★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　太田隆博・八木秀樹　幹事補佐　吉田隆弘

★情報セキュリティ研究会（ISEC）
専門委員長　藤岡　淳　副委員長　盛合志帆・廣瀬勝一
幹事　大東俊博・江村恵太　幹事補佐　面　和成・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　小澤佑介・中村　聡　幹事補佐　中村僚兵・Duong Quang Thang

◎IT 研究会と ISEC 研究会は参加費が必要になります.
ESS の技報電子化研究会に関する御案内ページ
https://www.ieice.org/ess/ESS/gihou-trial-ess2018.html

日時　3 月 7 日（木）　9：30～17：45
8 日（金）　9：00～17：35
会場　電気通信大学（調布市調布ヶ丘 1-5-1. 京王線：調布駅から徒歩 15 分. https://www.uec.ac.jp/about/profile/access　TEL〔042〕443-5366　八木秀樹）
議題
7 日午前　ISEC1（301 室）（9：30～10：45）
1. 背面カメラを用いた後方からの覗き見対策パスワード　○牛谷内翔太・宇田隆哉（東京工科大）
2. Tor クローラを用いたダークウェブにおける悪性 URL の探索　○川口雄己・小澤誠一（神戸大）
3. Coherence-based Spoken Machine Translation Recognition : Towards an Efficient Gateway to Detect Untrusted Information
○Nguyen Son Hoang Quoc・Tran Phuong Thao・Seira Hidano・Shinsaku Kiyomoto（KDDI Research）

ISEC2（301 室）（10：55～12：35）
4. BLS 曲線上での高速化手法を用いたペアリング暗号ライブラリ ELiPS の実装と評価
○高橋裕人・金成忠樹・南條由紀・カンダカル エムディ アルアミン・日下卓也・野上保之（岡山大）
5. 2 の冪乗位数をもつ Edwards 曲線の性質に関する考察　○三浦裕正・小林航也・日下卓也・野上保之（岡山大）
6. An New Family of Isomorphism of Polynomials　Bagus Santoso（UEC）
7. 任意の環におけるイデアル格子問題に基づいた本人確認方式　○竹牟禮　薫・バグス サントソ（電通大）

7 日午後　ISEC3（301 室）（13：40～14：55）
8. 深層学習を使うテキストデータのステガノグラフィ　○増井孝之・繁田大輝・森田　光（神奈川大）
9. 深層学習による画像のステガノグラフィ　○繁田大輝・森田　光（神奈川大）
10. エコー拡散法とオクターブ類似性を用いた会議録用音声データの改ざん検知の実装に関する研究
○大垣翔矢（北九州市大）・荒木俊輔（九工大）・宮崎　武・上原　聡（北九州市大）・野上保之（岡山大）

ISEC4（301 室）（15：05～16：45）
11. 出力局所性を持つコミットメント方式　○宮地秀至・河内亮周・宮地充子（阪大）
12. ストリーム暗号 Salsa, ChaCha の Diffusion 解析を用いた Round 関数の再設計　○松岡勇介・宮地充子（阪大）
13. マイコン実装した AES 暗号に対するニューラルネットワークを用いた最終ラウンド鍵の解析
○小杉聡志・城市　翔・生田　健・日下卓也・野上保之・高橋規一（岡山大）
14. TBA　○勝野凌介・米山一樹（茨城大）

招待講演 1（301 教室）（16：55～17：45）
15.〔招待講演〕 深層学習技術の進化と深化　庄野　逸（電通大）

7 日午前　IT1（306 室）（9：30～10：45）
16. マルコフ情報源に対する有限窓 zero 冗長度推定量の性能解析―アルファベットが状態毎に未知である場合―
○橋元雄祐・川端　勉（電通大）
17. 多端子仮説検定問題について　大濱靖匡（電通大）
18. f-ダイバージェンスを誤差尺度とした 2 次情報源 Resolvability レート　野村　亮（専修大）

IT2（306 室）（10：55～12：35）
19. 分割木で今後使われない節点を候補から外して符号化する二段階 LZY 符号　有村光晴（湘南工科大）
20. スライド窓を用いた接尾辞配列の動的構築

○深江裕忠（職業大）・太田隆博（長野県工科短大）・森田啓義（電通大）・眞田亜紀子（湘南工科大）
21. エントロピー符号化法 ANS のための確率近似法の多元情報源での評価
○井上レオナルド・横尾英俊（群馬大）
22. A New Variation of Asymmetric Numeral Systems　○Qi Xin・Hidetoshi Yokoo（Gunma Univ.）

7 日午後　WBS1（306 室）（13：40〜14：55）

23.〔奨励講演〕 無線 LAN を用いた干渉測位における位置推定誤差に関する一検討
○武者大樹・藤井雅弘（宇都宮大）
24.〔奨励講演〕 光無線通信ターボ符号システムにおける信号伝送形式の一検討
○孫　冉・羽渕裕真・小澤佑介（茨城大）
25. 拡張プライム系列符号を用いた可視光通信のための調光制御方式に関する一検討
○河本　椋・土居勇人・上村健夢・宮崎真一郎・大村光徳・松嶋智子・山嵜彰一郎（職業大）

IT3（306 室）（15：05〜16：20）

26. 畳込み符号のビタビ復号に伴う Innovations，σ-集合体，Martingales　田島正登
27. 符号化キャッシングとリクエスト数の分布に基づく部分空間　栗原正純（電通大）
28. 信頼度を考慮した q 入力 q ＊R 出力対称通信路における実用的短縮 RS 符号の性能評価
○白川恵嗣・古屋杏志郎・山口和彦（電通大）

8 日午前　ISEC5（301 室）（9：00〜10：40）

1. 疑似乱置換を用いない履歴非依存型順序付きアグリゲート認証方式
○廣瀬勝一（福井大／ジャパンデータコム）・四方順司（横浜国大）
2. サイドチャネル攻撃への耐性を有する認証暗号方式について
○廣瀬勝一（福井大）・菅原　健（電通大）・駒野雄一（東芝）
3. スマートコントラクトを用いたオンラインパチンコの安全性向上に関する提案
○山口功太郎・許　伯駒・宮地秀至・宮地充子・鄭　振牟（阪大）
4. 準巡回符号に基づく二者間秘匿大小比較プロトコル　○祁　儀穎・河内亮周・宮地充子（阪大）

ISEC6（301 室）（10：50〜12：30）

5. CAN 通信プロトコルに対するメッセージ認証機能の実装と計算遅延時間についての検討
○小椋央都・一色竜之介・日下卓也・野上保之・亀川哲志（岡山大）・前山祥一（香川大）・荒木俊輔（九工大）
6. Git とブロックチェーンを用いる文書管理方法　○池田大地・繁田大輝・森田　光（神奈川大）
7. 暗号資産における不正流出後の動向分析　○今村光良・佐藤哲平・面　和成（筑波大）
8. 国内外の仮想通貨取引所の実態調査（２）　○藤谷知季・面　和成（筑波大）

8 日午後　ISEC7（301 室）（13：30〜15：10）

9. ワンタイムプログラムとそのシュノア署名への応用　西出隆志（筑波大）
10. 複数鍵完全準同型暗号を用いた非対話型大小比較プロトコル　○樋口裕二・西出隆志（筑波大）
11. ノンスペースのハイブリッド暗号　○三島貴務・西出隆志（筑波大）
12. 初期文字列が 29 文字の 4 入力多数決 Privete PEZ プロトコル
○安部芳紀・山本翔太・岩本　貢・太田和夫（電通大）

ISEC8（301 室）（15：20〜16：35）

13. 数論変換におけるサイドチャネル情報を用いた Ring-LWE 暗号方式の秘密鍵復元攻撃
○大西健斗・國廣　昇（東大）
14. 検証可能委譲秘匿ビット比較演算　○白井直輝・米山一樹（茨城大）
15. 群依存バンドル言語に対する非対話証明システム　穴田啓晃（長崎県立大）

招待講演 2（301 教室）（16：45〜17：35）

16.〔招待講演〕 現代暗号研究の事始め―1 つのケーススタディ―　太田和夫（電通大）

8 日午前　IT4（306 室）（9：25〜10：40）

17. Equivalence theorem and comparison of optimal designs in qubit systems　Jun Suzuki（UEC）
18. 観測ノイズと大きなコヒーレンスがある線形観測による L1 正則化回帰の性能評価
○井原みのり・岩田一貴・三村和史（広島市大）
19. 深層学習によるスパース重ね合わせ符号復号器の改良
○飯田昌澄・押川祐也（九大）・三村和史（広島市大）・竹内純一（九大）

IT & ISEC（306 室）（10：50〜12：30）

20. 二元対称消失盗聴通信路における条件付情報漏洩量の分布　道脇右京・○實松　豊（九大）・大濱靖匡（電通大）
21. 混合型の攻撃に対する電子指紋符号の容量の評価　○關根達矢・古賀弘樹（筑波大）
22. 参加者が多いいくつかのアクセス構造に対する秘密分散法の最悪情報比　○久留嵩史・古賀弘樹（筑波大）
23. Evolving Secret Sharing on Multi-level Access Structure

○Partha Sarathi Roy（KDDI Research）・Sabyasachi Dutta（Kyushu Univ.）・Kazuhide Fukushima・Shinsaku Kiyomoto（KDDI Research）・Kouichi Sakurai（Kyushu Univ.）

8 日午後　WBS2（306 室）（13：30〜15：10）

24. 秘密分散と周波数ホッピングにより情報保護を強化した無線通信方式
○小野恭平・山嵜彰一郎・松嶋智子・宮崎真一郎・大村光徳（職業大）

25. 自己エネルギー再利用を行うフィルタ転送型リレーの性能評価　○古川純汰・宮嶋照行・杉谷栄規（茨城大）

26. OFDM と DFT-precoding を併用した秘匿通信に関する一検討　○山口良平・落合秀樹・四方順司（横浜国大）

27. チャネル推定を考慮したプリコーデッド OFDM 伝送の繰り返し復調器の特性評価　佐藤正知（広島商船高専）

IT5（306 室）（15：20〜16：35）

28. 多元 Shifted VT 符号の組織符号化　○佐伯豊彦・野崎隆之（山口大）

29. シフト演算を利用した噴水符号のシフト分布の詳細化　○立田維吹・野崎隆之（山口大）

30. LDPC 符号の Shuffle-BP 復号法における復号順序決定法に関する考察―ループや重みを考慮した復号順序決定―
○酒井龍馬・松尾有紗・山口和彦（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

【問合先】

面　和成（筑波大）

E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）

☆WBS 研究会今後の予定　〔　〕内発表申込締切日

5 月 15 日（水），16 日（木）　名城大天白キャンパス〔3 月 11 日（月）〕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】

Yusuke Kozawa（Ibaraki Univ.）

E-mail：kozawa@ieee.org