国際会議 ARES2013 参加報告 —セキュリティ共通問題の観点から—

大久保 隆夫[1,a)]　海谷 治彦[2,b)]　鷲崎 弘宜[3,c)]

概要：本稿では，2013 年 9 月にドイツ・レーゲンスブルクにおいて開催されたセキュリティの国際会議 ARES への参加について報告する．筆者らが本会議に参加した目的は，ソフトウェアのセキュリティパターンに関する研究発表を行なうとともに，ソフトウェアのセキュリティに関する共通問題の調査を行なうことである．ARES ではセキュリティモデルやソフトウェアセキュリティのセッションにおいて，対象となるソフトウェアのデータセットが扱われていたが，共通問題として扱われているものはなかった．この他本会議ではセキュリティ全般が幅広く扱われており，新しい分野への対応も早い．今回はモバイルや制御系，航空交通管理 (ATM) のセキュリティなどのテーマのセッションが見られた．

1. はじめに

著者らは，2013 年 9 月 2 日?9 月 6 日にドイツ・レーゲンスブルク大にて開催されたセキュリティの国際会議 ARES に参加した．本稿はその参加内容について報告する．

著者らが，ARES に参加した目的は発表，および調査の２つである．

- セキュリティのテストを容易にするセキュリティデザインパターンについて提案
- セキュリティに関わるソフトウェアの共通問題 (開発手法の実験，評価用の標準的なデータ) の現状についての調査

後者の共通問題は，ソフトウェアの開発において，開発手法の評価を行なうためのデータとして必要なものであるが，現在セキュリティを対象にした適切な共通問題がない．著者らは，平成 25 年度より共同で，セキュリティ，プライバシーのための共通問題の調査研究を行っている．

2. 会議の概要

ARES は正式名称を the international conference on Availability, REliability and Security と呼び，可用性，信頼性およびセキュリティを対象とした国際会議で，今回 8 回目となる．主催は ICT 知識移転学会および SBA Research センターである．今回の参加者数は 237 人であった．参加者の所在国は，ドイツ，オーストリア，イタリアなどヨーロッパ系が多いが，日本からの参加者は前述の 3 ヶ国に続いて 4 番目に多い（韓国は 7 位，中国は 13 位，米国は 6 位）．なお，会議の採択率は 24%以下である．

ARES は本会議の他に，多くのサブワークショップが併催されるのが特徴である．今回も下記の 14 のワークショップが開催された．

- ARES Industrial Track 2013
- FARES 2013 (The Eight International Workshop on Frontiers in Availability, Reliability and Security)
- SecSE 2013 (The Seventh International Workshop on Secure Software Engineering)
- WSDF 2013 (The Sixth International Workshop on Digital Forensics)
- RISI 2013 (The Third International Workshop on Resilience and IT-Risk in Social Infrastructures)
- SeCIHD 2013 (The 3rd IFIP International Workshop on. Security and Cognitive Informatics for Homeland Defense)
- SecOnT 2013 (The Second International Workshop on Security Ontologies and Taxonomies)
- IWSMA 2013 （The Second International Workshop on Security of Mobile Applications）
- MoCrySEn 2013 （The Second International Workshop on Modern Cryptography and Security Engi-

[1] 情報セキュリティ大学院大学 情報セキュリティ研究科
横浜市神奈川区鶴屋町 2-14-1
[2] 信州大学 工学部
[3] 早稲田大学 基幹理工学部
[a)] okubo@iisec.ac.jp
[b)] kaiya@shunshu-u.ac.jp
[c)] washizaki@waseda.jp

図 1 会場のレーゲンスブルク大学

図 2 本会議

neering)

- RaSIEM 2013 (The 2nd International Workshop on Recent Advances in Security Information and Event Management)
- RAMSS 2013 (The First International Workshop on Statistical Methods in Reliability Assessment of Complex Industr)
- ECTCM 2013 (The First International Workshop on Emerging Cyberthreats and Countermeasures)
- SecATM 2013 (International Workshop on Security in Air Traffic Management and other Critical Infrastructures)

また，今回の ARES は CD-ARES(Cross-Domain Conference and Workshop) と併催となっている．CD-ARES は，具体的には，計算機科学とその複数の適用分野の橋渡しを目的として，領域にまたがって情報システムに対する全体論的なテーマを扱う．2010 年に提案され，ARES の中では 2 度めの開催である．

図 3 レセプション会場

会議はドイツ南部バイエルン洲レーゲンスブルク市にあるレーゲンスブルク大で開催された．レーゲンスブルクは，現在は同大学を中心とした学生の割合が多い以外は閑静な住宅街である．しかし，同市は神聖ローマ帝国の首都となったこともあり，ユネスコの世界遺産にも登録されている．レセプションは歴史的建造物の並ぶ旧市街の旧市庁舎で行なわれた．また，2 日めには懇親会（ディナー）が同じく旧市街の Fu”rstliches Brauhaus(レストランの併設された醸造所) で開催され，民族衣裳の男女によるダンスなどが披露された．

3. 本会議

本会議の中で，注目した発表 (セッション) をいくつか紹介する．

3.1 共通問題の観点から

本会議およびワークショップの中で，評価のためのデータとして扱われていたものを以下に挙げる．

自作のものを用いているが，共通化に至っていないもの

小橋らの発表 [10] では，ホテルの予約システムをケーススタディとして用いている．これは，NII の TopSE プロジェクト「アスペクト指向講座」で用いられているものである [*1]．また，V. Ciancia らの発表 [2] では，航空券の購買サービスを，クラウドのセキュリティ要求策定に関する Beckers らの発表 [1] では，オンラインバンキングを用いている．これらの問題は，対象が限定されている上に特にセキュリティに特化して他で用いられているものではない．

Paulos らは，自律的環境におけるアプリケーションへの不正な入力を隔離する”Input Recuction”を提案している [13] が，安全性およびコストの評価にあたり，筆者ら自身が作成したファイル保存 Web サービスアプリケーションを用いている．アプリケーションは，入力値検査をしないなど，あえて脆弱性を残す形で構築されている．

公開されているデータを用いているもの

[*1] http://topse.jp/

Wright らは，ソフトウェアの脆弱性評価を特に SQL 障害報告をケーススタディとして行っている [16] が，これらのデータは実際には National Vulnerability Database (NVD) [*2] および Open Source Vulnerability Database (OSVDB) [*3] から採取されている．このように具体的な脆弱性に着目した場合は，公開されている脆弱性データベースを用いることができる．Li らの脆弱性評価に関する研究 [11] においても，NIST の SAMATE プロジェクトが提供するテストスイート Juliet Test Suite[*4] を用いている．Juliet Test Suite は Java および C，C++向けのテストスイートであり，約 100 種類の CWE ごとに 45309(C/C++向け．Java 向けは 14884) 個のテストケースが用意されている．

Fleck らは，ソフトウェア利用者の活動によって活性化されるマルウェアのふるまいを検出する PyTrigger を提案している [3]．PyTrigger の評価には 2 種類の対象が用いられる．前者はマルウェアそのものの検体であり，これらは MD:Pro プロジェクト l[*5]，Cyveillance 社 [*6] より提供されたもの，および Google malicious URL list[*7] より得ている．後者は利用者の活動のサンプルであるが，Fleck ら典型的な活動として以下の 7 つを選択している．

- e-mail(GMail, yahoo)
- SNS(Facebook)
- オンライン検索 (Google)
- オンラインバンキング (HSBC[*8])
- テキスト編集 (Windows エクスプローラ)
- ファイル参照 (Windows エクスプローラ)
- ファイル実行 (Windows エクスプローラ)

Jensen らは文献 [7] において ID 管理および usage control の産業界への適用への障害について述べているが，論文では実際にノルウェーの石油ガス業界をケーススタディとして論じている．しかし，具体的なソフトウェアの詳細ではなく，インタビューを行ない，その結果外部に提示可能な仕様に基づいた評価を行っており，ソフトウェアのより詳細な仕様までは対象としていない．

実際のソフトウェア（システム）を用いているもの

Ruiz らは，セキュリティモデリングのためのフレームワークとプロセス SecFutur を提案している [14] が，ケーススタディとして，実世界の検針（メータ）デバイスを用いている．Ruiz らの研究は，セキュリティ的な要求と法的な要求双方のモデル化を試みていて興味深いが，対象となっている検針デバイスについては，2 点の疑問点がある．1 点めは，実世界の検針デバイスと論文中に記述があるものの，その実世界との対応（構成や要求，法律はどの国のものか）が明示されれていない点である．2 点めは，対象が特殊なドメインへの適用であり，この対象への評価をもって，どのように帰納，一般化が可能かが明示されていない点である．

Meland らは，ゴール指向分析における脅威の扱いについて考察，提案を行っている [12]．Meland らはそのケーススタディの例として，航空交通管理 (Air Traffic Management: ATM) を用いている．ATM におけるセキュリティは近年ヨーロッパを中心に注目されており，ARES においても ATM のセキュリティに関連するワークショップ (International Workshop on Security in Air Traffic Management and other Critical Infrastructures: SecATM) が初開催されている．比較的研究の浅い分野であるため，用いられている ATM は評価の定まった問題というよりも，新規に脅威分析が必要な対象という性質が強い．したがって，ATM の問題を共通問題として採用するには，セキュリティに対する評価を確定されることが必要になると考えられる．

3.2 その他，注目の発表

ARES 本会議のセッション III Software Security では、ソフトウェアの開発時におけるセキュリティパターンを通じたセキュリティの作りこみや脆弱性・バグレポートの扱い、さらには、主として実行時における悪意のある外部入力やソフトウェア（マルウェア）の解析に関する研究発表があり、セキュリティの保証に向けて開発時と実行時さらには保守といったライフサイクル全体を通しての種々の取り組みの重要性があらためて感じられた。

具体的には、同セッションにおいて筆者らは”Validating Security Design Patterns Application Using Model Testing”と題し、ソフトウェアの設計においてセキュリティの非専門家が効率的かつ確実にセキュリティ対策を実施できるように支援する手法を提案した。具体的には、頻出する設計段階におけるセキュリティ上の問題と解決策をセキュリティ設計パターンとして準備したうえで、UML で表現された設計モデルのテスト実行により各パターンの問題の存在を自動検証し、問題が存在する場合は対応する解決策の適用を促し、人手による解決策の適用後に再度のテスト実行を通じて問題の解消ならびに当該セキュリティ設計パターンの解決策の正常な適用を検証する仕組みを実現している。このようなセキュリティパターンへの取り組みは、他にも併設ワークショップ SecSE においても一部紹介されており（Beckers らの発表”Structured Pattern-Based Security Requirements Elicitation for Clouds”）、過去の資産やノウハウを活用した実践的な取り組みとして今後の発展や広がりが期待される。

[*2] National Vulnerability Database, http://nvd.nist.gov/
[*3] Open Source Vulnerability Database, http://www.osvdb.org/
[*4] http://samate.nist.gov/SRD/testsuite.php
[*5] Malware Distribution Project https://www.frame4.net/mdpro/index.php
[*6] Cyveillance inc. https://www.cyveillance.com/
[*7] Google Developers Safe Browsing API https://developers.google.com/safebrowsing/?hl=ja&csw=1
[*8] HSBC http://www.hsbc.com/

また同セッションにおいてWrightらは”Estimating Software Vulnerabilities A Case Study Based on the Misclassification of Bugs in MySQL Server”と題して、バグレポートにおいてバグが脆弱性に関するものかどうかの分類がしばしば誤っている点に着目し、現実には報告済みのものよりも多数の脆弱性が存在する可能性を報告している。具体的には実証的ソフトウェア工学でよく見られるデータ分析を通じ、現実のOSS（MySQLサーバ）を対象として、報告済みのものの6倍から7倍強の脆弱性が、脆弱性ではないと誤って分類されている可能性があるという注目に値する知見を明らかとしている。このような開発履歴やバグレポートに対する実証的かつリポジトリマイニング（発掘）のアプローチは近年、（セキュリティに限らない）バグ一般の予測や開発効率、工数の観点で近年盛んであり、セキュリティについても有用であることを示している点が興味深い。リポジトリマイニングの領域では、発見されたバグに対して修正対応すべき開発者を推薦するといった開発者支援の研究に実績があり、セキュリティ上の知見と組み合わせた発展も期待される。

ARES本会議のセッションIVでは，Risk PlanningとThreat Modelingに関する興味深い三件の発表が行われた．まず，Mike Surridgeらによる Run-Time Risk Management in Adaptive ICT Systemでは，SERSCIS project [*9] の成果として，ICTシステムの実行時に自動的に脅威の検出をする手法の提案と評価が発表された．技術的には意味推論と，実行時のモニタ結果に基づく機械学習 (ベイズモデルを用いる) を組み合わせている．評価は空港における共同意志決定支援システムを題材として行われていた．本研究では脅威とその帰結を二段階にとらえ，一段階目を機械学習により実行時に識別し，二段階目を予めモデル化した意味情報に基づく識別するという戦略をとる．DoS攻撃による脅威を実行時に識別し，それによって可用性が低減する資源を意味推論で識別するのが典型例である．機械学習と意味推論のそれぞれの持ち味を活かし，有益な組み合わせを行っている点が優れている研究であるといえる．次に，Kristian Beckersらによる A Problem-Based Threat Analysis in Compliance with Common Criteriaでは，Problem Frames [6] のアイディアに基づきCommon Criteriaの文書 (Security Target, ST) を作成する手法を提案している．技術的にはProblem Framesを表現するためのUML profile (UML4PF) やOCLを用いている．STを記述するための対象IT製品や関連するドメイン知識を半形式的に記述しなければならない手間はあるが，その問題を無視すれば，STを記述するための有効な手法の一つと考えられる．我々もCCを用いたセキュリティ要求分析に関する研究を行っていることもあり [15]，特に興味深く発表を聞くことができた．最後に， Federica Paciらによる Detecting Insider Threats: a Trust-Aware Frameworkについて報告する．本発表では，i* [17] のセキュリティ拡張方言の一つであるSI*を用いて，組織内部における脅威を分析する手法を提案している．i*では情報システムおよびその関係者間のゴール達成，タスク遂行，資源 (アセット) 利用に関する依存関係がモデル化される．SI*では，それらに加えて，権限委譲や信頼の依存関係もモデル化される．本研究ではこれらの依存関係を追跡することで，脅威となるシステムの関係者，特に組織内部の者を識別する手法を提案している．発表者ら自身も述べていたが，この手法はSI*のモデルが漏れなく記述されいなければ機能しない．また，i*系のモデルはスケーラビリティに関して問題が多い．加えて，モデルの記述自体が容易でない．これらの問題を除ければ，提案手法は有益なものであると考えられる．また，我々も簡略化したi*のモデルを用いたセキュリティ分析の研究を進めているため [9]，特に興味深く発表を聞くことができた．

近年，プライバシーの問題は情報システムにおいて重要度を増している [18]．ARES本会議のセッションVでは，このプライバシーに関する発表が行われたが，その中で興味深いものを紹介する．会議会場となったレーゲンスブルク大学のC. Richthammerらによる Taxonomy for Social Network Data Types from the Viewpoint of Privacy and User Controlという発表では，近年重要性が増しているオンラインソーシャルネットワーク (OSN, 例えば，facebook, Google+, Twitter, LinkedIn 等) におけるデータをプライバシーの観点から分類することで，特にOSNシステムにおけるプライバシーを扱う手法等を比較検討する上での基盤を与えている．本研究は文献調査に基づき行われているため，単に著者らが提案する分類が有益であるというだけでなく，プライバシーの観点からデータ型を分類する先行研究の小規模サーベイにもなっており，今後，プライバシーに関する研究を進める研究者にとって有益な資料となっている．

4. ワークショップ

SecSEは今回で7回目となるセキュア・ソフトウェア工学に関するワークショップであり，一件の招待講演と，6件の一般講演が行われた．招待講演では，Gary McGrawが，BSIMM4: the Building Security in Maturity Modelという講演を行った．BSIMM4は名前が示すようにCMM等と同様のプロセス改善の考え方をセキュアなソフトウェア開発に適用したものである．BSIMM4のWebサイト [*10] から，著名な50社以上 (例えばAdobe, Microsoft, Siemens, Sony Mobile, Visa 等) の成熟度モデルをダウンロードする

[*9] http://www.serscis.eu/

[*10] http://bsimm.com/

ことが可能であり，これらと自社のデータを比較することによって，自社のセキュリティに関する改善の方向性を明確にすることができるとしている．このような多数の実証データ提供によって，企業における実践的なセキュリティ品質の改善につながると考えられる．一般講演の中で注目した発表を以下に紹介する．Per Hakon Meland らによる The Use And Usefulness of Threats in Goal-Oriented Modelling という講演では，ゴール指向要求分析におけるゴールと，セキュリティ要求分析における脅威の類似性に着目し，ゴール指向要求分析において脅威をどのように用いるべきかについての提案を行っている．この研究では i* [17] の方言に基づくツールである STS Tool を用いている．伝統的な脅威分析ではどのようにシステムが悪用されるかを示すために脆弱性を明確化する必要がある．ゴール指向要求分析段階では，脆弱性の想定無しで脅威をモデル化できるため，脆弱性を避けるための技術的な理由でゴールを変更するのではなく，もっと抜本的なレベルでの代替ゴールの発見に貢献すると結論付けている．ゴール指向要求分析の分野においては，ありふれた結論ではあるが，脅威をゴール指向要求分析において，どのように用いるべきかを体系的に議論した論文として興味深い．

FARES は今回で 8 回目となる 可用性，信頼性そしてセキュリティに関する新領域について議論するワークショップである．今回の FARES は 4 つのセッションが設けられ，10 件の興味深い発表が行われた．セッション毎の話題は順に組織に関するセキュリティ，ソフトウェアセキュリティとテスト，プライバシーとフォレンジクス，そしてネットワークとクラウドに関するセキュリティである．本ワークショップ中で特に目を引いた発表の概要を以下に紹介する．まず， Denisse Munante らの，An Approach Based on Model-Driven Engineering to Define Security Policies Using OrBAC という発表を紹介する．本発表ではモデル指向工学 (MDE) の考え方に基づき，セキュリティポリシィを段階的に詳細化する手法とツールの提案が紹介された．組織に基づくアクセスコントロールモデル (OrBAC) を用いてポリシィ記述を行い，モデル記述には，OrBAC 用に拡張した UMLsec [8] を用いている．UML であろうと UMLsec であろうと扱う範囲は仕様化以降であり，要求定義や妥当性確認が含まれているとは言えない．その意味からは，要求やゴール等の高次な概念とかかわりが深いポリシーを扱う場合，UML 系の記法に加え，ゴール指向等のより高次な記述との連携が不可欠と思われる．本研究でも，そのような観点に着目することで，より妥当なポリシー生成を可能とすると思われる．次に，総合研究大学院大学の宗藤誠治氏らの Model-Assisted Access Control Implementation for Code-Centric Ruby-on-Rails Web Application Development という発表を紹介する．Ruby on Rails だけでなく多くのアプリケーションフレームワークは典型的な脆弱性に対する対策を提供しているが，個々のアプリケーションにおいて設計および実装しなければならないセキュリティ機能もある．認証と権限付与はその典型例であり，この部分の設計・実装ミスが，セキュリティ上の問題を引き起こす場合がある．本発表では，このような問題意識に基づき，実装されたセキュリティ機能に脆弱性が無いことを網羅的に確認するための手法とツールを開発・評価した結果の報告を行った．技術的には，ソースコードから状態モデルを生成し，アクセスコントロールポリシーに正しく従っているかをチェックするアルゴリズムと手法を考案した．また，考案した手法を Ruby on Rails を対象として実現し，その評価を行った．この手法およびツールは，極めて実践的であり，現実のウエブアプリケーション開発にすぐにでも適用できる高い実用性がある．今後の運用および評価を通した手法とツールの洗練が期待できる．

5. キーノート，チュートリアル

本会議では二件の興味深いキーノート講演が行われた．最初のキーノートは，E. Ferrari 氏による Data Protection in Social Networks: Going Beyond Access Control である．オンラインソーシャルネットワーク (OSN) におけるデータやプライバシーの保護は，従来のアクセスコントロール技術だけではカバーできない問題を数多く抱えている．本キーノートでは，このような問題点を俯瞰しつつ，この問題に関する最新の研究成果の紹介があった．二番目のキーノートは，C. Gunter 氏による Six Research Challenges for the Security and Privacy of Health Information Technology である．今日の医療現場は医療情報システム (HIT) 無しでは機能しないのは明らかである．しかし，HIT において医療情報のセキュリティとプライバシーを担保するのは容易なことではない．本講演では，HIT において追求すべき研究課題を特に 6 種類に絞って提示し，それぞれについて研究動向を概説した．双方の講演ともに共通するのはプライバシーの問題であり，世界的な潮流としても，プライバシーに関する研究を促進すべきであるという潮流を垣間見ることができた．

本会議では 4 件のチュートリアルが行われた．特に興味深い内容であったものを紹介する．まず，地元，レーゲンスブルク大学の L. Fuchs による Tutorial on Secure Enterprise - wide Identity Management and Role Modeling を紹介する．多種多様な利用者が業務に関与する今日では，それぞれの利用者に対して適切なアクセス管理を行うことは難しい．本チュートリアルでは，Role-based Identity Management を用いて，この問題点を解決する手法についての講義が行われた．特に，Role Mining と Role Engineering という二つの相補的な技術の解説を通して，Identity 管理の難しさと重要性が説明された．Role Mining [4] は，実際の業務活動の分析を通して，どのような Role

が当該業務に必要かを分析するボトムアップな手法である．Role Engineering [5] は，ある業務の遂行にどのような Role が必要かをトップダウンに決定する手法である．これら双方を組み合わせによって，多種多様な利用者の Identity 管理に関する問題点の解決がなされることが講義された．多くの Role や Identity にかかわる研究では，Role や Identity をモデル化する枠組みや言語のみを提供しており，どのように Role や Identity を識別するかについては手薄な印象を受ける．本チュートリアルにおける Role Mining の考え方は，この点に関する一つの解法を提供していたという点で大変興味深い内容であった．次に， S. Katzenbeisser による Tutorial on Challenges in Data Protection - Privacy by Design を紹介する．このチュートリアルでは，巨大な分散システムで扱われるプライバシー保護を行うための，二つの技術的なアプローチについての講義が行われた．一つは細粒度のデータに関するアクセスコントロール技術であり，もう一つは Secure Multiparty Computation に基づく暗号化プロトコルである．これらの技術によって，OSN および OSN 間でのプライバシーに関する安全性改善法の一つを知ることができた．

6. CD-ARES

CD-ARES は，ビジネスと情報システムといった複数領域を横断する学際的な課題を扱う会議であり，2013 年は 21 件の発表があった．その中では，もともと異なるモデルや標準，枠組みを統合する取り組みが複数見受けられた．

例えば Beckers らは”Combining Goal-oriented and Problem-oriented Requirements Engineering Methods”と題して，要求工学における異なる要求分析手法であるゴール指向手法（具体的な対象としては SI*）と問題指向手法（具体的な対象としてはプロブレムフレーム）のシームレスな統合を通じて，要求の総合的なビューの提供といった効果を挙げようとする方法を提案している．SI*はステークホルダ間の関係の分析を得意とする要求分析手法 i*をセキュリティについて拡張したものであり，セキュリティ要求の総合的・多面的な捉え方や分析に向けて，提案のような複数の分析手法を組み合わせる方法は有用な可能性がある．

統合に関する他の発表としては，同じく Beckers らは”A Method for Re-using Existing ITIL Processes for Creating an ISO 27001 ISMS Process Applied to a High Availability Video Conferencing Cloud Scenario”と題して，情報システムの管理運用のガイドラインを与える ITIL と，組織における情報セキュリティマネジメントシステムに関する規格を与える ISO 27001 を併用するプロセスや方法を提案している．

また CD-ARES の会議全体の印象としては，採択率の厳しい ARES 本会議とは異なり，研究途上にあるアイディアや取り組みの報告が多いと感じられた．セキュリティは本来的に学際的な領域であり，このような学際的かつ萌芽的な会議の場から，今後のソフトウェアや情報システムのセキュリティの方向性を形づけるような革新的な成果が生まれる可能性に期待したい．

7. おわりに

セキュリティの共通問題の調査の目的で，セキュリティ国際会議 ARES を視察した．本会議やワークショップにおいてソフトウェア開発に関わる発表が多かったため，目的とする問題の収集は達成できたが，セキュリティのための汎用的な共通問題を用いた例はなく，標準的評価のためのソフトウェアデータセットの開発の必要性をあらためて認識することとなった．

筆者らは，SSR 産学戦略的研究フォーラム [*11] の本年度調査研究において，この解決となる共通問題案を提案する予定である．

謝辞 本会議への参加は，SSR 産学戦略的研究フォーラムの援助を受けて実現しました．ここに感謝の意を表します．

参考文献

[1] Beckers, K., Heisel, M., Cote, I., Goeke, L. and Guler, S.: Structured Pattern-Based Security Requirements Elicitation for Clouds, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 465–474 (2013).

[2] Ciancia, V., Martinelli, F., Matteucci, I., Petrocchi, M., Martin, J. and Pimentel, E.: Automated Synthesis and Ranking of Secure BPMN Orchestrators, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 455–464 (2013).

[3] Fleck, D., Tokhtabayev, A., Alarif, A., Stavrou, A. and Nykodym, T.: PyTrigger: A System to Trigger amp;amp; Extract User-Activated Malware Behavior, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 92–101 (2013).

[4] Fuchs, L. and Meier, S.: The Role Mining Process Model - Underlining the Need for a Comprehensive Research Perspective, *ARES*, pp. 35–42 (2011).

[5] Fuchs, L., Pernul, G. and Sandhu, R. S.: Roles in information security - A survey and classification of the research area, *Computers & Security*, Vol. 30, No. 8, pp. 748–769 (2011).

[6] Jackson, M.: *Problem Frames, Analyzing and structuring software development problems*, Addison-Wesley (2000).

[7] Jensen, J. and Nyre, A.: Federated Identity Management and Usage Control - Obstacles to Industry Adoption, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 31–41 (2013).

[8] Jürjens, J.: UMLsec: Extending UML for Secure Systems Development, *UML*, pp. 412–425 (2002).

[9] Kaiya, H., Okubo, T., Kanaya, N., Suzuki, Y., Ogata, S., Kaijiri, K. and Yoshioka, N.: Goal-Oriented Security Requirements Analysis for a System Used in Several Different Activities, *CAiSE Workshops*, pp. 478–489

[*11] http://www.iisf.or.jp/SSR/

(2013).
[10] Kobashi, T., Yoshioka, N., Okubo, T., Kaiya, H., Washizaki, H. and Fukazawa, Y.: Validating Security Design Patterns Application Using Model Testing, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 62–71 (2013).
[11] Li, H., Kim, T., Bat-Erdene, M. and Lee, H.: Software Vulnerability Detection Using Backward Trace Analysis and Symbolic Execution, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 446–454 (2013).
[12] Meland, P., Gjaere, E. and Paul, S.: The Use and Usefulness of Threats in Goal-Oriented Modelling, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 428–436 (2013).
[13] Paulos, A., Pal, P., Schantz, R., Benyo, B., Johnson, D., Hibler, M. and Eide, E.: Isolation of Malicious External Inputs in a Security Focused Adaptive Execution Environment, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 82–91 (2013).
[14] Ruiz, J., Arjona, M., Mana, A. and Carstens, N.: Secure Engineering and Modelling of a Metering Devices System, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 418–427 (2013).
[15] Saeki, M., Hayashi, S. and Kaiya, H.: Enhancing Goal-Oriented Security Requirements Analysis using Common Criteria-Based Knowledge, *International Journal of Software Engineering and Knowledge Engineering*, Vol. 23, No. 5, pp. 695–720 (2013).
[16] Wright, J., Larsen, J. and McQueen, M.: Estimating Software Vulnerabilities: A Case Study Based on the Misclassification of Bugs in MySQL Server, *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 72–81 (2013).
[17] Yu, E., Giorgini, P., Maiden, N. and Mylopoulos, J.: *Social Modeling for Requirements Engineering*, The MIT Press (2010).
[18] 吉岡信和，佐久間淳，竹之内隆夫：プライバシーを守った IT サービスの提供技術：0. 編集にあたって，情報処理，Vol. 54, No. 11, pp. 1104–1105 (2013).