REC for NS

自然科学研究教育センター講演会（第32回）

現代暗号理論の数理

暗号は，しばしば小説や映画の中にも登場しますが，その中で暗号はパズルや謎解きの一種として描かれることが少なくありません。現代の暗号学は単なるパズルでなく科学分野の１つとして発展しています。現代の暗号理論は，数学や情報科学等に跨る学際的研究分野であり，また現代情報社会における情報セキュリティ技術を支える基礎理論であるため，その内容は応用の観点からも重要です。本講演では，現代暗号理論において，暗号システムの安全性（セキュリティ）を如何に数学的立場から形式に考え，如何なる数学的構造により安全なシステムを実現できるか，について概説します。例えば，世界で広く利用されているRSA暗号の安全性は素因数分解問題の困難性に依存しており，このように整数論に関わる数学的構造以外にも，様々な代数構造や組合せ構造等も暗号システム構築の上で利用されています。また，本講演では，数学や情報科学分野で著名な研究者であるチューリングやシャノンの暗号学への関わり方や，これまでのチューリング賞受賞業績のうち暗号学に関わる内容についても平易に解説したいと思います。また最後に，未来の暗号技術とその応用を見据えて，今後の暗号理論の発展の方向性とそれに対する期待についても触れてみたいと思います。

2015年6月26日（金）16:30～18:00

会　場：慶應義塾大学日吉キャンパス 来往舎１階シンポジウムスペース
※日吉駅から徒歩３分

対　象：学生・教職員・一般

参加費：無料（申込不要）

講師：**四方 順司** 氏

◇横浜国立大学 大学院環境情報研究院 准教授

京都大学理学部数学科卒業，同大学院理学研究科 数学・数理解析専攻修士課程修了，大阪大学大学院理学研究科数学専攻博士後期課程修了。博士（理学）。その後，東京大学研究員，横浜国立大学講師・助教授を経て，現在は横浜国立大学大学院環境情報研究院准教授。また，2008～2009年はスイス連邦工科大学（ETH Zurich）に客員研究者として滞在。専門は，暗号理論，情報理論，理論計算機科学，計算数論等の分野であり，数学・情報学・コンピュータサイエンスに跨る学際的分野の理論研究に従事。これまで，平成22年度科学技術分野の文部科学大臣表彰（若手科学者賞）受賞，British Computer Society（英国計算機学会）から2006年度 The Wilkes Award 受賞，電気通信普及財団から第19回電気通信普及財団賞（テレコムシステム技術賞）受賞をはじめ，多くの受賞歴がある。

天災･交通事情など予期せぬ事態により変更･中止となる場合がございます。その場合，下記のウェブサイトでお知らせしますので，事前にご確認下さい。

慶應義塾大学 自然科学研究教育センター
Tel：045-566-1111　URL：http://www.sci.keio.ac.jp/　E-mail：office@sci.keio.ac.jp

URL