IT・数値解析特論

授業科目名	IT・数値解析特論		
担当教員（所属）	《富山大学大学院理工学研究部（工学)》田島正登，柴田啓司 《富山大学　総合情報基盤センター》沖野浩二 外部講師：《会津大学コンピュータ理工学部》大川 知 外部講師：《(独）産業技術総合研究所・情報セキュリティ研究センター》川村信一 外部講師：未定		
授業科目区分	スーパーエンジニア養成コース	授業種別	大学院修士課程実践教育特別講義科目
		対象所属	理工学教育部
講義日程	12月－2月　木曜日　6、7眼 (18：30 ～ 21：40)	対象学年	社会人技術者，大学院生
		単位数	2単位
連絡先（研究室、電話番号、電子メール等）	{tajima、shibata}@eng.u-toyama.ac.jp、okino@itc.u-toyama.ac.jp		
オフィスアワー（自由質問時間）			

授業のねらいとカリキュラム上の位置付け（一般学習目標）

コンピュータはネットワークに接続されて初めてその威力を発揮するという意味で，コンピュータ・ネットワークに関する理解は不可欠である。また，これに伴い，ネットワークの信頼性（誤り無く情報を伝達する）や安全性（セキュリティ）の問題が益々重要となっている。この講義では，ネットワークや情報セキュリティに関係する基礎的な内容を理解すると共に，最近の関連技術，また応用等の理解を深めることを目的とする。

達成目標

1）ICT（Information and Communication Technology）の現状や今後の展開等について理解する。
2）暗号等の安全性の根拠となっている計算量の問題や計算可能性について理解する。
3）暗号技術の基礎事項を理解すると共に，最新の暗号技術についても理解を深める。
4）ネットワークの構造やプロトコルなど，コンピュータ・ネットワークに関係する基本事項について理解する。
5）ネットワークを取り巻く脅威とその対策，また利用者が守るべき情報倫理等について理解を深める。

授業計画（授業の形式、スケジュール等）

第1回（12/13）	ICT 概論	ICT の広がりと現在の役割についての概論	沖野
第2回（12/13）	暗号技術（公開鍵暗号）	DH 型公開鍵配送法，RSA 暗号，ElGamal 暗号	田島
第3回（12/20）	計算可能性（1）	計算可能性および計算量について	大川
第4回（12/20）	計算可能性（2）	計算可能性および計算量について（続き）	大川
第5回（ 1/10）	暗号技術（秘密鍵暗号）	DES，AES，Feistel 構造，SPN 構造	川村
第6回（ 1/10）	最新の暗号技術	ヴェイユ対，双線形性，量子暗号	川村
第7回（ 1/17）	認証，PKI	認証方式，PKI 概論	田島
第8回（ 1/17）	伝送方式	誤り訂正符号など	田島
第9回（ 1/24）	TCP/IP（1）	OSI 参照モデルと TCP/IP	沖野
第10回（ 1/24）	TCP/IP（2）	ネットワークの構成要素	沖野
第11回（ 1/31）	コンピュータ・ウィルス	Computer Virus の実態	外部講師
第12回（ 1/31）	ネットワーク・セキュリティ	injection や exploit の実態	外部講師
第13回（ 2/ 7）	ネットワーク管理	サーバ管理とネットワーク管理	柴田
第14回（ 2/ 7）	リスク・マネジメント	情報リスクの把握	沖野
第15回（ 2/14）	知的財産，情報倫理，関係法令	情報関連法令	沖野

キーワード	ネットワーク，情報 / ネットワーク・セキュリティ，暗号，計算量，ネットワーク管理，リスク・マネジメント		
履修上の注意			
教科書参考書等			
成績評価の方法			
関連科目			
リンク先ＵＲＬ			
オープン・クラス		単位互換	
備考			

IT・数値解析特論：授業計画

回	主題と位置付け（担当）	学習方法と内容
1	ICT 概論 ICT の広がりと現在の役割についての概論 （沖野）	ICT の発達の歴史を振り返り、現在の社会における役割を考え、今後の学習の参考とする。
2	暗号技術（公開鍵暗号） DH 型公開鍵配送法、RSA 暗号、ElGamal 暗号 （田島）	DH 型公開鍵配送法は公開鍵暗号の概念を初めて与えたものである。また、代表的な公開鍵暗号方式である、RSA 暗号や ElGamal 暗号について学習する。
3	計算可能性（1） 計算可能性および計算量について （大川）	第 2 回で学習した公開鍵暗号の背景にある計算量 / 計算複雑性を理解することを目的として、計算可能性および計算量の議論を行なう。第 3 回では、主に計算可能性について学ぶ。
4	計算可能性（2） 計算可能性および計算量について（続き） （大川）	今回は、主に計算量 / 計算複雑性について学ぶ。これは、前回学んだ計算可能性がいわば絶対的な計算可能性であるのに対し、有限の存在である人間の視点から計算可能性を見ようとするものである。実際的な計算可能性として計算量 / 計算複雑性をとらえ、それを暗号の強度の保証に結び付けたのが現代の暗号理論である。
5	暗号技術（秘密鍵暗号） DES、AES、Feistel 構造、SPN 構造 （川村）	代表的な秘密鍵暗号である DES（Feistel 構造をもつ）および AES（SPN 構造をもつ）について、それらの基本構成や特徴について理解する。
6	最新の暗号技術 ヴェイユ対、双線形性、量子暗号 （川村）	ヴェイユ対や双線形性を利用した暗号方式、あるいは量子理論に基づく量子暗号など、最近の暗号技術について理解を深める。
7	認証、PKI 認証方式、PKI 概論 （田島）	認証は、秘匿と並んで暗号のもつ最も重要な機能である。最初に、公開鍵暗号を用いたディジタル署名について学ぶ。また、公開鍵の正当性を確認する枠組みとしての、公開鍵基盤（PKI）について学習する。
8	伝送方式 誤り訂正符号など （田島）	暗号は情報の安全性を守る技術の一つと見なせるが、一方、情報の信頼性を高める技術である、誤り訂正符号やその関連事項について学習する。
9	TCP/IP（1） OSI 参照モデルと TCP/IP （沖野）	通信プロトコルの基本概念である OSI 参照モデルは、機能を 7 階層に分類している。現在のネットワークで使用されている TCP/IP を OSI 参照モデルの各階層に対応させて機能・役割などを学習する。
10	TCP/IP（2） ネットワークの構成要素 （沖野）	異なるネットワークを接続・延長するハードウエア機器（ブリッジ、ルーターなど）はネットワーク構成上重要である。こうした機器の種類、しくみ及び役割等について学習する。
11	コンピュータ・ウィルス Computer Virus の実態 （外部講師）	実際のコンピュータ・ウィルスについて解説する。
12	ネットワーク・セキュリティ injection や exploit の実態 （外部講師）	データベース（DB）や Web アプリへの不正アクセス例について解説する。
13	ネットワーク管理 サーバ管理とネットワーク管理 （柴田）	実際のネットワーク運用を行うには、サーバ管理およびネットワーク管理知識が必要である。サーバおよびネットワーク管理における重要ポイントを解説する。

回	主題と位置付け（担当）	学習方法と内容
１４	リスク・マネジメント 情報リスクの把握 （沖野）	情報セキュリティを担保するには、リスクを正しく把握することが重要である。情報システムにおけるリスクおよびリスク解析手法を学習する。
１５	知的財産、情報倫理、関係法令 情報関連法令 （沖野）	実際に情報セキュリティを維持するには、技術だけでなく法的な規定も存在する。知的財産に代表される情報関係の法令知識を学習する。