★情報セキュリティ研究会（ISEC）

専門委員長　満保雅浩　副委員長　小川一人・藤岡　淳
幹事　駒野雄一・水木敬明　幹事補佐　大東俊博・須賀祐治・猪俣敦夫

日時　5月12日（金）　10：00～17：30

会場　機械振興会館地下3階研修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. 検索可能暗号の鍵更新の一提案―ID ベース鍵隔離暗号の適用について―
　〇松崎なつめ・穴田啓晃（長崎県立大）
2. Fully Secure な紛失キーワード検索　　黒澤　馨・〇根本雄輝（茨城大）
3. コミットメントのコピーに必要なカード枚数について
　〇宮原大輝（東北大）・林　優一（東北学院大）・水木敬明・曽根秀昭（東北大）
4. 〔招待講演〕 サイズ秘匿多者間秘密計算
　〇品川和雅（産総研）・縫田光司（産総研／さきがけ）・西出隆志（筑波大）・花岡悟一郎（産総研）・岡本栄司（筑波大）
5. 〔招待講演〕 How to circumvent the two-ciphertext lower bound for linear gabling schemes（ASIACRYPT 2016 より）　　菊池　亮（NTT）

午後（14：00～）

6. ネットワークセキュリティイベントの分析における事例と手法の検討　　水谷正慶（IBM）
7. IoT 機器群とクラウドからなるサービスに対するイベント収集・ルール適用処理基盤の提案とセキュリティインシデント検出への応用　　〇三品拓也・佐藤直人・佐藤史子（日本 IBM）
8. サンドボックス解析回避への耐性を高めるツール SandVeil の提案
　八幡篤司・〇石井　攻・横山日明・田辺瑠偉・吉岡克成・松本　勉（横浜国大）
9. 公開検証可能なプライバシー保護時系列データ統計計算　　江村恵太（NICT）
10. 〔招待講演〕 Public-Key Cryptosystems Resilient to Continuous Tampering and Leakage of Arbitrary Functions
　草川恵太（NTT）
11. 〔招待講演〕 Partitioning via Non-Linear Polynomial Functions：More Compact IBEs from Ideal Lattices and Bilinear Maps　　〇Shuichi Katsumata（Univ. of Tokyo）・Shota Yamada（AIST）
12. 〔招待講演〕 How to Obtain Fully Structure-Preserving（Automorphic）Signatures from Structure-Preserving Ones
　〇Yuyu Wang（TITech/AIST）・Zongyang Zhang（Beihang Univ.）・Takahiro Matsuda・Goichiro Hanaoka（AIST）・Keisuke Tanaka（TITech）

☆ISEC 研究会今後の予定　〔　〕内発表申込締切日
7月14日（金），15日（土）　内田洋行東京本社ショールーム〔未定〕テーマ：セキュリティ，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）