

学科名	ネットワークセキュリティ科
コース名	セキュリティ専攻
授業科目	セキュリティ応用
必選	必
年次	2年次
実施時期	後期
種別	実習
時間数	60
単位数	2
担当教員	勝島 貴之
実務経験	有
実務経験職種	システムエンジニア
授業概要	インターネットには様々な脅威があり、インターネットに接続するすべてのパソコン、スマートフォン、ネットワーク機器、IoT機器などのシステムが持つ脆弱性を攻撃してくる可能性がある。この授業ではその中でも特に攻撃対象として狙われる可能性の高いWebサービスを中心に上げ、Webサービスに対する各種攻撃手法などを理解し、適切な対策ができるようになることを目的とする。また、日々の運用・管理の中で異常な状態の発生を素早く検出することができるようになることを目的として、ログの管理方法や分析方法を学ぶ。
到達目標	インターネットで行われている各種攻撃手法（SQLインジェクション、コマンドインジェクション、クロスサイトスクリプティングなど）とその防御技術の具体的な仕組みを理解し、実際に適切な防御ができるようになる。また、脆弱性診断の流れを理解し、診断ツールを適切に使用し、不備の無い報告書が作成できるようになる。さらに、システムの運用管理で重要な役割を担うログの適切な管理と分析を行い、システムの安全性を管理できるようになる。
授業方法	さまざまな脆弱性とその事例を紹介し、適切な診断方法や対応の仕方を学習する。また、脆弱性診断の流れ、診断ツールの使い方、報告書の作り方なども学習する。さらに、セキュリティ運用で重要なログの分析・管理手法、ログ分析ツールの活用方法、攻撃などの痕跡を見つける手段などを学習する。
成績評価方法	試験・課題 80% 試験と課題を総合的に評価する 小テスト 10% 授業内容の理解度を確認するために実施する 平常点 10% 積極的な授業参加度、授業態度によって評価する
履修上の注意	本講義では最新のサービスを利活用する態度を重要視する。また、社会への移行を前提とした受講マナーで参加することを期待するため、講義中の私語や受講態度などには厳しく対応する。理由のない遅刻や欠席は認めない。授業時数の4分の3以上出席しない者は定期試験を受講することができない。
教科書・教材	「脆弱性診断スタートガイド」「セキュリティのためのログ分析入門」 配布資料

授業計画	
第1回	授業ガイダンス セキュリティ応用の授業で学ぶ内容の全体像を把握する
第2回	脆弱性(1) 脆弱性診断（必要な知識 T C P / I P、H T T P）ができるようになる
第3回	脆弱性(2) さまざまな脆弱性（S Q L インジェクション、コマンドインジェクション、他）を理解する
第4回	脆弱性(3) さまざまな脆弱性（クロスサイトスクリプティング、H T T P ヘッダーインジェクション、他）を理解する
第5回	脆弱性(4) さまざまな脆弱性（認証の脆弱性、許可制御やセッション管理の不備、他）を理解する
第6回	脆弱性(5) さまざまな脆弱性（情報漏洩、オープンリダイレクト、他）を理解する
第7回	脆弱性(6) 脆弱性診断の流れ、診断ツールの使い方、報告書の作り方を理解する
第8回	ログ分析(1) ログ分析とセキュリティを理解する
第9回	ログ分析(2) サーバー攻撃とセキュリティログ分析を理解する
第10回	ログ分析(3) ログ分析ツール（W i n d o w s、L i n u x）が使えるようになる
第11回	ログ分析(4) W e b サーバログの分析ができるようになる
第12回	ログ分析(5) プロキシログの分析ができるようになる
第13回	ログ分析(6) I P S ログ（概要、攻撃の痕跡、分析）が調べられるようになる
第14回	ログ分析(7) ファイアウォールログの分析ができるようになる
第15回	ログ分析(8) アクセスログに現れない攻撃の痕跡を調べられるようになる