

2011-11



94巻11号平成23年11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) 3433-6659  
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 安田 浩  
次期会長 吉田 進  
副会長 中嶋 信生  
北山 研一  
喜連川 優  
間瀬 憲一  
総務理事 江村 克己  
西原 明法  
会計理事 太田 直久  
小林 岳彦  
編集理事 今井 浩  
斎藤 洋  
企画理事 澤田 寛  
本島 邦明  
調査理事 荒川 薫  
佐々木 繁  
編集長 酒井 善則  
企画室長 持田 侑宏  
規格調査会委員長 三木 哲也  
監事 村上 篤道  
木戸出 正継

基礎・境界  
ソサイエティ会長 貴家 仁志  
次期ソサイエティ会長 山本 博資

通信  
ソサイエティ会長 萩本 和男  
次期ソサイエティ会長 田中 良明

エレクトロニクス  
ソサイエティ会長 小山 二三夫  
次期ソサイエティ会長 荒木 純道

情報・システム  
ソサイエティ会長 石田 亨  
次期ソサイエティ会長 萩田 紀博

北海道支部長 前田 純治  
東北支部長 作山 裕樹  
東京支部長 森川 博之  
信越支部長 佐々木 修己  
東海支部長 藤原 修  
北陸支部長 堀 俊和  
関西支部長 高橋 達郎  
中国支部長 羽野 光夫  
四国支部長 中野 好典  
九州支部長 山本 浩之

### 巻頭言

目次前 ICT の ICT による情報発信——編集の立場から—— 編集理事 今井 浩

### 特集 暗号世代交代と社会的インパクト

931 特集編集にあたって 編集チームリーダー 牧野光則

#### 1. 導入

932 1-1 IT 基盤を支える暗号技術と日本の情報セキュリティ政策  
国家の安全保障の根幹としての暗号技術利用とは？  
古原和邦 今井秀樹

#### 2. 暗号政策／方針

938 2-1 日本政府における暗号移行政策 山口利恵  
次世代暗号へのシームレスな移行に向けて

944 2-2 欧米諸国における暗号アルゴリズム選定方針 神田雅透  
これまでの暗号・これからの暗号——安全な暗号利用のための世代交代——

949 2-3 ISO/IEC における暗号アルゴリズムの標準化状況 近澤 武  
暗号アルゴリズムの標準化裏事情

954 2-4 IETF における暗号の世代交代に関わる動向 木村泰司 須賀祐治  
WWW のように相互運用性を保ちつつスムーズに世代交代するために

960 2-5 新しい電子政府推奨暗号リストに向けた CRYPTREC の取組み  
安心安全な暗号の世代交代  
松尾真一郎 山岸篤弘

#### 3. 暗号危たい化状況

966 3-1 共通鍵暗号 盛合志帆  
今日の暗号化技術はいつまで安全に使えるのか？

972 3-2 RSA/素因数分解 青木和麻呂  
古くて新しい素因数分解——RSA 暗号の安全性に与える影響とは？——

### その他

平成 23 年 12 月号小特集予定目次 1019 正誤 971 国内文献目次 1018  
図書寄贈一覧 1018 編集室 1020 複写される方へ 会告参照  
IEICE Global Plaza 会告前 会告 後付 論文誌目次 会告後  
広告目次 巻頭言前

977

3-3 離散対数問題に対する解読世界記録の推移  
暗号危たい化を予測するための暗号解読競争

林 卓也 高木 剛

982

3-4 ハッシュ関数の標準化動向  
安全な電子署名・認証のための基本技術

渡辺 大

987

3-5 暗号等価安全性  
暗号はいつまで安全か？分かりやすい暗号利用指針とは

森川郁也 下山武司

993

3-6 攻撃能力見積り手法  
あと何年、暗号が安心して使えるかが分かります

猪俣敦夫 岡本栄司

999

3-7 情報理論的安全性を有する暗号技術の展望  
攻撃者に負けない、本当に安全な暗号システムを目指して

四方順司

## 4. 各業界の動向

1004

4-1 金融業界における暗号技術の利用と移行問題  
みんなが安心して使える金融サービスを目指して

米山正夫 鈴木雅貴

1008

4-2 SSL 証明書における暗号世代交代  
技術選択のダイナミクスを社会的側面から考える

松本 泰

## ニュース解説

1013 高効率 Si 量子ドット太陽電池実現のための量子ナノ構造作製プロセスの確立

## 国際会議

1015 International Conference on IP+Optical Network

山中直明

1015 2011 IEEE MTT-S International Microwave Symposium

大石敏之

1015 2011 Symposium on VLSI Circuits

須永和久

1016 IEEE International Symposium on Access Space

山中直明

1016 10th International Symposium on Autonomous Decentralized Systems

広津鉄平

1016 2011 IEEE International Symposium on Antennas and Propagation and USNC/URSI  
National Radio Science Meeting

飯草恭一

1017 16th Opto-Electronics and Communications Conference

坂野寿和

1017 18th International Workshop in Active-Matrix Flatpanel Displays and Devices

田邊 浩

## 会誌編集委員会

編集長 酒井善則  
編集理事 今井 浩・斎藤 洋  
編集特別幹事 石井孝明・源田浩一  
吉川信行・苗村昌秀

## WG・A

主 査 石井孝明  
副 主 査 櫻田英樹・高橋篤司  
委 員 一色 剛・今井順一  
久保田 彰・小室信喜  
須賀祐治・土屋隆生  
中口俊哉・早川昭二  
比留間伸行・前田義信  
宮永喜一・山中克久  
湯川正裕

## WG・B

主 査 源田浩一  
副 主 査 吉野 仁・山岡克武  
委 員 飯草恭一・大垣健一  
大木英司・岡田 実  
小黒啓一・草間一宏  
白倉政志・蘇 洲  
高橋国康・辻 弘美  
成田篤信・深沢 徹  
藤崎清孝・不破 泰  
三浦俊二・山口真吾  
横井弘文

## WG・C

主 査 吉川信行  
副 主 査 松永高治・原市 聡  
委 員 五十嵐浩司・大寺康夫  
小野和雄・黒崎武志  
佐久間 健・関根優年  
筒井一生・沼田英俊  
廣本宣久・堀口健一  
丸山道隆・水野幸民  
八木英樹

## WG・D

主 査 苗村昌秀  
副 主 査 植野 研・堀田一弘  
委 員 池 司・伊藤靖朗  
城戸英彰・菅沼優子  
蝶野慶一・永岡 隆  
中藤良久・成田雅彦  
西田泰伸・服部 元  
藤木 淳・水野秀之  
皆川明洋・牟田英正  
望月貴裕・吉川大弘

## ニュース委員会

委 員 長 酒井善則  
幹 事 吉川信行・源田浩一  
委 員 五十嵐 讓・石丸勝洋  
井出 聡・大辻清太  
加藤 隆・河島 整  
川村卓也・曾我部靖志  
高木幸一・西海聡子  
長谷川英明・福田智恵  
藤田 卓・三浦 周  
山本邦彦・山本由香里  
吉川隆士会誌に対する御意見をお寄せ下さい。  
<http://www.ieice.org/jpn/books/kaishiiken.html>