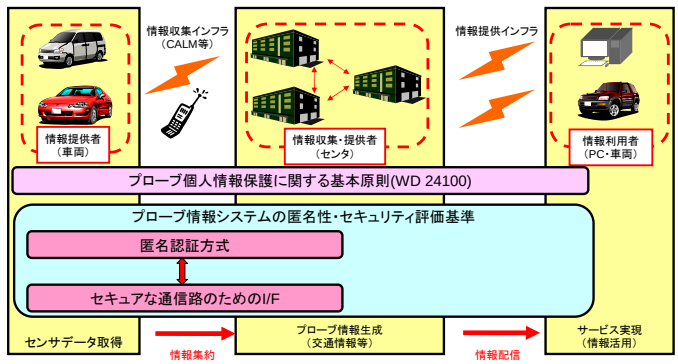
情報セキュリティ研究センター
Research Center for Information Security
慶應義塾大学
奈良先端技術大学院大学
NECソフトウェア　との共同研究
繁富 利恵　Rie Shigetomi

# 匿名認証方式を用いた セキュアなプローブシステムの検討

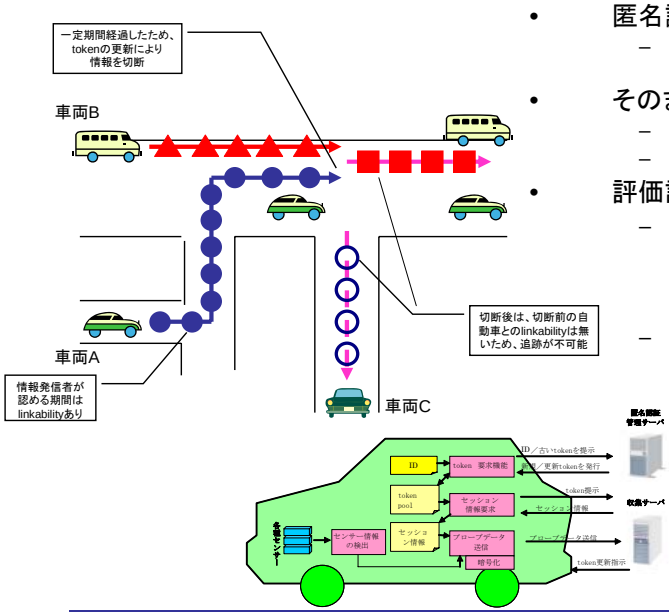
## プローブ情報システム

- プローブ情報システムとは？
  - 車からの情報（スピード、ワイパー利用状況 など）を収集して、二次情報へ利用
  - 各国で盛んに開発・展開
  - 共通のフレームワークは存在していない
  - データ提供者は不特定多数
  - 普及展開にはシステムの技術的な構築性と共に、ユーザが安心して情報を提供できる環境が必要
- “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（ISO/TC204/WG16 WD24100）”
  - プローブにおける個人情報の取り扱いの指針
  - より具体的な共通ルールや、システム構築の際のリファレンスが求められている
- Probe vehicle systems
  - should be secure（安全に対する措置を講じるべきである）
  - should protect personal data /privacy（個人情報・プライバシを保護するべきである）




プライバシを保ちつつ情報収集できる仕組みを！

## 提案手法




- 匿名認証（SENSU方式）
  - サービス提供者が権利を渡した人のうち，どの人が要求してきたのかわからない
    - つまり，サービスを受けている人が一人だったばあいは，匿名ということはできない
- そのまま利用すると、全ての情報が分断される
  - 場合によってはリンク（Linkability）が必要なときも
  - サービス提供者・ユーザが選択できるように
- 評価計画
  - 方針

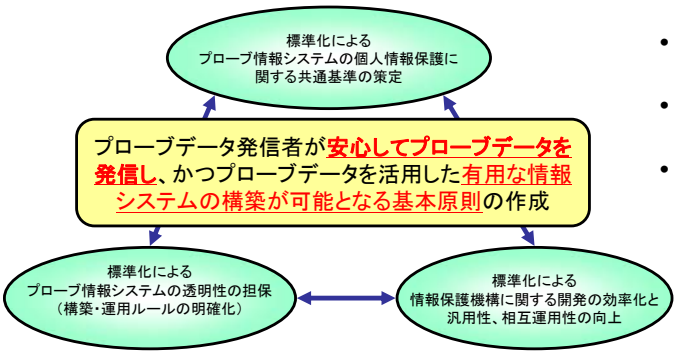
    匿名認証を利用したプローブ情報の収集において、実験システムを用いて実験を行い、機能及び性能について評価を行い、匿名認証を用いたプローブ情報システムの有効性やボトルネックを検証する。
  - 方法

    LAN環境で接続された机上環境で擬似的に車両を5000台発生させ、一連のプローブデータの収集を実施する。

    実験結果

    権利証の認証および更新において、更新が270秒ごとが適切であるとわかった

## 最終ゴール




- 車両から収集するプローブ情報には、（直接的/間接的な）個人情報が含まれている。
- プローブ情報の収集にあたって、個人情報保護のための対応を運用上・技術上で行う必要がある。
- プローブ情報システムの研究・開発は世界各国で行われており、早急的に国際的な基準の統一を図る必要がある。

プローブ情報システムにおける個人情報保護の基本原則を検討し、国際規格提案を行う