

瀬崎研究室

[都市空間センシングとモビリティ解析]

空間情報科学研究センター
Center for Spatial Information Science
http://www.mcl.iis.u-tokyo.ac.jp

情報通信学

新領域創成科学研究科社会文化環境学専攻
情報理工学系研究科電子情報学専攻

世田谷センシングプロジェクト

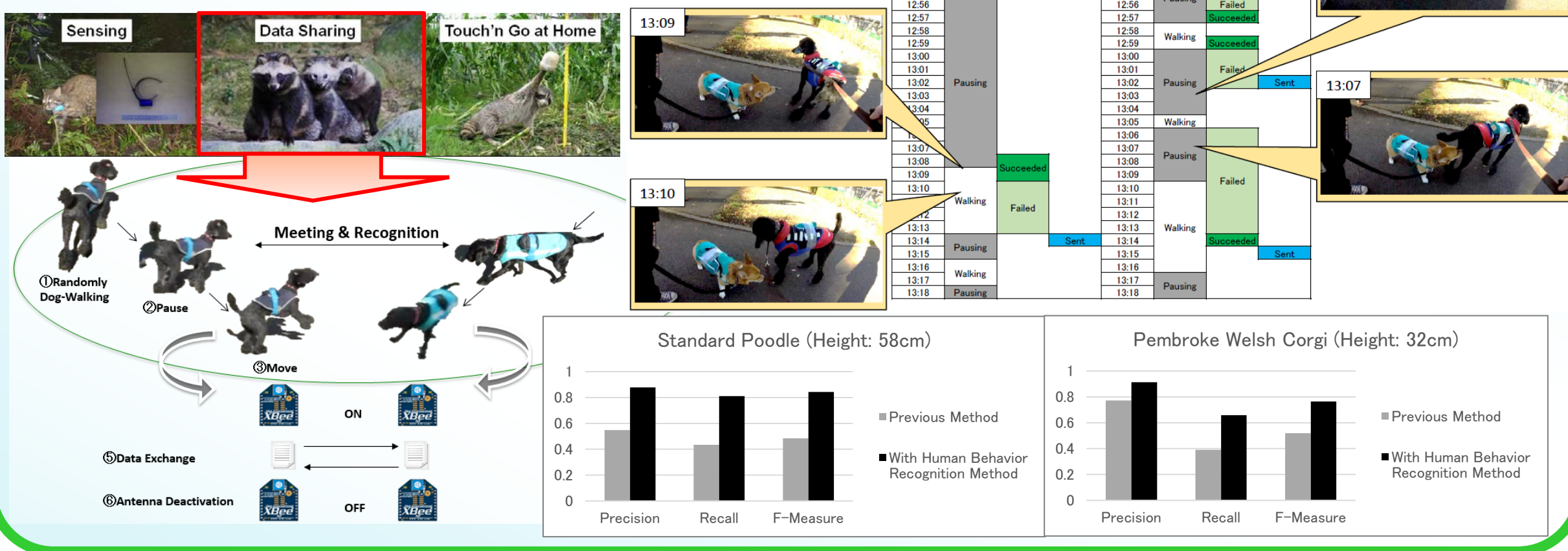
- 概要
- Androidアプリケーションを用いた足跡に沿ったセンシング(Trajectory sensing)
 - 調査区域：東京都世田谷区 (総面積 60 [km2])
 - 調査参加者：40 人
 - 調査期間：4日間 (約 170 時間)

新しい都市環境(住生活環境)の調査方法



生態相互作用を用いた効率的な動物間通信

- 安全かつ効率的な環境・生態調査の実現のため、野生動物に負担の少ないウェアラブルデバイスを用いた動物間のデータ交換を研究
- 動物の習性に着目し、省電力の動物間通信機構を開発
- ヒトの行動認識手法の導入によりシステムの精度が向上



無線ネットワークにおける情報理論的セキュリティ

既存の安全な伝送方式:

暗号化

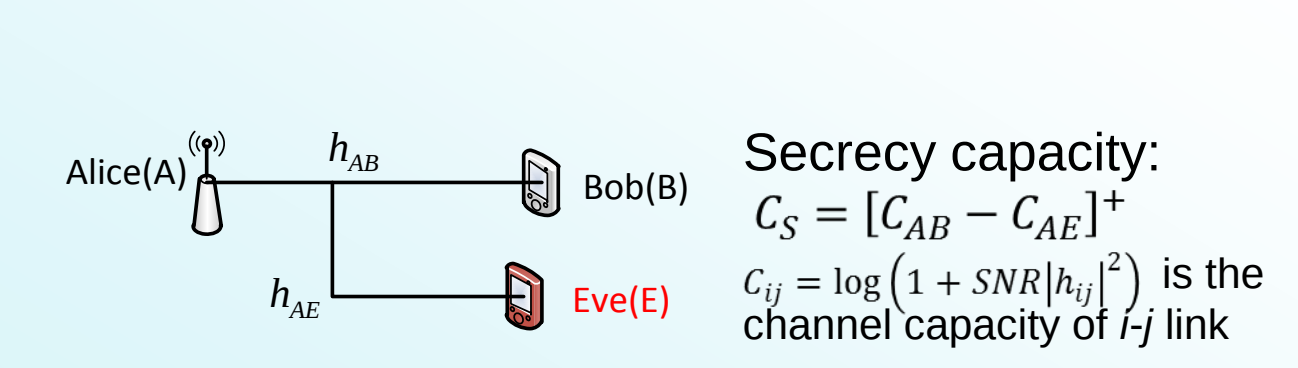
-計算困難性の仮定

-分散型または動的な無線ネットワークのための暗号化キーの管理は難しい

情報理論的セキュリティ

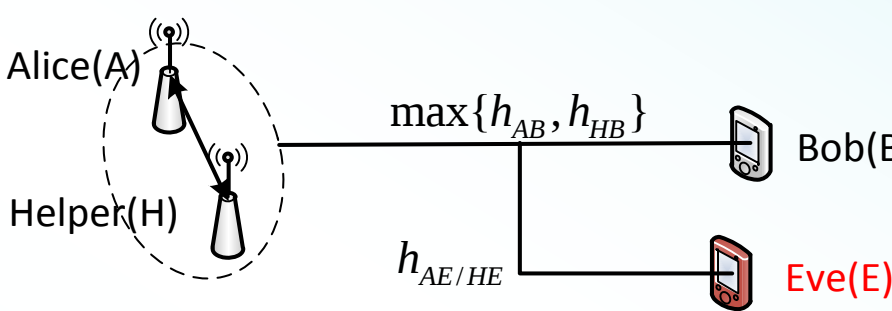
基本理念: 無線チャンネルの減衰を利用し、データ通信の安全性を高める。

-チャンネル減衰 h_{AB} と h_{AE} を独立且つ反転性と想定する



秘密容量は、完全にセキュアな状態に達するための最大データ伝送速度を示す。

目的: 秘密容量の向上
方法: 協調的なセキュリティ



参加型センシングのプライバシー保護

本提案手法では、参加型センシングで取得したデータをユーザの持つ端末側でプライバシー保護処理を行い、サーバ上で統計的なデータとして再構築を行う。本手法により、一般ユーザは第三者機関に頼ることなく参加型センシングに貢献することが可能となる。



モバイル端末データによる長期モビリティマイニング

目的

通信インフラ側に記録される携帯電話の通信履歴(CDR)により、自動的に居住地の移動を行ったユーザを検出

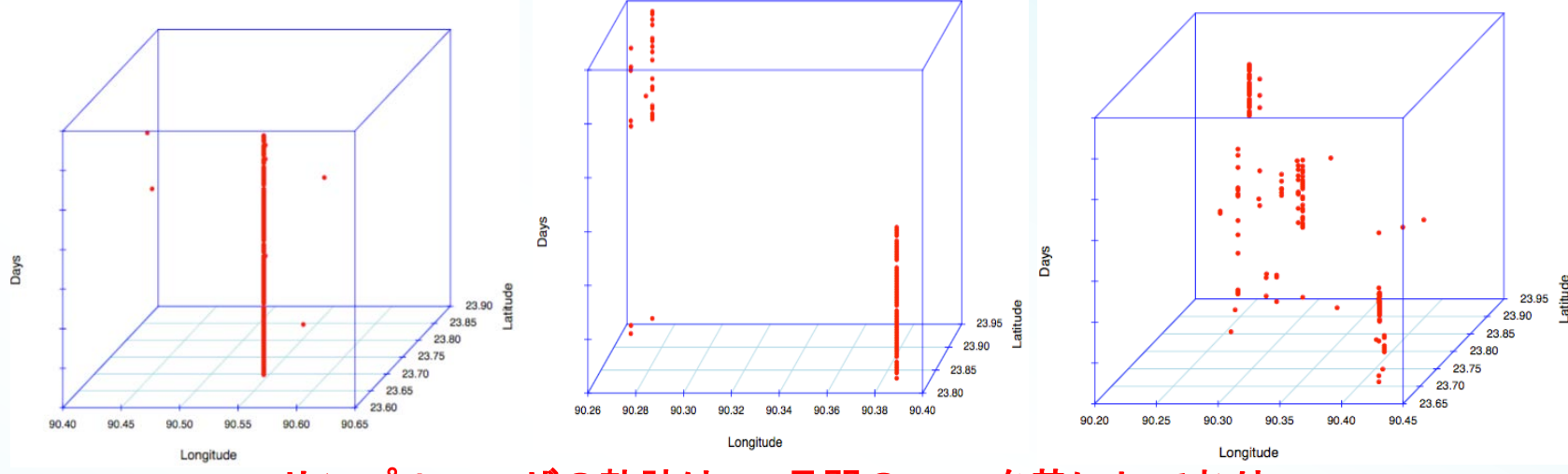
重要性

都市計画やビジネスインテリジェンスに役立つ人口移動の推測

手法

時空間シーケンシャルクラスタリング

大規模CDRデータによる解析結果



サンプルユーザの軌跡は4ヶ月間のCDRを基にしており、各図では以下のモビリティパターンを持つデータを使用している。
左図：居住地移動なし、中図：居住地移動あり、右図：移動の規則性なし

Performance Indicators averaged over ϵ parameter

Category	Detection rate(%)	False Positive rate(%)
Case 1	70.8	19
Case 2	67.9	14.2
Case 3	71.7	14.6

モバイル端末が創出する

パーソナルデータ利活用に関する意識調査

- 社会学的調査(「モバイル端末とプライバシー」を主題として半構造化インタビュー)
- 調査対象者: 31名 (総インタビュー時間: 約40時間)
- 調査場所: 都内

KJ法を用いた調査結果

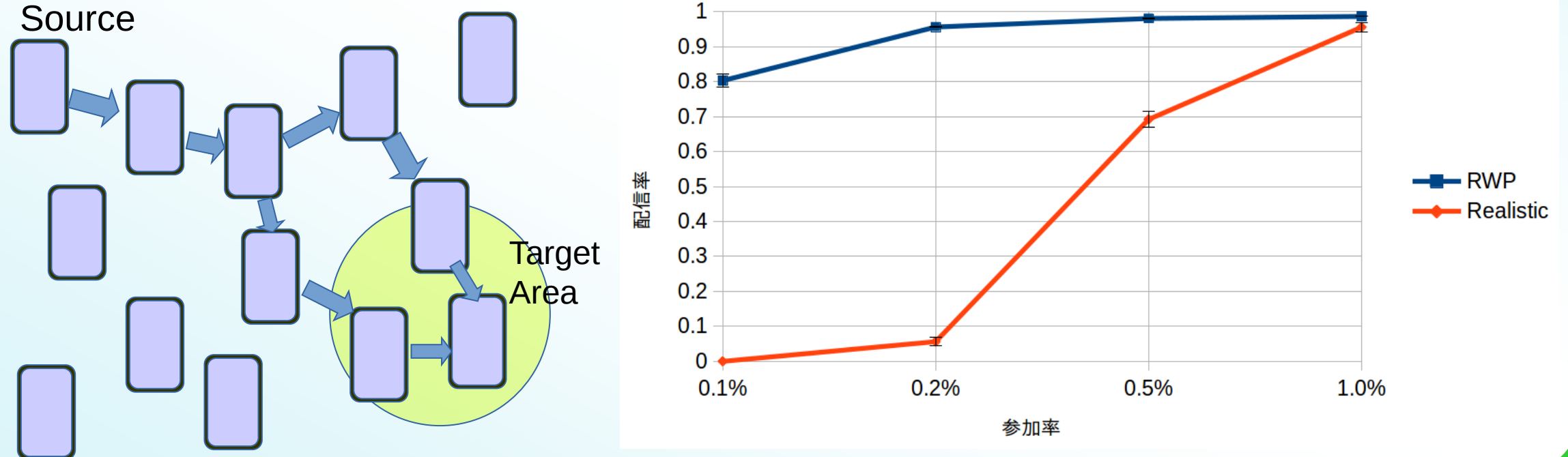
- プライバシーに関する感覚を4分類化
- 原則型グループ(プライバシー原理主義)
- 選択型グループ(実用主義)
- 開放型グループ(無関心)
- 締めグループ(本当は嫌だが仕方なくプライバシーの侵害を認める)

※「原則型グループ」「選択型グループ」「開放型グループ」の3分類はA.Westinによる



モバイルアドホックネットワーク上でのジオキャスト

- 地震等で通信インフラが利用できない場合などに、スマートフォン等との通信で必要な場所に必要情報を伝達
- シミュレーションにより具体的な災害時移動予測データを用いるとRWPなどの人工的な移動モデルの場合よりパフォーマンスが大きく落ちることが分かった。またその場合でも全体の1%が参加すれば十分な配信率が得られた。



人口密度分布の時変動を考慮した位置プライバシーに関する研究

概要

- 人口密度分布を事前情報として攻撃者の位置推定のための知識として取り入れ、既存のプライバシー保護手法への影響を検証

アプローチ

- 確率的にプライバシー保護レベルを評価するフレームワークを利用
- 人口密度分布から得られる事前確率分布を攻撃者の位置推定確率分布へ反映

評価

- ユーザの位置をより高い確率で推定できるほど、プライバシー保護レベルが低くなる評価指標を利用
- プライバシー保護レベルの低下、すなわち、攻撃者の位置推定性能向上を確認

※プライバシー保護レベル: 攻撃者の位置推定誤差の期待値

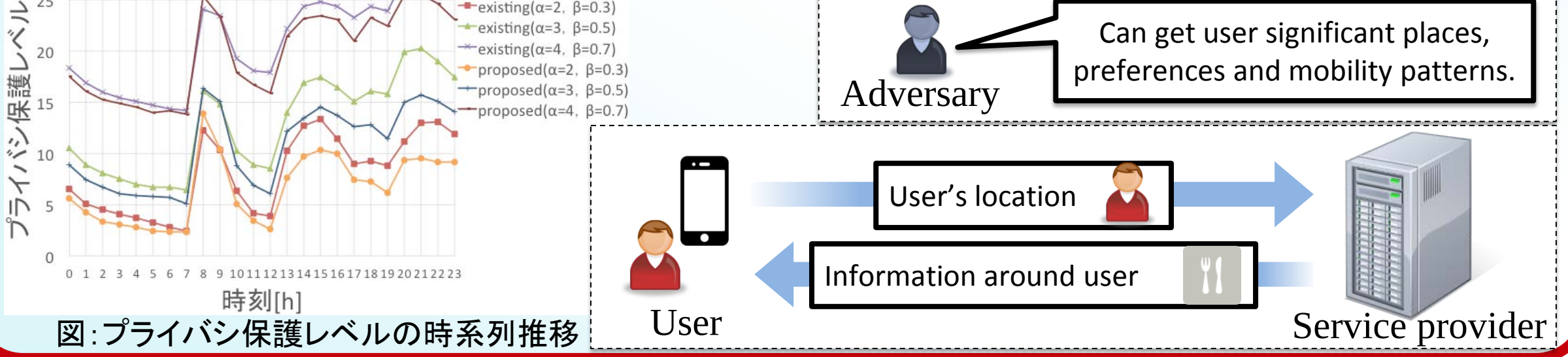


図: プライバシー保護レベルの時系列推移