SSR フォーラム平成２１年度調査研究提案書

連絡先
〒819-0395 福岡市西区元岡 744
九州大学大学院システム情報科学研究院・准教授・堀良彰
ＴＥＬ　092-802-3650
ＦＡＸ　092-802-3600
e-mail　hori@inf.kyushu-u.ac.jp

１．提案テーマ名
クラウドコンピューティング環境におけるセキュリティとプライバシに関する調査研究

２．研究調査の要旨
クラウドコンピューティングにおけるセキュリティとプライバシ確保のために、必要な所有権、アクセス制御ならびにそれらの評価に関し、ソフトウェア設計の観点から調査研究を行う。

３．キーワード：
クラウドコンピューティング、セキュリティ、プライバシ、オーナーシップ、アクセス制御

４．研究調査の目的

クラウドコンピューティングにおけるセキュリティとプライバシ確保のために、必要な所有権、アクセス制御ならびにそれらの評価に関し、ソフトウェア設計の観点から調査研究を行う。

クラウドコンピューティングに対する要求要件として、IBM 社らが協力している Open Cloud Manifesto [OCM09] では、今後取り組むべき課題として、セキュリティ、データとアプリケーションの相互接続性、データとアプリケーションのポータビリティ、ガバナンスと管理、計測と観測を挙げている。

従来のコンピューティング環境では、データへのアクセス制御は、コンピュータシステムに供えられたファイルシステムが有するアクセス制御機構により実施されていた。一方、クラウドコンピューティングにおいては、必要に応じて計算機資源の割り当てを行うため、データは元来のデータ所有者の手から離れ、サービス提供者のコンピューティング環境において蓄積され加工される。したがって、従来のコンピューティング環境と比較して利用者のデータやアプリケーションは、不正アクセス等の危険が増し、データのプライバシにおいても配慮が必要となる。

したがって、データの所有者を明確にし、所有者が想定するデータ取扱いポリシーを定義し、それにより当該データへのアクセス制御を行うための枠組みが必要となる。

データを中心とした適切な所有者情報管理とアクセス制御は、今後、情報通信ネットワーク基盤上に形成されるデータ指向コンピューティング環境において、適切にデータを管理するための枠組みを与える。これにより、プライバシに係るデータの管理を確実にし、データの内容に応じた適切な管理手法を実現し得る。

[OCM09] “Open Clould Manifesto,” http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf, March 30, 2009.

５．戦略的意義

クラウドコンピューティングにおける、重要情報保護を含むリスク管理をどのように行うかという問題は、2008 年 7 月に Communication of the ACM 誌中のクラウドコンピューティングの解説記事の中で簡単に触れられるなど、その重要性がようやく認識され始めた状況にある。クラウドコンピューティングや SaaS(Security as a Service)などの導入は、個々の計算機資源を意識することなく、「サービス」を情報システムを構成する柱と捉えることで、ハードウェア資源や従来のソフトウェア流通にかかるオーバヘッドを低減させようという効率化を目指すものである。従来のコンピューティング環境では、信頼性・安全性のよりどころとして主に物理的な方法によりデータを隔離し管理することで重要データの流出を防いできた。サーバ室の入退出管理、USB トークンを利用したファイルシステムの暗号化など結局行き着くところは物理的手法である。

ところが、クラウドコンピューティングや、SaaS などの枠組みでは一旦利用者の手からサービス提供者側に渡ったデータがどのように適切に管理するかという枠組みは十分に検討・構築されていない状況である。したがって、サービス指向コンピューティングの社会基盤として信頼できるものにするためには、これらの環境におけるデータ管理の枠組み構築が急務であるが、現在は研究コミュニティで問題提起が行われ始めた段階である。2008 年 11 月に報道された、Google Map を利用した個人情報流出事件も、プライバシに係るデータ管理が不十分であったことに起因している。

クラウドコンピューティングにおけるセキュリティならびにプライバシへの取り組みは、ようやく始まったばかりであり、2009 年 3 月に Open Cloud Manifesto が策定され、また、2009 年 4 月に Cloud Security Alliance (CSA) が組織され “Security Guidance for Critical Areas of Focus Cloud Computing” 文書が公開されるなど本年になって議論が開始されたばかりである。

そこで、本研究調査では、特に、クラウドコンピューティング環境におけるデータの所有者情報管理ならびにアクセスコントロールのための機構の研究開発に焦点を当て、最新の研究動向を調査するとともに、データ中心指向に基づいた新たなデータ管理手法を議論するとともに、それらの標準化動向について調査を行う。

［このテーマに関する内外の研究の動向］

2007 年 11 月に、サービス指向アーキテクチャ(SOA:Service Oriented Architecture)におけるデータプロベナンスシステムにおけるセキュリティ、プライバシ、信頼性の解析についての提案がなされている[TWCPCZ07]。

2008 年 1 月 14・15 日に米国プリンストン大学の Information Technology & Policy センターで、Computing in the Cloud に関するワークショップが開催された[W08]。そこでは、次の４つのパネルディスカッションが開催され集中して議論が行われた。そこでは、データの所有とオーナシップ、クラウドコンピューティング環境におけるセキュリティとリスク、クラウドにおける市民の知識共有、今後の展開について議論が行われた。

2008 年 7 月には、Communications of the ACM 誌に “Cloud Computing” と題する Brian Hayes 氏による解説記事[H08]が掲載され、その中の一部ではあるが、セキュリティ、プライバシおよび信頼性がクラウドコンピューティングにおいて緊急に取り組むべき問題であることが述べられている。

2008 年 9 月には、ACM の netWorker 誌に “Cloudy weather” と題する Lynn Greiner 氏による解説記事[G08]が掲載され、その中の一部ではあるが、クラウドコンピューティングにおいてもっとも優先して取り組むべき課題としてリスク管理があり、クラウドコンピューティングの客のプライバシを客がデータの所在をコントロールできない状況で、どのようにして保証するかが問題であることが述べられている。

上記のように、米国におけるクラウドコンピューティングにおけるセキュリティとプライバシについての関心が本年になって高まっている状況であるが、問題提起にとどまっており具体的なアーキテクチャ設計等には至っていない。

我が国においては、研究代表者が知る限り、情報処理学会コンピュータセキュリティ研究会、コンピュータセキュリティシンポジウム、暗号と情報セキュリティシンポジウム等、コンピュータセキュリティ関連分野の研究者が集まるコミュニティのいずれにおいてもまだ議論が開始されていない。

[TWCPCZ07] W. T. Tsai, Xiao Wei, Yinong Chen, Ray Paul, Jen-Yao Chung, Dawei Zhang,

[W08] Workshop on Computing in the Cloud, Center for IT and Policy, Princeton University, January 2008. (http://citp.princeton. edu/cloud-workshop/)

[H08] Brian Hayes, “Cloud Computing,” Communications of the ACM, Volume 51, Number 7, pp.9-11, July 2008

[G08] Lynn Greiner, “Cloudy weather,” netWorker, Volume 12, Number 3, pp. 11-13, ACM press, September 2008.

５．調査研究の進め方

研究目的を達成するために、クラウドコンピューティングにおける適切なデータ管理機構の実現に関して、ソフトウェア設計の観点から、次の副課題を設定し調査研究を進める。

［副課題１］クラウドコンピューティングにおけるデータとアプリケーションの所有権に関する調査研究

従来のコンピューティング環境と異なる要求に応じて計算機資源が割り当てられる環境において、データおよびアプリケーションの所有権について調査を行う。クラウドコンピューティングにおいては、割り当てる資源やサービスの粒度に応じて、SaaS (Software as a Service), PaaS (Platform as a Serveice), IaaS (Infrastructure as a Service) に分類できるが、それぞれについて調査研究を行う。

［副課題２］クラウドコンピューティングにおけるアクセス制御とポリシ適用に関する調査研究

従来のコンピューティング環境と異なる要求に応じて計算機資源が割り当てられる環境において、データおよびアプリケーションのアクセス制御とポリシ適用について調査を行う。クラウド

コンピューティングにおいては、割り当てる資源やサービスの粒度に応じて、SaaS (Software as a Service), PaaS (Platform as a Serveice), IaaS (Infrastructure as a Service) に分類できるが、それぞれについて調査研究を行う。

［副課題３］クラウドコンピューティングにおける所有権とアクセス制御機構に関する標準化に関する調査研究

副課題１ならびに副課題２で取り上げるクラウドコンピューティングにおける所有権とアクセス制御機構およびその周辺に関する標準化動向について調査を行う。

これらの３つの副課題は、互いに関連性を有するために、並行して調査研究を実施する。研究遂行のため、USENIX’09 および HotCloud '09 会議に参加し、最新の研究成果について調査を実施する。また、研究代表者の所属する九州大学では、大学組織として多数の電子ジャーナルを購読しているため、それらの文献調査も併せて実施する。

これらの調査研究により得られた成果は、情報処理学会コンピュータセキュリティ研究会が中心となって開催するコンピュータセキュリティシンポジウム 2009 および電子情報通信学会が中心となって開催する暗号と情報セキュリティシンポジウム等で発表を行い、研究成果を広く公開するとともに、当該分野における議論の喚起を行う。そのために、研究発表旅費および参加費を計上している。さらに、本調査研究課題について興味を持っていただける研究者に参加を求め、研究成果を共有し議論を深めるためのワークショップを企画する。ワークショップで得られた知見はウェブサーバ等を利用して広く一般に公開する。

［研究体制］

・学メンバ

九州大学大学院システム情報科学研究院・准教授・堀良彰（研究代表者）

1992 年九州工大・情報工・電子情報工学科卒。1994 年同大学院・情報工・情報システム専攻修士了。2002 年 3 月博士（情報工学）九州工業大学。1994 年 4 月九州芸工大芸術工学部助手。2004 年 3 月より現職。2005 年カリフォルニア大アーバイン校客員研究員。1997 年より日本学術振興会産学連携第 163 インターネット技術委員会運営委員。(財) 九州先端科学技術研究所特別研究員。電子情報通信学会情報通信システムセキュリティ研究専門委員会専門委員。ネットワークシステムセキュリティ、コンピュータシステムセキュリティに関する研究開発に従事。ネットワークシステムセキュリティ、コンピュータシステムセキュリティに関する研究開発に従事。

九州大学大学院システム情報科学研究院・教授・櫻井幸一

1986 年九州大・理・数学科卒。1988 年九州大・工・応用物理専攻修了。1993 年博士（工学）九州大学。1988 年三菱電機株式会社入社。情報電子研究所（現情報総合研究所）にて、暗号と情報セキュリティの研究開発に従事。1994 年 3 月九州大学工学部情報工学科助教授。現在、九州大大学院システム情報科学研究院情報学部門教授。ISO/IEC JTC1 SC27 委員。信学会情報通信システムセキュリティ研究専門委員会副委員長。(財) 九州先端科学技術研

究所情報セキュリティ研究室室長。情報セキュリティに関する研究開発に従事。特に、セキュリティプロトコルの安全性検証、コンピュータシステムセキュリティに関する研究開発に従事。

九州工業大学大学院情報工学研究院・准教授・光来健一

1997 年東大・理・情報科学卒。2002 年東大・理・情報科学専攻博士了。博士（理学）。2002 年日本電信電話（株）NTT 未来ねっと研究所。2003 年東工大大学院情報理工学研究科助手。2007 年デューク大学客員研究員。2008 年 10 月より、九州工大情報工学部准教授。情報処理学会システムソフトウェアとオペレーティング・システム研究運営委員会幹事。計算機ソフトウェアの観点から、分散システムにおける監視系の安全な構成法、仮想化技術ならびに侵入検知システムの研究開発に従事。SWoPP2004 若手プレゼンテーション賞（2004 年）、第１０回日本ソフトウェア科学会論文賞（2006 年）受賞。

［官メンバ］

財団法人九州先端科学技術研究所情報セキュリティ研究室・研究院・高橋健一

1999 年九州大・工情報工卒。2001 年九州大・システム情報科学研究科修士了。2004 年同博士了。博士（工学）九州大学。2004 年 4 月 九州大・システム情報科学研究院学術研究員。2004 年 11 月より（財）九州システム情報技術研究所情報セキュリティ研究室（当時第２研究室）研究員。組み込みソフトウェア向け SQL データベースセキュリティ。P2P 型コミュニティシステムのセキュリティの研究に従事。

財団法人九州先端科学技術研究所情報セキュリティ研究室・研究院・江藤文治

1988 年九州大・工・電気工学科（情報コース）卒業。1988 年富士通九州通信システム（株）入社（現、富士通九州ネットワークテクノロジーズ （株））。2009 年 2 月（財）九州先端科学技術研究所情報セキュリティ研究室研究員（出向）。これまで、ATM 交換機の UNI3.0/3.1, LANE, PNNI, MPLS 機能開発。ネットワーク管理システムにおけるシステム/品質測定アプリケーション開発。NGN の IP-MG 装置開発等を担当。

［会議運営計画］

学・官のメンバおよび産業界からの参画メンバが集中して議論を行う場として、２か月に１度をめどに連絡会議を開催する。開催地は、首都圏もしくは福岡を候補とする。会議においては、学・官メンバだけでなく、企業側メンバも技術発表を行い、それぞれの見地から調査研究の展開について議論を行う。

［成果の公表計画］

本研究の成果は、電子情報通信学会や情報処理学会におけるコンピュータシステムセキュリティに関係する研究会等において発表し、国内研究コミュニティにおける議論を喚起する。

［テーマに関する将来計画］

本研究成果の公表によって、多数の研究者の関心が得られた場合、翌年度も引き続き継続するための研究経費獲得を目指す。定期的なワークショップ開催等を通じて研究コミュニティを形成し、当該分野の研究をさらに推進する。特に、本課題で確立を目指すデータ管理手法を実システムにおいて実現するためには、ソフトウェアの研究開発を実施する企業等と連携し、実証的にその有用性を評価する研究開発を実施する。本研究は、それらの展開の基礎として調査研究と位置づけている。その後の、研究の展開にあたっては、自己資金では研究開発に必要な費用を賄うことができないため、科学研究費補助金や総務省情報通信研究開発推進制度等の外部資金制度を活用する。

［調査研究実施計画］

助成期間内予定線表	（平成２１年度）			
項目　年 月	第１四半期	第２四半期	第３四半期	第４四半期
［副課題１］クラウドコンピューティングにおけるデータとアプリケーションの所有権に関する調査研究	研究動向調査 ==========>			
		調査結果の整理・考察		成果発表
		==========>	==========>	
［副課題２］クラウドコンピューティングにおけるデータとアプリケーションのアクセス制御とポリシに関する調査研究	研究動向調査 ==========>			
		調査結果の整理・考察		成果発表
		==========>	==========>	
［副課題３］クラウドコンピューティングにおけるデータとアプリケーションの標準化に関する調査研究	研究動向調査 ==========>			
		調査結果の整理・考察		成果発表
		==========>	==========>	

[研究経費執行計画]

使途内訳

項　　目	算　出　根　拠	金 額（千円）				
研究調査旅費	USENIX’09 および HotCloud ’09 参加(米国カリフォルニア・サンディエゴ 7 泊 8 日)			4	5	0
研究打合せ旅費	福岡-東京 1 泊 2 日×10 人・回			7	0	0
会議参加登録費	USENIX’09 および HotCloud ’09 登録費				8	0
研究発表旅費	情報処理学会 CSEC 研究会 福岡-東京 1 泊 2 日				7	0
研究発表旅費	ｺﾝﾋﾟｭｰﾀｾｷｭﾘﾃｨｼﾝﾎﾟｼﾞｳﾑ 福岡-仙台 3 泊 4 日			1	1	0
研究発表登録費	情報処理学会 CSEC 研究会					4
研究発表登録費	ｺﾝﾋﾟｭｰﾀｾｷｭﾘﾃｨｼﾝﾎﾟｼﾞｳﾑ					5
会議開催費	会議室借料 25,200 円 ／ 8 時間				2	6
消耗品費	データ２次記憶装置×２台				4	0
消耗品費	ウェブ作成ソフトウェア 一式				1	5
合　　計			1	5	0	0