情報実験INEX 2020
第2回
情報実験機へのリモート
アクセス

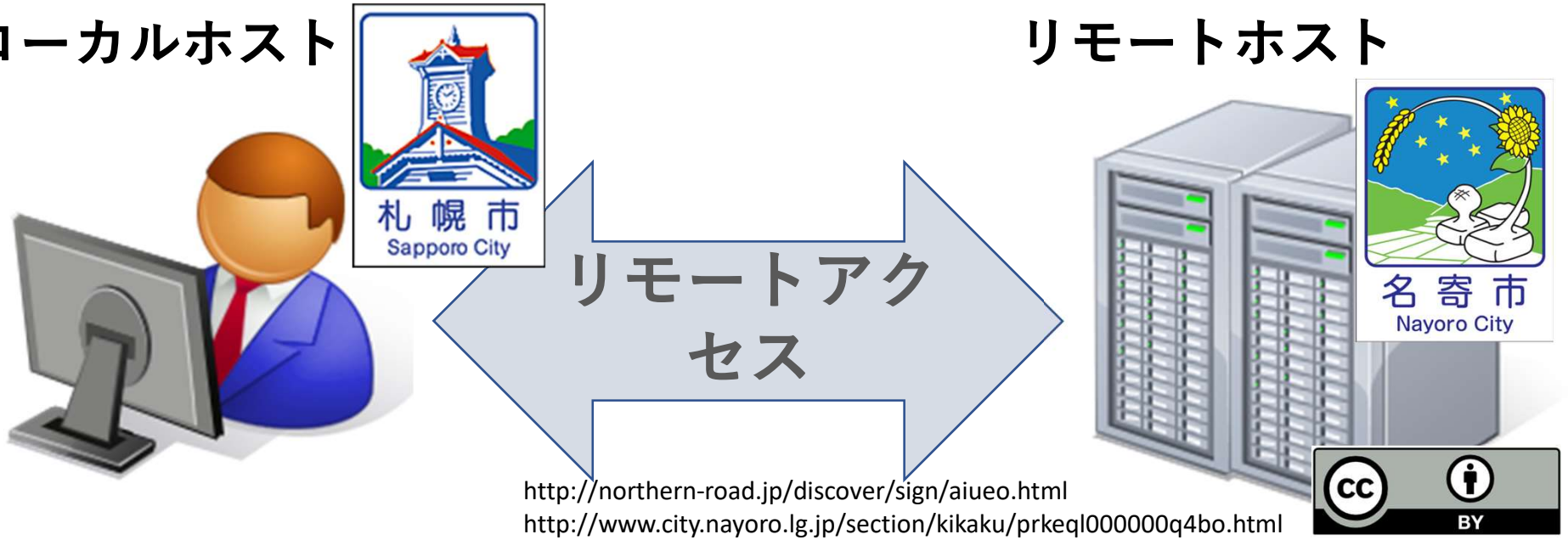
北海道大学理学院
宇宙理学専攻　修士課程２年
杉山 玄己

本日の内容

- リモートアクセスとは
- リモートアクセスに使用されるプロトコル
- リモートアクセスの危険性
- 公開鍵認証とは
- 実習：情報実験機にリモートログインしてみよう

リモートアクセスとは

- 手元の計算機(**ローカルホスト**)から別の計算機(**リモートホスト**)へネットワークを経由して接続・操作すること
  - リモートログイン
  - リモートアクセスを用いたファイル転送



http://northern-road.jp/discover/sign/aiueo.html
http://www.city.nayoro.lg.jp/section/kikaku/prkeql000000q4bo.html

リモートログイン

- ローカルホストからリモートホストへログインすること
  - ログイン: アカウント情報を用いて認証した後に, コマンド等を利用できる状態にすること
  - 事前にリモートホストのアカウントが必要
- 主に使用するコマンド
  - ssh

リモートログインのイメージ

ホスト名: joho18
アカウント名:
hoge

**ssh コマンドを用いて，
リモートログインを要請**

ログインパスワードを要求

ホスト名: joho24
アカウント名:
hero

```
hoge@joho18:~ $ ssh  hero@joho24
hero@joho24's  password:
```

リモートログインのイメージ

ホスト名: joho18
アカウント名:
hoge

ログインパスワードを送信

ログインを許可

ホスト名: joho24
アカウント名:
hero

```
hoge@joho18:~ $ ssh  hero@joho24
hero@joho24's  password: (パスワードを入力)
....
hero@joho24:~ $
```

リモートアクセスの危険性

ネットワーク
空間

joho18

joho24

リモートアクセスの要請

ユーザ名・パスワードの要求

ユーザ名・パスワードの送信

認証・アクセス許可

joho24 内でコマンド実行

第三者による盗聴

重要な情報が盗聴される危険性がある！

パケット盗聴

- ネットワーク上に流れる情報を盗み見ること
  - 情報はネットワーク上の様々な計算機を経由
  - いたるところで盗聴される可能性有り
- パケット盗聴への対策
  - 暗号化通信
    - 通信を暗号化し, 第三者に見られても内容が分からないようにする

ユーザー認証

- 接続を試みるユーザーが本当に正規のユーザーなのか（計算機の管理者からアカウントを取得したのか）確かめる必要がある
- 正規ユーザーしか持っていない情報で認証

  例えば
  - パスワード
  - 公開鍵
  - 指紋や虹彩などの生体情報
- 今回利用するのは公開鍵認証

リモートアクセスに関する用語

- **プロトコル：**
  - リモートアクセスを行うための共通の約束事
    - 送受信するデータの形式
    - やり取りする際の作法など
- **Telnet, FTP, SSH**
  - リモートアクセスを行うためのプロトコル
  - それぞれのプロトコルで用途や仕様が異なる
- **ポート**
  - ネットワークと情報をやり取りするための窓口（詳しくはまた別の回で）

Telnet(Teletype Network)

- 古くから利用されるリモートアクセス用プロトコル
- 使用ポート：23番
- **通信が暗号化されない(危険・非推奨)**
  - 現在は主にポートチェック(特定のポートの開閉を確認)に使用
- このプロトコルを利用する主なコマンド
  - telnet

FTP(File Transfer Protocol)

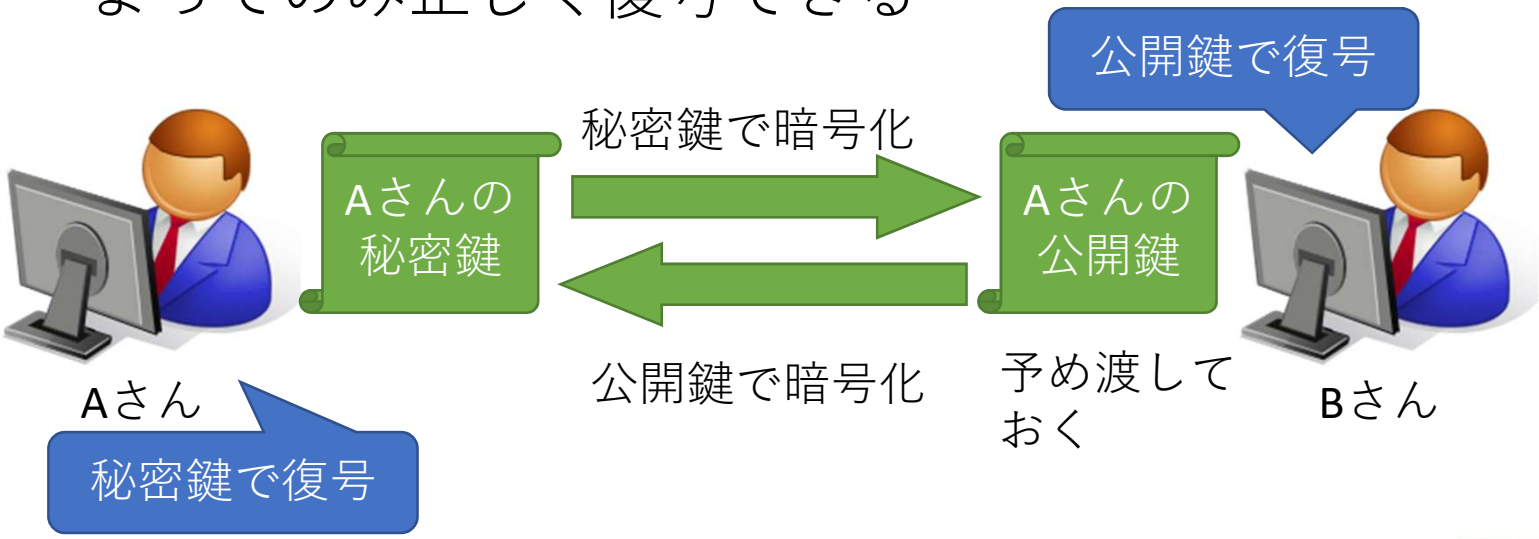
- 古くから利用されるファイル転送用プロトコル
- 使用ポート: 21番
- **通信が暗号化されない(危険・非推奨)**
  - 現在は匿名利用前提の通信で利用可能
    - Debian アーカイブミラーなど
- このプロトコルを利用する主なコマンド
  - ftp

SSH (Secure Shell)

- リモートアクセス用プロトコルの一つ。ネットワーク上に流れる情報を暗号化する
- 主なソフトウェア：
  OpenSSH（オープンソース）
- 使用ポート：22 番
- パケットを暗号化
  - Telnet, FTP など他のプロトコルよりも安全に通信可能
  - 暗号化する分通信速度低下
- このプロトコルを利用する主なコマンド
  - ssh, sftp, scp など

公開鍵暗号（RSA公開鍵暗号）とは

- 暗号化と復号のために「公開鍵」と「秘密鍵」のペアを用いる暗号化方法
  - 秘密鍵で暗号化されたデータは、対応する公開鍵によってのみ正しく復号できる
  - 公開鍵で暗号化されたデータは、対応する秘密鍵によってのみ正しく復号できる

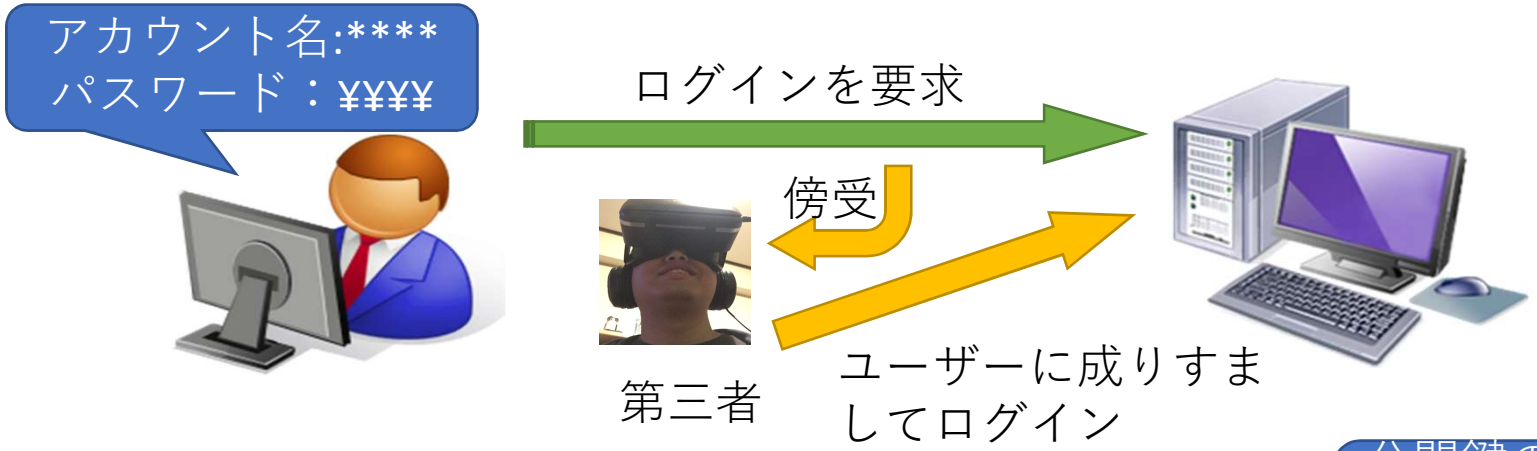


公開鍵を用いたユーザー認証

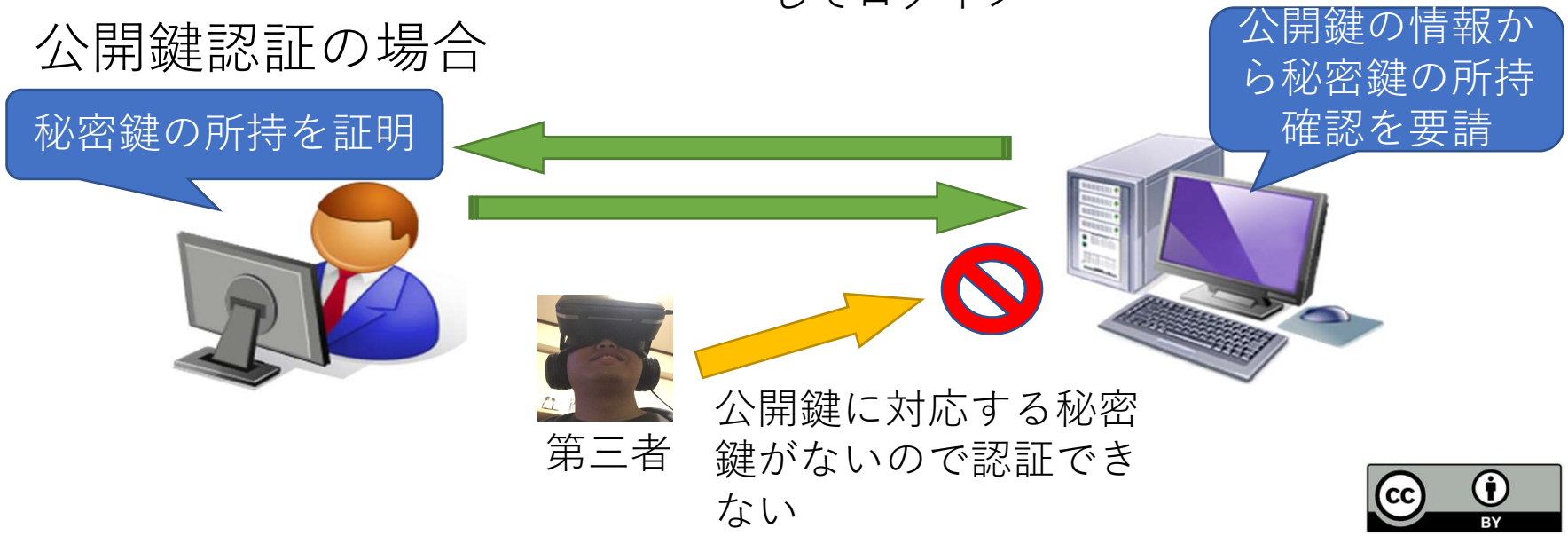
- 予め公開鍵をリモートホストに登録しておき、接続時にユーザーが対応する秘密鍵を持っているか確認する認証方式
- 利点：
  - パスワードなどの機密情報がネットワークに送信されない
  - パスワード推測攻撃に強い

公開鍵認証の必要性

- パスワード認証の場合



- 公開鍵認証の場合



実習：情報実験機へのリモートログイン

- 前回suuにアップロードした公開鍵を情報実験機に登録してありますので、さっそく接続してみましょう
- 詳細な手順は実技資料にて

参考資料

- 入門OpenSSH　新山 祐介
  https://www.unixuser.org/~euske/doc/openssh/book/index.html
- リモートアクセス/ネットワークセキュリティ情報実験 第8回 (2019/06/21)
  http://www.ep.sci.hokudai.ac.jp/~inex/y2019/0621