早稲田大学大学院国際情報通信研究科

博 士 論 文 概 要

論 文 題 目

匿名通信サービスの研究

Studies on Anonymous Telecommunication Services

申 請 者

岡本	学
Manabu	OKAMOTO

国際情報通信学専攻
情報通信ネットワーク研究Ⅱ

2009 年 11 月

電子商取引などの決済サービス，電子カルテなどの医療サービス，電子投票などの行政サービス等々，社会上のあらゆる分野のあらゆるサービスが電子化される中で，機密やプライバシーを守りつつ信頼性を維持するセキュリティ技術が特に重要になってきている．

これらセキュリティ技術の中で重要なものの一つに匿名性技術がある．例えば電子カルテのような他人には見せたくない情報の取扱いについては，内容と個人とが直接につながらないような管理の仕方が重要である．更に電子投票などは，投票内容と投票者が結び付けば選挙妨害や買収などにつながる重要な問題となり，匿名性を完全にした上でなければ成り立たないサービスである．このように様々な用途に向けた匿名性技術の実現が必要不可欠である．

本論文は，セキュリティ技術における匿名性技術についての新しい手法の確立を目的としている．特に，ネットワークを利用した各種サービスへの匿名性の適用を目的としており，匿名化が可能なネットワークそのものの議論から，更にはネットワークを利用した様々な情報通信の基本形態，すなわち情報の収集・配布・交換についての匿名性を検討している．これら基本形態の中で既存技術では解決できていない情報の配布及び交換について課題点を洗い出した上で新しい方式を提案している．また，これら匿名技術の集大成となるネットワークを利用したサービスの一つとして匿名電子投票方式の提案を行っている．

第1章は序論であり，研究の背景，目的及び論文の概要について述べている．

第2章では，本論文において前提となるセキュリティ技術の現状を初めとして匿名性技術の従来検討について述べている．

第3章では，匿名通信路の構築方法について新たな提案をしている．だれがだれに通信を行っているかを不明にする匿名通信路についてはこれまでもいくつかの提案方法があったが，ここではスパイネットワークと呼ばれる特殊なP2P通信での利用を提案している．スパイネットワークは，参加ノード数を不明にする点や送信者・受信者の両者を不明にする点などにおいてこれまでの匿名ネットワーク以上に厳しい条件が必要なネットワークである．ここでは環状に構成した新たな匿名通信路の構築を提案している．この方法では環状匿名通信路上を常にメッセージセットと呼ばれる通信情報が各ノードで更新されて周回することで匿名性を実現する方式である．

匿名通信路では本来は通信路自体を不明にする技術であるから一度目の通信と二度目の通信が同じ経路を通過したかどうかの判断も不可能であった．しか

しこの経路の同一性については逆に安全管理上確認する必要が出てくる場合があると想定される．更に本章では匿名通信路の匿名性は維持したまま経路の同一性の確認のみが可能な方法についても提案している．

第4章では，情報通信の基本形態のうち「配布」について，秘密情報の匿名配布方式を提案している．ポーカゲームなどに代表されるような，秘密情報をどの情報がだれに渡ったかをだれも知ることがなく配布を行うことは，セキュリティ上での重要な課題となる．これまで秘密情報を収集する際の匿名性の技術は様々な提案がされているが，これらの技術は，集計される際にどの情報がだれから提出されたかという送信者の匿名性を守る技術であった．しかし一方で逆に送信者は特定機関であり,受取者が複数いるような配布のケースにおいて,どの情報をだれが受け取ったかという受取者の匿名性技術については検討がなかった．この技術は例えばトランプのようなカードゲームはもちろんのこと，大規模なネットワーク上での信頼できる「くじ」の実施，暗号鍵配布や電子投票など様々な応用が期待できる．本章では，第三者機関による配布方法であり，受取者は配布作業そのものにかかわることなく簡易に配布を受けることができる一方で，危険性を分割するため，配布を行う第三者機関を任意数に分割でき，全機関が結託不正しない限り，受取者以外は配布物の内容を見ることができない秘密性の実現，どの情報がだれのところに到達したのかをだれも知ることができない非追跡性の実現，第三者の目から見ても正当な秘密情報配布が実施されたことが確認できる信頼性の実現，これらすべてが維持できる配布の方法を提案している．

第5章では，情報通信の基本形態のうち「交換」について，秘密情報の匿名情報交換を取扱い，ギフト交換プロトコルを提案している．近年，ネットワーク環境の普及やモバイル端末の普及などでP2Pネットワークが注目されており，特にP2Pにおけるファイル交換アプリケーションが注目を集めている．これらP2Pのファイル交換においてはその使用方法によっては匿名性が非常に重要となる．これまでの秘密情報交換では主に一対一送受信向けの技術であり，その上での送信者の匿名性を守るものが中心であった．しかしここで提案しているギフト交換は複数人を含むグループ間同士の情報の受渡しであり，送信者及び受取者の両者とも匿名ながら秘密情報をやりとりする新しい情報交換の方法である．ここでは第三者交換機関を利用した交換方式を提案し，交換される情報が第三者には盗み見ることのできない秘密性，だれの情報がだれのところに届いたの

かがだれにもわからない匿名性，及び確かに全交換機関を経て正しくギフト交換が行われ提出者及び受取者が正当なギフトの授受ができたことを確認できる信頼性を実現している．

第6章では，匿名技術の集大成としてネットワークを利用した無記名電子投票の方法について検討している．投票の電子化は従来の投票方式に比べ投票用紙の不要などによるコストの削減や，開票集計時間の短縮化など，様々な社会的・経済的効果が期待できる．しかし一方でネットワーク上での電子投票では，本人確認の実施が難しく，そのために二重投票や票の水増し・改ざん等が憂慮され，更に集計局が悪意をもてば，集計中にその結果をもらして利用する不正なども存在しうるため，安全性が憂慮される課題がある．本章では，前述の匿名配布技術を応用することで，投票候補に対応したカードを匿名に配布し，投票者は単に自分が投票したい候補に対応したカードを提出することで投票作業が完了し，得票計算も簡易に第三者が確認可能な方式を提案している．この方法では二重投票や不正投票，票の改ざんなどの不正行為を簡単にチェックすることができる一方で，だれがだれに投票したかが不明である匿名性の実現や投票及び集計作業の正当性が第三者の目からも明らかである開示性を維持している．また集計局を分散することなく，単独の集計局においても得票の途中経過情報を知ることができない方式であるため公平性を保つことができる．また既存の技術では実現が難しかった，自分がある候補に投票したことを証明できない無証拠性と呼ばれる機能をもつような方式に発展させることができ，票の買収などの脅威に十分に対抗できる方式である．

第7章では本論文で得られた成果をまとめて，考察を行っている．