

2007-6



90巻6号 平成19年6月
社団法人 電子情報通信学会

〒105-0011 東京都港区芝公園3-5-8機械振興会館内
電話 (03) 3433-6691(代) FAX (03) 3433-6669
E-mail: office@ieice.org 振替口座:00120-0-35300

目次

電子情報通信学会誌

会長 富永英義
次期会長 宮原秀夫
副会長 安田浩
雨宮真人
津田俊隆
伊藤弘昌
総務理事 萩本和男
坂庭好一
会計理事 江村克己
高橋達郎
編集理事 森川博之
山本浩治
企画理事 得井慶昌
西原明法
調査理事 喜多泰代
花澤隆
編集長 篠田庄司
企画室長 古井貞照
規格調査会委員長 羽鳥光俊
監事 後藤敏平
田康夫

基礎・境界
ソサイエティ会長 大石進一
次期ソサイエティ会長 小林欣吾

通信
ソサイエティ会長 吉田進
次期ソサイエティ会長 間瀬憲一

エレクトロニクス
ソサイエティ会長 安藤真
次期ソサイエティ会長 河内正夫

情報・システム
ソサイエティ会長 末永康仁
次期ソサイエティ会長 畑岡信夫

北海道支部長 野矢厚
東北支部長 羽深龍二
東京支部長 喜連川優
信越支部長 島田正治
東海支部長 伊藤卓志
北陸支部長 松本忠
関西支部長 山下勝己
中国支部長 藤岡清人
四国支部長 樋口弘志
九州支部長 相川正義

巻頭言

目次前

新たなイノベーションの基礎を
——自然事象基盤から人間事象基盤へのパラダイムシフト——

副会長 安田 浩

小特集 暗号技術の証明可能安全性

425

小特集編集にあたって

編集チームリーダー 岡本 健

426

1. 証明可能安全性理論に向けて
職人芸から科学へ、飛躍の「ココロ」と「アイデア」を解説する

太田和夫

431

2. 証明可能安全性を持つブロック暗号の構成法
代表的な共通鍵暗号方式の安全性を探る

盛合志帆

436

3. 選択暗号文攻撃安全な公開鍵暗号の構成法について
公開鍵暗号方式の安全な構成法を解説する

藤崎英一郎

442

4. デジタル署名の証明可能安全性と方式設計への帰還
安全性証明の見直しから発見されるデジタル署名方式の改良点

駒野雄一

447

5. ハッシュ関数の構成と証明可能安全性
ハッシュ関数の衝突? 安全な暗号・デジタル署名技術のために

廣瀬勝一

451

6. はん用的結合可能性と数理的技法
安全性証明の新たな方法論

岡本龍明

特別解説

457

デジタル交換技術の研究開発——人と技術の系譜——
れい明期のデジタル交換機開発における先人たちの苦闘

葉原耕平

解説

470

広域イーサネットサービス——商用サービスの歴史とプロトコル動向——
日本がけん引する大規模ネットワークサービスとそれを支える技術

浅見 徹

476

IEC/TC56 ディペンダビリティ関連規格の現状と将来動向
信頼性・安全性の高い製品開発を目指して

益田昭彦 夏目 武 佐藤吉信

483

研究会発表申込みシステムの概要と活用
——講演検索も容易になった新システムの紹介——
手続きの省力化に加え、活用の利便性も向上した新システムを紹介

辻岡哲夫

その他

図書紹介 502 国内文献目次 503 図書寄贈一覧 503 本会だより 504
編集室 508 複写される方へ 会告参照 会告 後付 論文誌目次 会告後
広告目次 巻頭言前

講座

488

情報通信の基礎と動向[II]——チャンネルと広帯域変調——
無線通信と光通信の概要がこれで分かる

大槻知明

寄書

495

e シルクロードとパンダ画像伝送プロジェクト
札幌発、IT がもたらした国際親善

青木由直

ニュース解説

498

金・銀・銅を触媒としたカーボンナノチューブの合成

男女共同参画のページ

500

科学技術振興調整費プログラム「女性研究者支援モデル育成」
——日本女子大学における「女性研究者マルチキャリアパス支援プロジェクト」の取り組み——

小館香椎子

国際会議

435

2006 IEEE International Ultrasonics Symposium

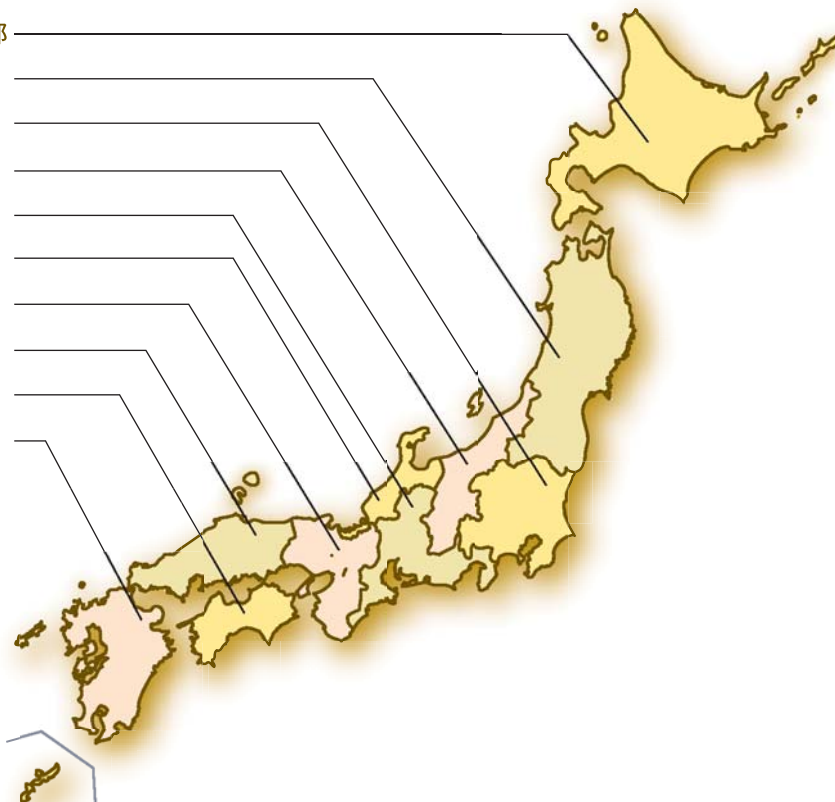
大森達也

456

The 7th International Workshop on Radiation Effects on Semiconductor Devices
for Space Application

新藤浩之

北海道支部
東北支部
東京支部
信越支部
東海支部
北陸支部
関西支部
中国支部
四国支部
九州支部



本誌に掲載された寄稿等の著作権は社電子情報通信学会に帰属します

会誌編集委員会

編集長 篠田庄司
編集理事 森川博之・山本浩治
編集特別幹事 趙晋輝・塩本公平
平川一彦・鷲見和彦

WG・A

主査 趙晋輝
副主査 真野健・酒井哲也
委員 大田恭士・加藤浩介
小峯一晃・近藤淳
坂主圭史・田中聡久
タンスリヤボン スリヨン
中里純二・中村一彦
藤芳明生・堀田裕弘
村松正吾・目黒光彦

WG・B

主査 塩本公平
副主査 辻岡哲夫・中村元
委員 居相直彦・池川隆司
大塚昌孝・加沢徹
笹田武志・周曉
杉山一雄・田上敦士
鶴岡哲明・中里学
藤野義之・松村宏一
村井仁・山本全昭

WG・C

主査 平川一彦
副主査 大見俊一郎・安藤淳
委員 石川光映・稲野滋
井上忠宣・杉山正和
多田哲生・辻寧英
中本正幸・檜枝護重
舟橋政樹・前田博己
松野典朗・山口雅史
山田隆宏

WG・D

主査 鷲見和彦
副主査 濱崎雅弘・奥田英範
委員 生駒洋子・石寺永記
内田誠一・神田準史郎
櫻井茂明・高野光司
武部浩明・豊泉洋
内藤正樹・苗村昌秀
中沢憲二・湯浅真由美
湯川高志・芳澤伸一
吉田昌司

ニュース委員会

委員長 篠田庄司
幹事 平川一彦・塩本公平
委員 五十嵐讓・岩間健宏
大久保洋幸・川村卓也
河島整・喜瀬智文
岸根桂路・北山賢一
久保田徹・黒木英生
鹿田實・西海聡子
西村公佐・藤田卓
松井裕一・宮田英之
山中秀昭

会誌に対する御意見をお寄せ下さい。

<http://www.ieice.org/jpn/books/kaishiiken.html>

©電子情報通信学会 2007