地理的位置情報管理システムにおける プライバシ制御の提案

和泉 順子　　砂原 秀樹
michi-i@is.aist-nara.ac.jp　　suna@wide.ad.jp

奈良先端科学技術大学院大学

近年、インターネットと携帯端末の急速な普及によりモバイル・コンピューティングが注目されている。この環境における重要なサービスとして、ネットワーク空間と現実世界の空間とを結び付けることがあげられる。

このため、ネットワーク上に存在するエンティティの論理的な位置と、その地理的な位置情報を対応づける機能をもつ Geographical Location Informasion (GLI) システム [1] が提案され、これによって、モバイル・ユーザは、現実世界の位置情報を用いてネットワーク上に存在するエンティティにアクセスすることが可能となった。

現在は、InternetCAR プロジェクト[1] において、車の位置情報を管理するために、この GLI システムが用いられている。しかし、このプロジェクトによって、GLI システムにプライバシ制御機能が必要であることが分かっているが、現在の GLI システムには この機能は実装されていない。

そこで、本研究では GLI システムにおけるプライバシ制御方法について提案する。

今回、認証された情報受信者であるクライアントは、情報の所有者と直接通信することなく、必要な情報を引き出すことのできるシステムを目指す。

GLI システム上にある保護すべき個人情報についてを、以下のポイントにおいて議論する。

1. GLI システム上での個人情報と公開情報との切り分けについて
2. 情報発信者と直接の通信をすることなく、GLI システムにおいて個人情報を保護する方法について
3. GLI システムに蓄積する”ID” の問題について

基本的には、以下にあげる情報を公開する：地理的な位置 [緯度、経度、高度]、エンティティの速度 [方向、速度]、エンティティの属性情報 [ライトの点灯、外気温等]。

これらの公開情報は、エンティティの地理的な位置と移動速度により交通情報を作成できることなどから、インターネット上で扱う情報として、非常に有益であると言える。

しかし、各エンティティ所有者のユーザ名は、全ての人に公開すべきではない。

そこで、これら個人情報へのアクセス制御方法について図 1 のようなモデルを提案する。今回の提案では、GLI サーバでは、暗号化された個人情報を蓄積する。このサーバは、情報を復号化する機能を持っていないため、アクセス制御表 (ACL) を付加したこれらのデータへのアクセス制御をするだけである。個人情報の復号化は、認証された受信者であるクライアントの役割であり、この方法を用いることで、個人情報への不特定多数による無制限なアクセスを防ぐ。

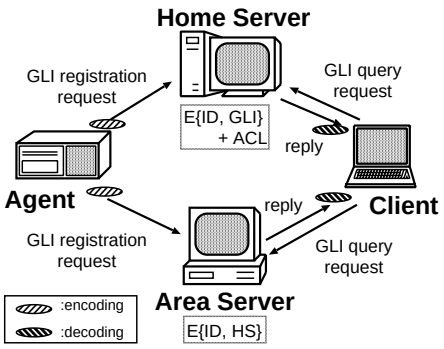

図 1: GLI システムにおけるアクセス制御モデル

また、本研究では、サーバに地理的位置情報を蓄積するために必要となる、一見意味をなさないような疑似 ID について考察している。現在のシステムでは、サーバにおいて情報を管理する識別子として、IP アドレスや FQDN (Fully Qualified Domain Name) が用いられているが、これでは地理的な位置情報の所有者が推察されてしまう。したがって、サーバで情報を蓄積／管理するための、一見無意味に見える疑似 ID を導入する。本物の (意味をなす) ID については、暗号化されてサーバ上に蓄積される。

現在、プライバシ制御機能を付加した GLI システムのプロトタイプを実装しており、また、プロトタイプ・システムの評価についても議論している。

参考文献

[1] Yasuhito Watanabe, Atsushi Shinozaki, Fumio Teraoka, Jun Murai: “The Design and Implementation of the Geographical Location Information System” Proc INET’96

[1] http://www.mist.sfc.wide.ad.jp/InternetCAR/