社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (21)
2007－CSEC－ 36 (21)
2007／3／1

# CCS2006とその併設ワークショップ，およびPST2006報告

高橋 健一† 堀 良彰†‡ 今本 健二‡ 櫻井 幸一†‡

†九州システム情報技術研究所
814-0001 福岡市早良区百道浜 2-1-22 SRP ビル 7F
{takahashi, sakurai}@isit.or.jp
‡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
{hori, imamoto}@itslab.csce.kyushu-u.ac.jp

**あらまし** 2006年10月30日～11月3日にアメリカのアレクサンドリアで開催されたThe 13th ACM Conference on Computer and Communications Securityとその併設ワークショップ，および10月30日～11月1日にカナダのオンタリオ州で開催された2006 International Conference on Privacy, Security and Trustに関して報告する．

# Reports of CCS2006 and its Workshops, and PST2006

Ken'ichi Takahashi† Yoshiaki Hori†‡ Kenji Imamoto‡ Kouichi Sakurai†‡

†Institute of Systems & Information Technologies/KYUSHU
2-1-22 Momochihama, Sawara-ku, Fukuoka, 814-0001, Japan
{takahashi, sakurai}@isit.or.jp
‡Faculty of Information Science and Electrical Engineering, Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
{hori, imamoto}@itslab.csce.kyushu-u.ac.jp

**Abstract** This paper reports on the 13th ACM Conference on Computer and Communications Security and its workshops, held on Oct 30 to Nov. 3, 2006, at the Hilton Alexandria Mark Center, Alexandria, VA, U.S.A, and 2006 International Conference on Privacy, Security and Trust, held on Oct 30 to Nov. 1, 2006, at the Hilton Suites Toronto/Markham Conference Centre, Markham, Ontario, Canada.

## 1 はじめに

2006年10月30日～11月3日にアメリカのアレクサンドリアで開催されたThe 13th ACM Conference on Computer and Communications Security (CCS2006) [1]とその併設ワークショップ [2]，および10月30日～11月1日にカナダのオンタリオ州で開催された2006 International Conference on Privacy, Security and Trust (PST2006) [6]に関して報告する．

## 2 ACM Conference on Computer and Communications Security

ACM Conference on Computer and Communications Security は 1993 年に初めて開催されてから 2006 年の開催で 13 回目を数える．2006 年の会議では 256 件の論文が投稿され，そのうちの 38 件の論文が採択された．論文採択率は 38/256 ≒ 14.8%である．表 1 に第 11〜13 回の投稿論文数，採択論文数，採択率を示す．

表 1: 第 11〜13 回の投稿論文数，採択論文数，採択率

| | 投稿数 | 採択数 | 採択率 (%) |
|---|---|---|---|
| 第 11 回 | 251 | 34 | 13.5 |
| 第 12 回 | 250 | 38 | 15.2 |
| 第 13 回 | 256 | 38 | 14.8 |

CCS2006 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ようである．図 1 に採択論文の分野別内訳[1]を示す．

CCS2006 では 11 のセッションが設けられ，これらの論文が発表された．また，CCS では 1997 年からチュートリアルが設けられるようになった．CCS2006 では

- "Digital Forensics: Research Challenges and Open Problems" (Yong Guan, Iowa State University)
- "Xen Worlds: Xen and the Art of Security Education" (Thomas Daniels and Benjamin Anderson, Iowa State University)
- "Cryptographic Protection for Networked Storage Systems" (Christian Cachin, IBM Zurich Research Lab)

がチュートリアルとして設けられた．これらのチュートリアルの概要については [3] で見ることができる．2000 年からはワークショップが開催されるようになり，CCS2006 では 11 のセキュリティに関するワークショップが Pre-Conference, Post-Conference として開催された．また，2003 年からはインダストリートラックが計画され，産業界や政府によるセキュリティプロダクトやシステムについての報告がされている．CCS2006 ではインダストリートラックとして

- Moving Toward Secure Software
- Security Priorities in Washington
- Security Perspectives in Telecommunications
- Emerging Security Threats

が設けられた．また，キーノートスピーチとして，SRI International の P. G. Neumann が"System and Network Trustworthiness in Perspective"を行った．

## 3 CCS2006 併設ワークショップ

CCS2006 では以下の 11 のワークショップが開催された．

1. Workshop on Privacy in Electronic Society (WPES)
2. Workshop on Digital Rights Management (DRM)
3. Workshop on Security of Ad Hoc and Sensor Networks (SASN)
4. Workshop on Quality of Protection (QoP)
5. Workshop on Storage Security and Survivability (StorageSS)
6. Workshop on Recurring Malcode (WORM)

[1] 発表されたセッションと論文キーワードを元に分類

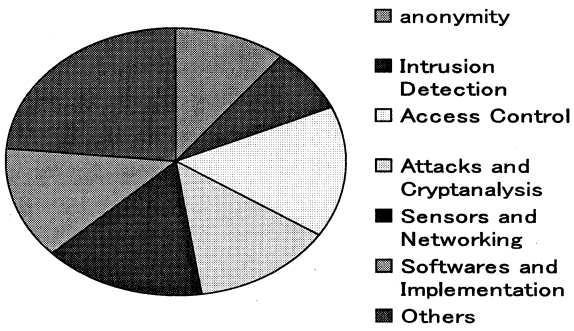


図 1: 採択論文の内訳

7. Formal Methods in Security Engineering (FMSE)
8. Workshop on Visualization for Computer Security (VizSEC)
9. Workshop on Scalable Trusted Computing (STC)
10. Workshop on Digital Identity Management (DIM)
11. Workshop on Secure Web Services (SWS)

1〜5 のワークショップは Pre-Conference として 10 月 30 日に CCS2006 と同じ会場で，6〜11 のワークショップは Post-Conference として 11 月 3 日に George Mason University，VA で開催された．各ワークショップのホームページへは [2] からリンクされている．

### 3.1 Workshop on Privacy in Electronic Society

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 5 回目を迎える．WPES2006 では 39 件の論文投稿があり，その内の 9 件がロングペーパーとして，7 件がショートペーパーとして採択された．採択率はロングペーパーだけで考えると 23.1%，ショートペーパーを含むと 41%であった．会議では"Anonymity"，"Privacy Preservation and Social Issues"，"Private Information Management"の 3 つのセッションと Short Papers のセッションが設けられ，これらの研究成果について議論された．

### 3.2 Workshop on Digital Rights Management

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著作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 6 回目を迎える．DRM2006 では 33 件の論文投稿があり，その内の 11 件が採択された．採択率は 33.3%であった．会議では，Legal Issues や Architecture，Watermarking 等，デジタルコンテンツ保護技術に関する幅広い研究結果の紹介がなされた．また，キーノートスピーチとして Hewlett-Packard の T. Kalker により"On Interoperability of DRM"が発表された．

### 3.3 Workshop on Security of Ad Hoc and Sensor Networks

Workshop on Security of Ad Hoc and Sensor Networks (SASN) は，アドホックネットワーク

ならびにセンサネットワークのセキュリティについて取り扱うワークショップである．2003年から毎年CCSの併設ワークショップとして開催され，2006年で4回目の開催である．SASN2006では5つのセッション，"Trust, Access Control and Privacy"，"Secure Routing"，"Secure Data Aggregation and Transmission"，"Attacks and Countermeasures"，"Broadcast Authentication and Key Management"が設けられ，30分の講演7件，および15分の講演9件の合計16件の発表が行われた．

### 3.4 Workshop on Quality of Protection

Workshop on Quality of Protection (QoP)は，セキュリティサービス等に量的な評価を与えるための研究開発について取り扱うワークショップである．2005年に第1回ワークショップがESORICS2005の併設ワークショップとして開催された．QoP2006では22件の投稿があり，その中から7件がフルペーパとして，2件がショートペーパとして採択された．会議では"Software Security Metrics"，"Network Security Metrics"の2つのセッションが設けられ，これらの研究成果について議論された．また，1件の基調講演 (Quality of Protection: Measuring the Unmeasurable?) と1件のパネルセッション (Is Risk a Good Security Metric?) が設けられた．

### 3.5 Workshop on Storage Security and Survivability

Workshop on Storage Security and Survivability (StorageSS2006)は昨年に引き続きCCSの併設ワークショップとして2回目の開催である．ストレージ技術は複雑な研究対象であり，セキュリティとサバイバビリティという2つの大きな問題を抱えている．具体的には，データの長期保存におけるセキュリティをどのように確保するかという課題等がある．StorageSS2006では16件の投稿があり，11件が採択された．会議は5つのセッション ("Studies and Surveys"，"Scaling Security"，"Protection and Trust"，"Secure Deletion"，"Redundancy") から構成された．なお，第1回のStorageSS2005の発表資料は[4]にて公開されているが，StorageSS2006の発表資料は公開されていない．

### 3.6 Workshop on Recurring Malcode

Workshop on Recurring Malcode (WORM)はワームの検知やその伝播についての解析，モデル化，対策手法について議論するためのワークショップである．本会議は2003年より毎年開催され，今年は4回目になる．本会議では10件の論文が発表された．また，招待講演が2件あり，Matthew Braverman (Microsoft)，Neel Mehta (ISS) らにより，それぞれMicrosoftが行うワーム対策，携帯電話を利用したマルウエアについて解説が行われた．パネルディスカッションでは，Jose Nazario (Arbor Networks)，Dan Ellis (MITRE)，Nicholas Weaver (ICSI)，David Dagon (GA Tech) らにより，"Where the worms aren't"というタイトルで議論が行われた．

### 3.7 Formal Methods in Security Engineering

The 4th ACM Workshop on Formal Methods in Security Engineering (FMSE2006)はフォーマルメソッドによるプロトコルのセキュリティ検証について議論するためのワークショップである．特に，セキュリティシステムへのフォーマルメソッド適用に関する理論研究を実用化することを目指している．本会議は2003年より毎年開催され，今年は4回目になる．本会議では21件の論文投稿があり，その内の7件が採択された．採択率は33.3%であった．また，招待講演が2件あり，J. Guttman (Mitre Corporation)，S. Zdancevic (University of Pennsylvania) らのセキュリティ検証に関する研究成果が紹介された．

### 3.8 Workshop on Visualization for Computer Security

Workshop on Visualization for Computer Security (VizSEC2006) は3回目の開催である．第1回は今回と同様 CCS 併設ワークショップとして開催されたが，第2回は IEEE Visualization 2005 併設であった．VizSEC2006 のテーマは，"Effective Internet Security Situational Awareness" であり，44件の投稿に対して19件が採択されている．VizSEC2006 では5つのセッション ("Tool Papers", "Long Papers", "Tool Update Demonstrations over Lunch", "VizSEC and VizBGP", "Short Presentations") が設けられ，これらの研究成果が発表された．また，VizSEC では研究コミュニティ形成にも力を入れており，過去3回の VizSEC の発表資料は [5] にて公開されている．

### 3.9 Workshop on Scalable Trusted Computing

Workshop on Scalable Trusted Computing (STC) 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．STC は今回が初めての開催である．STC2006 では17件の論文投稿があり，その内の7件が採択された．採択率は41.1%であった．会議では"Scalable Trust and Supporting Techniques", "Applications and Compliance", "Attestation and Binding" の3つのセッションによる発表と2件の招待公演 ("K P. Birman, Cornell Univ., Scalable Trust: Engineering Challenge or Complexity Barrier?", "G. Strongin, AMD, The Role of Trusted Computing in Internet Scale DRM") が行われた．

### 3.10 Workshop on Digital Identity Management

Workshop on Digital Identity Management (DIM) は Digital Identity について，特に User-Centric な Identity Management に関して議論するためのワークショップである．DIM は今回が2回目の開催である．DIM2006 では21件の論文投稿があり，その内の9件が採択された．採択率は42.9%であった．会議では"User-centric Identity Management Frameworks", "Applications and System Issues", "Security, Privacy and Anonymity" の3つのセッションによる発表と1件のパネルセッション (What is User-centric Identity Management?) が設けられた．本ワークショップで使われた発表資料の一部はホームページからダウンロードできる．

### 3.11 Workshop on Secure Web Services

Workshop on Secure Web Services (SWS) は，XML Security や WS シリーズ，SAML，XACML 等のウェブサービス関連の技術について議論するためのワークショップである．SWS は今回で3回目の開催である．SWS2006 では26件の論文投稿があり，その内の11件が採択された．採択率は42.3%であった．会議では"Access Control Policy/Model", "Security Architecture", "Trust Management" のセッションによる発表と，パネルディスカッション (E. Damiani, A. Gabillon, D. Staggs, B. Thuraisingham, M. Winslett, "Directions and Trends of XML and Web Service Security") が行われた．本ワークショップで使われた発表資料の一部はホームページからダウンロードできる．

## 4 International Conference on Privacy, Security and Trust

The 2006 International Conference on Privacy, Security and Trust (PST2006) [6] はプライバシ保護や信頼に関する技術について議論される会議である．今年のテーマは"Bridge the Gap Between PST Technologies and Business Services" となっており，学術的な研究をビジネスへ活かすことが目的のひとつとなっている．論文数は32編，他にショートペーパー28編が

発表され，信頼や安全性のモデル化，アクセス制御，Webベースの認証手法，匿名手法，暗号プロトコルなど，多彩なテーマが取り扱われた．また，会議ではキーノートスピーチが7件行われ，アクセス制御やネットワークセキュリティなどの具体的なテーマの他，セキュリティ教育の重要性を取り上げた講演などがあった．

2003年よりカナダにおいて毎年開催されており，今年で4回目になる．第1回目の会議はMontre'al，第2回および3回目はNew Brunswick，今回はOntarioで開催された．本会議のスポンサーはACM Special Interest Group on Security, Audit, and Control (SIGSAC)，Management Development Center (MDC)，Third Brigade，およびFaculty of Business and Information Technology (FBIT)となっている．本会議で発表された論文はACM Digital Libraryにて入手できる．また，キーノートスピーチで使用された資料は，本会議のウェブサイトで公開されている．

## 5 おわりに

本稿ではCCS2006とその併設ワークショップ，およびPST2006について報告した．


### 謝辞

本研究は科学技術振興機構の戦略的国際科学技術協力推進事業の支援を受けて行なった．


## 参考文献


[1] The 13th ACM Conference on Computer and Communications Security. http://www.acm.org/sigs/sigsac/ccs/CCS2006/.

[2] CCS2006 Workshops. http://www.acm.org/sigs/sigsac/ccs/CCS2006/workshop.html.

[3] CCS2006 Tutorials http://www.acm.org/sigs/sigsac/ccs/CCS2006/tutorial.html.

[4] StorageSS Project. http://www.projects.ncassr.org/storage-sec/.

[5] The VizSEC Community Homepage. http://www.projects.ncassr.org/sift/vizsec/.

[6] 2006 International Conference on Privacy, Security and Trust. http://www.businessandit.uoit.ca/pst2006/.