情報セキュリティ

科目ナンバー　3C327
専門　　選択　　2単位

盛　拓生

1. 授業の概要（ねらい）

現代社会において、情報セキュリティ技術は情報社会を支える基盤技術として必須のものとなってきており、その重要性は高まっています。

情報セキュリティといった場合に、その範囲は理論から応用まで幅広い分野を網羅しています。数論、代数系、計算機科学を基礎とする暗号理論、さらに暗号理論が現在の計算機システム及びネットワークと結びつくことで多様なサービスを提供することが可能となっています。

本講義では後者のネットワークを中心とするネットワークセキュリティを主なトピックとします。しかし、ネットワークセキュリティを構成する諸技術を理解するには、少なくとも、その理論的な基盤となる数学、計算機科学、暗号理論の基礎的な概念を理解することが必要となります。

そのため本講義では、まずはじめにこれらの基礎理論の概要を学んだ後に、ネットワーク社会の安全を保障するために利用されている、あるいは今後利用されるであろう技術、概念およびそこでの問題点等について学びます。

この科目では、学位授与の方針(ディプロマポリシー)DP4Cに関連する能力を修得します。

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、公開鍵暗号系を構成している初等整数論、抽象代数系の基礎について説明でき、そこで用いられる数式の意味を説明できる。
学生は、共通鍵暗号、公開鍵暗号の基本的な性質、暗号の利用モード、Hash関数についてを説明し、基本的な暗号化/復号の処理を行うことができる。
学生は、情報セキュリティ、暗号プロトコル、ネットワークプロトコルの目的、意味、概要を説明し、基本的なプロトコルの処理を説明または実行できる。
学生は、不正アクセスの原因の1つとなるマルウェアの分類ができ、不正アクセスへの対策について説明することができる。
学生は、個人認証、バイオメトリクスについて、その概要を説明し、目的、問題点について説明することができる。
学生は、現在までのセキュリティ評価、標準化の概要を説明できる。

3. 成績評価の方法および基準

中間レポート(50%)、期末試験の成績(50%)。
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またはオフィスアワーで対応します。

4. 教科書・参考文献

教科書
宮地充子,菊池浩明編著　IT Text 情報セキュリティ　オーム社、ISBN-13: 978-4274132841
参考文献
芹沢 正三著　素数入門―計算しながら理解できる　講談社、ISBN-13: 978-4062573863

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、講義中いつでも参照、書き込みできるようにしてください。
授業前にこれらの資料に1時間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授業に臨んでください。
授業後には、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

中間レポートが提出されない場合は単位の取得が著しく困難になります。中間レポートは締切を守って必ず提出するようにしてください。
自主学習支援のためにLMSを利用します。講義資料等はLMS上で公開されているので事前に入手し、講義中はノートをとることよりも、
講義を聞いて理解すること、演習問題を解くことに集中してください。
事前に履修すべき科目は、論理数学、線形代数、離散数学、コンピュータネットワーク、プログラミング言語論、グラフ理論、オートマトンと計算理論、情報システム開発技法、ウェブ技術、デジタル信号処理、画像情報処理です。
同時に履修すべき科目は、情報科学実習1、情報理論、情報システムデザイン、システム開発演習、ネットワーク演習です。
事後に履修すべき科目は、情報科学実習2、オペレーティングシステム、ソフトウェア工学、情報社会論、ウェブアプリケーションです。
この科目はJABEEプログラムの必修科目で、学習・教育到達目標中項目1-3及び5-1に対応しています。

7. 授業内容

【第1回】　情報セキュリティ
【第2回】　共通鍵暗号
【第3回】　公開鍵暗号・ディジタル署名の基礎理論1 -代数系,剰余類-
【第4回】　公開鍵暗号・ディジタル署名の基礎理論2 -数論的アルゴリズム-
【第5回】　公開鍵暗号とディジタル署名1 -離散対数問題に基づく公開鍵暗号,ディジタル署名の概要,Hash関数-
【第6回】　ディジタル署名2 -付録型署名,メッセージ回復型署名-
【第7回】　暗号プロトコル
【第8回】　ゼロ知識証明と社会システムへの応用
【第9回】　ゼロ知識証明/ネットワークセキュリティ
【第10回】　インターネットセキュリティ

【第11回】　不正アクセス
【第12回】　情報ハイディング/匿名通信路
【第13回】　バイオメトリクス
【第14回】　セキュリティ評価
【第15回】　テスト、まとめ