

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 (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, 学習保証時間 22.5時間)

担当教員 : 霧 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ーを学ぶ.情報セキュリティーとして必要な暗号理論,ネットワークセキュリティー,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ー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,情報セキュリティー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る.(定期試験と課題) | | | |
| (3) ネットワークセキュリティー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) セキュリティー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 | 1.情報セキュリティー技術 ・ セキュリティーへの脅威 ・ セキュリティー対策概要 | 情報化社会における,情報セキュリティー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 | 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ー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 | ・ 初等整数論 ・ 素因数分解方式(RSA) | | |
| 5 | 4.デジタル署名 ・ デジタル署名の概要 ・ 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ー ・ 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ー ・ IPSEC | | |
| 8 | ・ SSL(TLS),S/MIME | | |
| 9 | 7.不正アクセス ・ コンピュータウイルス ・ ファイアウォール | 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 | 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ー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.セキュリティー評価と情報通信倫理 ・ ISOにおけるセキュリティー評価 ・ 情報化社会における倫理 | | |
| 14 | | | |
| 15 | 前期期末試験 前期期末試験の解答と解説 | | 【試験の点数】 点 |
| 履修上の注意 | 講義の途中でわからなくなったら,何時でも質問してよいことにする. | | 【総合達成度】 |
| 教科書 | 宮路充子,菊池浩明 編著,「情報セキュリティー」,オーム社. | | |
| 参考図書 | 松本隆明,岡本龍明 編著「情報セキュリティー技術」,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 | コンピュータ (E科),データ通信工学(S科),アルゴリズム特論 | | |
| 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,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. | | |