柔軟なプライバシ保護を考慮した分散型位置情報システムの提案

Nor Zehan Binti Ahmad(zehan@cacao.cs.uec.ac.jp)
楯岡 孝道(tate@cs.uec.ac.jp)
阿部 公輝(abe@cs.uec.ac.jp)
2005年1月7日

本論文では、柔軟なプライバシ保護を実現した地理位置情報システム(GLIPSE システム)を提案する。GLIPSEシステムは、インターネットに接続している移動体(以下、Agentと呼ぶ)の地理位置情報(緯度・経度・高度)を管理する。従来の位置情報システムと異なり本システムでは、Agentが設定するプライバシポリシの元で公開する位置情報を制御できる。これは、アクセス制御表とルールを管理するサーバを導入することにより行う。公開する位置情報を制御することにより、第三者によるAgent特定、位置情報特定Agent追跡を防止する。また、IPsecのESPとAHを利用することにより、インターネットにおける盗聴防止、データ改竄防止、なりすまし防止も実現している。暗号や電子署名処理にかかる時間を測定し、本システムの性能を見積もる。

A Distributed Geographical Location Information System with Flexible Privacy and Security Enhancement Functions

In this paper we propose the Geographical Location Information System with Privacy and Security Enhancement (GLIPSE) functions. Our proposed system provides a way to manage geographical location information (latitude, longitude, altitude) of mobile entities (Agent), connected to the Internet. The novelty of this system compared to the conventional geographical location information system, lies in its ability to control location information accessibility based on the privacy policies set up by each agent. We propose the implementation of this function by introducing an Access Control List and access management servers. The Agents are protected from being unwillingly identified or tracked by a third party, through location information accessibility management. As this system uses Internet for transferring data, encryption and digital signature using ESP and AH in IPsec are proposed to protect the location information data from eavesdropping, interception, alteration or identity spoofing from outside. We evaluate the performance of the system by measuring the time required for processing encryption and digital signature.

1 はじめに

近年、インターネットと携帯端末の急速な普及により、移動するユーザの地理的な位置情報を利用するアプリケーションが多く開発されている。単純なアプリケーションとしては、NTTドコモが2000年1月より提供している「どこNavi」サービスがある。さらに、地理的位置情報を利用するアプリケーションが様々な場面で利用されることが期待されている[1]。しかしながら、地理的位置情報を管理することで享受するメリットの一方でプライバシ侵害などの新たな問題が予想される。

例えば、情報がサービス提供者以外に利用されてしまう、匿名で提供した位置情報が個人と対応づけられてしまうなどの問題が生じる。このような問題を防ぐためにIETFgeoprivワーキンググループでは、位置情報システムにおけるプライバシ保護を考慮するための要求仕様が議論され、[2]で公開している。だが、現状ではこれを実装したシステムはない。

[3]でプライバシ保護を考慮した地理位置情報システム(GLI: Geographical Location Information)が提案された。このシステムは現実世界を移動する移動体を対象とし、その識別子と位置情報および付帯情報の登録・検索機能を実現している。GLIでは、時とともに変化する匿名の識別子で登録することにより移動体の特定・追跡を防止している。また、この識別子は移動体と信頼関係にある者は移動体と対応づけることができ、信頼関係のない者には統計情報しか公開しないことでプライバシを保護している。

しかし、実際にプライバシを保護するためには位置情報を公開するか・しないかだけではなく、公開する情報を含めて、よりきめ細かく制御する必要がある。例えばユーザはある時間帯のみ、あるエリア内でのみ、または目的に応じて位置情報を公開するか・しないかを決めたい。このように様々な条件に応じて公開する位置情報を調整することが求められている。

この概念を考慮した例としては、[4]が知られている。しかし、位置情報システムの応用範囲を広げる、位置からその場にいる移動体を検索する機能がなく、サーバの分散化も考慮されていない。そこで、GLIシステムの高度な検索機能を損なうことなく、[2]で議論されているプライバシ保護の肝腎となる要求を適用した新たな位置情報システムGLIPSE(Geographical Location Information with Privacy and Security Enhancement)を提案する。

2 セキュリティ上の脅威とプライバシ保護の目標

GLIPSEシステムは、大きく分けて、位置情報を登録するエンティティ(以下、Agentと呼ぶ)、情報を管理するサーバ群(以下、Serversと呼ぶ)と、位置情報を検索しそれを利用するエンティティ(以下、Clientと呼ぶ)からなる。各エンティティはインターネットを介して通信を行う。プライバシ保護をするためには、各エンティティが管理するデータおよびそれぞれの通信に対する脅威からデータを守らなければならない。[5]では、IETFワーキンググループで議論された位置情報システムにおける脅威分析が公開されている。

ここでは、Serversを基本的に信用しないという前提の上でGLIPSEシステムのセキュリティ上における脅威を抽出し、プライバシ保護の目標を定める。

2.1 プライバシ侵害

GLIシステムでは信頼関係の有無でしか情報を制御できない。Agentと、信頼関係を結んでいるClient全てとの間で、同じ秘密を共有しているため、一度許可したClientのアクセスを再度禁止することが難しい。従って、Agentが許可した目的外で利用されることを防ぎにくくなり、Agentのプライバシを侵害される危険性がある。また、あるエリア内に登録するAgentが少ない場合においては、時と共に変化する匿名の識別子を利用しても、Agentを特定される可能性があり、プライバシ侵害につながる。従って、信頼関係があるかどうかでのみ制御するのではなく、様々な条件に応じて精度を含めて位置情報を制御できるシステムを設計する。

2.2 通信路での盗聴、改竄

インターネットを介して通信を行うことにより、通信データが盗聴されたり、改竄される可能性がある。通信中のデータには送信元のIPアドレスが含まれるため、そのデータを特定のAgentと対応付けられる可能性がある。また、過去に盗聴したデータを利用して、位置情報とすり替える再生攻撃も考えられる。従って、データが盗聴されても盗聴者に解釈できない、データが改竄されたり、古いデータを再送信された場合でも、各エンティティがそれを検出できるようにする。

2.3 なりすましの脅威

悪意を持つ要素がAgentになりすまして偽の位置情報を登録し、ServersになりすましてAgentが登録するデータを奪ったり、またあるClientになりすましてAgentがそのClientに許した位置情報を得てしまうなどの危険性がある。従って、なりすまし防止ができる、各エンティティが互いに認証し合えるメカニズムを扱えるようにする。

2.4 データベースの盗難・書換

位置情報を管理するServersはそれぞれAgentとその位置情報を対応づけられるデータベースを持っているので、Serversのデータベースが盗難されたら、Agent を特定される可能性がある。従って、データベースが盗難された場合においても、許されたエンティティ以外には解読できないようにする、またはAgentにとって最低限の被害しか及ばないようにシステムを設計する。

3 プライバシ保護のための機構

本章では、GLIPSEシステムにおけるプライバシ保護のための機構について述べる。

3.1 アクセス制御表とRule Serverの利用

ユーザのプライバシポリシはアクセス制御表(Access Control List, ACL)に記述される。ACLでは、何種類の精度の位置情報を用意するか、どのClientに対してどの情報を渡すかなどがリストされる。本論文ではACLについて、異なる精度の情報をn個生成する方法と、その選択ポリシをリストすることのみで、詳細は定めない。

Clientは位置情報を取得するためにACLを管理する要素から毎回許可を取得しなければならないため、Agent自身がACLを管理するのは現実的ではない。従って、サーバ群の中にはACLを管理するためのRule Serverを導入する。Clientにどの情報を渡すかを決めるためにはRule Serverに問い合わせる形にする。このようにすることによって情報取得権を持つClientのみが、Agentに許された情報を取得できることになり、2.1節の脅威に対処できる。

3.2 情報の暗号化と認証機能-IPsecの利用

通信路での機密性を高めるために、IP Security(IPsec)のESP(Encapsulating Security Payload) [6] を使用する。ESPで各エンティティでの送信時に位置情報と所有者情報を暗号化し、データの完全性や発信者認証も行う。これは、2.2節の盗聴対策に効果があり、過去のデータによる再生攻撃にも有効である。また、ESPの発信者認証機能により2.3節の悪意要素によるなりすまし防止もできる。改竄防止と発信者認証機能のみが必要な通信の場合は、IPsecのAH (Authentication Header) [7] を利用する。

IPsecを使用するためにはエンティティ間において秘密鍵の共有などのSecurity Association (SA)が必要になる。SA確立時にはIKE(Internet Key Exchange) [8] を用いる。

GLIPSE中にはPKI[9]を構築し、IKEで利用する各要素の公開鍵や電子署名の正当性をGLIPSEのCAが保証できるようにする。

3.3 Serversで管理するデータの分割

データベース盗難の対策として、各サーバで管理するデータを分割する。特に、位置情報とその所有者情報を対応付けられないようにこれらを別のサーバで管理する。両方の情報が別々に管理できない場合、一つの情報所有者に対して一台のサーバが管理するようにする。これにより、そのサーバが乗っ取られた場合でも、一人の所有者の情報のみ漏洩することになり、2.4節を満たすことができる。

4 提案システムの設計

4.1 構成

GLIPSEシステムは位置情報を登録するAgent(A)、ACLを管理するRule Server(RS)、位置情報を管理するData Server(DS)、各地理位置情報に対応したAgentの情報を管理するArea Server(AS)と位置情報を検索するClient(C)から構成される。分散管理については[10]と同様の手法を用いる。

本システムの説明をする準備として、以下のものを定義する。

- $E_A(M)$
  メッセージMを鍵Aで暗号化したもの(暗号文)。
- $S_A(M)$
  メッセージMにAの署名を付加したもの。
- $Cert_A$
  Aの証明書。
- L
  Agentが登録する位置情報。本システムで扱う位置情報は、現実世界で移動するエンティティの地理的な位置情報[緯度、経度、高度]である。LはACLで指定した異なる精度n種類で登録できる。
- ID
  Agentの元々の識別子。インターネット上のIPアドレス、FQDNやユーザ名、現実世界での名前などにあたる。
- $pseudoID$
  IDをスクランブルした、時と共に変化する識別子。第三者によるAgentのIDとの対応付けは困難である。この識別子はArea Server内でのAgentの匿名性を保っている[1]。
- ttd
  位置情報の有効期限。ある程度位置情報が更新

されないとき、各サーバのデータベースからAgentの情報を削除するまでの時間である。

- i
  位置情報の精度を表す番号。
- 正引き検索
  IDを鍵としてAgentの位置情報を検索する機能。例えば、あるAgentのIDを指定して検索すると、許可された精度の位置情報が得られる。
- 逆引き検索
  地理的な位置情報を鍵として、その領域に存在するAgentを検索する機能。例えば、検索する範囲を2点の位置情報で指定して(北緯50度〜51度、東経100度〜101度）検索すると、その範囲内にいるAgent群と、その位置情報のリストが得られる。

4.2 動作

本章では、登録処理、正引き処理と逆引き処理のそれぞれについて、通信手順を説明する。

4.2.1 登録処理

登録処理の手順を図1に示す。さらに詳しい手順を図2に示す。

Agentは位置情報LとID、オプションとしてACLとttdをRule ServerにESPで登録要求を送る。

Rule ServerはACLに基づいて位置情報Lをn通り計算し、各Lに対する鍵K_iを生成する。データセット$[ID, i, E_{ki}(L_i), ttd)]$($ttd$はオプション)のリストをESPでData Serverに登録要求として送る。このようにして、一つのAgentに対して様々な精度の位置情報をData Serverに登録する。

同様に、Rule Serverはデータセット$[pseudoID, i, L_i, ttd]$ (ttdはオプション) のリストをArea Serverに登録要求としてESPで送る。このようにして、一つの$pseudoID$に対し、様々な位置情報を登録することが可能である。

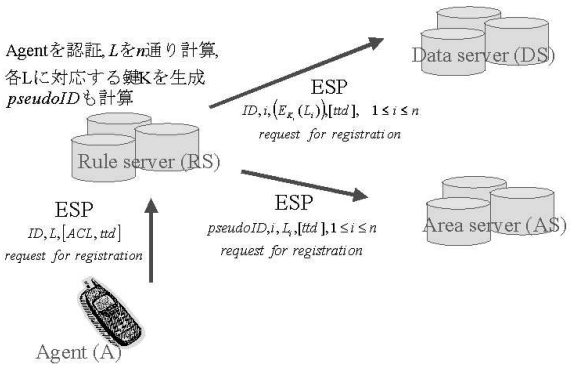

図 1: 登録手順

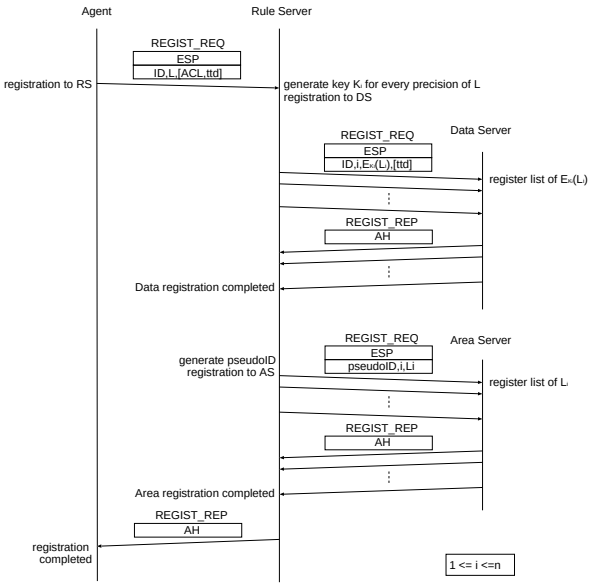

図 2: 登録処理(詳細)

4.2.2 正引き処理

正引き検索処理の手順を図3に示す。さらに詳しい手順を図4に示す。

Clientは検索したいIDをRule Serverに検索要求としてESPで送る。

Rule ServerはACLに基づいてClientに許された位置情報の精度iを決定し、その精度iに対する鍵K_iとアクセス許可をData Serverの公開鍵で暗号化し、データセット$[K_i, E_{DS}(S_{RS}(C, ID, i))]$をESPでClientに送り返す。

Clientはそのアクセス許可をData Serverに送る。Data Serverは鍵K_iで暗号化されたままの情報をAHでClientに送り返す。

ClientはData Serverから受信した鍵K_iで復号化し、Agentの位置情報を取得する。

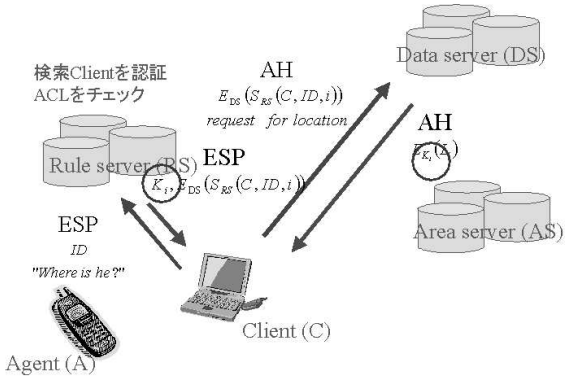

図 3: 正引き検索の手順(詳細)

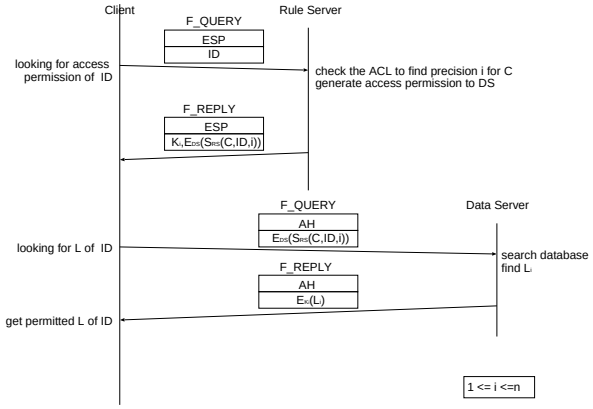

図 4: 正引き検索処理

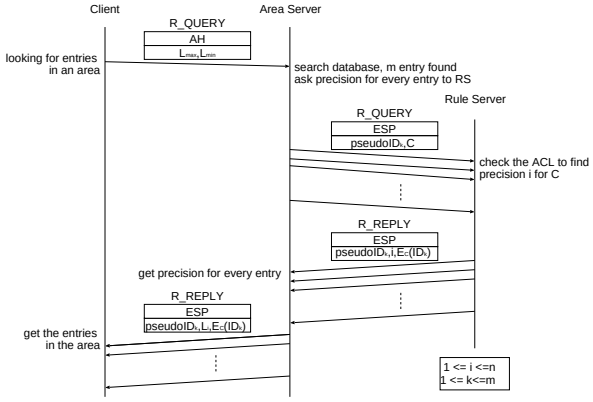

図 6: 逆引き検索処理(詳細)

4.2.3 逆引き検索

逆引き検索処理の手順を図5に示す。図6にその詳細を示す。

Clientは検索したい範囲指定し、Area ServerにAHで検索要求を送る。

Area Serverは要求された範囲にmエントリを発見すると、各エントリに対してどの位置情報を返せばいいのかをRule Serverに問い合わせる。Rule Serverは ACLを確認し、各エントリに対してAgentが許可した位置情報の番号iをArea Serverに返す。そのClientに対してAgentのIDを明らかにしてもよい場合には、そのIDをClientの公開鍵で暗号化して同時に返す。そうでなければ、$pseudoID$を渡す。このようにして、Agentが許可した情報しかClientに渡さないことになる。

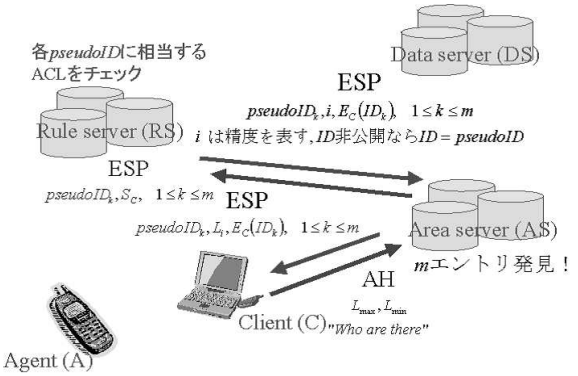

図 5: 逆引き検索の手順

5 評価および考察

本システムにおいては、暗号処理の部分に大きな負荷がかかると予想される。本実装に向けて、準備実験として本システムで利用する各種暗号の処理時間を測定し、システム全体の性能の見積もりを行った。また、電子署名の生成と認証の処理時間も測定した。

全ての実験はAiCryptoライブラリ関数[11]を使用して行った。測定は、Intel社製Pentium 4 (2.40 GHz) CPUを用いたFreeBSD 4.9R上で行った。

5.1 暗号の処理

まず、公開鍵暗号による暗号化と復号化の処理時間を測定した。測定に用いた関数はAiCryptoライブラリ[11]のRSAprv_doCrypt()とRSApub_doCrypt()という関数である。使用した鍵の長さはぞれぞれ、modulus INTEGER n 1024 bit、publicExponent INTEGER e 17 bitとprivateExponent INTEGER d 1024 bitである。ランダムな128byteの入力値で暗号化と復号化を10000回処理し、測定した。結果を表1に示す。

表 1: RSAにおける暗号化および復号化の処理時間

処理	平均処理時間
暗号化	1.2 msec
復号化	46.9 msec

同様に、共有鍵暗号による暗号化と復号化の処理時間を測定した。使用した関数はDES3_cbc_encrypt()とDES3_cbc_decrypt()である。192 bitの鍵長に、実装で使用するデータペイロードに十分な大きさとして、4096 byteの入力値を10000回処理し、測定した。結果を表2に示す。

表 2: 3DES CBCモードにおける暗号化および復号化の処理時間

処理	平均処理時間
暗号化	1.5 msec
復号化	1.4 msec

5.2 電子署名の処理

認証に使用する電子署名の生成および検証するための処理時間を測定した。利用した関数は電子署名生成の場合は、OK_do_signature()、その署名の検証の場合は、OK_do_digest() と OK_do_verify() である。128 byteの平文に128 byteの秘密鍵、SHA1withRSAEncryptionアルゴリズムで10000回処理し、測定した。結果を表3に示す。

表 3: SHA1およびRSA暗号化による電子署名の処理時間

処理	平均処理時間
署名の生成	47.4 msec
署名の検証	1.3 msec

5.3 登録、検索の性能見積り

IKE、ESP、AH、暗号や電子署名の処理回数を数え上げ、5.1節と5.2節の測定結果を代入し、登録や各検索全体の処理時間とその性能の見積もりを1回目と2回目以上の処理に分け、表4にまとめた。なお、nは公開する位置情報の精度の数。mは検索で発見したエントリ数。

表 4: 処理時間と性能の見積もり

処理		登録 ($n=2$)	正引き検索	逆引き検索($m=20$)
処理時間 ($msec$)	1回目	$148.8+3n$ $=154.8$	247.1	$148.7+5.6m$ $=260.7$
	2回目以上	$1.4+3n$ $=7.4$	99.7	$5.6m$ $=112$
性能 (req/sec)	1回目	6	4	4
	2回目以上	135	10	9

5.4 従来の位置情報システムとの比較

本節で、プライバシの保護について従来のGLIシステムと比較する。

GLIではAgentがある位置に長時間停止していると、匿名のIDが変化しても、その匿名のIDがどのAgentのIDであるかが対応づけられてしまう。また、GLIシステムでは、匿名のIDの有効期間内にはAgentの追跡ができてしまう。なぜなら、正引き検索で利用する検索鍵は逆引き検索で取得できるためである。しかし、GLIPSEシステムでは、アクセスをClient毎に制限することとそれぞれの検索に異なるIDを用いることにより、両方の問題を回避できる。

GLIシステムでは、Agentと信頼関係にあるClientは匿名のIDを生成し、偽の位置情報を登録可能である。それに比べ、本システムは電子署名により各エンティティの認証を行っているため、権限のあるエンティティ以外は要素以外は偽の登録ができない。従って、プライバシ保護の面においては、GLIPSEシステムがより優れていると言える。

5.5 サーバの盗難・書換

GLIPSEシステムで各サーバが管理する情報を表5にまとめた。Rule Serverは最も信頼されるサーバで、AgentとそのAgentの位置情報の対応を含めて全て管理している。本システムにおいては、一つのRule Serverは一台のAgentを管理するとする。従って、Rule Serverが乗っ取られた場合、一台のAgentの情報しか影響されないで済む。一つのRule Serverで複数のAgentを管理することも可能だが、サーバ運用コストとプライバシ保護の機能はトレードオフの関係にある。

Data ServerはAgentのID情報を持つが、管理する位置情報は暗号化されたものしか持たない、またArea Serverは位置情報を持つが、本当のIDは持たない。このため、一度に両方のサーバが乗っ取られても、Agentを特定・追跡されない。

表 5: 各サーバで管理する情報

サーバ	管理する情報
RS	A, DS, ASのIPアドレス、ACL、ID、$pseudoID$、鍵K_i、L
DS	RSのIPアドレス、ID、$E_k(L_i)$
AS	RSのIPアドレス、$pseudoID$、L_i

6 おわりに

本論文では、様々な条件に応じて位置情報の公開精度が制御できるGLIPSEシステムの枠組みを提案した。本システムでは、Rule Serverに登録するAgent毎のACL(アクセス制御表)を持たせることにより柔軟なプライバシ保護を実現した。また、IPsecのESPを利用することで各通信路での機密性を高め、データが盗聴されてもAgentの特定、追跡を防止できた。IPsecのAHを利用することで各要素の成りすましも防止した。最後には、現状の位置情報システム[3]に付加された機能の性能評価を行い、増加するオーバーヘッドの見積もりを行った。

本システムの問題点は、暗号にかかる処理時間である。従って、より性能の良いシステムを設計するためには暗号処理を軽減するための工夫が必要である。今後はそれについて改良と実装を行い、システム全体の性能を評価する。また、Rule Serverが管理する情報の機密

性を高める仕組みも検討する。さらに、このシステムを効果的に利用できるアプリケーションを検討する。

参考文献

[1] 和泉順子, 竹内奏吾, 渡辺恭人, 植原啓介, 砂原秀樹, 寺岡文男, 村井純 : “位置情報システムにおけるプライバシ管理方法の提案”,DICOMO2000 シンポジウム論文集, pp.667-672, June 2000.

[2] Cuellar, J., Morris, J., Mulligan, D., Peterson, J. and J. Polk, “Geopriv Requirements”, RFC 3693, January 2004.

[3] 渡辺恭人, 竹内奏吾, 栗栖俊治, 寺岡文男, 村井純 : “プライバシ保護を考慮した位置情報システムの実装と評価”, 電子情報通信学会論文誌 B, vol.J86-B, no.8, pp.1434-1444, August 2003.

[4] 上松啓, 吉川正人, 倉島顕尚, 坂田一拓, 市村重博, 小池雄一: “携帯Javaプログラムに向けたユーザ指向のポリシーベースプライバシ保護方式”,DICOMO2003 シンポジウム論文集, pp.553-556, June 2003.

[5] M.Danley, D. Mulligan, J., Morris, J. Peterson, “Threat Analysis of the Geopriv Protocol”, RFC 3694, February 2004.

[6] S. Kent and R. Atkinson., ”IP Encapsulating Security Payload (ESP)”, RFC 2406, November 1998.

[7] Kent, S., and R. Atkinson, ”IP Authentication Header(AH)”, RFC 2402, November 1998.

[8] D. Harkins and D. Carrel, ”The Internet key exchange (IKE),” RFC 2409, November 1998.

[9] 青木隆一, 稲田龍著, ”PKIと電子社会のセキュリティ”, 共立出版, October 2001.

[10] 栗栖俊治 : ”インターネットを利用した移動体の位置情報管理機構の構築”, 慶應義塾大学, 理工学部情報工学科卒業論文, February 2003.

[11] ”AiCryptoライブラリ”, http://mars.elcom.nitech.ac.jp/Research/MM/security/aicrypto.html