OS 第１３回予習確認テスト　　学生番号（　　）　　氏名（　　）

1） アクセス制御

ア） 一般論

アクセス制御は、（　　）×（　　）×（　　）の組合せごとに、○×で考える

これを表す表（行列）：（　　）

⇒ 上の 3 つのうち（　　）と（　　）を行と列にして、各欄に（　　）を書いたもの。

問題点 ⇒ 行列が（　　）なので、スペースがもったいない。 詰めたい。 表現を工夫する。

① 主体（誰が）ごとにリストを書く ⇒ （　　リスト）

主体1： ファイルA： 読み　ファイルB： 読み・書き　ファイルC： 読み・書き

主体2： ファイルB： 読み　ファイルC： 読み　ファイルD： 読み・書き　のように書く

② 対象（何を）ごとにリストを書く ⇒ （　　リスト）

ファイル1： ユーザA： 読み　ユーザB： 読み・書き　ユーザC： 読み・書き

ファイル2： ユーザC： 読み　ユーザD： 読み・書き　ユーザE： 読み　のように書く

イ） Linux や Windows ではファイルごとに②が付いている。

図の第 3 行目の rw-rw-r-- を説明せよ

r……w……―

r……w……―

r……―……―

```
ls -l
合計 392
-rw-rw-r--. 1 yamanouc yamanouc 102073  7 月 21  2015 3dxmeans.png
-rw-rw-r--. 1 yamanouc yamanouc   3263  7 月 22  2015 3dxmeans.py
-rw-rw-r--. 1 yamanouc yamanouc   2235 12 月 10  2015 3dxmeans.pyc
-rw-rw-r--. 1 yamanouc yamanouc 111857  7 月 22  2015 3dxmeans_0.1.png
-rw-rw-r--. 1 yamanouc yamanouc 145784  7 月 22  2015 3dxmeans_0.27.png
-rw-rw-r--. 1 yamanouc yamanouc   3800  1 月 30  2003 iris.csv
-rw-rw-r--. 1 yamanouc yamanouc    826  7 月 21  2015 plot3d.py
-rw-rw-r--. 1 yamanouc yamanouc   1280 12 月 10  2015 plot3d.pyc
-rw-rw-r--. 1 yamanouc yamanouc   4779  7 月 22  2015 xmeans.py
-rw-rw-r--. 1 yamanouc yamanouc   5584  7 月 22  2015 xmeans.pyc
```

2） 暗号

ア） 共通鍵暗号（秘密鍵暗号）と、公開鍵暗号の違い

共通鍵暗号は、従来から用いられていた方法で、暗号鍵（掛けるカギ）と復号鍵（戻すカギ）が（　　）。

従って、鍵は（　　）ければならない。 欠点は、受信側が遠隔だと鍵を（　　）。

他方、公開鍵暗号は 1976 年にデフィーとヘルマンが論文公開したもので、暗号鍵と復号鍵が（　　）、更には一方から他方が（　　）。 従って一方を公開しても秘密が保てる。 但し計算量は（　　）。

イ） 公開鍵暗号の利用形態

＜メッセージ秘匿＞　仕組の絵を描いてみよう。

3） ユーザ認証とは何か （　　）

ユーザ認証の方法を挙げ、やり方と、特徴と、利点・欠点を説明せよ

名称	方法	特徴、 利点・欠点