

●第2回情報通信システムセキュリティ研究会 (ICSS)

専門委員長 中尾康二 (KDDI、NICT)

副委員長 菊池浩明 (東海大)・櫻井幸一 (九州大)

日時 平成18年4月14日(金) 10:30~16:40

会場 鳴門教育大学 地域連携センター・多目的教室

(鳴門市鳴門町高島字中島 748 番地、

<http://www.naruto-u.ac.jp/shyomu/ss-akusesu.htm>

<http://www.naruto-u.ac.jp/shyomu/ss-tatemonohaiti.htm>)

参加費 一般 3,000 円 学生 1,000 円

参加申込 4月12日までに、下記の参加申込・問い合わせ先までメールでお申込み下さい。なお、事前にお申込み頂かなかった場合、当日の参加者数によっては予稿集をお渡しできない場合がございますので御了承下さい。

参加資格 特になし

研究会の内容

情報通信システムセキュリティ研究会 (ICSS) は、暗号理論等のセキュリティに関する要素技術だけではなく、システムとしての情報セキュリティに関わるアーキテクチャ等に対して広い視野からの意見交換を行うことができる場を提供することを目的として、平成17年度に新設された新しい研究会です。分散 OS やユビキタス情報環境 (ユビキタスコンピューティング、グリッドコンピューティング等) の新しい技術が普及する兆しが見えてきていますが、これらの分散情報環境に対してもセキュリティを考慮したシステムの構築が求められています。これまでに、暗号理論を中心としたセキュリティ技術に関する研究が活発に行われてきましたが、これらのセキュリティ要素技術を背景として、これからの分散情報環境に適したセキュリティ・アーキテクチャやセキュリティ・プロトコルなどのシステム・アーキテクチャの視点に立った情報通信システムに対するセキュリティ研究の重要性が増してきています。本研究会では、下記の研究分野をターゲットとして幅広いセキュリティ分野における研究の活性化を目指しています。

【研究分野】

{ネットワーク、アドホックネットワーク、P2P、センサーネットワーク、RFID、無線 LAN、モバイル、ホームネットワーク}に関するセキュリティ技術、アクセス制御、コンテンツセキュリティ、DRM、CDN、プライバシー保護、電子商取引、公開鍵認証基盤、セキュリティ・アーキテクチャ、セキュリティ・プロトコル、セキュリティ実装技術、セキュア OS、セキュリティ評価・認証

プログラム

午前

1. ストリーム暗号 Py の鍵回復攻撃に関する一考察
五十部孝典・大東俊博・桑門秀典・森井昌克（神戸大）
2. 結託攻撃に対する耐性を考慮した電子指紋方式
林直樹・栗林稔・森井昌克（神戸大）
3. 定点観測センサー間の相関について
菊池浩明（東海大）・寺田雅敏（日立）

午後

4. IP トレースバック相互接続におけるパケットの秘匿性に関する一考察
樫山寛章・門林雄基（奈良先端科学技術大学院大）・武智洋（横河電機）
5. マーキングを用いたアプリケーショントレースバック MapTB のセキュリティ向上に関する考察
吉岡克成・衛藤将史（NICT）・新井貴之（横河電機）・中尾康二（NICT）
6. DNSSEC の運用展開に関する一考察
力武健次（NICT）・中尾康二（NICT、KDDI）・
下條真司（阪大）・野川裕紀（東京医科歯科大）
7. ウイルス研究基盤の構築
星澤裕二（セキュアブレイン）・森井昌克（神戸大）・中尾康二（KDDI）
8. フィッシング行為を防御するためのネットワーク構築の一検討
原正憲・窪田歩・竹森敬祐・三宅優（KDDI 研）
9. サーバの安全性を IC カードを用いて検証するセキュリティ保証基盤の実装
竹森敬祐・三宅優（KDDI 研）
10. 実世界の信頼関係に基づいた個人ポータル間連携の検討
白神彰則・安部剛・岡本光浩・川島正久・水野修（NTT）
11. ホームネットワークに関するセキュリティ分析
根本繁幸・羽根慎吾・岡山祐孝・田中晶・佐藤洋平・藤城孝宏・手塚悟（日立）

【参加申込・問合せ先】〔幹事〕

E-mail: icss-request@mail.ieice.org

三宅 優（KDDI 研究所）

TEL [049] 278-7367, FAX [049] 278-7510

曾根 直人（鳴門教育大学）

TEL [088] 687-6502, FAX [088] 687-6102

◎最新情報は、情報通信システムセキュリティ時限研究会のホームページをご覧ください。

<http://www.ieice.org/~icss/>

主催 情報通信システムセキュリティ時限研究専門委員会