| | | | |
|---|---|---|---|
| 学期／Semester | 2022年度／Academic Year　1クォーター／First Quarter | 曜日・校時／Day・Period | 木／Thu 2 |
| 開講期間／Course duration | 2022/04/01～2022/06/12 | | |
| 必修選択／Required / Elective | 必修／required | 単位数(一般/編入/留学)／Credits (General /Transfer/Overseas) | 1.0//1.0 |
| 時間割コード／Time schedule code | 20223802010001 | 科目番号／Course code | 38020100 |
| 科目ナンバリングコード／Numbering code | ID-ID-2-100-1-116 | | |
| 授業科目名／Course title | 情報セキュリティⅠ／Information Security Ⅰ | | |
| 編集担当教員／Instructor in charge of the course syllabus | 荒井　研一／Arai Kenichi | | |
| 授業担当教員名（科目責任者）／Instructor in charge of the course | 荒井　研一／Arai Kenichi | | |
| 授業担当教員名（オムニバス科目等）／Instructor(s) | 荒井　研一／Arai Kenichi | | |
| 科目分類／Course Category | 共通科目，情報学基盤科目（コンピュータ科学） | | |
| 対象年次／Intended year | 3 | 講義形態／Course style | 講義／Lecture |
| 教室／Class room | グローバル教育・学生支援課　文教スカイホール | | |
| 対象学生（クラス等）　/Intended year (class) | 工学科（情報工学コース）3年次 | | |
| 担当教員Eメールアドレス/E-mail address | k-arai@nagasaki-u.ac.jp | | |
| 担当教員研究室/Office | 工学部 1 号館 4 階「教員・ゼミ室 405」 | | |
| 担当教員TEL/Tel | 095-819-2701 | | |
| 担当教員オフィスアワー/Office hours | 月曜 5 校時 | | |
| 授業の概要及び位置づけ/Course overview | 情報セキュリティ技術の基盤をなす暗号理論の基本的概念を習得する．<br>具体的には，公開鍵暗号および共通鍵暗号（秘密鍵暗号）の原理についての知識を習得する． | | |
| 授業到達目標/Course goals | ・情報データ科学分野に必要な基礎的知識を修得している（DP-①）．<br>具体的には，暗号の概念・仕組み・性質を理解し，その重要性を認識することができるようになる． | | |
| 知識・技能以外に、この授業を通して身につけて欲しい力（1つ以上3つまで）/Abilities other than knowledge and skills acquired mainly through the course ( pick 1 to 3 ) | ■主体性／Autonomy　■汎用的能力／Generic Competence　□倫理観／Ethics　□多様性の理解／Understanding Diversity　□協働性／Cooperativeness　□考えをやり取りする力／Ability to exchange ideas　□国際・地域社会への関心／Interest in international / local society | | |
| 学生の思考を活性化させるための授業手法/Teaching method to stimulate students' thinking | ■A.授業内容の理解度を確認したり自分で考えさせたりする活動 <br>/ Activities to check the degree of comprehension of the contents to the lesson or to think over<br>□B.多角的に考えるために他者と関わる活動 <br>/ Activities involving others to think from various perspectives<br>□C.技能修得のために実践する活動 <br>/ Activities to practice for acquiring skills<br>□D.問題解決のために知識を総合的に活用する活動 <br>/ Activities that comprehensively utilize knowledge to solve problems<br>□E.上記以外の学生の思考の活性化を促す授業手法 <br>/ Teaching methods to stimulate students' thinking other than the above<br>□F.教員からの講義のみで構成される <br>/ It consists only of lectures from teachers | | |
| 成績評価の方法・基準等/Method of evaluation | 定期試験（100点満点）で60点以上を合格とする．<br>成績評価については，「定期試験の成績」と「定期試験80%＋課題レポート20%」の良い方を評価点とする． | | |
| 各回の授業内容・授業方法（学習指導方法）/Course contents of each lesson | 詳細は授業計画詳細を参照 | | |
| 事前、事後学習の内容/Preparation & Review | （予習）教科書，参考書，配布プリント等で該当範囲について事前に読んでおくこと（2h）．<br>（復習）講義内容の復習および演習問題を解いて，理解を深めること（2h）． | | |
| キーワード/Keywords | 公開鍵暗号，共通鍵暗号（秘密鍵暗号），RSA暗号，ElGamal 暗号，DES，暗号利用モード | | |
| 教科書・教材・参考書/Materials | 教科書： プリントを配布<br>参考書： 笠原正雄・境隆一著「暗号－ネットワーク社会の安全を守る鍵」，共立出版<br>結城浩著「暗号技術入門 第3版」，SBクリエイティブ | | |
| 受講要件（履修条件）/Prerequisites | 授業への出席は必須． | | |

| | |
|---|---|
| アクセシビリティ/Accessibility (for students with disabilities) | 長崎大学では，全ての学生が平等に教育を受ける機会を確保するため，修学の妨げとなり得る社会的障壁の除去及び合理的配慮の提供に取り組んでいます。授業における合理的配慮等のサポートについては，担当教員（上記連絡先参照）または「アシスト広場」（障がい学生支援室）にご相談下さい。<br>アシスト広場（障がい学生支援室）連絡先<br>（TEL）095-819-2006　　（FAX）095-819-2948<br>（E-MAIL）support@ml.nagasaki-u.ac.jp |
| 備考（URL）/Remarks (URL) | |
| 学生へのメッセージ/Message for students | 抽象的な概念や理論を理解するには，時間をかけて考えることおよび演習問題を自分の力で解くことが重要である．従って，授業に集中し，予習・復習を十分行うこと． |
| 実務経験のある教員による授業科目であるか（Y／N)/Instructor(s) with practical experience | N |
| 実務家教員名／実務経験内容／実務経験に基づく教育内容（実務経験のある教員による授業科目のみ使用）/Name / Details of practical experience / Contents of course | |
| 授業計画詳細／Course Schedule | |
| 回(日時)／Time(date and time) | 授業内容／Contents |
| 第1回 | 現代暗号の概要（現代暗号の概要について説明できる） |
| 第2回 | 公開鍵暗号の概要（公開鍵暗号の概要について説明できる） |
| 第3回 | RSA 暗号（RSA 暗号の原理について説明でき，暗号化・復号の計算ができる） |
| 第4回 | ElGamal 暗号（ElGamal 暗号の原理について説明でき，暗号化・復号の計算ができる） |
| 第5回 | 共通鍵暗号（秘密鍵暗号）の概要（共通鍵暗号の概要について説明できる） |
| 第6回 | DES（DES の原理について説明でき，暗号化・復号の計算ができる） |
| 第7回 | 暗号利用モード（暗号利用モードの原理について説明できる） |
| 第8回 | 定期試験 |