★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

日時　5月19日（木）　9：35～17：30

会場　機械振興会館地下2階1号室（港区芝公園3-5-8．東京メトロ日比谷線：神谷町駅下車徒歩10分，JR：浜松町駅下車徒歩20分，都営地下鉄三田線：御成門駅・大江戸線：赤羽橋駅下車徒歩10分．http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm　TEL〔03〕3434-8211）

議題

1. Non-overlapping template matching testを用いたテンプレートの同定法の改善案
　○竹田裕一（神奈川工科大）・藤井光昭・鎌倉稔成・渡邉則生（中大）
2. 窓関数を適用した離散フーリエ変換による不正侵入検知システム
　○柘植裕介・岩井啓輔・田中秀磨・黒川恭一（防衛大）
3. プライバシを考慮した多機関データベースの属性別要素数の導出方式
　宮地充子（阪大／北陸先端大／CREST）・○吉田貴俊（北陸先端大）

招待講演：ASIACRYPT 2015 特集（1）

4.〔招待講演〕 いくつかの述語暗号間の変換と属性ベース暗号への応用
　アッタラパドゥン ナッタポン・花岡悟一郎・○山田翔太（産総研）
5.〔招待講演〕 Somewhere Statistically Binding HashingとPositional Accumulatorsの新しい構成について
　岡本龍明（NTT）

午後

6. 多素数・多変数公開鍵暗号方式（Multi Prime Numbers MPKC）の構成法とその組織通信への応用―耐量子コンピュータとIoT環境を考慮して―　○辻井重男・藤田　亮・五太子政史（中大）
7. 円分体に対するイデアル格子上の短い生成元の復元可能性について　○奥村伸也・安田雅哉・高木　剛（九大）
8. Analysis of Decreasing Squared-Sum of Gram-Schmidt Lengths for Finding Short Lattice Vectors
　○Masaya Yasuda（Kyushu Univ.）・Kazuhiro Yokoyama（Rikkyo Univ.）
9.「計測セキュリティ」の研究課題　松本　勉（横浜国大）
10. あるパルスLIDARシステムの反射光偽装に対する計測セキュリティ
　○相馬一樹・藤本大介・松本　勉（横浜国大）
11. 中間文を起点とすることによる積分攻撃の改良
　○大宮翔児・徳重佑樹・野島拓也・岩本　貢・太田和夫（電通大）

招待講演：ASIACRYPT 2015 特集（2）

12.〔招待講演〕 Midori : A Block Cipher for Low Energy
　Subhadeep Banik・Andrey Bogdanov（DTU）・○Takanori Isobe・Kyoji Shibutani・Harunaga Hiwatari・Toru Akishita（Sony）・Francesco Regazzoni（USI）
13.〔招待講演〕 How Secure is AES Under Leakage　Andrey Bogdanov（DTU）・○Takanori Isobe（Sony）
14.〔招待講演〕 Refinements of the k-tree Algorithm for the Generalized Birthday Problem　佐々木　悠（NTT）

【問合先】

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