科目名	サイバーセキュリティ演習							年度	2026
英語科目名	Cyber Security Exercises							学期	前期
学科・学年	ＩＴスペシャリスト科 セキュリティ専攻　3年次	必／選	必	時間数	30	単位数	2	種別※	講義
担当教員	吉川	教員の実務経験		無	実務経験の職種				

【科目の目的】

サーバーセキュリティの基礎知識と実践的なスキルを習得することを目指し、セキュリティリスクへの理解と防御対策の実装力を養う。

【科目の概要】

本科目は、サーバーの脆弱性、侵入テスト、脅威の検出と対応を中心に学ぶ演習型授業です。実際のサーバー構築とセキュリティ対策を通して、セキュリティ強化の技術を実践的に理解します。

【到達目標】

A. サーバーセキュリティの基礎知識を習得する
B. 脆弱性診断ツールを使いこなす
C. セキュリティリスクの評価と管理ができる
D. 侵入テストを実施できる
E. 実践的なセキュリティ対策を実行できる

【授業の注意点】

授業中の私語や受講態度には厳しく対応する
理由のない遅刻・欠席は認めない
授業時数の4分の３以上出席しない者は定期試験を受験することができない

評価基準＝ルーブリック

ルーブリック 評価	レベル５ 優れている	レベル４ よい	レベル３ ふつう	レベル2 あと少し	レベル１ 要努力
到達目標 A	セキュリティの概念とリスクを深く理解し、具体的な対策を立案・実行できる	セキュリティの基本概念を理解し、一般的な防御策を提案できる	セキュリティ概念を理解しているが、対策の実行に難しさがある	基本的なセキュリティ概念に理解があるが、対策の実行が不十分	セキュリティの概念が理解できておらず、対策を実施できない
到達目標 B	脆弱性診断ツールを駆使して診断を行い、結果に基づいた適切な改善策を提案できる	ツールを使って診断し、改善策を提案できるが、結果分析に改善の余地がある	ツールを使用して診断を行えるが、診断結果の解釈や改善策の提案に不安がある	ツールを使用するが、診断結果の活用方法に困難がある	ツールを使用できず、診断作業が進まない
到達目標 C	サーバーのセキュリティリスクを正確に評価し、適切な管理方法を立案・実行できる	リスクを評価し、管理方法を提案できるが、実行において改善点がある	リスク評価は行えるが、管理方法を実行する際に問題がある	リスク評価は部分的にできるが、管理策を提案することが難しい	セキュリティリスクの評価ができず、管理方法を実行できない
到達目標 D	実際のサーバー環境で侵入テストを実施し、脆弱性を発見して適切な対策を実行できる	侵入テストを実施し、脆弱性を見つけられるが、対策に改善が必要	侵入テストを行えるが、脆弱性の発見やその対策に困難がある	侵入テストを実施するが、脆弱性の発見が不十分である	侵入テストを実施できず、脆弱性を発見できない
到達目標 E	脆弱性を発見した後、効果的な防御策を実行し、サーバーのセキュリティを向上させる	発見された脆弱性に対して防御策を提案・実行できるが、実行に一部難しさがある	防御策を提案できるが、実行に時間がかかる、または効果的でない	防御策の提案が不十分で、実行に課題がある	適切な防御策を実行できない

【教科書】

ステップアップ脆弱性診断　ツールを比較しながら初級者から中級者に！

【参考資料】

【成績の評価方法・評価基準】

課題と試験の結果を総合的に判断する。

※種別は講義、実習、演習のいずれかを記入。

科目名	サイバーセキュリティ演習	年度	2026
英語表記	Cyber Security Exercises	学期	前期

回数	授業テーマ	各授業の目的		授業内容	到達目標＝修得するスキル	評価方法	自己評価
1	サーバーセキュリティの概要と重要性	セキュリティの基本概念、脆弱性の種類と影響	1	セキュリティの基本概念と重要性の理解	サーバーセキュリティの基本概念を理解し、なぜ重要か説明できる。	2	
			2	セキュリティリスクと脆弱性の分類	セキュリティリスクと脆弱性の分類を理解し、事例を挙げられる。		
			3	サーバー攻撃の一般的な手法	一般的なサーバー攻撃の手法を理解し、概要を説明できる。		
2	脆弱性診断のフロー	脆弱性診断の流れと計画の立て方	1	脆弱性診断の全体的な流れと目的	脆弱性診断の各ステップを理解し、目的を説明できる。	2	
			2	診断プロセスの重要性	診断プロセスの意義を理解し、具体的な流れを把握する。		
			3	セキュリティポリシーの概念	セキュリティポリシーの重要性を説明し、診断フローとの関連を理解する。		
3	診断対象の確認	サーバーやアプリケーションの特性と診断対象の理解	1	サーバーやアプリケーションの特性理解	診断対象のシステム構成を理解し、特徴を説明できる。	2	
			2	診断対象の把握方法	診断対象の確認手法を学び、適切に把握できる。		
			3	診断に適した情報収集の手法	情報収集の手法を理解し、診断の準備に活かせる。		
4	リスク分析と診断対象の選定	診断の優先順位を決める手法	1	リスク分析の基礎	リスク分析の基本手法を理解し、適用できる。	2	
			2	診断対象の優先順位の決定	診断対象の選定基準を理解し、優先順位を決定できる。		
			3	リスク評価の実践的な方法	リスク評価の手法を学び、実践的に評価できる。		
5	診断準備とツールの基礎1	OWASP ZAPのインストールと初期設定	1	OWASP ZAPのインストールと初期設定	OWASP ZAPを正しくインストールし、設定を行える。	2	
			2	基本的な操作方法の習得	OWASP ZAPの基本操作を理解し、実行できる。		
			3	ツールの主な機能の理解	OWASP ZAPの主要機能を説明し、活用方法を理解する。		
6	診断準備とツールの基礎2	Burp Suiteのインストールと初期設定	1	Burp Suiteのインストールと初期設定	Burp Suiteを正しくインストールし、設定を行える。	2	
			2	基本的な操作方法の習得	Burp Suiteの基本操作を理解し、実行できる。		
			3	ツールの主な機能の理解	Burp Suiteの主要機能を説明し、活用方法を理解する。		
7	診断の実施（OWASP ZAP）	OWASP ZAPを使用した基礎的な脆弱性スキャン	1	OWASP ZAPを使用した脆弱性スキャンの実施	OWASP ZAPを使って基本的なスキャンを実施できる。	2	
			2	診断結果の確認と分析	スキャン結果を理解し、分析方法を説明できる。		
			3	基本的なセキュリティリスクの検出	OWASP ZAPで一般的なリスクを検出し、対策を検討できる。		
8	診断の実施（Burp Suite）	Burp Suiteを使用した基礎的な脆弱性スキャン	1	Burp Suiteを使用した脆弱性スキャンの実施	Burp Suiteを使って基本的なスキャンを実施できる。	2	
			2	診断結果の確認と分析	スキャン結果を理解し、分析方法を説明できる。		
			3	特定の脆弱性リスクの検出と対策	Burp Suiteで特定のリスクを検出し、対応策を考えられる。		
9	自動診断の使い方	OWASP ZAPとBurp Suiteの自動診断機能と設定方法	1	自動診断機能の設定と実行	自動診断を設定し、実行できる。	2	
			2	自動診断のメリットとデメリット	自動診断の利点と欠点を理解し、活用方法を考えられる。		
			3	自動診断結果の解釈	自動診断の結果を正しく解釈し、報告に活かせる。		
10	診断結果の分析と考察	診断結果の解釈、リスク評価、対応の検討	1	診断結果の評価方法	診断結果を評価し、優先順位を設定できる。	2	
			2	リスク評価と改善策の考察	リスク評価を行い、改善策を提案できる。		
			3	分析結果の文書化	分析結果を報告書としてまとめられる。		
11	診断結果報告の作成	診断結果のレポート作成方法と報告の仕方	1	診断報告書の基本構成	診断報告書の基本的な構成を理解し、作成できる。	2	
			2	結果の視覚的な表現方法	図や表を用いて診断結果をわかりやすく報告できる。		
			3	クライアント向けの解説技術	クライアントに分かりやすい形で診断結果を説明できる。		
12	OWASP ZAPとBurp Suiteの比較	両ツールの機能や操作性の違いを分析	1	両ツールの機能と操作性の違い	OWASP ZAPとBurp Suiteの特性を比較し、特徴を説明できる。	2	
			2	使用シーンに応じたツール選択	使用場面に応じて適切なツールを選択できる。		
			3	組み合わせた診断手法の検討	両ツールを組み合わせた診断手法を考えられる。		
13							
14							
15							

評価方法：1.小テスト、2.パフォーマンス評価、3.その他

自己評価：S：とてもよくできた、A：よくできた、B：できた、C：少しできなかった、D：まったくできなかった

備考 等