★情報理論研究会（IT）

専門委員長　村松　純　副委員長　和田山　正
幹事　廣友雅徳・太田隆博　幹事補佐　八木秀樹

★情報セキュリティ研究会（ISEC）

専門委員長　盛合志帆　副委員長　廣瀬勝一・伊豆哲也
幹事　江村恵太・面　和成　幹事補佐　山本　大・須賀祐治

★ワイドバンドシステム研究会（WBS）

専門委員長　岡田　実　副委員長　大内浩司・滝沢賢一
幹事　中村　聡・荒井伸太郎　幹事補佐　Duong Quang Thang・森山雅文

日時　3月10日（火）　11：30～18：00
　　11日（水）　9：30～12：35

会場　兵庫県立大学神戸情報科学キャンパス（神戸ポートアイランド）719・720（神戸市中央区港島南町7-1-28　計算科学センタービル内．ポートライナー：京コンピュータ前駅下車，徒歩約2分．五十部孝典）

議題

10日午前　ISEC1（720）（11：30～12：20）

1. ブロックチェーン技術はSDGsに貢献するか？　○今村光良（筑波大）・面　和成（筑波大／NICT）
2. 暗号通貨Moneroへの Kleptographic 攻撃に関する考察　○南　翔・西出隆志（筑波大）

10日午後　ISEC2（720）（13：20～14：35）

3. NIZapを用いてゼロ知識証明方式に委任機能を付加する方法　○白取直也・多田　充（千葉大）
4. トラップドアを用いない格子 Aggregate 署名方式　○大井洸慈・多田　充（千葉大）
5. A Study of Randomized Authentication in Opportunistic Networks
　○Kai Wang・Kazuya Sakai（Tokyo Metropolitan Univ.）

ISEC3（720）（14：45～16：00）

6. Security of K（+）MVPKC Based on Message-Dependent Transformation—Along With Proposal of K（++）CBPKC—　Masao Kasahara（Waseda Univ.）
7. Division Step改良による逆元計算の効率化　○池田暢哉・宮地充子（阪大）
8. 署名順序を用いた閾値署名の提案　○猪本卓也・宮地充子（阪大）

招待講演1（720）（16：10～17：00）

9.〔招待講演〕 パス遮蔽数モデルの開発と5Gスモールセル内の伝送容量推定　多賀登喜雄（関西学院大）

招待講演2（720）（17：10～18：00）

10.〔招待講演〕 私見：情報理論からサイバーセキュリティへ　森井昌克（神戸大）

10日午前　IT1（719）（11：30～12：20）

11. コスト付き符号化を用いたステガノグラフィの実画像における有効性　○中澤　遼・渡辺　峻（東京農工大）
12. Weighted-BPにおける重み学習効果向上のための訓練データフィルタリング手法に関する検討
　○吉沢竜太・古田憲一郎・吉永悠真・鳥井　修・児玉知也（キオクシア）

10日午後　ISEC & IT（719）（13：00～14：15）

13.（2,3）しきい値拡張視覚復号型秘密分散法のQRコードへの適用　○大川直也・栃窪孝也（日大）
14. 出現文字を用いた機械学習によるDNSトンネル検出の研究—評価プログラムの実装に係る考察—
　○朝倉哲也・辰己丈夫（放送大）
15. 情報公開問題における統計的決定理論に基づくプライバシ保護評価
　○宮下有咲・鎌塚　明（早大）・吉田隆弘（横浜商科大）・松嶋敏泰（早大）

IT2（719）（14：25～15：40）

16. 最大ラン長が制限された単一挿入／削除訂正符号の符号化法　○武元玲央南・野崎隆之（山口大）
17. 定重み符号を利用した系列部分集合符号の構成と効率的な復号法　○江本智和・野崎隆之（山口大）
18. 2名の不正者をともに特定できる電子指紋符号の符号化定理　古賀弘樹（筑波大）

11日午前　ISEC4（720）（9：30～11：10）

1. KCipher-2に対する差分攻撃への耐性評価
　○寶木　仁・阪本光星（兵庫県立大）・峯松一彦（NEC）・五十部孝典（兵庫県立大／NICT）
2. アニーリング計算を用いたAESの差分特性探索
　○平野　遥・垣本修吾・米山一樹（茨城大）・山口純平（富士通研）
3. Ideal Cipherの繰り返し構造で構成される暗号学的置換の安全性証明　○中道良太・岩田　哲（名大）

4. A Remark on Improving Aggregate Message Authentication Codes with Detecting Functionality
〇Lu Cao・Shingo Sato・Junji Shikata（Yokohama National Univ.）

ISEC5（720）（11：20～12：35）

5. モバイルアプリケーションにおけるファイルヘッダー情報に着目した不正プログラムの検知
〇草間好輝・武田圭史・小林和真・中村　修（慶大）・李　明宰（LINE）
6. 直並列グラフで表現される順序構造に適用できる Aggregate MAC 方式　〇石井悠太・多田　充（千葉大）
7. 暗号文をノードに付与する ZDD の Garbled Circuit　〇増井孝之・森田　光（神奈川大）

WBS（719）（9：30～11：10）

8. 超広帯域レーダによる各種ドローンの識別に関する基礎検討　〇水嶋　巧・中村僚兵・葉玉寿弥（防衛大）
9. 拡張プライム系列符号と陪直交符号を組み合わせた光 CDMA 方式
〇小野恭平・山嵜彰一郎・松嶋智子（職能開発大）
10. A note on orthogonal variable spreading factor codes based on polyphase sequences
〇Tomoko K. Matsushima・Shoichiro Yamasaki（Polytechnic Univ.）
11. 屋内長距離高速イメージング MIMO システムの実験的性能評価
〇岩佐章史・小林健太郎・岡田　啓・片山正昭（名大）

IT3（719）（11：20～12：35）

12. On the existence of bonds for constrained systems
〇Akiko Manada（Shonan Inst. of Tech.）・Takahiro Ota（Nagano Pref. Inst. of Tech.）
13. *T*-Private Information Retrieval に対応する Smooth Locally Decodable Codes に関する一考察
〇風間皐希・鎌塚　明・松嶋敏泰（早大）
14. HQC 暗号を応用した秘匿内積計算プロトコル
〇廣友雅徳・中山太雅（佐賀大）・福田洋治（近畿大）・毛利公美（岐阜大）・白石善明（神戸大）

◆IEEE IT Society Japan Chapter 共催
☆IT 研究会
【問合先】
情報理論研究会幹事，幹事補佐
E-mail：it-sec@mail.ieice.org
☆ISEC 研究会
【問合先】
面　和成（筑波大）
E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）
☆WBS 研究会
【問合先】
中村　聡（神奈川大）
E-mail：akira-nakamura@kanagawa-u.ac.jp