**★情報理論研究会（IT）**

専門委員長　大橋正良　副委員長　村松　純
幹事　吉田隆弘・八木秀樹　幹事補佐　葛岡成晃

**★情報セキュリティ研究会（ISEC）**

専門委員長　小川一人　副委員長　藤岡　淳・盛合志帆
幹事　水木敬明・大東俊博　幹事補佐　江村恵太・駒野雄一・須賀祐治

**★ワイドバンドシステム研究会（WBS）**

専門委員長　前原文明　副委員長　浜村昌則・小野文枝
幹事　能田康義・小澤佑介　幹事補佐　中村　聡・中村僚兵

日時　3月8日（木）　9：00～17：50
　　9日（金）　9：00～17：00
会場　東京理科大学葛飾キャンパス講義棟（葛飾区新宿 6-3-1．JR 常磐線；金町駅，または京成金町線；京成金町駅，徒歩 8 分．https://www.tus.ac.jp/info/access/katcamp.html　中村　聡）
議題　IT・ISEC・WBS 合同研究会

8 日午前　IT1（605 教室）（9：00～10：40）

1. 真のパラメトリックモデルが未知のベイズ予測分布の misspecified な場合の性能解析
　○河野浩和・齋藤翔太・松嶋敏泰（早大）
2. ボルツマンマシンにおけるクラスター型模型への近似に関する情報幾何学的考察
　○豊田健太・小川朋宏（電通大）
3. 事前分布の推定に基づく無歪情報源符号の冗長度解析―エルゴード性に関する仮定の緩和―
　○五十嵐椋介・川端　勉（電通大）
4. 情報源近似と漸近十分統計量を用いた強ユニバーサル FV 符号の最悪冗長度の評価
　○有村光晴（湘南工科大）・長岡浩司（電通大）

IT2（605 教室）（10：50～12：05）

5. 局所訂正可能符号を用いた秘密分散法のアクセス構造　○中田昌伸・植松友彦・松田哲直（東工大）
6. 可算無限の参加者に対する小さなしきい値の秘密分散法の構成法　○久留嵩史・古賀弘樹（筑波大）
7. 組合せデザインを用いた（3,n）及び（4,n）型視覚暗号の構成と性能評価
　○岡田昂太郎・古賀弘樹（筑波大）

8 日午後　IT3（605 教室）（13：00～14：40）

8. 情報とエネルギーの同時伝送を行う 2 ユーザ MIMO 干渉通信路におけるアウテージ容量
　○池端健吾・植松友彦（東工大）・松本隆太郎（名大）・松田哲直（東工大）
9. AIFV-$m$ 符号の反復構成法における最適性　○藤田龍星・岩田賢一（福井大）・山本博資（東大）
10. 線形計画法を用いた最適な符号化キャッシュ方式　○神谷捷太・古賀弘樹（筑波大）
11. 符号化スロット化 ALOHA に対する時間シフトの適用　○江本智和・野崎隆之（山口大）

招待講演（605 教室）（15：00～17：50）

12.〔招待講演〕 追跡可能暗号とその周辺の話題に関して　山田翔太（産総研）
13.〔招待講演〕 次世代地上放送に向けた伝送技術の研究開発　竹内知明（NHK）
14.〔招待講演〕 多値論理多項式に対する離散フーリエ変換の応用と積の高速化　松井　一（豊田工大）

8 日午前　ISEC1（606 教室）（9：00～10：40）

15. Minalpher における攪拌要素が安全性に与える影響
　○岸　優樹・長船啓太・桑野裕太・佐々木太良・藤岡　淳（神奈川大）
16. XOR ベースの一般的な階層に適用可能な階層的秘密分散法の研究
　○島　幸司・土井　洋（情報セキュリティ大）
17. 簡潔 Oblivious RAM　○小野寺　拓・渋谷哲朗（東大）
18. 楕円曲線暗号におけるスカラー倍算の効率化の検証　○竹内　昇・木下俊之（東京工科大）

ISEC2（606 教室）（10：50～12：05）

19. 深層学習分類を用いる電子透かし　坂井麻守・○繁田大輝・森田　光（神奈川大）
20. 不正侵入パケットの検知における深層学習手法の評価　○上野智輝・原山美智子（岐阜大）
21. 機械学習を用いた Twitter ユーザー間のリプライ解析―リア友の推定―
　○高桑蘭佳・佐々木太良・藤岡　淳（神奈川大）

8 日午後　ISEC3（606 教室）（13：00～14：40）

22. On the number of rounds of card-based cryptographic protocols using private operations
Hibiki Ono・○Yoshifumi Manabe（Kogakuin Univ.）
23. 背面処理を用いたカードベース暗号における不正を考慮したプロトコル
○清水庸平・岸　優樹・佐々木太良・藤岡　淳（神奈川大）
24. Refining Provable Security with Quantum Random Oracle Model for Signatures from Fiat-Shamir Transform
Bagus Santoso（UEC）
25. Hash Encodings : for Lightweight Code-based Signatures
○Taiyo Yamaguchi・Bagus Santoso・Tomoyuki Ohkubo（UEC）

**9 日午前　IT4（605 教室）（9：00〜10：40）**

1. Polar 符号を用いた segmented deletion 誤り訂正の検討　○惟村　光・金子晴彦（東工大）
2. スパース重ね合わせ符号のための Bayes 最適 AMP 復号器
○波多江優和（九大）・三村和史（広島市大）・川喜田雅則・竹内純一（九大）
3. 信頼度を考慮した RS 符号の性能評価―GMD 復号法との関係―　○古屋杏志郎・山口和彦（電通大）
4. LDPC 符号のループ数に着目した順序制御に基づく Shuffle-BP 復号法　○酒井龍馬・山口和彦（電通大）

**IT5（605 教室）（10：50〜12：30）**

5. シフト演算を利用した噴水符号に対するスケジューリングを用いた逐次的反復復号法の効率化
○村山佳大・野崎隆之（山口大）
6. バースト削除が訂正可能な多元符号の構成　○佐伯豊彦・野崎隆之（山口大）
7. 双方向リレー通信路における LDPC 符号の漸近性能解析
○石松佑太・高邉賢史・和田山　正（名工大）・林　正人（名大）
8. WBAN に適した誤り訂正符号の考察　○山田大開・森田啓義・眞田亜紀子（電通大）

**9 日午後　IT6（605 教室）（13：30〜15：10）**

9. On the generalization of Fano's inequality for countably infinite alphabets, list-decoding, and general conditional information measures　Yuta Sakai（Univ. of Fukui）
10. Parameter orthogonalization method in quantum parameter estimation problem　Jun Suzuki（UEC）
11. ソーティングを用いた部分列数え上げ符号化法　○太田隆博（長野県工科短大）・眞田亜紀子（電通大）
12. K-best ビタビ復号アルゴリズムの誤り性能解析　吉川英機（東北学院大）

**IT7 & ISEC6（605 教室）（15：20〜17：00）**

13. 楕円ペアリング暗号のための 3 次拡大体における演算の効率化に関する考察
○リ キン・小寺雄太・上竹嘉紀・日下卓也・野上保之（岡山大）
14. 自動運転用の量子及び古典レーダーカメラと霧の効果-2―スパースモデリング―　廣田　修（玉川大）
15. 線形変換を用いた積和暗号　○村上恭通（阪電通大）・笠原正雄（早大）
16. 幾つかの多次多変数公開鍵暗号に対する攻撃法について　○境　隆一（阪電通大）・笠原正雄（早大）

**9 日午前　ISEC4（606 教室）（9：00〜10：40）**

17. ID ベース暗号における匿名性定義の関係―ID-CCA2 の場合―
○大友萌夢・佐々木太良・藤岡　淳（神奈川大）
18. 鍵更新機能付き検索可能暗号における再暗号化確認機能について
○迫田有香・大友萌夢・松永直樹・佐々木太良・藤岡　淳（神奈川大）
19. Plausible Deniability の妥当性について　○早稲田篤志・野島　良（NICT）
20. 非一様ランダム鍵を用いた情報理論的に安全な調停者付き認証符号について
○石川美穂・四方順司（横浜国大）

**ISEC5（606 教室）（10：50〜12：30）**

21. 盗聴通信路符号化におけるコセット符号化の安全性評価方法について　○森　雄喜・小川朋宏（電通大）
22. Cooperative Jamming を用いた主通信路に雑音のある Wiretap Channel II における暗号通信について
○飯塚寛貴・田中亮大・四方順司（横浜国大）
23. 分割データ通信における雑音通信路を用いた Keyless Aggregate Authentication について
○田中亮大・四方順司（横浜国大）
24. 物理層におけるメッセージ認証方式の構成法における一考察　○新村知香・四方順司（横浜国大）

**9 日午後　WBS1（606 教室）（13：30〜15：10）**

25. 送受信アレイアンテナを用いて時間空間同時処理によりパスに整合する MC-CDM 広帯域無線変調方式―高性能な誤り制御符号化も視野に―　○伊藤紘二・中村　聡・伊丹　誠（東京理科大）
26. 多値拡散符号による雑音強調抑圧における伝搬路推定誤差の影響　○元木達也・小林岳彦（東京電機大）
27. 無人航空機を用いたユーザ位置検出手法の測位精度指標に基づく特性比較　○石川博康・大貫紘季（日大）
28. 2.4 GHz 帯及び 5.7 GHz 帯を利用する無人移動体画像伝送システムのための電波伝搬特性の測定

○小野文枝・加川敏規・単　麟・三浦　龍・児島史秀（NICT）

WBS2（606 教室）（15：20～17：00）

29. 全二重フィルタ転送における適応自己干渉抑圧について　○手代森勇人・宮嶋照行・杉谷栄規（茨城大）

30. CSK-MPPM を用いる光無線路車間通信における路車間距離による同期誤差特性
○石川真行・羽渕裕真・小澤佑介（茨城大）

31. 光無線フレーム化 DOOK システムの同期性能を考慮した BER 特性の検討
○浅野裕太・羽渕裕真・小澤佑介（茨城大）

32. フェージング通信路における変形擬直交 M 系列対を用いる ROD-WSN の誤り率特性
○大川智広・羽渕裕真（茨城大）・橋浦康一郎（秋田県立大）

◆IEEE IT Society Japan Chapter 共催

☆IT 研究会

**【問合先】** IT 研究会幹事
E-mail：it-sec@mail.ieice.org（幹事，幹事補佐）

☆ISEC 研究会今後の予定 〔　〕内発表申込締切日
5 月 16 日（水） 東工大大岡山キャンパス〔未定〕テーマ：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】**
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

**【問合先】**
能田康義（三菱電機）
TEL〔0467〕41-2850
E-mail：ynouda@m.ieice.org