OS 第13回予習資料　　第13回の授業までに空欄を埋めて予習　　質問は事前＋当日受付けます

第13回　保護とセキュリティ

13－1．アクセス制御　～～～「資源」に対するアクセスを制御（制限）する

制御の仕方は、（　　）×（　　）×（　　）の組合せごとに、許可・不許可

アクセス制御行列：　上記のうち許可されたものだけを書く。

これがアクセス制御の基本。

疎な（つまり　　である）行列なので表現を工夫をして密になるようにしたのが、

①（　　リスト）と

②（　　リスト）

| 誰が＼対象 | ファイル1 | ファイル2 | デバイス1 | 誰１ | 誰２ | 誰３ |
|---|---|---|---|---|---|---|
| 誰１ | Read<br>Write | | Output | | | |
| 誰２ | Read | Read | | Switch | | Switch |
| 誰３ | | Read<br>Execute | | Switch | | |

①は、主体（誰が）ごとにリストを書く：　誰１は（　　）に（　　）を、（　　）に（　　）をしてよい。

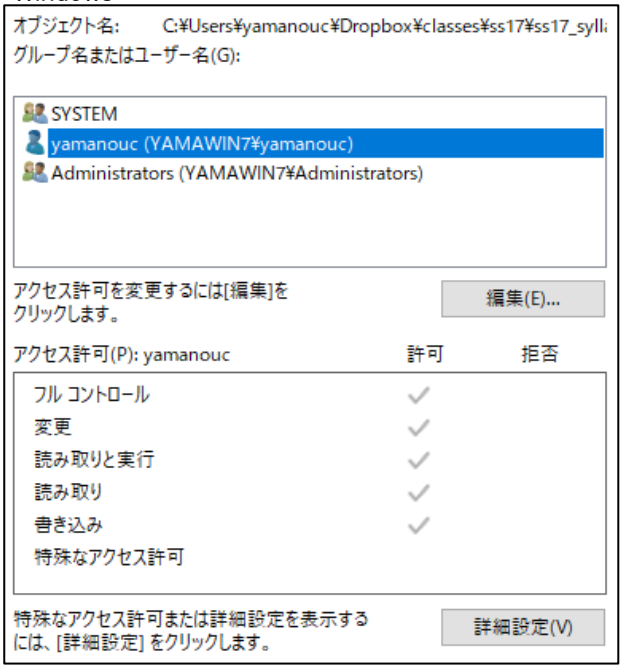
②は、対象ごとにリストを書く：　ファイル１は（　　）が（　　）を、（　　）が（　　）をしてよい。

＜Windows や Linux では、ファイルごとに②が付いている＞

Linux

```
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
```

Windows




13－2．　暗号

暗号とは、データを変換して（　　）すること

ことば：

暗号化・復号化　（　　）

平文　（　　）

鍵　（　　）

共通鍵暗号 vs 公開鍵暗号


| | 共通鍵暗号 | 公開鍵暗号 |
|---|---|---|
| 暗号・復号鍵が | | |
| 鍵を秘匿・公開？ | | |
| 鍵配送が | | |
| 計算量が | | |

公開鍵暗号の応用　　仕組の絵を描いてみよ

（1） メッセージ秘匿

（公開鍵だけを使う場合）

（公開鍵システムを使って共通鍵を交換し、本文は境界鍵を使う場合）　～～ なぜそうするのか？

（2） 送信者認証

（3） 改ざんの防止

13－3.　その他の話題　～～ ユーザ認証　ユーザ認証とは何か？（　　）

| 名称 | 方法 | 特徴、 利点・欠点 |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

13－4.　悪意のあるソフトウェア（キーワード）

基本情報試験ではそれぞれについて説明を求められる。
自分で調べて、一通りは説明できるようにしておくこと。

- マルウェア
- トロイの木馬
- スパイウェア、キーロガー
- コンピュータウィルス・バックドア
- ワーム
- ルートキット

- ソーシャルエンジニアリング・成りすまし・フィッシング
- サービス不能（DoS 攻撃、DDoS 攻撃）
- バッファオーバーラン

- アンチウィルスソフトウェア（ワクチン）
- ファイヤウォール、パケットフィルター
- サンドボックス