だからと言って,知り得た手口を

実際に行なってはいけません.

これは悪意の有無によりません.

知らなかったでは済まされません.

警察の御厄介にならないように.

インターネットセキュリティの基礎(3)どうやって守るか

- **必要の無いネットワークサービスの停止**
  - ⋆ 不要なソフトのアンインストール
  - ⋆ **ポート**(サービス毎に決ったデータの入り口)を塞ぐ
- **アクセス制限**
  - ⋆ 知っているホストからのアクセスのみを許可
- **ソフトウェアのバージョンは常に最新に**
  - ⋆ バグ情報，セキュリティ情報は常に注視
  - ⋆ セキュリティホール情報が出たら必ず対応

インターネットセキュリティの基礎(3)どうやって守るか

- **必要の無いネットワークサービスの停止**
  - ⋆ 不要なソフトのアンインストール
  - ⋆ **ポート**(サービス毎に決ったデータの入り口)を塞ぐ
- **アクセス制限**
  - ⋆ 知っているホストからのアクセスのみを許可
- **ソフトウェアのバージョンは常に最新に**
  - ⋆ バグ情報，セキュリティ情報は常に注視
  - ⋆ セキュリティホール情報が出たら必ず対応

実技編でこれらの対策をしてもらいます

参考(2): Windows の場合はMicrosoft と心中!?

それは嫌なので…

- **定期的に** Windows update!
  - ⋆ **自信の無い人は自動更新機能を使う(デフォルト).**
- **サービスを止めまくる.**
  - ⋆ **「ファイル名を指定して実行」→「**services.msc**」で不要なサービスを止めまくる. 止め過ぎに注意.**
- **ウィルス検知・駆除ソフトを使う.**
  - ⋆ Free **の検知ソフトとしては,** AVG Anti-Virus **がお勧めです.**
- **ファイアウォールソフト(ポートを塞ぐソフト)を導入する.**
  - ⋆ Free **では** ZoneAlarm **がお勧めです.**