Vol.2012-CSEC-58 No.45
Vol.2012-SPT-4 No.45
2012/7/20

IFIP TM 2012 参加報告

菊池 浩明[1,a)]　Anirban Basu[1,b)]

概要：国際会議 IFIPTM は，計算可能トラストモデル，トラストマネージメント，および，関連するセキュリティとプライバシーの課題についての研究成果を共有し，更なる研究の方向性と新たな課題を明らかにすることを目的としている．本稿では，2012 年 5 月 21 日から 24 日までインド Surat 市の，Sardar Vallabhbhai National Institute of Technology にて開催された第 6 回 IFIPTM 2012 における技術発表とトピックスを報告する．

キーワード：トラスト，プライバシー，評判

Report on IFIP TM 2012

Hiroaki Kikuchi[1,a)]　Anirban Basu[1,b)]

Abstract: IFIPTM annual conferences aim to share research outcomes to the problems in computational trust and trust management, including the related security and privacy issues; and to identify new issues and directions for future research. IFIPTM 2012 was held in Sardar Vallabhbhai National Institute of Technology in Surat, India between May 21 and May 24. This article reports the talks and topics in the conference.

Keywords: trust, privacy, reputation

1. はじめに

IFIP TM は, IFIP WG 11.11 主催によるトラストマネージメントに関する第 6 回目の国際会議である．2012 年 5 月 21 から 24 日までは，インド Surat の Sardar Vallabhbhai National Institute of Technology (SV NIT), 25 日は Munbai の Centre for Development of Advanced Computing (C-DAC) で開催された．60 名程度の参加者が世界各国から集まり，セキュリティ技術，プライバシー保護技術，計算可能トラスト，トラストモデル，評判モデルなどについて議論を行った．

本会議では世界 23 国から 51 件の投稿があり，12 件のフルペーパーと 8 件のショートペーパーが採録された．採択率は 24%(フルペーパー) であり，十分な技術的な品質が期待されている．論文予稿集は，Springer から IFIP Advances in Information and Communication Technology シリーズ 374[2] として発行されている．

本会議に加えて，会議の前日には，ソーシャルネットワーキングに関するワークショップ “REASON - RagE Against the Social Network” と，クラウドコンピューティングに関するチュートリアル “Tutorial: Building Trust in Cloud ” が開催された．British Telecom でのクラウドの事例を挙げて，トラストがどの様に現場に応用されようとしているか解説されていた．会議の最終日には，会場を 400km 離れた Mumbai に変えて，Industry, Government セッションが開催された．

2. トピックス

2.1 招待講演

本会議では，バンケットでの講演を含めて 4 件の招待講演が行われた．

Britis Telecom の Theo Dimitrakos は，Trust Manage-

[1] 東海大学
Tokai University, 2-3-23 Takanawa, Minato, Tokyo 108-8619, Japan
[a)] kikn@tokai.ac.jp
[b)] abasu@cs.dm.u-tokai.ac.jp

© 2012 Information Processing Society of Japan

ment resarch community のこの 15 年間の活動過程を振り返り講演した．Dimitrakos 博士は現在 IFIP WG 11.11 Trust Management のチェアを務めており，その立場から本分野での顕著な貢献を列挙していた．彼によると，1996 年の McKnight 教授の Meanings of Trust, 1998 年の Josang 教授の A Subjectie Metric of Authentication, 1996 年の Blaze の Decentralized Trust management (policy maker), そして, 1994 年の March 博士の Trust as a Computational Concept, これらが初期のブレークスルーと位置付けている．その後の iTrust から IFIP TM への変遷を述べて，将来のトラストマネージメントの方向性を展望した．

これに対して，理論ばかり先行して企業が採用しないで終わった技術の例の様にならないだろうかという懸念や，企業におけるトラストを用いた最も成功した例は何か，といった実用に向けるいくつかの質問と議論が行われた．

次の招待講演は，Tata Consultancy Services の Global Head である Sundeep Oberoi 博士によるインドにおけるトラストマネージメントの研究と企業での展開 (deploy) との間のギャップについて議論するものであった．インドにおける PKI の課題や韓国などの事例について述べ，理論的に出来ることと実践されることは異なることを主張した．実践展開可能性を，“deployability” と定義し，cost, smiplicity, robustness, scalability の４つがその条件であると定めた．

Rajat Moona 博士による招待講演では，IIT と CDAC との共同で研究開発が進められた Trusted and Secure File System に関する技術的なものであった．Moona 博士は，IIT Kanpur の Poonam and Prabhu Goel Chair 教授であって，現在は C-DAC の所長として勤務されている．インドにおける国民 ID の構築や，電子パスポートなどの ID に関する各種の行政にも関わっており，豊富な事例と正確な技術内容に関する本講演は，聴講者に多くの示唆を与えてくれた．

2.2 Willisum Winsborough 記念賞

昨年，自動トラスト交渉 (Automated Trust Negotiation) などで本分野で多くの業績をあげた IBM の William H. Winsborough 博士が亡くなった．IFIP WG 11.11 では，その業績を称えて Willisum Winsborough 記念賞の設置を決めた．

最初の受賞者は，オンライントラスト管理と主観論理 (subjective logic) に関する業績の顕著なオスロ大学の Audun Josang 教授であり，バンケットの会場で “Robustness of Trust and Reputation Systems: Does it Matter?” と題する記念講演を行った．

副題が表すように，トラストや評判システムにおける頑強性の必要性に疑問を投げかける趣旨の講演である．不十分な robustness は，悪意のある参加者に操作されてしまうリスクがある．特に，最近の SNS などの人間に関する評判システムには課題が多く，しばしば訴訟を招くことを問題提議した．従って，人に関する評判システムは負の評価ではなく，正の方向についてのみ行うべきである．新規参入者は誰にも評価されないので，なかなか評判を上げられないという “new commer” 問題も，正についてのみの評価ならば解決されるという．もうひとつは，monopoly の問題である．いかにトラストを公平に分配して行うか，多くの技術革新が必要であると締めくくっていた．

3. 主な技術発表

主会議のプログラム（概略）を表 1 に示す．

3.1 Trust Model に関する研究

3.1.1 Robustness of Trust Models and Combinations for Handling Unfair Ratings

シンガポールの Nanyang Technological University の Lizi Zhang と Jie Zhang 助教らによる研究で，商品の評判を意図的に操作する攻撃に対する既存のトラストモデルをテストベッドの上で評価して，より頑強性のあるモデルを提案している．

ここでは評判を操作する攻撃を，Constant Attack (単純に悪意の評価を続ける)， Camofulage Attack (信頼を得るために一旦真当な評価をして正直な評価者に偽装した後，不正な評価値を送る)， Whitewashing Attack (評判を落とした後で，別のアカウントを作って過去の悪い信頼度を洗い流す)，Sybil Attack (多くの架空のアカウントを作って不正行為を行なう）などに分類している．対象とするのは，Beta Reputation System (BRS), iCLUB, TRAVOS, Personalized の 4 つのトラストモデルである．これらを，Agent Reputation and Trust Testbed (ART) を用いて攻撃し，そのロバスト性を明らかにした．iCULB が比較的多くの攻撃に対して頑強であったが，Sybil Attack には弱く，単一のモデルでは解決できないと結論づけている．そこで，これらのモデルを組み合わせることを提案しており，それによると，Discount-then-Filter の組み合わせ (TRAVOS + iCLUB, または，Personalized+BRS, Personalized + iCLUB) が最も頑強である．

(感想）大規模な実験を行い多くのモデルを評価した結果は有益である．不正な評価者を取り除くのに，SNS の情報などを使えないだろうかと思われる．発表を行った Lizi 君は堂々とした学部生で，米国の大学の PhD コースへの入学が決まっているという．

3.1.2 Co-evolving trust mechanisms for catering user behavior

Slovenia の Tanja Azderska による，トラストの評価方法に依るバイアスの大きさを評価する研究である．

我々の社会における信頼の増減には，周りの環境などの

© 2012 Information Processing Society of Japan

表 1 Technical Program

May 22	
keynote 1	A perspective on the evolution of the international Trust Management research community in the last decade (Theo Dimitrakos).
Session 1	Perturbation based privacy preserving Slope One predictors for collaborative filtering (Anirban Basu, Jaideep Vaidya and Hiroaki Kikuchi).
	Robustness of Trust Models and Combinations for Handling Unfair Ratings (Lizi Zhang, Siwei Jiang, Jie Zhang and Wee Keong Ng).
Session 2	Co-evolving trust mechanisms for catering user behavior (Tanja A?derska).
	Incorporating Honeypot for Intrusion Detection in Cloud Infrastructure (Bhavesh Borisaniya, Avi Patel, Dhiren Patel and Hiren Patel)
Session 3 (Short papers)	Rendering unto Caesar the Things that are Caesar ' s: Complex Trust Models and Human Understanding (Stephen Marsh, Anirban Basu and Natasha Dwyer).
	Trust Management Framework for attenuation of Application Layer DDoS Attack in Cloud Computing (Dipen Contractor and Dhiren Patel).
	An Incentive Mechanism to Promote Honesty in E-marketplaces with Limited Inventory (Yuan Liu, Jie Zhang and Qin Li).
keynote 2	Robustness of Trust and Reputation Systems: Does it Matter? (Keynote – Audun Josang).
May 23	
Session 4	Integrating Indicators of Trustworthiness into Reputation-based Trust Models (Sascha Hauke, Florian Volk, Sheikh Mahbub Habib and Max Muhlhauser).
	Finding Trusted Publish/Subscribe Trees (Stephen Naicken, Ian Wakeman and Dan Chalmers).
Keynote 3	Operational Challenges in deploying Trust Management Systems - A practical perspective (Sundeep Oberoi).
Session 5	Trust Model for Optimized Cloud Services (P. S. Pawar, M. Rajarajan, S. K. Nair and A. Zisman).
	Post-Session Authentication (Naveed Ahmed and Christian D. Jensen).
Session 6	A Provenance-based Trust Model for Delay Tolerant Networks (Jin-Hee Cho, MoonJeong Chang, Ing-Ray Chen and Ananthram Swami).
	Trust Transitivity and Conditional Belief Reasoning (Audun Josang, Tanja A?derska and Stephen Marsh).
Session 7 (Short papers)	How Events Affect Trust: A Baseline Information Processing Model with Three Extensions (D. Harrison McKnight, Peng Liu and Brian T. Pentland).
	Improvements over Extended LMAP+: RFID Authentication Protocol (Jitendra Gurubani, Harsh Thakkar and Dhiren Patel).
	Automated Evaluation of Annotators for Museum Collections using Subjective Logic (Davide Ceolin, Archana Nottamkandath and Wan Fokkink).
May 24	
Session 8	An efficient approach for Privacy Preserving distributed K-Means clustering based on Shamir ' s secret sharing (Sankita Patel, Sweta Garasia and Devesh Jinwala).
	From subjective reputation to verifiable experiences - augmenting peer-control mechanisms for open service ecosystems (Sini Ruohomaa, Puneet Kaur and Lea Kutvonen).
Keynote 4	transCryptFS: A Trusted and Secure File System (Rajat Moona).
Session 9 (Short papers)	A New Data Integrity Checking Protocol with Public Verifiability in Cloud Storage (Mihir Gohel and Bhavesh Gohil).
	Document and Author Promotion Strategies in the Secure Wiki Model (Kasper Lindberg and Christian Damsgaard Jensen).

複雑な振舞いが影響する．信頼を得るのには長い間かかるのに，それを失うのは一瞬であったりする．そのような振舞いの一つとして，評価方法に依るバイアスの大きさを検討している．1) 数値による 1 から 5 段階の評価，2) 否定的な表現 (Not useful at all など)，3) 肯定的な表現 (Extremely useful) の 3 種類で，86 名の評価者を 3 分割して同一の対象を評価した．実験によると，肯定的な表現の影響が大きいことが明らかになった．

(感想) 社会認知学者や実験心理学者が行なっているようなテーマである．違いは，それらが科学的な目的で人の生体を明らかにするのに対して，この研究はそれらの知見を工学に応用するところにある．著者らは，評価者の顔の表情などを見て正直な度合いを評価できないかと，色々な観点で検討をしていた．なお，Skype でのテレビ会議で発表が行われていたが，十分に議論が出来ていた．

© 2012 Information Processing Society of Japan

3.1.3 Trust Transitivity and Conditional Belief Reasoning

Oslo 大学の Josang らによる，推論におけるトラストの推移性に関する研究である．主観論理の枠組みを仮定している．

主観論理 (Subjective Logic) では，信頼 (Belief) と不信頼 (Disbelief) の間に加えて，不確実性 (Uncertainty) という 2 つの軸での値で意見を定量化しており，その 3 点を頂点とする三角形のマップの上で信頼の度合いが表される．この時，X ならば Y という関係があり，X が主観論理で与えられた時，Y の信頼度をどう定めるかという問題を研究している．この問題に対して，いくつかの要請を元に，前提と結論の間の 2 つの三角形 (Frame) の信頼度の線形近似で与える方式を提案している．トラストの推移性に関しては様々な意見があり，まだ決定的な理論には定着していない．

(感想）主観論理はこのコミュニティではよく知られた理論のようで，初めて聞く報告者にはその必然性や背景がよく分からなかったが，信頼と不確定性という 2 つの独立した軸があることには同意が出来る．今回の発表に対しては，再帰的な推論を繰り返した時の保証や，古典的な 2 値論理との関係が疑問に残った．

3.1.4 Rendering unto Caesar the Things that are Caesar's: Complex Trust Models and Human Understanding

Canada の Communication Research Centre の Stephen Marsh らによる Position Paper で，複雑なトラストモデルをどうやって人々に理解してもらえるかについての意見を述べている．

90 年代から発達したトラストモデルの研究は，しばしば数学的に複雑な形に発達し，現実世界へ実践展開することが出来ないでいることの反省に立ち，シンプルな実践のための次の 6 つの要請を Manifesto for Simplicty として提案してる．

(1) The model is for people.
(2) The model should be understandable (専門家だけでなく一般の利用者にとって)
(3) Allow for monitoring and intervention. (透明性を高くする)
(4) The model should not fail silently. (失敗したらそれを明確に伝えるべきである)
(5) The model should allow for a deep level of configuration. (ベストなモデルは存在しないものと認識し，誰にでも合せられるように再設定を可能にする)
(6) The model should allow for querying. (不明な点を問い合わせできるインターフェースを用意すべきである)
(7) The model should cater for different time priorities. (時には精度より即応性を必要とする時がある)
(8) The model should allow for incompleteness. (人々が考えを変えても対応できるようにすべきである)

(感想)　今までのトラストモデルが学者の為のモデルになっていることを，自ら反省している姿勢が謙虚．マニフェストについては異論も出ていた．必ずしも守られないものがマニフェストであるかも．

3.2 Privacy に関する発表

3.2.1 An efficient approach for Privacy Preserving distributed K-Means clustering based on Shamir's secret sharing

SV NIT の Sankita Patel らによる，秘密分散による秘匿クラスタリング方式の提案と評価を行なっている．プライバシー保護データマイニング (PPDM) の一提案.

Jha らが ESORICS 2005 で提案した分散 k-means アルゴリズムでは，TTP を用いて分散処理をしていたのに対して，秘密分散をすることで TTP を取り除いている．同様の処理を準同型性暗号や秘匿多項式評価 (Oblivious Polynomial Evaluation) を用いて行った場合に比べて，通信コストも計算コストも著しく改善していることを主張している．

(感想) 提案方式では，各クラスタの重心が毎回全員に漏れることになり，他の PPDM の方式で目指しているものと要請条件が異なっている．実験評価も Matlab によるもので，その信頼性にも疑問が残る．著者は，これが主の研究テーマではないとのことで，今後の改善は期待できまい．会場からは，直ぐに “big data” への適用可能性を問う質問が出ていた．

3.2.2 Perturbation based privacy preserving Slope One predictors for collaborative filtering

報告者自身による情報推薦におけるプライバシー保護の一提案である．

Slope One と呼ばれる情報推薦アルゴリズムが，ランダム摂動化 (Random perturbation) に対してロバストであることを利用して，評価値に乱数を加算したままで情報推薦値を求めることを可能にしている．発表では，基本の方式に加えて，情報提供者がノイズを加える場合，被推薦者がノイズを加える場合，更に，加法準同型暗号を組み合わせた場合についての検討を行なっている．

(感想）本発表に対して，加法準同型性暗号の他の方式との比較や，しきい値暗号を用いることの可能性，摂動化をしないで暗号化のみで情報推薦出来ないのか，といった質問が寄せられた．暗号化を組み合わせるのは本発表の趣旨ではなく，既に暗号化のみによる情報推薦方式を発表済みであることを回答したが，多くの人の興味は摂動化でなく暗号に行ってしまった点は残念であった．

© 2012 Information Processing Society of Japan

3.3 Trust の応用に関する研究

3.3.1 Automated Evaluation of Annotators for Museum Collections using Subjective Logic

オランダの VU 大学の研究で，第二著者の Archana Nottamkandath が発表を行った．美術館における作品に対する注釈付 (annotation) をクラウドソーシングで行い，その注釈の品質を主観論理の上で評価する応用研究である．

1784 個の展示品の画像にタグ付を行い，そのタグが「有益」か「不要」かに分けた評価データを学習データとして，提案方式の評価を行なっている．その結果，0.7 以上のトラストレベルを持つ評価値は「有益」であるという判定が得られていた．

(感想）分かりやすい応用研究である．ただし，判定を行うアルゴリズムは，従来の主観論理の仕組みをそのまま使っているようで，そこに新規性は見られなかった．今後クラウドソーシングが盛んになることが予想され，この様な研究の重要性が増すものと考える．

3.4 Network における Trust モデルの研究

3.4.1 A Provenance-based Trust Model for Delay Tolerant Networks

US Army Research Laboratory の Jin-Hee Cho による軍用ネットワークにおけるトラストの応用研究である．

対象とするネットワークは，頻繁なリンクダウンや遅延を想定した互いの存在の保証がないという特殊なものである．この環境で正しく情報を交換するために，Provenance (来出所歴の記録）に基づくトラストモデルを提案している．移動を許されたノードを含むトラストの計算方式を定めて，ペトリネットによる評価結果を報告している．

(感想）ほとんど予備知識のない分野であったが，アカデミックからは遥かに距離があると思われていた軍でトラストが応用されている事実は興味深い．

3.4.2 Post-Session Authentication

デンマーク工科大学 (TUD) の N. Ahmed と C. D. Jensen による新しい認証スキームの概念の提案である．Jensen によって発表された．

Post-Session Authentication と呼ぶこの認証手順では，プロトコルの最初ではなくて，最後に認証を行い自分が正規の利用者であることを相手に納得させる．これは新しい概念ではなくて，既に実用的なプロトコルで運用されているものであり，その証拠として DH 鍵交換を行った後で認証の為のハッシュ値を交換する PGPfone の例と，商談が成立するまで互いに匿名のままでプロトコルを実行するコカインオークションの例を挙げた．本論文は，この概念を明確に定義して，要求条件を定めて定式化をしている．

(感想） 知っている筈の仕組みなのに，確かに正しく定められていなかった概念である．数学的に厳密な定式をして，いくつかのセキュリティの性質を証明している．理論と実践の両方をよく知っている研究者の仕事である．

4. その他

4.1 Banquet

Banquet は，初日 22 日の夜，Taj hotel グループの Gateway ホテルで開催された．前述したアワードなどの授賞式やスピーチの合間に，地元の少女のダンススクールによる本格的なインド舞踊が演じられて好評であった．食事はもちろんカレーを中心としているが，インド人向けのベジタリアンだけでなく，ノンベジーの料理も充実しており，辛すぎることもなく楽しめた．

4.2 Surat について

Surat は Munbai から 400km ほど北上したインド第 9 番目に人口が多い地方都市であり，ダイヤモンドの錬磨やシルク産業で世界的に知られている．世界のダイヤモンドの 92%はこの都市で磨かれるそうだ．しかし，この街には道路も広く終日交通量も多いのに，信号機がない (!)．交差点を右折するには，クラクションを鳴らし続けてのチキンレースをすることになり，毎回肝を冷やした．大学からの送迎バスがなければ，歩いて渡ることすらおぼつかない．なお，Gujarat 州に属していて，飲酒は州の法律で禁じられている．

4.3 Industrial Truck

最終日に開催された Industrial Truck では，本会議のスポンサーになっている Tata Consulting Service や国立の研究組織である CDAC (Centre for Development of Advanced Computing) の技術者が交流して，トラストモデルの意義や応用に関する議論が行われた．

欧米では，トラストの利用がオンラインの商取引で重要な役割を果たすであろうことが既に認識されてビジネスの観点で動き始めているが，インドではまだ興味はよりインフラに近いセキュリティにあることが議論を通じて感じられた．

4.4 インド人しか買えないチケットの謎

Mumbai から Surat までは，Low-cost carrier の Spice Air で一日一往復の便を利用するか，電車で 3 時間か，車で 5 時間かの選択肢しかないが，この航空券を外国から購入することが出来なかった．ウェブページは英語で丁寧に作られているが，どの種類のクレジットカードを使っても受理されることがなく，会議の参加者はみな途方に暮れた．結局，実行委員長の Patel 教授に E-ticket を立て替えてもらい，現地で支払うことになった．

なぜ海外から購入できなかったのか?

まず，英語で書いてあるから外国人向きというのが大きな誤解であった．インドには 700 を超える言語があると言

© 2012 Information Processing Society of Japan

われており，地域が違うと意思の疎通が出来ないほど多様性が高い．この社会の中で共通に会話をするためには，英語が公用語として使われている．つまり，英語で書かれているのは，インド人向けでだった訳である．次に，インドでは人口が多いので，国内向けの需要だけで十分にビジネスになり，海外観光客などの配慮が要らないという背景があった [1]．更に，日本国内でルピーが換金できないとか，WiFi のアカウントがインド内の銀行口座がないと支払えないとか，他国を無視する様な事例に接するたびに，そのことを強く実感した．

5. おわりに

SNS や電子商取引，オンラインマーケットの広がり共に，トラストや評判システムの応用分野は広がっており，その必要性がますます増していることを認識した．その一方で，理論と実践との間にまだ距離があることも多くの人が課題として受け止めている．

実行委員長である SV NIT の Dhiren Patel 教授のホストは行き届いており，参加者へのホテルや空港への送迎や大学のゲストハウスでの食事の招待など，きめ細かなサービスが行われていた．当初は大都市の Mumbai で開催するつもりだったが，多くの人の勧めもあり Surat での開催を断行したという．そのお陰で，より生のインドの生活やスリリングな交通事情を味合うことが出来ただけでなく，健康的な一週間であった．

参考文献

[1] 白水 和憲，「本当はどうなの？これからのインド」，中経出版，2009.
[2] Theo Dimitrakos, Rajat Moona, Dhiren Patel and D. Harrison McKnight eds., “Trust Management VI”, 6th IFIP WG 11.11 International Conference, Proceedings, 2012.

© 2012 Information Processing Society of Japan