★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

★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　山肩大祐・宮田純子　幹事補佐　多川孝央

★情報通信システムセキュリティ研究会（ICSS）

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

★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　越前　功　副委員長　鵜木祐史・西村竜一
幹事　栗林　稔・小嶋徹也　幹事補佐　市野将嗣・薗田光太郎

日時　7月3日（木）　10：15～17：00
　　4日（金）　10：15～15：30
会場　サン・リフレ函館（函館市大森町 2-14．http://www.city.hakodate.hokkaido.jp/docs/2014032300166/　白勢政明（公立はこだて未来大））
議題　セキュリティ，一般
3日午前　セッション A-1：ISEC（10：15～11：55）
ISEC-1．サイドチャネル認証に向けた基礎的考察
　○松原有沙・李　陽（電通大）・林　優一（東北大）・崎山一男（電通大）
ISEC-2．携帯端末への電子証明書発行方法の提案　○梅澤克之（日立）・手塚　悟（東京工科大）
ISEC-3．中間者攻撃に対して安全なプライバシ保護型 RFID Yoking-Proof プロトコル　森山大輔（NICT）
ISEC-4．プライバシー保護条件付き情報開示 II　○只木孝太郎・辻井重男（中大）
セッション B-1：CSEC（10：15～11：55）
5．Consideration of a mobile payment system using endorsement in MANETs for a disaster area
　Ojetunde Babatunde・Shibata Naoki・Juntao Gao・Ito Minoru（NAIST）
6．悪性文書ファイル内の ROP 攻撃コード検出（仮題）　田中恭之・後藤厚宏（情報セキュリティ大）
7．Android における高速な簡易スタックトレースの実現とパーミッション制御手法への応用
　高瀬拓歩・日置将太・齋藤彰一（名工大）・瀧本栄二・毛利公一（立命館大）・松尾啓志（名工大）
8．車車間通信における自律分散型認証手法の提案
　日浦博昭・北山翔馬・双紙正和（広島市大）・大場　充（工房知の匠）
セッション C-1：ICSS（10：15～11：55）
ICSS-9．ハイブリッド・クラウドにおける動的セキュリティ制御基盤方式
　○梶浦悠生・金井　敦（法政大）・谷本茂明（千葉工大）・佐藤周行（東大）
ICSS-10．標的型攻撃対策に向けた欺瞞機構を用いた防御アーキテクチャ
　○角丸貴洋・渡部正文（NEC）・吉岡克成（横浜国大）・島　成佳（NEC）
ICSS-11．HW/SW 協調によるアノマリ検知の高速化のための FPGA 部実装
　○柳瀬　駿・嶋田　創・山口由紀子・高倉弘喜（名大）
ICSS-12．車載ネットワーク CAN の実証実験環境　大石和臣（静岡理工科大）
3日午後　セッション A-2：ISEC（13：25～15：05）
ISEC-13．非可換代数を利用した D-H 型 PKA の構成とその実装
　入山聖史・○田中芳治・原　利英・大矢雅則（東京理科大）
ISEC-14．非可換代数を基にした擬似乱数生成とその実装
　○入山聖史・田中芳治・原　利英・大矢雅則（東京理科大）
ISEC-15．複数の復号指数を持つ RSA 暗号の安全性　○高安　敦・國廣　昇（東大）
ISEC-16．Perfect Conjugate-Addition Sequence を用いた新たな事前計算テーブル計算手法について
　○高橋良太（北陸先端大）・宮地充子（JAIST）
セッション B-2：CSEC（13：25～15：05）
17．グレーリストを用いたホワイトリスト／ブラックリストの生成によるマルウェア感染検知方法の検討
　角田　朋・大鳥朋哉・藤井康広・谷口信彦・木城武康（日立システムズ）

18. マルウェア動的解析結果の可視化の一手法　星澤裕二・神薗雅紀（セキュアブレイン）
19. SDN 活用によるマルウェア調査のためのネットワーク切り替え手法の提案
来間一郎・甲斐　賢・磯部義明（日立）・木城武康（日立システムズ）
20. マルウェア対策のための研究用データセット―MWS Datasets 2014―
秋山満昭（NTT）・神薗雅紀（セキュアブレイン／NICT）・松木隆宏（FFRI）・畑田充弘（NTT コミュニケーションズ）

セッション C-2 : EMM＋ICSS（13：25～15：05）

EMM-21. 適応型テンプレートによる行動的特徴を用いたモバイル端末認証
○苅田成樹・中村公美（阪大）・河野和宏（関西大）・伊藤義道（阪電通大）・馬場口　登（阪大）
ICSS-22. スマートフォンの特徴を活かした認証方式の提案　○荒谷　光・金井　敦（法政大）
EMM-23. SNS におけるプライバシーの漏洩防止を支援する公開範囲設定システムの評価
○町田史門（総研大）・梶山朋子（青学大）・嶋田　茂（産技大）・越前　功（NII）
ICSS-24. 統計情報を用いた個人情報露出量算出方式　○白山智康・金井　敦（法政大）

セッション A-3 : ISEC（15：45～17：00）

ISEC-25. センサネットワークにおける放送型通信に適したデータ認証方式
○坂井昭仁・楫　勇一・伊藤　実（奈良先端大）
ISEC-26. Forward-Secure Sequential Aggregate Message Authentication Revisited
○Shoichi Hirose（Fukui Univ.）・Hidenori Kuwakado（Kansai Univ.）
ISEC-27. 情報セキュリティの標準化動向について―ISO/IEC JTC1/SC27/WG2 2014 年 4 月香港会議報告―
○宮地充子（北陸先端大）・近澤　武（情報処理推進機構）・竜田敏男（情報セキュリティ大）・大熊建司（東芝／IPA）・渡辺　創（産総研）・松尾真一郎（NICT）

3 日午後　セッション B-3 : CSEC＋SPT（15：20～17：00）

28. Distributed Pseudo-Random Number Generation and Its Application to Cloud Database
Chen Jiageng・Miyaji Atsuko・Su Chunhua（JAIST）
29. KVM における機密情報の拡散追跡機能の設計　藤井翔太・山内利宏・谷口秀夫（岡山大）
30. 情報システム・サービスの利用者の安心感と納得感の関係に関する調査
奥村香保里（名工大）・白石善明（神戸大）・毛利公美（岐阜大）・岩田　彰（名工大）
31. プライバシに配慮したデータ処理技術の研究動向（EDBT 2014 参加報告）　川本淳平（九大）

セッション C-3 : SITE（15：20～17：00）

SITE-32. ゴッフマンの相互行為論にもとづく情報通信ネットワークにおけるプライバシー・匿名性理解の試み―対面行為から非対面的行為への拡張―　大谷卓史（吉備国際大）
SITE-33. 各都道府県の個人情報保護条例の比較　○伊藤　新・上原哲太郎（立命館大）
SITE-34. 検定教科書等のデジタル化に関する課題の検討―著作権処理に着目したデジタル教科書作成の新たな提案―
○芳賀高洋（岐阜聖徳大）・鈴木二正（慶應幼稚舎）・大谷卓史（吉備国際大）
SITE-35. 異業種共同の情報倫理　村上祐子（東北大）

4 日午前　セッション A-4 : ISEC（10：15～11：55）

ISEC-1. On Hidden Credential Retrieval　○SeongHan Shin・Kazukuni Kobara（AIST）
ISEC-2. Cryptanalysis of a matrix variant of NTRU
○Takanori Yasuda・Xavier Dahan（ISIT）・Yuya Yamaguchi（Kyushu Univ.）・Kouichi Sakurai（ISIT）
ISEC-3. Piccolo の新しい高階差分特性　○芝山直喜（航空自衛隊）・金子敏信（東京理科大）
ISEC-4. タイミング攻撃により漏洩する情報の量的評価―RSA 暗号に対する実行時間バケット法の効果に着目して―
○小林靖幸・楫　勇一（奈良先端大）・関　浩之（名大）・伊藤　実（奈良先端大）

セッション B-4 : EMM（10：15～11：55）

EMM-5. 帯域幅の異なるマイクに対応したオーディオノイズハイディング技法
○山本恭徳・姜　錫・坂本雄児（北大）
EMM-6. データハイディングを用いた防災無線システムに関するいくつかの性質
○大泉明弘・小嶋徹也（東京高専）
EMM-7. 3D プリント用デジタルデータの著作権保護のための情報ハイディング技術
○ピヤラット シラパスパコォンウォン・鈴木雅洋・海野　浩・上平員丈（神奈川工科大）・高嶋洋一（NTT）
EMM-8. 宿泊施設の Web 予約データの統合方法　○一藤　裕・曽根原　登（NII）

4 日午後　セッション A-5 : SITE＋ISEC（13：25～15：05）

SITE-9. マルコフ過程を用いた安全かつ入力が容易なパスワード生成法に関する考察（２）
○稲葉宏幸・玉井拓人（京都工繊大）
SITE-10. ブルームフィルタを用いた高速な検索可能暗号方式の提案　○木村俊介・稲葉宏幸（京都工芸大）

ISEC-11. 準同型暗号を用いた生体認証方式に対するなりすまし攻撃
　○酒見由美・武仲正彦・鳥居直哉・安田雅哉（富士通研）
ISEC-12. 準同型暗号を用いた生体認証方式に対するテンプレート復元攻撃
　酒見由美・○武仲正彦・鳥居直哉・安田雅哉（富士通研）
セッション B-5 : ICSS（13：25〜15：30）
ICSS-13. Android アプリケーションの自動リパッケージに対する耐性評価
　○金井文宏・庄田祐樹・吉岡克成・松本　勉（横浜国大）
ICSS-14. サンドボックス解析結果に基づく URL ブラックリスト生成方式に関する事例調査
　○畑田充弘・稲積孝紀・有川　隼・田中恭之（NTT コミュニケーションズ）
ICSS-15. Some distinct features of malicious authoritative DNS servers
　○Yin Minn Pa Pa・Katsunari Yoshioka・Tsutomu Matsumoto（Yokohama National Univ.）
ICSS-16. 時空符号化方式における DDoS 攻撃経路の再構成
　○佐藤　敬・下泉政樹（北九州市大）・双紙正和（広島市大）
ICSS-17. Backdoor Shell に着目した新しい Web 攻撃基盤分析手法の一考察　　神薗雅紀（横浜国大／NICT）
セッション C-5 : CSEC（13：25〜14：40）
18. a user mode implementation of filtering rule management plane on virtualized networking environment
　安藤類央（NICT）
19. マルチレイヤ・バインディング・ルータによるサイバー攻撃対策の提案と，OpenFlow を用いた実装評価
　小林　浩・八槇博史・末廣友貴・上野洋一郎・佐野　香・佐々木良一（東京電機大）
20. TCP 再送タイマ管理の変更による低量 DoS 攻撃被害緩和の実験評価　　細井琢朗・松浦幹太（東大）
◆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
◎3 日研究会終了後，懇親会を予定していますので御参加下さい．詳細は後日御連絡致します．
☆ISEC 研究会今後の予定 〔　〕内発表申込締切日
　9 月 5 日（金） 機械振興会館〔7 月 15 日（火）〕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】
　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）
☆SITE 研究会
【問合先】
　杉山典正
　TEL〔06〕6954-4189，FAX〔06〕6954-4164
　E-mail：sugiyama@ip.oit.ac.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 18 日（木），19 日（金） 高知工科大〔7 月 11 日（金）〕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