日本工学院八王子専門学校	開講年度	2019年度（平成31年度）	科目名	セキュリティ応用

科目基礎情報

開設学科	パソコン・ネットワーク科	コース名	ネットワーク・セキュリティコース	開設期	後期
対象年次	2年次	科目区分	選択	時間数	60時間
単位数	4単位	授業形態	講義		
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				

担当教員情報

担当教員	村上	実務経験の有無・職種	有・ネットワークエンジニア

学習目的

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サービスを中心に取り上げ、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、ＨＴＴＰヘッダーインジェクション、認証の脆弱性、許可制御やセッション管理の不備、情報漏洩、オープンリダイレクトなど）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。

教育方法等

授業概要	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。
注意点	授業中の私語や受講態度などには厳しく対応する。また遅刻や欠席は認めない。授業に出席するだけでなく、社会への移行を前提とした受講マナーで授業に参加することを求める。1年次後期科目「情報セキュリティ」や2年次科目の「Webセキュリティ実習」の授業と関連性をもって学習すること。試験は定期試験を実施する。ただし、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。

評価方法	種別	割合	備考
	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
	レポート	0%	
	成果発表（口頭・実技）	0%	
	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

授業計画（１回～１５回）

回	授業内容	各回の到達目標
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。
２回	脆弱性(1)	脆弱性診断（必要な知識 ＴＣＰ／ＩＰ、ＨＴＴＰ）ができるようになる。
３回	脆弱性(2)	さまざまな脆弱性（ＳＱＬ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。
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、ＨＴＴＰヘッダーインジェクション、他）を理解する。
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。
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。
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。
８回	ログ分析(1)	ログ分析とセキュリティを理解する。
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。
１０回	ログ分析(3)	ログ分析ツール（Ｗｉｎｄｏｗｓ、Ｌｉｎｕｘ）が使えるようになる。
１１回	ログ分析(4)	Ｗｅｂサーバログの分析ができるようになる。
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。
１３回	ログ分析(6)	ＩＰＳログ（概要、攻撃の痕跡、分析）が調べられるようになる。
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。
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。