暗号と情報セキュリティ論

専門　　選択　　2単位

盛　拓生

1. 授業の概要（ねらい）

　情報セキュリティは、理論から実際のネットワークあるいは情報システムまで含めた多岐に渡る分野を含みますが、この講義では主に、実際の情報システムに起こりうるセキュリティの問題について、実践的に対処するための方法を基礎から体系的に理解することを目標とします。

　この科目は、理工学研究科(通信教育課程)情報科学専攻の学位授与の方針(ディプロマポリシー)1、4に対応します。

2. 授業の到達目標

　この科目では次のような能力を修得することを目標とします。
学生は,不正アクセスに関して、基本的な原理を説明でき、基本的な対策を示すことができる。
学生は、Webアプリケーションへの基本的な攻撃の原理を説明でき、基本的な対策を示すことができる。
学生は、マルウェアに関して、基本的な動作原理を説明でき、基本的な対策を示すことができる.
学生は、不正侵入検知/防止システムについて、基本的な原理を説明できる。
学生は、基本的なアクセス制御技術を示すことができ、状況に応じて適切な技術を選択できる。
学生は、基本的な情報セキュリティプロトコルについて説明できる。
学生は、情報セキュリティシステムの構築/運用に際して注意すべき点を説明できる.
学生は、基本的なセキュリティマネジメントの概要を説明できる。

3. 成績評価の方法および基準

レポート課題の合格を前提として、試験(100%)。
講義内容、レポート、試験への質問,フィードバック等は原則的にLMS、電子メールで対応します。

4. 教科書・参考文献

教科書
佐々木良一監修、電子情報通信学会編　現代電子情報通信選書「知識の森」 ネットワークセキュリティ

　オーム社、ISBN-13: 978-4274215179
参考文献
徳丸 浩著　体系的に学ぶ 安全なWebアプリケーションの作り方 脆弱性が生まれる原理と対策の実践
　SBクリエイティブ、ISBN-13: 978-4797361193
Justin　Seitz著,青木,新井,一瀬,岩村,川古谷,星澤訳　サイバーセキュリティプログラミング,Pythonで学ぶハッカーの思考　オライリー・ジャパン、
ISBN-13: 978-4873117317

5. 準備学修の内容

　予め、各回の講義資料をLMS上で公開します。講義資料はPC、タブレット、スマートフォン等にダウンロードするか紙に印刷するなどして、参照、書き込みできるようにしてください。

　これらの資料に1時間30分程度目を通した上で、理解できた点、理解できていない点をそれぞれ把握してください。

　1時間30分程度かけてLMS上のテストで理解度を確認し、復習してください。

6. その他履修上の注意事項

　レポート作成に関して、参考文献等を引用する場合は出典を明示し日本の著作権法に違反しない目的形式で引用してください。

　事前に必要となる知識は、学部程度の論理数学、代数、数論、計算量理論、ネットワーク技術、プログラミング言語論、データベース論、情報セキュリティに関する知識です。

　同時に履修すべき科目は、量子情報科学です。

7. 授業内容

【第1回】　ネットワークセキュリティの動向
【第2回】　不正侵入手法 -パスワードクラック-
【第3回】　不正侵入手法 -Webアプリケーションセキュリティの基礎-
【第4回】　不正侵入手法 -インジェクション、XSS-
【第5回】　不正侵入手法 -CSRF、バッファオーバフロー、ドライブ・バイ・ダウンロード-
【第6回】　マルウェア
【第7回】　侵入検知システム
【第8回】　アクセス制御
【第9回】　アクセス制御 -認証,FireWall-
【第10回】　セキュリティプロトコル
【第11回】　セキュリティシステムの構築と運用
【第12回】　情報セキュリティマネジメント
【第13回】　ネットワークセキュリティの新たな動向 -標的型攻撃/IPv6-
【第14回】　ネットワークセキュリティの新たな動向 -スマートフォンのセキュリティ-
【第15回】　サイバーセキュリティプログラミング