

学科名	学年	授業のタイトル (科目名)	
工業専門課程 情報処理システム科	1	情報セキュリティ	
授業の種類	授業担当者	実務経験	
<input checked="" type="checkbox"/> 講義 <input type="checkbox"/> 演習 <input type="checkbox"/> 実習	寺井 健一郎	●有 ○無	
[実務経験歴]			
IT企業にシステムエンジニアとして15年勤務し、メインフレームやUNIX上で稼働するソフトウェア製品の新規開発、機能拡張、日本語化、及びインシデント発生時のサポートに従事した。			
単位数 (授業の回数)	時間数	配当時期	必修・選択
2 単位 (30 回)	60 時間	<input type="checkbox"/> 前期 <input type="checkbox"/> 後期 <input checked="" type="checkbox"/> 通年	<input type="checkbox"/> 必修 <input checked="" type="checkbox"/> 選択
[授業の目的・ねらい]			
①情報セキュリティに対する脅威 (マルウェア、各種攻撃など) を理解する ②脅威に対する対策 (暗号化、認証、署名など) のしくみを理解する ③セキュリティを強化する技術的な方法 (ファイアウォール、サーバのセキュリティ対策など) を理解する ④情報セキュリティポリシーの設定やセキュリティ情報の入手など、セキュリティ管理者の作業を理解する			
[授業全体の内容の概要]			
①セキュリティの3要素 (機密性・完全性・可用性) と、脅威・脆弱性について ②各種攻撃と、その対策 (暗号化、認証、署名など) について ③リスク分析・評価方法、セキュリティ関連の法規、ガイドラインについて ④システム構築におけるセキュリティ対策について			
[授業終了時の達成課題(到達目標)]			
①情報セキュリティに関して、ひとりひとりが気を付けること、職場のセキュリティ管理者が行うこと、プログラマやSEとして留意すること、を理解し、行動できること ②基本情報技術者試験 および 情報セキュリティマネジメント試験の、セキュリティ分野の問題が理解できる			
[準備学習の具体的な内容]			
毎授業ごとに復習の有無の確認を行い、講義・実習を進める。授業終了時には、講義内容の確認と次回の授業内容を説明し、復習・予習ができるようにする。			
[使用テキスト]		[単位認定の方法及び評価の基準]	
使用テキスト 令和08年 情報セキュリティマネジメント合格教本 (技術評論社) 参考文献 必要に応じて授業の中で紹介する。		定期試験と出席日数の両方が次の規定に達した場合に認定する。 ・試験の点数は60点以上を合格点とする。 ・全出席日数の4分の3以上の出席が必要。 評価基準 定期試験70%、平常点 (出席、講義の参加度、ワークシートなどの提出物) 30%とする。	
[授業の日程と各回のテーマ・内容・授業方法]			
1回	授業内容について (オリエンテーション)、初回アンケート、セキュリティの3要素		
2回	情報セキュリティの概要、資産価値、脅威、脆弱性とリスクの関係性		
3回	脅威と脆弱性の種類		
4回	マルウェアの種類と対策		
5回	脅威と脆弱性のまとめ、パスワード関連の攻撃		

6回	パスワード関連関連の攻撃、サイバー攻撃手法（不正アクセス、盗聴など）
7回	サイバー攻撃手法（なりすまし、フィッシング、標的型攻撃など）
8回	まとめと振り返り
9回	サイバー攻撃手法（DDoS攻撃、ソーシャルエンジニアリングなど）
10回	サイバー攻撃手法（SQLインジェクション、XSSなど）
11回	暗号化（暗号化の目的、共通鍵、公開鍵・秘密鍵）
12回	暗号化（盗聴防止方法）
13回	認証（パスワード、チャレンジレスポンス認証、ワンタイムパスワード）
14回	認証（生体認証、2段階認証）
15回	まとめと振り返り
16回	デジタル署名（ハッシュ関数、改ざん検知、本人確認）
17回	公開鍵基盤（PKI）、認証局(CA)、SSL/TLSのしくみ、常時SSL/TLS化
18回	暗号化・認証・デジタル署名のまとめ
19回	TCP/IPの概要、ネットワークを利用した攻撃（ポートスキャンなど）
20回	ネットワークを利用した攻撃（ICMP Flood、DNSキャッシュポイズニングなど）
21回	リスクマネジメント（分析、評価、対応）
22回	まとめと振り返り
23回	情報セキュリティポリシー、基本方針・対策基準・対策実施手順
24回	ISMS認証、JIS Q 27000シリーズ
25回	セキュリティ関連のガイドライン、セキュリティの窓口（CSIRT、JPCERT/CC）
26回	マルウェア（種類、感染経路、対策、ビヘイビア法など）
27回	システムへの不正アクセス防止（ファイアウォール、DMZ、プロキシサーバ）
28回	システムへの不正アクセス防止（IDS、RADIUS、SSH など）
29回	システムへの不正アクセス防止（VPN、ログ管理 など）、人的対策
30回	まとめと振り返り