科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月　 ５ 日現在

機関番号：１２６０１
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５０００７９

研究課題名（和文）認証・権限情報を制御可能なワークフロー特定ドメイン言語システムの研究

研究課題名（英文）A Domain Specific Language in which Authentication/Authorization control is Enabled

研究代表者
佐藤　周行（SATO, Hiroyuki）

東京大学・情報基盤センター・准教授

研究者番号：２０２２５９９９

交付決定額（研究期間全体）：（直接経費）　　3,900,000円、（間接経費）　　1,170,000円

研究成果の概要（和文）：ワークフローが構成されるドメインのトラストにつき、特にクラウドを対象としたトラストモデルを提案できた。さらにトラストのダイナミクスとして、低い保証性を持った情報を集めて高い保証性にelevateする機能の解析を行うことができた。さらにMapReduceを対象としてセキュリティドメインの制御を行うことができた。加えてサーバー間でのポリシー調停を行うWebサービスの枠組のプロトタイプ実装を完了した。副産物として、リスク評価において、対投資効果を勘案できる新公式を提案できた。全体として、ワークフローの各機能を実現するコンポーネントの設計と実装に集中することで高機能化につながる研究が果たせた。

研究成果の概要（英文）：We have proposed (1) a (cloud) trust model in which a workflow is deployed,(2)a trust elevation model in which low LoA informations are colledted to elevate to a higher LoA, and made some analysis on trust elevation, (3) a control system of MapReduce in which insecure programs are not allowed to execute, and (4) a policy consumption Web service architecture in which participants evaluate and negotiate the policies of the peers, and decide to subscribe services for oneselves. Those are all component functions of workflow. Having focused on the design and prototype implementation of those components, we have achieved the design and analysis of high functionality components in a workflow.

研究分野：複合領域

科研費の分科・細目：情報学，計算機システム・ネットワーク

キーワード：認証　ワークフロー　ポリシー調停　トラスト　セキュリティ　プライバシー

１．研究開始当初の背景

SOA（Service Oriented Architecture）において、小さいサービスをコンポーネントとして、より大きなサービスを構成するためのワークフローの表現は本質的である。SOA の中で提案されてきたワークフロー表現のための枠組としては BPEL があるが、そのほかにも XMLPipeline 言語などが提案されている。これらが必要となった背景としては、プログラム（プロセス）が、人間が実行するものでは必ずしもなく、プロセスがプロセスを起動し、プロセス間でデータをやりとりすることで新しいデータを構成することがあたりまえになったことがある。これらの言語ではワークフローがコンポーネントとなるサービスを結合させて作られ、プロセスの並行性や causality が自然な形で表現されている。

しかし、メタな意味ではワークフローはセキュリティやディスカバリーサービスとの連携を含むようになり、動的にプロセスのアクセス管理をしたり、自プロセスの相手を動的に発見することも求められるようになった。このときに、BPEL に代表される、プロセスのグラフとしてワークフローを理解することがあまり適切でなくなってきた。

さらに、Web Service の枠内で、サービス提供側がフェデレーションを組み、一定のセキュリティ条件を満たす Id に対して、連携してサービスを提供できるようになった。SAML や OpenID は、フェデレーションのためのセキュリティプロトコルであり、OAuth は、サービス間で Id の承認を前提にしたサービス連携のプロトコルである。これらでは、認証サーバや属性サーバをコンポーネントとしたサービスアーキテクチャが構築されている。

このように、サービスがメタな意味で巨大化、複雑化し、さらにサービス間の連携も当然のようになってきている今、その制御が必要とされている。そのためには、表現のための言語を元にして、解析を行なうのがその第一歩であった。

２．研究の目的

ワークフロープロセスを表現するプログラミング言語を定義、実装し、実行環境を構築する。実装には、各プロセス間でネゴシエーションを含むデータ交換を双方向に行うことを含む。

（言語の設計について）

１．ワークフローを表現でき、プロセスの並行性、causality を自然に表現できる（この意味で、既存の言語（BPEL,XMLPipeline など）の自然な拡張になる）

２．ワークフロー内でのデータ通信やアクセス制御における認証や権限付与・消滅を表現できる。ここにおいては、プロセスの動的な生成や権限の動的な証明ができる枠組を与える。ベースとしては model carrying document の概念を採用する。

（言語の実装について）

３．上で設計を行なったプログラミング言語の処理系（プロトタイプ）を実装する。Model carrying document は、SSL 中の CMS で実装する。加えて、従来のワークフローでおこなわれたことのなかった、ワークフローの（コンパイラ最適化の意味での）最適化・高速化を行なう。ワークフローでは、本質的に手続き間で重複した情報を使うことから、手続き間解析とそれに基づいたコンパイラ最適化が有効である。これも実証する。

（言語の実行環境について）

４．言語の実行環境として、リアリティの

あるシステムを用意する。特に、RBAC で権限を管理している環境に適合させるための属性管理のためのインタフェースを用意し、実際のセキュリティ制約の中で、正しく動作する（権限のあるデータにアクセスでき、権限があると証明されないデータにはアクセスしない）環境を構築する。

３．研究の方法

ワークフロー特定ドメイン言語の設計と実装を行う。特に必要となる機能の洗い出しと実装に注力する。また、ワークフローの部品プロセスをまたがったフローの最適化に取り組む。加えて、実世界で RBAC をベースに権限管理を行っている LDAP や SELINUX 等、ある程度の複雑さをもったシステムと Shibboleth など実際のポリシー記述を行っているシステムを統合して実験環境を構築し、その上にセキュリティ要件を記述するポリシーエンジンを構築する。

４．研究成果

全体として、ワークフロー用プログラミング言語の設計は既存のものを使うものの、各機能を実現するコンポーネントの設計と実装に集中することで、高機能化につながる研究が果たせた。特にセキュリティ・トラストに関係する分野で成果を上げることができた。

初年度は、目的とするドメイン言語の設計に先立ち、トラストモデルの拡張について研究し、カバーすべき範囲を見極めた。具体的には、クラウドのトラストモデルを、トラストの階層として理解し、その中でワークフローがどう制約されるかを研究した。さらに、オンライントラストにおける中心的な話題であるレベルの階層においてワークフローがどのように制約されるか、またトラストの階層があった場合に、ワークフローを超えて認証情報をどのように引き渡すことが合理的かについて成果（雑誌論文①③⑤等）を得た。

さらに、セキュリティのコストモデルがワークフローをどのように制約するかについて成果を得た。附属的な成果として、セキュリティのリスク分析において、ROSI を考慮した新公式を考案した（雑誌論文⑥）。また、実際に RBAC で制御を有効に利用している AIRAVAT において、権限情報をセキュリティエンハンスメントに反映できる形で実装した（学会発表①）。

２年目は、ワークフロー言語の設計のコンポーネントとして必要なセキュリティに関する研究を推進した。具体的に大規模分散ファイルシステム Hadoop のコードスキャンを用いたセキュリティ強化と、認可手続きに必要な属性情報の信頼レベル演算の一般的な形式（Trust Elevation）の研究、さらにそれらに付随したオンライントラストに関する一般的な研究である。

Hadoop のセキュリティ強化については、従来の会である Airvat 上で書ける MapReduce のコードのスキャンの能力を向上させ、Airvat と比較してより広い範囲のコードを受け入れ可能にした。これによって使用可能コンポーネントとして広い範囲の MapReduce/Hadoop が利用可能になった(雑誌論文⑩)。さらに認可手続きに必要なリリースされた属性の信頼性評価のための形式的な枠組を構築した。複数のソースから信頼性の低い属性を収集して、より高いレベルのトランザクションの認可に利用するときに信頼レベルを elevate させるための理論の枠組を構築した(雑誌論文⑭)。従来は、信頼レベルの高い属性の保守には大きなコストが必要とされてきたが、サービス提供側が属性を収集し、複数のソースから得られた場合の信頼レベルを一定の規則に従って elevate することで、属性の保守側のコストを合理的な範囲にとどめたまま、必要なだけ高い信頼レベルを計算することが可能になった。

最終年度は、ワークフロー言語機能の一部として、サーバ同士が相互にそのポリシーを交換して評価しあうポリシー評価パートの設計と実装を行った。他とともに実施した認証＋プライバシー保護機能と合わせることでワークフロー記述のためのコンポーネントの開発をおおむね終了することができた。

これらは Web サービスアーキテクチャの枠内で実装できるように XML をベースとしており、構成数の削減のために XSLT を利用して RESTful な形にすることができた。さらに従来自然言語で記述され、機械処理にはハードルの高かったポリシー文書の XML 化および DTTD の提案を PKI の CP/CPS およびプライバシーポリシーに対して試み、一部成功した。具体的に CP/CPS の XML 化では 285 要素、165 属性、Kantara の標準ラベル対応のプライバシーポリシーでは 25 要素、29 属性という規模になった。さらにこれらが動作するためのトラストモデルについて検討した。結果として、ワークフローが実効的に動くためのトラスト面からの解析が必要であることを明らかにした（学会発表⑨，雑誌論文 21）。

さらに、実際のアクセスフェデレーション内でのポリシーメーキングについて検討を

重ねた。「学生証を提示する」モデルのオンライン版の実装のためのポリシーメーキングと、ワークフローのためのコンポーネントの設計と実装ができた（雑誌論文⑱⑲）。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 22　件）

① SATO Hiroyuki, Kanai Atsushi, Tanimoto Shigeaki: Building a Security Aware Cloud by Extending Internal Control to Cloud, Proceedings of 10th IEEE International Symposium on Autonomous Decentralized Systems (ISADS 2011), 323--326, 2011. doi>10.1109/ISADS.2011.48

② Shigeaki Tanimoto, Manami Hiramoro, Motoi Iwashita, Hiroyuki Sato, Atsushi Kanai: Risk Management on the Security Problem in Cloud Computing, Proceedings of Conference on Computers, Networks, Systems and Industrial Engineering (CNSI 2011), 147--152, 2011. doi>10.1109/CNSI.2011.82

③ SATO Hiroyuki, KUBO Akira.: Graded Trust of Certificates and its Management with Extended Path Validation, Journal of Information Processing, vol. 19, 263--273, 2011. doi> 10.2197/ipsjjip.19.263

④ Shigeaki Tanimoto, Masahiko Yokoi, Hiroyuki Sato, Atsushi Kanai: Quantifying Cost Structure of Campus PKI, Proceedings of 11th IPSJ/IEEE International Symposium on Applications and the Internet (SAINT), MIDARCH 2011, 315--320, 2011. doi>10.1109/SAINT2011.60

⑤ SATO Hiroyuki, NISHIMURA Takeshi:Federated Authentication in a Hierarchy of IdPs by using Shibboleth, Proceedings of 11th ISPJ/IEEE International Symposium on Applications and the Internet (SAINT), MIDARCH 2011, 327--332, 2011. doi>10.1109/SAINT2011.62

⑥ SATO Hiroyuki: A New Formula of Information Security Risk Analysis that takes Risk Improvement Factor into Account, Proceedings of IEEE 3rd International Conference on Privacy, Security, Risk and Trust, 1243--1248, 2011. doi> 10.1109/PASSAT/SocialCom.2011.44

⑦ 藤巻文孝, 金井敦, 斉藤典明, 谷本茂明, 佐藤周行:情報資産価値を用いた最適保存先決定手法,情報処理学会 第 19 回 マルチメディア通信と分散処理ワークショップ (DPSWS2011), 200--207, 2011. http://id.nii.ac.jp/1001/00089881/

⑧ Tatsuya Miyagami, Atsushi Kanai, Noriaki Saito, Shigeaki Tanimoto, Hiroyuki Sato:Alternation methodology of schedule information on public cloud for preserving privacy,Proceedings of IARIA International Conference on Digital Society,132--139, 2012. http://www.thinkmind.org/index.php?view=article&articleid=icds_2012_6_20_10103

⑨ Shigeaki Tanimoto, Masahiko Yokoi, Hiroyuki Sato, Astushi Kanai: Quantifying Cost Structure of Campus PKI Based on Estimation and Actual Measurement, Journal of Information Processing 20(3), 640--648, 2012. doi> 10.2197/ipsjjip.20.640

⑩ Tran Quang, Hiroyuki Sato: A Solution for Privacy Protection in MapReduce, Proceedings of 36th IEEE International Computer Software and Applications Conference, 515--520, 2012. doi> 10.1109/COMPSAC.2012.70

⑪ Shigeaki TANIMOTO, Shinichi MIZUHARA, Msasahiko YOKOI, Hiroyuki SATO, Atsushi KANAI: Analysis of Security of PKI Operation with Multiple CP/CPS Based on Level of Assurance, Proceedings of IEEE Computer Software and Applications Conference Workshop (Middleware Architecture in the Internet), 100--105, 2012. doi>10.1109/COMPSACW2012.28

⑫ 横谷 百合, 宮上 達矢, 金井 敦, 谷本 茂明, 佐藤 周行: クラウドスケジュールサービスにおける日付偽装のための鍵共有方式の検討, Proceedings of DPS Workshop 2012 (30), 2012. http://id.nii.ac.jp/1001/00090375/

⑬ 宮上 達矢, 横谷 百合, 金井 敦, 斉藤 典明, 谷本 茂明, 佐藤 周行: クラウドスケジュールサービスにおけるプライバシー保護のための日付偽装方式の評価, Proc. DPS Workshop 2012 (31), 2012. http://id.nii.ac.jp/1001/00090376/

⑭ Sato, Hiroyuki: A Formal Model of LoA Elevation in Online Trust, Academy of Science and Engineering Science Journal 1(4), 166--178, 2012. http://ojs.scienceengineering.org/index.php/science/article/view/56/pdf

⑮ Shigeaki Tanimoto, Yorihiro Sakurada, Yoshiaki SEKI, Motoi Iwashita, Hiroyuki Sato, Atsushi Kanai, A Study of Data Management in Hybrid Cloud

Configuration, Computer Information Science, Vol. 492, 247--257, 2013. doi>10.1109/SNPD.2013.22

⑯ 谷本茂明，関良明，岩下基，佐藤周行，金井敦:ビッグデータを活用したサービスに関するリスクアセスメント，電子情報通信学会論文誌 A，Vol.J96-A，No. 4，189--194，2013. http://ci.nii.ac.jp/naid/110009596936

⑰ 西村 健，中村 素典，山地 一禎，佐藤周行，大谷 誠，岡部 寿男，曽根原 登:参加者ごとに異なるポリシーを反映可能な認証フェデレーション機構の実現，電子情報通信学会論文誌 D，Vol.J96-D，No. 6，1400--1412，2013. http://ci.nii.ac.jp/naid/110009611652

⑱ SATO, Hiroyuki, OKABE, Yasuo, NISHIMURA, Takeshi, YAMAJI, Kazutsuna, NAKAMURA, Motonori: Privacy Enhancing Proxies in Attribute Releases: Two Approaches, COMPSAC W(MidArch 2013), 379--384, 2013. doi>10.1109/COMPSACW.2013.65

⑲ Motonori Nakamura, Takeshi Nishimura, Kazutsuna Yamaji, Hiroyuki Sato, Yasuo Okabe: Privacy Preserved Attribute Aggregation to Avoid Correlation of User Activities Across Shibboleth SPs, COMPSAC W(MidArch 2013), 367--372, 2013. doi>10.1109/COMPSACW.2013.52

⑳ Yuuki KAJIURA, Atsushi KANAI, Hiroyuki SATO, Shigeaki TANIMOTO: A File-distribution Approach to Achieve High Availability and Confidentiality for Data Storage on Multi-cloud, COMPSAC W(SAPSE 2013), 212--217, 2013. doi>10.1109/COMPSACW.2013.125

21 SATO, Hiroyuki, TANIMOTO Shigeaki, KANAI Atsushi: A Policy Consumption Architecture that enablesDynamic and Fine Policy Management, to be published in Proceedings of 3rd ASE Int'l Conf. CyberSecurity 2014.

〔学会発表〕（計 12　件）

① Tran Quang，佐藤周行: MapReduce におけるプライバシーの手法の提案，2D1-5E，暗号と情報セキュリティシンポジウム (SCIS 2012)，金沢，2012/1/31.

② 榎本真也、金井　敦、谷本茂明、佐藤周行:ダイナミックに制御する情報漏洩対策システムの検討，第 11 回情報科学技術フォーラム（FIT2012）論文集，2012.

③ 末次 正人，榎本 真也，金井 敦，谷本茂明，佐藤 周行: 侵入者の距離によりダイナミックにセキュリティレベルを制御するシステムの検討，第 154 回 情報処理学会 DPS 研究会，4A-25，東京，2013/3/14.

④ 中村素典，西村健，山地一禎，佐藤周行，岡部寿男: 学割サービス実現のための SAML-OpenID ゲートウェイの試作，IPSJ IOT 研究会，2013-IOT-21(28)，1--7. 弘前，2013/5/9

⑤ Motonori NAKAMURA, Takeshi NISHIMURA, Kazu YAMAJI, Hiroyuki SATO, Yasuo OKABE, Takao YAMASAKI, Tsuyoshi MINAMI, Nat SAIKIMURA: PEOFIAMP: Privacy Enhancements for Open Federated identity/Access Management Platforms, Terena Networking Conference 2013 (Poster), Maastricht, 2013/6/2.

⑥ 岡部 寿男，佐藤 周行，西村 健，山地一禎，中村 素典: 属性提供サーバに対してサービス提供サーバを秘匿する匿名化プロキシ，マルチメディア，分散，協調とモバイル(DICOMO2013)シンポジウム，8F-2，帯広，2013/7/12

⑦ 中村 素典，西村 健，山地 一禎，佐藤周行，岡部 寿男，山崎 崇生，崎村 夏彦: 情報流通連携のためのオープンな ID 連携プラットフォームにおけるプライバシー保護機能の高度化，マルチメディア，分散，協調とモバイル(DICOMO2013)シンポジウム，8F-4，帯広，2013/7/12

⑧ 島岡正基，佐藤周行: 学認における属性交換フレームワーク，コンピュータセキュリティシンポジウム 2013，486--493，高松，2013/10/22

⑨ Sato, H., Tanimoto, S., Kanai, A.: Dynamic and Fine Grained Control of Policies by XMLed Policy management, 3C2-1，暗号と情報セキュリティシンポジウム (SCIS)，鹿児島， 2014/1/23

⑩ 五十嵐綾，金井敦，谷本茂明，佐藤周行: 秘密分散を用いたセキュリティ強度可変プロトコルの提案，3F1-1，暗号と情報セキュリティシンポジウム (SCIS)，鹿児島，2014/1/23

⑪ 岡部寿男，佐藤周行，山地一禎，中村素典: 属性情報と認可条件を相互に秘匿する認証連携プロキシ，電子情報通信学会第 88 回インターネットアーキテクチャ研究会 67--72，加賀市，2014/2/27

⑫ 横谷 百合，金井 敦，谷本 茂明，佐藤周行: ダイナミックなクラウド選択のための SLA の XML 化に関する提案，情報処理学会　第 158 回 DPS 研究会，東京，2014/3/7

〔図書〕（計０　件）

〔産業財産権〕
○出願状況（計０　件）
○取得状況（計０　件）

〔その他〕
ホームページ等

なし

６．研究組織

(1)研究代表者

佐藤　周行（SATO, Hiroyuki　　）
東京大学・情報基盤センター・准教授
研究者番号：20225999