教科目名　情報セキュリティー　(Information Security)

学科名・学年　：電気電子情報工学専攻　1年
単位数など　：選択　2単位　（前期1コマ，学習保証時間22.5時間）
担当教員　：鷺　浩二

授業の概要

本授業では，情報を安全に管理，運用するための技術として情報セキュリティを学ぶ．情報セキュリティとして必要な暗号理論，ネットワークセキュリティ，個人認証技術，耐タンパデバイスについて，理論と応用技術を習得する．また，実際の導入例など具体的なセキュリティ技術を適宜紹介することにより，実践的な知識を養う．

達成目標と評価方法　　**大分高専目標（E1），JABEE目標(d2a)**

(1) 情報化社会における，情報セキュリティ技術の重要性を理解する．（定期試験と課題）
(2) 暗号技術に関する理論と実際の応用例に関して学ぶ．（定期試験と課題）
(3) ネットワークセキュリティ技術と不正アクセスに対する対処法を習得する．（定期試験と課題）
(4) セキュリティシステムを構築するための装置，システム，評価方法を学ぶ.(定期試験と課題)

回	授業項目	内容	理解度の自己点検
1	1．情報セキュリティ技術 ・ セキュリティへの脅威 ・ セキュリティ対策概要	○ 情報化社会における，情報セキュリティ技術の重要性を理解する．	【理解の度合い】
2	2．共通鍵暗号 ・ ブロック暗号の構造 ・ ＤＥＳ，ＡＥＳ	○ 共通鍵暗号方式について，そのしくみと特徴および応用方法を習得する．	
3	3．公開鍵暗号 ・ 公開鍵暗号の原理，実現方法	○ ネットワークセキュリティの重要な技術である公開鍵暗号方式に関して，そのしくみと特徴および応用方法を習得する．	
4	・ 素因数分解方式（ＲＳＡ） ・ 楕円曲線公開鍵暗号方式		
5	4．ディジタル署名 ・ ディジタル署名の概要 ・ ハッシュ関数	○ データの改ざんを防止するディジタル署名の理論と特徴を理解する．	
6	5．ネットワークセキュリティ ・ クライアント認証 ・ 公開鍵認証社会基盤（ＰＫＩ）	○ 高度情報化社会を構築する上で，必要になる認証，公証などのディジタル化技術，不正アクセス検出のしくみ特徴を理解する	
7	6．インターネットセキュリティ ・ ＩＰＳＥＣ		
8	・ ＳＳＬ（ＴＬＳ），Ｓ／ＭＩＮＥ		
9	7．不正アクセス ・ コンピュータウイルス ・ ファイヤーウォール	○ 不正行為を未然に防ぐ技術や耐タンパデバイス，個人認証技術に関して，そのしくみと特徴，実際の応用例に関して習得する．	
10	・ 不正侵入検出技術 8．耐タンパデバイス ・ 耐タンパデバイスの原理		
11	・ ＩＣカード	○ 今後必要となってくるセキュリティ評価に関する考え方と，情報化社会における倫理について理解する．	
12	9．個人認証技術（バイオメトリクス） ・ 必要性と技術 ・ 個人認証技術の応用例		
13	10．セキュリティ評価と情報通信倫理 ・ ISOにおけるセキュリティ評価		
14	・ 情報化社会における倫理		
15	前期期末試験		【試験の点数】　　点
	前期期末試験の解答と解説		

履修上の注意	講義の途中でもわからなくなったら，何時でも質問してよいことにする．
教科書	宮路充子，菊池浩明　編著，「情報セキュリティ」，オーム社．
参考図書	松本隆明，岡本龍明 編著「情報セキュリティ技術」，電気通信協会． 楫 元 著「工科系のための初等整数論入門」，培風館．
関連科目	データ通信工学，アルゴリズム特論，情報理論
総合評価	達成目標の(1)～(4)について，定期試験と課題で評価する． 定期試験の成績(80%)および課題の評価(20%)を合計し，その合計から，出席状況・授業態度により20%を上限とした減点を行い，これを総合評価とする．単位取得条件は，総合評価が60点以上とする．

【総合達成度】

【総合評価】　　点