プライバシを考慮した地理位置情報サービスの提案

永廣　悠介†　　小柳　和子†

† 情報セキュリティ大学院大学

1　はじめに

今日携帯電話やカーナビゲーション・システム，携帯ＧＰＳ端末等，地理的な位置情報を活用する機器が普及し様々なサービスに活用されている．これらの機器から地理位置情報を収集・蓄積することで，時間的・空間的に詳細で広範囲な移動体の情報を把握可能となることから，ネットワーク上での地理位置情報の取り扱いに関する研究も行われている．[1][2]

本論文ではこのような地理位置情報を収集する際の問題点について述べ，問題を解決した地理位置情報サービスのモデルを提案する．

2　地理位置情報収集における問題

地理位置情報収集における問題点は，収集データ量の問題，提供情報の利用制御の問題の２点が考えられる．

サービスを提供するにあたり有用な情報を得るためには，携帯電話やカーナビ等移動体からの位置情報データを，できる限り幅広く収集することが重要である．しかし現在は地理位置情報を利用するサービス事業者が，移動体からデータを収集・蓄積しサービスに利用するシステムを独自に構築し運用している．そのため各サービス事業者は移動体の位置座標や時刻情報といった同様の情報を利用しているにも関わらず限定された移動体からしか情報を収集できないため，収集データ量が限られてしまう．これが１点目の問題である．

この問題点を解決するためには，全てのサービス事業者が利用できる共有の地理位置情報収集・蓄積基盤を構築する方法が考えられる．このような共有の地理位置情報収集・蓄積基盤を利用した場合，蓄積されたデータに全てのサービス事業者がアクセスできるため，地理位置情報の提供者である移動体は，自身の地理位置情報の柔軟な制御ができないというプライバシ上の問題が生じる．これが２点目の問題である．

次章では以上の２点の問題を解決した地理位置情報サービスを提供するためのモデルを提案する．

3　提案する地理位置情報サービスのモデル概要

提案する地理位置情報サービスには次の３者が関連する．

移動体　地理位置情報の提供者である．本論文では通信機能を有し，ＧＰＳ等により得られる地理的位置座標をサービス事業者に対し提供可能な車載器を搭載した車両を想定する．

サービス事業者　移動体から送信される地理位置情報を収集・蓄積し，それを利用したサービスを提供する．

認証局　移動体がサービスの利用を開始するにあたり，正規の端末であることを確認し，承認を与える役割を果たす．認証局にて認証が完了した移動体のみがサービス事業者に対して地理位置情報の送信が可能となる．

システムに求められる要件は次の３点が考えられる．

- 移動体は自身が選択した複数のサービス事業者に対し地理位置情報を送信できる
- 移動体は情報の送信先サービス事業者毎に，送信する地理位置情報の開示レベルを段階的に選択できる
- サービス事業者への地理位置情報送信にあたり，移動体固有のＩＤ情報が秘匿される

以上３つの要件を満たすため，次に挙げる２つの手法を利用する．

グループ署名　サービス事業者が移動体の固有ＩＤを受信せずに正規に利用登録された移動体であることを認証するために，グループ署名を利用する．本論文では，研究目的で公開されているグループ署名ライブラリを利用した．[3][4]

段階開示暗号化　移動体から送信する地理位置座標（緯度，経度）を予め設定された桁で分割し，分割した座標値を開示レベル毎の鍵で暗号化する．

4　地理位置情報送信処理手順

移動体の登録から，サービス事業者への地理位置情報送信に至るまでの処理手順について述べる．

初期設定　まず地理位置情報システムの利用を希望する移動体が，認証局への登録要求を行う．認証局は，登録要求のあった移動体から提示された移動体情報を確認し，問題なければ移動体に固有のユーザ鍵を生成し，グループ公開鍵とともに移動体へ送信する．生成したユーザ鍵は移動体情報と結び付けて認証局に保存され，認証局による移動体の特定（グループ署名を用いた匿名性の剥奪）に使用される．移動体は受信したユーザ鍵をグループ公開鍵とともに，グループ署名作成に使用する．この初期設定手順は，地理位置情報システムの利用開始時に１度行うだけでよい．以上を図１に示す．なお，グループ公開鍵はシステムを利用する全ての移動体，サービス事業者に対し公開される単一の鍵データである．これに対しユーザ鍵は，システムを利用する移動体それぞれに対し個別に生成される鍵データであり，個々の移動体と認証局のみが知りえるように取り扱われる．

セッション開始時セットアップ　移動体がサービス事業

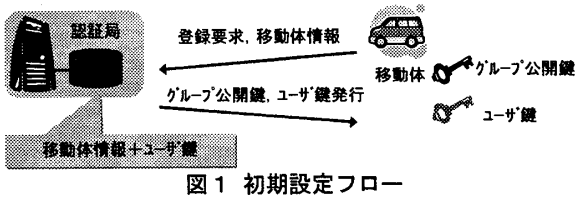

図１　初期設定フロー

A Geographical Location Information Service Considering Privacy
Yusuke Nagahiro†
Kazuko Oyanagi†
† Institute of Information Security

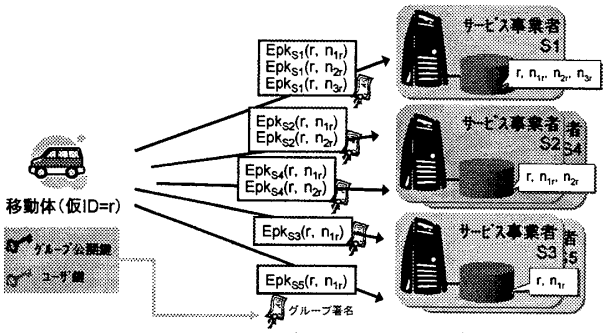

図２ セッション開始時のセットアップフロー

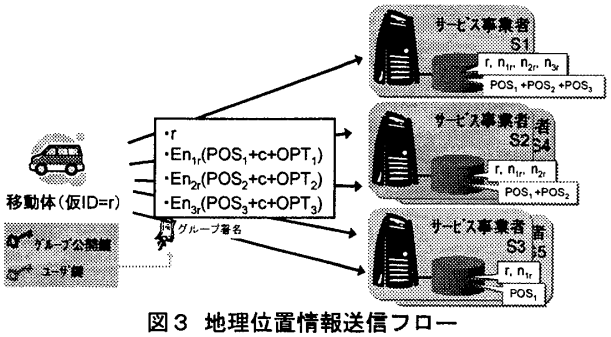

図３ 地理位置情報送信フロー

者に対し地理位置情報の送信を開始するには，まずセッション用の仮ＩＤである ｒ を生成する．さらに送信する地理位置座標を暗号化・復号化するための共通鍵 n_{ir} を生成する．ｒは仮 ID ｒが有効なセッション中に使用すること，ｉ は地理位置情報の開示レベルに合わせて複数共通鍵を生成することを表している．次に移動体側で地理位置情報の送付先としてサービス事業者を選択する．選択した送付先ごとに地理位置情報の開示レベルを決定する．それぞれの送付先に仮 ID ｒと，決定した開示レベルとそれより低いレベルの共通鍵 n_{ir} を送付先サービス事業者の公開鍵で暗号化し，送付メッセージとする．この送付メッセージに対しグループ署名用のユーザ鍵，グループ公開鍵を使用してグループ署名を付与し，サービス事業者へ送付する．メッセージを受信したサービス事業者は，メッセージに付与されたグループ署名を認証局から提供されるグループ公開鍵を利用して検証を行う．正規に登録された移動体による署名であればこの検証をパスできるが，具体的にどの移動体により付与された署名であるかは割り出すことができない．この検証で正規の移動体であることが確認されれば，受信した仮 ID ｒ と共通鍵 n_{ir} を紐付けて登録する．以上を図２に示す．

地理位置座標の段階開示暗号化　移動体からの地理位置情報の送信は，セットアップ時に作成した共通鍵 n_{ir} を用いて暗号化を行う．まず地理位置座標（緯度，経度）を表１の例に示すように開示レベル別に分割し，分割した情報を上位桁側から POS_1～POS_3 と呼ぶ．この情報を暗号化し送信メッセージを作成する．送信メッセージの再送攻撃を防止するため，暗号化メッセージにカウンタ ｃ を加える．また，必要に応じて付加する追加メッセージを OPT とし，レベルに応じて付加する．

以上をまとめると，開示レベル ｉ の暗号化送信メッセージは，$E_{n_{ir}}(POS_i+c+OPT_i)$ となる．

地理位置情報の送信　移動体は，分割・暗号化したメッセージを全て結合し，仮 ID ｒとともにグループ署名を付与し，サービス事業者に対し送信する．グループ署名の付与はセッション開始時セットアップ時と同様，グループ署名用ユーザ鍵とグループ公開鍵を使用する．以上の手順でグループ署名が付与された暗号化メッセージ，仮 ID ｒ は図３のように送信される．メッセージを受け取ったサービス事業者は，メッセージに付与されているグループ署名を検証し，正規の利用者として登録された移動体からのメッセージであることと，メッセージが通信経路上で改ざんされていないことを確認する．その後，メッセージに含まれている移動体の仮 ID ｒ に対応する，登録済みの共通鍵を使用して暗号化された地理位置情報を復号する．復号後，カウンタ ｃ の値が既に受信済みのものよりも大きい値になっていることを確認する．カウンタ ｃ が受信済みのメッセージと同じ場合，そのメッセージは再送されたものであるため破棄する．以上の処理を行った後，分割された地理位置情報をつなぎ合わせ，各サービス事業者で蓄積・利用する．

表１ 地理位置座標の開示レベルによる分割例

開示レベル	1 (粗)	2	3 (詳細)
緯度	北緯 35.46	8	139
経度	東経139.62	3	195

単位:度(°)

５　まとめと今後の課題

本論文で提案した地理位置情報サービスのためのモデルでは，地理位置情報提供者自身が情報の提供先を選択し，かつ提供する情報の開示レベルを選択可能とした．さらに，移動体の認証にグループ署名を使用することで移動体固有のＩＤを秘匿可能とし，プライバシを考慮した位置情報の取り扱いが可能となった．

また，複数のサービス事業者が共通の情報収集システム基盤を利用し地理位置情報の収集を行う方式としたことで，個々のサービス事業者がそれぞれ独立して収集するよりも幅広い地理位置情報を収集することが可能となった．

今後の課題としては，グループ署名，データの暗号化，通信処理を含むシステム全体の具体的な設計を行った上で処理性能測定を行い，システムとしての実現可能性を評価することが挙げられる．また，提案したシステムにおいて要求されるグループ署名の安全性と処理性能について，調査，検討を行うことも課題として挙げられる．

参考文献

[1] WIDE プロジェクト，インターネットにおける地理位置情報の管理手法，WIDE プロジェクト 2004 年度 研究報告書 第 23 部，pp. 363-390，2004

[2] 中西 健一，高汐 一紀，徳田 英幸，粒度の動的変更による位置匿名性についての考察，情報処理学会論文誌，Vol. 46，No. 9，pp. 2260-2268，2005

[3] 側高 幸治，松田 誠一，土井 洋，岡本 健，小松 文子，岡本 栄司，匿名署名を実現するための Pairing を用いたグループ署名ライブラリの実装，マルチメディア，分散，協調とモバイル(DICOMO2007)シンポジウム，pp. 1398-1402，2007

[4] 多田 真崇，芦野 佑樹，安 健司，佐々木 良一，側高 幸治，松田 誠一，土井 洋，岡本 栄司，電子文書の内容から通報者発覚の防止が可能な匿名内部告発システムの提案と試作，マルチメディア，分散，協調とモバイル(DICOMO2007)シンポジウム，pp. 1190-1199，2007