【120】

氏名	河野和宏（こうのかずひろ）
博士の専攻分野の名称	博士（工学）
学位記番号	第　２３８３８　号
学位授与年月日	平成22年３月23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	A Study on Policy Integration and Anonymous Communication for Protecting Personal Information （個人情報保護のためのポリシー統合と匿名通信に関する研究）
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に行った個人情報を保護するためのポリシー統合と匿名通信に関する研究成果をまとめたものであり，以下の６章より構成した．

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，本論文で扱う２つの個人情報保護技術，ポリシー統合技術と匿名通信方式3-Mode Netの概要について述べた．また，ポリシー統合技術および3-Mode Netを含む匿名通信方式における既存研究の問題点を示すことにより，本論文で取り組む課題を示し，本論文の位置づけを明確化した．

第３章では，アクセス制御システムを一括して扱うことが可能なポリシー統合システムについて述べた．ポリシー統合技術はアクセス権の継承関係を用いて各システムに適切なポリシーを作成する技術であり，ポリシーを生成するために各システムの継承関係を統合する必要がある．そこで本論文では，継承関係の統合に焦点を絞り，サブジェクト，リソース，アクションという３つのカテゴリにおいて継承関係を用意し，これらの継承関係を統合する手法を提案した．また，本手法は実際にシステムを構築することを考慮し，継承関係を統合するためのアルゴリズムを全て行列演算に帰着している．ポリシー統合技術の開発により，各システムに対する管理者の手間・時間を大幅に減少させることが可能となった．また，ヒューマンエラーや設定ミスを未然に防ぐため，システムの適切な運用が可能となった．

第４章，および第５章では，匿名通信方式3-Mode Netの性能を解析した．まず第４章では，3-Mode Netを用いた通信で必要となる中継ノード数と暗号化処理回数について評価した．具体的には，それぞれの確率分布，期待値，分散を求めた．これらの導出にはランダムウォーク理論を用いた．導出された結果から，3-Mode Netにおける中継ノードのモードの選択確率と初期多重度が3-Mode Netの動作特性に与える影響を考察した．

第５章では，メッセージの送信者を特定するために互いに結託する不正ノードに対し，送信者の匿名性について評価した．この送信者の匿名性を，3-Mode Netを用いて通信を行う際に，最初に不正ノードに送信したノードがメッセージの送信者である確率によって定義した．この確率は，確率母関数を使って導出した．得られた結果から，中継ノードにおけるモードの選択確率と初期多重度が送信者の匿名性に与える影響を考察した．第4章およ

び第5章で得られた結果を用い，要求される動作特性から3-Mode Netの設定パラメータの値があらかじめ算出可能となった．

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、システムセキュリティ、ネットワークセキュリティなど様々な観点が存在し、とりわけ個人情報の保護については多くの克服すべき研究課題を有している。システムセキュリティにおいては、複数の情報システムのアクセス権を管理する際に生じうる、管理者の設定ミスによる個人情報漏洩を防ぐことが喫緊の課題の一つとされており、その解決手段として複数の情報システムのアクセス権を一括して管理できる統合化されたアクセス制御ポリシーを自動的に生成する手法が望まれている。一方、ネットワークセキュリティにおいては、通信の送受信者を知ることにより、送受信者の交友関係、趣味、嗜好などプライバシーに関わる情報が推測されるという懸念から、送受信者双方を秘匿する匿名通信が注目を集めている。近年、従来の匿名通信方式であるオニオンルーティングとクラウズの利点を相互補完的に併せ持った 3-Mode Net と呼ばれる匿名通信方式が提案されたが、3-Mode Net の挙動を決定づけるモード選択確率の決定法に関する明確な指針が明らかになっていない。

本論文は、個人情報の保護を目的に、情報システムに設定されるアクセス制御ポリシーの統合法および匿名通信方式 3-Mode Net 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）複数の情報システムを一括して扱うことが可能な統合化アクセス制御ポリシーの作成手法を具体化している。本手法は各システムにおけるアクセス権の継承関係に着目し、それらを統合した継承関係に基づいてアクセス制御ポリシーを統合する。本手法は、サブジェクト・リソース・アクションの３カテゴリーにおけるすべての継承関係を考慮していること、任意の数のシステムや継承関係を扱いうること、統合アルゴリズムが行列演算に帰着されるため実装が容易であること、という従来手法にない特徴を有している。

（２）匿名通信方式 3-Mode Net の挙動に関する詳細な理論的解析を行っている。具体的には、通信に要する中継ノード数や暗号化処理回数の確率分布、平均、分散、および通信者の匿名性に関する指標を、ランダムウォークの理論や確率母関数の性質を利用することによって解析的に導いている。

（３）これらの解析結果は、3-Mode Net に対する要求仕様を満足するため、中継ノードにおけるモード選択確率および初期暗号化多重度の決定に明確な規範を与えるものである。

以上のように本論文は個人情報の保護を目的とするアクセス制御ポリシーの統合法ならびに匿名通信方式 3-Mode Net 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。