★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

★技術と社会・倫理研究会（SITE）

専門委員長　吉開範章　副委員長　岡田仁志・森住哲也
幹事　宮田純子・多川孝央　幹事補佐　芳賀高洋

★情報通信システムセキュリティ研究会（ICSS）

専門委員長　三宅　優　副委員長　西出隆志・白石善明
幹事　植田　武・高倉弘喜　幹事補佐　吉岡克成・神谷和憲

★マルチメディア情報ハイディング・エンリッチメント研究会（EMM）

専門委員長　伊藤彰則　副委員長　鵜木祐史・川村正樹
幹事　市野将嗣・薗田光太郎　幹事補佐　岩田　基・河野和宏

日時　7月2日（木）　10：15～16：35
　　3日（金）　10：15～11：55
会場　名古屋市中小企業振興会館吹上ホール（http://www.nipc.or.jp/fukiage/sub/access.html）
議題　セキュリティ，一般
2日午前　セッション A-1 : ISEC（10：15～11：55）
ISEC-1. Attribute-Based Two-Tier Signatures
　○Hiroaki Anada（ISIT）・Seiko Arita（IISEC）・Kouichi Sakurai（Kyushu Univ.）
ISEC-2. On Anonymous Password-based Authentication Protocol　○SeongHan Shin・Kazukuni Kobara（AIST）
ISEC-3. 疑似乱数生成器 QP-DYN に対する選択初期値攻撃　○荒井研一・五十嵐保隆・金子敏信（東京理科大）
ISEC-4. 共通番号（マイナンバー）制度の民間サービス利用時における個人情報漏洩のリスク評価に関する研究
　○新山剛司・北　寿郎（同志社大）
セッション B-1 : CSEC（10：15～11：55）
5. 格子の最短ベクトル問題において格子基底の質が探索効率に及ぼす効果について
　深瀬道晴（早大／秀明大）・山口和紀（東大）
6. マルウェア対策のための研究用データセット―MWS Datasets 2015―　神薗雅紀（NICT）
7. 残余ネットワークを用いた安全なネットワーク符号化　藤本竜矢・岩村惠市（東京理科大）
8. 除算を含む四則演算に適用可能な秘密分散法を用いた秘匿計算手法の提案　神宮武志・岩村惠市（東京理科大）
2日午後　セッション A-2 : ISEC（13：25～14：40）
ISEC-9. Proposals of K(AI) and K(AII) Schemes for augmenting code-based PKC and product-sum type PKC
　Masao Kasahara（Waseda Univ./Chuo Univ.）
ISEC-10. Security Analysis of AONT-based Regenerating Codes
　○Hidenori Kuwakado（Kansai Univ.）・Masazumi Kurihara（Univ. of Electro-Comm.）
ISEC-11. Tree intersection ORAM　○Karin Sumongkayothin・Atsuko Miyaji・Chunhua Su（JAIST）
セッション B-2 : SITE（13：25～15：05）
SITE-12. 個人情報利活用における包括的同意について　大谷卓史（吉備国際大）
SITE-13. 情報セキュリティ行動サイクルへの対策実行意思モデルの応用に関する考察　吉開範章（日大）
SITE-14. 自動道徳判断概説　村上祐子（東北大）
SITE-15. 著作者人格権の侵害場面を用いた教材の開発とその試行　○鍋島尚子・宮寺庸造・櫨山淳雄（学芸大）
セッション A-3 : EMM（15：20～16：35）
EMM-16. Fuzzy Commitment Scheme に基づくセキュアかつロバストな JPEG 画像の同定
　○飯田健太・塩田さやか・貴家仁志（首都大東京）
EMM-17. 評価用 RAW 動画の撮影と時間軸方向の DCT を用いた動画電子透かしの提案
　○國井夏樹・姜　玄浩・岩村惠市（東京理科大）
EMM-18. カラー難視性パターンによる拡張現実システムへの応用
　○富田若南（東京理科大）・金田北洋（阪府大）・岩村惠市（東京理科大）
セッション B-3 : SPT（15：20～16：35）
19. Social Proof の影響を利用したパスワード強度メーターの提案　大山敬博・金岡　晃（東邦大）
20. 匿名通信システム Tor におけるウルフウェブサイトの提案　中田謙二郎・松浦幹太（東大）

21. QOL を考慮したスマートフォンに関するプリシード・プロシードモデルの応用
向後朋美・井上久美子・阿部　史・角田真二・泉　直子（十文字学園女子大）

3 日午前　セッション A-4 : SITE＋ISEC＋ICSS（10：15〜11：55）

SITE-1. 初中等教育のデジタル著作物利活用を適切に促進する利用許諾契約締結のためのガイドライン
○芳賀高洋（岐阜聖徳大）・鈴木二正（慶應幼稚舎）・小野永貴（千葉大）・大谷卓史（吉備国際大）

ISEC-2. NIST 耐量子暗号ワークショップ参加報告　○安田貴徳（九州先端研）・高木　剛（九大）

ISEC-3. Mutant Groebner Base アルゴリズムの改良　○五太子政史・辻井重男（中大）

ICSS-4. クラウド型の情報システムの間接利用の不安因子について
○福田洋治（愛知教大）・白石善明（神戸大）・廣友雅徳（佐賀大）・毛利公美（岐阜大）

セッション B-4 : CSEC（10：15〜11：55）

5. デルタ ISMS モデルの提案―事故データベースに基づく ISMS の強化―
堀川博史（静岡大）・大谷尚通（NTT データ）・高橋雄志（東京電機大）・加藤岳久（東芝）・間形文彦（NTT）・勅使河原可海・佐々木良一（東京電機大）・西垣正勝（静岡大）

6. プロセス特定困難化のためのプロセス情報の置換手法の評価　佐藤将也・山内利宏・谷口秀夫（岡山大）

7. SHSS：オブジェクトストレージ向けの超高速秘密分散ライブラリ　五十嵐　大・露崎浩太・川原祐人（NTT）

8. マルウェア検体共有の悪用による動的解析環境のフィンガープリント収集と解析回避
横山日明・田辺瑠偉・吉岡克成・松本　勉（横浜国大）

◆情報処理学会；コンピュータセキュリティ研究会／情報セキュリティ心理学とトラスト研究会連催

☆ISEC 研究会今後の予定 〔　〕内発表申込締切日

9 月 4 日（金） 機械振興会館〔未定〕テーマ：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）

☆SITE 研究会

【問合先】

山肩大祐
TEL〔090〕5996-7189
E-mail：yamakata@jamisri.jp

◎公式 Web サイト
http://www.ieice.org/ess/site/

☆ICSS 研究会

【問合先】

三宅　優（KDDI 研）
TEL〔049〕278-7367，FAX〔049〕278-7510
E-mail：icss-request@mail.ieice.org

◎最新情報は，ICSS 研究会ホームページを御覧下さい.
http://www.ieice.org/~icss/index.html

☆EMM 研究会今後の予定 〔　〕内発表申込締切日

9 月 10 日（木），11 日（金） 名大東山キャンパス〔未定〕テーマ：マルチメディア通信／システム，ライフログ活用技術，IP 放送／映像伝送，メディアセキュリティ，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