

# 科目シラバス (2021年度)

--

## ■科目基本情報

科目名	セキュリティ特論Ⅱ	科目コード	8384
授業時数/週	4 時間/週	年次・学期	3 年 ・ 後期
必修/選択区分	選択必修	授業形態	実習
担当教員	湯瀬達也		
教員の実務経験	実務経験のある教員による授業科目		
職業実践専門課程		連携企業等	
備考			

## ■科目詳細情報

授業概要	セキュリティ特論Ⅰの内容に基づき、引き続き脆弱性についての学習を行いつつ、最新のセキュリティ事情についての知識も習得する。前期同様PHPが中心であるが、重要なセキュリティ発生時などは適宜追加で解説していく											
到達目標	Webアプリケーション開発における脆弱性の注意点を学び、開発時に留意できるようになる。脆弱性の情報は絶えず新しいものが出てくるので、自分で情報を追えるようになる。											
授業方法	実習による操作練習と脆弱性の検出、および関連事項の座学。											
実践的教育の内容	サーバーアプリケーション構築・運用経験から、アプリケーション構築時からのセキュリティへの意識を持つことが重要であり、コード上に存在する問題点を意識できるようにしている。											
成績評価方法	筆記試験 定期試験	0%	筆記試験 小テスト	40%	実技試験	0%	課題評価	60%	平常評価	0%	その他	0%
	実習における作業成果を評価する											
授業外における学修	各自の持つXAMPP環境・仮想環境による自習											
教科書・教材	体系的に学ぶ安全なWebアプリケーションの作り方(第2版) ISBN:9784797393163											
参考文献・資料	特になし											
履修上の留意点	特になし											
授業計画	第1週	構造化データにまつわる問題 実行時評価に伴うインジェクション脆弱性を確認する										
	第2週	共有資源やキャッシュに関する問題 競合状態発生時の脆弱性などについて確認する										
	第3週	Web API実装における脆弱性 JSON形式データのやり取りに関する脆弱性について確認する										
	第4週	Web APIとCSRF API呼び出し時に発生しうるCSRF脆弱性について認識する										
	第5週	認証に関する注意事項 ログイン関連の注意点、暗号化やダイジェスト(ハッシュ)について										
	第6週	文字コードの扱いについて 文字コードの扱いとセキュリティについて										
	第7週	脆弱性診断の実習 OWASP ZAPを用いた「ローカルWebサイトの脆弱性」を診断する										
	第8週	サーバーへの攻撃経路及び対策 最近のサーバーソフトウェアの脆弱性などについて学習する										
	第9週	3年生最終課題(1) チームと開発テーマを決定										
	第10週	3年生最終課題(2) 開発作業と教員レビュー										
	第11週	3年生最終課題(3) 開発作業と教員レビュー										
	第12週	3年生最終課題(4) 開発作業と教員レビュー										
	第13週	3年生最終課題(5) 開発作業と教員レビュー										
	第14週	3年生最終課題(6) 開発作業と教員レビュー										
	第15週	3年生最終課題(7) 開発作業と教員レビュー										
	第16週	3年生最終課題(8) 開発作業と教員レビュー										
	第17週	3年生最終課題(9) 合評会、デジタルワークス、相互評価										