★情報セキュリティ研究会（ISEC）
専門委員長　廣瀬勝一　副委員長　伊豆哲也・國廣　昇
幹事　面　和成・山本　大　幹事補佐　米山一樹

★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　加藤尚徳・吉永敦征　幹事補佐　鈴木大助・藤井秀之

★バイオメトリクス研究会（BioX）
専門委員長　大塚　玲　副委員長　青木隆浩・市野将嗣
幹事　高田直幸・奥井宣広　幹事補佐　佐野恵美子・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　池田　誠　副委員長　島崎靖久・永田　真
幹事　小野貴継・高橋順子

★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・藤吉正明
幹事　稲村勝樹・河野和宏　幹事補佐　長谷川まどか・吉田真紀

日時　7月20日（月）　10：00～17：00
　　21日（火）　10：00～17：00
会場　オンライン開催
議題　セキュリティ，一般
20日午前　SITE/BioX（会場1）（10：00～11：40）
SITE-1. 欧州SATORIプロジェクトにおける研究開発倫理ガイドライン開発（2）―EIA審査のCEN標準案とその背景―
　○大谷卓史（吉備国際大）・神崎宣次（南山大）・久木田水生（名大）・大澤博隆（筑波大）・西條玲奈（阪大）
SITE-2. データ保護に関する国際政策動向調査報告―欧州における顔識別規制に関する一考察―
　○加藤尚徳（KDDI総合研究所／理研AIP）・鈴木正朝（新潟大／理研AIP）・村上陽亮（KDDI総合研究所）
BioX-3. 深層学習を用いた可視光虹彩認証のための特徴抽出器の開発　○本田哲也・高野博史（富山県立大）
BioX-4. 知覚できない視覚刺激を用いた個人認証―ウェーブレット変換と機械学習による識別性能の改善―
　○三宅崇弘・金城希望・中西　功（鳥取大）
20日午後　ISEC（1）（会場1）（13：00～14：15）
ISEC-5. 分散機械学習手法を用いたビッグデータシステムのプライバシー保護　○陳　昭衡・面　和成（筑波大）
ISEC-6. 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（2）
　○田口　渉・今村光良（筑波大）・面　和成（筑波大／NICT）
ISEC-7. 指数ブラインディングされたSliding Window法を用いたCRT-RSAに対するサイドチャネル攻撃に関する検討　○大澤創紀・上野　嶺・本間尚文（東北大）
CSEC（1）（会場2）（13：00～14：15）
8. 対象スレッドの違いによるマルウェア検知精度の比較　梶原友希・鄭　俊俊・毛利公一（立命館大）
9. Windowsにおけるハッシュ値の伝播によるスレッドインジェクション機能を持つマルウェアの特定手法
　田中大樹（立命館大）・川古谷裕平・岩村　誠（NTT）・鄭　俊俊・毛利公一（立命館大）
10. 詐欺メール対策の試作　今橋泰則（NEC）
企画セッション（14：30～15：30）
11. 企画セッション（1）
ISEC（2）（会場1）（15：45～17：00）
ISEC-12. Sum of Even-Mansour擬似ランダム関数に対する量子攻撃　○品川和生・岩田　哲（名大）
ISEC-13. 効率的なタグ生成を用いた格子ベース署名方式と実装評価
　○梶田海成・大竹　剛（NHK）・小川一人（NICT）・縫田光司・高木　剛（東大）

ISEC-14. ストカスティック演算を用いた確率的準同型暗号の構成に関する検討
〇小関隆介・上野　嶺・本間尚文（東北大）
CSEC（2）（会場 2）（15：45〜17：00）
15. スペクトル領域上の雑音摂動法における雑音抑圧手法　黄　緒平（都立産業技術大）・川島龍太（名工大）
16. Acoustic information hiding based on voice activity detection　黄　緒平（都立産業技術大）
17. 脆弱性データベースを使用した脅威分析―トピックモデル分析による攻撃事例と大規模脆弱性 DB の突合手法の複数事例への適用―　小柳洋貴（湘南工科大）・寶木和夫・三科雄介（産総研）・梅澤克之（湘南工科大）
21 日午前　HWS（会場 1）（10：00〜11：40）
HWS-1. ラッチを用いた物理乱数生成器の乱数の性能評価　鳥居直哉・〇大前 ケビン 秀明（創価大）
HWS-2. 直線型バスにおける不正機器検出　〇福田國統・安永貴仁・礒山芳一・朝夷名 巧・畑　洋一（住友電工）
HWS-3. LiDAR-based SLAM における姿勢推定のための ICP アルゴリズムに対する敵対的スキャン生成攻撃
〇吉田康太・藤野　毅（立命館大）
HWS-4. 車載通信向けメッセージ認証コードに対するサイドチャネル解析　〇永戸謙成・ヴィッレ ウリマウル・上野　嶺（東北大）・遠山　毅・小熊　寿（トヨタ自動車）・本間尚文（東北大）
CSEC（3）（会場 2）（10：00〜11：15）
5. テレビ視聴ロボット用外部クラウドインターフェースにおけるセキュリティ対策
村崎康博・星　祐太・萩尾勇太・上村真利奈・金子　豊・山本正男（NHK）
6. スマート家電に適した PKI の運用方法の考察　山川大貴・上原哲太郎（立命館大）・猪俣敦夫（立命館大／阪大）
7. リンクデコレーション及び CNAME クローキングによるクッキー共有のリスク分析
高田雄太・伊藤大貴・熊谷裕志・神薗雅紀（デロイトトーマツサイバー）
8. Web アプリケーションを安全にする新しいフレームワークの機能　久保田康平・小出　洋（九大）
21 日午後　ICSS（会場 1）（13：00〜14：15）
9. LED の個体識別における温度変化の影響　〇土屋彩夏・藤　聡子・李　陽・崎山一男・菅原　健（電通大）
10. TLS バージョン移行と EV 証明書利用に関する局所的調査（FY2019 4Q）　須賀祐治（IIJ）
ICSS-11. 低出力局所性を持つ準同型性コミットメント方式　〇宮地秀至・宮地充子（阪大）
SPT/CSEC（4）（会場 2）（13：00〜14：15）
12. 侵入検知に向けたシステム内悪性活動の紐付け及び可視化手法の検討
末次信貴（アイネス総合研究所）・橋本正樹（情報セキュリティ大）
13. Android アプリケーションにおける暗号 API 利用動向の基礎調査　河合惇丞・金岡　晃（東邦大）
14. 自律的なセキュリティ行動変容ステージモデルの定義とユーザ要因の影響分析
佐野絢音・澤谷雪子・山田　明・窪田　歩（KDDI 総合研究所）
企画セッション（14：30〜15：30）
15. 企画セッション（2）
ISEC（3）（会場 1）（15：45〜17：00）
ISEC-16. 送・受信者間での鍵交換が不要な共通鍵暗号のための鍵共有方式―TS システムの提案―
鈴木伸治・佐々木浩二（アドイン研）・辻　敏雄（立命館大）・〇辻井重男（中大）
ISEC-17. 任意の BLS 曲線の最終べきの hard part について
〇白勢政明（公立はこだて未来大）・南條由紀（岡山大）
ISEC-18. Secure and Compact Elliptic Curve LR Scalar Multiplication　〇Yaoan Jin・Atsuko Miyaji（Osaka Univ.）
◎本研究会は完全オンライン開催になります．オンライン開催に関する情報は随時展開致します．
◆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 11 日（金） テーマ：2020 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