★情報理論研究会（IT）

専門委員長　大濱靖匡　副委員長　和田山　正
幹事　岩本　貢・葛岡成晃　幹事補佐　日下卓也

★情報セキュリティ研究会（ISEC）

専門委員長　角尾幸保　副委員長　満保雅浩・小川一人
幹事　花岡悟一郎・駒野雄一　幹事補佐　伊豆哲也・水木敬明・山下哲孝

★ワイドバンドシステム研究会（WBS）

専門委員長　羽渕裕真　副委員長　前原文明・岡田　実
幹事　松波　勲・佐藤正知　幹事補佐　小澤佑介・中村　聡・中村僚兵

日時　3月10日（木）　9：50～17：45
　　11日（金）　10：00～14：55
会場　電気通信大学東3号館3階301／306（調布市調布ケ丘1-5-1．京王線：調布駅から徒歩5分．http://www.uec.ac.jp/about/profile/access/　岩本　貢）
議題　IT・ISEC・WBS合同研究会

10日午前　IT（1）301会場（9：50～11：30）

1. 符号理論を用いた数独の理解　　名波伸将・○平野伸将・山口和彦（電通大）
2. random coding exponent functionの数値計算における有本アルゴリズムの高速化
　○渡邉広樹・長岡浩司（電通大）
3. マルコフ・フラクタル事前分布をもつ情報源に対するユニバーサル符号の冗長度解析
　○松上直矢・川端　勉（電通大）
4. 任意の事前分布を用いたネットワーク内ウィルス感染源のベイズ推定
　○木戸涼介・松田哲直・松本隆太郎・植松友彦（東工大）

WBS（1）306会場（10：40～11：30）

5. 2機の無人航空機を用いた位置検出法のエリア構成に関する特性評価　　○石川博康・戸来　信・佐藤俊介（日大）
6. OFDMシステムにおける副情報を用いない反復型PTSに基づくPAPR低減の検討
　○吉田萌子・宮嶋照行（茨城大）

10日午後　IT（2）301会場（12：50～14：55）

7. 拡張プライム系列符号を用いたMUIキャンセラのCDMA無線通信への応用
　佐藤紘樹・○宮崎真一郎・松嶋智子・大村光徳・山嵜彰一郎（職能開発大）
8. Insertion/Deletion/Substitution通信路に対する確定シンボルを用いた同期処理法
　○柴田　凌・細谷　剛・八嶋弘幸（東京理科大）
9. 条件付きShannonエントロピーとノルムの期待値との関係とその応用　　○阪井祐太・岩田賢一（福井大）
10. 受信者の事前情報が重複しないインデックス符号化における最小符号語長の導出
　○高橋　優・松田哲直・松本隆太郎・植松友彦（東工大）
11. Intrinsic Randomness Problem for Correlated General Sources
　○Tomohiko Uyematsu・Tetsunao Matsuta（Tokyo Inst. of Tech.）

ISEC（1）306会場（12：50～14：55）

12. Revisiting Isomorphism of Polynomials with Two Secrets　　Bagus Santoso（UEC）
13. 告発アルゴリズムのスコア分布を考慮したTardos符号の検出性能の改善　　○井上　諒・山口和彦（電通大）
14. レインボーテーブルにおける衝突を完全に排除したテーブル構造
　○田畠佑紀・岩井啓輔・田中秀磨・黒川恭一（防衛大）
15. Message Preprocessing for MD Hash Functions
　○Hidenori Kuwakado（Kansai Univ.）・Shoichi Hirose（Univ. of Fukui）
16. 254ビット素数の自乗を位数とする有限体乗算器を64ビット単位パイプライン化モンゴメリ乗算を用いて構成するアーキテクチャ　　○長浜佑介・藤本大介・松本　勉（横浜国大）

IT（3）301会場（15：05～16：45）

17. (11, 5, 2)-巡回差集合より構成される定重み符号における距離特性と相関特性について
　○戒田高康（近畿大）・鄭　俊如（九州女子大）
18. The Effective Method of Improving Berlekamp-Preparata Convolutional Codes Decoding by Tail-Biting Technology　　○Tianyi Zhang・Masato Kitakami（Chiba Univ.）
19. 畳込み符号のConstant Log-MAP復号におけるビット誤り率の解析　　吉川英機（東北学院大）

20. Algebraic Construction of KV Trellises for Linear Block Codes　Masato Tajima

IT(4)306 会場（15：05〜16：45）

21. 半量子鍵配送プロトコルの鍵レートの改善　○山田健斗・松本隆太郎（東工大）
22. エネルギー伝送を行う協力妨害局を用いた盗聴通信路における秘密通信レート
　○小宮山智也・松本隆太郎・松田哲直・植松友彦（東工大）
23. 平文と鍵の推測確率を考慮した暗号システムの基本的性質　○神谷捷太・古賀弘樹（筑波大）
24. インタリーブ攻撃に対する電子指紋符号の容量について　○古賀弘樹・板橋　薫（筑波大）

招待講演(1)301 会場（16：55〜17：45）

25.〔招待講演〕 量子暗号の最近の動向　鶴丸豊広（三菱電機）

11 日午前　IT(5)301 会場（10：00〜12：05）

1. q 入力 r 出力対称通信路における q 元線形符号の性能評価システム　○藤川朋大・山口和彦（電通大）
2. 記憶のある通信路における空間結合 MacKay-Neal 符号の性能解析　○岡崎卓弥・笠井健太（東工大）
3. 局所探索による LDPC 符号の Sum-Product 復号法の改善について
　○河内祐貴・榎　洋史・渡辺宏太郎・片岡靖詞（防衛大）
4. 整数計画法に基づくマルチレベルフラッシュメモリに適した WOM 符号の構成
　○藤野陽樹・和田山　正（名工大）
5. 最隣接点誤り多レベル通信路のゼロエラー容量の漸近評価　○中野貴文・和田山　正（名工大）

ISEC(2)306 会場（10：00〜12：05）

6. Fail-Stop 署名方式及びその UC 安全性に関する再考察　○野村昌弘（元千葉大）・中村勝洋（千葉大）
7. 高速復号可能かつ一般的なアクセス構造を実現した属性ベース暗号
　○土田　光・金山直樹・西出隆志・岡本栄司（筑波大）
8. Non-Programmable ランダムオラクルモデルで安全性証明可能かつ複数の鍵発行機関が存在可能な属性ベース暗号
　○土田　光・金山直樹・西出隆志・岡本栄司（筑波大）
9. 多変数多項式暗号方式 SRP と ABC 方式の性能比較　○安田貴徳（九州先端研）・櫻井幸一（九大）
10. 暗号化データにおける k-匿名化技術　○吉野雅之・長沼　健・佐藤尚宜・福澤寧子（日立）

11 日午後　招待講演(2)301 会場（13：05〜13：55）

11.〔招待講演〕 いくつかの高機能な暗号技術・ツールについての歴史・性質・応用の俯瞰と研究動向
　松田隆宏（産総研）

招待講演(3)301 会場（14：05〜14：55）

12.〔招待講演〕 状態を有する通信路に対する最適符号化レート解析の精密化　八木秀樹（電通大）

◆IEEE IT Society Japan Chapter 共催

☆IT 研究会

【問合先】

IT 研究会幹事，幹事補佐
E-mail：it-sec@mail.ieice.org

☆ISEC 研究会今後の予定

5 月 19 日（木） 機械振興会館　テーマ：一般

【問合先】

水木敬明（東北大）
E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）

☆WBS 研究会今後の予定 〔 〕内発表申込締切日

5 月 19 日（木），20 日（金） 名工大〔3 月 11 日（金）〕テーマ：符号化，変復調・信号処理技術及び一般

【発表申込先】 下記研究会発表申込システムからお申込み下さい．
http://www.ieice.org/jpn/ken/kenmoushikomi.html

【問合先】

佐藤正知（東京都市大）
TEL〔03〕5707-0104（ext. 2968），FAX〔03〕5707-2180
E-mail：tsato@tcu.ac.jp