★情報セキュリティ研究会（ISEC）

専門委員長　廣瀬勝一　副委員長　伊豆哲也・國廣　昇
幹事　面　和成・山本　大　幹事補佐　米山一樹

日時　5月19日（水）　10：00～16：00
会場　オンライン開催
議題　一般
（10：00～10：50）

1. Card-based Cryptographic Protocols with a Standard Deck of Cards Using Private Operations
　　○Yoshifumi Manabe・Hibiki Ono（Kogakuin Univ.）
2. ブロックチェーンを用いた医療情報共有システムの提案に向けて　　○上野隆治・面　和成（筑波大）

招待講演：国際会議特集（11：05～12：05）

3.〔招待講演〕 Six-Card Finite-Runtime XOR Protocol with Only Random Cut（from APKC 2020）
　　○豊田航大（東北大）・宮原大輝（東北大／産総研）・水木敬明・曽根秀昭（東北大）
4.〔招待講演〕 Efficient blockchain-based IoT firmware update considering distribution incentives（from IDC 2021）
　　○福田竜央（筑波大）・面　和成（筑波大／NICT）

午後（13：00～14：15）

5. 検索可能暗号を用いた暗号化ストレージ・チャットシステムの実装評価
　　○江村恵太・金森祥子・野島　良（NICT）・渡邉洋平（電通大／NICT）
6. Ring-LWE 問題で使用可能な定義体の高速乗算手法
　　○大久保佑弥・奥村伸也（阪大）・宮地充子（阪大／北陸先端大）
7. Romulus-N 及び Rolumus-M に対する識別攻撃及び汎用的偽造攻撃
　　○土生　亮（名大）・峯松一彦（NEC）・岩田　哲（名大）

招待講演：国際会議特集（14：30～16：00）

8.〔招待講演〕 Security Definitions on Time-Lock Puzzles（from ICISC 2020）
　　○Daiki Hiraga（Tokyo Inst. of Tech.）・Keisuke Hara（Tokyo Inst. of Tech./AIST）・Masayuki Tezuka・Yusuke Yoshida・Keisuke Tanaka（Tokyo Inst. of Tech.）
9.〔招待講演〕 Efficiency and Accuracy Improvements of Secure Floating-Point Addition over Secret Sharing（from IWSEC 2020）　　○Kota Sasaki・Koji Nuida（Univ. of Tokyo）
10.〔招待講演〕 Simple Electromagnetic Analysis Against Activation Functions of Deep Neural Networks（from AIHWS 2020）　　○Go Takatoi・Takeshi Sugawara・Kazuo Sakiyama（UEC）・Yuko Hara-Azumi（Tokyo Inst. of Tech.）・Yang Li（UEC）

【問合先】

面　和成（筑波大）
E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐）