科目名 Course Name	開講年次	開講学期	曜日・時限
情報セキュリティ基礎 Information Security Basics	2年	後期	別途、時間割参照

単位数	授業の形態	授業の性格	履修上の制限
2単位	講義	選択　（特になし）	特になし

当該科目の理解を促すために受講しておくことが望まれる科目

特になし

同時に履修しておくことが望まれる科目

特になし

担当者に関する情報

氏名	研究室の場所	オフィスアワー	電話番号・メールアドレス
亀田和則	講義棟２階	月曜日	授業中に指示します

授業の概要

情報化社会の進展により、情報資産の侵害に対する脅威が問題となっている。本講義では、情報セキュリティの基礎として、セキュリティの考え方や基礎技術について学ぶ。

授業の目標

①ネットワークに潜む脅威について、説明できるようにする。
②暗号技術とＰＫＩについて、説明できるようにする。
③セキュリティ対策について、説明できるようにする。
④セキュリティポリシーの重要性について、説明できるようにする。

授業の方法

毎時間、理解できたことをレポートとしてまとめ提出する。
理解度の確認を２回実施する。

学習の成果（学習成果）

授業の目標①②③④を達成すると、情報セキュリティの重要性やネットワークのリスクを小さくするための方策を説明することができる。

授業のスケジュールと内容

第1回目	ガイダンス（学習成果、成績評価）情報セキュリティとは　　情報セキュリティの位置付けと意義
第2回目	情報セキュリティの考え方 情報セキュリティの6要素，時系列で見た考え方，管理方法で見た考え方，リスク管理で見た考え方
第3回目	脅威（１） 情報資産と脅威，脅威の分類，不正アクセスの手順，ポートスキャン
第4回目	脅威（２） パスワード・クラック，バッファーオーバーフロー，セキュリティホールの利用，クロスサイトスクリプティング，盗聴
第5回目	脅威（３） リソースの不正利用，コンピュータウイルス，ノートPCの脆弱性，ソーシャルエンジニアリング，無線LANの脆弱性，SQLインジェクション，フィッシング詐欺
第6回目	理解度の確認１と解説

第7回目	暗号技術とPKI（１） 共通鍵暗号，公開鍵暗号，ハッシュ関数，電子署名
第8回目	暗号技術とPKI（２） PKI，X.509証明書，SSL，S/MIME
第9回目	セキュリティ対策（１） 技術面の対策，ファイアウォールとは，ファイアウォールの機能，ファイアウォールの種類
第10回目	セキュリティ対策（２） サーバの要塞化，脆弱性検査，有効なウイルス対策，spamメール対策，アクセス制御
第11回目	セキュリティ対策（３） 認証の強化，バイオメトリックス認証，VPN，IDS・IDP
第12回目	セキュリティ対策（４） 可用性対策，運用面の対策，廃棄方法，災害対策
第13回目	セキュリティ対策（５） インシデント対応，リモート接続の脆弱性対策，ポリシー策定による対策，情報漏洩対策
第14回目	セキュリティポリシー策定 情報セキュリティマネジメントの必要性，情報セキュリティポリシーの概念，情報セキュリティポリシーのマネジメントサイクル
第15回目	理解度の確認２と解説

成績評価の方法と基準

評価の領域	割合	評価の基準
授業参加態度		
レポート	40%	毎時間のレポートがが該当する。満点となる条件は「丁寧な文字が書かれており、一回読むと内容が理解できる」である。
調査報告書		
小テスト	60%	理解度の確認が該当する。試験１つあたりの配点は60点/2である。満点となる条件は「すべての解答が正解」である。
試験		
発表内容（態度含む）		
その他		

教科書と参考図書

教科書：「図解入門よくわかる最新　情報セキュリティの基本と仕組み」（出版：秀和システム）（著者：高橋寛）※必ず購入し、第一回目の授業から持参すること。

履修上の留意点・ルール

教科書を購入していない学生はこの授業を履修出来ない。
２回の遅刻は１回の欠席となる。