

オープンなセンサを共有するセンシング Web のための広域分散アーキテクチャ

神林 亮^{†1} 佐藤 三久^{†1}

建物や街中、道路や駅構内といった様々な場所に、カメラや赤外線センサ、マイクなどのセンサデバイスが設置されつつあり、それらをネットワークで結びつけて活用する技術が期待されている。センシング Web は、クローズドなネットワークのみならず、広域ネットワークに接続されたオープンなセンサ群を接続して社会全体で共有利用を行おうとするプロジェクトである。センシング Web では、従来の単純なセンサを対象とする従来のセンサグリッドと異なり、画像や音声も対象とする。そのためにプライバシーの保護に配慮することが必要となる。また、画像データなどのデータは大量であるが、不必要なデータも多く、プライバシーに配慮する必要になるため、データは蓄積せずにセンサの直近で処理することが望ましい。そのためのアーキテクチャとして、遠隔プログラム実行によりセンサプライバシー情報や不要なデータを除去可能で、かつ認証機構によるアクセス制御が可能なセンシング Web のアーキテクチャを提案する。

A Distributed System Architecture of Sensing Web for Shareing Open Sensor Nodes

RYO KANBAYASHI^{†1} and MITSUHIKA SATO^{†1}

Recently sensor devices such as video cameras, infrared sensors and microphones on various places such as the building, in the town, and roads and the station yards are being placed. It is a promising technology to make use of these sensors connected by the network. Sensing web is a project to share sensors open to the public in wide-area network, not only sensors closed in a network. Different from existing sensor grids for simple sensor devices, the Sensing web includes sensor devices such as video cameras and microphone. This requires consideration for privacy on the data from sensors. While sensor data such as images is relatively large, required information in the data may often be small and include privacy. So it is desirable to process the data and extract the information near the sensors. In this paper, we propose the architecture which can protect privacy information and remove useless data by shipping the remote program execution into the node near to a sensor with the access control by the authentication mechanism.

1. はじめに

今日、建物や街中、道路や駅構内といった様々な場所に、カメラや赤外線センサ、マイクなどのセンサデバイスが設置されつつあり、それらをネットワークで結びつけて活用しようとするユビキタスセンサネットワーク (USN) 技術が有望視されている。

ただし、これまでに行われてきたのは監視カメラによるセキュリティ保護や定点カメラによる交通流調査のように、クローズドなネットワークで特定の利用者が限られた用途のためだけにセンサを利用するといったものが大半であった。これに対し近年、センサを広く公開して世界中の人々に共有しようという動きが活

発になってきており、その一つとしてセンシング Web と呼ばれるコンセプトが提案されている。

センシング Web¹⁾ は、"Web" という言葉が意味する通り、World Wide Web(WWW) のように、誰もが自由にセンサデバイスの出力する実観測データを扱うことができるシステムを目指したものである。センシング Web においては、自身が管理していないセンサでも必要があれば利用可能で、それらのセンサを利用するアプリケーションやサービスの提供も自由に行える。このため、これまでのようなクローズドなシステムでは想定されていない利用方法の出現が期待される。例えば、ある者がどこかに忘れ物をしてしまった場合、今日の世界においてはその者が思い当たる場所を全て探すしかないが、センシング Web によって、ブラウザから世界の誰かが提供する忘れ物探しのサービスを利用する事で、労せずして忘れ物の場所を知る

^{†1} 筑波大学大学院システム情報工学研究科
Graduate School of Systems and Information Engineering,
University of Tsukuba

事ができるかもしれない。

センシング Web の実現のためにはプライバシーの問題の解決が必要である。また、センサによる観測データには不必要なデータも多く、そのようなデータを効率的に扱う手段が必要である。そこで本稿では、遠隔プログラム実行によりセンサの直近でプライバシー情報や不要なデータを除去可能で、かつ認証機構によるアクセス制御が可能なセンシング Web のアーキテクチャを提案する。

次章ではセンシング Web の概要について述べる。3章では関連研究について述べ、解決すべき問題点を示す。4章では遠隔プログラム実行モデル、認証・認可モデルおよびプライバシー保護手法の設計を述べる。5章ではまとめと今後の課題について述べる。

2. センシング Web

本章では、センシング Web のコンセプトについて述べた後、センシング Web を実現をするにあたり求められる要件について述べる。

2.1 コンセプト

提案アーキテクチャは以下の2点の基本コンセプトに基づく。

- プライバシーの保護

センシング Web ではビデオカメラによる画像や音声を対象としている。従来のセンサグリッド²⁾は、主に温度や湿度などの単純なデータが対象であり、プライバシーの問題が存在しないセンサを対象としたものであった。画像や音声は多くのプライバシーに関する情報を含むため、センシング Web ではプライバシー保護のための仕組みが必要不可欠である。

- センサ直近でのデータの処理

センサグリッドなどのセンサデータ利用への取り組みでは、センサデータはまずストレージに一度蓄積してから必要に応じて取り出して利用することが多かった。しかしながら、特定の場所を監視している監視カメラのデータなどに見られるように、データが大量であるが必要なデータは少ない場合が多い。また、センサデータには上述の通りプライバシー情報が含まれることが多く、データを蓄積した場合、被観測者がプライバシー情報の取り扱いに関して懸念を抱く可能性がある。したがって、提案アーキテクチャではセンサデータをそのままストレージに蓄積せずにセンサ直近で適切にデータの処理を行い、必要なデータのみを扱うことを基本的なアーキテクチャとする。

想定する環境は、図1に示すように、従来のクラウドなセンサネットワークがインターネットを介して複数結びついた環境である。しかしセンシング Web ではそれに加え、個人的に所持している USB カメラ

などのように、ネットワークを構成していない独立したセンサデバイスも利用される事を想定する。

アプリケーションの例としては、1章で述べた忘れ物探しアプリケーションや、監視カメラの映像からの天候マップの作成などがあり、センシング Web のアーキテクチャ、またシステムはこれらのアプリケーションが無理なく実現できるものでなければならない。

2.2 利用モデル

センシング Web においては、被観測者、センサ設置者、システム管理者、アプリケーション開発者(ユーザ)およびエンドユーザの6つの役割が存在する。被観測者はセンサにより観測を受ける者である。例えば監視カメラの映像に写りこむ者などは被観測者である。センサ設置者は実際にセンサを物理的に設置する者である。ビル内の監視カメラを考えた場合には、設置を決定したビルの管理者などが設置者にあたる。システム管理者はセンシング Web を実現するためのシステム(以下センシング Web システム)の管理者である。センシング Web のためのミドルウェアを運用し、アプリケーション開発者のレジストレーションやセンサネットワークに関する情報を提供するポータルを提供する。センサにアプリケーション開発者がアクセスするための権限管理なども主にシステム管理者により行われる。アプリケーション開発者はセンサデータを取得し加工してアプリケーションやサービスを開発する者である。

各役割がどのようにシステムと関わることでセンシング Web が実現されるかを以下に述べる。

- (1) センシング Web を実現するシステムの構築
システム管理者がセンシング Web システムを構築する。構築においては最低限、センサにアクセスするために必要なロケーション情報を管理するディレクトリサービスなどのセットアップが行われなければならない。他にもいくつかのサービスが一般的にはセットアップされるであろうがここでは共通項を挙げるに留める。
- (2) センサの登録
センサ設置者がセンサをセンシング Web システムに追加する。追加の単位としては、センサネットワークの単位で追加が行われる場合と、単独で存在するセンサの単位で追加が行われる場合の2通りが考えられる。
- (3) センサデータの取得
アプリケーション開発者がセンシング Web システムを介してセンサデータを取得する。取得に際しては、センサへアクセスするためのアドレスや手順についてディレクトリサービスに問い合わせを行った上で、データの読み出しなどが行われる。
- (4) サービスやアプリケーションの提供
アプリケーション開発者はデータを取得しそれ

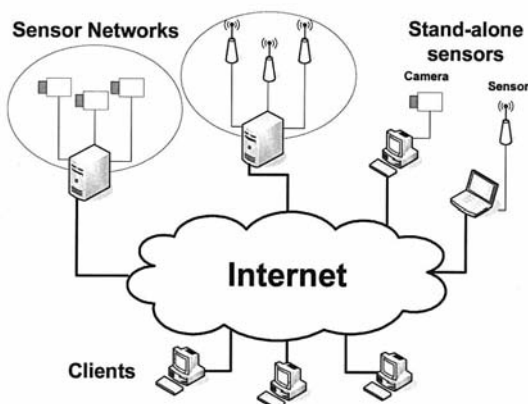


図1 センシング Web の想定環境

を利用したアプリケーションやサービスを提供する。

(5) エンドユーザによる使用

エンドユーザがアプリケーション開発者により提供されたアプリケーションやサービスを利用する。

2.3 センシング Web の要件

資源へのアクセス提供と管理を行うためのシステムとして以下の要件を満たす必要がある。

- アクセス制御のための認証機構
各センサにおいてユーザごとへ異なったアクセスポリシーを設定できる必要がある。例えば、自宅に設置してあるビデオカメラへのアクセスを自身と家族には許可するが、その他の者には許可しないといったポリシーが実現できなければならない。
- 柔軟な資源アクセスインタフェース
資源の利用方法はアプリケーションによって異なる。したがって、資源へのアクセスのインタフェースは様々な要求に対応可能な柔軟なものでなければならない。もしくは、ユーザに合わせてインタフェースが定義できなければならない。

また以下のような要件もセンシング Web 特有の要件として考慮される必要がある。

- 異機種混合環境への対応
センサデバイスでもその仕様はそれぞれ異なっており、自身に OS を搭載し、自律的に動作するデバイスがあれば、PC にアタッチして使用するタイプのデバイスも存在する。また、使用するプロトコルや出力するデータの形式も多岐にわたる。センシング Web ではそれらのデバイス全てを統合して利用可能でなければならない。また、センサデバイスが PC にアタッチされて利用するタイプの場合、センサデバイスだけではなくセンサデバイスを接続する PC の異機種混合も問題となる。
- プライバシの保護

センシング Web では、USN と異なりセンサの設置者のみならず世界中の不特定多数がセンサデータにアクセスするため、プライバシー保護の要求は USN の場合と比べより大きなものとなる。

- ストリーミングデータの効率的な処理
ビデオカメラなどのストリーミングデータは一般にデータサイズが大きいため、センサデータを全てネットワークへ送出するとネットワーク資源を過大に消費してしまう。しかし、その一方でストリーミングデータの大部分は利用者にとって必要のないデータが占める。したがって、必要なデータのみを抽出してネットワークに送出することにより、ネットワーク資源の消費を抑えることが可能な仕組みが必要となる。

3. センシング Web の設計

本章では 2.3 で挙げた要件を踏まえ、提案するアーキテクチャのコンセプトを述べる。その後、提案アーキテクチャを構成するモデルについて、遠隔プログラム実行モデル、認証・認可モデル、プライバシー保護モデルの順で述べる。

3.1 遠隔プログラム実行モデル

提案アーキテクチャではセンサデータの取得を遠隔プログラム実行機構を用いて行う。遠隔プログラム実行機構の構成を図 2 に示す。遠隔プログラム実行機構は、機能追加を行った軽量 Linux バイナリ実行システム BEE³⁾ とバイナリを配置するための機構を組み合わせることで実現する。以下のような利点がある。

- 日常的に利用しているプログラミング言語の表現力を駆使し柔軟なデータの処理が可能となる。
- 必要なデータのみをネットワークに送出すること、およびプライバシー情報を適切に除去することが容易に実現可能となる。また、任意のプログラムを実行可能なため、処理を行ったデータをクライアントに返すためのインタフェースを柔軟に設定することができる。
- BEE はシステムコールのエミュレーションとメモリアラインメントの調整を行うことにより、Linux バイナリを Windows 環境上で動作させる事が可能である。そのため異機種混合環境への対応が可能となる。
- BEE のシステムコールのエミュレーションを行うという特性により、BEE 上で動作させるプロセスと BEE を動作させるマシン間、また BEE 上の各プロセス間でサンドボックスが可能となる。信頼できない第三者にプロセスの実行を行わせる場合、サンドボックスを行うことは重要である。

BEE の他にもグリッドミドルウェアである Globus Toolkit などを用いることで遠隔プログラム実行を行

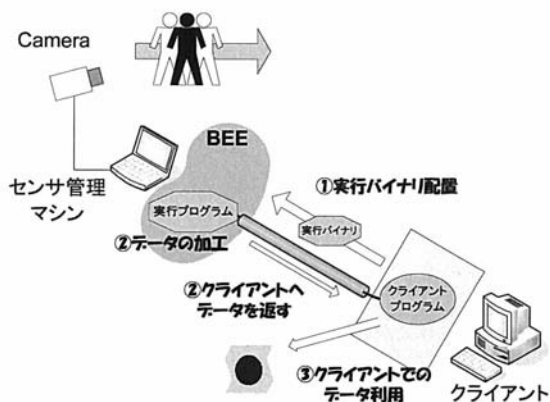


図2 遠隔プログラム実行モデル

うことも可能であるが、Globus Toolkitはグリッド環境へログインできるようなアカウント体系を前提としており、センサへのアクセスのみを必要とする今回のケースで利用するのは適当ではない。また、Javaのダイナミッククラスローディングとサンドボックス機構を用いても同様の処理を実現できる。しかしながら、Javaを用いた場合は、ネイティブコードを実行可能なBEEを用いる手法と比べ得られる性能は低くなる。また、プロセスあたりのメモリ消費量などもネイティブプログラムと比べて大きくなるため、単一マシンで多数のプロセスが起動される可能性のあるセンシングWebでは、スケーラビリティが制限されてしまう可能性がある。さらにネイティブコードで使う事に前提に開発されたライブラリが利用できない。

実行バイナリの配置は、Webサービスの枠組みとの親和性のため、SOAPやXMLRPCなどのプロトコルを用いて行う。したがって、サーバへの実行バイナリの配置時、実行バイナリはSOAPメッセージやXMLRPC内に種々のパラメータと共にXMLメッセージ内にエンコードされる。このような配置方法をとることにより、スケジューリングアルゴリズムに基づいて、人手を介さずにプログラムの配置を行うといった発展的な利用も可能となる。

提案する遠隔プログラム実行機構では、BEEに仮想デバイスの機能を実装し、それを用いることでセンサデバイスからのデータの読み出しや、加工したセンサデータのクライアントへの送信を可能とする。これは入出力のインタフェースとして仮想デバイスを用いることを意味している。センサデータの読み込みは、BEEが提供するセンサデータ読み出し用仮想デバイスを利用することで行う。センサデータ読み出し用仮想デバイスは実デバイスであるセンサデバイスをラッピングしており、readアクセスによって適切なセンサデバイスからデータが読み出せる。このとき、BEE上で動作するプロセスは/dev/sensorなどのパス名で表

現されるデバイスファイルとして読み出し用仮想デバイスにアクセスする。センサデータのクライアントへの送信は、同様に/dev/clientにwriteアクセスすることによって可能となる。ただし、/dev/clientはストリームデータなどを送信するためだけに利用し、他の通信に対してはWebサービスによる遠隔手続き呼び出しのインタフェースを提供し、クライアントとの柔軟なインタラクションを実現する。

3.2 認証・認可モデルの検討

センシングWebの認証・認可のモデルを考える上で考慮すべき要件として以下の4つがあり、本節では以下の要件を満たす認証・認可モデルを検討する。

- パフォーマンス
必要とする処理量が許容できないほど大きなものであってはならない。
 - 管理コスト
センシングWebシステムの管理者に大きな労力を要求してはならない。特にユーザアカウントの発行にかかる労力などは注意しなければならない。
 - 利用コスト
センシングWebシステムの利用者に大きな労力を要求してはならない。ここで利用者としては、センサの利用者だけでなく、センサの設置者も含む。
 - 複数組織に跨るセンサの透過的な利用
センシングWebにおいて、全てのセンサは単一の組織の管理下に置かれているわけではない。したがって、複数組織に跨る複数のセンサの利用がユーザ透過に行えなければならない。
- センシングWebにおけるセンサの利用形態はセンサの管理単位により以下の2つの場合に分類できる、
- センサネットワーク単位でセンサ管理が行われている場合。この形態では、認証・認可においてセンサをグループ単位で扱う事が可能である。このため、全てのセンサを個別に扱う場合と比べ、アカウント管理の労力や認証・認可の処理にかかるコストは小さくて済む。また、複数のセンサネットワークを一つのVirtual Organization(VO)⁶⁾としてグループ化することで、複数組織に跨るセンサを透過的に扱うことが可能である。VOとはユーザの目的を実現するために必要な資源から構成される一種のグループである。
 - 単独で存在する個人所有のセンサ（以降、単独センサ）の単位でセンサ管理が行われている場合。この場合では、センサネットワーク単位でのセンサ管理の形態の場合と異なり、センサの管理は個人が行っているためVOを構成する作業を行う者を適切に設定できない。このため、VOでセンサをグループ化することは困難である。したがって、単独センサの単位でセンサ管理が行われている場合には、VOなどを用いずに各センサ個別での認証・認可を行う必要がある。

しかし、各センサ個別での認証・認可は複数の単独センサを利用しようとする場合に、ユーザに大きな負荷を強いる可能性がある。例えば、単独センサを数百個使って動作するアプリケーションを考えた場合に、システムが基づく認証・認可のモデルが、ユーザはセンサ利用に先立って各サイトからアクセス許可を受けなければならないというものであったなら、ユーザは数百のサイトの管理者に対して E-Mail を送る、もしくは数百のポータルにアクセスしてアカウントの発行を依頼しなければならない。これはユーザにとって許容できない。したがって複数の単独センサの利用をサポートするためには、人手をまったく介さずに、各センサごとの認証・認可までが行えるモデルが必要である。

個別のサイトでのアカウントの発行を必要とせずに、各センサ個別での認証・認可を可能とするモデルとして、ポリシーベースのモデルと信頼の連鎖に基づくモデルの2つが考えられる。ただしポリシーベースのモデルは認可を実現するためのモデルであり、認証については他のモデルで対応する必要がある。

ポリシーベースのモデルでは、センサの持つポリシーと利用者の属性のマッチングで認可を行う。ポリシーベースのモデルにはユーザの属性による制約に基づくアクセス制御を、人間が介さずに行うことができるという利点がある。しかしその一方で、ポリシーとして記述できる内容がユーザ側で列挙されている属性の数や内容に制限される。また、必要十分な属性の項目を事前に列挙することは一般に困難である。したがって、ポリシーベースの認可モデルは、ある程度の強さの制約条件のもとでセンサの利用を可能としたい場合に適しているが、厳格な制約条件を求める場合の利用には適していないと言える。

信頼の連鎖に基づくモデルとしては代表的なものとして Pretty Good Privacy(PGP)⁷⁾がある。PGPでは“信頼している友人の友人は、信頼できる”というルールの下、草の根的に信頼関係を築いていくことで、認証サーバなどを用いることなく認証・認可を行うことが可能となる。

信頼の連鎖に基づく認証・認可のモデルをセンシング Web に導入すると、過去に A 小学校のセンサ A にアクセスが許可されたのであれば、同じく小学校 B に設置されたセンサ B にもアクセスを許可するといった、連鎖的な認証・認可が可能となる。しかしながら、センサの管理者間で信頼関係が成り立っているパスでしか連鎖的な認証・認可は発生しないため、本来ならアクセスする許可が与えられるべきセンサでもアクセスできないといった事が起きる。また、センサ間の信頼関係は各センサの管理者が申し出る必要があり、モデルが機能するか否かが単独センサ管理者のアクティビティの程度に左右される。

以上で述べた各モデルは相互排他的なものではな

く、各々を適材適所で使い分ける事が可能である。提案アーキテクチャでは複数のモデルを利用する事を検討している。

3.3 プライバシ保護モデル

提案アーキテクチャはセンサ直近での遠隔プログラム実行によりプライバシーの保護を行う。その方針は、ユーザがセンサに送り込んだプログラムにはプライバシー情報を含むセンサデータへの無制限のアクセスを許可するが、同時にユーザにはプライバシー情報を処理してからネットワークに送出する責任を負わせるというものである。これにより、プライバシー情報のセンサ外への流出を防ぐことが可能である。具体的には以下のような手順でプライバシーの保護が行われる。ここでは例として、繁華街に設置された監視カメラによって歩道を歩く人間の数を調査しようとした場合を考える。その手続きを図2に示し、以下で説明を行う。

- (1) プログラムのセンサ管理マシンへの配置
クライアントがセンサ管理マシンへ実行バイナリの配置を行う。実行バイナリの処理内容は監視カメラから得た画像データに対して画像処理を施し、単位時間あたりの通過人数という情報を求めるというものである。
- (2) センサでのプログラム実行
配置されたバイナリがセンサ管理マシンにおいて実行される。実行されたプログラムは求めた通過人数をクライアントへ返す。
- (3) 加工データのクライアントでの利用
クライアントはセンサから返された通過人数を用いてグラフなどを作成し、エンドユーザに提示する。

この例では、監視カメラにおいて歩行者の顔や自動車のナンバーなどが映りこんでいる可能性があるが、遠隔プログラム実行により、それらの情報を含まない必要な情報だけをクライアントに返すことができる。これは、遠隔プログラム実行を用いることでプライバシーを保護しつつセンサのデータを利用できることを示す。

ただし、提案アーキテクチャの遠隔プログラム実行によるプライバシーの保護の枠組みにおいては、少なくとも遠隔プログラムを実行可能なユーザはプライバシー情報を入手可能である。また、そのユーザがもし仮に悪意を持ったユーザであったり、怠惰なユーザであった場合、プライバシー情報が正しく処理されないまま、クライアントに送信されてしまう。悪意を持ったユーザであった場合ではさらに、クライアントにおいて不特定多数に公開されてしまうことが起きる可能性もある。

3.4 プライバシ保護についての問題点

プライバシー情報の流出を防ぐためには、遠隔実行されるプログラムにおいてプライバシーを保護できないといけない。しかし、それを正しく行うためには遠隔

実行されるプログラムが、センサから読み出したデータから、プライバシーを保護すべきデータの領域などのメタデータを取得できる必要がある。これを実現する仕組みとして、特徴量や識別子に基づく方法がある。

識別子による手法は、センシングされる個人をRFIDタグなどで一意に識別可能にして、指定した識別子に対応する者以外の人物に関する観測データを取り除いてしまう方法である。識別子による方法はプライバシーの保護を行う上で極めて有用であり、実現が期待されているが、識別子による個人の認識は一般に普及していないため現時点での利用は困難である。

特徴量による手法は、識別子による方法の識別子を、観測対象の者の何らかの特徴量に置き換えたものである。特徴量としては、事前に撮影しておいた対象の個人の写真や音声データなどから抽出したものをを用いることができる。被観測者の側にRFIDなどの特別なコンポーネントを必要としないため、現時点でも実現可能な手法である。そのため、提案アーキテクチャではこちらの特徴量による手法の採用を検討している。

4. 関連研究

センシング Web とほぼ同様のコンセプトのセンサ Web を実現するためのアーキテクチャとして国際標準化団体 Open Geospatial Consortium(OGC)により Sensor Web Enablement(SWE)³⁾ が提案されており、いくつかのプロジェクトで実際に採用が行われている。Rajkumar Buyya らは 2) にて SWE に準拠した Open Sensor Web Architecture(OSWA)を提案しており、4) でその実装も行っている。

SWE には、ストリーミングデータを効率的に処理する事ができないという問題がある。なぜなら、SWE はセンサデータの取得を問い合わせ言語により行うが、SWE の実装が提供する問い合わせ式の表現力は SQL とほぼ同程度であり、ストリーミングデータに対して適用しても意味のある抽出操作は期待できないためである。したがって、扱うセンサがビデオカメラのようなストリーミングデータを出力するものであった場合、既存の SWE の実装では、センサが出力するデータのほぼ全てをクライアントに送信せざるおえない。しかしながら、ストリーミングデータは一般にサイズが大きいためネットワークへの送出を行うとネットワーク資源を過大に消費してしまう。この問題は世界中に存在する膨大な数のセンサを共有しようとするセンシング Web では致命的である。また、少数のセンサに限った場合においても、ユビキタス環境において潤沢なネットワーク資源は仮定できないため、ネットワーク資源の大きな消費は看過できない問題である。

提案アーキテクチャでは、遠隔実行するプログラムで処理することにより、これらの問題を解決している。

5. まとめと今後の課題

本稿ではセンシング Web の概要について述べ、現状のセンシング Web には、柔軟性、通信帯域の消費、認証・認可、プライバシー保護に問題点があると述べた。また、それらの問題点を解決可能なセンシング Web のアーキテクチャを提案した。柔軟性、通信帯域の消費、プライバシー保護の問題を解決するために遠隔プログラム実行モデルを設計し、ユーザの利便性と管理コストを重視した認証・認可モデルを検討した。

今後は設計内容をより詳細に検討した後、設計に基づいた実装を行う。そして、センシングの研究者と共同で実証実験を行う。

謝辞 本研究の一部は、科学技術振興調整費「センサ情報の社会利用のためのコンテンツ化」および筑波大学プレ戦略イニシアティブ「実世界計算情報学の基盤創成拠点」による。

本研究について様々なアドバイスを頂いた 大田友一教授(筑波大学計算科学研究センター)、北原格講師(筑波大学計算科学研究センター)、対馬崇氏(筑波大学システム情報工学研究科)に感謝する。

参考文献

- 1) Sensing WEB:<http://www.imell.kuis.kyoto-u.ac.jp/sweb/index.html>
- 2) Chen-khong Tham, and Rajkumar Buyya, SensorGrid: Integrating Sensor Networks and Grid Computing, Special Issue on Grid Computing, Computer Society of India, July 2005.
- 3) George Percivall, Carl Reed, OGC Sensor Web Enablement Standarts, Sensors & Transducers, Vol. 71, Issue 9, September 2006, pp. 698-706.
- 4) Xingchen Chu, Open Sensor Web Architecture:Core Service, The University of Melbourne, December 2005.
- 5) Yoshifumi Uemura, Yoshihiro Nakajima, Mitsuhsa Sato, Direct Execution of Linux Binary on Windows for Grid RPC workers, IPDPS, Vol.33, No.12, pp.1-8(2007)
- 6) I. Foster et al. The Physiology of the Grid:Making the Global Infrastructure a Reality, Wiley, 2003
- 7) Open PGP:<http://www.openpgp.org/>