★情報セキュリティ研究会（ISEC）
専門委員長　藤岡　淳　副委員長　盛合志帆・廣瀬勝一
幹事　大東俊博・江村恵太　幹事補佐　面　和成・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　川口嘉奈子・壁谷彰慶　幹事補佐　加藤尚徳・吉永敦征・鈴木大助

★ハードウェアセキュリティ研究会（HWS）
専門委員長　松本　勉　副委員長　川村信一・池田　誠
幹事　三浦典之・国井裕樹

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

★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　岩村惠市　副委員長　栗林　稔・小嶋徹也
幹事　姜　玄浩・村田晴美　幹事補佐　今泉祥子・金田北洋

◎SITE 研究会を除く研究会は参加費が必要になります.
ESS の技報電子化研究会に関する御案内ページ（ISEC/HWS）
https://www.ieice.org/ess/ESS/gihou-trial-ess2018.html
ISS の技報完全電子化研究会に関する御案内ページ（ICSS/EMM）
https://www.ieice.org/iss/jpn/notice/e_gihou.html

日時　7 月 25 日（水）　9：55～17：05
26 日（木）　9：30～16：30
会場　札幌コンベンションセンター（札幌市白石区東札幌 6 条 1-1-1. 地下鉄東西線：東札幌駅下車徒歩約 8 分. https://www.sora-scc.jp/access/）
議題　セキュリティ，一般
25 日午前　B-1 : ISEC（1）：204（9：55～11：35）
ISEC-1. 現実的な結託者数のもとで最もシェア長の短いロバスト秘密分散法
〇渡邉洋平・大原一真・岩本　貢・太田和夫（電通大）
ISEC-2. 適応的に安全な鍵失効機能付き階層型 ID ベース暗号の構成　高安　敦（東大）
ISEC-3. Code-Based Signature Scheme via Fiat-Shamir Transformation　〇Partha Sarathi Roy（KDDI Research）・Kirill Morozov（Univ. of North Texas）・Kazuhide Fukushima・Shinsaku Kiyomoto（KDDI Research）
ISEC-4. セキュアチャネルフリー検索可能暗号と公開鍵暗号との安全な併用について
〇鈴木達也（東海大）・江村恵太（NICT）・大東俊博（東海大）
C-1 : CSEC（1）：207（9：55～12：00）
5. Infrasturucture as code によるシステム試験環境の自動生成及び自動試験による情報セキュリティリスクの検出手法の提案　〇沼田晋作・中井悠人・橋本昭二・柏　大（NTT コミュニケーションズ）
6. Man In The Browser 攻撃対策を実現する人間・銀行サーバ間のセキュア通信プロトコル（その 3）
〇向平浩貴・神農泰圭・土屋貴史・大木哲史（静岡大）・高橋健太（日立）・尾形わかは（東工大）・西垣正勝（静岡大）
7. FIDO 認証を用いて Web メールサービスを S/MIME 対応にする提案
須賀祐治（インターネットイニシアティブ）
8. Transport Layer Security（TLS）1.3 の安全性に関する研究動向　〇米澤祥子・菅野　哲（レピダム）
9. ブロックチェーンと中央集権型サーバの連携による実用的スマートコントラクトの実現手法
〇福光正幸（北海道情報大）・長谷川真吾・磯辺秀司（東北大）・岩田直樹（デンソー）・岩﨑淳也・小泉英介（東北大）・中田恒夫（デンソー）・酒井正夫（東北大）
25 日午後　A-2 : HWS（1）：201，202（13：10～15：15）
HWS-10. 超音波距離計に対する変調波を利用した対策手法の検討　〇藤本大介・林　優一（奈良先端大）
HWS-11. ToF 距離画像カメラの測定パルス光なりすましに対する計測セキュリティ評価システム

○櫻澤　聡・藤本大介・松本　勉（横浜国大）

HWS-12. 計測妨害と幻視攻撃に対するステレオカメラの計測セキュリティ評価方法に関する研究
吉田直樹・○野平浩生・岩田康志・松本　勉（横浜国大）

HWS-13. ガウス雑音を用いた暗号モジュール遠方からの故障注入法に関する基礎検討
○岡本拓実・藤本大介・林　優一（奈良先端大）・本間尚文（東北大）

HWS-14. 選択音を用いたスマートデバイスからの電磁波を通じた音情報漏えい評価
○仁科泉美・藤本大介・林　優一（奈良先端大）

B-2 : ISEC（2）：204（13：10〜14：40）

ISEC-15.〔招待講演〕 Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model
Tsunekazu Saito・Keita Xagawa・○Takashi Yamakawa（NTT）

ISEC-16.〔招待講演〕 Obfustopia Built on Secret-Key Functional Encryption
○Fuyuki Kitagawa（Tokyo Inst. of Tech.）・Ryo Nishimaki（NTT）・Keisuke Tanaka（Tokyo Inst. of Tech.）

ISEC-17.〔招待講演〕 Memory Lower Bounds of Reductions Revisited　○Yuyu Wang（Tokyo Inst. of Tech./AIST/IOHK）・Takahiro Matsuda・Goichiro Hanaoka（AIST）・Keisuke Tanaka（Tokyo Inst. of Tech.）

C-2 : CSEC（2）：207（13：10〜15：15）

18. インターネット依存社会における情報発信者・情報送信機器の匿名性と特定・追跡性
○才所敏明・辻井重男（中大）

19. 複数回にわたる匿名加工情報の提供に対する再識別リスク評価方法：PWSCUP2017 における安全性指標の考察と分析から　○チャン クワン カイ・坂本一仁・松永昌浩（セコム）

20. 経営マネジメント状況による情報漏洩インシデント削減効果の評価
○山田道洋・池上和輝・菊池浩明・乾　孝治（明大）

21. セーフティ機能のセキュリティ脅威に対する効果の分析　大久保隆夫（情報セキュリティ大）

22. 金融サービスのセキュリティに対する量子コンピュータの影響と今後の暗号の移行について
宇根正志（日本銀行）

A-3 : SITE（1）：201，202（15：25〜16：40）

SITE-23. セキュリティ意識の向上を目的としたサーバ侵入演習の実践と評価　鈴木大助（北陸大）

SITE-24. ブロックチェーンを利用した匿名性と追跡可能性を有する公共 Wi-Fi 認証方式
三田智之・○稲葉宏幸（京都工繊大）

SITE-25. 利息を記録可能な仮想通貨管理プログラムの設計　○金子雄介（三井住友 FG／日本総研）・長田繁幸（日本総研）・安土茂亨（ハウインターナショナル）・岡田仁志（NII）・山崎重一郎（近畿大）

B-3 : ISEC（3）：204（15：25〜17：05）

ISEC-26. Degenerate Curve Fault Attack on Base Point Decompression and Application to the Bitcoin Curve
○Akira Takahashi（Kyoto Univ.）・Mehdi Tibouchi・Masayuki Abe（NTT）

ISEC-27. RSA 暗号の部分鍵導出攻撃の拡張　○鈴木海地・高安　敦・國廣　昇（東大）

ISEC-28. カード組を用いた秘匿ランキング計算
○高島　健・阿部勇太・佐々木達也・宮原大輝（東北大）・品川和雅（東工大）・水木敬明・曽根秀昭（東北大）

ISEC-29. まぜるな危険準同型暗号を用いた医療データに対する χ^2 独立性検定
○江村恵太・林　卓也（NICT/JST）・陸　文傑（筑波大／JST）・盛合志帆（NICT/JST）・佐久間　淳（筑波大／JST／理研）・山田芳司（三重大／JST）

C-3 : CSEC（3）：207（15：25〜17：05）

30. 権限の変更に着目した権限昇格攻撃防止手法の ARM への拡張　○吉谷亮汰・山内利宏（岡山大）

31. SELinux CIL を利用した不要なポリシ削減手法の提案　○齋藤凌也・山内利宏（岡山大）

32. ランダムパルス発生器 Atomic Pulse Generator の確率密度モデルと適合度検定
○近藤龍一・五十嵐保隆・金子敏信（東京理科大）

33. KLEE と Libfuzzer を組み合わせたハイブリッド型 KleeFuzzer に関する提案
○三嶋秀宗・中沢　実・西川幸延（金沢工大）

26 日午前　A-4 : SPT : 201，202（9：30〜10：45）

1. プライバシ保護設定推測における推測値の平行シフトが受容度に与える影響　○中村　徹（ATR）・アダムス アンドリュー A.（明大）・清本晋作（KDDI 総合研究所）・村田　潔（明大）・鈴木信夫（ATR）

2. プライバシー保護技術の事業活用に関する一考察　○杉尾信行・青野　博・関野公彦（NTT ドコモ）

3. 日本人が付けるパスワードの特性調査と他国データとの比較　愛野乃子・○金岡　晃（東邦大）

B-4 : EMM : 204（9：30〜10：20）

EMM-4. 手品のトリックにみる情報ハイディングのヒント　青木直史（北大）

EMM-5. 音響波形の下位ビット置換による情報秘匿の有無検出における高周波数成分の影響

西村　明（東京情報大）

C-4 : CSEC（4）：207（9：30〜11：10）

6. マルウェア対策のための研究用データセット—MWS Datasets 2018—　○高田雄太（NTT）・寺田真敏（日立）・松木隆宏（FFRI）・笠間貴弘（NICT）・荒木粧子（ソリトンシステムズ）・畑田充弘（NTT コミュニケーションズ）

7. シンボリック実行を活用したマルウェア解析作業の効率化の研究
　○窪　優司・大久保隆夫（情報セキュリティ大）

8. サイバー攻撃を観測するセンサーの設置手法と分析手法に関する検討
　○芦野佑樹・鮫島礼佳・矢野由紀子・島　成佳（NEC）・中村康弘（防衛大）

9. サイバー攻撃を目的とした通信の分類手法の提案
　○鮫島礼佳・芦野佑樹・矢野由紀子・島　成佳（NEC）・中村康弘（防衛大）

A-5 : SITE（2）：201，202（11：20〜12：35）

SITE-10. モバイル周波数保有に関する政府・規制当局の方針：米国及び欧州の事例
　山條朋子（KDDI 総合研究所）

SITE-11. 機械学習における著作権権利制限に関する一考察—改正法案の検討—
　○加藤尚徳（KDDI 総合研究所）・鈴木正朝（新潟大／理研）・村上陽亮（KDDI 総合研究所）

SITE-12. 確率測度空間に於いて脱構築装置を内在するアクセス制御について
　○森住哲也・木下宏揚（神奈川大）

B-5 : ICSS : 204（11：20〜12：35）

ICSS-13. 楕円ペアリングを用いた放送型暗号によるグループ鍵共有プロトコルの提案と実装
　○渡邊建太・三嶋美和子（岐阜大）

ICSS-14. 非負値 Tucker 分解を用いたリアルタイムボットネット検知システムの構築　○金原秀明・村上佑磨（早大）・島村隼平（クルウィット）・高橋健志（NICT）・村田　昇（早大）・井上大介（NICT）

ICSS-15. A Machine Learning-based Approach for Identifying Applications from Encrypted Traffic
　○William Gounot（Kobe Univ./INSA Lyon）・Akito Nishizawa・Yoshiaki Shiraishi・Masakatu Morii（Kobe Univ.）

C-5 : CSEC（5）：207（11：20〜12：10）

16. FPGA インスタンスを用いたクラウドログ異常検知の実装と評価
　○千田拓矢・杉尾信行・青野　博・関野公彦（NTT ドコモ）

17. ファイルサーバーにおける HIDS の適用研究　○宮脇一晃・辰己丈夫（放送大）

26 日午後　A-6 : HWS（2）：201，202（13：45〜15：50）

HWS-18. 市販の暗号鍵管理デバイスに関する考察　○磯部光平・長谷川佳祐・伊藤忠彦（セコム）

HWS-19. Compensation of Flipping-Bits of CMOS SRAM PUF by Adaptive Body-Bias
　○Xuanhao Zhang・Xiang Chen・Hirofumi Shinohara（Waseda Univ.）

HWS-20. XOR 型 PUF のサイドチャネル対策手法とその評価　○野崎佑典・吉川雅弥（名城大）

HWS-21. Fuzzy Extractor の誤り訂正回路に対するサイドチャネル攻撃
　○後藤裕太・汐崎　充・藤野　毅（立命館大）

HWS-22. パス遅延故障に基づくハードウェアトロイの系統的挿入法とその評価
　○伊東　燦・上野　嶺・本間尚文・青木孝文（東北大）

B-6 : ISEC（4）：204（13：45〜15：50）

ISEC-23. 多素数法に基づく多変数公開鍵暗号方式（MPKC）の提案—耐量子コンピュータ暗号の実現に向けて—
　○辻井重男・藤田　亮・五太子政史（中大）

ISEC-24. A New Embedding Method for Generalized LWE
　○Weiyao Wang・Yuntao Wang・Atsushi Takayasu・Tsuyoshi Takagi（Univ. of Tokyo）

ISEC-25. 安全性を高めた共通鍵暗号の量子アルゴリズムに対する詳細な安全性評価
　安井　捷・○國廣　昇（東大）

ISEC-26. 反復性のある鍵相関を用いた WPA-TKIP に対する平文回復攻撃　○伊藤竜馬・宮地充子（阪大）

ISEC-27. 多機関参加型の汎用的な秘匿積集合演算の構成　○宍戸克成・林　基・宮地充子（阪大）

C-6 : CSEC（6）：207（13：45〜15：25）

28. 非対称秘密分散法に適した秘密情報の検証方法　○今井理人・岩村恵一（東京理科大）

29. 実数上の秘密計算手法における計算精度評価方法　金岡　晃（東邦大）

30. 1 台のサーバで実行可能な秘密分散法を用いた秘匿計算法
　○山根将司・岩村恵市（東京理科大）・安田裕之（東大）

31. 2 ビット毎に大小比較を行う暗号文出力型の秘匿比較方式の提案　○小林拓美・伯田恵輔（島根大）

◎全体企画セッション　これからの夏のセキュリティワークショップ開催に向けて（16：00〜16：30）

◎25 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．詳細及び申込み方法は後日公開します．

◆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 7 日（金） 機械振興会館〔未定〕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.
https://www.ieice.org/jpn/ken/kenmoushikomi.html
【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】
芳賀高洋
TEL〔058〕279-6784
E-mail：site-contact@mail.ieice.org
◎公式 Web サイト
http://www.ieice.org/ess/site/
☆HWS 研究会
【問合先】
三浦典之（神戸大）・国井裕樹（セコム）
E-mail：hws-admin@mail.ieice.org
☆ICSS 研究会
【問合先】
白石善明（神戸大）
E-mail：icss-adm-req@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 27 日（木），28 日（金） ビーコンプラザ（別府国際コンベンションセンター）〔7 月 9 日（月）〕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.
https://www.ieice.org/jpn/ken/kenmoushikomi.html