WIDE Technical-Report in 2006

プローブ情報サービスにおける個人情報保護の標準化について

wide-tr-icar-probeprivacy-00.pdf

WIDE Project : http://www.wide.ad.jp/

If you have any comments on this document, please contact to ad@wide.ad.jp

Title: プローブ情報サービスにおける個人情報保護の標準化について
Author(s): Yasuhito Watanabe (riho-m@cuc.ac.jp)
Date: 2006/01/24

１．概要

プローブ情報システムは、車をプローブ(Probe: 触角、探索針) と見なし、車固有の様々なセンサーデータを車外に発信させ、リアルタイム・オンサイトの情報として収集し、車や社会全体に提供するシステムである。プローブ情報システムは、車両からセンサーデータを収集するが、どのようなセンサーデータを収集するにも位置情報、時刻情報、通信におけるアドレスなどの情報がともに収集される。収集する対象が一般個人の車両であった場合、個人情報が正しく保護されていなければ、車の情報、センサーデータを提供しようとは感じられないであろう。一般個人が安心してセンサーデータを提供できることで、より多くのセンサーデータからプローブ情報を生成することができる。したがって、プローブ情報サービスを運営する事業者が技術的にも運用上でもセンサーデータを提供する個人情報の保護が必要である。

これまでプローブ情報システムにおける個人情報保護について、一般個人を対象としたプローブ情報の収集における個人情報保護に関して、プローブ情報サービス事業者が遵守すべき基本的なルールとしてガイドラインおよび基本原則の検討を行い、ISO への国際標準化提案の活動を行っている。

プローブ情報システムは、ITS 分野でのアプリケーションの一つであり、InternetCAR WG のアプリケーションとしても関係が大きい。また、今後のアプリケーションにとって個人情報保護は重要な課題である。本稿では、これまでの検討状況と国際標準化活動について述べる。

2．コンセプト

プローブ情報システムでは、プローブ情報の発信者の認証を行うことで予め認められた発信者からのみプローブ情報を受け付ける。認証により、情報の正当性や、システムの対攻撃性を高め、情報精度の向上やプローブ情報の価値を高めることができる。

プローブ情報システムの個人情報保護の検討では、発信者の認証を行うプローブ情報システム構築の際に、データソース本人の個人情報を保護するために必要な基本原則について記述し、この標準化を行う。基本原則に準拠したプローブ情報システムには、データ提供者（本人）は安心して情報を送信することができる。

3. これまでの検討（2002 年～2004 年）と位置付け

これまでの検討と位置付けを図に示す。本検討にあたっては、まず国内法制度である個人情報保護法や各省庁ガイドライン、また海外法制度としては、EU 指令・OECD ガイド

ライン等の欧米各国個人情報保護法を参照し、プローブ情報サービスにおける個人情報保護ガイドライン作成準備のための調査を行った。

また、プローブ情報のサービスを一般化して記述するため、プローブ情報サービスの明確化、システムの構成、情報の流れを整理し、プローブ情報サービスにおける脅威分析を行った。

以上の検討から、プローブ情報サービスにおける個人情報保護ガイドライン（案）の検討を行った。本ガイドラインでは、プローブ情報サービスにおける個人情報について議論を行いその規定を行った。またプローブ情報サービスにおける個人情報保護の考え方として、運用面での対応と、技術的対策に分けて検討を行った。

本ガイドラインの検討と並行して、国内での関連団体等への照会と意見収集を行い、フィードバックを得たまた、個人情報保護の仕組みを組み込んだプローブ情報システムの開発、評価を行った。具体的には、SNMPv3 を利用したシステムを構築し、フィールドでの評価を行った。

国際標準化提案準備の実施としては、各国の状況を踏まえたプローブ情報サービスにおける個人情報保護の基本原則作成の検討を行い、ISO において標準化活動を開始した。

4．コンセプトと策定内容

プローブ情報システムのコンセプトと策定内容について、図１に示す。

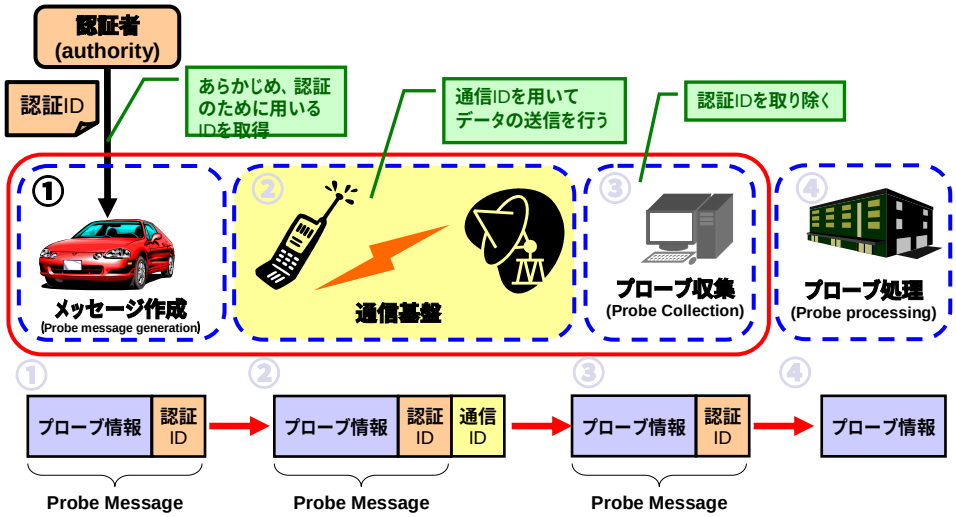

図１： コンセプトと策定内容

プローブ情報システムは、①車両でプローブメッセージを作成する機能（Probe message generation）と②プローブ情報を収集する機能（Probe Collection）と③プローブ情報を処理する機能（Probe processing)、①と③は、②通信基盤で接続されデータの送信が行われ

る。

あらかじめ認められた車両のみからプローブ情報を収集するため、①の機能を持つ車両は③に認証される必要がある。このため①から発信されるプローブメッセージは、プローブ情報に認証のための情報（認証 ID）が付加される。②の通信基盤においては、通信 ID を用いてデータの送信を行うため、プローブメッセージに通信 ID が付加される。③においては、通信 ID は取り除かれ、認証後認証 ID も取り除かれ、その後④に送られる。

プローブ情報システムで、本標準で対象とする部分は、個人を特定する情報が取り扱われる①～③までの機能となり、この部分に関して個人情報保護に関する基本原則の策定を行っている。検討事項としては、①、②、③における認証 ID の取り扱い（認証以外には用いない、通信 ID と結び付けない等）、②における通信 ID の取り扱い方法がある。

5.ISO TC204/WG16/SWG16.3 における活動経緯

ISO では、TC204 WG16 SWG16.3 において、Basic principles for personal data protection in probe vehicle information services として検討を進めている。本 SWG は、プローブ情報システムにおけるデータフォーマットの標準化を行っており、日本側からの提案を契機とした議論により内容的に接近した本 SWG で取り扱うこととなった。

6. ISO CD 22837 との関連

本標準のスコープとなる部分
（ISO CD22837内のRAより）

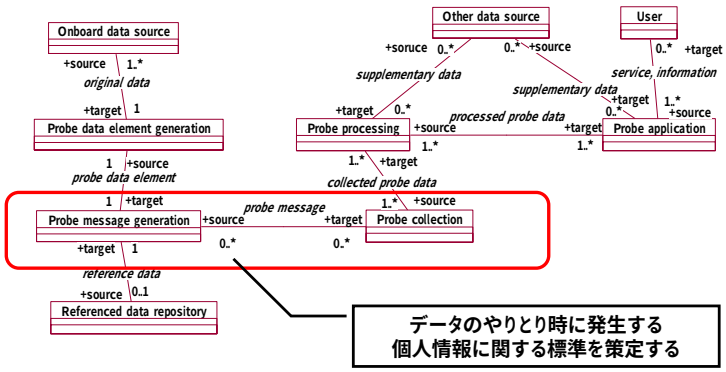

図２： 本標準のスコープとなる部分

ISO CD 22837(Vehicle Probe Data for Wide Area Communications)では、各車両の持つ情報を収集し、交通情報などの生成を行うシステム(プローブシステム)におけるデータフレームワークと、車両の持つ情報のデータの構成およびフォーマット(車両データ辞書)に関する標準化を行っている。この標準では、個人情報保護についての規定は、プローブメッセージには個人を特定する情報は含まないとしているため、通信等を考慮した個人情報保護について検討することとなった。基本的にはこの標準を参照しながら検討することとなっており、ISO CD 22837 のリファレンスアーキテクチャにおける個人情報保護の対象は、通

信基盤を含んだ収集に関する機能の部分である。その部分を図２に示す。

7．本標準のスコープ

①　本標準のスコープについて、図３に示す。プローブデータの収集時に発生する個人情報の取り扱いを含むプローブ情報システムのリファレンスアーキテクチャの規定。規定に際しては、本標準の前提となる CD22837 のリファレンスアーキテクチャを拡張する形で作業を行う。

②　プローブ情報システムの構築、運用時の物理的構成と、取り扱われるデータについてモデル化したプローブ情報システムのフィジカルリファレンスモデルの規定。実構築時に取り扱われる情報、およびその流れ（データフロー）を明確化することで、対象となる個人情報、および遵守すべき基本原則を導出する。

③　コンテキストモデルで取り扱われる個人情報の定義。定義に際して、OECD が定める個人情報保護のガイドライン(1980 年)を参照する。

④　プローブデータ発信者の個人情報を保護するため、プローブデータの収集時における個人情報の適正な取り扱いに関して遵守すべき基本原則の規定。本標準における基本原則は、OECD 個人情報保護のガイドラインの中で規定している 8 原則のフレームワークに準拠する形で規定する。

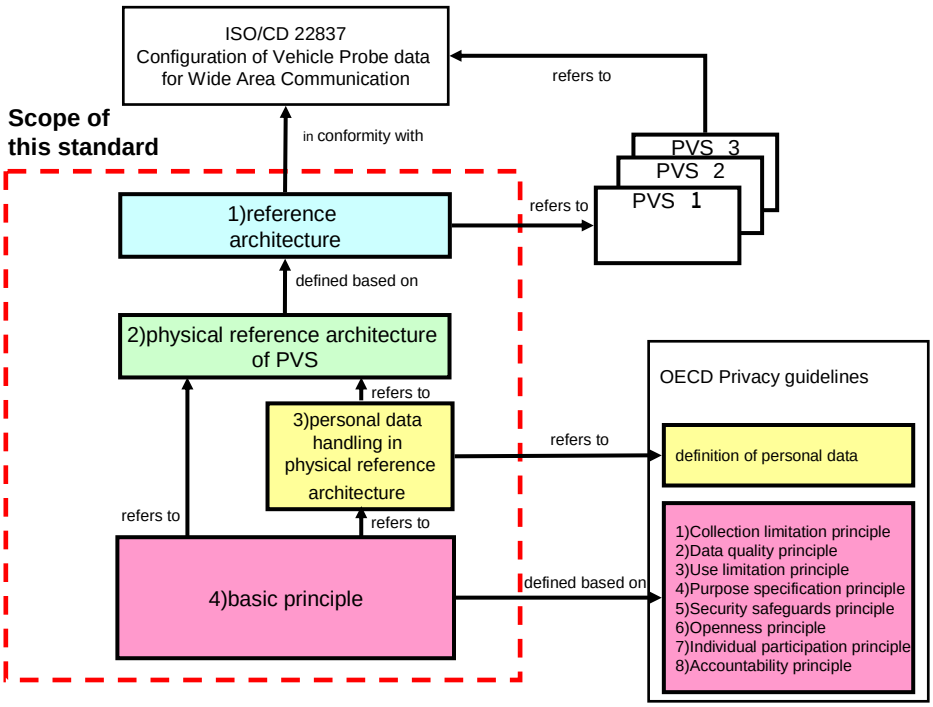

図３：　本標準のスコープ

8．個人情報の考え方

個人情報は、OECD8 原則、および我が国の個人情報保護法の第 2 条を踏襲し、直接的に個人を識別できないものであっても、間接的に個人を識別できるのであれば保護の対象とする。

したがって、CD22837 で定義されているプローブ情報システムにおいて、暗号化、認証機能等を用いてプローブデータの収集を行う際に取り扱われる情報のうちで、個人に関する情報であって、特定の個人を識別できるもの。また他の情報と容易に照合することができ、それにより特定の個人を識別できるものも含む。

9．プローブメッセージとコアデータの組み合わせによる課題

CD22837 におけるプローブメッセージは､送信時に位置と時間と組み合わせて送信する。私有地等の特定の状況においてはプローブデータの収集時に個人情報を収集主体が持ちうる可能性もある。この課題についての議論を深め、取り扱い方法を検討する。

10．活動現状と今後の作業

2004 年度までは、WG で標準化する項目を議論、検討し、PWI(Preliminary Work Item)（予備段階）を提出することができた。2005 年度は、WG で標準化の適用範囲などについて議論と検討を進め、NP (New work item Proposal)（提案段階）提案し、投票が承認された。現在、作成したディスカッションペーパに基づく議論を行い、合意された部分からワーキングドラフト(WD)の素案として整理する作業を並行して行っている。