Vol.2009-ITS-37 No.6
2009/6/12

プライバシを考慮した匿名認証方式による プローブ情報システムの構築

佐藤雅明[†1] 繁富利恵[†2] 上田憲道[†4]
党聡維[†4] 和泉順子[†3] 植原啓介[†1]
砂原秀樹[†1] 村井純[†1]

プローブ情報システムでは，収集される情報に車両が情報を取得した際の位置と時間が含まれる．情報発信者のプライバシ保護の観点では，情報は車両を識別することが出来ない匿名で，かつ発信される情報に依存関係が無い状態で収集されることが望ましい．しかし，そのような環境では，プローブ情報システムは悪意ある情報発信者による虚偽情報の大量発信を排除できない．また，旅行時間等の連続したデータを必要とするプローブ情報の生成は難しい．

本論文では，プライバシを考慮したプローブ情報システムの構築のための匿名認証方式の提案を行った．本方式を用いることにより，情報収集者は，情報発信者の匿名性を担保した上で，連続したプローブ情報の収集が可能となる．また，提案した方式の動作を検証するために，匿名認証システム，およびプローブ車両シミュレータとプローブ収集センタの設計と実装を行った．

Anonymous Authentication Protocol for Probe Vehicle Information System

MASAAKI SATO,[†1] RIE SHIGETOMI,[†2]
NORIMICHI UEDA,[†4] CONGWEI DANG,[†4]
MICHIKO IZUMI,[†3] KEISUKE UEHARA,[†1]
HIDEKI SUNAHARA[†1] and JUN MURAI[†1]

In the current Probe Vehicle Information system, collected information includes the position and the time when the vehicle obtained the information.

In order to protect the privacy, a vehicle should not be identified by the collected information. For the information collector, it is better to eliminate the possibility of the attacks to the system using the information such as identity thief or fallaciousness by malicious third party. In order to generate high quality service, continuous information such as the travel time on a road is required.

In this paper, we proposed the anonymous authentication system for developing the probe vehicle information system considering the privacy. By utilizing the proposed system, probe information can be collected continuously while keeping the anonymity of the information sender. The proposed system was designed and developed in order to verify the feasibility of the proposed system using probe vehicle simulator.

1. 背　　景

プローブ情報システムは，自動車の保持するセンサデータ (プローブデータ) を，インターネット等の汎用的な情報通信基盤を用いて収集して，統計的な処理等を施すことで，交通情報や気象情報，安全運転支援情報等の価値ある情報（プローブ情報）の生成・提供を実現する高度道路交通システム (ITS:Intelligent Transport Systems) の 1 つである．

プローブ情報システムは世界各国で積極的な研究開発が行われており，Floating Car Data(FCD, XFCD)[1] 等，実用化がなされている事例もある．

日本では，2003 年に名古屋市の中心部を対象として半年間に渡り 1500 台のタクシーをプローブ車両としてセンサデータを収集し，渋滞情報や降雨情報等の情報提供を行うプローブ情報システム[2)3)4)] の大規模実験が行われた．

一方，自動車から収集される情報は情報発信者の挙動や行動を直接的あるいは間接的に示すこともある．個人情報やプライバシ保護の観点から，プローブデータは適切に取り扱われることが求められ，こうした方策についての議論に注目が集まっている[5)]．

2. 目　　的

プローブ情報システムにおいて，情報発信者のプライバシ保護の観点では，プローブデー

†1 慶應義塾大学
Faculty of Keio University
†2 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
†3 奈良先端科学技術大学院大学
Faculty of Nara Institute of Science and Technology
†4 NEC ソフト株式会社第一官庁ソリューション事業部
1st Government Solutions Division,NEC Soft,Ltd.

タの収集は，情報発信者の特定ができないように匿名で，かつ発信情報間の依存関係が無い状態で行われることが望ましい．

一方，情報収集者の観点では，収集される情報の中から，悪意ある第三者による虚偽報告等のシステムへの攻撃を排除できる必要がある．また，旅行時間の計測等には，道路を交差点から交差点までの方向別に区切った切片である道路リンク毎の所要時間が算出できる必要がある．しかし，プローブデータに依存関係が無い状態では，このような一定期間の依存関係を必要とするプローブ情報が生成できない．

そこで本論文では，プローブ情報システムにおける情報発信者のプライバシの保護を実現した上での連続したプローブ情報の収集を目的とし，プローブ情報システムに求められる部分的に連続性を持った匿名による情報収集を可能とする認証方式の提案を行う．なお，本研究における連続性とは，ある情報群について同一の情報発信者から発信されたものであることが担保されている特性を示す．

また，提案する匿名認証システム，およびプローブ車両シミュレータとプローブ収集センタの設計と実装を行い，提案した方式が求められる要件に基づき動作することの検証と，シミュレーション環境における処理時間の測定を行う．

3. プローブ情報システムに求められるプライバシ

自動車の持つデータを集約し統計処理等を施すことで価値ある情報を生成・提供を行うプローブ情報システムは，いかに多くの自動車から利用可能な情報を取得するかが基盤としての価値を高める重要な鍵となる．

本研究が想定するプローブ情報システムのモデルを図 1 に示し，用語を以下に定義する．

情報発信者

プローブ情報の元となるプローブデータを発信する主体であり，本研究では自動車を指す．

情報収集者

プローブデータを収集し，統計等の処理を施す事でプローブ情報を生成する主体であり，本研究ではプローブ情報センタを指す．

認証局

情報収集者に対して，情報発信者の正当性や権利を示す認証情報を発行する機関．

通信基盤

プローブデータの発信と収集に用いられる通信基盤．プローブ情報システムにおいては無線環境が前提となる．本研究では，インターネット等の汎用的な通信基盤を想定している．

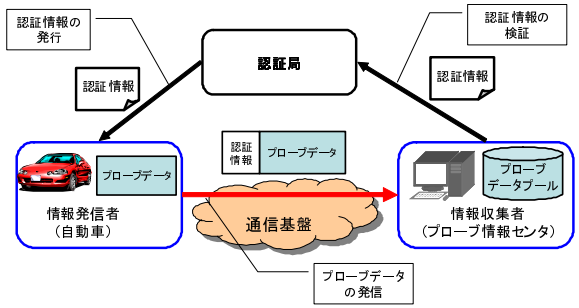

図 1 本研究の想定するプローブ情報システムモデル
Fig. 1 Model of Probe Vehicle Information System

プローブデータ

情報発信者のセンサ等から生成される速度やワイパ作動等のデータ．プローブデータには必ずそのデータを生成した位置と時間が含まれる．

プローブデータプール

情報収集者が保持する，情報発信者から発信されたプローブデータを蓄積する機構．

認証情報

認証局によって発行される情報発信者の正当性や権利を示す情報．プローブデータに添付する形で発信される．

プローブ情報システムでは，情報収集者であるプローブ情報センタが，情報発信者である自動車のセンサ等から自動車の位置と時間を含むプローブデータを収集し，収集されたプローブデータを集約して統計的な処理等を施すことによって，渋滞や降雨情報等の特定の第三者や広く一般に提供するプローブ情報を生成する．

前述のように，プローブデータの収集は匿名であることが望ましいが，収集するプローブデータから悪意ある情報発信者からの攻撃等を排除するためには，情報発信者の正当性や権利を確認する必要がある．特に，自動車の数を偽装して多数の虚偽情報を発信し交通情報の混乱を招くような事態を防ぐことは，プローブ情報システムが社会的基盤となる上で不可欠である．

したがって，プローブ情報システムは，認証局を利用した何らかの認証機構を持つことを

前提とする．

このようなプローブ情報システムにおいて，プライバシに関する課題を以下に挙げる．

認証情報からの情報発信者の特定

プローブ情報システムにおいて，個々の自動車が特定できるような認証情報を用いた場合には，プローブデータと情報発信者の”紐付け”が可能となるため，これは情報発信者にとって脅威となる．

始点・終点や連続したプローブデータからの情報発信者の特定

情報発信者である自動車の走行状態や走行履歴は，搭乗者・所有者の挙動や行動履歴と深く関係がある．セッション毎のランダム ID を用いる等の，個々の自動車が特定されないような手法で認証を行った場合でも，プローブデータは「位置」と「時間」を必ず含んでいるため，移動の始点・終点に関する情報は，位置情報データベース等と関連付けられることで，情報発信者の個人情報やプライバシの漏洩に繋がる可能性がある．また，連続したプローブ情報が描く軌跡から個人の行動履歴を推定される可能性もある．これらは情報発信者にとって脅威となる．

プローブ情報システムを構築する際には，こうした脅威に対処する必要がある．同時に，悪意ある情報発信者による虚偽情報の同時多数発信の検知や，旅行時間の計測等を実現するための，道路リンク毎の所要時間を算出することが可能な範囲での連続したプローブデータの収集が出来る事が求められる．

上記に基づき，プライバシに関する課題を考慮したプローブ情報システムにおけるプローブデータ収集は，以下の 3 つの要件を満たしている必要がある．

(1) 情報発信者を特定することなく，情報発信者の有する権利 (プローブ情報収集主体と正式な契約関係にある等) を確認できること．
(2) 情報発信者が同時に多重の情報を発信している場合に，それを検出できること．
(3) 情報発信者を特定することなく，情報発信者が認める期間内において，情報発信者の同一性を確認できること．また，異なる期間においては同一性を確認できないこと．

4. 匿名認証方式

本章では，プライバシの問題を解決した上で認証を可能とする手段である匿名認証方式について，まず匿名認証方式の分類について述べ，次に本研究の提案手法の基礎となる Refreshable token scheme について述べる．

4.1 匿名認証方式の分類

プライバシ問題の解決手法の一つとして，匿名化がある．これは，情報の発信者を特定できないようにすることで，情報発信者と情報の結合を不可能にする手法である．

個人，あるいは集団が持っている権利を認証する手法としては属性認証がある．これは個人や集団しか持ち得ないパスワード等の知識や，所有物，特徴等を基に認証を行う方式で，属性証明証[6] を用いた認証等，既に実用化されているものも存在する．しかし，属性認証はあくまで所有する権利の有無を確認する手法であり，個人が特定されるか否かについては担保されるものではない．

そこで，個人が特定されないような匿名性を有した上で，権利の確認を行うという要求を満たす手法が，暗号技術を利用した匿名認証方式である．匿名認証方式では，利用者は自らの権利を示すために権利証 (token) を提示する．サービス提供者は，この token を確認することで，利用者の権利を確認することが出来る一方，原則的には権利発行者自身も，利用者の匿名性を解除することは不可能である．また，利用者は必要に応じて匿名性を自身で確認することが可能である．

匿名認証方式は，利用者の有する token の利用形態によって分類できる．表 1 にそれぞれの特徴を示す．

表 1 匿名認証方式の分類
Table 1 Classification of Anonymous Credential

項目	One-show	Multi-show	Refresh token scheme
token の利用形態	一回のみ利用可能	複数回利用可能	利用後に更新が可能
主な利用例	音楽データ・映像データのダウンロードや，アンケート回答等	所属グループ毎のデジタルデータ共有や，チャットルームの入退室管理等	図書館における匿名での本の貸し出し (返却されていない場合に貸し出し停止)
実現手法	ブラインド署名	グループ署名	ブラインド署名とゼロ知識証明

One-show 方式では，匿名の token は一度だけ利用可能であり，利用した token の再利用は不可能である．従って，データそのものに課金する場合や，サービスの回数毎に課金する従量課金等に適している．一方，token の利用毎に token を発行してもらう為の本人確認が必要であるため，連続した利用の際にはコストが高い．

Multi-show 方式では，利用者は自由に何回でも token を活用する事が可能であり，会員向けの広報提供や，グループウエア等での情報共有等に適している．しかし，一度に複数の

token を利用出来るため，同時利用を制限するようなサービスには適さない．

Refreshable token scheme[7)8)9)] は，token の更新 (refresh) が可能な方式である．token の更新は，token の発行者によってのみ可能であり，利用者自身では行うことが出来ない．利用者は他の方式同様 token を利用し，再度必要な際には token を更新することで複数回の利用を実現するが，token の二重使用等の不正が検出された場合には，token の更新を無効化することで，利用者の権利をコントロールすることが可能である．

本研究では，前章のプライバシ要件を満たすために，Refreshable token scheme を基礎としたプローブ情報システムのための匿名認証方式の提案を行う．

4.2 Refreshable token scheme の概要

Refreshable token scheme は，ブラインド署名とゼロ知識証明を応用した匿名認証技術である．Refreshable token scheme の処理の流れを図 2 に示す．

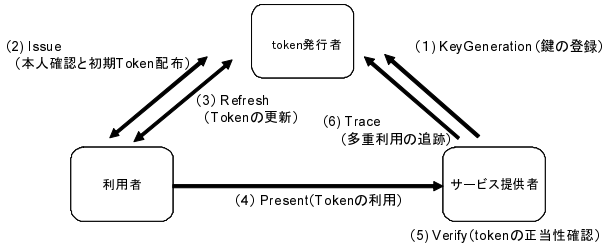

図 2 Refreshable token scheme の処理の流れ
Fig. 2 Overview of Refreshable token scheme

(1) KeyGeneratoin：サービス提供者が用意した公開鍵を token 発行者に登録する．

(2) Issue：利用者は token 発行者に個人情報を示し，token 発行者はそれに基づく本人確認をして利用者 ID を作成する．また，利用者 ID とサービス提供者の公開鍵から初期 token を生成して利用者に送信する．

(3) Refresh：利用者が token を token 発行者に提示する．token 発行者は，提示された token(初回の場合には初期 token) とサービス提供者の公開鍵を元に新しい token を発行する．

(4) Present：利用者がサービス提供者に token を提示し，サービスを利用する (token の利用)．

(5) Verify：サービス提供者は Present で提示された token と，過去に提示された token を比較し，token の正当性 (多重利用されていないか) を確認する．

(6) Trace：サービス提供者が token の多重利用を確認した場合には，token を token 発行者に提示して該当する token の refresh の停止を依頼する．token 発行者は必要に応じて token を辿ることによって (追跡)，利用者を特定することが出来る．

Refreshable token scheme では，利用者は Issue でのみ token 発行者に個人情報を開示すれば良く，それ以降の Refresh 等の処理は全て匿名で行われる．また，サービス提供者は，token の多重利用を防止するためには Present された token を保持している必要がある．

Refreshable token scheme の要求事項を以下に示す．

Anonymity

利用者のサービス提供者に対する匿名性を担保する性質であり，”Untraceability”と”Unlinkability”の二つから成る．”Untraceability”は，token から利用者が一意に識別出来ない事であり，”Unlinkability”は，ある二つの token の利用者が同一人物かどうかが識別出来ない事である．

Double-Use Traceability

サービス提供者が，利用者の token の多重利用を検出可能できる性質であり，サービス提供者が token を提示することで利用者のサービス利用を停止することが出来る．また，token 発行局は，必要に応じて token の更新履歴を辿ることで，多重利用を行った利用者を追跡できる．

なお，Refreshable token scheme では，Traceability は本人確認の信頼性と精度に依存する．本人確認が正しく行われなかった場合には，利用者の特定が出来ない．また，匿名性は複数の利用者 (token 所有者) が前提となっている．利用者が一人であった場合には，匿名性を担保する事は出来ない．

5. プローブ情報システムのための匿名認証方式の提案

本章では，提案するプローブ情報システムのための匿名認証方式について述べる．

第 4 章で述べた Refreshable token scheme をプローブ情報システムに適用した場合には，情報発信者の匿名性を担保した上で，悪意ある情報発信者を検出する事が可能となる．これは第 3 章で挙げた要件の 1 と 2 を満たす．しかし，要件 3 は，Refreshable token scheme の Unlinkability という性質と矛盾する．そこで本論文では，3 つの要件を満たす手法として，Refreshable token scheme を基礎とした部分的に Linkability を保持する事が可能となるような匿名認証方式を提案する．

一般的なプローブ情報システムでは，プローブデータは位置・時間で指し示される地点の情報として生成され，プローブ情報センタに発信される．従って，個々の情報発信時に Refreshable token scheme の Present を行った場合，情報の一つ一つは分断される．しかし，プローブ情報システムの情報収集に際しては，その品質や精度を高めるために，ある一定期間だけ連続性を持った情報を取得したいというケースがある．そのため本論文では，期間毎にプローブデータの群を形成し，群の内部では Linkability を実現し，群と群の間では Unlinkability を実現する方式を提案する．

部分的な linkability を付加した Refreshable token scheme の先行研究[10] のように，専用の公開鍵を交換し，公開鍵暗号方式を用いて実現する方法もある．この場合，情報交換の際には暗号化は必要としない反面，全ての情報発信において公開鍵による暗号化が必要となる．しかし，本研究が想定する環境においては，多数の情報発信者から大量のプローブデータが発信される．そのため，規模性を考慮した場合に，より処理コストが低い手法の方が望ましい．また，情報収集者と情報発信者の間には情報収集に関する合意が事前に確立されている必要性と，プローブデータの盗聴を防ぐという観点から，鍵交換に安全な (暗号化された) 通信路を用いる事を前提とすることが出来る．

したがって，本論文ではプローブ情報システムのための匿名認証方式として，token で present をした際に，一定期間だけ利用可能なセッション鍵として共通鍵を付与し，その鍵に基づくセッションの間だけ Linkability を実現する方式を提案する．本方式に基づく匿名認証処理の概要を図 3 に示す．

車両 A は，ある一定期間，例えば 10 分間毎のプローブデータの連続性を許可しているとする．この場合，最初の 10 分間の間は，token の present によって付与される共通鍵によってプローブ情報センタとの間にセッションを張り，プローブデータの発信を行う (図 3 中の丸印)．これにより，プローブ情報センタには，自動車の特定は出来ないものの，同一の自動車から発信されたプローブデータであることが分かる．(部分的 Linkability の実現)．

その後 10 分が経過すると，自動車は token の更新を行う事で，新たな token を取得し，それ以降はまた 10 分間新たな token に基づくプローブデータの発信を行う．これにより，プローブ情報センタのプローブデータプール内で更新前と更新後の情報は切断され，群間の Unlinkability が実現される．図 3 では，更新がなされた段階で，プローブ情報センタからはそれ以降のプローブデータが車両 A，B，C のいずれか分からず，車両 A がそれ以降どのように走行したのかを把握することは出来ない．また，情報発信を開始したことや停止したことも，同様に把握する事が出来なくなり，自動車の始点と終点も検出不能である．

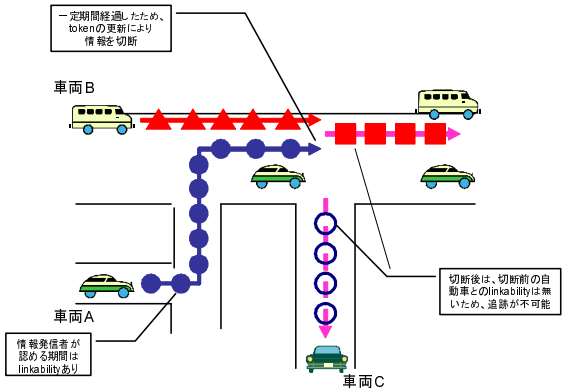

図 3 プローブ情報システムのための匿名認証方式の概念
Fig. 3 Concept of Anonymous Authentication for Probe Vehicle Information System

本システムにおける安全性は，用いる匿名認証の安全性と，採用する共通鍵暗号方式の安全性に依存する．そのため，システムを構築する際には，その時点で最良の方式が採用できるようにする必要がある．そこで，車両，匿名認証サーバ，および収集サーバとの通信には，多様な匿名化処理，暗号化処理技術に対応できるような共通のインターフェイスを作成し，将来的な拡張性を保つことが望ましい．

6. 設　　計

本章では，第 5 章で述べた提案に基づく，プローブ情報システムのための匿名認証方式の設計について述べる．

6.1 匿名認証モデルの設計

部分的に Linkability を保持する事が可能な匿名認証方式を用いた，プローブ情報システムの認証モデルを図 4 に示す．

このモデルは，情報発信者である自動車，情報発信者の個人情報等で本人確認をして token を発行する token 発行者である認証局，及び自動車の情報を収集する情報収集者であるプローブ情報センタから構成される．図 4 における処理の流れを以下に示す．なお，下線が引かれている処理は，Refreshable token scheme と同じ処理であることを示す．

(1) KeyGeneration：プローブ情報センタが用意した公開鍵を認証局に登録する．
(2) Issue：自動車は認証局に個人情報を示し，認証局はそれに基づく本人確認をして利用

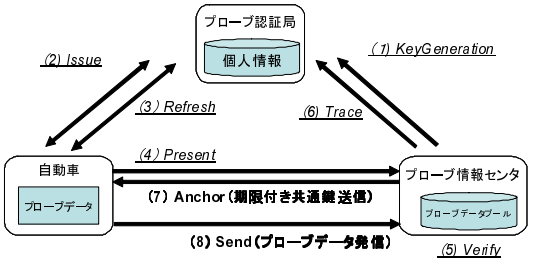

図 4 匿名認証方式によるプローブ情報システムの認証モデル
Fig. 4 Model of Anonymous Authentication for Probe Vehicle Information System

者 ID を作成する．また，利用者 ID とプローブ情報センタの公開鍵から初期 token を生成して自動車に送信する．

(3) Refresh：自動車が token を認証局に提示する．認証局は，提示された token(初回の場合には初期 token) とプローブ情報センタの公開鍵を元に新しい token を発行する．

(4) Present：自動車がプローブデータ発信のためのセッションを開始するために，プローブ情報センタに token を提示する．

(5) Verify：プローブ情報センタは Present で提示された token と，過去に提示された token を比較し，token の正当性 (多重利用されていないか) を確認する．

(6) Trace：プローブ情報センタが token の多重利用を確認した場合には，token を認証局に提示して該当する token の refresh の停止を依頼する．認証局は必要に応じて token を追跡し，利用者 ID から自動車を特定することが出来る．

(7) Anchor：プローブ情報センタは Verify に成功すると，自動車との間にセッションを張るための鍵として，自動車が許容できる期間だけ有効な共通鍵を自動車に送信する．

(8) Send：自動車は，Anchor によって受け取った共通鍵を用いてプローブ情報センタとの間にセッションを確立し，プローブデータを発信する．

このモデルに沿う形で，プローブ情報システム用の匿名認証方式の設計を行った．システムの構成と，システムにおけるプローブデータの収集方法を図 5 に示す．

6.2 車両の機能構成

車両はあらかじめ用意した本人確認用の情報 (ID 情報) を使用し，匿名認証管理サーバに token の発行要求を行う．次に，発行された token を使用し，収集サーバに対しセッション情報の要求を行う．その後，得られたセッション情報を使用してプローブデータを暗号化し

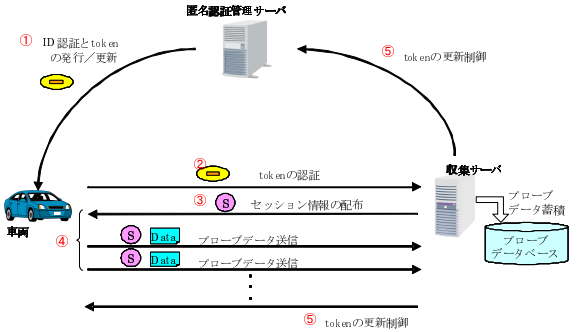

図 5 システムの構成とプローブデータの収集手順
Fig. 5 Acquisition Procedure of Vehicle Information

収集センターに送信する．

セッション情報はある一定期間有効な情報で，有効な間は何度もプローブデータを発信することが可能である．有効期間を経過すると，再度匿名認証管理サーバへ token の更新を実施する．以降この手順を繰り返しプローブデータの送信を行う．車両の各機能と各サーバ間の通信内容を図 6 に示す．

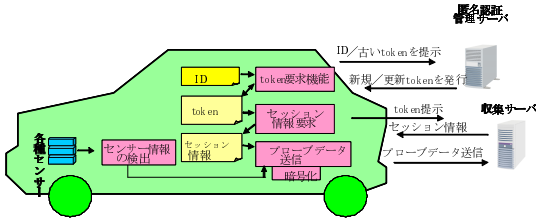

図 6 車両の機能構成
Fig. 6 Functional Composition of Vehicle

6.3 匿名認証管理サーバの機能構成

匿名認証管理サーバは，車両から送信される ID 情報を認証し，本人確認が出来た場合に token を発行する．一度 token を発行した後は，古い token を認証して，token の更新を行う．この際，何らかの不正があった場合等で収集サーバから token の更新不可の通知を受け

ていた際には，token の更新を行わない．

車両と匿名認証管理サーバ間の通信は，セキュリティ上暗号化することが望ましいため，処理技術共有用の共通インターフェースを使用する事で実現する．匿名認証管理サーバの各機能と通信内容を図 7 に示す．

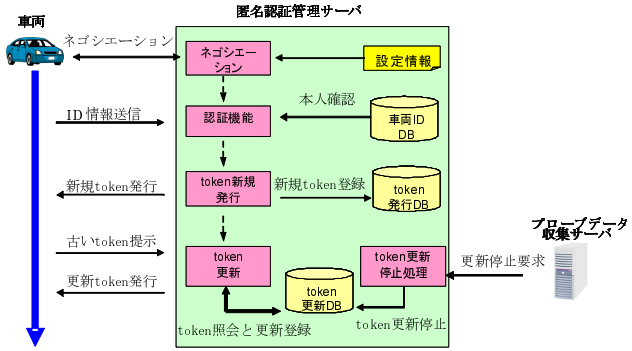

図 7 匿名認証管理サーバの機能構成
Fig. 7 Functional Composition of Anonymous Credential Server

6.4 収集サーバの機能構成

収集サーバは，車両から提示された token を検証し，セッション情報を配布し，プローブデータの収集を行う．token の検証時に，過去に利用された token と照合して多重利用が検出された際には，匿名認証管理サーバへ該当する token を提示し，Refresh の停止を依頼する．そうでない場合には，利用された token を登録する．収集サーバの構成を図 8 に示す．

7. 実　　装

プローブ情報システムのための匿名認証方式の有効性を評価するために，システムの実装を行った．本章では，実装したシステムについて述べる．

7.1 システム構成と実装方式

第 6 章で示した設計に基づいて，評価のためのシステム構成を検討した．

実装に際しては Refreshable token scheme の公開ライブラリである SENSU[11] を使用した．システムの実装方式を表 2 に示す．

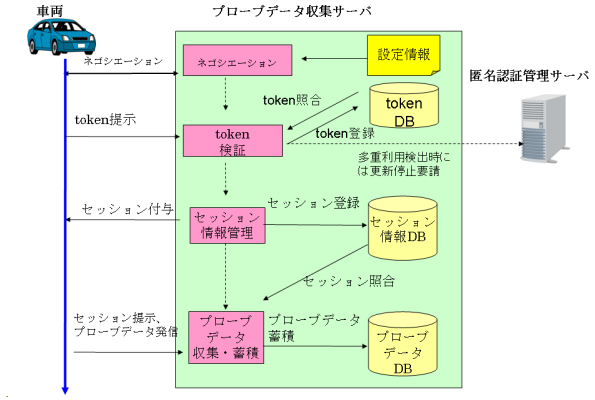

図 8 収集サーバの機能構成
Fig. 8 Functional Composition of Probe InformationServer

表 2 システムの実装方式
Table 2 System Implementation

項目	実装方式
token 発行時の認証方式 (本人確認)	ID/Password 方式
匿名認証方式	Refreshable token scheme(SENSU)
セッション管理方式	セッション ID によるセッション識別，暗号化の共通鍵によるセッション方式
プローブデータの暗号化方式	共通鍵暗号化方式 (AES)
収集するプローブデータ	取得時刻，取得位置 (緯度・経度・高度)，瞬間方位，瞬間速度，瞬間加速度，総走行距離
token 取得・更新時の通信プロトコル	SSL on TCP/IPv6
プローブデータ送信の通信プロトコル	UDP on IPv6

7.2 実装の構成と処理シーケンス

システムの実装時に用いたライブラリ，およびソフトウエアを表 3 に示す．

次に，各要素間の処理シーケンスを図 9 に示す．

処理シーケンスは，以下のような手順で実施される．

(1) 車両シミュレータは起動後，匿名認証管理サーバと収集サーバそれぞれの共通インターフェイスを取得する．共通インターフェイスには，匿名認証方式や暗号化方式などに関するパラメータが含まれている

表 3 使用したソフトウエアライブラリ
Table 3 Software Library List

項目	内容
プローブデータ用データベース	MySQL 5.0
token 用データベース	MySQL 5.0
SSL ライブラリ	OpenSSL FIPS 1.1.2，および YaSSL 0.9.2
AES 暗号化ライブラリ	MIRACLE 5.3.2
匿名認証ライブラリ	SENSU 1.0 Build 831

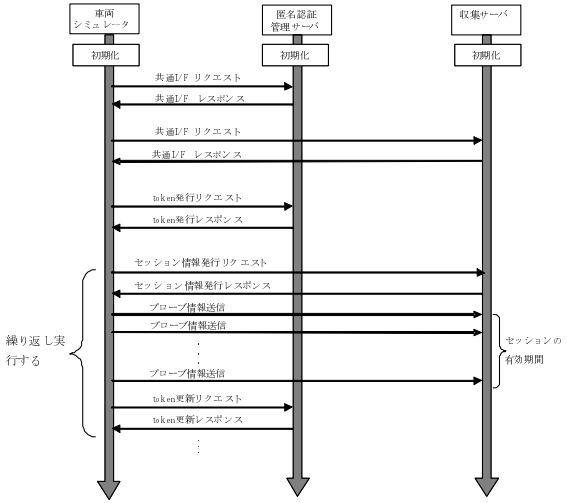

図 9 処理シーケンス
Fig. 9 Sequence of Processes

(2) 車両シミュレータは匿名認証管理サーバに token の発行要求を行い，token を取得する
(3) 車両シミュレータは収集サーバにセッション情報の発行要求を行い，セッション情報を取得する
(4) 車両シミュレータはセッション情報を用いてプローブデータを暗号化し収集サーバに送信する（セッションの有効期限が切れるまで複数回送信）
(5) セッションの有効期限が切れたら，車両シミュレータは匿名認証管理サーバに token の更新要求を行い，token を更新する．

その後，3 以降を繰返し実行することで，継続したプローブデータの発信を行う．

8. 評　　価

本章では，実装されたシステムを用いて行った実験とその評価結果について述べる．

8.1 実 験 環 境

実装されたシステムに基づいて実験を実施し，提案するプローブ情報システムのための匿名認証方式に関する機能及び性能について評価を行い，提案手法の有効性と，動作時のボトルネックの検証を行った．

実験では，匿名認証管理サーバと収集サーバを各 1 台，および車両シミュレータに関しては 500 台分のプローブ車両を動作させた PC を 10 台用意する事で，擬似的に 5000 台規模のプローブ情報システムの環境を構築した．車両からはプローブデータとして時刻，位置 (緯度・経度)，方位，速度，加速度，類型走行距離に関する情報を毎秒発信した．また，各 PC 間は有線 LAN(1000BASE-TX) で接続を行った．

図 10 に実験環境を示す．

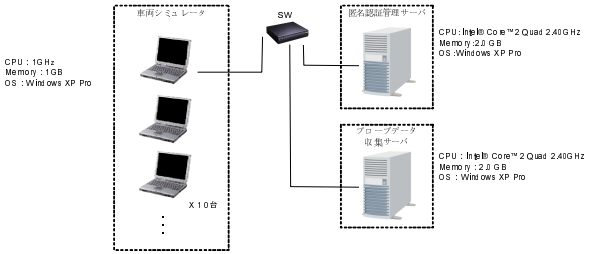

図 10 実験環境
Fig. 10 Experiment Environment

8.2 定性的評価

実装したシステムの機能について，車両シミュレータが動作している状態を監視ツールで確認したものを図 11 に示す．図中左側が個々の車両に着目して ID を表示している状態であり，右側が各車両が描く軌跡を表示している状態である．

定性的評価として確認した機能とその結果を，以下に示す．

共通インターフェイスによる情報の交換

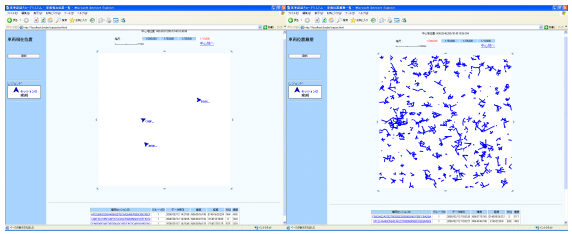

図 11 実験の様子
Fig. 11 Situation of Operation

車両シミュレータ，匿名認証管理サーバ，収集サーバのログを確認し，それぞれが用いている匿名認証技術，暗号化技術に関する情報を交換出来る事が確認された．

token の新規発行

車両シミュレータ，匿名認証管理サーバのログを確認し，各シミュレータの要求に対する有効な token を新規発行出来る事が確認された．

token の更新

車両シミュレータ，匿名認証管理サーバのログを確認し，各シミュレータの要求に対する有効な token の更新が出来る事が確認された．

token の検証

車両シミュレータ，匿名認証管理サーバ，収集サーバのログを確認し，各シミュレータの token を検証出来ることが確認された．

token の照合

車両シミュレータ，匿名認証管理サーバ，収集サーバのログを確認し，使用済み token を present した場合に検出し，token の refresh を停止出来ることが確認された．

プローブデータの生成

車両シミュレータのログを確認し，車両シミュレータが，1) 同一の車両データを継続して算出していること， 2) 設定された間隔でプローブデータを発信していること，を実現している事が確認された．

セッションの作成

車両シミュレータ，収集サーバのログを確認し，token の認証がなされた後にセッションの作成が出来る事が確認された．

プローブデータの送受信

車両シミュレータ，収集サーバのログを確認し，作成されたセッションを用いてプローブデータの送受信が出来る事が確認された．

8.3 定量的評価

実験環境においてプローブデータの収集を行い，匿名認証の各処理に掛かる処理コスト等を計測し評価を行った．なお，評価環境においては，token の署名鍵は 1152 ビット，プローブデータの暗号化に用いた AES の鍵は 192 ビットである．

評価に先立ち計測した，匿名認証管理サーバのベンチマークの結果を表 4 に示す．

表 4 匿名認証管理サーバのベンチマーク
Table 4 Benchmark of Anonymous Credential Server

CPU	GenuineIntel Intel(R) Core(TM)2 Quad CPU Q6600(2.4GHz)
メモリ	2.0GB
整数演算	5285 MIPS(Dhrystone により計測)
浮動小数点演算	2369MIPS(Whetstone により計測)

各処理における処理コストを，車両シミュレータで車両を 1 台分のデータを処理毎に計測したところ，token の新規発行処理と更新処理コストが高く，token の認証およびセッションの作成コストは低い事が確認された．そこで，Linkability と token 更新に掛かる処理コストの関係を検証するため，車両シミュレータ 5000 台の環境において部分的な Linkability を有する期間を 30 秒づつ変更し，各処理の負荷を計測した．測定結果を表 5 に示す．

表 5 匿名認証処理時間
Table 5 Measurement Result of Anonymous Authentication

Linkability を有する期間 (秒)	token 新規発行 (ミリ秒)	token の更新 (ミリ秒)	token の認証 (ミリ秒)
360	321	490	50
330	326	531	60
300	334	999	62
270	360	5454	79
240	408	6180	90
210	443	6548	113

測定では，Linkability を有する期間を 210 秒に設定したところで，CPU 使用率が 9 割を超えて推移し，車両から匿名認証管理サーバへの接続エラーが頻発した．実験環境におけ

る論理的な Linkability 期間の限界は，以下によって 217 秒程度であるから，これが今回の実験環境の限界だと考えられる．

- 1 件の token 更新処理に平均して 171 ミリ秒程度掛かる
- 匿名認証管理サーバは 4 つの core からなるため，処理に際しては M/M/4 待ち行列モデルが適用できる．そのため論理的な限界値は 1 件の token 更新処理の 1/4 である 43 ミリ秒程度
- 1 秒間に処理できる件数の限界は 1000(ミリ秒) / 43 から約 23 件であり，5000 台の更新要求が Linkability 更新期間に均等に分布すると仮定した場合の論理的な更新期間は 217 秒程度

Linkability を有する期間と token の更新処理時間の関係を図 12 に示す．Linkability を有する期間が 300 秒から 270 秒に狭まった際に急激な処理時間の増加が見られる．これは，通信量の増大によるネットワーク品質の低下による再送や，処理の順番待ちによる性能の劣化が原因である．また，今回は車両から毎秒のプローブデータ発信を行うことを想定しているため，token 処理コストが 1 秒未満となる 300 秒は，本実験環境における 1 つの指標であると考えられる．

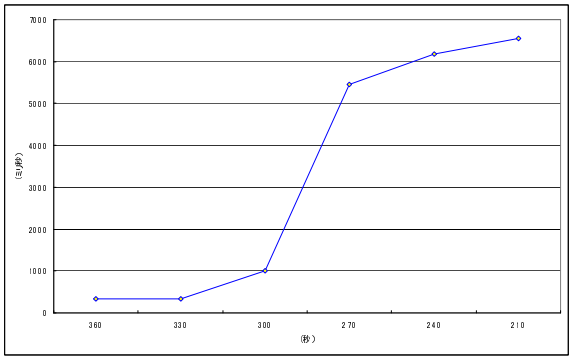

図 12 Linkability を有する期間と token 更新処理時間の関係
Fig. 12 correlation of interval time and refresh time

一方，車両におけるプローブデータ送信時の処理時間は，セッション作成時間が 1.5 ミリ秒，1 回のプローブデータ発信処理時間 (暗号化含む) は 0.4 ミリ秒程度であり，1 秒間隔での情報発信という想定においても，十分に小さい値であった．

8.4 実験結果の考察

提案方式の特徴の 1 つは，車両の始点および終点を隠蔽できる点にある．車両の始点および終点は，車両の走行履歴から個人の行動履歴を推察する手掛かりとなりうるため，この情報が隠蔽できることは，情報発信者のプライバシ保護の観点から優位である．他に始点を隠蔽する方法として，車両が走行を開始してから一定時間の経過，もしくは一定距離を走行するまではプローブデータを発信しない等の方法も考えられるが，この方式では家や職場等の定期的に始点になる部分の周囲だけ情報が集まらないことが逆に個人を特定する可能性があることや，終点の隠蔽が難しいため，本提案方式の方がプライバシの点で有効である．

また，実時間性とのトレードオフで，情報発信者で一定期間プローブデータを蓄積し，一括送信することで Linkability を実現する方式も考えられる．しかし，この方式では情報収集主体は認証情報が付与された軌跡情報を取得することとなるため，本提案方式の方がプライバシの点で有効であると考えられる．さらに，この際の認証情報についても，一時的な ID とグループ証明等では虚偽情報の同時多数発信等の攻撃を防ぐことが出来ない為，本提案方式が優位である．

トヨタ自動車株式会社が行っているプローブ情報システムである「G-BOOK」や日産自動車株式会社が行っている「CAR-WINGS」等における情報収集間隔の最短が 300 秒 (5 分) である．これらは 300 秒間データを蓄積して一括送信しているため，本実験環境においても，こうした商用プローブ情報システムと同程度の Linkability を有しつつ，各プローブデータ群毎の非連続性を担保出来る事が分かった．

想定環境における最短の Linkability を有する期間を 300 秒とした場合の，実道路における影響を考察する．東京近郊の道路リンクのリンク長を財団法人デジタル道路地図協会の基本道路網から算出すると，一般道の平均リンク長は 158m であった．平成 11 年度の道路交通センサスによると人口集中地区の平均旅行速度は時速 20.6km である．したがって 300 秒での移動距離は 1716m 程度となり，これは 11 リンク弱の移動長となり，各道路リンク毎の平均旅行時間の計測が可能であることが分かる．同様に平成 11 年度の道路交通センサスによると，乗用車の一日の平均走行距離は 35.3km, 関東圏の平均旅行回数は 2.8 回であることから，1 回の移動はおよそ 13km 程度である．したがって，Linkability を有する期間を 300 秒とした場合には，1 回の移動がおよそ 7 つ程度に分割される事となる．

情報発信者の安心は，総移動距離・時間，および状況によって異なるが，始点・終点の隠蔽と移動の分断によって，本提案方式によって，交通情報を生成するために必要なプローブデータの収集を実現した上で，情報発信者のプライバシを考慮したプローブ情報システムの

構築が可能であると考えられる．

9. ま と め

本論文では，まず初めにプローブ情報システムに求められるプライバシについての考察を行い，情報発信者のプライバシを保護した上で，質の高い交通情報生成のための連続したプローブデータの取得を実現する部分的な Linkability を保持する事が可能な匿名認証方式を提案した．この匿名認証方式では，Refreshable token scheme による token 認証後に，情報発信者と情報収集者の間で一定期間情報セッションを保持する事で，発信された情報の Linkability を実現する．

その後，提案の有効性を評価するために，各機能の設計と実装を行い，プローブ車両シミュレータを用いて 5000 台規模の環境において実験を行い，定性的評価と定量的評価を行った．

その結果，実装したシステムによって，提案する匿名認証方式によって情報発信者のプライバシを保護した上で，部分的に Linkability を有するプローブデータの収集をする事が可能である事が分かった．

一方，実験結果から，token の更新がシステム全体のボトルネックであることが分かった．今後の課題としては，以下が挙げられる．

token 更新処理の高速化と最適化

token の更新に用いる暗号化アルゴリズムの見直しや，複数 token の同時更新等を実現する事で，token 更新のための処理コストを下げ，システム全体の高速化を図る事が考えられる．しかし，暗号強度と処理コストは比例関係にあるため，プローブ情報システムにおけるプライバシ保護の基準を検討し，情報発信者の状況や周辺環境等に応じて，安心を得られるのに必要な更新頻度を選択できるようにする必要がある．

匿名認証管理サーバの分散化

処理の高速化には限界があり，また，実環境では各処理においてネットワークによる遅延が発生する．そこで，匿名認証管理サーバの分散化を実現し，token の認証，および更新については，複数台の匿名認証管理サーバの中から，負荷が低くネットワーク的に近いものを利用できる環境が望ましい．しかし，その場合には，二重使用等の不正を防ぐために複数あるサーバ間で使用された token 情報の共有が不可欠であり，この共有に掛かるコストも考慮した分散化を実現する必要がある．

謝辞

本研究は，経済産業省事業として行われた結果を取りまとめたものである．

本研究を進めるにあたって，多大なご指導とご助言を頂いた研究委員会の皆様，およびシステム開発ワーキンググループのメンバーの皆様に感謝致します．また，日頃の議論や研究活動に協力して下さった慶應義塾大学の関係者の皆様，および WIDE プロジェクトの皆様に感謝致します．

参 考 文 献

1) Huber W., Ladke M., R. Ogger, ”Extended floating car data for acquisition of traffic information”, Proc of the 6th World Congress on ITS, Toronto, Canada. 1999.
2) K.Uehara, H.Sunahara, J.Murai, ”Problems and Tentative Solutions in InternetCAR Testing with IPv6”, Proc. of SAINT2003 IPv6 Workshop, Jan 2003.
3) T.Ernst, K.Uehara, K.Mitsuya, ”Network Mobility from the InternetCAR Perspective””, Proc. of AINA2003, Mar 2003
4) U. Keisuke, S. Hideki, M. Jun, ”The InternetCAR network architecture: Connect vehicles to the internet using IPv6” ITST2005, June2005, pp. 187-190
5) Masaaki Sato, Michiko Izumi, Hideki Sunahara, Keisuke Uehara, Jun Murai, ”Threat analysis and protection methods of personal information in vehicle probing system”, The Third International Conference on Wireless and Mobile Communications(ICWMC), March 2007.
6) S. Farrell, R. Housley, ”An Internet Attribute Certificate Profile for Authorization”, RFC 3281, April 2002.
7) Rie SHIGETOMI, Akira OTSUKA, Takahide OGAWA, Hideki IMAI, ”Anonymous Refreshability of Tokens”, 第 25 回情報理論とその応用シンポジウム予稿集, 第 1 分冊,p.43-46, 情報理論とその応用学会，Dec 2002.
8) Rie SHIGETOMI, Haruhiro YOSHIMOTO, Hideki IMAI, ”A System of Anonymous Tokens for Two Dimensional Pattern”, Joho Shori Gakkai Shinpojiumu Ronbunshu VOL.2004, NO.11(CD-ROM), PAGE.10B-2, 2004.
9) Rie SHIGETOMI, Akira OTSUKA, Jun FURUKAWA, Keith MARTIN, Hideki IMAI, ”A Provably Secure Refreshable Partially Anonymous Token and Its Applications”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 2006 E89-A(5), 1396-1406, 2006.
10) 繁富利恵, 大塚玲, KeithMartin, 今井秀樹, ”部分的な linkability を付加した Refreshable Tokens ”, 信学技報, Vol.104, No. 200，pp.165-172, 2004.
11) Sensu Project Home PAGE(2008/03/31 現在), http://aatoken.aitea.net/