審査の結果の要旨

氏名　　沼尾　雅之

本論文は「IT システムのためのプライバシー保護技術に関する研究」と題し，インターネット等による IT システムの発展に伴い重要性が増しているプライバシー保護について論じ，創案，開発した新技術について記しており，７章から構成されている．

第１章「序章」ではまず，コンピュータによる個人情報利用の形態を，ホスト計算型，クライアント・サーバ型，企業型，P2P(Peer-to-Peer)型，コミュニティ型に分類し，それぞれの形態で必要とされるプライバシー保護について論じている．そして，プライバシー保護の基礎的要素技術として，マルチパーティ秘匿計算，忘却通信(Oblivious Transfer)，知識の証明(Proof of Knowledge)，閾値暗号システム，グループ鍵配信，アクセス制御を挙げ，本論文に記す P2P 環境におけるグループ鍵配信，P2P データ共有における暗号化データ復号権限委譲，リストマッチング，属性鍵配信によるコミュニティ生成，プライバシーポリシーに基づくアクセス制御の各技術を，これらの基礎的要素技術と関連させて位置付けている．

第２章「P2P 環境における動的グループ鍵配信」では，P2P 環境ではホスト同士の結託の可能性もあることから，クライアント・サーバ型モデル下での受信者結託閾値に基づいたグループ鍵暗号法が不適切になる課題に対する技術を提案している．すなわち，P2P 環境のように全体集合や受信グループを予め指定できない動的グループ指定の条件下で，グループに属するホストだけが復号できるグループ鍵で暗号化されたメッセージを発信できるグループ鍵構成法を提示している．この構成法は，復号処理のためにグループ内のホスト同士の通信が必要になるが，受信グループ以外のユーザの結託に対して耐性がある．

第３章は「P2P データ共有における暗号化データアクセス制御」である．P2P に基づくデータ共有では，ホスト(Peer)のネットワークからの離脱や再参加が頻繁に行われる一方で，非接続状態にあるホストの復号鍵を必要とする場面が起こる．そこで，復号鍵を行使する権限を時限的に他のホストに委譲できれば，柔軟なセキュリティサービスの構築が可能になる．本論文では，これを変換サーバと呼ぶ中立な第３者機関を利用することで実現する枠組みを提示している．この手法は以下の特徴を有する．(1)閾値復号技術を応用することで秘密鍵を分散し，変換サーバのチェックを通過した場合のみ暗号文の復号処理を行えるようにできる．(2)一方向性ハッシュ関数を利用し，復号処理に権限委譲期間のチェック機能の含めることにより，変換サーバが行う復号時間のチェックを通過しない限り復号が出来ない．(3)変換サーバの公開鍵を利用することで，受信者が単独で委任鍵を生成して復号処理の代行者に与えるだけで，復号権限の委譲を可能にする．

第４章は「リスト表現多項式を利用したリストマッチング」であり，二人以上の参加者が持つリストの共通部分だけを，個々の参加者の持つリスト内容を明らかにすることなく計算し，その結果の共通部分だけをお互いに共有するリストマッチング問題を，秘匿性と公平性の観点から扱っている．リストの項目を根に持つリスト表現多項式を提案し，これを利用してそれぞれの多項式の和である共通リスト表現多項式を生成する方法を提示している．また，非公開型

共通根検査をする場合についてのプロトコル構成を示し，調停機関としてオンライン型の第３者機関(TTP)を導入した非公開共通根検査による方法が，秘匿性と公平性の要件を満たすことを証明している．

第５章「属性指定による動的コミュニティ生成」では，個人情報を共通属性に使った動的コミュニティ生成のためのセキュリティとプライバシー技術を，オフライン型の属性鍵配信システムを対象にして提示している．この場合の送信者は，指定した属性を満たしたユーザにだけメッセージを配信することができ，一方，ユーザは自分の属性を送信者を含めた誰にも知られることなく，自分宛のメッセージを復号することができる．この技術として，１対１のプロトコルである忘却通信を多対多のマルチキャストメッセージ配信に対応させるために，オンライン属性鍵管理サーバを導入し，主催者，ユーザ，鍵管理サーバという３者のプロトコルを構成している．

第６章「プライバシーポリシーに基づく顧客データのアクセス制御」では，CRM(Customer Relation Management)などの企業 IT システムにおいて，OECD 準拠のプライバシー保護システムを構築するための方法を示している．企業は個人情報の取り扱いに関するポリシーを公開し，アプリケーションシステムが顧客データをアクセスする時に，このポリシーに準拠させる必要があるが，ここではプライバシーポリシーを如何に展開すればよいかを提示し，データベースアクセス制御に関して具体例を示している．

第７章は「結論」であり，本論文の成果をまとめ，今後の課題について述べている．

以上を要するに，本論文はインターネット等による IT システムで重要性が増しているプライバシー保護について論じ，P2P 環境での動的グループに対する鍵配信法，P2P データ共有における暗号化データ復号権限の委譲によるデータアクセス制御法，秘匿性と公平性を考慮した共有リスト部分のリストマッチング問題への対応法，属性指定によるプライバシーを保護した動的コミュニティ生成法，プライバシーポリシーに基づく顧客データアクセス制御法の新手法を提示したものであり，電子情報学上貢献するところが少なくない．

よって本論文は博士（情報理工学）の学位論文として合格と認められる．