IEEE Symposium on Security & Privacy 2013 参加報告

松本 晋一† 松浦 幹太‡ 井家 敦§ 岡本 学§

†(公財)九州先端科学技術研究所
814-0001 福岡市早良区百道浜 2-1-22
smatsumoto@isit.or.jp

‡東京大学
153-8505 東京都目黒区駒場 4-6-1
kanta@iis.u-tokyo.ac.jp

§神奈川工科大学

243-0292 神奈川県厚木市下荻野 1030

inoie@nw.kanagawa-it.ac.jp, manabu@nw.kanagawa-it.ac.jp

あらまし 本稿では，2013年5月19日から22日に米国カリフォルニア州サンフランシスコにて開催されたIEEE Symposium on Security and Privacy 2013，および同月23，24の両日に開催された併催ワークショップに関し，その概要を報告する[1].

A report on IEEE Symposium on Security & Privacy 2013

Shinichi Matsumoto† Kanta Matsuura‡ Atsushi Inoie§ Manabu Okamoto§

†Institute of Systems, Information Technologies and Nanotechnologies
2-1-22 Momochihama, Sawara-ku, Fukuoka 814-0001, JAPAN
smatsumoto@isit.or.jp
‡University of Tokyo
Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, JAPAN
kanta@iis.u-tokyo.ac.jp
Kanagawa Institute of Technology(KAIT)
1030 Shimo-ogino, Atsugi-city, Kanagawa, 243-0292, Japan
inoie@nw.kanagawa-it.ac.jp, manabu@nw.kanagawa-it.ac.jp

Abstract This paper repots on the 34th IEEE Symposium on Security and Privacy, held on May 19 to 22, 2013 at San Francisco, CA, U.S.A and co-located workshops held on May 23 and 24 at the same place.

[1]**謝辞** IEEE S&P への参加は，PRACTICE: 国際連携によるサイバー攻撃技術の研究開発(総務省)の支援を受けています.

1　はじめに

本稿では，2013 年 5 月 19 日から 22 日に米国カリフォルニア州サンフランシスコにて開催された IEEE Symposium on Security and Privacy 2013 [1]，および同月 23, 24 の両日に開催された併催ワークショップ [2] に関し，その概要を報告する.

2　シンポジウム概要

IEEE Symposium on Security and Privacy (以下，IEEE S&P とする)は，1980 年の初回開催から，今回で 34 回目を数える. 初回から一昨年度までは，カリフォルニア州オークランドで開催されていたが，昨年度より同州サンフランシスコで開催されている.

主催は IEEE Computer Society on Security and Privacy と IACR(International Association for Cryptologic Research)の共催による. スポンサーは以下の各社，及び団体である.

- Google
- Symantec
- Cisco Systems
- CERT, Carnegie Mellon University's Software Engineering Institute
- NSA
- Microsoft Research
- Yahoo!
- Facebook
- Lincoln Laboratory, MIT
- VMware
- IAI (Intelligent Automation, Inc)
- Technicolor

本会議の会期は，5 月 20 日(月)から 22 日(水)までの三日間であったが，受付は会期前日の 19 日(日)夕方から開始された. 会期初日の夕方にはポスターセッションが開催された [3]. また本会議の翌日から二日間，23 日(木)，24 日(金)の両日に，併設の 6 つのワークショップが開催された.

2.1　運営体制

本大会の運営体制は，以下からなる.

- General chair
  Robin Sommer (International Computer Science Institute and Lawrence Berkeley National Laboratory)
- Program chairs
  Wenke Lee (Georgia Tech), Michael Backes (Saarland University) and Adrian Perrig (Carnegie Mellon University)
- Vice Chair and Treasurer
  Greg Shannon (CMU CERT)
- Registration Chair
  Sean Peisert (UC Davis and Lawrence Berkeley National Laboratory)
- Donations Chair
  Alvaro Cárdenas (Fujitsu Laboratories of America)
- Publications Chair
  Kevin Butler (University of Oregon)
- Site Chair
  Chris Switzer (International Computer Science Institute)
- Publicity and Media Chair
  Ulf Lindqvist (SRI International)
- Student Travel Committee Chair
  Terry Benzel (USC Information Sciences Institute)
- Poster Chair
  Sophie Engle (University of San Francisco)
- Web Chair
  Devdatta Akhawe (UC Berkeley)

2.2　Call for Paper

IEEE S&P の Call for Paper では，コンピュータセキュリティ/プライバシの様々な側面に寄

与する研究が募集された．特に関係するトピックとして以下を挙げてられたが，これらは，一部順序が前後している事を除けば昨年と同様である．

- アクセス制御
- アカウンタビリティ
- 匿名性
- アプリケーションセキュリティ
- 攻撃と防御
- 認証
- 検閲と検閲対策
- 分散システムセキュリティ
- 組込システムセキュリティ
- フォレンジクス
- ハードウェアセキュリティ
- 侵入検出
- モバイルセキュリティ
- マルウェア
- メトリクス
- 言語ベースセキュリティ
- ネットワークセキュリティ
- プライバシ保護システム
- プロトコルセキュリティ
- セキュア情報フロー
- セキュリティ及びプライバシポリシイ
- セキュリティアーキテクチャ
- システムセキュリティ
- ユーザビリティとセキュリティ
- Web セキュリティ

また 2010 年より，SoK (Systematization of Knowledge) paper と呼ばれる枠が設けられている．これは，これまでに得られた知識を評価し，体系化し，文脈を明らかにする研究を促すことを目的としており，新しい研究的貢献を含まないが，コミュニティに非常に貴重な価値をもたらすものを対象としている．

2.3 投稿論文

表 1 に，本年度を含めた過去 7 回の投稿論文数，採択論文数，採択率を示す．投稿論文数は漸増傾向にあるが，昨年度の投稿数は落ち込み，本年度は増加し過去最多となった．また本年度の採択数は，過去最多であった昨年度に次ぐ 38 本となった．

採択率は例年 10%台前半を保っている．2010 年は採択率が低いが，当該大会では SoK 論文を採択数に含めていない．2011 年～2013 年は SoK 論文が採択数に含まれており．これを勘案すると 2010 年の採択率はほぼ例年通りとなる．2012 年は，採択数の大幅な増加を受けて採択率が上昇したが，本年度は投稿数が増加した結果，昨年度を下回っている．

表 1 IEEE S&P の投稿採択論文数

	投稿数	*採択数*	*採択率*
2007 年	246	29	11.8%
2008 年	249	28	11.2%
2009 年	254	26	10.2%
2010 年	267	26	9.7%
2011 年	309	34	11.0%
2012 年	289	40	13.8%
2013 年	315	38	12.1%

2.4 IEEE S'&P 2013 のセッション構成

以下に本年度を含めた過去 4 回のセッションの構成を示す．各項目の括弧内の数字は，セッション内の発表論文数を示す．

- 2013 年セッション構成
  - Programming Language Security(4)
  - Anonymous Network Communication (2)
  - Botnets and Other Underground Activities (3)
  - Jamming Uses and Defenses (3)
  - Secure Operating Systems (5)
  - Cryptographic Tools for Building Verifiable Cloud Computing (3)
  - Hardware Security (3)
  - Privacy (3)
  - Application Security(Voting, Sybil, Bitcoin)(3)
  - Formal Methods for Building Secure Systems(3)
  - Crypto(3)

- SSL/TLS, Web Security(3)

- 2012 年セッション構成
  - System Security(8)
  - Malware(3)
  - Attacks(6)
  - Foundations(3)
  - Access Control & Attestation(3)
  - Privacy(4)
  - Network Security(3)
  - Web Security(3)
  - Privacy and Anonymity(4)
  - Passwords(3)
- 2011 年セッション構成
  - Security of authentication and protection mechanisms (3)
  - Hardware Security (2)
  - Systematization of Knowledge (4)
  - Browsing Security and Privacy (3)
  - Secure Information Flow and Info. Policies (4)
  - Privacy and Social Networks(3)
  - Virtualization & Trusted Computing (4)
  - Program Security Analysis (3)
  - Underground Economy/Malware (2)
  - Vulnerability Analysis (4)
  - Anonymity and Voting (2)
- 2010 年
  - Special Papers for the 30th Anniversary of the Symposium (3)
  - Malware Analysis (3)
  - Information Flow (4)
  - Root of Trust (3)
  - Information Abuse (4)
  - Network Security (3)
  - Systematization of Knowledge (5)
  - Secure Systems (3)
  - Analyzing Deployed Systems (3)
  - Language-Based Security (3)

セッション構成として，2010 年，2011 年は SoK をまとめて独立したセッションとして設けていたが，昨年から各テーマを掲げるセッション内に組み込まれた形式となっている.

3 IEEE S&P における発表

3.1 本会議

以下に本会議における発表論文タイトルを挙げる. 本会議における発表件数は 38 件であり，その内 SoK 論文が 5 件であった.

- **Session 1: Programming Language Security**
  - [1a] All Your IFCException Are Belong to Us
  - [1b] Declarative, Temporal, and Practical Programming with Capabilities
  - [1c] Towards Practical Reactive Security Audit Using Extended Static Checkers
  - [1d][SoK] Eternal War in Memory
- **Session 2: Anonymous Network Communication**
  - [2a] The Parrot Is Dead: Observing Unobservable Network Communications
  - [2b] Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization
- **Session 3: Botnets and Other Underground Activities**
  - [3a][SoK] P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets
  - [3b] Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures
  - [3c] The Crossfire Attack
- **Session 4: Jamming Uses and Defenses**
  - [4a] Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors

[4b] On Limitations of Friendly Jamming for Confidentiality

[4c] Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time

- **Session 5: Secure Operating Systems I**

[5a] Practical Timing Side Channel Attacks against Kernel Space ASLR

[5b] PrivExec: Private Execution as an Operating System Service

- **Session 6: Cryptographic Tools for Building Verifiable Cloud Computing**

[6a] A Hybrid Architecture for Interactive Verifiable Computation

[6b] Pinocchio: Nearly Practical Verifiable Computation

[6c] ObliviStore: High Performance Oblivious Cloud Storage

- **Session 7: Hardware Security**

[7a] Hiding Information in Flash Memory

[7b] PUFs in Security Protocols: Attack Models and Security Evaluations

[7c] [SoK] Secure Data Deletion

- **Session 8: Privacy**

[8a] Anon-Pass: Practical Anonymous Subscriptions

[8b] Privacy-Preserving Ridge Regression on Hundreds of Millions of Records

[8c] A Scanner Darkly: Protecting User Privacy from Perceptual Applications

- **Session 9: Application Security**

[9a] Caveat Coercitor: Coercion-Evidence in Electronic Voting

[9b][SoK] The Evolution of Sybil Defense via Social Networks

[9c] Zerocoin: Anonymous Distributed E-Cash from Bitcoin

- **Session 10: Formal Methods for Building Secure Systems**

[10a] seL4: From General Purpose to a Proof of Information Flow Enforcement

[10b] Design, Implementation and Verification of an eXtensible and Modular Hypervisor Framework

[10c] Implementing TLS with Verified Cryptographic Security

- **Session 11: Crypto**

[11a] An Ideal-Security Protocol for Order-Preserving Encoding

[11b] Efficient Garbling from a Fixed-Key Blockcipher

[11c] Circuit Structures for Improving Efficiency of Security and Privacy Tools

- **Session 12: SSL/TLS and Web Security**

[12a] [SoK] SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements

[12b] Lucky Thirteen: Breaking the TLS and DTLS Record Protocols

[12c] Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting

- **Session 13: Secure Operating Systems II**

[13a] Practical Control Flow Integrity and Randomization for Binary Executables

[13b] Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization

[13c] Welcome to the Entropics: Boot-Time Entropy in Embedded Devices

図 1 に，ワークショップ及びポスターを除いた本会議での発表論文の国別内訳を示す．米国からの発表が約 2/3 を占めた．以下，独，英と続く．アジアからの発表は 1 件のみであった．

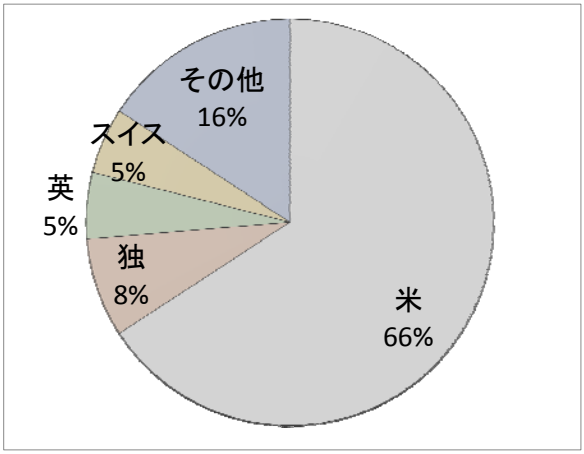

図 1 本会議の国別採択論文内訳

また筆頭著者の所属に基づいた，発表組織の産官学の別については，大学からの発表が 9 割以上と大多数を占めた.

国別，組織種別の傾向は昨年と同様であり，米国の大学が主要な位置を占める学会であることが判る.

3.2 表彰論文

表彰論文は，会期二日目の朝に発表され，以下が表彰された.

- Best Paper Award
  [6b] Pinocchio: Nearly Practical Verifiable Computation
- Best Practical Paper Award
  [2a] The Parrot Is Dead: Observing Unobservable Network Communications
- Best Student Paper Award
  [13b] Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization

3.3 本会議トピック

本節では，本会議の中ので特に興味深かった発表をいくつかピックアップし紹介する.

[6b] Pinocchio: Nearly Practical Verifiable Computation

本論文は，VC: Verifiable Computation の実現方式に関する研究発表であり，今会の Best Paper として表彰された.

クラウドサービスを用いた計算処理のアウトソースにおいて，得られた計算結果の検証方法，これまでいくつか提案されてきたが，いずれも検証に要する計算量が，クライアント側でのネイティブな計算の計算量よりも非常に大きく，非現実的であることが課題であった.

本論文では，計算処理を記述した C 言語プログラムを回路表現(算術演算回路，論理演算回路)に変換後，それぞれを二次計画法(QAP: Quadratic Arithmetic Program, QSP: Quadratic Span Program)に変換し，検証プログラムを生成することで，検証処理の大幅な高速化に成功している.

計算検証効率の評価において 7 種のアプリケーション

- Fixed Matrix—行列とベクトルの積
- Two Matrices – 二つの行列の積
- MultiVar Poly –多変数多項式計算
- Image Matching – 画像マッチング処理
- Short Paths – ワーシャル-フロイド法
- LGCA–格子ガス・セルオートマトン
- SHA-1

を用い，従来の提案に対し検証時間の大幅な効率化に成功している. 結果，上記アプリケーションの内，前 3 者についてネイティブな計算処理よりも検証処理を低廉化せしめている.

本論文において，VC における検証の大幅な効率化の実現が評価されたことが，Best Paper 表彰の理由と思われる.

[2a] The Parrot Is Dead: Observing Unobservable Network Communications

本論文は，通信における検閲回避方法の複数の実装について，その実効性を検証するものであり，今会の Best Practical Paper として表彰された.

当該論文では，検閲に対する観測不可能性を実現するために，偽の通信トラヒックを発生させ撹乱する(unobservability by imitation)方式を parrot circumvention system と呼び，このための実装である SkypeMorph, Stego

Torus, CencorSpoofer について，偽造されるトラヒックが，検閲者にとって容易に識別可能であることを示した．

この結果を受けて，Unobservability by imitation というアプローチが抱える根本的な欠陥について示した後，検閲回避のためにはステガノグラフィ的なアプローチの方が有効であると結論付けている．

3.4 ポスターセッション

ポスターセッションは，20 日の夜に催され，34 件が発表された．国別内訳としては米国からのものが 6 割以上であり，続いて独，カナダと続いている．日本からの発表は 1 件であった．

3.5 ポスターセッション発表

ポスターセッションにて，著者(岡本，井家)らが以下の発表を行った．

- Single Sign-on Using Portable IdP on USB Flash Drive, Takahiro Ishii, Atsushi Inoie, Manabu Okamoto

本発表は認証技術のひとつである「シングル・サインオン」(一回パスワード入力を行うだけで複数サービスを個別認証なしで受けることができる技術)に関する発表であり，ユーザが集中的に認証を受ける Identity Provider (IDP) なるサーバをポータブルに USB メモリに配置することで，ユビキタス性やセキュリティ性を高める研究である．

「IDP を持ち出す」新しいアイディアには「落としたり失くしたりしたらどうするのか」等の基本的な質問等，数々の活発な議論がなされた．

3.6 ワークショップ

IEEE S&P 会期後の二日間で以下の六つのワークショップが開催された．個々のワークショップの会期はそれぞれ一日であった．ワークショップの予稿集は USB メモリで配布されたが，一部の発表については，各ワークショップの WEB ページから参照できる．

- CREDS: Cyber-security Research Ethics Dialog & Strategy [4]

サイバーセキュリティ研究における倫理的側面についての議論を目的としたワークショップであり，関係者の考え方が揃わない時に共通の利益を見いだす一つの考え方として，セキュリティとプライバシーに関わる取り組みの教育的効果が挙げられていたことが印象的であった．これに関し著者(松浦)も挙手してコメントし，日本での CSEC/MWS における取り組みの教育的効果を紹介，宣伝を行った．

発表内容の予稿については，Web ページから入手可能である．

- DUMA: 4th International Workshop on Data Usage Management [5]

アクセス制御の概念をより一般化させた Data Usage の概念について論じる事を目的としたワークショップであり，ポリシイ，ユーザアクションと技術的事象の間の関係，抽象化階層を跨るデータのトラッキング，論理的/物理的システム，ポリシイエンフォースメント，エンフォースメントシステムの保護と保証を含む．

基調講演後に 3 件の研究発表と 5 件のポジションペーパー発表，ならびにパネルディスカッションが行われた．

- MoST: Mobile Security Technologies [6]

モバイルデバイスやアプリケーション，システムの研究者や開発者などを対象として，モバイルデバイスハードウェアや OS,ミドルウェアなどのセキュリティについて扱うワークショップであり，招待講演 1 件と 10 件の研究発表(内 2 件はショートペーパー)が行われた．

発表内容の予稿，並びに一部のスライドについては，Web ページから入手可能である．

- IWCC: International Workshop on Cyber Crime [7]

サイバー攻撃の脅威の急激な進展を受け，デジタルフォレンジックスの分野における最新の研究成果を交換するとともに，違法なサイバー活動を調査するためのツールとテクニックを示すワークショップであり，招待講演 1 件と，10 件の研究発表が行われた．投稿は 30 件であり，採択率は 33%となる．

本ワークショップでは Best Paper として，

- Understanding Network Forensics Analysis in an Operational Environment
- Do Private and Portable Web Browsers Leave Incriminating Evidence?

の 2 件が選出された.

前者は，ネットワークフォレンジックスに関し，複数の情報源(Snort の出力やブラックリスト，サーチエンジンの出力等)を関連付けてインシデント分析を行う方法についての研究である.

また後者は，Web ブラウザの多くが備えるプライベート閲覧モード，またポータブルブラウザに関して，これらが閲覧セッション後に何らかの証拠を残すか否かについての検証を行い，検証を行った全てのブラウザで，何らかの閲覧の証拠が得られたことを示した.

- WRIT: Workshop on Research for Insider Threat [8]

インサイダーからの脅威 (IT: Insider Threat)に固有の問題に，多数の視点(IT，行動科学，犯罪学など)から焦点を当てる事を目的に開催されたワークショップである.

昨年，IEEE S&P との併催で第一回が開催され，今回が 2 回目となる. 基調講演と，9 件の研究発表が行われた.

- W2SP: Web 2.0 Security and Privacy [9]

Web 2.0 におけるセキュリティとプライバシの問題を扱うワークショップである. 2007 年より IEEE S&P 本会議との併催が続いており，本年で 7 回目の開催である. 基調講演と，8 件の研究発表(うち 3 件がショートペーパー)が行われた.

発表内容の予稿，並びにスライドについては Web ページから入手可能である.

4 おわりに

本稿では，2013 年 5 月 20 日から 22 日に米国カリフォルニア州サンフランシスコにて開催された IEEE S&P 2013，および同月 23，24 両日に開催された併催ワークショップに関し，その概要を報告した.

参考文献

[1] IEEE Symposium on Security and Privacy 2013
http://www.ieee-security.org/TC/SP2013/index.html

[2] IEEE Symposium on Security and Privacy 2013 Workshops
http://www.ieee-security.org/TC/SPW2013/

[3] IEEE Symposium on Security and Privacy 2013(Poster Session)
http://www.ieee-security.org/TC/SPW2013/

[4] Cyber-security Research Ethics Dialog & Strategy Workshop (CREDS 2013)
http://www.caida.org/workshops/creds/1305

[5] 4th International Workshop on Data Usage Management
http://dig.csail.mit.edu/2012/IEEESP-DUMA13/

[6] Mobile Security Technologies (MoST) 2013
http://mostconf.org/2013/

[7] International Workshop on Cyber Crime (IWCC)
http://stegano.net/IWCC2013/

[8] SEI Community | writ2013 | Workshop on Research for Insider Threat (WRIT)
http://www.sei.cmu.edu/community/writ2013/

[9] W2SP 2013: Web 2.0 Security & Privacy 2013
http://www.w2spconf.com/2013/