OUKA
The University of Osaka
Institutional Knowledge Archive

Title	アクセス制御ポリシーの生成技術及び整合性検証技術に関する研究
Author(s)	鴨田, 浩明
Citation	大阪大学, 2009, 博士論文
Version Type	VoR
URL	https://hdl.handle.net/11094/2674
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

【28】

氏名	鴨田浩明（かもだひろあき）
博士の専攻分野の名称	博士（工学）
学位記番号	第 23370 号
学位授与年月日	平成21年9月25日
学位授与の要件	学位規則第4条第1項該当 工学研究科電気電子情報工学専攻
学位論文名	アクセス制御ポリシーの生成技術及び整合性検証技術に関する研究
論文審査委員	(主査) 教授 馬場口 登 (副査) 教授 滝根 哲哉　教授 北山 研一　教授 小牧 省三 教授 三瓶 政一　教授 井上 恭　教授 河崎善一郎 教授 鷲尾 隆　教授 溝口理一郎

論文内容の要旨

本論文は，筆者が大阪大学大学院工学研究科電気電子情報工学専攻在学中，及び(株)NTT データ技術開発本部在籍中に研究開発を行ったアクセス制御ポリシーの生成技術及び整合性検証技術に関する研究成果をまとめたものであり，以下の6章より構成される．

第1章は序論であり，本論文の背景となる技術分野に関して現状を述べ，本研究の目的を明らかにした．

第2章では，最初に本論文で対象とするアクセス制御ポリシーの定義について述べた．その後，アクセス制御ポリシーを用いたシステム制御を実現するために必要となる3つの大きな技術要素である，アクセス制御ポリシー記述技術，アクセス制御ポリシー検証技術，アクセス制御ポリシー生成技術についてそれぞれ述べ，技術的な課題を明らかにすることにより，本論文で議論するアクセス制御ポリシーの生成技術及び整合性検証技術の位置づけを明確にした．

第3章では，アクセス制御ポリシーに含まれる矛盾や冗長性を検出する技術について論じた．アクセス制御を必要とするシステムにおいて，ポリシーの設定間違いは，セキュリティ上の重大な脆弱性やシステムの性能低下に結びつくことから，アクセス制御ポリシーの整合性をシステム稼動前に検証することで安全性を証明することが求められる．そこで，アクセス制御ポリシーの整合性をタブロー法を拡張した自由変数タブロー法を用いて検証するアクセス制御ポリシー整合性検証技術について述べた．そして，シミュレーションにより，アクセス制御ポリシー整合性検証技術の実用面での有効性を検証した．

第4章では，アクセス制御ポリシーの内容をシステムの設定情報に反映するアクセス制御ポリシー生成技術について論じた．アクセス制御をシステム上で実現するためには，様々なシステムを整合的かつ安全に制御することが必要であり，それを手動で正確に行うことは容易ではない．そこで，オンデマンドVPN システムを事例にして，任意の二地点間で信頼性の高いセキュアな暗号化通信を実現するために必要となるシステムの構成情報を，アクセス制御ポリシーから自動的に生成する，アクセス制御ポリシー生成技術に関して述べた．そして，アクセス制御ポリシー生成技術を実装したプロタイプを用いて実証実験を行い，そこから得られた結果について考察した．

第5章では，設定されたアクセス制御ポリシーとシステム要件との整合性を検証する技術について論じた．第3章及び第4章で述べる技術により，整合性が検証されたアクセス制御ポリシー通りに，システムが動作するこ

とを保証することが可能となった．しかしながら，その動作が必ずしも本来のシステム要件に合致していることは保証されていない．そこで，ドキュメント管理システムを事例に，システム要件とアクセス制御ポリシーの間に矛盾がないことを検証する，システム要件とアクセス制御ポリシーの整合性検証技術について論じた．そして，検証技術を用いることにより，実際にシステム要件を満足しているかどうかを確認できることを検証した．

第６章は結論であり，本研究で得られた成果を総括した．

論文審査の結果の要旨

今日の情報通信システムにおいて、情報セキュリティの重要性は急速に増大しつつある。情報セキュリティには、ネットワークセキュリティ、データセキュリティ、システムセキュリティなど様々な観点が存在し、いずれも多くの克服すべき研究課題を有している。その中でシステムセキュリティについては、個人情報、医療情報、クレジット情報など機密性の高い情報が情報システムから一たび漏洩すると、ネットワーク社会においては個人的のみならず社会的な損害は甚大で、その対応手段の確立が喫緊の課題といえる。この課題の本質は、本来アクセスを許すべきでないリソースに対するアクセス制御の不備に還元されるため、情報システムの動作、挙動を記述したシステム要件たるアクセス制御ポリシーを如何に適正に構成するかが要点となる。

本論文は、個人情報など機密性の高い情報の漏洩を防ぐことを目的に、情報システムに設定されるアクセス制御ポリシーの生成および整合性検証に関する方式についての考察をまとめたものである。主たる研究成果を要約すると以下の通りとなる。

（１）アクセス制御ポリシーの集合に含まれる矛盾や冗長性を検出する整合性検証手法を具体化している。本手法は、一階述語計算という形式論理に基づく手法であるため、ポリシーにおける整合性を検証しうる健全な手法である。形式論理に基づく手法は、一般に計算コストが高いが、本手法では、自由変数タブロー法を導入し、1000 個のポリシー集合に対し、100 秒程度で整合性を検証し得ることを実験的に示し、手法の実用性を確認している。

（２）人間が記述したアクセス制御ポリシーを、情報システムが処理可能なマシンリーダブルな形式に自動変換する技術、すなわちアクセス制御ポリシー生成技術を新たに提案し、医療機関で利用されるオンデマンド VPN システムを事例として、提案技術の有効性を検証している。医療情報という極めて機密性の高い情報に対し、任意の二地点間で信頼性の高いセキュアな暗号化通信を実現するために必要となるシステムの構成情報をアクセス制御ポリシーから自動的に生成し得ることを実証している。

（３）設定済みのアクセス制御ポリシーに従い情報システムが要件通りに正しく動作するか否かを検証する技術について議論している。特に、機密性と可用性に着目し、アクセス制御ポリシーをモデル検査ツール SPIN が適用可能な記述に変換することにより、システム要件とポリシーとの不整合を実用的な検査時間で検出する手法を実現している。

以上のように本論文は情報システムのアクセス制御ポリシーの生成と整合性検証に関する数多くの有用な知見を与えており、情報通信工学、特に情報セキュリティ工学の発展に寄与するところが大きい。よって本論文は博士論文として価値あるものと認める。