★情報セキュリティ研究会 (ISEC)

専門委員長 小川一人 副委員長 藤岡 淳・盛合志保 幹事 水木敬明・大東俊博 幹事補佐 江村恵太・駒野雄一・須賀祐治

★技術と社会・倫理研究会(SITE)

専門委員長 岡田仁志 副委員長 森住哲也・小川 賢 幹事 芳賀高洋・川口嘉奈子 幹事補佐 壁谷彰慶・加藤尚徳

★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 植田 武・高倉弘喜 幹事 吉岡克成・神谷和憲 幹事補佐 笠間貴弘・山田 明

★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 日置尋久・栗林 稔 幹事 生源寺 類・藤吉正明 幹事補佐 姜 玄浩・村田晴美

日時 7月14日(金) 10:05~17:00 15日(土) 10:15~15:05

会場 内田洋行東京本社ショールーム「ユビキタス協創広場 CANVAS」(中央区新川 2-4-7. JR 京葉線:八丁堀駅, 徒歩 6 分, 東京メトロ日比谷線:八丁堀駅, 徒歩 4 分, 東京メトロ日比谷線/東西線:茅場町駅, 徒歩 5 分. http://www.uchida.co.jp/company/showroom/canvas/tokyo/ TEL〔0120〕077-266(内田洋行ショールームお客様相談センター) 芳賀高洋(岐阜聖徳学園大))

議題 セキュリティ, 一般

14 日午前 SITE セッション 1 (10:05~11:45)

SITE-1. 周波数領域におけるパッチワーク方式を用いた動画像電子透かしの性能評価

○木村崇也·稲葉宏幸 (京都工繊大)

SITE-2. プライバシーを考慮したブロックチェーン技術によるディジタルコンテンツ転々流通システムの改良

○三浦広平・稲葉宏幸(京都工繊大)

SITE-3. プライバシー問題における信頼の役割 大谷卓史(吉備国際大)

SITE-4. 多層行為論理の意味論的性質 村上祐子(東北大)

CSEC セッション1 (10:15~11:30)

- 5. サイト関連情報に基づいた Web サイト脅威度推定機能の提案 ○藤井翔太・鬼頭哲郎・重本倫宏 (日立)
- 6. 長期間に渡るインターネットノイズの観測に基づいたサイバー攻撃活動の初期段階で用いられる発信源分類手法の 提案 ○芦野佑樹・山根匡人・矢野由紀子・島 成佳 (NEC)
- 7. MDS を用いた結託型走査グループの活動状況の分析手法 ○梶川慶太・中村康弘 (防衛大)

ICSS セッション1(10:15~11:05)

ICSS-8. ユーザ環境における RIG Exploit Kit の実態調査方法の提案 ○嶌田一郎・太田敏史(構造計画研)

ICSS-9. 高機能暗号の社会実装に係る課題の抽出 ○国井裕樹・伊達浩行(セコム)

14 日午後 SPT セッション 1 (13:25~14:40)

10. 企業統計業務の電子投票による効率化提案

林 達也 (慶大/レピダム)・〇水越一郎 (NTT 東日本/情報セキュリティ大)

- 11. リレーアタックに耐性を持つインタラクティブな動画 CAPTCHA 方式の検討
 - ○立田怜平・山場久昭・油田健太郎(宮崎大)・朴 美娘(神奈川工科大)・岡崎直宣(宮崎大)
- 12. 表面筋電位による個人認証システム実現のための相互相関係数を用いた個人識別手法の検討
 - ○黒木聡舜・山場久昭・油田健太郎(宮崎大)・朴 美娘(神奈川工科大)・岡崎直宣(宮崎大)

CSEC セッション 2 (13:25~16:10)

- 13. 金融分野における高機能暗号の活用と今後の課題 宇根正志 (日銀)
- 14. 高機能暗号の金融分野での応用に関する考察

○清藤武暢(日銀金融研)青野良範(NICT)四方順司(横浜国立大)

15. RWC2017 参加報告 須賀祐治 (インターネットイニシアティブ)

ICSS セッション1 (13:25~14:40)

ICSS-16. ドライブ・バイ・ダウンロード攻撃によるインシデントを再現するフォレンジック調査のための支援システム ○奥田裕樹・福田洋治・井口信和(近畿大)・白石善明(神戸大)

ICSS-17. DBI を用いたランサムウェアのファイルアクセス解析の一検討 ○与那嶺 俊・門林雄基(奈良先端大)

ICSS-18. リンク構造に基づく Web サイトのクラスタリングと悪性サイトの識別

〇永井達也(神戸大)・神薗雅紀 (PwC サイバーサービス)・白石善明 (神戸大)・毛利公美 (岐阜大)・高野泰 洋・森井昌克 (神戸大)

ISEC セッション1 (15:20~17:00)

ISEC-19. Presentation of fundamental schemes for augmenting several public key cryptosystems Masao Kasahara (Waseda Univ.)

ISEC-20. 2^m-ary 法に基づく誤りつき演算情報を用いた CRT-RSA 秘密鍵復元アルゴリズム ○大西健斗・國廣 昇 (東大)

ISEC-21. DeepLLL を用いた解読報告 〇山口純平 (九大)・安田雅哉 (IMI)

ISEC-22. PUF を用いる認証方式について ○駒野雄一(東芝)・岩本 貢・太田和夫(電通大)

SITE t = 20 - 16 = 35

SITE-23. Considering usability in the discussions about central bank issued digital currency

OVanessa Bracamonte · Hitoshi Okada (NII)

SITE-24. テクストの相互情報量により非文字オントロジー間を接続する概念の提案とそのケーススダディ―潜在的テクストを確率変数として見る場合― 〇宋 先波・森住哲也・木下宏揚(神奈川大)

SITE-25. 秘密保護法と情報処理 小池 誠 (マイクロ特許)

CSEC セッション3 (15:20~17:00)

- 26. Use-After-Free 脆弱性攻撃防止手法におけるメモリ解放契機の評価 〇伴 侑弥・山内利宏 (岡山大)
- 27. プロセス管理表へのアクセス制御機能の評価 ○佐藤将也・山内利宏・谷口秀夫(岡山大)
- 28. TLS サーバ証明書の冗長化技術の提案とそのプロトタイプ実装 山本 宏・金岡 晃 (東邦大)・岡田雅之 (日本ネットワークインフォメーションセンター/東邦大)
- 29. 覗き見耐性を持つマウス操作を用いた個人認証方式の提案

○長友 誠(神奈川工科大)・喜多義弘(東京工科大)・朴 美娘(神奈川工科大)・岡崎直宣(宮崎大)

15 日午前 SPT セッション 2 (10:15~11:55)

1. 情報セキュリティ疲れ:情報セキュリティコンディションマトリクスの提案 ○畑島 隆 (NTT)・谷本茂明 (千葉工大)・金井 敦 (法政大)

2. Android アプリケーションにおける Runtime Permission 要求時の挙動調査 河合佑紀・明田修平(立命館大)・半井明大・窪田 歩(KDDI 総合研究所)・瀧本栄二・○毛利公一(立命館大)

3. クラウドソーシングを利用した Usable Security and Privacy 研究に関する考察 金岡 晃 (東邦大)・○島岡政基 (セコム)

4. ユーザのサイト真偽判断行動と思考特性との関係性の検討 小倉加奈代(岩手県立大)

SITE セッション3(10:15~11:55)

SITE-5. 初中等教育における著作権教育の再考—中学校での権利処理に関する教育実践—

○芳賀高洋(岐阜聖徳学園大)・我妻潤子・臼井洋子(シュバン)・大谷卓志(吉備国際大)・小野永貴(日大)・鈴木二正(慶應幼稚舎)・高瀬浩之(和名ケ谷中)・塚本初恵(ICT工房)・豊福晋平(GLOCOM)・中駄康博(富士ソフト)・西尾琢郎(桜台小)・森棟隆一(白百合中高)・三輪吉和(学習開発研)・工藤紗貴子(文理)・渡辺光輝(お茶の水女子大附属中)

SITE-6. IT Enabled Service の展開―地域活性への取り組みについて― 上杉志朗(松山短大)

SITE-7. 広域地域ブランドの価値評価法に関する考察―マクロ経済学的観点から― 森田正大(松山大)

SITE-8. マルチエージェント・シミュレーションを用いた地域ブランド価値の評価に関する考察 森田正大(松山大)

CSEC セッション4 (10:15~11:30)

9. 演算の連続に対して安全な秘密分散法を用いた秘匿計算

○Mohd Kamal Ahmad Akmal Aminuddin・岩村恵市(東京理科大)

- 10. 仮名化による個人情報の保護に配慮したパブリッククラウド型フィッシングメール対応訓練システムの開発 ○東野正幸・川戸聡也・大森幹之・川村尚生(鳥取大)
- 11. 2016 年における個人情報漏えいインシデント調査とその分析 〇加藤雅彦・小松文子(長崎県立大)

EMM セッション1 (13:25~14:40)

EMM-12. Investigation of spikegram-based signal representation for speech fingerprints ODung Kim Tran • Masashi Unoki (JAIST)

EMM-13. ステガノグラフィ (ANGO) と局所特徴量を用いたテンプレートマッチングにおけるノイズ耐性の比較について ○石塚裕一(三菱電機)・越前 功 (NII)・岩村恵市(東京理科大)・櫻井幸一(九大)

EMM-14. 次世代シーケンサーデータへの情報埋め込み 高木基成(サントリーシステムテクノロジー)

ISEC セッション2 (13:25~15:05)

ISEC-15. スマートフォンを利用した視覚復号型秘密分散法による個人認証方式の提案

○水野 涼・稲葉宏幸(京都工繊大)

ISEC-16. TEE システムアーキテクチャとそのオープンソース実装のセキュリティ評価

○吉田直樹 (横浜国大)・福島和彦・宮内成典 (ルネサス エレクトロニクス)・坂本純一・藤本大介・松本 勉 (横浜国大)

ISEC-17. 高機能暗号向け Zynq 利用コプロセッサ開発環境とその評価 ○三好孝典・松本 勉 (横浜国大)

ISEC-18. 軽量なセキュアクラウドストレージのための Proof Of Retrievability

○トラン フン タオ (KDDI 総合研究所)・面 和成 (筑波大)

- ◆情報処理学会;コンピュータセキュリティ研究会/情報セキュリティ心理学とトラスト研究会連催
- ◎本プログラムは本内容を記載した時点(2017/05/22)では暫定的な内容であり、今後セッションが追加され、それに伴い個々の発表の時間帯が現在のものから別の時間帯に移る可能性があります。
- ◎現在記載されている各セッションのほか, 現在招待講演についての企画中です.
- ◎懇親会が企画されています. 詳細は決定後各研究会より告知致します.

☆ISEC 研究会今後の予定 〔 〕内発表申込締切日

9月4日(月) 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.

http://www.ieice.org/jpn/ken/kenmoushikomi.html

【問合先】

水木敬明 (東北大)

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

☆SITE 研究会

【問合先】

多川孝央

TEL (092) 802-2645

E-mail: site-contact@mail.ieice.org

◎公式 Web サイト

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

☆ICSS 研究会

【問合先】

三宅 優 (KDDI 総合研究所)

TEL (049) 278-7367, FAX (049) 278-7510

E-mail: icss-request@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