氏　　名	來間　啓伸	
学位（専攻分野）	博士（学術）	
学位記番号	総研大甲第950号	
学位授与の日付	平成１８年３月２４日	
学位授与の要件	複合科学研究科　情報学専攻 学位規則第６条第１項該当	
学位論文題目	ポリシに基づくサービス・コミュニティのための形式モデルの研究	
論文審査委員	主　査　教授	中島　震
	教授	武田　英明
	助教授	細部　博史
	教授	佐藤　健
	助教授	渡部　卓雄（東京工業大学）
	教授	本位田　真一（国立情報学研究所）

論文内容の要旨

World Wide Web を通じて提供・利用・仲介される Web サービスは、急速に変化する社会環境に適応できる柔軟な情報システムを構築するための、基本的な基盤と考えられている。例えば、旅行代理店システムでは、Web サービスとして提供されているホテル予約機能を呼び出して利用することで、ホテル予約をユーザに仲介することができる。このように構成されたシステムは、呼び出す Web サービスを変更することでホテルの追加や削除に対応できる、部屋の提供条件変更などに Web サービスを提供する側で対応できる、などの特徴を持つ。また、このシステムが旅行代理店機能を Web サービスとして提供することによって、他のシステムに構成要素として組み込まれることも可能である。しかしながら、システムが複雑になるにつれて全ての構成要素を把握することが困難になり、ホテル予約サービスが当初の設計意図とは異なる使われ方をされる場合も起こり得る。このようにして構成されるシステムは、異種かつ自律的な要素からなりシステムの構成が動的に変化するオープンなシステムであり、堅牢なシステムを開発するための技術は未だ研究途上にある。特に、システムの構成要素となる Web サービスやユーザ（以下ではまとめてプレイヤと呼ぶ）を他のプレイヤの不正なアクセスから守るアクセス制御は、不正利用や情報漏えいを防ぐために不可欠であるが、システムの柔軟性を損なうことのないアクセス制御ポリシをどのように設計し、それを実現する仕組みをどのように作るかは、課題のまま残されている。

従来から、多くのアクセス制御モデルが提案されているが、オペレーティング・システムなどにおける計算資源へのアクセス制御を起源とするため、中央集約的な管理機構を持たないオープンなシステムには適用できない。また、実社会の構造に適合するアクセス制御モデルとして広く知られ標準化されている Role Based Access Control モデル（RBAC モデル）でも、任意の時点で全てのプレイヤを一意に識別できることが前提となる。さらに RBAC モデルでは、RBAC によって制御されたシステムを別の RBAC によって制御されたシステムの一部として取り込む場合のアクセス制御を、プレイヤの一意性を保つためにシステム全体について RBAC を構成し直すことなしには取り扱うことができない。このように、オープンなシステムにおけるアクセス制御の問題は未解決であった。

本研究では、上記の問題を解決するために、オープンなシステムのためのアクセス制御モデルとして COAC（Community Oriented Access Control）モデルを提案する。COAC モデルでは、システムに関わるプレイヤの集まりをコミュニティと呼び、コミュニティに対してアクセス制御ポリシを設定する。より詳細には、コミュニティは、システムの中で担う役割（以下ではパートと呼ぶ）毎に集めたプレイヤの集まり（プレイヤの集まりの集まり）である。コミュニティのアクセス制御ポリシは、各々のパートに属するプレイヤ間のアクセス許可を定め、各パートのプレイヤに強制される。すなわち、COAC モデルでは、コミュニティのアクセス制御ポリシを、パートに基づいて規定する。また、COAC モデルでは、１つのシステムを別のシステムの要素として組み込むことを、各システムに対応するコミュニティのアクセス制御ポリシの間に対応関係を与えるポリシ（連合のポリシ）に基づくコミュニティの連合とみなす。連合のポリシは、異なるコミュニティのパート間に対応関係を与える。先述の例では、ユーザが属するパート、旅行代理店システムが属する

パート、ホテル予約サービスが属するパートから成るコミュニティを構成し、プレイヤ間で許可するアクセスをパートの関係として表現する。その結果、コミュニティのアクセス制御ポリシは不変のまま、ホテル予約サービスを追加あるいは削除することができる。また、旅行代理店機能をWebサービスとして提供して他のシステムに組み込む場合、例えば旅行代理店サービスを利用するシステムが属するコミュニティのパートとユーザのパートを連合のポリシで対応付け、後者を前者に拡張したアクセス制御ポリシを設定することで、各システムを利用するプレイヤのレベルで再構築をすることなくアクセス制御ポリシを拡張することが可能になる。

また、本研究ではCOACモデルのコミュニティを実現する論理的なシステム・アーキテクチャを示し、その中のアクセス制御機構を設計するためのCOACフレームワークを提案した。システム・アーキテクチャは、各パートに属するプレイヤのメッセージ送受信を制御するアクセス・コントローラと、連合するコミュニティ間のメッセージ送受信を制御するバウンダリ・コントローラから構成される。COACフレームワークは、コミュニティのアクセス制御ポリシにしたがうプレイヤ間のメッセージ送受信を、メタ階層構造を持つモデル記述言語を使って多階層で表現するためのフレームワークであり、コミュニティの連合とアクセス制御ポリシの実現のための基本構造を与える。COACフレームワークのメタ階層の中で、上位階層は下位階層のメッセージ送受信を監視し、コミュニティのアクセス制御ポリシに違反するメッセージ送受信を拒否する機能を担う。したがって、COACフレームワークの下位階層にはパートに属するプレイヤが行うメッセージ送受信を記述し、上位階層には論理的なアクセス制御機構を記述して、下位のメッセージ送受信がコミュニティのアクセス制御ポリシにしたがうことを示すことで、そのアクセス制御機構はコミュニティのアクセス制御ポリシを実現することが検証できる。なお、上位階層の機能は、システム・アーキテクチャにおいてアクセス・コントローラおよびバウンダリ・コントローラの機能に対応する。

COACモデルは、アクセス制御ポリシと連合のポリシをパート間の関係に基づいて形式化したモデルであり、連合によってできたコミュニティのアクセス制御ポリシが各コミュニティのアクセス制御ポリシと整合することを検証するための基盤を与える。COACモデルでは、個々のプレイヤはアクセス制御ポリシには現れない。したがって、各々のプレイヤを一意に識別する必要はなく、オープンなシステムに適合するアクセス制御ポリシの構築が可能となった。ホテル仲介システムと航空券仲介システムを結合するケーススタディを通じて、COACモデルの妥当性と、単純なコミュニティから複雑なコミュニティを構成する連合の有効性を確認した。また、コミュニティのアクセス制御機構がCOACフレームワークを使って記述され、かつ、連合による結合が柔軟に行われ得ることを確認した。COACモデルではパートを通じてプレイヤのアクセスを制御するため、RBACモデルのように個々のプレイヤを対象とするアクセス制御は行えないが、ケーススタディの範囲では支障はなかった。現在の段階では、COACモデルによるコミュニティの連合はパートの間に1対1ないし1対nの対応関係を設定できるときにのみ可能である。しかし、現実のシステムで詳細なアクセス制御を行う場合にはパート間に明確な対応関係がないことがあり、その場合にも適用できるようCOACモデルを拡張することは今後の課題である。

論文の審査結果の要旨

急速に変化する社会環境に適応できる柔軟なシステムとして、サービス指向アーキテクチャ（ＳＯＡ, Service-Oriented Architecture）の考え方が産業界で提案されている。具体的な技術基盤としては、ＷＷＷに基づくＷｅｂサービスを用いるものである。ＳＯＡでは非集中的な構成方法を採用することで、構成要素の変化ならびに組み合わせ方を柔軟に行うことが可能である。逆に集中的な管理機構を持つことができないため、堅牢なシステムの基盤となるアクセス制御を行うことが難しい。すなわち、システムの柔軟性を損なうことなくアクセス制御を行う方法はＳＯＡの分野で未解決であった。

来間君の論文は、オープンなシステムを対象とするアクセス制御のモデルとしてＣＯＡＣ(Community Oriented Access Control)を考案し、さらに、ＣＯＡＣモデルに基づくコミュニティを実現するシステム・アーキテクチャを提案するものである。システムに関わる構成要素の集まりをコミュニティとみなし、コミュニティに対してアクセス制御ポリシを与える。コミュニティへの出入りによって構成要素の柔軟な変化を可能とし、また、複数コミュニティにまたがる連合のポリシというアイデアを導入することで柔軟な組み合わせを実現する。実現アーキテクチャではメタ階層構造を利用することで、複雑化するアクセス制御機構を見通しよく実現できることを示した。さらに、ＣＯＡＣモデルを厳密に形式化することで、コミュニティ連合を安全に行うための条件をあきらかにした。

論文は、本文全８章と付録からなる。第１章で研究の動機について触れ、第２章で現状のアクセス制御モデルをオープンなシステムに適用する際の問題点を明らかにする。また、必要とされる要件を整理する。第３章で、本研究の中心的なアイデアであるＣＯＡＣモデルを提案する。ＣＯＡＣモデルならびに連合の考え方を厳密に定式化しシステムを安全に組み合わせる連合の条件を示す。さらに、ＫＱＭＬ (Knowledge Query Manipulation Language)で規定しているサービス仲介の基本パターンの記述実験を行うことで、提案する連合ポリシの表現力を確認する。第４章でメタ階層構造の概念を明示的に持つモデル記述言語を導入する。第５章でＣＯＡＣモデルを実現する論理的なシステム・アーキテクチャを示す。次いで、アクセス制御機構のフレームワークを第４章のモデル記述言語で表現することで、当該フレームワークがＣＯＡＣモデルを実現していることを示す。第６章では、２つの事例を通して、提案ＣＯＡＣモデルの有用性を確認する。第７章では、ＣＯＡＣモデルが第２章で挙げた要件を満たすことを議論する。また、現在、集中型のアクセス制御機構の標準として産業界で利用されているＲＢＡＣ (Role-Based Access Control) およびＷｅｂサービスでのアクセス制御を中心とする関連研究と比較することで、提案方式の新規性を評価する。第８章で、実用化に際しての留意点を含めて今後の展望を示す。付録では、本文で説明した概念・事例などに関わる具体的な記述を示す。

審査委員会は、本研究が、ＳＯＡに代表されるオープンなシステムのアクセス制御方法の発展に関して、重要な学術的かつ技術的な提案を与え、産業界への貢献も十分に期待できると判断し、新規性・有用性・信頼性の観点から、博士論文として十分な内容であると認めた。