

コンピュータ演習

01. オリエンテーション

目次

1. 初めに
2. アンケート
3. Teams登録
4. 総合情報技術センターからのお知らせ
5. セキュリティと情報モラル
 - i. Lesson1 コンピューターウイルスを防ぎましょう
 - ii. Lesson2 スパイウェアを防ぎましょう
6. まとめ

初めに

1. 名簿を確認してください。

1組：606

2組：104

です。間違えないように。

2. カードリーダーに学生証かざしましたか？終了時にもかざしましょう。

3.

- Macの人前から座って下さい。

- Windowsの人後ろから座って下さい。

納品間に合わなくて今日持ってきていない場合には、予定の方で座って下さい。

4. モニタの電源を入れて下さい。資料がみれます。

教員・SA紹介

パソコン・テキストは必ず持ってこよう

この演習では「各自のノートパソコンを持参して受講する」となっています。忘れないようにして下さい。

修理などでどうしても持って来れない場合には、相談しにきて下さい。

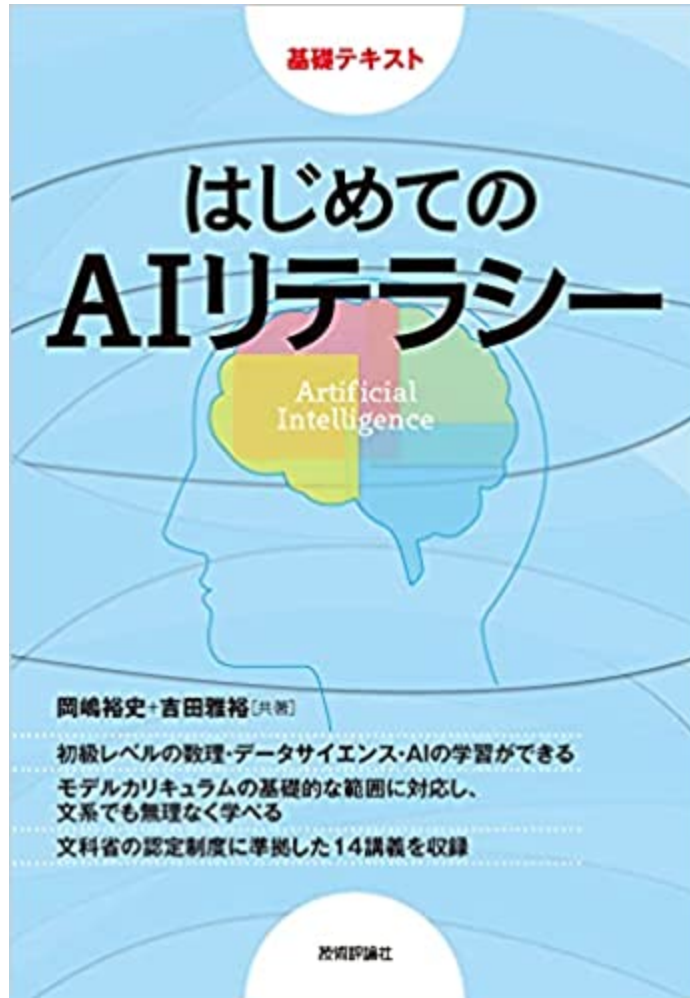
テキストは2冊利用します。

1. noa出版(著)「イチからしっかり学ぶ!Office基礎と情報モラル Office365・Office2019対応」 noa出版(ISBN 978-4-908434-35-8)
2. 岡嶋,吉田(著)「はじめてのAIリテラシー」 技術評論社(ISBN 978-4-297-12038-2)

イチからしっかり学ぶ!Office基礎と情報モラルOffice365・Office2019対応



はじめてのAIリテラシー



流石にパソコンと教科書2冊は...

重いよね。基本は

- ノートパソコン
- 教科書「Office基礎と情報モラル」

を持ってきて下さい。初めてのAIリテラシーを使うときは「来週持ってきて」というようにします。

必修科目

「コンピュータ演習」は必修科目です。落とすと来年、もう一度再履修となります。確実に取りましょう。

前期後期の通年授業で30回です。

演習序盤について

- デジタルデザイン基礎演習I
- コンピュータ演習

パソコンに慣れるための内容となりますので、多少内容被ると思います。

基本操作がわからないと何もできませんから、確実に身につけて下さい。

HPの資料

<https://sammyppr.github.io/>

に置きます。これは学外からも閲覧可能です。予習復習にはもちろん、あれなんだったけー？みたいな時に利用してください。

シラバス

確認してみましょう。

これが共通シラバスなのですが、本コースでは中身を少し変えながら行います。

今日すること

納品の間に合っていない学生もいることが予想されますので、今日はパソコンは基本的に使いません。

次回からパソコン使っていきます。

1. アンケート

2. Teams登録

3. セキュリティと情報モラル: Lesson1 Step1,2

アンケート

<https://forms.office.com/r/URUULca1Jf>



Teams登録

「3qnywjy」で「2022_メ文_コンピュータ演習」に参加して下さい。

通知はONにして下さい。

[参考](#)

総合情報技術センターからのお知らせ

いくつか配布資料が来ています。確認してみましょう。

- 総合情報技術センターからのお知らせ
- パスワードの適切な管理、及びパスワードルール周知のお願い
- ユーザーIDとパスワードの取り扱いについて
- 大学メールの設定方法について
- 学内情報サービスについてのお知らせ
- 有線LANネットワーク 接続手順書

なお、学生便覧P.63-65にある程度まとまっています。

セキュリティと情報モラル

STEP1 セキュリティを高めましょう

Lesson1 コンピューターウイルスを防ぎましょう

Lesson2 スパイウェアを防ぎましょう

Lesson1 コンピューターウイルスを防ぎましょう

セキュリティとは？

コンピュータを利用するにあたっての安全性を確保すること

被害者になるだけでなく...

加害者になる可能性もある。

深刻な 3 つの問題

1. コンピュータウイルスなどのマルウェア (悪意のあるソフトウェア)
2. 不正アクセスによる情報漏えい
3. フィッシング詐欺

1. コンピュータウイルス

特徴

- 破壊活動を行う
- 自己増殖する

感染経路

- ネットから意図せずダウンロード
- Eメール添付
- CD-R や USB メモリからのコピー
- 悪意ある Web ページの閲覧
- ファイル交換ソフト

などから侵入してくる

ウイルスの種類

トロイの木馬：安全と見せかけて破壊活動を行う

ワーム：自己増殖を繰り返しながら破壊活動を行う

ボット：外部からの指令を受けて情報を送信したり他のコンピュータに対して一斉攻撃をしかけたりする

症状は？

- 頻繁にハングアップする
- システムが起動しない
- ファイルがなくなる・破壊されている
- 妙なアイコンがでる
- 勝手にインターネットに接続しようとする
- 画面表示が以上になる
- ウイルス対策ソフトの更新サイトなどに接続できなくなる
- いつもと何か違うと感じる

どうすればいい？

セキュリティ対策を行う必要がある。

- 定期的な OS アップデート
- セキュリティ対策ソフトの導入
- ウイルス定義ファイルの定期的な更新

ウイルス感染予防の心構え

- 差出人に心当たりのないメールの添付ファイルは開かない
- 特に.exe ファイルは開かない (mac では開けないけど)
- .doc, .docx, .docm, .xls, .xlsx, xlsx, .ppt, .pptx, .pptm も知らない人からのファイルは危険
- メール本文中の URL は安易に開かない
- ファイルのダウンロードは信頼できるページから
- 提供元が不明なフラッシュメモリ、CD-ROMなどを接続しない。

One point! 拡張子

ファイルの種類を表すもの。

基本は「ファイル名.xxxx」の様にファイル名の後ろにピリオドと数文字の形式となる。

OSの設定によって、見えなくなっていることがある。

感染したら？

- ネットワークから遮断
- 詳しい人に相談!

最悪、データをリセットかける (初期化) 必要があります。データのバックアップは大事!

番外 1:Android の人

- iPhone では本当にウイルスの数が少ない
- Android では 200 万種類以上出回っていると言われている
アプリの配布形態の違いによる。

Androidの人は必ずウイルス対策ソフトを入れよう。

番外 2:IoT 機器が盲点

- 最近では、多くの家電がインターネットに接続されている
- 接続されているものは全てコンピュータ
- コンピュータであれば、家電であってもウイルス感染の恐れがある

NHK スペシャル「あなたの家電が狙われている ~インターネットの新たな脅威~」 (18:51-28:28)

Lesson2 スパイウェアを防ぎましょう

スパイウェアとは？

コンピュータに侵入してユーザの行動や個人情報などを収集し、外部へ送り出すプログラムのこと

ユーザに気づかれないように動作しています。

個人情報が出ると？

非常に大きな被害につながる可能性があります。ID,Password が盗まれてしまえば、なりすまされてしまいます。

共用パソコンでは特に注意

パスワードを保存してしまうと、他の誰かがあなたのふりをできることになります。

共用パソコンでは

- ID/Passwordを保存しない
- Webサービスを利用した後は必ずログアウト・サインアウト

としましょう。

スパイウェアの侵入経路

インターネットから入手できるオンラインソフトに組み込まれているケースがほとんど。

利用条件にスパイウェアを明記している場合が多いですが、読まないために知らずに許諾している場合が多い。

そのため、違法であるとは言い切れない。

スパイウェアから送り出される情報

- 本名・住所・電話番号・メールアドレスなどの個人情報
- ブラウザーで閲覧した Web サイトや何をクリックしたかの履歴
- Web サービスで入力したユーザ ID・パスワード・クレジットカード番号など
- キーボードから入力した文字や、インストールされているソフトウェアの種類など

スパイウェア侵入後の症状

多くの場合は、気づきません。ですが

- ポップアップ広告が表示される
- インジケータに見知らぬアイコンが追加される
- ブラウザーの起動時に表示されるページが変更される
- ブラウザにツールバーが追加される
- システムが不安定になる

などの症状が現れることがあります。

対策

Windows10,11 には「Windows Defender」というソフトがあり、スパイウェア対策をしてくれますが、ウイルス対策はしてくれません。(と教科書に書いてありますが、最近のはウイルス対策もしてくれる気がします...)

来週みんなに推奨するウイルスバスター(Win用)Avira(Mac用)はスパイウェア対策・ウイルス対策の両方の機能が備わっています。

まとめ

それでは来週必ず

- ノートパソコン
- 教科書「Office基礎と情報モラル」

を持ってくる下さい。

帰りに学生証ピッも忘れずに