ISS-SP-040

ウェブデータストア上での個人情報共有にむけた ロールベース細粒度アクセス制御フレームワーク

山西　雄大† 　鎌田　十三郎†† 　高木　由美†† 　太田　能†††
† 神戸大学工学部情報知能工学科 †† 神戸大学大学院システム情報学研究科
††† 神戸大学大学院科学技術イノベーション研究科

1. 背景

現在，クラウドコンピューティングの普及に伴い，様々なデータをクラウド上に保存・活用することが注目を集めている．公共クラウドのデータベース上に車の情報や個人情報を保存しておき，その情報を各ユーザがサードパーティ製のアプリなどを介して利用できるような環境を実現したいとする．この時，個人情報に対するアクセスはアプリケーションに応じた制限が必要となる．ユーザが求める適切なデータ保護を実現するためには，レコード単位の細粒度アクセス制御が求められる．

2. アクセス制御機構について

現在，Web サービスのアクセス制御はサーバプログラムの一部として記述されるのが一般的である．本研究ではデータ構造に基づくルールを与えるだけでアプリケーションに応じた細粒度アクセス制御を導入できるようなフレームワークの実現を目指す．開発するシステムの概要を図 1 に表す．使用するデータベースは MongoDB などの NoSQL 系を想定する．サービス開発者は JSON 形式に関するスキーマ言語である JSON Schema [1] を用いてデータ構造を定義し，アクセス制御ルールを拡張構文により定義する．システムは，これらの定義に基づきアクセス制御を実現する．[2] と同様ロールベース制御を採用する．

3. アクセス制御ルール

車の情報を保存するための JSON 形式のインスタンス例を図 2 に，そのデータ構造定義およびアクセス制御ルールを図 3 に示す．図 3 の ① の “Role” 要素には，ロール名と，そのロールに割り当てるユーザ ID が格納される場所が記される．図 2 の例では “ownerRole” の値が “ownerId” フィールドから取得され，ID: “b34” のユーザが割り当てられる．アクセス制御は，フィールド毎に指定可能である．図 3 の ② では，アクセス種別ごとに許可を与えるロールの一覧が記される．図 2 の例では，“ownerId” に対して編集可なロールとして “ownerRole”，読み込み可なロールとして “carRole” と “ownerRole” が指定されている．

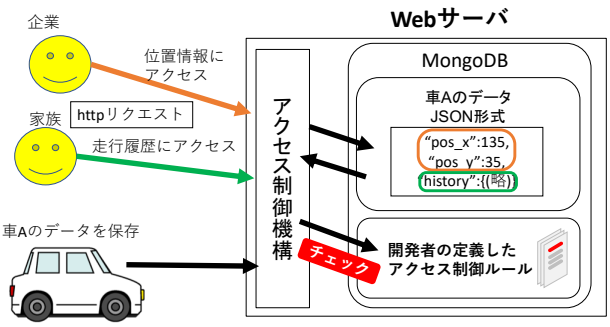

図 1 アクセス制御機構の概要

```
{
 “carId”:”a1234”,
 “driverId”:“a12”,
 ”ownerId”:”b34”,
 “familyId”:[”c56”,”d78”],
 “pos”:{
    ”x”:135.3,
    “y”:35.7
 },
 “history”:{
    “15:00”:{
       “pos_x”:134.5,
       “pos_y”:36.2,
    }    (略)
```

図 2 車の情報を保存する JSON 形式

```
{                    (略)
    ”type”:”object”,
     “Role”:{      ・・・①
       “ownerRole”:”ownerId”,
       “carRole”:”carId”,
       “familyRole”:”familyId”
     },              (略)
“properties”:{
   “ownerId”:{
    ”type”:”string”,
     ”Permission”:{  ・・・②
       ”write”:[“ownerRole”],
       “read”:[“carRole”,
                ”ownerRole”]
     }              (略)
```

図 3 データ構造およびアクセス制御ルール

4. 今後の課題および展望

現在は基本的なロールベースのアクセス制御については実装済みで，動作確認も完了している．しかし，実現できていない機能が一部あるので完成に向けて実装してゆくつもりである．本研究は IoT 時代の情報共有基盤の構築に役立つことを目指しており，また [3] で提案しているエッジ計算基盤への導入を計画している．

謝辞　本研究の一部は科研費（基盤研究（C）15K00125）による．

参考文献

[1] json-schema.org, JSONSchema, http://json-schema.org
[2] 仙波，鎌田，“個人/共有データを格納するためのロールベースアクセス制御機構付き Web データベースの提案”，DEIM Forum 2012.
[3] 長門他，“明示的なデータ分散管理を記述可能なエッジ環境向け分散データベースプラットフォームの提案”，第 9 回 ICN 研究会ワークショップ，2017.