

人間センシングシステムに関するガイドライン (案)

第1章 目的、定義、範囲

1.1 目的

本ガイドラインは人間からデータを収集・処理するセンシングシステムの設計や運用について、科学技術成果の積極的活用と普及を図りつつ運用の適切度を高め、もって健康、安全・安心、福祉、環境、エネルギー管理などの社会経済の向上に資することを目的とする。

1.2 定義

(1) センシング

状態や機能等のある物理量で計測すること。

(2) センサ

センシングを行う素子や装置等。

(3) センサデータ

センサにより計測された最小単位状態のデータ。

(4) 原データ

センサデータにシステム側等が属性等を付与して、ある個人からある状態について得られた意味のあるデータ。

(5) 加工データ

原データを加工し、他のデータと組み合わせたりして利用しやすい形式となったデータ。

(6) ネットワーク

有線ないし無線でデータを送受信する媒体や方式。

(7) データ/データベース

データはセンサデータまたは原データまたは加工データである。データベースは、データのある体系のもとで利用しやすくすべく収集・整理したものであるが、本ガイドラインでは特に人間から収集されたセンサデータや原データ、加工データ等の集合体を指す。

(8) (人間センシング) システム

センサやネットワークを活用して種々の技術を利用し組合せ、ある妥当な目的のために設計・運用がなされる技術システム。

(9) システムの外 (内)

上記のシステムが扱うセンサやネットワーク、サーバやソフトウェアなどからなる技術要素範囲の外 (範囲の内)。ここでは、ネットワークについては外部からの侵入が困難なローカルネットワーク内であって処理部がすべてのデータを制御できる範囲をシステムの内とし、その内から外部へデータが流れる場合に外とする。インターネット接続は外として扱われる。

(10) データ保護のグレード

センサを通じて収集された原データについて、その保護を行うデータの範囲に関して設定されるレベル。

1.3 範囲

本ガイドラインは人間から接触・非接触を問わずその状態や機能のある物理量で測定し、ある妥当な目的のために解析等の処理、データ蓄積を行うシステムを対象範囲とする。ネットワークを活用するシステムが多いと考えられるが、それに限定されない。

第2章 センシングされる人間との関係

2.1 基本的な考え方

人間センシングシステムの研究開発や設計、運用、人間への適用を行う場合、それに従事する技術者は、憲法、民法、個人情報保護法等関係する法令を遵守し、個人の尊厳に最大限の配慮を払わなければならない。
また、情報セキュリティ技術の動向に常に注意を払いその最新技術を極力取り入れるものとする。

2.2 センサの取り付け

センサ取り付けにあたっては、目的およびデータ保護のグレードを説明し、本人の了解を得て行う。
児童についてはその両親、親権者の了解を得る。
認知症の方についても、極力本人とその家族の了解を得る。

2.3 データの扱い

センシングされたデータについては、データが個人情報を含むところから、「個人情報の保護に関する法律」に従って取り扱う。次章の技術的なガイドラインを参照。

2.4 個人差

データ保護に関する考え方には個人差があると考えられる。データ保護についてはグレードを複数設け、取り付けられる人間はその中から保護レベルを選択ができるようにする。次章を参照。

第3章 センシングシステムの技術的なガイドライン

3.1 原データ

センサデータは、℃、m/sec、Gal、rad/sec、kg、lx 等単位を持った数値であり、これに計測時間、個人の氏名や年齢等の個人属性、環境情報等が加わると個人に関する意味のある原データとなる。これらの属性や環境情報はシステムが自動的に生成したり、個人が入力したりして付加されることが一般的である。

原データは原則として個人情報である。

センサデータは通常は個人情報ではないと考えられるが、システム設計時に、これによって個人を特定することはできないことを十分確認するものとする。

3.2 原データのシステムでの取扱い

原データはシステムの外に流出しないよう設計と運用を図らなければならない、システム内においても権限を付与された人以外はアクセスできないよう設計・運用がなされなければならない。

外のシステムにおいて他のデータと組み合わせられて利用がなされる場合は、個人の保護に関するグレードに従ってデータ保護がなされる。データ保護のグレードについて個人別の確認がとれない場合には、個人属性が知り得ないようシステム内で加工・処理がなされた上でシステム外へ渡されなければならない。

3.3 データ保護に関するグレード（システム内）

データ保護については個人差を考慮し、以下のようにグレードを設け、センシングされる人間の了解を得る。以下は、システム内でシステム管理者以外の利用者に対するものである。

- (1) 個人の属性を示すデータはすべてアクセス不可。

- (2) 本人を特定できないデータ範囲(【例】年齢、性別、場所(都道府県、市町村単位))では可。
- (3) 本人特定につながる可能性があるが限定可(【例】番地を除く住所、職業、)。
- (4) さらに広い範囲で可(【例】氏名、生年月日)。

3.4 データ保護に関するグレード(システム外へ出る場合)

データ保護については個人差を考慮し、以下のようにグレードを設け、センシングされる人間の了解を得る。以下は、システム内のデータがシステム外へ出る場合のグレードである。

- (1) 個人の属性を示すデータはすべて削除。
- (2) 本人を特定できないデータ範囲(【例】年齢、性別、場所(都道府県、市町村単位))では可。
- (3) 本人特定につながる可能性があるが限定可(【例】番地を除いた住所、職業、)。
- (4) さらに広い範囲で可(【例】氏名、生年月日)。

3.5 データの扱い

システムの内にあつては、原データは上記のグレードにしたがつて、本人かシステム管理者またはシステム管理者が認めた者のみがアクセスできるよう設計や運用基準が定められなければならない。また、システムの外に出る場合は本人に説明し、保護のグレードを確認し、システム外でのデータの利用者にその目的や技術を確認した上で最大の技術的な配慮を払った上でシステム外へ渡すものとする。

3.5 データの目的外への利用

既に了解を得ている目的以外にデータを利用しようとする場合は、本人の了解を得て行う。

システム外においては、目的外に利用される可能性の有無、制御可能な範囲を予め説明するものとする。

第4章 補足

4.1 審査委員会

本ガイドラインにつきさらに明確化が必要な場合には、関係者が中立者を交えた「審査委員会」を設けてその判定を基準とすることができる。

4.2 見直し

本分野での技術進歩は急速であるので、時々本協議会において見直しを行う。

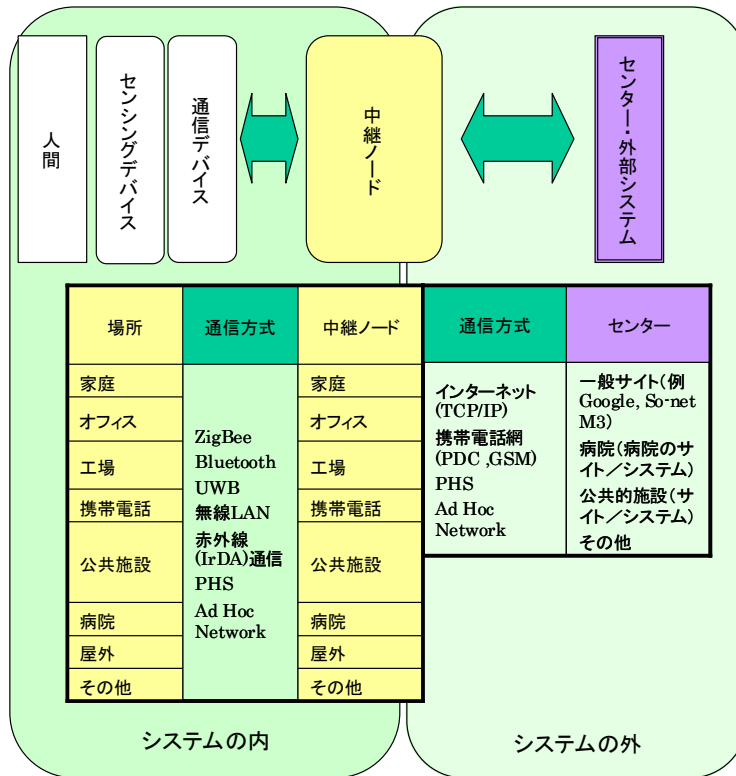
4.3 制定・改訂履歴

第1版 平成22年 月 日

社会・環境型センサーネットワーク協議会委員名簿

注

- システムを制御できる範囲内と必ずしもすべて制御できるとは限らない外に分けた。



参考図 システムの内と外

- データ保護のレベルとして、個人差を取り入れ複数レベルを設けた。ある範囲のデータを提供しても良いと考える人、一切拒否する人等種々の考え方があり得ると想定した。