科　　目　　名
情報セキュリティ **Information Security**

3年　後期　2単位　選択

吉　岡　大三郎

概　　要

Eコマースや電子マネー、電子政府など、高度 IT 化社会の実社会での運用においては安全性、信頼性を確保するためのセキュリティ技術が不可欠であり、情報セキュリティ技術の知識を有する人材のニーズは今後益々高まるものと思われる。本講義では、IT 社会のセキュリティを支える基盤技術となる暗号理論を中心に情報セキュリティ技術の解説を行い、その暗号技術が IT 社会においてどのように活用されているのか学習する。

目　　標

① IT 社会における情報セキュリティ技術の役割を理解する。
② 初等整数論を身につけ、暗号技術の基礎的理解力を養う。
③ 情報セキュリティ関連法案と情報倫理について理解する。

授業計画

	テーマ	内　　容
1	導入および本講義の位置づけ、目標	本講義の授業内容と目標、評価のしくみについて説明する。 インターネット上に潜むさまざまな脅威について紹介し、情報セキュリティ技術の重要性を認識する。
2	情報セキュリティの基礎	情報セキュリティの3要素、情報資産とその脅威およびリスクについて解説する。
3	情報セキュリティの脅威	情報資産を脅かすさまざまな技術的脅威について解説する。
4	暗号の基礎	暗号の基礎事項、秘密鍵暗号と公開鍵暗号について解説する。
5	ストリーム暗号	1ビット単位で暗号化を行うバーナム暗号とストリーム暗号について解説する。
6	DES（Data Encryption Standard）とAES（Advanced Encryption Standard）	米国連邦政府情報処理標準において推奨される代表的なブロック暗号である DES と AES 暗号について解説する。
7	剰余演算と一方向関数	暗号技術の数学的基礎となる剰余演算と一方向関数の性質について解説する。
8	ディフィー・ヘルマン鍵交換方式	2者間による鍵共有方法であるディフィー・ヘルマン鍵交換方式について解説する。
9	ナップサック暗号	ナップサック問題とその応用であるナップサック暗号について解説する。
10	RSA 暗号	RSA 暗号について解説する。
11	デジタル署名	公開鍵暗号に基づくデジタル署名のしくみについて解説する。
12	公開鍵基盤	鍵管理手法である公開鍵基盤について解説する。
13	情報セキュリティ関連法案と情報倫理	情報セキュリティ関連法案と情報倫理について解説する。
14	暗号技術の未来	量子コンピュータ、量子暗号について解説する。
15	定期試験	定期試験により本講義の習熟度を評価する。

授業方法

プリントを配布し、プロジェクタを用いた授業を行う。
適宜、復習として演習問題を課す。

評価方法

定期試験（80点満点）と講義中に行われる演習問題（20点満点）の合計点で評価し、60点以上を合格とする。

教　　材

プリント
参考書：「情報セキュリティプロフェッショナル総合教科書」佐々木良一 著　秀和システム
「情報セキュリティ」宮地充子 著　オーム社
「暗号技術大全」ブルースシュナイアー 著　山形浩生 監修
Softbank Creative 社