

開講学科	生命情報学科	前橋工科大学 シラバス			
科目名	情報セキュリティ	標準対象年次	選択/必修	科目コード	
		3年次	選択	15100301	
担当教員	優 乙石	単位数	学期	曜日	時限
		2単位	前期	木曜日	3時限
授業の教育目的・目標	情報ネットワークを安心して利用できる前提となる情報セキュリティの確保について、その具体的な内容、セキュリティに必要な機能、用いられる技術の概要を把握する。				
学科の学習・教育目標との関係	増え続けるゲノム情報や生体認証情報など、生命情報の管理や送受信において、情報の暗号化やセキュリティの確保は最も重要な項目である。				
キーワード	情報ネットワーク、インターネット、情報システム、不正アクセス、電子認証、電子署名、コンピュータウイルス、暗号、機密保持、ブロックチェーン、生命情報				
授業の概要	現代はカード情報や医療情報などの個人情報から、企業・国家レベルの機密情報までが高度に電子化され、そのデータ量も増加の一途をたどっている。このような機密情報を安全に送受信・保管するために開発された近代暗号や、電子認証・署名の基礎について学び、高度情報化社会に生きるための基礎知識を獲得する。				
授業の計画	第1回： 情報セキュリティの概要 第2回： 共通鍵暗号(1) 第3回： 共通鍵暗号(2) 第4回： 公開鍵暗号(RSA暗号) 第5回： 公開鍵暗号(楕円曲線暗号) 第6回： ハッシュ関数 第7回： 電子署名、電子認証 第8回： ウェブのセキュリティ 第9回： 情報セキュリティの要素技術のまとめ 第10回： 電子メールのセキュリティ 第11回： 無線通信のセキュリティ 第12回： 不正アクセス・ハッキング 第13回： 仮想プライベートネットワーク 第14回： 新しい技術 1 ブロックチェーン 第15回： 新しい技術 2 生命情報とセキュリティ				
受講条件・関連科目	情報ネットワークを受講していること。				
授業方法	講義形式。パワーポイントと配布プリントを使用。				
テキスト・参考書	情報セキュリティ、宮地充子・菊池浩明、オーム社(参考書)				
成績評価	・試験(60%) ・宿題レポート(40%)				
履修上の注意	漫然と講義に出席するのではなく、自分で自分の情報を守る術を身につけるという積極的な態度で臨むこと。試験の他に、暗号技術に関する簡単なプログラムを自作して提出してもらいます。				