シラバス詳細

タイトル「2023年度　情報学部 [IN-B]」、カテゴリ「【新カリ】情報科学科-【新カリ】情報科学科（選択）」

科目情報

ナンバリング
IN013260070

科目名
Basic SecCap演習

クラス
1クラス

担当教員
西垣　正勝

学年
3年、4年

キャンパス区分
（共通）

開講学期
前期

開講時期
前期前半　～　前期後半

曜日・時限
集中講義

講義室
C＆C

単位区分

単位数
1

講義情報

キーワード

No	キーワード
1	Webサーバ・DBサーバの構築法
2	Webセキュアプログラミング（PHP/MySQL等）
3	標的型メールの調査・分析
4	インシデントレスポンス
5	データサイエンス
6	
7	
8	
9	
10	

授業の目標

多岐にわたるWebシステムへのサイバー攻撃の原因を理解し，インシデントに対する初動対応から再発防止策まで技術面だけでなく情報連絡系統についてもケーススタディを通して体感し，実践で役立たせるための基礎能力を養うことを目標とする．

学修内容

１．全体ガイダンス
２．Webサーバ，DBサーバの構築法
３．Web/DBサーバの脆弱性
４．Web/DBサーバの対策
５．脆弱なサーバに対する攻撃演習
６．脆弱なサーバに対する対策演習１
７．脆弱なサーバに対する対策演習２
８．技術者倫理教育
９．メールの仕組み
１０．メールを悪用した主な攻撃の概要と事例
１１．不審なメールを見分ける，調査する
１２．ケーススタディに基づく初動対応と再発防止策
１３．テストベッド上に設けられた技術的な課題をクリアすることで基本的なインシデント解析技術を習得
１４．グループディスカッションと発表による実習のまとめ
１５．全体のまとめ

授業計画

１．全体ガイダンス
２．Webサーバ，DBサーバの構築法
３．Web/DBサーバの脆弱性
４．Web/DBサーバの対策
５．脆弱なサーバに対する攻撃演習
６．脆弱なサーバに対する対策演習１
７．脆弱なサーバに対する対策演習２
８．技術者倫理教育
９．メールの仕組み
１０．メールを悪用した主な攻撃の概要と事例
１１．不審なメールを見分ける，調査する
１２．ケーススタディに基づく初動対応と再発防止策
１３．テストベッド上に設けられた技術的な課題をクリアすることで基本的なインシデント解析技術を習得
１４．グループディスカッションと発表による実習のまとめ
１５．全体のまとめ

回	内容
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

受講要件

情報科学実験Aの履修を済ませていること（Basic SecCap演習は夏季集中講義です。3年生は前期に情報科学実験Aを受講した後、続けてBasic SecCap演習を受講可能です）

テキスト

適宜PPT、配布資料、WEB教材により講義を進める

参考書

予習・復習について

配布資料、WEB教材に基づいて予習復習を行うこと。関連項目を自ら調査して自学自習を行うこと。

成績評価の方法･基準

各学習項目の達成度により評価する

オフィスアワー

常時（ただし、事前に連絡して下さい）。メールでの連絡も可能です。

担当教員からのメッセージ

アクティブ・ラーニング（●＝対象）

対象	種別	補足説明
	事前学習型授業	
	反転授業	
	調査学習	
	フィールドワーク	
	双方向アンケート	
	グループワーク	
	対話・議論型授業	
	ロールプレイ	
	プレゼンテーション	
	模擬授業	
	ＰＢＬ	
	その他	

実務経験のある教員の有無（●＝対象）

対象	内容	補足説明
●	実務経験教員あり	
	実践的教育から構成	

実務経験のある教員の経歴と授業内容

インシデント対応に関する学習項目は、実務経験のある教員から講述。

教職科目区分

授業実施形態（●＝対象）

対象	形態	補足説明
●	対面授業科目	
	オンライン授業科目	

オンライン授業（詳細）

対面授業を基本と考えていますが、コロナ禍等の状況によってはオンラインリアルタイム配信を併用する予定です。