モバイル環境における情報開示制御機構

本田篤史†　朝倉義晴†　才田好則†
NEC システムプラットフォーム研究所†

1. はじめに

ユビキタス社会の到来に伴い、センサ等の機器が利用され始めている。そして、これら機器を利用し、各機器のユーザやその周辺環境に関わるデータを収集し、端末及びサーバが提供するサービスで活用するための環境が整いつつある[1]。しかし、これらデータにはプライバシ情報が含まれることが考えられる。そのため、収集データやその公開先に応じて適切に開示の制限を行い、プライバシを保護する必要がある。

そこで、我々は収集したデータの開示制御をモバイル端末において実施する情報開示制御機構を提案する。本稿では、提案する情報開示制御機構とその実装例について述べる。

2. 課題

センサのように、温度や生体情報などの様々な情報を収集する機器が増加してきている。ネットワークに接続されたこれら機器からデータを収集し、収拾したデータを活用して有用なサービスや情報を提供することが試みられている。しかし、これらデータは、個人のプライバシにつながる情報を含む場合がある。また、単体のデータではプライバシ情報とはならないが、複数のデータを組み合わせることでプライバシ情報となる場合もある。例えば、位置情報と ID を含むデータと、氏名と ID を含むデータを組み合わせることで、特定の人の位置情報を得ることができる。よって、プライバシを保護するためには、これらデータの提供先を注意深く選択する必要がある。そのため、データの所有者が、その提供先を選択できることが望ましい。

3. 情報開示制御機構

3.1. システム構成

我々は、データ所有者が、データの開示先や開示条件を選択可能にする情報開示制御機構を提案する。この機構が想定しているシステムの構成要素は以下の 3 種類であり、そのシステム構成を図 1 に示す。

・センサ：
　データを取得する端末。取得したデータは下記モバイル端末へ送信する。
・モバイル端末：
　携帯電話や PDA。センサより送信されたデータを下記サービス提供者へ転送する。情報開示制御機構が存在し、転送時にデータ（センサ）の種類毎に開示制御を実施する。
・サービス提供者：
　センサよりデータを収集し、それらを用いたサービスを実施するサーバや管理者。

このような構成にすることで、センサが取得したデータは、必ず情報開示制御機構を搭載したモバイル端末経由でサービス提供者へ流通する。そのため、漏れなくデータの開示制御を実施することができる。また、モバイル端末は、ユーザが常時保持し、その管理下にあるため、情報開示制御機構を搭載することで第 3 者への不必要なデータの提供を防げる。

3.2. 機能

情報開示制御機構は、下記の機能を保持する。
・開示先に応じた開示制御
・開示先に応じたデータの粒度変更
・組み合わせに応じた開示制御
これら機能の詳細を以降で述べる。

3.2.1. 開示先に応じた開示制御

サービス提供者に応じて開示を許可するデータを制御する。制御はデータ（センサ）の種類毎に行う。この制御は、サービス提供者毎に開示可能なデータ種別を規則として設定しておき、この規則に基づいて実施する。この規則は、新たなサービス提供者や、新たなデータを制御対

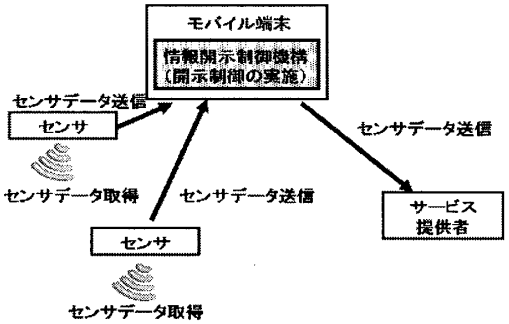

図 1：システム構成

Information disclosure control mechanism for mobile environment.
† Atsushi Honda, Yoshiharu Asakura and Yoshinori Saida
System Platforms Research Laboratories, NEC corporation

象とする際に、ユーザへ制御設定の問い合わせを行い、その結果を基に構築していく。

3.2.2. 開示先に応じたデータの粒度変更

サービス提供者に開示するデータの粒度変更を行う。“粒度変更”とは、近似値への変更や送信間隔の制御を行い、サービス提供者が詳細なデータを取得することを防ぐための制御である。この制御は、サービス提供者とデータ種別の組ごとに規則を設定しておき、この規則に基づいて実施する。この規則も前節で述べた規則と同様に、ユーザへ制御設定の問い合わせを行い、その結果を基に構築していく。

3.2.3. 組み合わせに応じた開示制御

同一のサービス提供者に複数のデータを提供する場合、それら複数のデータの組み合わせによる新たなプライバシ侵害の発生を検知する。どのサービス提供者にどのデータ種別のセンサデータを開示したのかの履歴を保持しておく。また、プライバシ侵害が発生し得るデータの組み合わせを記述した規則も所持する。そして、データを開示するときに、過去の開示履歴とこの規則に基づきプライバシ侵害の発生が発生し得る場合、ユーザに問い合わせを行う。

4. 試作

情報開示制御機構の試作を行った。実装環境を表 1 に示す。表 1 にあるように本試作の通信には、SIP を利用した。そして、SIP メッセージ内に、情報開示制御用の値を追加することで情報開示制御を実現した。また、本試作の情報開示制御機構の“開示先に応じたデータの粒度変更”では、数値データの切捨て/切り上げの機能と、文字列データの切捨ての機能と、送信間隔制御の機能を実装した。

5. 評価

前章で述べた試作を用いて情報開示制御機構の性能評価を行った。評価項目は、モバイル端末にてセンサデータを受信し、サービス提供者

表 1：実装環境

モバイル端末	HP iPAQ 212
センサ端末	78K0 UZ Stick-R 利用のダミーセンサ(3 種類)
サービス提供者	PC 上に実装した Web サービス(2 種類)
センサとモバイル端末間の通信	軽量シグナリングプロトコル [1]
モバイル端末とサービス提供者間の通信	PartySIP[2]

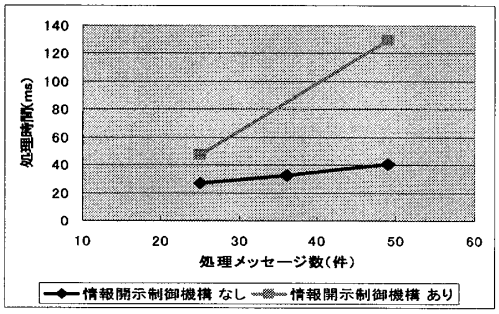

図 2：データ転送時の処理時間

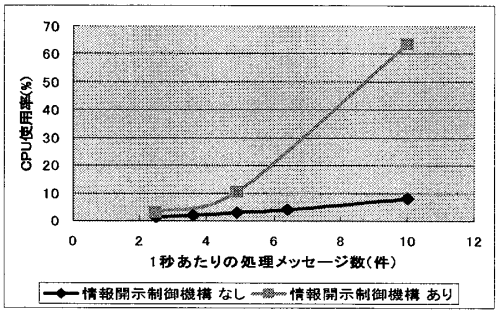

図 3：データ転送時の CPU 利用率

へ送信する際の処理時間と CPU 利用率である。結果を図 2、図 3 に示す。結果より、本機構は処理メッセージ数が増加すると、負荷の増加率が著しいことが分かる。そのため、より軽量な実装方式を検討する必要がある。

6. おわりに

本稿では、データの開示制御をモバイル端末において実施する情報開示制御機構を提案した。そして、その試作と評価について述べた。今後の課題としては、情報開示制御機構の軽量化があげられる。また、データの種類やデータの粒度変更方法と、プライバシ侵害の関係性を検討し、情報開示制御の精度を向上していくことも考えられる。

謝辞

本研究の一部は、情報通信研究機構(NICT)の委託研究「次世代ネットワーク(NGN)基盤技術の研究開発」プロジェクトの成果である。

参考文献

[1]岡部稔哉，静野隆之，“NGN センサ網のための軽量シグナリングプロトコル開発概要”，電子情報通信学会総合大会講演論文集，VOL.2009，通信 2，pp599，2009

[2]The partysip SIP proxy server
http://www.partysip.org/