

# コンピュータ概論 A/B

-- Malware に注意/暗号化 --

数学科 栗野 俊一 (TA: 浜津 翔 [院生 1 年])

2013/10/01 コンピュータ概

# 伝言

---

## 私語は慎むように !!

### □ 席は自由です

- できるだけ前に詰めよう

### □ すぐやること

- Note-PC の電源ケーブルを継ぎ、電源を入れ、今週の資料を読む

### □ 色々なお知らせについて

- 栗野の Web Page に注意する事

<http://edu-gw2.math.cst.nihon-u.ac.jp/~kurino>

### □ 【注意】

- 講義の速度が早過ぎたら

▶ 「遅くするように／もう一度説明するように」と申し出る

- 今聞いた内容を、友達に聞きたければ

▶ 「友達に確認したいので、時間が欲しい」と申し出る(勝手に話をしない)

- 来週の月曜日(2限)も「補習」します(1214 GW 室です)

▶ 是非、質問を抱えてやってきてください。

**IP Address : 10.9.209.107**

# 前回(2013/09/24)の内容

---

## □ 前回(2013/09/24)の内容

### ○ 後期の方針：前期と同じ

▶ 人に迷惑をかけるな / 実習重視 / ネットワークを利用しよう

### ○ 前期の復習：コンピュータの色々な使い方を学んだ

▶ PC の機能は自分で拡張できる / 組み合わせが重要 / PC の基本知識

## □ 講義内容

### ○ ソフトウェアの更新：ソフトは **update/upgrade** が必要

▶ ソフトにも保守(更新)が必要 / 自ら管理 / セキュリティ問題の回避

▶ バックアップの必要性 / 「復元ポイント」の利用

# 本日(2013/10/01)の予定

---

- 本日(2013/10/01)の予定
  - マルウェア/セキュリティ/暗号化
    - ▷ 暗号化と TrueCrypt
- 実習
  - [演習 1] TaskManager の利用
  - [演習 2] truecrypt のインストール
  - [演習 3] truecrypt の使い方
  - [演習 4] 課題の作成

# 本日の課題 (2013/10/01)

---

## □ 前回 (2013/09/24) の課題

○ 次のファイルを excel で作成して CST Portal に提出してください

▶ ファイル名 : 20130924-YYYY.xlsx (YYYY は学生番号)

▶ 内容 : 自分の成績の偏差値は ?

▶ 形式 : xlsx 形式 ( sample-20130924.xls を参照 )

## □ 今回 (2013/10/01) の課題

○ 次の TrueCrypt のボリュームを作成し、CST Portal から提出

▶ 表題 : TrueCrypt のボリュームファイルの提出

▶ ファイル名 : 20131001-YYYY.tc (YYYY は学生番号)

▶ 詳しくは、配布した sample-20131001.tc の内容を参照

# PC セキュリティ (復習)

---

## □ PC のセキュリティを守ろう

- 知る事：最新の知識を身に付ける

  - ▶ cf. セキュリティホール Memo

- 危険をさける

  - ▶ セキュリティホールをなくす ( update する )

  - ▶ 対策ソフトを入れる

- 善後策を練る (怪我をしても血がでなければ良い)

  - ▶ 暗号化を行う：情報が流出しない

  - ▶ バックアップを行う：情報が消失しない

## □ 結局は、意識の問題

- 恒常的な努力が必要

  - ▶ 最新情報の入手/適切な判断/効果的な対策の実施

# マルウェア

---

## □ マルウェアとは(What)

### ○ 悪意のあるソフトウェア

- ▶ 利用者でなく作成者の都合で動くソフト(悪さをするソフト)
- ▶ 利用者の情報を勝手に送信する/宣伝を表示する/悪い事の踏台になる

### ○ [反] 通常のソフトは、コンピュータ所有者の都合で、利用される

- ▶ TeX 文章を Typeset したい → PLaTeX システムをインストール/利用
- ▶ 数式処理をしたい → Mathematica をインストール/利用

## □ マルウェアもソフトウェアの一種

### ○ 「動かない」限り「ただのファイル(ディスクの肥やし)」でしかない

- ▶ 「起動」すると「悪さ」をする事になる
- ▶ 勝手に起動する / 利用者を騙して、起動するように誘導する事が多い

### ○ [反] 通常のソフトは、コンピュータ所有者が利益を得るために意識的に起動する

## □ マルウェアの分類

- コンピューターウイルス：勝手にインストールされる/他の PC に感染する
- トロイの木馬：こちらから何か(Web Access)をすると罠に掛けて、マルウェアを起動
- スパイウェア / キーロガー：個人情報勝手に送信してしまう
- アドウェア：此方が望んでいない宣伝表示を勝手に行う
- 他にも色々：詳細は調べよう (人の悪意とはいやはや..)

# マルウェアをさけるには

---

## □ 何故マルウェアに感染してしまう (Why)

### ○ コンピュータの危険対策状態に問題がある

▶ セキュリティホールを放置 (Windows Update / ソフトアップデートをサボる)

▶ ウィルス対策ソフトがない/情報が最新でない (最低限る MSE を..)

### ○ 利用者が騙されてしまう

▶ 脅迫型 : Web アクセス中に突然「危険だ、対策ソフトを入れろ」といわれ..

▶ 利益誘導型 : このソフトを入れると便利になるよ..

## □ マルウェアをさけるには (How To)

### ○ ウィルス対策ソフトのシグネチャ(ウィルス手配書)データ更新 / ソフトの更新

### ○ 安易にソフトウェアをインストールしない

▶ そのソフトが安全かどうかを「確認して」からインストールする

▶ その名前で「ググれば、安全かどうかを判定」する事ができる

## □ マルウェアに「やられているのでは」と思った時は .. (When)

### ○ 挙動が普段と異なる : マルウェア感染を心配してみよう..

▶ 妙に遅い/意図しないサイトのページが表示される/頻繁にエラーが表示される

▶ メールを送ったら、相手から「ウィルス付きのメールが届いた」といわれた

### ○ 情報を収集しよう

▶ 詳しい人(友達/先輩/親/栗野 !!)に相談 / ググってみよう..



# 実習 1: TaskManager の利用

---

## □[実習 1-1] TaskManager の利用

- [Ctrl]+[Alt]+[Delete] でメニューを表示させる事ができる
- 「タスクマネージャの起動(T)」を選ぶと、タスクマネージャが起動する
- 「プロセス」タブを選択すると、色々のプログラムが動いている事が解る
  - ▶ [注意] より高度(危険)なマルウェアの技術に rootKit を利用したものがあるが、これは、これでは発見できない

## □[実習 1-2] プロセスの内容の確認

- プロセスの一覧で表示されている
- 適当な名前を選んでググってみる(ファイル名で検索している事に注意)
  - ▶ 例 1: 「skype.exeとは」で検索 → 当然「スカイプ」のソフトである事が解る
  - ▶ 例 2: 「tvnserver.exeとは」で検索 → TightVNC である事が解る
- 場合によっては、「マルウェア」である事が判明する事もある
  - ▶ [注意] 正常なファイルの名前を、ウイルスが勝手に名乗っている可能性がある

# 暗号化

---

## □ 暗号とは

### ○ コーディングの一種

- ▶ なんらかの「規則」で、「情報を表現する」方法
- ▶ その「規則」が解らないとそれが「表現している情報」が得られない

## □ 暗号の用語

### ○ 文(ファイルの形式)

- ▶ 平文：調べれば、「それが表現する内容」が得られる
- ▶ 暗号文：その表現(ファイル)だけでは内容を知るのが大変困難な表現(鍵があれば見れる)

### ○ 変形(操作)

- ▶ 暗号化(encode)：「平文」を「暗号文」にすること
- ▶ 平文化(decode)：「暗号文」を「平文」にすること

### ○ 鍵(情報を秘密にするための「種」)

- ▶ 暗号化したり平文化するために、必要な情報(cf. パスフレーズ)
- ▶ 対称鍵暗号方式：暗号化と平文化で「同じ鍵」を利用する
- ▶ 公開鍵暗号方式：暗号化と平文化で「異なる鍵」を利用する

# TrueCrypt

---

## □ TrueCrypt とは

### ○ ファイルの「暗号化を行う」ためのツール

- ▶ ファイルを暗号化して入れる「箱(暗号化ボリューム)」が作れる
- ▶ 暗号化ボリュームを作る時にパスワードを設定する
- ▶ 暗号化ボリュームは暗号化されていてパスワードを知らないと見れない

### ○ 暗号化ドライブを作る事ができる

- ▶ 暗号化ボリュームはマウントできる
- ▶ マウントするには、作成した時に利用したパスワードが必要
- ▶ マウントすると、ドライブ(USBメモリみたいなもの)になり、普通にファイルが記録できる
- ▶ 利用しない場合はアンマウントしておく

## □ 暗号化ボリュームとパスワード

### ○ 暗号化ボリュームは暗号化されているので、普通に交換してよい

- ▶ メールや **skype** で送ったり **web** で公開してもよい

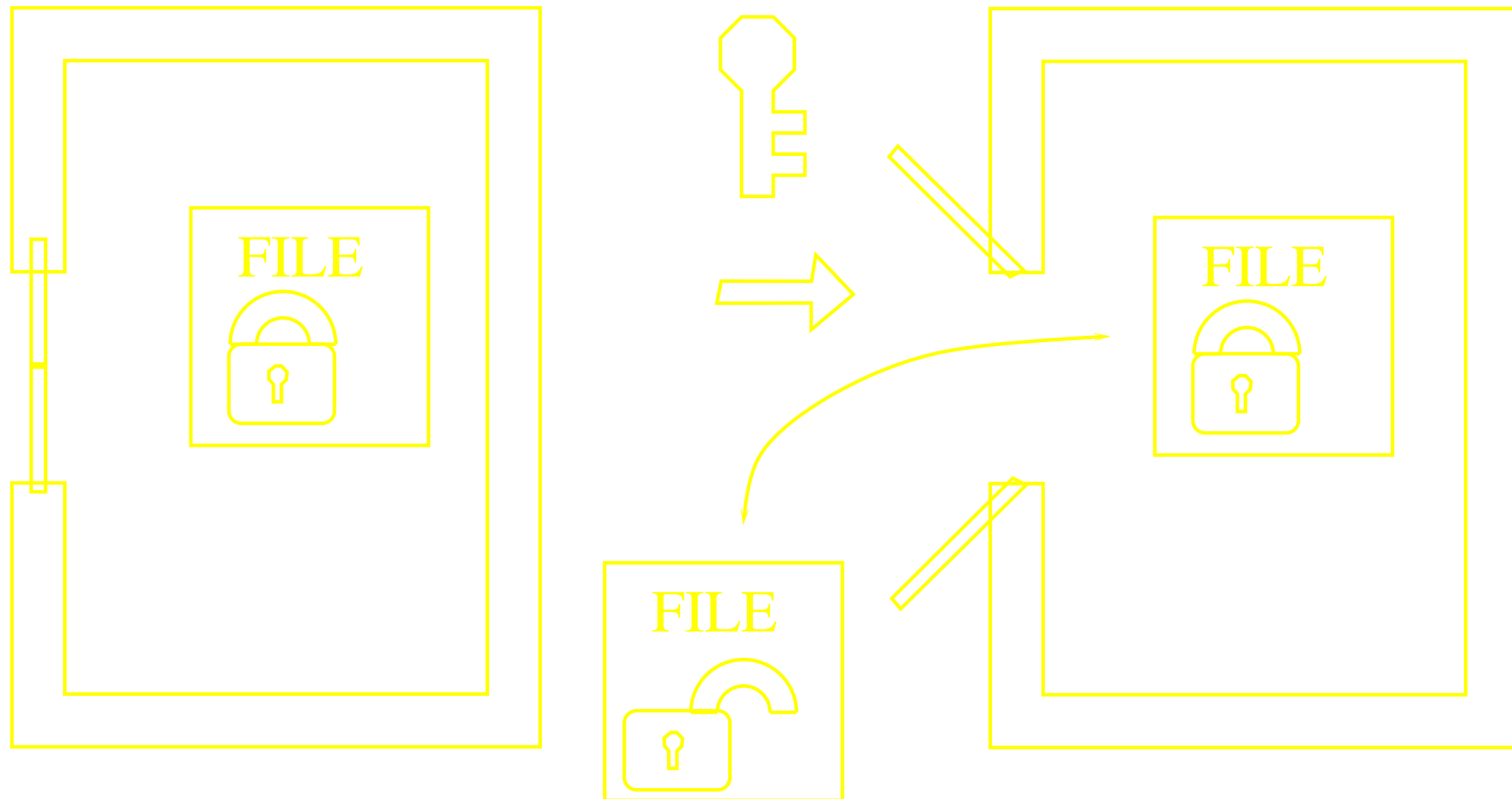
### ○ 暗号化ボリュームの内容を参照するには、パスワードが必要

- ▶ パスワードは、本当は「安全な方法」で送る必要がある
- ▶ 今回は、**skype** を使うが、本当は良くない ( **skype** が覗きされる可能性がある )
- ▶ 理想は「手渡し」だが...

# Truecrypt の仕組み(マウント/アンマウント)

---

マウントする



# 実習 2: TrueCrypt のインストール

---

## □ [実習 2.1] TrueCrypt のインストール

- TrueCrypt のインストールファイルのダウンロード
- TrueCrypt のインストール
  - ▶ 右クリックメニューから、「管理者として実行」すること
- TrueCrypt の言語ファイルのダウンロード
- TrueCrypt の言語ファイルのインストール
  - ▶ Language.ja.xml を c:\Program Files\TrueCrypt にコピーする

## □ [実習 2.2] TrueCrypt の動作確認

- sample-20131001.tc をデスクトップにダウンロード
- TrueCrypt を起動 (sample-20131001.tc をダブルクリックでもよい)
  - ▶ sample-20131001.tc を d: にマウントする
  - ▶ パスフレーズは skype で伝達
  - ▶ ファイルの中身を確認の事 (課題に関する情報がある)

# 実習 3: 自分用のボリュームを作る

---

## □[実習 3.1] 新規ボリュームファイルの作成

- TrueCrypt で、新規ボリュームファイルを作成する

  - ▷ サイズ : 1 M byte / ファイル名 : 自由 / パスフレーズ : 自分で決める

## □[実習 3.2] 内容の作成

- TrueCrypt で、新規ボリュームを e: マウントする

- e: にテキストファイルを作成し、メッセージを入れる

- TrueCrypt で、新規ボリュームをアンマウント

- skype で、ボリュームファイルとパスフレーズを友人におくる

## □[実習 3.3] 手に入れたファイルの確認

- 手に入れたファイルをパスフレーズを利用して e: にマウントする

- 内容を確認する

- e: をアンマウントする

# 実習 4: 課題の提出

---

## □[実習 4.1] 新規ボリュームの作成

- TrueCrypt で、新規ボリュームを作成する

- ▷ サイズ / ファイル名 / パスフレーズ : message.txt を参照

## □[実習 4.2] 課題の作成

- TrueCrypt で、実習 4.1 のボリュームを e: にマウント

- e: に次の二つのファイルを作成する ( message.txt を参照 )

- ▷ message.txt

- ▷ password.txt

- e: をアンマウントする

- 20131001-QQQQ.tc を CST Portal に提出