★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

★技術と社会・倫理研究会（SITE）

専門委員長　岡田仁志　副委員長　森住哲也・小川　賢
幹事　多川孝央・芳賀高洋　幹事補佐　川口嘉奈子

★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　白石善明・植田　武
幹事　高倉弘喜・吉岡克成　幹事補佐　神谷和憲・笠間貴弘

★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　川村正樹・日置尋久
幹事　薗田光太郎・岩田　基　幹事補佐　生源寺　類・藤吉正明

日時　7月14日（木）　13：00～17：30
　　15日（金）　9：30～16：10
会場　中市コミュニティーホール Nac 多目的ホール A・B（山口市中市町 3-13. JR 山口駅から徒歩 15 分程度. http://www.yamaguchi-machinaka.com/mtx/archives/1233079473/1233793907.html　TEL〔083〕933-5701　川村正樹）
議題　セキュリティ，一般

14日　セッション A-1 EMM（13：00～15：05）

EMM-1. 攻撃によって生じる雑音を考慮した電子透かし方式への誤り訂正符号の適用と考察
　○重本章吾・栗林　稔・舩曳信生（岡山大）
EMM-2. ケルクホフスの原理に基づく電子透かし方式の安全性において特徴選出及び信号処理の重要性
　○山下晃一郎・栗林　稔・舩曳信生（岡山大）
EMM-3. クリアインクを用いた難視性パターンからの情報抽出に関する研究
　○松江勇輝（東京理科大）・金田北洋（阪府大）・岩村恵市（東京理科大）
EMM-4. 内壁の構造化による 3D プリンター造形物への情報埋め込み技術
　○中村耕介・鈴木雅洋・高沢渓吾（神奈川工科大）・高嶋洋一（NTT）・鳥井秀幸・上平員丈（神奈川工科大）
EMM-5. ジグソーパズル解法に対するブロックスクランブル画像暗号化法の評価
　○中満達也・栗原健太・貴家仁志（首都大東京）

セッション B-1 SITE（13：00～15：05）

SITE-6. 覗き見耐性を有する背景パターンスライド認証方式の実装と利便性評価
　○田中基偉・稲葉宏幸（京都工繊大）
SITE-7. 検知時刻の関連性に着目した IDS アラートの分類手法に関する考察
　○久野寛明・稲葉宏幸（京都工繊大）
SITE-8. 情報安全教育のシンプルモデルに関する研究―従来の情報モラル教育からの脱却―
　○芳賀高洋（岐阜聖徳大）・五十嵐晶子（内田洋行）・西岡勝郎（ウチダ人材開発）
SITE-9. 電子コミュニケーションを終了するためのルールの探求　　吉永敦征（山口県立大）
SITE-10. アイデンティティとプライバシー―プライバシーの社会的機能の解明に向けて―
　大谷卓史（吉備国際大）

セッション A-2 ICSS（15：25～17：05）

ICSS-11. 電波再帰反射攻撃成立条件の評価と対策
　○星野　遼（早大）・衣川昌宏（仙台高専）・林　優一（東北学院大）・森　達哉（早大）
ICSS-12. 教師なし学習を用いたマルウェア通信の分類
　○畑田充弘（早大／NTT コミュニケーションズ）・森　達哉（早大）
ICSS-13. IoT 時代における制御システムネットワークセキュリティ
　○高山祐磨（MFE）・越島一郎・青山友美（名工大）
ICSS-14. パッキングサービスにより保護されたアプリの静的判別手法を用いた Android マーケットの実態調査
　○中野弘樹・楊　志勇・森　博志・吉岡克成・松本　勉（横浜国大）

セッション B-2 CSEC（1）/SPT（15：25～17：30）

15. 金融業界において注目されている情報セキュリティ上の研究課題について　　○中村啓佑・宇根正志（日本銀行）

16. サイバーセキュリティ脅威対策のためのビジネスリスク評価システムの提案
　○磯部義明・杉本暁彦・仲小路博史（日立）
17. マルウェア対策のための研究用データセット―MWS Datasets 2016―
　○高田雄太（NTT）・寺田真敏（日立）・村上純一（FFRI）・笠間貴弘（NICT）・吉岡克成（横浜国大）・畑田充弘（NTT コミュニケーションズ）
18. アンチウイルスソフトによるマルウェアの検出状況の時系列変化に関する考察　○鬼頭哲郎・寺田真敏（日立）
19. 第一回 IEEE European Symposium on Security and Privacy 参加報告
　○松本晋一（九州先端科学技研）・松浦幹太（東大）

15 日午前　セッション A-3 ISEC（1）（9：30～11：35）

ISEC-1. 拡張ローレンツ方程式を利用した使い捨てパッド型カオス暗号　○長　憲一郎・宮野尚哉（立命館大）
ISEC-2. Vector Stream Cipher の安全性の向上について　○岩崎　淳・梅野　健（京大）
ISEC-3. 改良型 Winternitz one time 署名の提案と安全性証明
　○弥谷圭朗・ジェイソン ポール クルーズ・楫　勇一（奈良先端大）
ISEC-4. 委託可能な属性ベース暗号の実装評価
　○大竹　剛（NHK）・レイハネーサファヴィナイニ（カルガリー大）・リャンフェン チャン（上海科技大）
ISEC-5. Fully Secure Secret-sharing schemes Based on Obfuscation
　○Hui Zhao・Sakurai Kouichi（Kyushu Univ.）

セッション B-3 CSEC（2）（9：30～11：35）

6. 複数端末でのグループ鍵共有法に対するマンハッタン距離の適用　○濱崎　純・岩村恵市（東京理科大）
7. HTML ハイブリッドアプリケーションの静的解析による CSP 自動適用手法　○竹内俊輝・齋藤彰一（名工大）
8. プロセス情報不可視化のための仮想計算機モニタによるメモリアクセス制御機能の評価
　○佐藤将也・山内利宏・谷口秀夫（岡山大）
9. ナイーブベイズ分類器を用いた DNS Water Torture 攻撃のフィルタリング手法に関する検討
　○吉田琢朗（豊橋技科大）・竹内優也（カーネル・ソフト・エンジニアリング）・小林良太郎（豊橋技科大）・加藤雅彦（長崎県立大）・岸本裕之（コムワース）
10. 顔認識を用いる Glassware のためのプライバシー保護ツールキット　○岩崎　誠・掛下哲郎（佐賀大）

15 日午後　セッション A-4 ISEC（2）（13：00～14：15）

ISEC-11. 省メモリデバイス上での効率的な離散ガウス分布の生成手法
　○太中裕貴（NEC）・青野良範（NICT）・寺西　勇・峯松一彦（NEC）
ISEC-12. ブロック簡約格子に対する最短ベクトル探索の最悪時計算量評価　○高安　敦・國廣　昇（東大）
ISEC-13. 有限体上の代数曲面に関する求セクション問題から生じる連立方程式の準正則性について
　○奥村伸也（ISIT）・秋山浩一郎（東芝）・高木　剛（九大）

セッション B-4 CSEC（3）（13：00～14：15）

14. 非対称秘密分散法に適した分散情報の更新手法　○金子直人・岩村恵市（東京理科大）
15. k-匿名性による特定可能性分析に基づいたデータプライバシーのリスク分析
　○山岡裕司・伊藤孝一（富士通研）
16. 差分プライバシに基づく一括開示と対話開示のデータ有用性の評価
　○山口高康（電通大／NTT ドコモ）・寺田雅之（NTT ドコモ）・吉浦　裕（電通大）

セッション A-5 ISEC（3）（14：30～15：45）

ISEC-17. 代数曲面暗号の再考察
　○駒野雄一・秋山浩一郎（東芝）・後藤泰宏（北海道教大）・縫田光司・花岡悟一郎（産総研）
ISEC-18. パイプライン型剰余乗算器と逆元演算器で構成する 254 bit 素数ペアリング計算ハードウェアの高速実装法
　○藤本大介・長浜佑介・松本　勉（横浜国大）
ISEC-19. 金属箔人工物メトリクスにおける耐久性の評価　○吉田直樹・松本　勉（横浜国大）

セッション B-5 CSEC（4）（14：30～16：10）

20. $n<2k-1$ における統計秘匿計算に関する安全性に関する検討及び非対称秘密分散への応用
　青井　健（東京理科大）
21. 秘密計算フィッシャー正確検定（1）―標本数が少ない場合―
　○千田浩司・長谷川　聡・濱田浩気（NTT）・荻島創一・三澤計治・長﨑正朗（東北大）
22. 秘密計算フィッシャー正確検定（2）―標本数が多い場合―
　○濱田浩気・長谷川　聡・千田浩司（NTT）・荻島創一・三澤計治・長﨑正朗（東北大）
23. プライバシ保護ゲノム解析のための秘密計算フィッシャー正確検定
　○長谷川　聡・濱田浩気・千田浩司（NTT）・荻島創一・三澤計治・長﨑正朗（東北大）

◆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2日（金） 機械振興会館 テーマ：一般
【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 研究会今後の予定 〔 〕内発表申込締切日
10月3日（月） 日大理工学部駿河台キャンパス〔未定〕テーマ：情報教育，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】
多川孝央
TEL〔092〕642-4031
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15日（木），16日（金） 愛知県立大〔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
【問合先】
川村正樹（山口大）
TEL & FAX〔083〕933-5701
E-mail：kawamura@sci.yamaguchi-u.ac.jp
◎EMM 研究会 Web サイト：http://www.ieice.org/iss/emm/