★情報セキュリティ研究会（ISEC）
専門委員長　盛合志帆　副委員長　廣瀬勝一・伊豆哲也
幹事　江村恵太・面　和成　幹事補佐　山本　大・須賀祐治

★技術と社会・倫理研究会（SITE）
専門委員長　森住哲也　副委員長　小川　賢・大谷卓史
幹事　壁谷彰慶・加藤尚徳　幹事補佐　吉永敦征・鈴木大助

★バイオメトリクス研究会（BioX）
専門委員長　大塚　玲　副委員長　大木哲史・青木隆浩
幹事　市野将嗣・高田直幸　幹事補佐　渡部大志・堀江亮太

★ハードウェアセキュリティ研究会（HWS）
専門委員長　川村信一　副委員長　池田　誠・島崎靖久
幹事　国井裕樹・小野貴継

★情報通信システムセキュリティ研究会（ICSS）
専門委員長　高倉弘喜　副委員長　吉岡克成・神谷和憲
幹事　笠間貴弘・山田　明　幹事補佐　木藤圭亮・山内利宏

★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　川村正樹　副委員長　岩田　基・小嶋徹也
幹事　秋山寛子・金田北洋　幹事補佐　稲村勝樹・河野和宏

日時　7月23日（火）　9：55～18：00
　　24日（水）　9：05～15：50
会場　高知工科大学永国寺キャンパス教育研究棟（高知市永国寺町2-22．JR高知駅から徒歩約15分．https://www.kochi-tech.ac.jp/english/about/access/　福本昌弘）
議題　セキュリティ，一般
23日午前　A-1：ISEC（1）：101（9：55～12：00）
ISEC-1．脆弱性情報を利用したゼロデイ攻撃対策システムにおける構成情報収集機能及び脆弱性評価機能の実装
　○楠目　幹・喜田弘司・最所圭三（香川大）
ISEC-2．擬似的な標的型攻撃の実行に向けた攻撃シナリオ生成方式の提案
　○髙橋佑典・島　成佳・内藤厚典（NEC）・田辺瑠偉・吉岡克成（横浜国大）
ISEC-3．ブロックチェーンネットワークにおけるハニーポット設置に向けた悪意あるユーザのプロファイリング
　○原　和希・佐藤哲平・今村光良（筑波大）・面　和成（筑波大／NICT）
ISEC-4．ブロックチェーン技術の分散性による無停止メカニズムのリスク分析
　○田口　渉・今村光良（筑波大）・面　和成（筑波大／NICT）
ISEC-5．ビットコインにおけるユーザへの信頼性付与の手法
　○鈴木明日香・佐藤哲平（筑波大）・面　和成（筑波大／NICT）
B-1：CSEC（1）：213（9：55～12：00）
6．金融サービスにおける機械学習システムの適切な活用について：セキュリティと品質に焦点を当てて
　○清藤武暢・宇根正志（日本銀行）
7．対象者の人数と人間関係に制約のない移動履歴とSNSアカウントの照合
　○大岡拓斗・松本　瞬・市野将嗣・吉浦　裕（電通大）
8．マルウェア対策のための研究用データセット―MWS Datasets 2019―　荒木粧子（ソリトンシステムズ）・○笠間貴弘（NICT）・押場博光（FFRI）・千葉大紀・畑田充弘（NTT）・寺田真敏（東京電機大）
9．擬似C＆Cサーバを用いたIoTマルウェア駆除手法の検討　○三須剛史・高田一樹（セキュアブレイン）
10．観測ロケットMOMO3号機によるセキュア通信方式の基礎実験
　○吉田真紀（NICT）・森岡澄夫（インターステラテクノロジズ）・尾花　賢（法政大）
D-1：BioX：328（9：55～11：35）
BioX-11．PRNUノイズに基づく画像クラスタリングにおける類似度計算手法の評価
　○内田麻衣・富岡洋一（会津大）
BioX-12．生後24時間以内の新生児指紋用2,400 ppi指紋撮像機の開発

○幸田芳紀・高橋　愛・伊藤康一・青木孝文（東北大）
BioX-13. 手のひら伝搬信号の二階差分位相スペクトルを用いた個人識別
○藤田航平・石本雄也・中西　功（鳥取大）
BioX-14. 顔検出防止技術の評価実験　○江藤一樹・脇　一史・森　駿文・菊池浩明（明大）

23 日午後　A-2 : ISEC（2）：104（13：10〜15：15）

ISEC-15. 適応的安全でより効率的な格子鍵失効機能付き ID ベース暗号の構成　高安　敦（東大）
ISEC-16. クラウドセンシング向け失効可能グループ署名における匿名性の強化　○中澤勇人・中西　透（広島大）
ISEC-17. A CSIDH Group Action Based Even-Mansour Construction　Hector Hougaard（Osaka Univ.）
ISEC-18. 剰余逆元計算の新しい量子アルゴリズムと楕円曲線離散対数問題への応用
○鞍馬　遼（東大）・國廣　昇（筑波大）
ISEC-19. Attribute-Based Group Signatures for Revocable Members
Maharage Nisansala Sevwandi Perera（ATR）

B-2 : HWS（1）：213（13：10〜15：15）

HWS-20. ガロア体算術に基づく暗号ハードウェアの形式的トロイフリー性検証
○伊東　燦・上野　嶺・本間尚文（東北大）
HWS-21. IC チップレベル消費電流シミュレーションによる暗号モジュールのサイドチャネル漏洩評価
○門田和樹・安田一樹・月岡暉裕・三浦典之・永田　真（神戸大）
HWS-22. 動的電力制御によるサイドチャネル対策の検討　請園智玲（福岡大）
HWS-23. パイプライン型剰余乗算器を用いたペアリング計算 FPGA のサイドチャネルセキュリティ評価
○山﨑満文・坂本純一・奥秋陽太・松本　勉（横浜国大）
HWS-24. パイプライン型剰余乗算器を用いたペアリング計算器の FPGA 実装における Post Adder の改良
○奥秋陽太・坂本純一・藤本大介・松本　勉（横浜国大）

D-2 : SITE（1）：328（13：10〜14：50）

SITE-25. 部分的な忘却に対応するパスワードリマインドシステムの提案と実装
○細田涼太・稲葉宏幸（京都工繊大）
SITE-26. 破滅的忘却を軽減するニューラルネットワークを用いたスパムフィルタの提案
○川原秀一・シン ルー・稲葉宏幸（京都工繊大）
SITE-27. フレーム間のパーシステントホモロジーの差異を用いた動画像電子透かし
木村崇也・○稲葉宏幸（京都工繊大）
SITE-28. ホログラフィと視覚復号型秘密分散法を利用した三次元画像暗号化の検討
○高澤　匠・鈴木一弘・髙田直樹（高知大）

招待講演：104（15：30〜16：30）

29. 未定　高木浩光（AIST）

全体企画セッション（1）：104（16：30〜17：30）

30. トップカンファレンス採録への道（仮称）

全体企画セッション（2）：104（17：30〜18：00）

31. サイバーセキュリティ研究の倫理的配慮のためのチェックリスト（仮）

24 日午前　A-3 : ISEC（3）：104（9：05〜10：45）

ISEC-1. Securing the USB interface
○Jan Goette（Waseda Univ.）・Naoto Yanai（Osaka Univ.）・Tatsuya Mori（Waseda Univ.）
ISEC-2. FPGA における CSIDH の効率的な実装手法　○小寺健太・鄭　振牟・宮地充子（阪大）
ISEC-3. A Performance Analysis on Supersingular Isogeny Diffie-Hellman with Several Classes of the Extension Field of Degree 2　○Yuki Nanjo（Okayama Univ.）・Masaaki Shirase（Future Univ. Hakodate）・Takuya Kusaka・Yasuyuki Nogami（Okayama Univ.）
ISEC-4. 文書データに対するリスク評価
○三本知明・清本晋作（KDDI 総合研究所）・北村光司（産総研）・宮地充子（阪大）

B-3 : HWS（2）：213（9：05〜10：45）

HWS-5. ダブルレーザー照射装置を用いた TVC に対する命令置換フォールト攻撃
○鈴木朋郎・坂本純一・松本　勉（横浜国大）
HWS-6. ASIC 実装した Ring-Oscillator PUF への電磁界解析攻撃　○汐﨑　充・藤野　毅（立命館大）
HWS-7. 電磁的情報漏えいを強制的に誘発する照射周波数決定法に関する基礎検討
○鍛治秀伍（奈良先端大）・衣川昌宏（仙台高専）・藤本大介・林　優一（奈良先端大）
HWS-8. 複数の受光素子を用いたパルス方式測距 LIDAR の計測セキュリティ
○末廣達也・一ノ瀬竜矢・櫻澤　聡・吉田直樹・松本　勉（横浜国大）

C-3 : SITE（２）：210（9：30〜10：45）

SITE-9. Boid 的アノーテーションと Labeled-LDA による家族的類似の推論規則生成―推論攻撃分析と covert channel 攻撃分析を統合する機械学習的アプローチ―　○紅林宏祐・森住哲也・木下宏揚（神奈川大）

SITE-10. OODA ループの「暗黙の誘導制御」に関する一考察―フィッシングサイトへの対抗策―
○瀧川雄一（防衛大）・辰己丈夫（放送大）

SITE-11. 脆弱性評価と修復プロセスを取り入れたサーバ構築演習　鈴木大助（北陸大）

A-4 : CSEC（２）：104（10：55〜12：35）

12. n＜2k-1 において計算結果の正当性を検証可能な秘密分散を用いた秘匿計算
○落合将吾・岩村恵市（東京理科大）

13. ブロックチェーンを用いた IoT システム向け証明サービス基盤の提案
○大久保隆夫（情報セキュリティ大）・田嶋　健・上原敏幸（アイビーシー）

14. ブロックチェーンを用いた公正なオンラインゲームの確立手法　○佐古健太郎・森　達哉（早大）

15. Ethereum ブロックチェーンで綿菓子を巻く方法　須賀祐治（IIJ）

B-4 : EMM/ICSS : 213（10：55〜12：35）

ICSS-16. マルウェア検知システムにおけるブロックチェーンベースのマルウェア情報共有手法の検討
○藤　竜成・臼崎翔太郎・油田健太郎・山場久昭・片山徹郎（宮崎大）・朴　美娘（神奈川工科大）・白鳥則郎（中大）・岡崎直宣（宮崎大）

ICSS-17. 能動的攻撃観測環境における端末の自動駆動システム　○安田真悟・金谷延幸・井上大介（NICT）

EMM-18. 規範的影響による同調行動を考慮した違法コンテンツの利用抑制の検討
山口央貴・○河野和宏（関西大）

EMM-19. システムチップ依存の音響歪みに基づく録音機器識別　西村　明（東京情報大）

C-4 : SITE（３）：210（10：55〜12：10）

SITE-20. 必ずしも完全に分有されないロゴスと言語ゲームをつなぐ確率的存在者―セキュリティモデルの限界と人工知能の可能性―　森住哲也（神奈川大）

SITE-21. いわゆる AI に関する国際規制動向調査報告―欧州委員会ガイドラインのパブリックコメントによる影響分析―　○加藤尚徳（KDDI 総合研究所）・鈴木政朝（新潟大／理研）・板倉陽一郎（ひかり総合法律事務所／理研）・村上陽亮（KDDI 総合研究所）

SITE-22. 北米及び欧州におけるインターネット研究倫理ガイドラインについて―代表的ガイドラインの紹介と分析―
○大谷卓史（吉備国際大）・大澤博隆（筑波大）・神崎宣次（南山大）・久木田水生（名大）・西條玲奈（京大）

24 日午後　A-5 : ISEC（４）：104（13：45〜15：50）

ISEC-23. 究極の本人確認のための 3 層構造公開鍵暗号の提案―STR の秘密鍵への埋め込みとその利用に向けて―
○辻井重男・才所敏明・山沢昌夫・四方　光（中大）・佐々木浩二・鈴木伸治（アドイン研）

ISEC-24. 楕円曲線に基づく匿名公開鍵証明書　大石和臣（静岡理工科大）

ISEC-25. 鍵更新機能付き共通鍵型検索可能暗号の一実現方式　○松崎なつめ・穴田啓晃（長崎県立大）

ISEC-26. 第 9 回バル＝イラン大学冬季暗号学スクール参加報告　穴田啓晃（長崎県立大）

ISEC-27. ボチュバルの 3 値論理による Garbled Circuit　○林　隼輔・佐々木太良・藤岡　淳（神奈川大）

B-5 : HWS（３）：213（13：45〜15：50）

HWS-28. 高位設計フローにベイズ最適化法を応用した設計空間探索
○中山亮平（東大）・粟野皓光（阪大）・池田　誠（東大）

HWS-29. 乗法的オフセットに基づく高効率 AES ハードウェアアーキテクチャの設計
○上野　嶺（東北大）・森岡澄夫（IST）・三浦典之・松田航平・永田　真（神戸大）・Shivam Bhasin（NTU）・Yves Mathieu・Tarik Graba・Jean-Luc Danger（TPT）・本間尚文（東北大）

HWS-30. 準同型性を有する Paillier アルゴリズムに向けた高性能プロセッサの設計
○蔡　純・池田　誠（東大）・粟野皓光（阪大）

HWS-31. Potential Method to Extract Uniqueness from Non-Ideality of Sensor Device
○Thibaut Constant・Makoto Nagata・Noriyuki Miura（Kobe Univ.）

HWS-32. USB 機器の電圧変化による個体識別の可能性　○外山　拓・坂本純一・吉田直樹・松本　勉（横浜国大）

C-5 : SPT : 210（13：45〜15：50）

33. メールにおける誘導手口の推定手法に関する検討　○山本　匠・西川弘毅・岩崎亜衣子（三菱電機）・上原航汰（静岡大）・Harsham Bret・Wang Ye・Hori Chiori・河内清人（三菱電機）・西垣正勝（静岡大）

34. 新聞で報道される情報漏えい事故の属性分析　○新原功一・菊池浩明（明大）

35. セキュリティやプライバシーに関する SoK 論文やサーベイ論文を SoK する　金岡　晃（東邦大）

36. ソーシャルエンジニアリング攻撃の成否とユーザ特性との関係性の検討　小倉加奈代（岩手県立大）

37. 情報セキュリティに関連するガイドラインの Doc2Vec を用いた文書内容の可視化手法の提案とその評価

尾崎敏司（筑波大／トレンドマイクロ）

◆情報処理学会；コンピュータセキュリティ研究会／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 6 日（金） 機械振興会館 テーマ：2019 年暗号と情報セキュリティワークショップ

【問合先】

面 和成（筑波大）

E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）

☆SITE 研究会

【問合先】 SITE 研究会幹事

壁谷彰慶

E-mail：site-contact@mail.ieice.org

◎公式 Web サイト

http://www.ieice.org/ess/site/

☆BioX 研究会

【問合先】

BioX 研究専門委員会幹事団

E-mail：biox-kanji@mail.ieice.org

☆HWS 研究会

【問合先】

三浦典之（神戸大）・国井裕樹（セコム）

E-mail：hws-sec@mail.ieice.org

☆ICSS 研究会

【問合先】

高倉弘喜（NII）

E-mail：icss-adm-req@mail.ieice.org（幹事団宛）

◎最新情報は，ICSS 研究会ホームページを御覧下さい．

https://www.ieice.org/iss/icss/index.html

☆EMM 研究会今後の予定 〔 〕内発表申込締切日

9 月 19 日（木），20 日（金） 新潟大駅南キャンパス〔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，メディア処理（AI，深層学習），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