★情報セキュリティ研究会（ISEC）
専門委員長　伊豆哲也　副委員長　國廣　昇・花岡悟一郎
幹事　山本　大・米山一樹　幹事補佐　松田隆宏

★技術と社会・倫理研究会（SITE）
専門委員長　小川　賢　副委員長　大谷卓史・辰己丈夫
幹事　吉永敦征・鈴木大助　幹事補佐　藤井秀之・橘　雄介

★バイオメトリクス研究会（BioX）
専門委員長　今岡　仁　副委員長　市野将嗣・高田直幸
幹事　奥井宣広・佐野恵美子　幹事補佐　鈴木裕之・早坂昭裕

★ハードウェアセキュリティ研究会（HWS）
専門委員長　島崎靖久　副委員長　永田　真・鈴木大輔
幹事　高橋順子・藤本大介

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

★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　西村竜一　副委員長　藤吉正明・市野将嗣
幹事　長谷川まどか・吉田真紀　幹事補佐　今泉祥子・高嶋洋一

日時　7月19日（月）　9：10～18：10
　　20日（火）　9：00～17：35
会場　オンライン開催
議題　セキュリティ，一般（セキュリティサマーサミット2021）
19日午前　PWS企画セッション（トラック1）（9：10～10：15）
1. オンライン広告プライバシーについて／PWSCUP2021について
CSEC1（トラック1）（10：30～12：10）
2. マルウェア検知に対するバックドアポイズニング攻撃の対策としてのオートエンコーダの定量的評価
　○松本悠希（東北大）・成定真太郎・披田野清良（KDDI総合研究所）・内林俊洋（九大）・菅沼拓夫・樋地正浩（東北大）
3. IoT機器のWebUIを模したハニーポットの自動生成フレームワーク
　○山本萌花・掛井将平・齋藤彰一（名工大）
4. 監視カメラシステムによる人物検出に耐性を持つ衣類の作成　○金井春輝・宇田隆哉（東京工科大）
5. コンピュータセキュリティシンポジウムCSS2020オンライン開催報告
　○白石善明（神戸大）・掛井将平（名工大）・瀧田　愼（兵庫県立大）・磯部光平（セコム）・田宮寛人（NEC）・毛利公美・箕浦翔悟・冨田裕涼（岐阜大）・古本啓祐（NICT）・廣友雅徳（佐賀大）・福田洋治（近畿大）・池上雅人（キヤノンマーケティングジャパン）・甲斐　博（愛媛大）・曽根直人（鳴門教育大）・森井昌克（神戸大）
19日午後　HWS1（トラック1）（13：30～14：45）
HWS-6. RNS表現によるバイナリ拡張ユークリッド互除法を用いたペアリング計算における逆元計算の高速実装に関する検討
　○森本康太・藤本大介・大須賀彩希（奈良先端大）・川村信一・照屋唯紀（産総研）・林　優一（奈良先端大）
HWS-7. BLS12-381曲線上ペアリング暗号の省メモリ実装
　○安西　陸・坂本純一・宋　子豪・吉田直樹・松本　勉（横浜国大）
HWS-8. 並列化Quotient Pipelining モンゴメリ乗算に基づくFp2乗算器データパスの設計とその同種写像暗号への応用に関する検討　○上野　嶺（東北大／JSTさきがけ）・本間尚文（東北大）
CSEC2（トラック1）（15：00～16：40）
9. ビットコイン利用者の特定・追跡の仕組みに関する考察（2）
　○才所敏明（IT企画）・辻井重男（中大）・櫻井幸一（九大）
10. サーバ台数n＜2k-1において実数演算可能な秘匿計算法の提案
　○納所勇之介・岩村恵市（東京理科大）・稲村勝樹（広島市大）

11. n＜2k-1 において malicious な攻撃者に対しても安全な秘密分散を用いた秘匿計算の高速化
　　○工藤凌也・岩村恵市（東京理科大）・稲村勝樹（広島市大）
12. サーバ台数 n＜2k-1 における高速な秘匿計算の実装と比較
　　○黒井大智・岩村恵市（東京理科大）・稲村勝樹（広島市大）

SPT1（トラック 1）（16：55～18：10）

13. セキュリティインシデント対応の組織及びプロセスのシミュレーションによる検討手法の提案と評価
　　○粕淵　卓（NTT 西日本／東大）・稗方和夫（東大）
14. Web 上認証サイトのパスワード構成ポリシー表示方法に関する大規模調査
　　○藤田真浩・山中忠和・松田　規（三菱電機）・金岡　晃（東邦大）
15. アプリトラッキング透明性に対するダークパターンの調査　　坂本一仁（DataSign）

19 日午前　ISEC1（トラック 2）（10：30～12：10）

ISEC-16. A Website Fingerprinting Attack based on the Virtual Memory of the Process on Android Devices
　　○Tatsuya Okazaki・Hiroya Kato・Shuichiro Haruta・Iwao Sasase（Keio Univ.）
ISEC-17. Rogue Access Point Detection by Using ARP Failure under the MAC Address Duplication
　　○Kosuke Igarashi・Hiroya Kato・Iwao Sasase（Keio Univ.）
ISEC-18. 誤検知軽減システムを導入した分散型 Slow HTTP DoS 攻撃検知手法の検証
　　○田村恒輝・布田裕一（東京工科大）・鈴木智道（PitApp）
ISEC-19. SVM を用いた制御システムに対する偽装命令攻撃の検知
　　○原田雄基・布田裕一（東京工科大）・岡崎裕之（信州大）

19 日午後　SITE シンポジウム（トラック 2）（13：30～16：30）

SITE-20.〔招待講演〕 データサイエンスの ELSI　　村上祐子（立教大）
SITE-21.〔招待講演〕 放送大学における数理・データサイエンス・AI リテラシー講座・「心得」編
　　辰己丈夫（放送大）
SITE-22.〔招待講演〕 データサイエンスの法と倫理　　加藤尚徳（KDDI 総合研究所／理研）
SITE-23.〔招待講演〕 人工知能の倫理とその教育　　久木田水生（名大）
SITE-24.〔招待講演〕 データサイエンスの実践と法・倫理　　森下壮一郎（サイバーエージェント）

ISEC2（トラック 2）（16：55～18：10）

ISEC-25. ガロア環上の漸近的に良い乗法的線形秘密分散法と Z/pkZ 上の秘密計算への応用についてのノート
　　穴田啓晃（長崎県立大）
ISEC-26. 認証鍵交換方式 FSXY におけるハイブリッド安全性の検証
　　○川口武瑠・鈴木誠十郎・藤岡　淳・佐々木太良（神奈川大）
ISEC-27. Efficient Face Template Protection System Based on Packed Homomorphic Encryption
　　○Hiroto Tamiya・Kengo Mori・Toshiyuki Isshiki（NEC）・Satoshi Obana（Hosei Univ.）・Tetsushi Ohki（Shizuoka Univ.）

20 日午前　SPT2（トラック 1）（9：00～10：15）

1. Windows Update に関するユーザの行動と環境・心理学的要因の関係の調査
　　○河田真由子・古川和快（富士通）・角尾幸保（東京通信大）
2. 個人特性を活用したデータ流通に向けた一貫性選好に関する検討
　　○大橋盛徳・藤村　滋・土屋志高・中平　篤（NTT）
3. ユーザブルセキュリティ研究における満足度評価の実態調査　　金岡　晃（東邦大）

CSEC3/BioX1（トラック 1）（10：30～12：10）

4. サーバレスアプリケーションにおけるデータの変化に伴う機密度再計算手法の提案
　　○田村　悠・磯部義明（日立）
5. 情報理論的に安全な数鍵を用いた通信認証システム　　○白石桃子・相田　仁（東大）
6. An anti-forensics Acoustic Watermarking Based on Integer Rotation towards DCT Coefficients
　　黄　緒平（都立産技大）

BioX-7. Black-box Adversarial Attack による顔認証へのなりすまし可能性に関する検討
　　○ヴォ ゴック コイ グエン・寺田崇倫・西垣正勝・大木哲史（静岡大）

20 日午後　招待講演（共通）（13：10～14：10）

8. IoT におけるサイバー攻撃の最新動向―IoT マルウェアの多様化―　　田辺瑠偉（横浜国大）

HWS2（トラック 1）（14：25～15：40）

HWS-9. Wi-Fi チャネル状態情報を用いた位置推定による不正機器検知技術の検討
　　○千賀功平・鈴木大輔（三菱電機）
HWS-10. マスキング対策された暗号ハードウェアへの深層学習を用いたサイドチャネル解析

小嶋健太・○伊東　燦・上野　嶺・本間尚文（東北大）
HWS-11．ハードウェア実装された未対策 AES 及び RSM-AES に対する深層学習サイドチャネル攻撃
○福田悠太・吉田康太・橋本尚志・藤野　毅（立命館大）
HWS3（トラック 1）（15：55～17：10）
HWS-12．PUF を信頼の基点とした RISC-V TEE 環境の実装
○吉田康太（立命館大）・須崎有康（産総研）・藤野　毅（立命館大）
HWS-13．CMOS イメージセンサを利用した物理乱数生成器の性能評価
○龍野隼人・大山達哉・白畑正芳・大倉俊介・藤野　毅（立命館大）
HWS-14．リングオシレータ型真性乱数生成器の実装と評価（２）
○皆川隆一・大前ケヴィン秀明・鳥居直哉（創価大）
20 日午前　ISEC3（トラック 2）（9：00～10：15）
ISEC-15．鍵紛失時における非常ボタン式資産退避手法の実用化に関する考察
○松崎なつめ・喜多義弘（長崎県立大）
ISEC-16．Dogecoin ネットワークの特徴とセキュリティリスクの考察
○今村光良（筑波大）・面　和成（筑波大／NICT）
ISEC-17．NFT の信頼性にみるセキュリティリスクの考察
○木村圭吾（筑波大）・今村光良（野村アセットマネジメント）・面　和成（筑波大）
EMM1/ICSS1（トラック 2）（10：30～12：10）
EMM-18．Minecraft を活用した AI リテラシー学習ツールの開発　　岸本彗佳・○河野和宏（関西大）
EMM-19．Hybrid Multiplicative Secret Sharing　　Maki Yoshida（NICT）
ICSS-20．Twitter で収集された Android アプリのアクセシビリティサービスの利用率と API Level の分析
○市岡秀一（岡山大）・三村隆夫・中嶋　淳（セキュアブレイン）・山内利宏（岡山大）
ICSS-21．ID/Password 設定に不備のある IoT 機器におけるマルウェア感染可能性の大規模調査
○村上洸介・笠間貴弘・井上大介（NICT）
20 日午後　招待講演（共通）（13：10～14：10）
22．IoT におけるサイバー攻撃の最新動向―IoT マルウェアの多様化―　　田辺瑠偉（横浜国大）
ISEC4（トラック 2）（14：25～15：40）
ISEC-23．x^{-1}-POSEIDON$^{\pi}$ への代数攻撃　　○大井脩平・米山一樹（茨城大）
ISEC-24．ForkSkinny に対する MILP を用いた差分パス探索
○岡崎雅哉（名大）・佐々木　悠（NTT）・岩田　哲（名大）
ISEC-25．暗号ハッシュ関数を利用した仮想通貨採掘の時間分散に対する計算機実験評価
○池辺　慶・櫻井幸一（九大）
SITE1（トラック 2）（15：55～17：35）
SITE-26．DCT ブロックに適応的にゲインを乗じる変換領域利用型ステガノグラフィの検討
○大沼海仁・宮田純子（芝浦工大）
SITE-27．トランスクリエーションを利用したプログラミング教育方法の開発　　森田正大（松山短大）
SITE-28．意思決定支援としての研究倫理―AoIR 倫理ガイドラインの原理と倫理分析―
○大谷卓史（吉備国際大）・大澤博隆（筑波大）・壁谷彰慶（東洋英和女学院大）・神崎宣次（南山大）・久木田水生（名大）・西條玲奈（阪大）
SITE-29．いわゆる AI に関する国際規制動向調査報告―欧州委員会による AI 規則提案の分析 2―
○加藤尚徳（KDDI 総合研究所／理研）・鈴木正朝（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・花原克年（KDDI 総合研究所）
◆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
【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　加藤尚徳
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 研究会幹事団
E-mail：biox-kanji@mail.ieice.org
☆HWS 研究会
【問合先】
小野貴継（九大）・高橋順子（NTT）
E-mail：hws-sec@mail.ieice.org
☆ICSS 研究会
【問合先】
ICSS 研究会幹事団
E-mail：icss-adm-req@mail.ieice.org（幹事団宛）
◎最新情報は，情報通信システムセキュリティ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
8 月 25 日（水），26 日（木） オンライン開催（FIT2021 と併催）〔締切済〕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
【問合先】
EMM 研究会
E-mail：emm-admin@mail.ieice.org（幹事団）