

次号予告

特集 意外と身近な存在, 情報化社会の暗号技術

情報化社会における暗号技術の役割	神田雅透 (N T T)
暗号のための基礎理論	田中圭介 (東京工業大学)
公開鍵暗号 (RSA/楕円曲線暗号) の安全性	高木 剛 (はこだて未来大学)
共通鍵暗号のしくみと安全性評価	松井 充 (三菱電機)
Σプロトコルとその応用	尾形わかは (東京工業大学)
公開鍵暗号危殆化対策のためのリスク評価	佐々木良一 (東京電機大学)
量子公開鍵暗号とその後の動向	宮澤俊之 (N T T)

編集後記

●私は今年の前期にデータ解析入門の講義を受け持ちました。内容は確率と統計の基礎を、大学2年生を対象として教えるものです。受講者は高校でのクラスが理系と文系ほぼ半分ずつでした。順列・組み合わせから始まって、母平均の検定までを半期15コマで教えたのですが、履修後のアンケートを読んでみると授業の進み方が早く理解が充分でなかったとの意見があり、来年度により良い授業をすべく思案中です。

●データ解析は、客観的な数値をもとに意思決定をするというORの根幹の部分の司っており重要な思考法と考えます。また経営学や品質管理、心理学実験の解析等、文系理系を超えたあらゆる分野に横断的に使用されているツールであり、ゆえにその使い方や概念の

理解は正確でなければなりません。

●市販されているもの、無料でインターネットからダウンロードできるものまで数多くの統計ツールが簡単に手に入ります。PCは瞬時に何万、何十万ものデータを計算し、グラフ化してくれます。しかしそのような状況だからこそ、正しい使用法がますます求められてきていると考えます。Garbage in, Garbage out (ゴミを入れればゴミしか出てこない) ではないのです。

●本特集のデータ解析コンペティションは、高度な技術を競い合ういわば統計のオリンピックに当たるものと思いますが、データ解析をわかりやすく普及させる教育的技術にも、より時代に合わせた変化が求められていると考えています。(増田浩通)

オペレーションズ・リサーチ 編集委員会

委員長 山下英明 (首都大学東京)

委員 池邊淑子 (東京理科大学), 岡野裕之 (日本アイ・ビー・エム(株)), 木村新之介 (東京ガス(株)), 草刈君子, 栗田佳文 (防衛省), 高野正次 (日本電信電話(株)), 齋藤彰一 (株構造計画研究所), 高嶋隆太 (東京大学), 田島博之 (秀明大学), 田村一軌 (財鉄道総合技術研究所), 豊泉 洋 (早稲田大学), 生田目崇 (専修大学), 廣津信義 (順天堂大学), 牧本直樹 (筑波大学), 増田浩通 (千葉工業大学), 村井雅彦 (株東芝), 八木恭子 (東京大学) 渡邊 勇 (財電力中央研究所)

本誌に掲載された記事についての著作権は、社団法人 日本オペレーションズ・リサーチ学会に帰属する。

オペレーションズ・リサーチ

平成21年2月号 第54巻 第2号 通巻578号

代表者 伏見 正 則

発行所 社団法人 日本オペレーションズ・リサーチ学会

東京都文京区弥生2-4-16 学会センタービル

電話 03-3815-3351(代) FAX 03-3815-3352 〒113-0032

<http://www.orsj.or.jp/>

編集人 山下 英 明

発売所 株式会社 日科技連出版社

東京都渋谷区千駄ヶ谷5-4-2 〒151-0051

●本誌のご注文は直接

日本オペレーションズ・リサーチ学会へ 定価970円(本体924円)年間予約購読料11,040円(税込)

●本誌への広告お申し込みは明報社(3546-1337)へ