次号予告

特集　東芝の経営と顧客向け製品・サービスにおけるOR

東芝の経営改革活動とOR ……澤田静雄（東　　芝）
省エネルギー・環境システムにおけるOR—エネルギー・上下水道管理システムの運用改善—
……村井雅彦（東　　芝），他
実用性を重視した組合せ最適化技術の応用—多様な解の出力と計算資源制約—
……田中俊明（東　　芝），他
最適性とリスクを考慮した企業の意思決定支援技術—与信管理と市場品質管理における適用事例—
……西川武一郎（東　　芝），他
原子力分野のリスク評価技術の他分野への適用—情報システムの信頼性評価と管理—
……竹澤伸久（東　　芝），他

編集後記

●特集は，「意外と身近な存在，情報化社会の暗号技術」でしたが，この準備期間中に，無線LANの暗号方式の脆弱性について，多くのニュースが流れました．

●昨年10月，森井昌克教授を中心とする神戸大学と広島大学の研究グループが，「WEPは10秒で解読可能」とコンピュータセキュリティシンポジウム2008で発表しました．検証に使用したPCのスペックは，CPUがAthlon 64 X2 4600＋2.41 GHz，メモリ1 GB，OSはWindows XP SP2という平均的なマシン環境で，104 bitのWEP鍵の解読に成功したとの報告です．

●さらに，11月には「WPA暗号の解読に部分的に成功した」との発表が続きました．要する時間は12分から15分．この研究は，Erik Tews氏によるものですが，彼こそ，60秒でWEPを解読してその脆弱性を明らかにした人物でした．これが，2007年4月ですから，わずか18ヶ月の間に，WEPの解読に要する時間が1/6の短縮されたわけです．数年以内に，WPAも10秒で解読可能になることと予想できるかもしれません．

●わが国の総務省の「国民のための情報セキュリティサイト」には重要なお知らせとして，WEPの利用に関する注意喚起が載せられています．しかし，世の中にはWEPにしか対応できない通信機器が多く使われ続けていて，WEPを利用しているユーザが半数を超えると危惧されています．暗号技術の寿命が，ハードやソフトの高速化によっていよいよ短くなり，ごく普通の人々の生活の安心・安全が脅かされることが空想世界ではないことを感じました．　　（高野正次）

オペレーションズ・リサーチ

平成21年3月号　第54巻　第3号　通巻579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㈹ 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（税含）
●本誌への広告お申し込みは明報社（3546-1337）へ