

科目名	情報セキュリティ特論		英文表記	Advanced Information Security		2016/3/22	
科目コード	6309					作成	
教員名:伊波靖 技術職員名:							
対象学科/専攻コース			学年	必・選	履修・学修	単位数	授業形態
創造システム工学専攻・情報工学コース			専2	選	学修	2単位	講義
科目目標 【MCC目標】		情報セキュリティを確保するためにOSに実装された機能と、セキュリティポリシーに基づいたセキュアOSの設定法について理解する。また、実際の不正アクセスに使用される脆弱性の利用法を理解し、それを検知する脆弱性検査手法について具体的なツールにより理解する。Webアプリケーションに対する不正プログラムの具体的な手法を理解し、それを防ぐセキュアプログラミング手法について理解する。 【V-D-8】コンピュータを扱っている際に遭遇する脅威に対する代表的な対策について説明できる。 【V-D-6】主要なサーバの構築方法を理解している。					
総合評価		課題および演習を実施し作成したレポートで評価(100%)し、60%以上を合格とする。					
科目達成度目標とJABEE目標との対応	目標割合	科目達成度目標(対応するJABEE教育目標)	達成度目標の評価方法	ルーブリック			
				理想的な到達レベル(優)	標準的な到達レベル(良)	最低限必要な到達レベル(可)	セルフチェック
	40%	① 情報セキュリティを確保するためにOSに実装された機能と、セキュリティポリシーに基づいたセキュアOSの設定法について理解する(A-2)	各種OSに実装された機能と、セキュリティポリシーに基づいたセキュアOSの設定法に関する演習を行いレポートで評価する	情報セキュリティを確保するためにOSに実装された機能と、セキュリティポリシーに基づいたセキュアOSの設定法について理解できる。	情報セキュリティを確保するためにOSに実装された機能と、セキュリティポリシーに基づいたセキュアOSについて理解できる。	情報セキュリティを確保するためにOSに実装された機能について理解できる。	
	30%	② 脆弱性検査手法について具体的なツールにより理解する(A-2)	脆弱性検査手法に関する演習を行い作成したレポートで評価する	脆弱性検査手法について具体的なツールを用いて、脆弱な設定について検出ができる。	脆弱性検査手法について具体的なツールの使用法について理解できる。	脆弱性検査手法について理解できる。	
30%	③ 不正プログラムの具体的な手法を理解し、それを防ぐセキュアプログラミング手法について理解する(A-2)	Webアプリケーションを作成し、不正アクセスに対する対策法を実装し作成したレポートで評価する	Webアプリケーションにおける攻撃手法について理解し、それを防ぐセキュアプログラミング手法について理解できる。	実際の不正プログラムに基づき、具体的な手法について理解できる。	バッファオーバーフローやXSSなどの不正プログラムで用いられる手法について理解できる。		
本科・専攻科教育目標	1	2	3	4	JABEEプログラム名称	メディア情報工学	
			◎		JABEEプログラム教育目標	A-2	
評価方法と評価項目および関連目標に対する評価割合							
評価項目	目標との関連	定期試験	小テスト	レポート	その他(演習課題・発表・実習・成果物)	総合評価	セルフチェック
基礎的理解	①②③	0	0	90	10	100	
応用力(実践・専門・融合)	①②③			40		40	
社会性(プレゼン・コミュニケーション・PBL)	①			50		50	
主体的・継続的学修意欲					10	10	
主体的・継続的学修意欲						0	
授業概要、方針、履修上の注意	情報セキュリティを確保するためにOSに実装された機能と、実際の不正アクセス手法とその防御法について学ぶ。セキュリティポリシーに基づいたセキュアOSの設定法について学ぶ。また、脆弱性検査手法について具体的なツールにより理解を深め、それを防ぐためのセキュアプログラミング手法について学ぶ。						
教科書・教材	自作教材及びパワーポイントなどのプレゼン資料						

授 業 計 画

週	授 業 項 目	時間	授 業 内 容	自学自習 (予習・復習) 内容	セル フ チエッ ク
1	ガイダンス	2	授業の進め方や成績評価方法、受講上の注意事項など。	講義資料の予習	
2	OSにおけるセキュリティ機能の変遷	2	OSにおけるセキュリティ機能の変遷について学ぶ。	講義資料の予習	
3	セキュアOS(1)	2	各種セキュアOSの考え方について学ぶ。 【V-D-6:3-1】主要なサーバの構築方法を理解している。	講義資料の予習	
4	セキュアOS(2)	2	各種セキュアOSの設定方法について学ぶ。 【V-D-6:3-1】	講義資料の予習	
5	セキュアOS(3)	2	各種セキュアOSの設定方法について学ぶ。 【V-D-6:3-1】	講義資料の予習	
6	様々な脆弱性(1)	2	不正アクセスに用いられる脆弱性について学ぶ。 【V-D-8:3-2】コンピュータを扱っている際に遭遇しうる脅威に対する代表的な対策について説明できる。	講義資料の予習	
7	様々な脆弱性(2)	2	不正アクセスに用いられる脆弱性について学ぶ	講義資料の予習	
8	脆弱性検知手法(1)	2	脆弱性検知手法等について学ぶ。 【V-D-8:3-2】	講義資料の予習	
9	脆弱性検知手法(2)	2	脆弱性検知手法等について学ぶ。 【V-D-8:3-2】	講義資料の予習	
10	不正アクセス手法と防御(1)	2	不正アクセス手法と防御について学ぶ。 【V-D-8:3-2】	講義資料の予習	
11	不正アクセス手法と防御(2)	2	不正アクセス手法と防御について学ぶ。 【V-D-8:3-2】	講義資料の予習	
12	Webセキュアプログラミング(1)	2	Webセキュアプログラミングの開発手法について学ぶ。 【V-D-8:3-2】	講義資料の予習	
13	Webセキュアプログラミング(2)	2	Webセキュアプログラミングの開発手法について学ぶ。 【V-D-8:3-2】	講義資料の予習	
14	Webセキュアプログラミング(3)	2	Webセキュアプログラミングの開発手法について学ぶ。 【V-D-8:3-2】	講義資料の予習	
15	Webセキュアプログラミング(4)	2	Webセキュアプログラミングの開発手法について学ぶ。 【V-D-8:3-2】	講義資料の予習	
期末	期末試験	[2]	実施しない		
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
期末	期末試験	[2]			
学習時間合計		30	実時間		22.5
自学自習(予習・復習)内容(学修単位における自学自習時間の保証)					標準的所用時間
①	予習・復習				1時間×15回
②	レポート(講義内容に沿った内容についてレポートを課す。)				2時間×5回
③	課題発表(テーマに沿った課題について調べ、発表資料を作り発表する)				4時間×2回
備考欄					
(JABEE関連共通記述)					
・ この科目はJABEE対応科目である。その他必要事項は各コースで定める。					

(各科目個別記述)

・ この科目の主たる関連科目はメディア情報工学科、情報工学コース科目関連図一覧表を参照のこと。

(モデルコアカリキュラム)

・ 対応するモデルコアカリキュラム(MCC)の学習到達目標、学習内容およびその到達目標を【】内の記号・番号で示す。

(航空技術者プログラム)

・ 【航】は航空技術者プログラムの対応項目であることを意味する。

(学位審査基準の要件による分類・適用)

科目区分 専門科目 A 計算機システムに関する科目

学習時間は、実時間ではなく単位時間で記入する。(45分=1、90分=2)

前期科目は前期部分のみ記述、後期部分は後期のみ記述し、実施期間が見た目すぐわかるようにする。(開講
しない時期は空欄)