

関連科目，教科書および補助教材	
関連科目	なし
教科書	マスタリングTCP/IP 入門編 第4版, 竹下 隆史ら (オーム社)
補助教材等	Powerpoint スライドの縮小版を配布する
学習上の留意点	
<p>情報ネットワークを支える技術は、暗号化技術を除けば、単純なアルゴリズムの集まりである。故に、論理的に考えれば技術概要を理解するのは容易と言える。技術的な詳細は概ね RFC (Request For Comments) に書かれており、講義で取り上げるテーマと関連した RFC を随時、紹介するから、関心のある者は各自で読むことを勧める。</p> <p>暗号化技術は数学、特に近年は代数学が多用されており、独力での理解が困難になりつつあるが、講義の最中に関連書籍を紹介するから、関心のある者は読んで欲しい。</p> <p>指定した教科書がなくても理解できるように講義を進めるが、技術の詳細の理解やレポート課題に取り組む上では購入した方がよい。なお、この教科書はエンジニア向けに書かれているため、将来的にも役立つだろう。</p>	
担当教員からのメッセージ	
<p>担当教員が情報ネットワークに関心を持ったのは、大学院修士課程の頃に情報処理センターにUNIXマシンが導入されてからである。これをきっかけにIT企業に就職し、ネットワーク関連の部署にて勤務した(配属希望が通ってラッキーだった)。そこで感じたのは、ネットワーク技術は学問的な部分と人間くさい実装が同居した世界ということである。論理的に理解できる箇所、準最適でよとする箇所が混在しているという点に面白みを感じる。</p> <p>また、ネットワーク技術を含む情報技術分野はアップデートが頻繁であり、10年前の常識があったという間に通用しなくなる。講義中に最新情報を提供できるよう努めるが、本講義の受講者もネットワーク技術の進化に敏感であって欲しい。</p>	

授業の明細			
回	授業内容	到達目標	自学自習の内容 (予習・復習)
1	TCP/IPの基礎(1): ・OSI参照モデルとTCP/IP ・IPv4からv6への移行	・OSI参照モデルとTCP/IP階層モデルを対応付け、各層の役割を理解できる。 ・パケットの概念、IPヘッダ、TCPヘッダの有する情報、IPアドレスクラス、DNSの概要を理解できる。	(復習) IP/TCPヘッダを構成する各フィールドの役割を調査し、レポートにまとめる。
2	TCP/IPの基礎(2): ・ネットワークプロトコルの実装(イーサネット(CSMA/CD)、トークンリング)	コンテンション方式、トークンパッシング方式それぞれの仕組み、特徴、利点・欠点を理解できる。	(復習) early token release等、現在のトークンパッシングで用いられている技術を調査する。
3	誤り制御(1): ・誤り制御の考え方 ・ARQ (Automatic Repeat reQuest) とFEC (forward Error Correction)	・Stop-and-Wait, Go-Back-N, Selective Repeat の各ARQの考え方および現実的なRTOの決定方法を理解できる。 ・FECの必要性和概要を理解できる。	(復習) V. Jacobsonの論文を読み、RTOの決定アルゴリズムを理解する。
4	誤り制御(2): パリティ損失の検出方法、パリティチェック、ハミング符号	CRC誤り検出、ハミング符号による誤り訂正の理論的背景を理解できる。	(復習) ハミング符号に関する演習問題を解く。
5	IP(1): ルーティングの概念、RIP (Routing Information Protocol), OSPF (Open Shortest Path First)	・ルーティングの概要を理解できる。 ・RIPにおけるルーティングテーブルを構築できる。 ・RIPとOSPFの組み合わせが現実的解だと理解できる。	(復習) 仮想的なネットワークに関して、RIPによるルーティングテーブル構築の課題に取り組む。
6	IP(2): IPの分割処理と再構築処理、ARP, ICMP	・様々なデータリンク間での通信のためのパケット分割の必要性を理解できる。 ・ARPによるMACアドレスの取得、ICMPによる障害通知の仕組みを理解できる。	(復習) パケット分割処理の抱える問題点への解答のひとつである経路MTU探索について調査する。
7	TCP: TCPの基礎、ウィンドウ制御、フロー制御	・通信速度を向上させるためのウィンドウ制御とフロー制御の必要性を理解できる。 ・輻輳制御によるネットワークの混雑解消の仕組みを理解できる。	(復習) ウィンドウ制御、フロー制御に関する演習問題を解く。
8	アプリケーションプロトコル: DNS, WWW, 電子メール, 遠隔ログイン	HTTP, Cookie, SMTP, POP, telnet の各プロトコルの概要を理解できる。	(復習) POP before SMTP 等、セキュリティ向上のための仕組みを調査する。
9	中間まとめ	中間まとめとしてネットワークプロトコル、ルーティング、パケット分割を再整理するとともに、中間試験を実施する。	
10	セキュリティ(1): ネットワーク・セキュリティの概要	不正アクセス事例を把握し、セキュリティ確保の必要性を理解できるとともに、ポートスキャンやDoS等の準備行動の技術的背景を理解し説明できる。	(復習) 近年の不正アクセスの事例を調査し、その大規模化・社会問題化を理解する。
11	セキュリティ(2): 共通鍵・公開鍵暗号と電子署名の理論およびその実装	・共通鍵暗号・公開鍵暗号の概要を理解するとともに、DESやRSAの実装を理解できる。 ・共通／公開鍵暗号のハイブリッドの必要性を理解できる。	(復習) 暗号化技術の正当性を担保するPKIについて調査する。
12	無線LANの概要: IEEE802.11規格, CDMA/CA	・CSMA/CAの仕組みと特徴を理解できる。 ・IEEE802.11a/b/g/n/acの特徴を説明できる。 ・MIMOとチャネル・ボンディングの概要を説明できる。	(復習) IEEE802.11acで用いられる高速化技術を調査する。
13	無線LANのセキュリティ: WEP/WPA/WPA2とその技術	・ワイヤレスネットワーク特有の脆弱性を認識できる。 ・WEP/WPA/WPA2の概要の理解とともに、その技術的背景であるTKIP, AES等の暗号化技術の詳細を理解できる。	(復習) TKIP, AESとWPAとを比較し、前者のセキュリティ上の強度をレポートにまとめる。
14	無線PAN (Personal Area Network): IEEE802.15 RFID, Bluetooth, ZigBee	・PANの必要性、BluetoothやZigBeeの仕様を理解できる。 ・Bluetooth, ZigBeeのネットワーク構成を理解できる。	(復習) Bluetoothのネットワーク構成であるピコネット、スキャタネットについて調査する。
		期末試験	
15	学習事項のまとめおよび授業改善アンケートの実施	・情報ネットワークを支える技術を整理し、wired / wireless / mobileそれぞれの分野での技術の共通性や特性を理解できる。	
総学習時間数			90時間
講義			30時間
自学自習			60時間