科目名	セキュリティプログラミング							年度	2026
英語科目名	Security Programming							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	60	単位数	2	種別※	実習
担当教員	大村	教員の実務経験		有	実務経験の職種		プログラマー		

【科目の目的】

ネットワークとセキュリティの基本概念を理解し、Pythonによる実践的なプログラミングを通して、問題解決に適用できる能力を養う。

【科目の概要】

ネットワークとセキュリティ分野の基礎理論と実践的なプログラミングスキルの習得を目指します。具体的には、TCP/IP通信、ファイル操作、データ解析、エラーハンドリング、セキュリティ対策といったテーマをPythonプログラミングを通して学習し、ハンズオン演習で理解を深めます。また、実践的なネットワーク通信やセキュリティログの解析、エラーハンドリングなど、セキュリティリスクを考慮したシステム構築の基礎を学び、セキュリティに対する意識と実装スキルを養成します。

【到達目標】

A. ネットワークとセキュリティの理解
B. ファイル操作とデータ処理のセキュリティ
C. ログ収集とネットワーク通信の解析
D. 暗号化とデータ保護の技術
E. 総合問題解決能力

【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	ネットワークとセキュリティの基本概念および技術を深く理解し、応用力を持って活用できる	基本概念を十分に理解し、技術を活用できる	基本概念を理解し、指導のもとで技術を活用できる	基本概念の理解に一部欠け、指導がないと技術の活用が難しい	基本概念が理解できておらず、技術の応用ができない
到達目標 B	ファイル操作とデータ解析のセキュリティリスクを把握し、自律的に安全な処理を設計・実装できる	セキュリティリスクを理解し、適切にファイル操作を実施できる	リスクを理解し、指導のもとで安全なファイル操作ができる	リスク理解が一部不足し、指導を受けることで安全な操作が可能	リスクを理解せず、ファイル操作が不安定である
到達目標 C	ログ収集や通信解析を自律的かつ適切に行い、異常検出や問題対応を行うことができる	ログ収集や通信解析を行い、異常検出や対応を適切に行うことができる	ログ収集と解析を行い、指導のもとで異常検出と対応ができる	ログ収集と解析が不安定で、指導を受けることで異常検出と対応が可能	ログ収集と解析ができず、異常検出や対応が困難である
到達目標 D	暗号化やデータ保護技術を理解し、安全なプログラムを自律的に設計・実装できる	基本技術を理解し、安全なデータ保護を意識した実装ができる	基本技術を理解し、指導のもとでデータ保護を実装できる	基本技術の理解が不足し、指導を受けることでデータ保護が行える	暗号化技術の理解が不十分で、安全なプログラムを実装できない
到達目標 E	学んだ知識と技術を統合し、実務に応用できるプログラムを自律的に設計・実装できる	学んだ知識と技術を活用し、応用的なプログラムを指導のもとで作成できる	学んだ知識を活用し、基礎的な問題解決ができる	基礎的な問題解決に課題があるが、指導を受けることで解決できる	基礎的な問題解決ができず、応用的なプログラム作成が困難である

【教科書】

適宜資料を配布する。

【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	セキュリティプログラミング	年度	2026
英語表記	Security Programming	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	セキュリティとPythonプログラミングの導入	セキュリティの基本とPython基礎を理解する	1	セキュリティ概念	セキュリティ概念の理解	2	
			2	Python基礎	データ型・制御構文の知識		
			3	スクリプト作成	簡単なスクリプトの実装		
2	Pythonでのファイル操作とデータ取り扱い	ファイル操作とセキュリティデータ処理を学ぶ	1	ファイル操作	ファイルの読み書き操作ができる	2	
			2	ログ解析	セキュリティログを解析できる		
			3	ログ自動化	自動解析ツールの作成ができる		
3	Pythonでのエラー処理とセキュリティ	安全なエラーハンドリングを実装する	1	エラー処理	エラー処理の設計スキル	2	
			2	情報漏洩対策	情報漏洩防止の知識		
			3	ロギングシステム	安全なロギングの実装		
4	ネットワーキングの基礎	ネットワーク通信の基本とPython実装を学ぶ	1	TCP/IP概要	TCP/IPの基礎を理解	2	
			2	ソケットモジュール	Pythonで通信ができる		
			3	クライアント通信	クライアント通信の実装		
5	Pythonによるネットワークスキャン	ネットワークスキャンの基礎と実装を習得する	1	スキャン概念	ネットワークスキャンを理解	2	
			2	ポートスキャン	ポートスキャナを作成できる		
			3	Nmap連携	Nmapとの統合操作		
6	パケット解析	パケット解析の技術を学び通信内容を監視する	1	キャプチャ基礎	パケットキャプチャの実施	2	
			2	Scapy操作	Scapyによるパケット解析		
			3	トラフィック解析	ネットワーク解析の基礎知識		
7	Webセキュリティ入門	Web脆弱性を理解し攻撃をシミュレートする	1	脆弱性概念	Web脆弱性の理解	2	
			2	SQL/XSS攻撃	攻撃の種類と影響を理解		
			3	脆弱性スキャン	脆弱性スキャナの実装		
8	暗号化の基礎	暗号化の基本とPythonでの実装を学ぶ	1	暗号化概要	暗号化・復号の基礎知識	2	
			2	対称/非対称暗号	各暗号の違いを理解		
			3	暗号化スクリプト	データ暗号化の実装ができる		
9	ハッシュ化とデータ整合性	ハッシュ化でデータ保護と整合性を学ぶ	1	ハッシュ関数	ハッシュの役割を理解	2	
			2	MD5/SHA	ハッシュアルゴリズムを理解		
			3	整合性チェック	ハッシュによる整合性確認		
10	認証と認可	認証と認可の基礎を理解し実装に応用する	1	認証/認可の違い	認証と認可の違いを理解	2	
			2	トークン認証	トークン認証の仕組みを理解		
			3	認証システム	認証システムの設計と実装		
11	フォレンジックとデジタル証拠収集	デジタル証拠収集の基礎を学びツールを作成する	1	フォレンジック概要	デジタル証拠の収集基礎を理解	2	
			2	メタデータ抽出	メタデータの取得方法を理解		
			3	フォレンジックツール	証拠収集ツールの実装ができる		
12	Pythonでのマルウェア分析	マルウェアの解析手法を学び分析ツールを作成する	1	マルウェア動作	マルウェアの動作を理解	2	
			2	静的/動的解析	静的・動的解析手法を理解		
			3	マルウェア検出	検出ツールの開発ができる		
13	ペネトレーションテストツールの作成	ペネトレーションテストの基礎とツール開発を学ぶ	1	テスト手順	テストの基本手順を理解	2	
			2	攻撃シミュレーション	攻撃シミュレーションができる		
			3	自動化ツール	自動化ペネテストツールを作成		
14	Pythonでのセキュリティ自動化	セキュリティ自動化技術を学びツールを作成する	1	タスク自動化	セキュリティ自動化の基礎知識	2	
			2	脆弱性スキャン	脆弱性検出の自動化実装		
			3	検知ツール作成	脆弱性検知ツールを構築		
15	実践プロジェクト	セキュリティツールの総合プロジェクトを実施する	1	プロジェクト設計	プロジェクト計画と設計ができる	2	
			2	ツール開発	開発・改善の基礎が身に付く		
			3	プレゼンテーション	発表とフィードバックができる		

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