Vol.2017-IOT-39 No.6
Vol.2017-SPT-25 No.6
2017/9/29

IFIPTM 2017 参加報告

島岡政基[†1]　真野健[†2]　西垣正勝[†3]

概要：国際会議 IFIPTM は，関連するセキュリティとプライバシーの問題を含む，トラストおよびトラストマネジメントに関する問題の研究成果を共有し，今後の研究開発の新たな課題と方向性を明らかにすることを目的としている．本稿では，2017 年 6 月 12 日から 16 日までスウェーデン Göteborg 市において Chalmers | University of Gothenburg の Lindholmen キャンパスで開催された第 11 回 IFIPTM 2017 における技術発表とトピックスを報告する．

キーワード：IFIPTM，トラスト，トラストマネジメント

Report on IFIPTM 2017

Masaki SHIMAOKA[†1]　Ken MANO[†2]
Masakatsu NISHIGAKI[†3]

Abstract: IFIP WG 11.11 International Conference on Trust Management (IFIPTM) aims to share research solutions to problems of Trust and Trust management, including related Security and Privacy issues, and to identify new issues and directions for future research and development work.　11th IFIP WG 11.11 International Conference on Trust Management　was held on the Lindholmen campus of Chalmers | University of Gothenburg, Sweden between June 12th to June 16th.　This article reports the talks and topics in the conference.

Keywords: IFIPTM, Trust, Trust Management

1. はじめに

IFIPTM2017[a]は，情報処理国際連合(IFIP，International Federation for Information Processing)の WG 11.11 が主催するトラストマネジメントに関する第 11 回目の国際会議である．2017 年 6 月 12 日から 16 日までスウェーデン Göteborg 市の Chalmers | University of Gothenburg の Lindholmen キャンパスで開催された．約 30 名の参加者が世界各国から集まり，トラスト，およびその隣接分野（社会技術，経済学，社会学，評判管理，アイデンティティ管理，セキュリティ，プライバシー，大規模化など）との境界領域ついて議論を行った．

IFIPTM2017 は，前半 2 日間の Graduate Symposium と，後半 3 日間の本会議で構成されている．本会議では，29 件の投稿から 8 件のフルペーパーが採録され，これとは別に 6 件のショートペーパーが採録された．採択率は 27.6%（フルペーパー）で，十分な品質が確保されていると言えるだろう．論文集は Springer から IFIP Advances in Information and Communication Technology シリーズ 505 として発行されている[1]．Graduate Symposium のチュートリアルと本会議の各セッションについて表 1 に後述する．

2. Graduate Symposium

前半 2 日間に開催された Graduate Symposium は，主に大学院生を対象としたシンポジウムで，チュートリアル，インタラクティビティ，研究テーマ紹介がそれぞれ行われた．

チュートリアルでは，計算可能トラストや，トラストアプリケーションとしてのセキュリティやプライバシー，さらには今回の本会議の特別テーマでもある自動車ネットワークにおけるトラストについて講義が行われた．

インタラクティビティは，信頼に関するトピックとチームをその場で決めて，2 日間に分けてディスカッションを行い，最後に発表を行った．今回は，ブロックチェーン，信頼情報のデータセット構築という 2 つのトピックを扱ったが本稿では詳細は割愛する．インタラクティビティでは，チーム内のコミュニケーションによる相互信頼を深めることも明な目的のひとつであり，IFIPTM らしい企画と言える．

研究テーマ紹介は，文字通り学生による自身のテーマ紹介だが，一度目の発表で会場から出た意見を踏まえて翌日再度発表を行い，評価の高かった学生は本会議でもテーマ紹介の機会を与えられる，というものである．これは若手のエンカレッジという点で非常に興味深い取組みであった．

2.1 チュートリアル

主筆者は今回初めての参加だったことと，チュートリアルが聴けることを目当てに本シンポジウムにも参加した．

†1 セコム株式会社 IS 研究所
SECOM CO., LTD., Intelligent Systems Laboratory
†2 日本電信電話株式会社 NTT コミュニケーション科学基礎研究所
NTT Communication Science Laboratories, NTT Corporation
†3 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

a http://wp.portal.chalmers.se/ifiptm2017/

シンポジウム参加者は学生含め 10 名ほどと小規模だった半面，IFIPTM のキープレイヤーたちを中心にかなり濃い議論が交わされていた．

チュートリアルでは，トラストという多義的な概念を様々な切り口から論じることによって，参加者の共通認識を深めることに成功しているように感じた．例えば Marsh は，トラストに類似あるいは関連する概念として自信，確率，評判，安全(Safety)，合理性，制御，セキュリティ，リスクについてトラストとの共通点や差異を論じた上で，トラストを扱うシステムには必ず人間が包含されており，トラストをモデル化するにはその人間を理解することこそが重要であることを繰り返し述べた．また Dwyer は，これまでの様々なトラストに関する議論を引用し，コミュニケーションとしてのトラストと社会デザインの関係性や，トラストの 3 つの構成因子である能力（competence），動機付け（motivation），一貫性（continuity）についても丁寧に論じた．いずれも論であって学ではなく，チュートリアルと言えどまさに研究者のためのチュートリアルであり，大いに刺激になった．

トラストマネジメントという学際的な領域での議論において，ともすれば発散しがちなトラストという用語の理解が，情報セキュリティに限らず様々な分野から参加する研究者の間でほとんどブレていなかったのは特筆すべき点であり，中心メンバーが継続的に参加してこうした啓発を続けてきた賜物なのだろうということを強く実感した．

3. 基調講演

本会議では 3 件の基調講演が行われた．

1 本目の基調講演者であるドイツ Darmstadt 工科大学の Max Mühlhäuser 教授によれば，信頼性のレベル・度合いを評価する計算可能トラストは，評判システムや確率的アプローチなどによって研究が進んでおり，セキュリティのためのトラストとしてはサービスの信頼を評価できる必要があることを述べた．その一例として，クラウドサービスの信頼性を評価する Cloud Security Alliance による Security, Trust & Assurance Registry (STAR) や，ルート認証局の信頼性を自動的にレピュテーション評価する CA-TMS (Certification Authority Trust Management System) が紹介された．CA-TMS は Mühlhäuser 教授の研究室で取り組んでいる研究テーマのひとつであり，実装もオープンソースで提供されている．一方のトラストのためのセキュリティとしてプライバシー保護技術が挙げられた．しかしながら，プライバシーとトラストは両立しない時もあり，セキュリティとトラストもまた両立しない時があるとも述べており，引き続き議論が必要であると感じた．

開催地である Göteborg 市に本社を構える Volvo Group の Mathias Widman は，2 本目の基調講演の中で，自動車がネットワークを介して様々なサービスと接続するようになる，いわゆる拡張車両(Extended Vehicle)のためのトラストとセキュリティについて講演した．拡張車両には膨大な数の制御機器が搭載されるだけでなく，長期保守の中でそれらが様々な品質のものに入れ替わっていく可能性がある．計算可能トラストは，これを解決可能な技術として期待している．しかし，拡張車両のトラストとセキュリティを実現するには多岐にわたる課題がある．膨大な制御機器の個体識別を含む信頼性やその製造拠点のセキュリティ，鍵生成を含む安全な鍵管理，さらに流通後においてはディーラー以外での制御機器の換装や路上修理，車両廃棄手続き，セキュリティの保守をどう実現するか，などが挙げられた．

3 本目の基調講演は, IFIPTM から HP Labs の Siani Pearson 博士への 2017 年度 William Winsborough 記念賞授賞(IFIP WG 11.11 が授与する annual award)を記念しての講演であった．同博士は，IT の急激な発展に伴うプライバシーやセキュリティのリスクが高まる中で，法的責任(Liability)より広い概念としてのアカウンタビリティを適用することが行政に限らずビジネスにおいても有用である，更には信頼性を向上させる強力な根拠となり得るような「強いアカウンタビリティ」が重要である，と述べた．アカウンタビリティはトラストを高めることができるが，必要条件でも十分条件でもない．そこで，法律や契約，倫理にもとづく規範への準拠という通常のアカウンタビリティを拡張し，その証跡としてのログの生成・検証も含めた「強いアカウンタビリティ」が必要であると述べ，その具体例としてプライバシーと EU 一般データ保護規則の関係を引き合いに出しながら解説された．

4. 本会議

本節では，筆者らにとって興味深かった発表を各セッションから 1 件ずつ概説する．個々の詳細は[1]を参照されたい．

4.1 Novel Sources of Trust and Trust Information

本セッションからは，ショートペーパーだが興味深い研究として Davide Ceolin らの“Social Network Analysis for Trust Prediction”を概説する．オンラインサービスとオフラインサービスの関係が密接になるにつれ，オンラインサービスにおけるエンドユーザの信頼管理はますます重要になる．Ceolin らは，ソーシャルウェブにおけるユーザプロファイルから各ユーザの信頼を推定するフレームワークを提案する．このフレームワークは，3 つのユーザ特徴(人口統計，知識プロファイルに加えて次数中心性など 5 つのネットワーク中心性)を用いてユーザの信頼を評価する．ここでは KONNEKTid[b]が提供するデータセット(2012 年 9 月～2015 年 8 月までの約 37 千件のログ)を用いて評価した．KONNEKTid とは，ある技術を学びたい時に近所から教師を見つけ，実際に会って指導を受けることを実現する，い

b https://www.konnektid.com/

わゆるマッチングサービス型の知識共有プラットフォームである．各ユーザの 1) 活動(アクティビティ)件数，2) 他ユーザとの活動件数，3) 平均活動頻度，4) 承認したリクエスト件数，5) 承認した予約(指導)件数について，5 つのネットワーク中心性を用いて信頼性を推定した．推定には分類アルゴリズムとして Support Vector Machine および Naive Bayes)を用い，43〜99%の推定精度が得られた．今後は測定値を拡充するとともに精度の向上や他の予測アルゴリズムについても検討していく予定とのことである．

4.2 Trust Metrics

本セッションのフルペーパーから，真野健らの“Trust Trust Me (The Additivity)”を概説する．本発表では，質と量のペアを用いて定量的なトラストを定式化し，トラストが加法性を持つという仮定にもとづいてトラストの合成演算やその計算の妥当性を論じた．トラストを加重値とみなすことで計算結果が総和を超えないという健全性を有する．また，信頼関係の演算子として並列合成⊎と逐次合成∗を定義し，これら代数的属性を用いて，トラスト計算のプロトコルとその有用性を示した．トラストの定式化では，確率論に基づく Subjective Logic が知られているが，代数的属性だけで定式化した点は大変興味深い．

4.3 Information Sharing and Personal Data

本セッションのフルペーパーである，Shuo Chen らの “A Flexible Privacy-preserving Framework for Singular Value Decomposition under Internet of Things Environment”を概説する．IoT 環境ではデータ分析の大半がフォグコンピューティングによって処理されると予想される．Chen らは，特異値分解を応用することで，信頼できないフォグコンピューティングにおいて柔軟なプライバシー保護を実現するデータ分析フレームワークを提案した．このフレームワークは，特異値分解演算を 2 つの固有ベクトル分解演算に分割し，2 つのタスクを異なるデバイスに分配する．想定するフォグコンピューティングは，データを入力(または測定)する Environmental Device (ED)の上に，ED と直接通信してデータを収集する First Layer Fog Device (FD)と，FD からデータを受け取って特異値分解演算を行う 3 種類の Second Layer Fog Device との二層によって構成される．FD および SD は honest-but-curious であるが，相互に結託はしないものと仮定することで，FD および SD による盗聴や漏洩や各ノード間の通信は安全であることを証明した．性能分析により，処理効率(演算および通信)に最も影響するのはデータ次元であることが示された．本フレームワークの応用先の一例として，多数の評価者(住民)が近隣の飲食店の評判を入力しつつ，ローカルなネットワーク内での評価者のプライバシーを保護するような飲食店評判システムが挙げられた．

4.4 Reputation Systems

“Reputation-Enhanced Recommender Systems”はドイツ Regensburg 大学の Christian Richthammer らによる発表で，今回 Best Paper Award を受賞している．推薦システムの研究には，評判システムを組み合わせて強化する取組みも多く，著者らは，この両者を組み合わせている既存研究についてサーベイを行っている．なお，ここで想定する推薦システムとは，物品購入などのアイテムを推薦する類であり，同様に評判システムとは，あるユーザの振る舞いに対して例えば別のユーザが評点をつける類のものを指す．本発表では両者の組み合わせ方，適用領域，推薦アルゴリズムに使われる各種手法など 6 つの評価軸によって，26 件の研究について分類を行い，それを踏まえて今後の両者の組み合わせ方についての考察を行った．評価軸は，ごく単純なものを除けばいずれも既存のサーベイ手法を引用して丁寧に論証を与えており，この点も評価されたものと思われる．

4.5 Applications of Trust

本セッションのフルペーパーとして Giuseppe Primiero らによる“Managing software uninstall with negative trust”について概説する．著者らは負の信頼について信頼を拒否する状態(trust denial)と信頼のない状態(trust removal)を区別しており，前者を distrust，後者を mistrust と呼び，これらを記述する自然演繹の論理体系として(un)Secure ND をこれまでに提案している．本発表は，この(un)Secure ND をソフトウェア構成管理の整合性問題に応用する提案である．例えばインストールしたくないパッケージがある場合，それを必要としない(依存関係を持たない)パッケージを決定する必要がある．一方，インストールしたいパッケージがある場合には，それとの競合を解決するためにいくつかのパッケージをアンインストールするかも知れない．前者のインストールしたくないパッケージは distrust と定義し，後者のいくつかのパッケージがアンインストールされたシステムは mistrust と定義する．著者らはこれらを定式化し，現在は定理証明器 Coq を用いて検証を試みている最中である．

5. おわりに

トラストをテーマのひとつとして扱う国際会議はいくつかあるものの，IFIPTM はトラストそのものをメインテーマとして扱い，かつ隣接分野と多彩な交流を実践している点で非常に興味深いものであることを改めて認識した．特にトラストの概念が多義的であるが故に，多分野からの交流は議論が発散しがちである．しかし，IFIPTM では多分野から集まった研究者が多角的かつ丁寧に議論を積み重ねることでお互いのトラストに対する共通認識が深まっており，その上でそれぞれの観点からトラストについて論じ研究を進めていることが強く実感できた．これは，国内での本分野における研究コミュニティを形成していく上での大きな示唆となり得る．

開催地の Göteborg は，ストックホルムとは反対(西)側に

位置する港湾都市で, スウェーデン第 2 位の人口 52 万都市である．会場は繁華街とは運河を挟んだ対岸にあるが，フェリーの定期運航があり，人々にとって船が日常的な交通機関であることがよく実感できた．日本語の観光ガイドなどではしばしば「ヨーテボリ」または「イェーテボリ」と記されているが，現地ではまったく通じず，聞いてみると現地のスウェーデン人(n=2)も交通機関のアナウンスも「ゲーゼンバーグ」と発音していることがわかった．読み方もグローバル化が進んでいるようである．スウェーデンかつ港湾都市ということもあって，食事が大変美味しかった．スウェーデンと言えば固めのクネッケが有名だが，パンもとても美味しく，これだけでワインが飲み続けられるほどよく合うし，もちろんスモークサーモンやニシンのマリネも鉄板である．

参考文献

[1] Steghöfer, Jan-Philipp, and Babak Esfandiari. “Trust Management XI,” 11th IFIP WG 11.11 International Conference, IFIPTM 2017, Gothenburg, Sweden, June 12-16, 2017, Proceedings, *IFIP AICT*, Vol.505, 229p (2017).

表 1　Technical Program[c]

Graduate Symposium	
Tutorial	Introducing Computational Trusts, its uses, and Systems (Stephen Marsh)
	Computational Trust and its relationships with IT Security (Christian Jensen)
	Trust as a Social Construct, its uses in the online world (Natasha Dwyer)
	Trust in Application Security: Can't live with it, can't live without it (Musard Balliu)
	Homomorphic Encryption - an answer to privacy? (Anirban Basu)
	Trust in Vehicular Networks (Jan-Philipp Steghöfer)
Day 1	
Keynote 1	Trust for Security – Security for Trust(Max Mühlhäuser)
Session 1	Novel Sources of Trust and Trust Information
	The Game of Trust: Using Behavioural Experiment as a Tool to Assess and Collect Trust-Related Data (Diego de Siqueira Braga, Marco Niemann, Bernd Hellingrath and Fernando B. de Lima Neto)
	Social Network Analysis for Trust Prediction (Davide Ceolin and Simone Potenza)
	Investigating Security Capabilities in Service Level Agreements as Trust-Enhancing Instruments (Yudhistira Nugraha and Andrew Martin)
Session 2	Trust Metrics
	Trust Trust Me (The Additivity) (Ken Mano, Hideki Sakurada and Yasuyuki Tsukada)
	Towards Statistical Trust Computation for Medical Smartphone Networks Based on Behavioral Profiling (Weizhi Meng and Man Ho Au)
	Advanced Flow Models for Computing the Reputation of Internet Domains (Hussien Othman, Ehud Gudes and Nurit Gal-Oz)
Session 3	Information Sharing and Personal Data
	Partial commitment – "Try before you buy" and "Buyer's remorse" for personal data in Big Data & Machine learning (Lothar Fritsch)
	VIGraph – a framework for verifiable information (Anirban Basu, Mohammad Rahman, Rui Xu, Kazuhide Fukushima and Shinsaku Kiyomoto)
	A Flexible Privacy-preserving Framework for Singular Value Decomposition under Internet of Things Environment (Shuo Chen, Rongxing Lu and Jie Zhang)
Day 2	
Keynote 2	Extended vehicle trust and security (Mathias Widman)
Panel Discussion	Trust on the road: vehicular networks beyond security
	(Max Mühlhäuser, Siani Pearson, Christian Sandberg, Mathias Widman, Tomas Olovsson, Moderator: Jan-Philipp Steghöfer)
Session 4	Reputation Systems
	Reputation-Enhanced Recommender Systems (Christian Richthammer, Michael Weber and Günther Pernul)
	Self-reported verifiable reputation with rater privacy (Remi Bazin, Alexander Schaub, Omar Hasan and Lionel Brunie)
Day 3	
Keynote 3	Strong Accountability and the New IT (Siani Pearson)
Session 5	Applications of Trust
	Managing software uninstall with negative trust (Giuseppe Primiero and Jaap Boender)
	Towards Trust-aware Collaborative Intrusion Detection: challenges and solutions (Emmanouil Vasilomanolakis, Sheikh Mahbub Habib, Rabee Sohail Malik, Pavlos Milaszewicz and Max Mühlhäuser)
	Self-trust, Self-Efficacy and Digital Learning (Natasha Dwyer and Stephen Marsh)

c 一般セッションのイタリック体はショートペーパー．太字は本稿にて紹介している論文である．