## ★情報セキュリティ研究会（ISEC）

専門委員長　櫻井幸一　副委員長　角尾幸保・満保雅浩
幹事　岩田　哲・花岡悟一郎　幹事補佐　伊豆哲也・川本淳平・駒野雄一・島　成佳・水木敬明

**日時**　12月19日（金）　14：00～16：55

**会場**　機械振興会館地下3階研修2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. 組織暗号の1クラスK(II)SOPKCの提案　　笠原正雄（早大／中大）
2. Non-overlapping template matching testを用いたテンプレートの同定
   ○竹田裕一（神奈工科大）・藤井光昭・鎌倉稔成・渡邉則生（中大）
3. Space-Time Encoding Schemeに適した識別符号　　○白石良介・佐藤　敬・下泉政樹（北九州市大）
4. 国際会議CRYPTO2014報告　　大久保美也子（NICT）
5. 〔招待講演〕 Self-bilinear Map on Unknown Order Groups from Indistinguishability Obfuscation and Its Applications
   ○Takashi Yamakawa（Univ. of Tokyo）・Shota Yamada・Goichiro Hanaoka（AIST）・Noboru Kunihiro（Univ. of Tokyo）
6. 〔招待講演〕 Round-Efficient Black-Box Construction of Composable Multi-Party Computation
   Susumu Kiyoshima（NTT）

☆ISEC研究会今後の予定　〔　〕内発表申込締切日
3月2日（月），3日（火）　北九州市大ひびきのキャンパス〔未定〕テーマ：IT・ISEC・WBS合同研究会

**【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】**
岩田　哲（名大）
TEL〔052〕789-5722，FAX〔052〕789-5723
E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）