オペレーティングシステム（山内）　第１３回　保護とセキュリティ・暗号　　授業前の予習資料

1）「保護」・「セキュリティ」について、ビデオや教科書 176 ページを参照して、この2つの視点があることを整理しておこう。

保護とは：.....

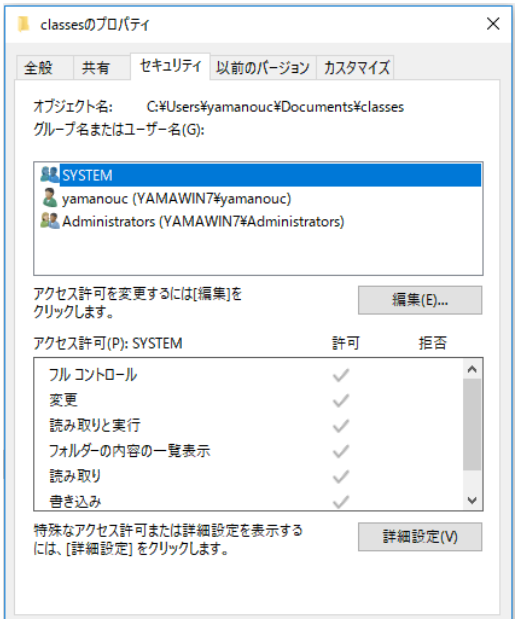
セキュリティとは：.....

2） アクセス制御行列の考え方を整理しておこう。（教科書 177～179 ページ）

ア） アクセス制御行列とはどういうものか、構成要素と書き方を整理しよう

イ） アクセス制御行列と、ケーパビリティリスト・アクセス制御リスト、との関係を整理しよう

ウ） MS Windows や Linux で、ファイル等に対してアクセス制御をしている。



① MS Windows では、それぞれのファイルやフォルダのプロパティを見る（ファイルリストを表示して右クリック⇒最下段の「プロパティ」をクリック⇒「セキュリティ」タブをクリック）と、＜グループ名またはユーザー名＞ごとに＜アクセス許可＞が表示される。 これを開いてみて、どの操作に対して許可が出ているかを見てみよう。

② Linux でも同じように、それぞれのファイルについて、アクセス制御の情報を見ることができる。たとえば、ls -l コマンドを実行すると、

```
-rwxr-x--- 1 712007yn apache 9907 11 月 25  2013 openmpPi
-rwxr-x--- 1 712007yn apache 1030 11 月 25  2013 openmpPi.c
```

のように表示されるが、それぞれの行の先頭の

```
-rwxr-x---
```

が、アクセス制御情報を表している。第1文字目は、ディレクトリの場合は d、ファイルの場合は-を表示、残りの9文字は、3文字 rwx ずつの組になっており、それが3回（ファイル所有者の権限、同じグループに属するユーザの権限、その他のユーザの権限）繰り返される。それぞれの3文字は、r＝read、w＝write、x＝execute であり、権限があれば文字が、権限がなければ-が書かれる。

③ ①②はそれぞれ、上記イ）のどの形式に従っているだろうか？

（教科書 「束モデル」は触れない）

3） 暗号の仕組（原理）を整理しよう。（教科書 181～183 ページ）

ア） 平文、暗号文、暗号化、復号化、鍵、送信者、受信者の関係を、図に表してみよう。

イ） 非常に単純な暗号として、入力の１文字を、出力の１文字に（表を使って）置き換える「単一換字暗号」が考えられる。

① アルファベット順に1文字ずつずらす（a を b に、b を c に、c を d に、z を a に置き換える）暗号を試してみよ。

I have a pen　⇒ .....

② 仮に、置き換え方をランダムな変換表にしたとしよう。 ①と比べると分かりにくさで何が違うだろうか？

③ 通信を傍受して、たくさんの例文を集めたとしよう。（英語で）変換表を推定する方法は？

シャーロックホームズの「踊る人形」（The Adventure of the Dancing Men）でもこの原理に言及している。

（暗号化の細かい理論については、これ以上触れない。数理の暗号の授業にて勉強してください）

ウ） 暗号には、「共通鍵暗号」と「公開鍵暗号」の2種類がある。（教科書ページ 181～183）

① それぞれの動作と使い方を説明してみよう。（公開鍵暗号の数学的な原理は数理の暗号の授業で勉強してください）

② 公開鍵暗号の応用：（1）情報の秘匿、（2）送信者の認証、（3）改ざんの防止、について、目的（やりたいこと）と原理（どう公開鍵暗号を使って目的を達成するか）を説明してみよう

4） 一般にユーザ認証（＝あなたが本当にあなたであるのか）をする方法として、次のものの原理と問題点を説明してみよう。

① パスワード　② ワンタイム・パスワード　③ ハードウェア・キー（IC カードキーなど）　④ 生体認証（指紋など）