# プライバシ保護を考慮した地理位置情報システムの設計と実装

渡辺 恭人（riho-m@sfc.wide.ad.jp） 竹内 奏吾（sohgo@csl.sony.co.jp）
佐藤 雅明（saikawa@sfc.wide.ad.jp） 寺岡 文男（tera@csl.sony.co.jp）
村井 純 （jun@sfc.wide.ad.jp）
慶應義塾大学 (株) ソニーコンピュータサイエンス研究所

## 概要

プライバシー保護を実現した地理位置情報管理システム（GLIsecシステム）を提案する．我々が提案しているGLIシステムは，インターネットに接続している移動体の地理位置情報を地球規模で管理するものである．移動体は自分の位置をサーバに登録し，検索者は移動体の識別子を鍵とした位置検索，および地理範囲を鍵とした移動体検索が可能である．GLIシステムはサーバの階層化による分散管理により地球規模での運用を実現する．提案するGLIsecシステムは，GLIシステムを拡張する形で設計・実装した．本稿では，GLIsecシステムの設計と，インターネット自動車を利用した実験について述べる．

## プライバシ保護の目標

本稿で目標とするプライバシー保護とは，第三者による移動体の特定防止，追跡防止，なりすまし防止およびインターネットにおける盗聴防止，データ改竄防止である．

## 実現方法

移動体の特定防止は，移動体の識別子をその移動体と信頼関係にある検索者との間で秘密の識別子として共有し，GLIシステムのサーバ群に，その秘密の識別子から生成される第三者には無意味な識別子を登録することで実現される．この第三者には無意味な識別子をHID(Hashed ID)と呼ぶ．このHIDは，秘密の識別子と時刻情報をハッシュ関数に入力することで生成される．HIDはこの入力値を共有する信頼関係にある検索者だけが生成でき，通信することなく共有することができる．また時刻情報を用いて，頻繁にHIDを変更することで追跡を防止する．

移動体がHIDと位置情報を登録する場合，それを蓄積するサーバに直接登録すると，送信元IPアドレスとHIDが対応付けられるおそれがある．移動体のIPアドレスとHIDの関係を無くすため，登録サーバを介して登録する．認証された移動体のみに登録させるため，登録サーバは認証も行う．移動体と登録サーバ間ではIPsecのESPを利用して盗聴の防止と認証を行い，その他のサーバ間では，IPsecのAHを使用して，改竄を防止する．

## GLIsecシステム

以上の実現手法から既存のGLIシステムを拡張し，図1のようなGLIsecシステム構成を導入する．

本システムは，登録クライアント，登録サーバ，HIDサーバ，エリアサーバ，検索クライアントから構成される．移動体では，登録クライアントが特定の登録サーバから認証され，HIDとGLI（Geographical Location Information）を送信する．GLIは移動体の地理位置情報であり，緯度，経度，高度によって指定される1地点を示し，公開情報として扱う．登録サーバは，HIDとGLIをHIDサーバとエリアサーバへ送信する．HIDサーバとエリアサーバはHIDとGLIを蓄積し、検索クライアントからの検索要求を受け付ける。前者はHIDを鍵とした検索(正引き)を，後者は位置を鍵とした検索(逆引き)を受け持つ．(詳細は[1]を参照)

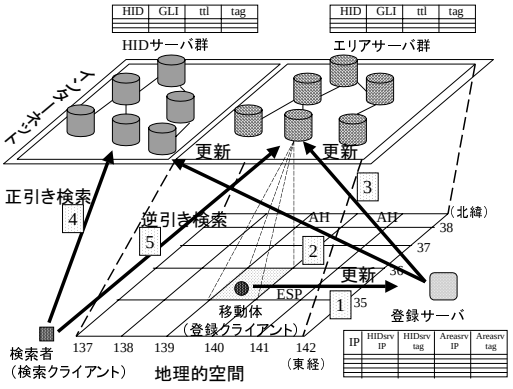


図 1: GLIsecシステム構成

## 実装状況と今後の予定

以上の設計から実現可能性を確かめるために実装を行っている．現状では，移動体と信頼関係にある検索者において同時刻にHIDが生成され，基本的な登録と検索が行える．また，本年9月に慶應義塾大学にて行われたオープンリサーチフォーラムにおいて，インターネット自動車を利用した実験デモを行った．デモでは，インターネット自動車のHIDとGLIを登録し，HIDを指定した正引き検索した結果を地図上に表示するアプリケーションを動作させた．今後，本システムの実装を継続し，本システムの評価について議論していく．

## 参考文献

[1] 渡辺 恭人, 竹内 奏吾, 寺岡 文男, 村井 純: プライバシ保護を考慮した地理位置情報システム, 情報処理学会 コンピュータセキュリティ研究会, (2000-CSEC-11-4), pp. 19-24, Sep. 2000