資料１－８

映像センサー使用大規模実証実験に関する
プライバシポリシー策定について

1. プライバシ保護の考え方に関する文書の構成について

本実験を遂行するにあたり、プライバシ保護に関する考え方を定めるために以下の 2 種類の文書を策定する。

(1) プライバシポリシー

(2) プライバシポリシーを守るための実施要項、セキュリティ対策、運用に関する規程

これらの文書は、以下の法令、規程等との関係を整理した上で記述する。

- 独立行政法人等の保有する個人情報の保護に関する法律
- 独立行政法人等の保有する個人情報の保護に関する法律施行令
- 独立行政法人情報通信研究機構個人情報管理規程
- 独立行政法人情報通信研究機構個人情報開示等取扱規程
- 独立行政法人情報通信研究機構の保有する個人情報の開示請求に対する開示決定等に係る審査基準
- 独立行政法人情報通信研究機構情報セキュリティ管理規定
- 独立行政法人情報通信研究機構のセキュリティに関する宣言
- 独立行政法人情報通信研究機構生体情報研究倫理委員会規程
- 独立行政法人情報通信研究機構組換えＤＮＡ実験安全委員会規程

2. プライバシポリシーの骨子（案）

- 本実験で収集した情報は、実験の目的以外には利用しない。
- 実験参加者は、本実験における個人情報保護、プライバシ保護に関する方策に同意した人に限定する。
- 個人を特定できる情報、および他の情報と照合して個人の行動が追跡できる情報については、実験の目的に照らしてその情報にアクセスする必要がある最低限の人、およびプログラムからアクセスに限定する。
- 提供される人流統計情報については、提供先において管理規程を定める。
- プライバシポリシーが遵守されていることを監査できるようにする方策を講じる
- プライバシ保護機構の設計に当たっては、リスク分析、プライバシ影響評価を行い、分析・評価の結果示されたリスクを十分に軽減する。

3. 規程等における主な記述内容（案）

3.1. 実験参加者について

- Step1 については、オプトインの実験参加者に限る。
- Step2 については、オプトアウトによる実施方法を検討する。

3.2. 大阪実験に関するデータに関しては、以下の 2 つの観点でプライバシ保護を行う。

(1)個人を特定できる情報の管理
(2)個人の移動経路情報の蓄積範囲の限定と制御

以下にその考え方を示す
(1)個人を特定できる情報の管理（流出防止）
●以下の情報は、人間からアクセス出来ないようにする（特定の計算機上のプロセスからのみ）

- 撮像情報
- 特徴量情報、場所、時刻、性別、年齢
- 性別、年齢、移動経路情報

●限定した人のみがアクセス可能とする（JR 西日本の特定の人、特定の役職）

- JR 西日本が取得する人流統計情報：
  k 匿名の k のパラメータについては第三者委員会で議論
  どの属性までを開示するかも第三者委員会で議論
  JR 西日本においても、情報管理規定の策定が必要

(2)個人の移動経路情報の蓄積範囲の限定と制御
・同じ人から出たデータであることを識別できる情報が蓄積されている装置の範囲を極力限定する
・上記で限定された範囲の装置に対しては、人が直接アクセスできないようにして、特定のプロセスからのアクセスのみが許可されるようにする。

3.3. 運用について

- 3.2.で示したプライバシ保護が継続して行われるように、システム稼働期間中のシステムセキュリティの確保（脆弱性がないように保つこと、定期的なペネトレーションテストの実施）を行う。
- 3.2.で示したプライバシ保護が行われていることを第三者が検証できるログを残し、監査を実施する。

3.4. プライバシ保護機構の設計における考え方

- カメラやネットワーク機器を含むすべてのデバイス、光ファイバ、JGN-X を含むすべての通信路はすべて攻撃者の攻撃対象と考える。
- データだけでなく、各サーバで動作するプロセスへのアクセス権を正しく管理する。人がアクセスしてはいけないデータにアクセスするプロセスの動作権限の管理を適切に行う。