

2026 年度シラバス

科目分類/Subject Categories			
学部等/Faculty	/工芸科学部 : /School of Science and Technology	今年度開講/Availability	/有 : /Available
学域等/Field	/設計工学域 : /Academic Field of Engineering Design	年次/Year	/2年次 : /2nd Year
課程等/Program	/情報工学課程・課程専門科目 : /Specialized Subjects for Undergraduate Program of Information Science	学期/Semester	/後学期 : /Second term
分類/Category	/:/	曜日時限/Day & Period	/火1 : /Tue.1

科目情報/Course Information				
時間割番号 /Timetable Number	12222101			
科目番号 /Course Number	12260031			
単位数/Credits	2			
授業形態 /Course Type	講義 : Lecture			
クラス/Class				
授業科目名 /Course Title	情報セキュリティ : Information Security			
担当教員名 / Instructor(s)	/稲葉 宏幸/榎田 秀夫 : /INABA Hiroyuki/MASUDA Hideo			
その他/Other	インターンシップ実施 科目 /Internship	国際科学技術コース提供 科目 /IGP	PBL 実施科目 /Project Based Learning	DX 活用科目 /ICT Usage in Learning
				○
	実務経験のある教員による 科目 /Practical Teacher			
科目ナンバリング /Numbering Code				

授業の目的・概要 /Objectives and Outline of the Course	
日	現在の情報通信システムでは、情報セキュリティを考慮することが必要不可欠である。本講義では、現在の情報通信システムにおいて用いられる情報セキュリティ技術とその数学的基盤について述べる。
英	Information security is indispensable for information communication system. We will focus on the typical information security technology and the mathematical basis in this lecture.

学習の到達目標 /Learning Objectives	
日	情報セキュリティに必要な要件を列挙できる 情報セキュリティ技術を支える数学的基盤に関する知識を有している 公開鍵認証基盤(PKI)の必要性とそのしくみについて説明できる 基本的な公開鍵暗号方式についてそのしくみを説明できる 電子署名について代表的な方式に関する知識を有している セキュリティに対する主な脅威とその対策手法を説明できる デジタルコンテンツの保護技術に関する基礎的知識を有している 個人認証技術に関する基礎的知識を有している
英	To list important matters required for information security. To learn mathematical basis that support information security. To explain a requirement of PKI and the system. To explain fundamental public key crypto systems. To learn typical digital signature scheme.

	To explain typical threat in network security and its countermeasures. To learn fundamental technology for managing digital contents rights. To learn fundamental biometrics authentication.
--	--

学習目標の達成度の評価基準 / Fulfillment of Course Goals (JABEE 関連科目のみ)	
日	
英	

授業計画項目 / Course Plan			
No.		項目 Topics	内容 Content
1	日	情報セキュリティとは	情報セキュリティとは何か。情報の機密性、完全性、可用性について。暗号技術の変遷。共通鍵暗号。
	英	Introduction of Information Security	To learn confidentiality, integrity, and availability. To learn history of crypto technology. To learn symmetric crypto system.
2	日	整数論の基礎(1)	ユークリッドの互除法、整数の合同関係
	英	Fundamentals of number theory (1)	To learn Euclidean algorithm, congruences.
3	日	整数論の基礎(2)	一次合同式、中国の剰余定理、剰余類
	英	Fundamentals of number theory (2)	To learn how to solve linear congruence equation, chinese remainder theorem, and residue class ring.
4	日	整数論の基礎(3)	群・環・体、オイラーの関数
	英	Fundamentals of number theory (3)	To learn group, ring, and field. To learn Euler's phi function.
5	日	公開鍵暗号(1)	共通鍵暗号と公開鍵暗号の違い、公開鍵暗号の原理、RSA 暗号、ElGamal 暗号、Rabin 暗号、楕円曲線暗号
	英	Public key encryption (1)	Public key encryption (1)
6	日	公開鍵暗号(2)	公開鍵暗号の概念と PKI、素数生成と素因数分解、公開鍵暗号の安全性
	英	Public key encryption (2)	To learn PKI, generation of prime numbers, prime factorization, and security of public key cryptosystem.
7	日	電子署名	電子署名の原理、RSA 署名、ElGamal 署名、ハッシュ関数、デジタル署名の安全性
	英	Digital signature	To learn principles of digital signature, RSA signature, ElGamal signature, and hash functions. To learn security of digital signature.
8	日	セキュリティプロトコル(1)	鍵共有とは、DH 鍵共有方式、楕円曲線 DH 鍵共有方式、秘密分散法、マルチパーティープロトコル、Tor
	英	Secure protocols (1)	To learn principles of key sharing, DH and DH over elliptic curve key sharing method, secret sharing scheme, multi party computation protocols and Tor.
9	日	セキュリティプロトコル(2)	平方剰余とは、ゼロ知識証明、量子鍵配送
	英	Secure protocols (2)	To learn quadratic residue, zero knowledge interactive proof, and quantum key distribution.
10	日	セキュリティプロトコルの応用技術	電子マネー、電子投票、ブロックチェーン、ビットコイン
	英	Applications of secure protocols	To learn electronic money, BitCoin, blockchain, and electronic voting.
11	日	クライアント認証	チャレンジレスポンス、ワンタイムパスワード、公開鍵認証
	英	Client authentication	To learn challenge-response scheme, one-time password, and public key authentication.
12	日	インターネットセキュリティ(1)	ネットワークプロトコル階層とセキュリティ、IPSEC、SSL/TLS、VPN
	英	Internet security (1)	To learn network protocol layer and secure protocols, IPsec, SSL/TLS, and VPN.
13	日	インターネットセキュリティ(2)	マルウェア、電子メールセキュリティ、ウェブセキュリティ、ファイアウォール、IDS
	英	Internet security (2)	To learn malware, e-mail security, web security, firewall and IDS.
14	日	個人認証技術とデジタルコ	個人認証技術の種類、バイオメトリクスとは、認証精度の評価、DRM、電子透かし

		コンテンツの保護技術	
	英	Biometrics authentication and Digital Rights Management	To learn fundamentals of personal authentication, biometrics, authentication accuracy. To learn DRM and digital watermark.
15	日	量子コンピュータと暗号解読、まとめ	量子コンピュータとは、ショアのアルゴリズム、まとめ
	英	Quantum computer and cipher braking, Wrap-up	To learn basic concept of quantum computer, Shor's algorithm. To review the contents of the lectures, and to learn remaining problems.

履修条件 /Prerequisite(s)	
日	
英	

授業時間外学習（予習・復習等） /Required study time, Preparation and review	
日	<p>補足資料やレポート課題は LMS(Moodle)上で提示されるので、定期的に確認すること。</p> <p>講義終了後、LMS 上で復習テストに回答すること。</p> <p>講義終了後、次回講義までに、教科書、ノート、補足資料を熟読し復習しておくこと（2時間以上）。</p> <p>演習およびレポートを数回課すので、期日までに必ず提出すること。</p>
英	<p>Materials and report theme will be provided on LMS(Moodle).</p> <p>After the class, a short reviewing exam will be provided on LMS.</p> <p>2 hours reviewing are required.</p>

教科書／参考書 /Textbooks/Reference Books	
日	教科書「情報セキュリティの基礎」（佐々木良一監修、手塚悟編著、共立出版）／参考書「情報セキュリティ-暗号・認証・倫理まで」（辻井重男・笠原正雄編著、昭晃堂。）、「情報セキュリティ」（宮地充子・菊池浩明編著、オーム社）、「暗号と確率的アルゴリズム入門」（H.デルフス・H.クネーブル著、シュプリンガー・フェアラク東京）、「ネットワークセキュリティ」（菊池 浩明、上原 哲太郎著、オーム社）、「情報セキュリティ基礎講義」（松浦幹太著、コロナ社）
英	The textbook is Fundamentals of Information Security by Kyoritsu pub.

成績評価の方法及び基準 /Grading Policy	
日	学期末試験 60%、講義への積極的関与(レポート、復習テスト、質問等)40%により評価する。
英	Performance evaluation of this subject will be conducted by the term-end exam (60%) and reports, reviewing exams (40%).

留意事項等 /Point to consider	
日	<ul style="list-style-type: none"> ・レポートは、文章を引用する際は、引用箇所が明確にわかるようにし、出典を記載すること。度を越えた引用は慎むこと。引用部分は誤字を含めて改変しないこと。 ・他人が作成したレポートを自分が作成したとして提出しないこと
英	<p>Ensure that when quoting text in reports, the source of the quotation is clearly indicated and properly cited. Avoid excessive quotations, and do not alter quoted passages, even to correct typographical errors.</p> <p>Do not submit a report that you did not create yourself; in other words, do not present someone else's report as your own.</p>