Vol.2009-CSEC-47 No.5
2009/12/18

ACM CCS2009 会議ならびに 併設ワークショップ参加報告

江藤文治[†]　西出隆志[†,††]　堀良彰[†,††]　櫻井幸一[†,††]

この 2009 年 11 月 9 日から 11 月 13 日の間、米国イリノイ州シカゴで開催された第 16 回 ACM CCS 2009 (Conference on Computer and Communications Security 2009) ならびに、CCS2009 併設ワークショップに関して報告する。

ACM CCS 2009 and workshops report

Fumiharu Etoh[†]　Takashi Nishide[†,††]　Yoshiaki Hori[†,††]
and Kouichi Sakurai[†,††]

This paper reports on the 16th ACM CCS 2009 (Conference on Computer and Communications Security 2009) and CCS2009 workshops, held on November 9 to November 13, 2009, at Hyatt Regency Chicago, Chicago, IL, U.S.A.

1. はじめに

本稿では、2009 年 11 月 9 日から同月 13 日の間に米国イリノイ州シカゴで開催された第 16 回 ACM CCS 2009 (Conference on Computer and Communications Security 2009) [1]とその併設ワークショップ[2][3]に関して報告する。

2. ACM CCS 2009 の概要

ACM Conference on Computer and Communications Security（以下、CCSとする）はACM SIGSAC (Special Interest Group on Security, Audit and Control)が主催する年次コンファレンスのひとつであり、その名の通りコンピュータおよび通信におけるセキュリティに関する話題を取扱う。1993年に初めて開催されてから2009年の開催で16回目を数え、2002年以降の会議はワシントンDCかその郊外に位置するアレクサンドリア市にて開催され、特に、2005年以降の4カ年はバージニア州アレクサンドリア市のヒルトン・アレクサンドリア・マークセンターホテルで開催されていたが、今年度はシカゴ市のハイアット・リージェンシー・シカゴにて開催された。会期は月曜日から金曜日までの5日間であるが、初日と最終日は併設ワークショップの開催であり、本会議は火曜日から木曜日の3日間の開催である。
表1 に、過去6カ年（2004年から2009年）の投稿論文数、採択論文数、採択率を示す。2004から2006年までは、投稿数は250件程度であったが、2007年、2008年および2009年は302件、280件および315件（CCSで過去最高）であり、この分野における関心の高さを伺わせる。これはプログラム編成にも影響を与え、2006年までは、いわゆる学術論文発表の講演はシングルトラックであったが、

表 1　ACM CCS 2004～2009 の投稿採択状況

	投稿数	採択数	採択率
CCS2004	**251**	**34**	**13.5%**
CCS2005	**250**	**38**	**15.2%**
CCS2006	**256**	**38**	**14.8%**
CCS2007	**302**	**55**	**18.2%**
CCS2008	**280**	**51**	**18.2%**
CCS2009	**315**	**58**	**18.4%**

[†]（財）九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies (ISIT)
[††] 九州大学大学院システム情報科学研究院情報学部門
Department of Informatics, Kyushu University

2007年以降デュアルトラックとなり採択数が増えることとなった[4][5][6]。2009年の会議では、31カ国からの315件の論文の投稿のうち、58 件の論文が採択された。したがって、論文採択率は18.4%とここ数年とほぼ同じで、過去5,6年と比較すると若干上昇しているが、20%未満と低い採択率であるには変わらない。

CCS2009 本会議の会議録は、会場では冊子版と CD-ROM 版の両方が配布された。一方で、CCS2009 併設ワークショップでは CD-ROM 版のみ配布された。例年と同様に CCS2009 本会議ならびに併設ワークショップの会議録は ACM デジタルライブラリ[a]により参照可能である。

CCS2009 では、コンピュータセキュリティに関する理論的な研究と実用的な研究（事例研究や実施経験を含む）の双方の論文が採択されている。しかし、CCS では理論的な研究論文であっても、説得力のあるアプリケーションを例示し、実用的な面での重要性に関する議論を行うことを求めている。すなわち、CCS では実用面での関連性を重要視している。

CCS2009 のプログラムは、2 つの研究発表講演トラックと 1 つのチュートリアルトラックから構成された。2007 年度まであったインダストリアル＆ガバメント（I&G）トラックは、昨年と同様に設定されなかった。

CCS2009 ではリサーチトラックとして 18 のセッションが設けられ、前述の 58 件の論文発表が行われた。その他に、チュートリアルが 4 件企画された。これらのタイトルを次に示す。行頭の記号 K-#は基調講演、T-#はチュートリアルを表す。

K-1. Your/My Password Has Expired (DOROTHY E. DENNING, Naval Postgraduate School)
T-1. "Cyber Security For The Power Grid" (Mel Gehrs ,Gehrs Consulting), (Himanshu Khurana, UIUC) and (Andrew Wright ,N-Dimension Solutions)
T-2. An introduction to usable security (Jeff Yan, Newcastle University))
T-3. Security Risk Analysis of Computer Networks: Techniques and Challenge (Anoop Singhal, NIST) and (Xinming Ou, Kansas State University)
T-4. Securing Wireless Systems (Panos Papadimitratos, EPFL)

リサーチトラックにおける CCS2006 以前のセッション数はシングルトラック×3 日間の開催であったため 11 前後であったが、CCS 2007 以降では前述のようにリサーチトラックがデュアルトラックとなったためにセッション数が 18 と増えることとなった。次にセッション名を挙げる。セッション名の後の“(2)”は 2 つのセッションから構成されていたことを示す。

- Attacks (2)
- Applied Cryptography
- RFID
- Anonymization (2)
- Formal Techniques
- Cloud Security
- Security of Mobile Services
- Anonymization Techniques
- Software Security using Behavior
- Embedded and Mobile Devices
- Systems and Networks
- Techniques for Ensuring Software Security
- Privacy
- Designing Secure Systems
- System Security
- Malware and Bots

CCS2009の参加者は全体で500名程であった。しかし、2つのリサーチトラックにおける聴講者は各々40～200名程度であった。日本からの参加者は10数名程度であった。

3. CCS2009 併設ワークショップ

CCS2009 では前述の通り、会期の初日（月曜日）と最終日（金曜日）に併設ワークショップが開催された。初日及び最終日のワークショップ共に本会議と同じ会場で開催された。ここ数カ年、最終日は別会場での開催であったが、本年は例年と異なるスタイルであった。2009 年は、次の 12 の併設ワークショップが開催された。

(1)Workshop on Assurable and Usable Security Configuration (SafeConfig 2009)
(2)Workshop on Digital Rights Management (DRM 2009)
(3)Workshop on Virtual Machine Security (VMSec 2009)
(4)Workshop on Security and Artificial Intelligence(AISec 2009)
(5)Workshop on Secure Execution of Untrusted Code (SecuCode 2009)
(6)Workshop on Privacy in the Electronic Society (WPES 2009)
(7)Workshop Cloud Computing Security(CCSW 2009)
(8)Workshop on Digital Identity Management (DIM 2009)
(9)Workshop on Information Security Governance (WISG 2009)
(10)Workshop on Scalable Trusted Computing(STC 2009)

a) ACM Digital Library, http://portal.acm. org/dl.cfm

(11)Workshop on Secure Web Services(SWS 2009)
(12)Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS 2009)

2008 年に開催された併設ワークショップのうち Workshop on Formal Methods in Security Engineering (FMSE)・Workshop on Quality of Protection (QoP)・Workshop on Computer Security Architectures (CSAW)・Workshop on Network Data Anony-mization (NDA)・Workshop on Storage Security and Survivability (StorageSS)の 5 ワークショップが開催されず、SafeConfig・SecuCode・CCSW・WISG・SPIMACS は 2009 年に新たに開催されたものである。2008 年から開催されている AISec・VMSEC と併せ、12 の内 7 ワークショップがこの 2 年に新設されたものであり、この分野における技術の進化と研究対象の変化が伺われる。

3.1. SafeConfig 2009

Workshop on Assurable and Usable Security Configuration (SafeConfig 2009)は、セキュリティ構成の抽象化、確認、施行、配布、最適化、テスト、視覚化および他の関連するトピックスの発表の機会の為に企画された。今回が初の開催である。
21 件の投稿があり、その中から6 件がフルペーパとして、5件がポジションペーパ／ショートペーパとして採択された。3つのセッションShort and Position Papers,Network Configuration and Protocol Analysis,Security and Privacy Configurationにおいて計11件の発表講演が実施された。
また、招待講演が2件あり、Vision of SCAP と題してTony Sager (National Security Agency)氏が、Security Automation - Convergence That Mattersと題してKent Landfield (McAfee)氏とJohn Banghart (NIST)氏が、講演を行った。
さらに、Future Research on Usable Security Configuration: NSF Reportと題してパネルディスカッションが行われ、モデレータ : Ehab AlShaer (UNC Charlotte)氏とパネラー: Tony Sagel (National Security Agency)氏、Kent Landfield (McAfee)氏及びJohn Banghart (NIST)氏により、Netork security configurationの課題等の議論が展開された。

3.2. DRM 2009

Workshop on Digital Rights Management (DRM)は、インターネット上のデジタルコンテンツに関する知的所有権保護方式やコピープロテクション、デジタルコンテンツ保護のためのアクセス制御について議論するためのワークショップである。DRMは今回で9 回目を迎えた。5つのセッションFormal Models, Cryptographic Techniques, Experience, Software Protection, Architectureにおいて、23件の投稿の中から採択された計9件の研究成果の講演と議論が行われた。
また、基調講演が 3 件あり、Randal Picker (University of Chicago, School of law)教授により “The Uses and Abuses of Control at a Distance” と題して、Edward Felten (Princeton University) 教授により “Non-Traditional Applications of DRM” と題して、Scott Watson Senior VP 兼 CTO(Walter Disney Imagineering Research and Development)により"Digital Rights and Wrongs"と題して、それぞれ講演が行われた。
加えて、The future of Digital Rights Managementと題して、Edward Felten教授, Rei Safavi-Naini(University of Calgary)教授, Scott Watson氏, Moti Yung氏の各パネリストにより、パネルディスカッションが行われ、「(DRMに関して、)技術的ソリューションに加えて社会的なソリューションと法的ソリューションの考慮が必要」等の議論が実施された。

3.3. VMSec 2009

Workshop on Virtual Machine Security (VMSec)は、仮想化技術とセキュリティに関して最新の研究成果を持ち寄り議論する場として企画された。VMSec は 2008 年に続いて 2 回目の開催である。但し、Workshop on Secure Execution of Untrusted Code (SecuCode 2009)との合同 Workshop として開催された。
今回の投稿論文件数は未公表であるが、Recovery & Introspection および Hot Topics in Security Virtualization の 2 つのセッションにおいて、6 件の発表講演が実施された。

3.4. AISec 2009

Workshop on AISec は 2008 年に続いて 2 回目の開催である。セキュリティ研究コミュニティと AI 研究コミュニティの共同研究を刺激しようと企画されている。24 件の投稿があり、うち 4 件の研究論文と 6 件のポジション論文が採択された。5 つのセッション Position Papers 1, CAPTCHAs, Botnets, Position Papers 2 および Malware and Network Intrusions において計 10 件の研究成果の講演と議論が行われた。
また、基調講演として、Vitaly Shmatikov (The University of Texas at Austin) 准教授が“The End of Anonymity, the Beginning of Privacy: New Directions in Privacy-Preserving Data Analysis” と題して講演を行った。
さらに、招待講演として、Elena Zheleva (University of Maryland)氏が “Privacy in social networks” と題して講演を行った。

3.5. SecuCode 2009

Workshop on Secure Execution of Untrusted Code (SecuCode 2009)は、低信頼コードに対してソフトウェアシステムの保護に取り組む、産業界と学界の研究者と実践者が一堂に会して共同作業することを目的としており、今回が初の開催である。但し、Workshop on Virtual Machine Security (VMSec 2009) との

合同Workshopとして開催された。
今回の投稿論文件数は未公表であるが、Software Securityの1セッションにおいて、3件の発表講演が実施された。
また、招待講演が1件あり、From Dependable Multi-user Operating Systems to Dependable Multi-application Operating Systems と題してWolfram Schulte (Microsoft Research)氏が講演を行った。

3.6. WPES2009

Workshop on Privacy in Electronic Society (WPES) は現在のコンピュータネットワークに潜在しているプライバシの問題とその解決方法について議論するためのワークショップである。WPES は今回で 8 回目を迎える。フルペーパ 23 件とショートペーパ 5 件の計 28 件の論文投稿があり、その内のフルペーパ 10 件、ショートペーパ 2 件がそれぞれ採択された。さらに、フルペーパとして投稿の中から 3 件がショートペーパとしての発表が依頼された。4 つのセッション Privacy metrics and techniques, Privacy protocols, Privacy in new applications および Short papersにおいて 15 件の研究成果の講演と議論が行われた。

3.7. CCSW 2009

Workshop Cloud Computing Security (CCSW 2009)は、クラウド中心のコンピューティングとアウトソーシング化されたコンピューティングの全てのセキュリティの解釈を研究者と実際の開発者が一堂に会して共同作業することを目的としており、今回が初の開催である。30 件の投稿があり、その中から11件がフルペーパとして、3件がショートペーパとして採択された。
4つのセッションWeb 2.0, Data Outsourcing, New Challenges および Applicationsにおいて計14件の研究成果の講演と議論が行われた。
また、招待講演が3件あった。1件目は “Plus ca Change: Security in the Ether; Security in the Cloud” と題して”Diffie-Hellman鍵交換”のWhitfield Diffie (University of London)教授により、コンピュータ利用に関し、TTS処理方式との比較から、クラウドの利用により少人数でのビジネス展開の可能性等の、講演が行われた。2件目は“When all the world's a stage Security in an uberconnected world” と題して” Grid Computingの父”のIan Foster(Argonne National Laboratory)教授による講演で、生成(create)、発見(discover)、構成(compose)に加えて、出版(publisher)を得た、とGrid/Cloudを表現していた。加えて、”Grid = federation、Cloud = hosting”の定義が印象に残った。もう1件は、“Effectively and Securely Using the Cloud Computing Paradigm” と題してPeter Mell (NIST)氏により講演が行われた。

3.8. DIM 2009

Workshop on Digital Identity Management (DIM) は Digital Identity 管理について扱うワークショップであり、セキュアかつプライバー保護された方法でサービスを利用可能な identity を提供することを目指しており、かつ、最新の調査結果を共有し、鍵となる挑戦を認識し、議論を示唆し、共通認証サービス基盤に向けて、産業と学界の間の協同を促進することを目的としている。本年は、5 回目の開催であり、21 件の論文投稿があり、その内の 7 件の論文と、4 件のショートペーパが採択された。会議は、4 つのセッション Social Identities, Mash Up and Governance, Communications and Proxy および Security and Policy から構成され、計 11 件の発表講演が実施された。
また、基調講演が 1 件あり、Kenji Takahashi (NTT)氏により ”Identity and Context a Changing World”と題して講演が行われた。
尚、本ワークショップに関しては、例年のように、発表講演スライドがウェブで公開[b]されている。

3.9. WISG 2009

Workshop on Information Security Governance (WISG 2009)は、リスク管理、報告及び説明責任に関わる組織において、効果的な情報セキュリティ戦略を実施するフレームワークを確立することを目的としており、今回が初の開催である。16 件の投稿があり、その中から6 件がフルペーパとして、3件がショートペーパとして採択された。
3つのセッションKeynote Talk, Compliance and Governance および Security Risk, Policy and Privacyにおいて計11件の研究成果の講演と議論が行われ、Panelセッションにおいて、"How to Make Decisions for Security Governance?" と題して、Yurdaer Doganata (IBM TJ Watson Research Center, USA)氏、Eijiroh Ohki (Kogakuin University, Japan)氏、Ketil Stolen (SINTEF, University of Oslo, Norway 氏の3人のパネリストによるパネルディスカッションが行われた。

3.10. STC 2009

Workshop on Scalable Trusted Computing (STC 2009) は Trusted Computing を大規模なシステムに適用したときに発生するスケーラビリティやそのときにセキュリティ上の問題について議論するためのワークショップである。STC2008 は第 4 回の開催であり、今回の投稿論文件数は未公表であるが、5 件のフルペーパと、4 件のショートペーパが採択された。 2 つのセッション Software-based Approaches to Secure Computing および Architectural Approaches to Secure Computing において計 5 件の発表講演が実施され、Short Papers セッションにおいて 4 件の研究成果の講演と議論が行われた。

b) http://www2.pflab.ecl.ntt.co.jp/dim2009/program.html

また、基調講演として、Adrian Perrig 氏が“Designing Secure Systems with Attestation” と題して TPM(Trusted Platform Module)を用いた技術が紹介され、Ernie Brickell 氏が”A Vision for Platform Security”と題して講演を行った。

3.11. SWS 2009

Workshop on Secure Web Services (SWS 2009)は、サービス指向アーキテクチャと XML に関するセキュリティを取り扱う。今年で、第 6 回目の開催である。14 件の論文投稿があり、その内の 7 件が採択された。2 つのセッション Secure Service-Oriented Architectures および Policy Models and Languages for Services において計 7 件の研究成果の講演と議論が行われた。

また、“Toward WS-Certificate”と題して、Ernesto Damiani 氏と Antonio Manã 氏による招待講演が実施された。

3.12. SPIMACS 2009

Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS 2009)は、医療や介護のようなセキュリティとプライバシが、最も脆弱な個人的なデジタル空間を確保する挑戦に取り組むべきコンピュータと社会科学者を一つに共同させることを目的としており、今回が初の開催である。今回の投稿論文件数は未公表であるが、9 件の論文が採択された。 3 つのセッション Privacy Policies: Technical and Political, Data Access and Control および In Situ Evaluations of Caregiving Technology において計 9 件の研究成果の講演と議論が行われた。

また、Panel セッションにおいて、" Authentication in iHealth Care" と題して、モデレータ : Kevin Fu 氏、と Charles Horowitz(MITRE)氏、Jim O'Leary(Microsoft)氏、Avi Rubin(John Hopkins)氏、Umesh Shankar(Google)氏の 4 人のパネリストによるパネルディスカッションが行われた。

4. CCS2009 本会議におけるコンピュータシステム関係発表

以上のように、CCS2009 本会議および併設ワークショップにおいて取り扱われるトピックは多岐にわたることから、ここでは CCS 2009 本会議において研究発表が行われた論文から、コンピュータシステムおよびそのアーキテクチャにかかわる最近のトピックについて紹介する。

a) A New Cell Counter Based Attack Against Tor [Zhen Ling(Southeast University) et al.]

Tor(The Onion Router)における新たなセルカウンタ攻撃の攻撃を報告している。秘匿通信の為に共通サイズ(Tor の場合、512byte)のセルのカウンタ値を変更することにより、秘匿通信するユーザ間の関係を短時間で認識可能とする。Tor において実験を行い、その実現可能性と効果を示し、効果的で失敗が少なく、かつ、検知されにくいと報告している。

b) HAIL: A High-Availability and Integrity Layer for Cloud Storage [Kevin Bowers(RSA lab, US) et al.]

著者らは複数のクラウドストレージプロバイダを利用した RAID に類似したデータ保存方法を提案している。著者らの方法を用いれば幾つかのストレージプロバイダーがダウンしてもデータを全て失うことはなく安全であると主張している。またストレージプロバイダを攻撃者と仮定した場合の安全性についても議論している。

c)Battle of Botcraft: Fighting Bots in Online Games with Human Observational Proofs [Steven Gianvecchio(The College of William and Mary, US) et al.]

オンラインゲームにおいて，プレイヤーに有利な状況を作り出すことで不正を行うボットの検出方法を提案している。そのためにキーボードやマウス操作などを監視し，ボットが操作しているか人間が操作しているかの差異を検出し，監視サーバへ不正状況を伝えるシステムを提案している。
実験結果では 99%の確率で検出に成功したと主張している。

d)Hey, You, Get Off My Cloud! Exploring Information Leakage in Third- Party Compute Clouds [Thomas Ristenpart(University of California) et al.]

仮想マシン環境で提供されるクラウドコンピューティングにおける新たな脆弱性発見を報告している。Malicious VM を攻撃対象の VM と同一ハード環境へ配置(placement)すること、及び、攻撃対象 VM からの情報抽出(extract)によるサイドチャネル攻撃の可能性を Amazon EC2 をケーススタディとして報告し、この新たな脆弱性に対する解決方法を提案している。

5. CCS 2010 について

来年秋に開催される CCS2010[7]は、今年度と同様に、米国イリノイ州シカゴでの開催が予定されている。会期は、今年より 1 カ月ほど早い 2010 年 10 月 4 日（月）から同月 8 日（金）の 5 日間である。会議場は同じく、ハイアット・リージェンシー・シカゴとアナウンスされている。研究発表講演を行うための論文の投稿締切は 2010 年 4 月 17 日とアナウンスされている。

Vol.2009-CSEC-47 No.5
2009/12/18

6. おわりに

本稿では、2009 年 11 月 9 日から同月 13 日の間に米国イリノイ州シカゴで開催された第 16 回 ACM CCS 2009 (Conference on Computer and Communications Security 2009)とその併設ワークショップに関して、その概要を紹介した。さらに、CCS 2009 本会議で発表されたコンピュータシステムセキュリティに関するいくつかの研究について概要を示した。

謝辞

本調査研究の一部は、財団法人情報科学国際交流財団の産学戦略的研究フォーラム（SSR）の支援、科学研究費補助金 基盤研究 B（課題番号：20300005）の支援、および、科学研究費補助金 若手研究（B)（課題番号：21700091）の支援を受けて実施したものである。

参考文献

1 The 16th ACM Conference on Computer and Communications Security (ACM CCS 2009). http://www.sigsac.org/ccs/CCS2009/
2 ACM CCS 2009 Pre-Conference Workshops. http://www.sigsac.org/ccs/CCS2009/preworkshops.shtml
3 ACM CCS 2009 Post-Conference Workshops. http://www.sigsac.org/ccs/CCS2009/postworkshops.shtml
4 高橋健一, 堀良彰, 今本健二, 櫻井幸一, CCS2006 とその併設ワークショップ, および PST2006 報告, 情報処理学会研究報告, CSEC, Vol.2007, No.16(20070301) pp. 123-128, March 2007.
5 堀良彰, ル・マレコエルワン, 櫻井幸一, ACM CCS2007 会議ならびに併設ワークショップ参加報告. 情報処理学会研究報告 Volume 2008, No. 21, pp.139-144, 2008-CSEC-40, March 6, 2008
6 堀良彰, 櫻井幸一, ACM CCS2008 会議ならびに併設ワークショップ参加報告, 情報処理学会研究報告, 2009-DPS-138(4), 2009-CSEC-44(4), pp. 19-24, March 2009
7 The 17th ACM Conference on Computer and Communications Security (ACM CCS 2010). http:/www.sigsac.org/ccs/CCS2010/cfp.shtml