## ★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

**日時**　3月2日（月）　9：40～16：40
　　3日（火）　9：10～16：40
**会場**　沖縄県青年会館（那覇市久米 2-15-23. モノレール旭橋駅下車徒歩 5 分. http://www.okiseikan.or.jp/user.php?CMD=1154016000000　TEL〔098〕864-1780）
**議題**　セキュリティ，トラスト，一般

**2 日午前　ICSS（1-1）**

ICSS-1. サイバーセキュリティの定量的な評価に基づくバックアップ戦略に関する考察
　○蓮池大我・満保雅浩（金沢大）
ICSS-2. 設計モデルを用いた情報資産セキュリティ特性の推測手法
　○植田　武・清水孝一・日夏　俊・大松史生（三菱電機）
ICSS-3. 5 人の管理者の場合の複数割り当て法による情報比の評価　○新間祐太郎・栃窪孝也（日大）

**ICSS（1-2）（11：10～12：10）**

ICSS-4. Alloy Analyzer を活用した Infrastructure as Code の正当性検証　○長谷　亮・松浦陽平（三菱電機）
ICSS-5. LED の個体識別における温度変化の影響　○土屋彩夏・藤　聡子・李　陽・崎山一男・菅原　健（電通大）
ICSS-6. ブロックチェーンを用いたログ保存システム
　○池田貴志・廣友雅徳（佐賀大）・福田洋治（近畿大）・毛利公美（岐阜大）・白石善明（神戸大）

**2 日午後　ICSS（1-4）（13：30～14：50）**

ICSS-7. ファームウェアに着目した IoT 機器のセキュリティ機能の調査
　○白石周碁・福本淳文（岡山大）・塩治榮太朗・秋山満昭（NTT）・山内利宏（岡山大／JST さきがけ）
ICSS-8. ニューラル機械翻訳モデルを用いた異なるアーキテクチャ間における類似バイナリコードの検索
　○青柳守俊・辻　秀典・橋本正樹（情報セキュリティ大）
ICSS-9. AddressSanitizer を併用したデバイスドライバに対するファジングの有効性検証
　○石井健太郎（神戸大）・伊沢亮一（NICT）・森井昌克（神戸大）
ICSS-10. ランサムウェア感染時の復旧対策ツールの開発【続報】
　○古門良介（神戸大）・池上雅人・長谷川智久・原田隆史・木谷　浩（キヤノン MJ）・森井昌克（神戸大）

**ICSS（1-6）（15：00～16：40）**

ICSS-11. IoT 機器の通信機能を起点としたバックドア検知手法の提案　○依田みなみ・櫻庭秀次・山本純一（電通大）・清　雄一（電通大／JST さきがけ）・田原康之・大須賀昭彦（電通大）
ICSS-12. Android に対する JavaScript を用いたサイドチャネル攻撃
　○杉田敬亮（神戸大）・伊沢亮一（NICT）・森井昌克（神戸大）
ICSS-13. ダークネット観測における大規模スキャナの判定指標の提案
　○遠藤由紀子・森　好樹（NICT）・島村隼平（クルウィット）・久保正樹（NICT）
ICSS-14. 広域スキャンとダークネット観測に基づく IoT マルウェア感染状況の分析
　○森下　瞬・小川航汰・田辺瑠偉・吉岡克成・松本　勉（横浜国大）
ICSS-15. Mirai はあなたがスマートスピーカーに話しかけたかわかる―ホームルータに侵入した攻撃者によるプライバシ侵害について―　○奥田翔也・玉井達也・藤田　彬・吉岡克成・松本　勉（横浜国大）

**3 日午前　ICSS（2-1）（9：10～10：30）**

ICSS-1. HTTP リクエストの調査と偽の User-Agent 値の識別方法の提案
　○井上仁人・橋本正樹（情報セキュリティ大）
ICSS-2. Web 上のリアルタイム情報を利用した WAF シグネチャ生成の初期検討
　○熊崎真仁・長谷川皓一・山口由紀子・嶋田　創（名大）
ICSS-3. 全ポート待受型の簡易 TLS ハニーポットにより観測されたサイバー攻撃の分析
　○牧田大佑（NICT）・島村隼平（clwit）・久保正樹・井上大介（NICT）
ICSS-4. 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（2-2）（10：40～12：00）**

ICSS-5. ダークウェブ上に蔓延する違法有害情報の自動分類エキスパートシステムの開発
　○小林華枝・橋本正樹（情報セキュリティ大）
ICSS-6. 様相 $\mu$ 計算による RNN のモデル検査　○青島達大・碓井利宣（NTT）
ICSS-7. ニューラル機械翻訳システムに対する敵対的攻撃　○坂本岳史・森　達哉（早大）
ICSS-8. Adversarial Beats : Spoofed Arrhythmia in Automated ECG Diagnosis

○Taiga Ono（Waseda Univ.）・Takeshi Sugawara（UEC）・Tatsuya Mori（Waseda Univ.）

3 日午後　ICSS（2-4）（13：10〜15：10）

9. ICSS 特別企画セッション

ICSS（2-5）（15：20〜16：40）

10. マルウェアの動的解析におけるログ出力が停止する現象の実態調査
○森本康太・鄭　俊俊・瀧本栄二（立命館大）・齋藤彰一（名工大）・毛利公一（立命館大）

ICSS-11. 悪性スクリプト検出のための活動痕跡の大規模実態調査
○碓井利宣（NTT／東大）・幾世知範・川古谷裕平・岩村　誠・三好　潤（NTT）・松浦幹太（東大）

ICSS-12. 効果的な single-sided RAMBleed の提案
長濱拓季（神戸大）・瀧田　愼（兵庫県立大）・○廣友雅徳（佐賀大）・森井昌克（神戸大）

ICSS-13. 脆弱性記述に基づく脆弱性特性の自動評価　○中川舜太（神戸大）・古本啓祐（NICT）・白石善明（神戸大）・瀧田　愼（兵庫県立大）・毛利公美（岐阜大）・森井昌克（神戸大）

2 日午前　SPT（1-1）（9：40〜11：00）

1. 情報セキュリティ意識における楽観主義バイアスの影響分析　○宮地勇作・小松文子（長崎県立大）

2. 個人のリスク認知と情報セキュリティ対策行動　田﨑来実（長崎県立大）

3. 児童を対象としたパスワードに関する知識・行動の日米比較研究
○坪根　恵・森　啓華（早大）・長谷川彩子・秋山満昭（NTT）・森　達哉（早大）

4. バーチャル YouTuber 技術を用いたセキュリティ教育コンテンツの作成　○中山実咲・上原哲太郎（立命館大）

ICSS（1-3）（11：10〜12：10）

ICSS-5. 脆弱性情報の自動監視に基づく警告・初動対応自動化技術の構築
高橋健志・○牛込龍太郎・鈴木未央・井上大介（NICT）

ICSS-6. セキュリティ通知における連絡先の有効性評価
○斉藤美織・田辺瑠偉・藤田　彬・吉岡克成・松本　勉（横浜国大）

ICSS-7. コンテンツフィルタを回避する敵対的映像データ　○大森敬仁・森　達哉（早大）

2 日午後　ICSS（1-5）（13：30〜14：50）

ICSS-8. アグリゲートメッセージ認証方式の実証システムの評価　○山岸篤弘・武内良男（ジャパンデータコム）・竹久達也・西浦英一・鄒　家発（ニッシン）・今村　祐（ジャパンデータコム）・四方順司（横浜国大）・廣瀬勝一（ジャパンデータコム）・中尾康二（横浜国大）・石田祐子・今井秀樹・平田康夫（ジャパンデータコム）

ICSS-9. ハッシュチェーンアグリゲーションを用いた認証方式の拡張　○平井晨太・双紙正和（広島市大）

ICSS-10. ストリーム暗号 Salsa20/ChaCha における逆関数の特性を用いた安全性解析
○松岡勇介・宮地充子（阪大）

ICSS-11. 低出力局所性を持つ効率的で高機能なコミットメント方式　○宮地秀至・宮地充子（阪大）

2 日午後　SPT（1-2）（13：00〜14：40）

12. ドローンにおけるセーフティ分析とセキュリティ分析の統合リスク分析　○和田健治・小松文子（長崎県立大）

13. オストリッチ ZIP の総合的リスクアセスメント　中山道裕・○金岡　晃（東邦大）

14. フェイクニュースによるだまされやすさと対策の基本検討
○佐藤　直・辻井重男・白鳥則郎・山口　浩・才所敏明・趙　晋輝・五太子政史（中大）・近藤　健（セキュア IoT プラットフォーム協議会）・山澤昌夫・山本博資（中大）

15. エンドユーザはフィッシングサイトを見破ることができるか？視線追跡装置と半構造化インタビューを用いたユーザ行動分析　○シュウ インゴウ・森　啓華・櫻井悠次・坪根　恵・飯島　涼（早大）・坂本一仁（DataSign）・島岡政樹（セコム）・森　達哉（早大）

16. Brand Validation 証明書の提案及び評価―Web サイトのアイデンティティ表示の改善―
○奥田哲矢・千葉直子・秋山満昭・福永利徳・鈴木亮平（NTT）・神田雅透（情報処理推進機構）

3 日午前　SPT（2-1）（9：10〜10：30）

1. 半教師ありトピックモデルによるセキュリティレポートの分類について
○杉本健太・長田侑樹（神戸大）・瀧田　愼（兵庫県立大）・古本啓祐（NICT）・白石善明（神戸大）・高橋健志（NICT）・毛利公美（岐阜大）・髙野泰洋・森井昌克（神戸大）

2. セキュリティレポートの時系列トピックモデルを用いた分析　○長澤龍成（神戸大）・古本啓祐（NICT）・瀧田　愼（兵庫県立大）・白石善明（神戸大）・高橋健志（NICT）・毛利公美（岐阜大）・髙野泰洋・森井昌克（神戸大）

3. Automatic extraction of Indicators of Compromise from unstructured technical reports
○THEINTHIN THARAPHE・江澤友基・中川舜太（神戸大）・古本啓祐（NICT）・白石善明（神戸大）・毛利公美（岐阜大）・森井昌克（神戸大）

ICSS-4. トピックモデルとクラスタリングによるセキュリティレポートのマルチラベル分類
○長田侑樹（神戸大）・瀧田　愼（兵庫県立大）・古本啓祐（NICT）・白石善明（神戸大）・高橋健志（NICT）・毛

利公美（岐阜大）・髙野泰洋・森井昌克（神戸大）

3日午前　ICSS（2-3）（10：40～12：00）

ICSS-5. スマートコントラクトを用いた安全なセカンドプライスオークションの提案
○杉谷勇気・宮地充子（阪大）

ICSS-6. セッション型を用いたアクセス制御システムの評価　○西口朋哉・高野祐輝・宮地充子（阪大）

ICSS-7. 属性ベース暗号を用いたプライバシポリシーの実現方法とその応用　○林　基・宮地充子（阪大）

ICSS-8. ブロックチェーンを用いた認可プロトコルの一実装　○江澤友基（神戸大）・掛井将平（名工大）・白石善明（神戸大）・瀧田　愼（兵庫県立大）・毛利公美（岐阜大）・森井昌克（神戸大）

3日午後　ICSS（2-6）（15：20～16：40）

9. 属性ベース暗号方式を用いたFIDO2の拡張による代理認証の実現
○大川悠人・猪俣敦夫・上原哲太郎（立命館大）

ICSS-10. Compact and secure elliptic curve scalar multiplication based on affine
○Jin Yaoan・Atsuko Miyaji（Osaka Univ.）

ICSS-11. ベクトル命令によるCurve25519の高速実装　○Chenyu Wang・Tung Chou・宮地充子（阪大）

ICSS-12. 楕円曲線に基づく匿名公開鍵証明書の実装の検討　大石和臣（静岡理工科大）

◆情報処理学会；セキュリティ心理学とトラスト研究会連催

【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