論文の内容の要旨

論文題目　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

氏　　名　沼尾　雅之

インタネット及び PC の普及に伴い，情報利用の形態が，従来のサーバからクライアントへの一方的な情報発信に有利なクライアント・サーバ型モデルから，クライアント間の情報の受発信に優れた P2P 型モデルやその応用型に変化しつつある．それに伴って，個人情報の管理，利用法も，サーバにすべての情報を預けて，サーバを介して利用する方法から，重要な情報は個人が管理し，第三者を介さずに，個人が直接利用にも関与する方法が採られ始めている．

本論文では，プライバシー保護技術を論ずるには，個人情報の利用法を考慮することが前提だとの考えの下に，まず，個人情報利用モデルを定義するものとして，信頼関係の確立方法，個人情報の保管形態，個人情報の利用形態を挙げ，これらと実際のビジネスアプリケーションが前提としている IT システムのモデルとの関連について研究する．そのために，以下のような P2P 型，コミュニティ型，および企業システム型という典型的な IT システムモデル上で，個人情報を利用するアプリケーションを実際に構築することによって，個人情報利用形態とプライバシー保護技術の関係を考察する．

- P2P 環境における動的グループ鍵配信
- P2P データ共有における暗号化データアクセス制御
- リスト表現多項式を利用したリストマッチング
- 属性指定による動的コミュニティ生成
- 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

P2P 型モデルにおけるプライバシー保護技術を論じるにあたっては，クライアント・サーバモデルとの差異を明らかにし，P2P 型モデル特有のプライバシー要件を定義する必要がある．**P2P 環境における動的グループ鍵配信**においては，以下の問題を扱う．

・動的グループ鍵配送問題を P2P 環境という条件下で再定義する．システムの要件として，動的グループ鍵生成，動的復号閾値生成，協調復号，結託耐性，全体集合非依存性などを定義する．
・P2P 環境下でのシステム要件を満たす動的グループ鍵配送法を閾値 ElGamal 暗号をベースにして構築する．また，上記要件と秘密鍵サイズ，送信メッセージサイズ，復号メッセージサイズについて，既存グループ鍵暗号システムと比較し，大規模な P2P 環境に適していることを示す．
・提案方法のビジネス応用として，コンテンツ配信システム，合議事項伝達システム，サーバ訪問メータリングシステムなどへの適用について説明する．

また，P2P 型において，ホスト間で復号権限を委譲するための **P2P データ共有における暗号化データアクセス制御**においては，以下の問題を扱う．

・P2P データ共有モデルとして，複数のホストが提供する仮想暗号化データに対して，複数の復号権限保持者による連続処理のモデルを提案する．そして，復号権限保持者（受信者）が，一時的に代行者に復号権限を委任するための要件として，受信者の秘密鍵のプライバシーと送信者の暗号文が受信者または代行者にしか読めないという送信者のプライバシーなどの要件を定義する．
・一時的復号委任プロトコルを，TTP である変換サーバを導入して構築する．また，変換サーバと代行者と結託する攻撃を防ぐために，閾値暗号を利用して，変換サーバを複数にする構築法も示す．
・変換サーバを利用したビジネス応用として，代理復号サービスプロバイダ，複数デバイスによる暗号化データのアクセス制御などへの適用について説明する．

さらに，P2P 型において，ホスト間で共通属性だけを秘密計算するための**リスト表現多項式を利用したリストマッチング**では，以下の問題を扱う．

・複数のパーティの持つ属性リストの共通部分だけを共有するというリストマッチング問題における要件として，共通部分以外のプライバシーと，パーティの一方の能動的攻撃に対しての公平性を定義し，属性値を根に持つようなリスト表現多項式による問題の解決方法を提案する．
・複数のリスト表現多項式の和多項式が，共通属性だけを根に持つことから，この共通リスト表現多項式を利用したプロトコルを，結果計算サーバが単一の場合と，分散 OT を用いて複数化した場合について，構築する．
・リスト表現多項式による OPE では，共通根の場合に関数値が 0 となるという性質を利用して，OPE に対する入力が，かならず自分の属性値であることを検査するプロトコルを，ElGamal 暗号を使った OPE 上で構築する．また，これによって，共通部分以外のプライバシーが守られることを証明する．
・誤った OPE 値を返すという能動的攻撃に対して公平性を守るために，オフライン TTP を調停者として用いた Fair Exchange を利用したリストマッチングプロトコルを構成

する．また，このプロトコルによって，パーティの両者がともに共通属性を共有するか，どちらもなにも得られないかのどちらか一方に必ずなること（公平性）を証明する．

P2P 型における 2 者の関係を N 者に拡張し，コミュニティモデルにおけるプライバシーの問題を論じるものとして，**属性指定による動的コミュニティ生成**では，以下の問題を扱う．

- 年齢，職業など第三者に認定してもらう属性ではなく，趣味や嗜好など個人的コミュニティ形成に必要な任意属性についてのセキュリティ･プライバシー要件を定義する．また，主催者による動的属性指定など，コミュニティ生成のための要件についても定義する．
- オフライン型の属性鍵管理サーバによって，属性鍵の OT による事前配布によって，要件を満たすシステムが構築できることを示す．また，主催者による受信者属性の指定方法として，複合属性条件や数値属性条件も扱えるような方法を示す．
- 提案方法のビジネス応用として，マッチメーキングサービス，パーソナライズドメールサービス，分散検索サービスなどへの適用について説明する．

最後に，クライアント・サーバ型に属しているが，個人情報をサーバ側に委託する企業モデルにおけるプライバシーの保護を論じるものとして，**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**については以下の問題を扱う．

- 法律やガイドラインに準拠した個人情報保護システムの構築法として，P3P プライバシーポリシーに基づく顧客データベースのアクセス制御法を提案する．
- 典型的な Web アプリケーションサーバのアーキテクチャの中で，個人情報へのアクセスをモニターし，プライバシーポリシーに照らして，制御するためのプライバシーモニターの構成を示し，アプリケーションとデータベースを結ぶ JDBC をモニターにすることを提案する．
- JDBC 中の SQL から，プライバシーポリシーの判断に必要な，カラム解析や所有者キー解析をするための解析法を示し，この結果を表現するための SQL アノテーション言語を設計する．また，実際の SQL 検索に対して，結果表のセルごとにアクセス結果が異なるセルレベルのアクセス制御が実現されることを確認する．

結論では，これらの IT モデル，個人情報利用形態，プライバシー保護技術の間の関係について，ID・鍵や属性情報といった個人情報の種類やオンライン型やオフライン型といった TTP の利用形態などから比較，検討をする．そして，個々のアプリケーションに依存しない一般的なプライバシー保護技術の構築法について考察し，さらに将来の研究の展望を与える．