教科目名　情報セキュリティー　(Information Security)

専攻名・学年　：　電気電子情報工学専攻　1 年　（教育プログラム　第 3 学年　○科目）
単 位 数 な ど　：　選択　2 単位　（前期 1 コマ,授業時間 23.25 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説明できる.(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を説明でき，自主的・継続的に学習できる.(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説明できる.(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,評価方法を説明できる.(定期試験と課題)

回	授　業　項　目	内　容	理解度の自己点検
1 2 3 4 － 6 7	1.情報セキュリティ技術 ・　セキュリティへの脅威，対策 2.共通鍵暗号 ・　ブロック暗号の構造 ・　ＤＥＳ，ＡＥＳ 3.公開鍵暗号 ・　公開鍵暗号の原理,実現方法 ・　初等整数論 ・　素因数分解方式（ＲＳＡ） 4.ディジタル署名 ・　ディジタル署名の概要 ・　ハッシュ関数	○　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. ○　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. ○　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 ○　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	【理解の度合い】
8	前期中間試験		【試験の点数】　　点
9 10 11 12 13 14	前期中間試験の解答と解説 ５．暗号プロトコル ・　秘密分散法 ・　マルチパーティプロトコル ６．・ゼロ知識証明と社会システム ・　ブラインド署名，電子現金 ７．ネットワーク・インターネットセキュリティ ・　クライアント認証，ＰＫＩ ・　IPSEC,SSL(TLS),S/MINE ８．不正アクセス ・　ウイルス・ファイヤーウォール ・　不正侵入検出技術 ９．耐タンパ・バイオメトリクス ・　必要性と技術，原理 ・　ＩＣカード・個人認証技術 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 ・　情報化社会における倫理	○　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 ○　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. ○　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.	【理解の度合い】
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 事前に Web ラーニングプラザで「情報セキュリティコース」を受講しておくことが望ましい（http://weblearningplaza.jst.go.jp）	【総合達成度】
教　科　書	宮地充子,菊池浩明,「情報セキュリティ」,オーム社	
参 考 図 書	鷺 浩二 「Excel で学ぶ暗号技術入門」，オーム社 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 「工科系のための初等整数論入門」,培風館.	
自学上の注意	5 課題×3 時間以上の自宅学習と試験準備 2 回×8 時間で合計 30 時間以上の自学自習が必要	
関 連 科 目	ネットワークアーキテクチャ，情報理論(E 科),通信工学Ⅰ・Ⅱ(S 科)	
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. 総合評価＝定期試験の成績(中間 40%+期末 40%)＋課題の評価(20%) 単位取得条件は,総合評価が 60 点以上とする．再試験の受験資格は,課題を全て提出した者に与える.	【総合評価】　　点