

授業科目名 <英訳>	人文研ゼミ 暗号解読と言語解読の歴史 History of deciphering and decoding			担当者氏名	人文科学研究所 准教授 伊藤 順二				
群	拡大群	系列	人社系	単位数	2単位	週コマ数	1コマ	授業形態	ゼミナール
開講期	前期	受講定員	12人	配当学年	1回生	対象学生	全学向		
曜時限	火5			教室	総合研究4号館/人文科学研究所 318室 伊藤研究室(本部構内)				
キーワード	西洋史 / 暗号 / 言語 / 情報								
【授業の概要・目的】									
<p>情報の迅速かつ安全な伝達は、「情報社会」ということばが使われるよりはるか以前から、人間の社会と文化にとって重要な課題でした。言語の研究は西欧では植民地の拡大、世界観の革新と並行してすすみ、認識論の変化をも促しました。</p> <p>現在の情報の多くはデジタルな領域で流通されていますが、少なくとも暗号に関する限り、数学的操作を情報伝達に利用する発想は古くからありました。暗号技術は19世紀以降に急速な発展を遂げますが、これも通信技術の発展や政治的経済的な世界の一体化と並行して起こっています。</p> <p>このゼミでは、暗号解読にまつわる基本的テキストを読み、コミュニケーションと認識とコトバの基本的問題点を歴史的に学んでいく予定です。</p>									
【授業計画と内容】									
<p>教科書を輪読します。後半は教科書を踏まえつつ、自由な報告をしていただく予定です。 (授業計画は、受講人数や受講生の希望によって適宜変更します。以下は教科書の目次を大まかに並べたものです)</p> <ol style="list-style-type: none"> <li>1. イントロダクション + 簡単な暗号を解いてみる</li> <li>2. 換字式暗号と頻度分析</li> <li>3. ヴィジュネル式暗号とその解読法</li> <li>4. エニグマ</li> <li>5. ナヴァホ語暗号・線文字B解読</li> <li>6. 公開鍵暗号</li> <li>7. RSA</li> <li>8. 量子暗号</li> <li>9以降. 自由報告</li> </ol>									
【履修制限の方法】									
受講定員を超える受講申込があった場合は無作為に抽選を行います。									
【履修要件】									
特になし									
【成績評価の方法・基準】									
一人2回の報告(40×2),および出席点(20) ただし「出席点」は単なる出席ではなく授業中の議論への参加度を考慮します。									
【教科書】									
サイモン・シン 『暗号解読(上・下)』(新潮社(新潮文庫)) ISBN:978-4-10-215972-9, -215973-6									
【その他(授業外学習の指示等)】									