国際会議 ASIACCS2014 報告

穴田 啓晃[†1]　佐藤 将也[†2]　山内 利宏[†2]　堀 良彰[†3]　盛合 志帆[†4]　櫻井 幸一[†5†1]

†1 公益財団法人九州先端科学技術研究所
〒814-0001 福岡県福岡市早良区 2-1-22 福岡 SRP センタービル 7 階
{anada,sakurai}@isit.or.jp

†2 岡山大学大学院自然科学研究科
〒700-8530 岡山市北区津島中 3 丁目 1 番 1 号
m-sato@swlab.cs.okayama-u.ac.jp, yamauchi@cs.okayama-u.ac.jp

†3 佐賀大学全学教育機構
〒840-8502 佐賀市本庄町 1 丁目
horiyo@cc.saga-u.ac.jp

†4 独立行政法人情報通信研究機構
〒184-8795 東京都小金井市貫井北町 4-2-1
shiho.moriai@nict.go.jp

†5 九州大学大学院システム情報科学研究院
〒819-0395 福岡市西区元岡 744 番地
sakurai@inf.kyushu-u.ac.jp

あらまし ASIACCSは計算機械学会 ACM（Association for Computing Machinery）により年一回アジア及び大洋州地域で開催される，情報セキュリティのトップカンファレンスである．マルウェア，プライバシー保護，認証，暗号等のテーマを含み，現実に影響の大きい最先端技術が発表され論じられる．第9回を数える今回は約180名（過去4年で最高）を集め，投稿255件から採択された50件の選りすぐりの研究論文が発表された．本報告者らは当カンファレンス及び併催ワークショップに運営側また聴講者として参加した．以下，抜粋した数件の発表の内容や所見，また運営や交流について報告する．

A Report on International Conference ASIACCS2014

Hiroaki ANADA[†1]　Masaya SATO[†2]　Toshihiro YAMAUCHI[†2]

Yoshiaki HORI[†3]　Shiho MORIAI[†4]　Kouichi SAKURAI[†5†1]

†1 Institute of Systems, Information Technologies and Nanotechnologies (ISIT)
Fukuoka SRP Center Bldg.7F, 2-1-22, Momochihama, Sawara-ku, Fukuoka-city, 814-0001
†2 Graduate School of Natural Science and Technology, Okayama University
3-1-1,Tsushimanaka,Kita-ku,Okayama-city,700-8530
†3 Organization for General Education, Saga University
1-chome, Honjoumachi, Saga-city, 840-8502
†4 National Institute of Information and Communications Technology (NICT)
4-2-1, Nukui-Kitamachi, Koganei-city, Tokyo, 184-87

†5 Faculty of Information Science and Electrical Engineering, Kyushu University
744, Motooka, Nishi-ku, Fukuoka-city, 819-0395

Abstract ASIACCS is an annual, top-level conference in information security, which is held in the area of Asia and Oceania by ACM (Association for Computing Machinery). Major themes including malware, privacy protection, authentication and encryption are treated and new technologies that will have significant influence are discussed. This year it is the ninth, and about 180 people (the largest in the last four years) attended. 50 peer-reviewed research papers accepted from 255 submissions were presented. We participated in the conference and co-located workshops as organizers and listeners. In this paper we report some remarkable presentations, our interchanges as well as our administration.

1 はじめに

ACM ASIACCS (ACM Symposium on Information, Computer and Communi- cations Security) は，コンピュータ・通信セキュリティに関する国際会議 ACM CCS (ACM conference on Computer and Communi- cations Security) の関連シンポジウムとしてアジア・オセアニア地域で 2006 年から開催が始まった. ASIACCS2014 は 6 月 3 日から 6 日まで京都ガーデンパレスにて開催された. 日本での開催は 2008 年(東京 秋葉原)に続き，2 回目となる.

情報セキュリティ技術の重要性がますます認識され，関連する分野が広がっている昨今，暗号技術のみならず情報セキュリティ技術を幅広くカバーするトップカンファレンスが日本で開催される意義は大きい.

2 ASIACCS2014 概要

本章では，ASIACCS2014 の運営組織，併催ワークショップ，参加者数について述べる.

2.1 ASIACCS2014 の運営組織

運営組織の方々を下記に示す

Steering Committee

- Robert Deng (Chair), SMU, Singapore
- Shiuhpyng Shieh, NCTU, Taiwan
- Elisa Bertino, Purdue University, USA
- Mike Reiter, University of North Carolina at Chapel Hill, USA
- Ninghui Li, Purdue University, USA
- Li Gong, Mozilla Online Ltd., USA
- Vijay Varadharajan, Macquarie University, Australia
- Kouichi Sakurai, Kyushu University, Japan
- Elena Ferrari, University of Insubria, Italy
- Dieter Gollmann, Hamburg University of Technology, Germany
- Yi Mu, University of Wollongong, Australia
- Dong Hoon Lee, Korea University, Korea
- Duncan Wong, City University of Hong Kong, Hong Kong
- Dongdai Lin, Institute of Information Engineering, Chinese Academy of Sciences, China
- Giovanni Russello, University of Auckland, New Zealand
- Atsuko Miyaji, Japan Advanced Institute of Science and Technology, Japan

General Chair

- Shiho Moriai, NICT, Japan（本稿著者）

Program Co-chairs

- Trent Jaeger, Penn State University, USA
- Kouichi Sakurai, Kyushu University, Japan（本稿著者）

2.2 Session 構成

ASIACCS2014 の Session 構成を下記に示す.

- Keynote Speech
- Session 1: Network
- Session 2: Reputation and Location
- Session 3: Processing encrypted data
- Session 4: Applications 1
- Session 5: Crypto
- Session 6: Access control and Flow analysis
- Session 7: Software and Systems security
- Session 8: Applications 2
- Session 9: Authentication
- Session 10: Android
- Session 11: Short 1: Network
- Session 12: Short 2. Software

2.3 併催ワークショップ

ASIACCS2014 に先立ち, 6 月 3 日(火)終日に亘り 5 つのワークショップが併催された.

- 2014 ACM Asia Public Key Cryptography Workshop (ASIAPKC '14)
- Second international workshop on Security and Forensics in Communication Systems (ASIACCS-SFCS 2014)
- The First International Workshop on Information Hiding and its Criteria for evaluation (IWIHC2014)
- Asia Workshop on Security, Privacy and Dependability for CyberVehicle (AsiaCyCAR2014)
- The 2014 International Workshop on Security in Cloud Computing (SCC'14)

2.4 参加者数

ASIACCS2014 の会議への参加者数と, その国別内訳概要を表 1に示す. 29 か国から計 176 名が参加した.

表 1 ASIACCS2014 参加者数

Japan	68	United States	36
China	36	South Korea	13
France	13	Germany	8
Singapore	8	Hong Kong	7
Indonesia	7	Australia	6
Austria	6	Canada	4
Sierra Leone	4	United Kingdom	3
Belgium	3	Czech Republic	2
Denmark	2	Egypt	2
Finland	2	Hungary	2
India	2	Italy	2
Luxembourg	2	Malaysia	2
New Zealand	2	Norway	1
Sweden	1	Switzerland	1
Tunisia	1	—	—

2.5 論文採録状況

論文採録状況を下記に示す.

- 投稿数:255 件／採択数:50 件. 内 short paper が 8 件. 採択率は 19%(例年と同様).

また, 国別の投稿者数と採択者数を表 2に示す. 32 か国から 522 人の著者が投稿し, 内 18 か国の 152 人の論文が採択された.

表 2 ASIACCS2014 国別投稿者数, 採択者数

国	投稿者数	採択者数
US	159	65
China	59	15
Germany	54	10
France	30	11
Italy	25	5
Singapore	24	10
Hong Kong	20	7
UK	13	6
Belgium	13	0
South Korea	13	0
Brazil	12	0
Luxembourg	11	4
Japan	10	0

Australia	9	4
Canada	9	3
Sweden	7	0
India	6	2
Austria	6	3
Greece	5	0
Spain	5	1
Taiwan	5	0
Israel	5	0
Estonia	4	0
Netherlands	4	0
Saudi Arabia	4	0
Hungary	2	1
Finland	2	1
Czech Rep	1	1
Norway	1	1
Denmark	1	1
New Zealand	1	1
Switzerland	1	0

3 Presentation

本章では，著者らが聴講した発表の内から数件を選び，その内容と所感を報告する．

併催ワークショップ（2014 年 6 月 3 日）

ASIAPKC2014

公開鍵暗号をテーマとする本ワークショップ：ACM ASIA Public-Key Cryptography Workshop (ASIAPKC) は今回で第 2 回を数える．2014 年からは DBLP にも掲載されるなど，ステータスが上がってきている．

会場の聴講者は 20 名程度で，活発に議論が行われた．6 件の内の 2 件について報告する．

“Two Applications of Multilinear Maps: Group Key Exchange and Witness Encryption”, S. Arita and S. Handa. ここ数年研究が盛んになってきている多重線型写像についての発表であった．多重線型写像は鍵共有のスキームに適用しやすいことは想像されるが，本発表では期待通りの方向で提案がなされており，かつ，効率の点で先行研究の改善を行っていた．

“Attribute-Based Signatures without Pairings via the Fiat-Shamir Paradigm”, H. Anada, S. Arita and K. Sakurai. 本稿の第一著者による発表であった．双線型写像を使わずに属性ベース署名スキームを構成したことがポイントで，ただし安全性証明はランダムオラクルモデルの下でである．発表後，検証者のチャレンジメッセージの分割が指数オーダに発散しないか質問を頂き，多項式オーダに収まる旨を回答した．

AsiaCyCAR2014

自動車の情報セキュリティは，近年，自動車メーカに加え ICT 企業が加わり，特に車車間通信や自動運転（自律運転）の研究開発などが盛んである．

ACMCCS でも 2013 年にワークショップ CyCar の第 1 回が開催されたが，本ワークショップはその ASIACCS 版とも位置付けられる．第 1 回である今回は，松本勉教授（横浜国大），Dennis Kengo Oka 氏, Camille Vuillaume 氏（両氏共にイータス㈱），松井充氏（三菱電機㈱）の 4 氏からチュートリアル的な講演がなされた．

ASIACCS2014（2014 年 6 月 4 日-6 日）

Keynote: “Fighting Malicious Code - An Eternal Struggle”

招待講演者の Kruegel 氏はマルウェアの解析と検知を専門とする教授であり，同分野で“Lastline Inc.”を起業する等の活発な活動で知られている．講演では情報通信機器の半数以上を現在占めるモバイルデバイスの特徴（計算資源少，またそれゆえクラウド環境に計算を委託する，等）を脆弱性として突いたマルウェアの脅威について解説した．次いで，マルウェアの進化や被害件数が留まらない状況に対し，研究発表の件数が減少している事実に触れ，この分野への研究者の参入を啓発した．

Session 1: Network

“Letting the Puss in Boots Sweat: Detecting Fake Access Points using Dependency of Clock Skews on Temperature”, Fabian Lanze, Andriy Panchenko, Benjamin Braatz, Thomas Engel. 水晶振動子の個々の物理特性に起因し，温度の変化によって無線 LAN アクセスポイントのクロックスキューが異なることを利用し，偽のアクセスポイント

を見つける手法を提案している.

“Covert Ephemeral Communication in Named Data Networking”, Moreno Ambrosin, Mauro Conti, Paolo Gasti, Gene Tsudik.

コンテンツの名前を用いて通信を行う Named Data Networking(NDN)
において，同じコンテンツを利用する利用者間に隠れチャネルが存在することを指摘し，その評価を行っている.

“Scanner Hunter:Understanding HTTP Scanning Traffic”, Guowu Xie, Huy Hang, Michalis Faloutsos.

HTTP サーバの脆弱性を発見するための HTTP スキャンナを検知する Scanner Hunter を提案. HTTPリクエストの記録に対して二部グラフを構築し，クラスタリングにより解析する.

“Detection of Stealthy Malware Activities with Traffic Causality and Scalable Triggering Relation Discovery”, Hao Zhang, Danfeng Yao, Naren Ramakrishnan.

マルウェアはマウスクリックなどの利用者の操作とは独立に動作することに着目し，ネットワークトラヒックと利用者の操作イベントを関連づけるグラフを用いて，マルウェアによるトラヒックを検出する手法を提案している.

“Towards Automated Protocol Reverse Engineering Using Semantic Information”, Georges Bossert, Frédéric Guihéry, Guillaume Hiet.

リバースエンジニアリングにより，ネットワークアプリケーションのメッセージフォーマットを解析する手法の提案. マルウェア解析やボットネット対策に寄与できる.

Session 3: Processing encrypted data

高機能暗号の中でも特にクラウドサーバ上での処理を主題にしたセッションで，5 件の発表があった.

“Privacy of Outsourced k-Means Clustering”, Dongxi Liu, Elisa Bertino, Xun Yi. データの所持者が完全準同型暗号で暗号化したデータを，k-平均法でクラスタリングする際の，暗号化された距離情報の扱いについて論じた発表であった. 所持者にトラップドアを持たせることで距離の比較を可能としている.

Session 4: Applications 1

3 件の発表が行われ，活発な議論が行われた.

"On the Effectiveness of Risk Prediction Based on Users Browsing Behavior", Davide Canali, Leyla Bilge, Davide Balzarotti. Canali らの発表では，Web 閲覧履歴の解析のみにより，Web 攻撃を受けやすいユーザの傾向を分析していた. 分析では HTTP ヘッダを用いた機械学習により，Web 閲覧傾向と攻撃を受ける可能性についての相関が示されていた. この対策は HTTP ヘッダを利用しているため，クライアントやサーバだけでなく ISP が対策に参加できる点が実用的であると感じた.

"Protecting Users Against XSS-based Password Manager Abuse", Ben Stock, Martin Johns. Stock らの発表では，Web ブラウザが持つパスワードマネージャを悪用したパスワード取得攻撃の可能性を示し，その対処を示していた. 攻撃例として，パスワードマネージャによるパスワード自動入力をクロスサイトスクリプティングにより悪用し，パスワードを攻撃者のサーバに送信させる攻撃がある. 攻撃への対処では，パスワード欄には生成した乱数を入力しておき，パスワードを送信する前に，Web サイトのオリジンやパラメータを解析する. 解析結果に基づき，正規の Web サイトに対して許可したリクエストの場合か否かを判定し，パスワード送信の条件に合致する場合のみ正規のパスワードを含むリクエストを送信する手法が提案されていた.

"A Three-Way Investigation of a Game-CAPTCHA: Automated Attacks, Relay Attacks and Usability", Manar Mohamed, Niharika Sachdeva, Michael Georgescu, Song Gao, Nitesh Saxena, Chengcui Zhang, Ponnurangam Kumaraguru, Paul C. Oorschot, Wei-Bang Chen. Mohamed らの発表では，ゲーム CAPTCHA の一つである Dynamic Cognitive Game (DCG) CAPTCHA による認証について，画像処理技術により自動的に突破する方法，リレーアタック，およびユーザビリティについて考察が示されていた. リレーアタックは，CAPTCHA をインターネット上の一般利用者に解決させ，その結果を利用して CAPTCHA を突破する攻撃方法である.

Mohamed らの報告では，DCG CAPTCHA は，リレーアタックに一定の耐性を持ち，高いユーザビリティを持つことが確認されていた．しかし，Mohamed らの画像処理プログラムは，DCG CAPTCHA を突破できると示されており，DCG CAPTCHA をより強固にするには，画像処理の時間が長くなるように巨大な画像を利用するか，タイムアウト時間を短く設定するのが有効であると述べられていた．

Session 5: Crypto

暗号の，オムニバス形式とも呼ぶべき，話題の寄せ集めのセッション．5 件の発表があった．

“Modelling After-the-fact Leakage for Key Exchange”, Janaka Alawatugoda, Douglas Stebila, Colin Boyd. 鍵共有のセッションが完了した後の鍵情報漏えいを扱った研究発表であった．新たに leakage-resilient NAXOS trick の概念と実現方法を提案していた．

Session 6: Access control and Flow analysis

4 件の発表が行われ，活発な議論が行われた．

"Efficient, Context-Aware Privacy Leakage Confinement for Android Applications without Firmware Modding", Mu Zhang, Heng Yin. Zhang らの発表では，Android におけるプライバシ漏洩を防止する手法が提案されていた．提案手法は，情報フローの追跡とポリシによる制御のために，Android アプリのバイトコードを書き換える．これにより，ファームウェアの変更が必要なく，性能低下の小さいプライバシ漏洩防止手法を実現していた．また，バイトコードレベルでの解析時に最適化を行うことで，プログラムサイズを半分程度まで削減できたと報告されていた点が興味深い．実際に配布されている Android アプリを解析し，33%に情報漏洩の可能性があることも示されていた．公式のマーケットを通じて多くの Android アプリが配布されている現状では，提案手法を適用した Android アプリの配布方法が問題になると考えられる．

"Malware Detection with Quantitative Data Flow Graphs", Tobias Wüchner, Martín Ochoa, Alexander Pretschner. Wuchner らの発表は，データフローグラフ(Data Flow Graph, DFG)に基づくマルウェア検知手法に関するものであった．提案手法は，システムコールや関数呼び出しを検出することで DFG を生成し，データの複製，システムの完全性やデータの機密性を改ざんする処理，および DFG におけるエッジとノードの関係をもとにマルウェアを検出する．評価では，検体のうち約 96%を提案手法によりマルウェアとして検出できたと報告されていた．

"Abstract Model Counting: A Novel Approach for Quantification of Information Leaks", Quoc-Sang Phan, Pasquale Malacaria. Phan らの発表は，Satisfiability Modulo Theories (SMT)を用いてプログラムを静的解析することで情報漏洩を検出する手法を示していた．

"ConXsense – Automated Context Classification for Context-Aware Access Control", Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, N. Asokan. Miettinen らの発表は，コンテキストに応じたモバイル機器向けのアクセス制御フレームワーク ConXsense を提案している．ConXsense は，モバイル機器のセンサ情報をもとにコンテキスト情報を生成し，コンテキストに応じた細粒度なアクセス制御を実現している．コンテキストは，位置情報とソーシャル情報により生成され，位置情報には GPS や Wifi，ソーシャル情報には Bluetooth を利用している．また，生成したコンテキストに応じてアクセス制御ポリシを作成することで，プライバシ情報の漏洩を防止している．ConXsense は，自動的に写真を撮影し，画像を攻撃者に送信するマルウェアなど，モバイル機器のセンサ情報を利用するマルウェアへの有効な対策の一つである．モバイル機器が持つ特徴に着目したアクセス制御手法であり，興味深い内容であった．

Session 7: Software and Systems security

4 件の発表が行われ，活発な議論が行われた．

"On the Feasibility of Software Attacks on Commodity Virtual Machine Monitors via Direct Device Assignment", Gábor Pék, Andrea Lanzi, Abhinav Srivastava, Davide Balzarotti, Aurélien Francillon, Christoph Neumann

Pek らの発表では，仮想計算機へ直接デバイスを割り当てる機能を利用した攻撃方法を報告していた．また，攻撃可能な箇所を検出する PTFuzz を作成し，

Xen や KVM の問題点を検出していた. 広く利用されている仮想計算機モニタを攻撃可能であることが実際に示されている点が興味深い.

"After We Knew It: Empirical Study and Modeling of Cost-Effectiveness of Exploiting Prevalent Known Vulnerabilities Across IaaS Cloud", Su Zhang Xinwen Zhang, Xinming Ou

Zhang らの発表では, IaaS (Infrastructure as a Service) において, あらかじめ用意された仮想計算機イメージに対してテストを行い問題点を調査することで, 同じイメージを用いた他の仮想計算機への攻撃コストが低下する問題を指摘していた.

"Prospect: Peripheral Proxying Supported Embedded Code Testing", Markus Kammerstetter, Christian Platzer, Wolfgang Kastner, Kammerstetter らの発表では, 組み込みシステムで利用される応用プログラムのテストの難しさを低減する PROSPECT が提案されていた. 組み込みシステムでは, オペレーティングシステムが改造されているため, 改変なしに仮想計算機上で動作させるのは難しい. PROSPECT は, 組み込みシステムの応用プログラムを QEMU 上で動作させ, 周辺機器へのアクセスのみ実際のデバイスに転送する. これにより, 既存の解析手法を組み込みシステムの応用プログラムに適用可能とし, 組み込みシステムの解析を効率化している. 組み込みシステムが増加している現状に即した実用的な研究であるといえる.

"Scanning of Real-World Web Applications for Parameter Tampering Vulnerabilities", Adonis P. H. Fung, Tielei Wang, K.W. Cheung, T. Y. Wong. Fung らの発表では, Web アプリケーションの脆弱性検査において, リクエスト間のパラメータの依存関係に着目した検査方法が提案されていた. 提案手法は, リクエスト間で依存関係のあるパラメータを抽出し, 依存関係のないパラメータのみを変更したリクエストをクライアントから送信することで, Web アプリケーションの脆弱性検査を行なっている. これにより, 既存の検査手法では, 実際に検査したい処理に到達する前に, リクエストが拒否され, 検査に失敗していた問題に対処していた.

Session 10: Android

4 件の発表が行われ, 活発な議論が行われた.

"Evading Android Runtime Analysis via Sandbox Detection", Timothy Vidas, Nicolas Christin. Android malware が, 仮想マシンやエミュレータなどの解析環境を検知する手法とその評価結果について述べている. 現状では, エミュレータなどの情報は, いろいろな方法で検知できてしまうので, 現状ではすべて隠すのは難しいという結果が示されていた.

"VirtualSwindle: An Automated Attack Against In-App Billing on Android", Collin Mulliner, William Robertson, Engin Kirda. Android アプリとサーバがやりとりする課金情報を, 偽装して Android アプリに送ることで, 実際には課金されていないのに, ゲーム等に課金されている認識させる攻撃が可能であることを示している. 実際に実験を行ったデモを動画で説明し, 課金されることなくゲーム内のアプリを購入した状態にできることを示していた. また, この攻撃手法に対する対策も提案している.

"DroidRay: A Security Evaluation System for Customized Android Firmwares", Min Zheng, Mingshen Sun, John C.S. Lui. Android のファームウェアやプリインストールアプリに, 最初からマルウェアが仕込まれていることを実際に検証した結果を報告している. また, malicious firmware やプリインストールされたマルウェアを分析するシステムである DroidRay を提案し, 分析した結果について報告している.

"APKLancet: Tumor Payload Diagnosis and Purification for Android Applications", Wenbo Yang, Juanru Li, Yuanyuan Zhang, Yong Li, Junliang Shu, Dawu Gu. アプリを解析し問題のあるプログラム部分を取り除いて安全なアプリを生成する APKLancet というシステムを提案している. 評価では, 提案システムの適用によりマルウェアと検知される確率が大幅に低下できたことが示されている.

4 論文賞, ポスター賞

論文賞(Best paper awards)及びポスター賞(Best

poster awards)には下記の 2 件及び 4 件がそれぞれ選出された.

Best paper awards

- "Re^3: Relay Reliability Reputation for Anonymity Systems", Anupam Das, Nikita Borisov, Prateek Mittal, Matthew Caesar.
- "ConXsense - Automated Context Classification for Context-Aware Access Control", Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, N. Asokan.

Best poster awards

- "Performance Evaluation of a Privacy -Enhanced Access Log Management Mechanism", Sanami Nakagawa, Keita Emura, Goichiro Hanaoka, Akihisa Kodate, Takashi Nishide, Eiji Okamoto, and Yusuke Sakai.
- "Vehicle ECU Hacking", Dennis Kengo Oka, Camille Vuillaume, and Takahiro Furue.
- "SSL/TLS servers status survey about enabling forward secrecy (+ rapid survey after the Heartbleed Bug)", Yuji Suga.
- "Understanding consistency between words and actions for Android apps", Takuya Watanabe and Tatsuya Mori.

5 運営側の視点から

ASIACCS2014 は参加者が 175 名(うち海外から 107 名)と, 昨年の 89 名, 一昨年の 59 名という実績を大幅に上回る数の参加者を集めることができた. これは, 京都という開催地に助けられたこともあるが, 関係者の皆様の貢献によるところが大きい. この場を借りて, 改めてお礼を申し上げたい.

会場は, 例年の参加者数と予算規模をもとに京都ガーデンパレスを選定した. 参加者数は予想の倍近くになったが, 結果的に大きすぎず, メイン会場, 併設ワークショップ, コーヒーブレイク会場等がワンフロアでおさまるちょうどよい規模であったと思う. さらに, 昨年度は実施されなかったポスターセッションを行い, 17 件もの発表があった. コーヒーブレイク会場で行ったことで, 活発な意見交換に貢献できたように思う.

運営は, 京都ローカル事情に詳しい(株)CS センター様からの多大なサポートのもと, NICT ネットワークセキュリティ研究所のセキュリティ基盤研究室メンバ総動員で行った. 海外からの参加者が多かったこともあり, ビザ対応や食物アレルギーや宗教, 信条等の理由で食材に制限のある参加者への対応が予想以上に大変であった. バンケットには, 祇園東より舞妓さん, 芸妓さん, 地方(じかた)さんに来て頂き, 祇園小唄をご披露頂いたほか, 優秀論文賞・優秀ポスター賞の表彰式もお手伝い頂き, 京都ならではのおもてなしができたかと思う.

6 むすび

ASIACCS2014 はここ 4 年で最多数の参加者を集め, 12 のセッションが行われ, また 5 つのワークショップも開催された. 次回:ASIACCS2015 は, シンガポールで, 2015 年 4 月 14 日から 17 日の 4 日間開催される.

謝辞

第一著者は本シンポジウムへの参加に関し, 次の研究費に部分的に支援を受けております. ここに深謝申し上げます.

- 総務省委託研究　国際連携によるサイバー攻撃の予知技術の研究開発「PRACTICE」

第六著者は本シンポジウムへの参加に関し, 次の研究費に部分的に支援を受けております. ここに深謝申し上げます.

- 日本学術振興会 科研費／挑戦的萌芽研究, 研究課題番号:25540004「確率検査証明理論に基づく非対話型ゼロ知識証明の構成理論と暗号系への実用強化」

参考文献

[1] ASIACCS2014 Web サイト
http://asiaccs2014.nict.go.jp/index.html
[2] ASIACCS2015 Web サイト
http://icsd.i2r.a-star.edu.sg/asiaccs15/