Vol.2012-DPS-152 No.28
Vol.2012-GN-85 No.28
Vol.2012-EIP-57 No.28
2012/9/14

スマートシティ向け情報管理基盤における データアクセス制御方式の提案

河田洋平[†1]　矢野浩仁[†1]　水野善弘[†2]　寺田博文[†1]

都市インフラをスマート化する「スマートシティ」の取り組みにおいて，適切な情報利活用事業者に対してのみ機器や設備から収集した情報を提供するデータアクセス制御が必要となる．本稿では，スマートシティ向け情報管理基盤におけるデータアクセスの特徴や課題からデータアクセス制御に求められる要件を整理する．次に，整理した 3 つの要件を満たす，アクセス対象のデータの内容に基づいたインタフェース非依存のアクセスポリシーを権限付与対象ごとに定義し，データ利活用時はアクセスポリシーの範囲に該当するデータのみをフィルタリングするデータアクセス制御方式を提案する．

Data Access Control Method on Information Management Platform for Smart Cities

Yohei KAWADA[†1]　Kojin YANO[†1]
Yoshihiro MIZUNO[†2]　Hirofumi TERADA[†1]

In the smart city projects which make urban infrastructures “smartize”, a new access control technology to offer appropriate user’s data to the appropriate application is required. In this paper, we analyze characteristics and problems of the data access in the smart city and define three requirements for data access control. Next we propose access policies which are satisfied those requirements. The access policies are consisted of an access authority and access conditions. The access authority is defined by general items in data access contracts. The access conditions are defined by data items which are in the target information of the access. Finally we implement data access judgment processing based on access policies.

1. はじめに

近年，低炭素化社会の実現に向けた再生可能エネルギーや EV(Electric Vehicle)などの大量導入に伴う電力の安定供給や効率的な発電，需要予測を含んだ「スマートグリッド」に関する取り組みが進められている．最近では，電力のみならずエネルギー，水，交通などの都市インフラ全てをスマート化する「スマートシティ」構想が注目を集めており，日本を含めた一部の国で実証実験も始まっている [1]．ここでいうスマート化とは，近い将来の開発途上国における都市人口の爆発的増加，および先進国におけるエネルギーや水道，交通などの都市インフラ設備の老朽化に対し，IT を用いることで都市の住民の利便性を損なわずに効率性の高い都市生活を実現することを意味する．特にスマートシティの中心的な取り組みである電力分野においては，都市人口の増加・生活水準の向上により需要の重負荷（ピーク）時と軽負荷時との差が拡大する．重負荷時に合わせて供給側の設備を用意し運用しようとすると膨大な設備投資，運用・メンテナンスのための人員が必要になり，非効率である．この問題に対し，大口需要家のみならず小口需要家を含めた需要量を細かく把握することで，需要家の利便性を損なわない範囲で需要量のピークカット・ピークシフトを行うことにより，電力需要量の平準化を実現し，供給側の設備・人員を抑制することが求められている．また，低炭素化を目的とした太陽光発電等の分散型電源の大量導入に伴い，需要量だけでなく供給量も細かく把握し，それに合わせて需要量を調整することで，供給電圧低下や停電などの発生を防止し需要家の利便性を損なわないようにすることが求められている [2]．

上記のような都市インフラのスマート化を実現するために IT に求められる役割として，機器や設備からの時々刻々と変化する需要量・供給量のリアルタイムでの情報取得，取得した情報を収集・管理しゲートウェイサービスとして情報利活用者へ情報提供を行う情報管理，提供された情報を活用した需要量・供給量の予測および需給調整を行う情報利活用の 3 つが挙げられている．そしてこれらをそれぞれセンサ層，システム層，サービス層に対応させるスマートシティ向けのシステムアーキテクチャが提案され，特にシステム層については，多種多様なセンサ層の機器・設備と接続して情報を収集し，サービス層の各種アプリケーションにそれらの情報を提供することで需給調整を初めとする様々なサービスを実現する情報管理基盤により実現することが提案されている [3)6)]．

情報管理基盤に求められる機能として，機器・センサごとに異なるデータフォーマットや項目の変換・共通化のほか，情報の利活用者に対する情報提供においては，需要者との契約等に基づき，適切な利活用者に対してのみ情報を

†1 (株)日立製作所　横浜研究所
Yokohama Research Laboratory, Hitachi Ltd.
†2 (株)日立製作所　情報・通信システム社
Information & Telecommunication Systems Company, Hitachi Ltd.

Vol.2012-DPS-152 No.28
Vol.2012-GN-85 No.28
Vol.2012-EIP-57 No.28
2012/9/14

提供するアクセス制御が必要とされており，そのあり方が論じられている [1]．例えば電力分野においては，従来の需要家－電力事業者の二者間のビジネスモデルから，需要家の電力使用情報を活用して使用量の見える化や将来的にはデマンドレスポンス等を行う「アグリゲータ」と呼ばれる第三の事業者が介入するアグリゲータ事業者モデルが提案されている [4]．需要家はアグリゲータ事業者と個々に契約を結び節電対策や電力使用時間帯シフトの支援を受けることが想定されているが，アグリゲータ事業者に対しては，契約を結んだ需要家の電力使用量実績を契約の範囲に制限して参照を許可する必要がある．

以降，本報告では，特に電力分野を想定し，情報の利活用者に対する情報提供時のアクセス制御について述べる．なお，本報告では設備や機器から収集した履歴に関する情報を「実世界情報」と呼び，情報管理基盤を「スマートシティ向け情報管理基盤（SC 基盤）」と呼ぶこととする．

以下, 2 章では SC 基盤における実世界情報へのデータアクセスの特徴を整理し，それらからデータアクセス制御に対する要件を抽出する．3 章では，データアクセス制御に関する従来技術である RBAC(Roll-Based Access Control), およびそれを SC 基盤に適用した場合の問題点について述べる. 4 章では SC 基盤向けのデータアクセス制御方式として情報利活用者のロールと需要家－情報利活用者間の個々の契約の両方を考慮したデータアクセス制御方式を提案し, 5 章では提案方式を電力需要量情報管理へ適用した例について述べる．

2. SC 基盤におけるデータアクセスの特徴

2.1 実世界情報のアプリケーションへの提供形態

本報告が前提とする SC 基盤を含むシステム構成を図 1 に記す．この図が記すように，SC 基盤は機器や設備から送信された需要量・供給量に関する実世界情報を収集・管理し，それを各アプリケーションに提供する．本報告における実世界情報とは，前章にて述べたとおり設備や機器から収集したセンサの計測値やイベントの履歴情報を意味する．表 1 に実世界情報の例（データ種別 : 電力需要量情報）を記す．この例では，機器や設備をユニークに識別する「機器 ID」，機器の種類を表す「機器種別」，機器や設備の所有者を表す「所有者 ID」，計測した日時やイベントが発生した日時を表す「日時」, 機器や設備の状態を表す「消費電力」「積算消費電力量」「電源」を保持する．なお，「電源」は状態が変化した（ON から OFF，もしくは OFF から ON）場合にのみ値が格納され，その値は変化後の状態を表している．なお，電力需要量情報の他，電力供給量情報や機器稼動情報など，様々なデータ種別の実世界情報を SC 基盤で保持することが可能である．

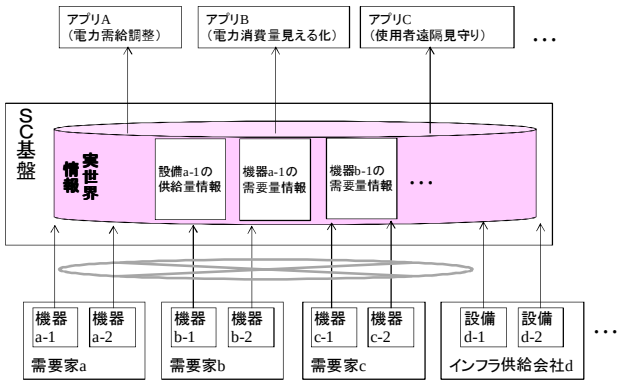

図 1　前提とするシステム構成

表 1　実世界情報の例

機器ID	機器種別	所有者ID	日時	消費電力(kW)	積算消費電力量(kWh)	電源
機器a-1	スマートメータ	需要家a	5/11 10:00:00	23	4500	
機器a-2	蓄電池	需要家a	5/11 11:00:00	30	20000	OFF
機器b-1	スマートメータ	需要家b	5/11 10:00:00	103	85500	
機器b-2	給湯器	需要家b	5/12 12:00:00	5	10002	ON

SC 基盤がこの実世界情報をアプリケーションに提供する際の提供方式は大別して以下の二つである．

- プッシュ型（イベントドリブンを想定）

機器や設備から送信された実世界情報に対し，指定の項目の閾値が超えている場合など任意の条件に合致したイベントを検出した場合に，その内容をアプリケーションに通知する形態である. SC 基盤がトリガーとなって行う情報提供の形態である．例えば，機器の電源状態の変化を把握してその機器の使用者の生活が問題なく営まれているかを把握する使用者遠隔見守りアプリケーションが該当する．

- プル型（バッチを想定）

SC 基盤に蓄積されている実世界情報に対し, アプリケーションがそれぞれ指定の検索条件に該当する実世界情報をアプリケーションの任意のタイミングで取得する形態である．例えば，昨日 1 日分の需要家の電力使用量を日が変わったタイミングで纏めて取得し，その使用量情報を分析して翌日の電力使用量予測を行う電力需給調整アプリケーションなどが該当する．また，使用者遠隔見守りアプリケーションについても，活動履歴のレポートを任意のタイミングで情報提供先に送信する場合はこちらに該当する．

上記のうちプッシュ型についてはあらかじめイベント通知条件にて設定されたアプリケーションに対し設定された内容の情報提供を行うことと想定し，本報告の対象外とする．次節以降はプル型の情報提供において，データアクセスの特徴を整理する．なお，以降では実世界情報のことを単にデータとも記す．

Vol.2012-DPS-152 No.28
Vol.2012-GN-85 No.28
Vol.2012-EIP-57 No.28
2012/9/14

2.2 プル型提供におけるデータアクセスの特徴と課題

SC 基盤がアプリケーションに対しプル型でデータを提供する際の特徴として,以下(1)(2)(3)の 3 つが挙げられる.

(1)アクセス権限付与対象とデータ所有者ごとの契約内容に基づくアクセス権限定義

どのようなデータならばアプリケーションが参照可能かどうかは，アプリケーションを提供するサービス事業者とデータの所有者（データを誰に提供するかを決める権限を所有する者）との間の契約内容に依存する．データの所有者になりうるのは，スマートメータ等を設置し SC 基盤を運用する電力会社などのほか，昨今の個人情報保護に対する社会的要請を鑑みると，インフラの需要家が所有者ともなりうる．特に後者の場合，サービス事業者のアプリケーションにどの範囲までのデータ参照を許可するか，の条件は契約ごとに異なる（図 2 参照）．たとえば，以下の想定アプリケーションでは参照可能なデータの範囲が以下のようにそれぞれ異なる．

- 電力需給調整アプリ A

需要家単位での需給調整を行うため，運用事業者と「すべての需要家の機器種別が「スマートメータ」のデータが参照可能 」という契約を締結する. 例えば図 2 の例では，機器種別が「スマートメータ」のデータのみ参照可能である．

- 電力消費量見える化アプリ B

需要家ごとに契約を締結．どの機器のデータが参照可能かは，需要家との契約内容（どの機器を見える化の対象とするか）による．例えば図 2 の例では，需要家 a と電力消費量見える化情報を提供する契約を締結し，その対象が機器 a-1，機器 a-2 であるため，これら二つの機器のデータのみ参照可能である．

- 使用者遠隔見守りアプリ C

機器の使用状態により機器の使用者(=需要家)の生活が問題なく営まれているかを把握し，その内容を使用者の家族等の情報提供先に提供する.需要家ごとに契約を締結し，見守り対象の需要家の，契約上指定された機器の契約期間中のデータのみ参照可能である．例えば図 2 の例では，見守り対象として需要家 b と契約し，需要家 b が所有する機器 b-2 の状態を把握し情報提供先に提供する．したがって，機器 b-2 の契約期間中の日時のデータのみ参照可能である．

図 2　アクセス可能なデータの例

以上より, SC 基盤ではさまざまな契約形態に基づいたアクセス権限定義に対応できる必要がある．

(2)アクセス権限有無の判定対象となるデータの件数が大量

電力見える化アプリケーションが電力使用量の推移グラフを描画し需要家に提供するため,「地域内の全需要家の機器の使用電力」のような要求を受け付けた場合，SC 基盤の中で要求に該当するデータを検索する処理時間は主に「アプリケーションが指定した検索条件に該当するデータを検索する処理時間」と「検索条件に該当したデータに対しアプリケーションがアクセスする権限の有無を判定する処理時間」で構成される．この場合，前者の検索条件に該当するデータが大量となると，後者の処理時間はその量に比例して増大する可能性がある．

たとえば, 1 つの情報管理基盤で管理する世帯数を 10 万世帯と想定し，1 時間ごとに積算消費電力量の推移を把握しようとした場合，1 需要家あたり機器 10 個，収集間隔が 3 分に 1 回の場合，1 需要家の 1 時間分のデータは 200 件，全需要家とすると 2 億件となり，この中からアプリケーションが指定の検索条件に該当するデータを提供する．今後予想される都市内の爆発的な人口増加や，機器数の増大，機器からの収集頻度の増加，アプリケーションへの提供頻度の増加により，アプリケーションに提供する単位時間当たりのデータの件数は爆発的に増加する可能性がある．この場合，アクセス権限有無判定の処理のための時間も大量になる可能性がある．

(3)さまざまなアプリケーションの要求に対応可能な，汎用的な検索条件の指定が可能な検索インタフェース（I/F）への対応が必要

スマートシティで想定されるアプリケーションの 1 つに，機器や設備から収集したデータを活用してそれらの保守やメンテナンスに活用するサービスが期待されている．これは，アプリケーションが対象機器の実世界情報を参照することで，異常の検出やメンテナンス・リプレースのタイミングの判定を行うものである．この場合，アプリケーションのデータ検索条件としては以下のパターンが考えられる．

・契約を締結した需要家の機器
・契約対象の機器
・契約対象のロケーションに設置された機器
・動作情報中の任意項目の値の範囲（異常値など）
・機器メーカが保守も請け負う場合，そのメーカが製造した機器
・前回検査時以降に登録された動作情報

上記のように機器の保守・メンテナンスだけでもさまざまな検索条件のパターンが考えられる．将来的には多種多

Vol.2012-DPS-152 No.28
Vol.2012-GN-85 No.28
Vol.2012-EIP-57 No.28
2012/9/14

様なサービスの出現が考えられるが，それらのデータ参照要求に対応するためには，データ検索の I/F はできるだけ汎用化する必要がある．また，アプリケーションからの要件の追加・変化に伴い，今後検索 I/F の種類が拡張される可能性もある．このような場合でもアクセス制御を適用するためには，アクセス制御の仕様は I/F の仕様とは独立したものとする必要がある．

2.3 SC 基盤におけるデータアクセス制御の要件

前節で述べた特徴により，SC 基盤が備えるデータアクセス制御の要件は以下と考えられる．

① アクセス権限付与対象とデータ所有者ごとのさまざまな契約内容に基づいたデータアクセス権限を設定できること．（要件①）
② アプリケーションへの提供候補となる実世界情報の件数によって，権限有無判定のための処理時間が大量に増加しないこと．（要件②）
③ 汎用的な検索 I/F，および今後の I/F 拡張に対しても適用可能なアクセス制御であるために，I/F の検索条件等の仕様とは独立したものであること．（要件③）

3. 従来研究

本章ではデータアクセス制御の従来技術である Role-Based Access Control(RBAC)について述べるとともに，それを SC 基盤に適用した場合の問題点について述べる．

3.1 Role-Based Access Control(RBAC)

現在アクセス制御方式として広く普及している Role-Based Access Control(RBAC)[5]は，「データアクセスの権限は個々のユーザにではなく，仕事の役割（ロール）に対して割り当てられるべきである」という概念に基づいたアクセス制御方式である．ロールに対して権限が割り当てられ，ユーザとロールが多対多で関連付けられることにより，ユーザに複数のロールを割り当てられる．また，ロールの階層構造をもつことにより，下位のロールを上位のロールが継承することができる．これらの手法をとることで RBAC は複雑なアクセス制御を可能とし，特に組織内のユーザの権限を管理するのに非常に適した方式である．

3.2 RBAC の SC 基盤への適用

SC 基盤のデータアクセス制御への RBAC の適用を検討する．データ所有者が運用事業者である場合や需要家間でアプリケーションに付与する権限に差がない場合は RBAC をそのまま適用可能である．例えば，前章で述べた電力需給調整アプリ A に対しては「電力需給調整」というロールを定義する．このロールには機器種別が「スマートメータ」であるデータのみ参照権限を付与することで，電力需給調整アプリ A はスマートメータのデータのみ参照可能となる．アプリ A を提供する事業者とは異なる事業者から同じように需要家単位での電力需給調整を行うアプリ A’が提供された場合，このアプリ A’に対しても同じロール「電力需給調整」を割り当てることで，同様にスマートメータのデータのみ参照可能となる．このように，ロールの役割を果たすのに必要な範囲のアクセス権限をロールに対し定義することで，アプリケーションが必要とする最低限の範囲にデータ参照を限定することが可能になる．同じロールでも必要なデータの範囲が異なる場合には別のロールを定義することになるが，データ所有者とアプリケーションの関係は１：N なので，最大 N 個のロールを定義することになる．

一方，データ所有者が各需要家の場合で，需要家ごとにデータ提供の範囲に関する契約内容が異なる場合には，前述の要件①のようにアプリケーションを提供する事業者と各需要家との個々の契約内容に基づいたアクセス制御が必要である．RBAC を適用しようとすると，需要家の観点から各アプリケーションに対しロールを定義することは可能であるが，需要家とアプリケーション提供事業者ごとに契約内容が異なるため，需要家間でアプリケーションに定義するロールが異なる．例えば図 3 の例では，需要家 a から見れば電力消費量見える化アプリ B は所有するすべての機器の消費量見える化を行うロールであるのに対し，需要家 b から見れば照明とエアコンのみ消費量見える化を行うロールである．このようなアクセス権限の定義を RBAC で実現しようとすると， 図 3 に示すように，需要家とアプリケーション事業者間の契約ごと，最大 M：N の組合せの数だけロールを定義することになる．これは，アクセス権限付与対象にロールを紐付け，そのロールに対し権限を割り当てることで定義する権限の数を低減し，運用を簡略化できるというロールの利点が生かされないことを意味する．

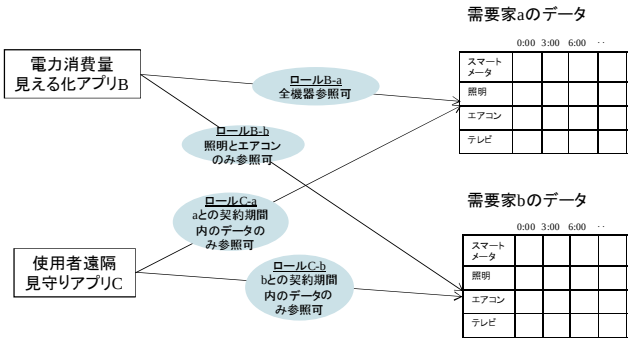

図 3 RBAC を SC 基盤のアクセス制御に適用した例

次に，要件②の観点から RBAC の適用可能性を検討する．需要家とアプリケーションを提供する事業者とが個々にデータ提供に関する契約を締結している環境において，あるアプリケーションが特定の需要家のみのデータを要求した場合，そのアプリケーションと需要家との間のロールに定義された権限の範囲に該当するデータと，検索条件に該当

Vol.2012-DPS-152 No.28
Vol.2012-GN-85 No.28
Vol.2012-EIP-57 No.28
2012/9/14

するデータの AND がアプリケーションに提供するデータとなる．ここで複数の需要家に跨るデータを要求された場合，需要家によってアプリケーションに定義されたロールが異なると，検索条件に該当するデータに含まれる需要家ごとにロールに割り当てられた権限の範囲か否かを判定する必要がある．需要家の数だけこの処理を行う必要があるため，需要家が多くなるとそれだけ権限有無判定のための処理時間が必要になる．これを避けるために，アプリケーションからの検索では需要家一つに限定した検索のみ許可するという制限を設けると，これは要件③で述べた検索 I/F の検索条件の仕様に制限を加えることになり，検索 I/F の拡張性がアクセス制御の仕様により制限されることになる．

以上により，SC 基盤のデータアクセス制御方式としては，RBAC は前章で述べた要件を十分に満たしているとは言えない．

4. データアクセス制御方式の提案

2 章にて導出された 3 つの要件を踏まえ，権限付与対象者ごとにアクセス可能なデータの範囲を指定した「アクセスポリシー」を定義し，権限付与対象者からのアクセス要求時にこのアクセスポリシーを参照することでデータの取得や書込みを許可するデータアクセス制御方式を提案する．なお，アクセス制御の対象とするデータは 2.1 に記載の実世界情報とする．

4.1 提案するアクセスポリシーの定義方式

2 章で導出した要件①では，権限付与対象者とデータ所有者との間の契約内容に基づいたアクセス権限を設定することが求められている．そこで，以下の方針に基づいたアクセスポリシーの定義方式を提案する．

＜方針①＞

契約内容は例えば契約期間のような「実世界情報の内容とは無関係の内容」と，参照可能とする機器や機器種別，日時など「実世界情報の内容に関する内容」の 2 つから構成されると考え，前者と後者を分けてアクセスポリシーの設定を行うこととした．前者についてはデータアクセスの契約にかかわる一般的な項目（契約期間，アクセス対象データ種別）でのアクセス権限の定義を行うこととする．また，後者については，さまざまな実世界情報のデータ種別に対応できるアクセスポリシーの定義が可能なように，アクセス対象のデータが保持するデータ項目名とその値の組合せでアクセス可否の条件を指定できるようにする．

＜方針②＞

要件③では，検索 I/F の仕様に依存しないアクセス制御であることが求められている．そこで，アクセスポリシーに実世界情報のデータ項目名を指定して定義することで，アクセス制御対象とする実世界情報のテーブルが保持するデータ項目に基づいたアクセスポリシーの定義を行うこととする．これはアクセスポリシーがアクセス対象とする実世界情報のテーブル定義に基づいて定義されることを意味し，テーブル定義と検索 I/F が独立していれば，検索 I/F の仕様とは独立したアクセスポリシーの定義が可能となる．

以上の方針に基づき提案するデータアクセス制御方式におけるアクセスポリシーについて説明する．アクセスポリシーは，アクセス権限とアクセス条件の二つより構成する．アクセス権限の例を表 2 に，アクセス条件の例を表 3 に記す．

アクセス権限は，1 つのレコードが 1 つの権限付与対象（アプリケーションもしくはロール）に対し付与される権限（任意のデータ種別に対し実行可能なアクセスの種類（参照，登録等）の組合せ）を表し，権限を一意に特定する権限 ID，権限付与対象がロールか否かを表すロール，権限の対象であるアプリケーションなどの権限付与対象，権限の有効期間，実行可能なアクセスの種類を表す権限内容，権限の対象となるデータの種別を表す対象データ種別，権限の対象となるデータの登録日時の期間を表すデータ登録期間，を保持する．同一の権限付与対象に対しては権限内容，対象データ種別のいずれかが異なれば複数のレコードが保持可能とする．権限の有効期間はアプリケーションを提供する事業者とデータ所有者との契約期間に一致する．

アクセス条件はアクセス権限に紐づき，アクセス権限に定義された権限が有効となるデータの条件を意味する．これは，アクセス条件にて定義されている内容と合致するデータであれば，アクセス権限にて定義されている範囲でアクセスが可能であることを意味する．1 つのレコードが 1 つの条件（項目名と値の組合せ）を表し，紐づく先のアクセス権限を表す権限 ID，条件の対象となるデータ項目名を表す項目名，条件の種別を表す条件種別，項目名の項目に保持されている値，を保持する．1 つのアクセス権限に対し複数のアクセス条件の紐付けが可能であり，その場合は同じ項目名に対する条件であれば OR 条件，異なる項目名に対する条件であれば AND 条件とする．

たとえば，表中の権限 ID「1」の例では，権限付与対象である「アプリ A」のアクセス権限として，電力需要量情報の参照が可能と定義されている．ただしその条件として，電力需要量情報のデータ項目である「機器 ID」の値が「機器 a-1」もしくは「機器 a-2」に一致する電力需要量情報のみ参照可能であることを意味する．データ登録期間の指定がないため，アクセス条件を満たすすべてのデータ登録日のデータが参照可能である．同様に，権限 ID「2」の例では，「機器種別」が「スマートメータ」であれば，全ての需要家の電力需要量情報が参照可能であることを意味する．

Vol.2012-DPS-152 No.28
Vol.2012-GN-85 No.28
Vol.2012-EIP-57 No.28
2012/9/14

表 2　アクセス権限

権限ID	ロール	権限付与対象	有効期間（開始）	有効期間（終了）	権限内容	対象データ種別	データ登録期間(開始)	データ登録期間(終了)
1	false	アプリA	2012/1/1		参照	電力需要量情報		
2	false	アプリB	2012/3/1	2012/12/31	参照	電力需要量情報	2012/3/1	2012/12/31
3	false	アプリC	2012/1/1		参照	電力需要量情報		
4	false	アプリD	2012/4/1	2013/3/31	登録	電力需要計画情報		
5	true	ロールE	2012/4/1		参照	電力需要計画情報		

表 3　アクセス条件

権限ID	項目名	値
1	機器ID	機器a-1
1	機器ID	機器a-2
2	機器種別	スマートメータ
3	所有者ID	供給者d
5	機器種別	照明

また，アクセス権限の権限付与対象にロールを定義し，ロールとアプリケーションとの関係を表 4 に示す関係情報にて保持することで，ロールごとにアクセス権限を定義することも可能になる．例えば表 2 の例では，権限 ID「5」の権限付与対象に「ロール E」が指定されている（権限付与対象にロールが定義されている場合は，項目名「ロール」に true を指定する．それ以外の場合は false を指定）．ロール E を割り当てられたアプリケーションは表 4に記載のようにアプリ F およびアプリ G であるため，アプリ F とアプリ G は権限 ID「5」のアクセス権限およびそれに紐づくアクセス条件に該当するデータが参照可能である．ただし，各アプリケーションにロールが割り当てられる期間を関係期間として保持し，その関係期間内であればアプリケーションは割り当てられたロールのアクセスポリシーを付与されることとする．

表 4　関係情報

ロール	アプリケーション	関係期間（開始）	関係期間（終了）
ロールE	アプリF	2012/1/1	
ロールE	アプリG	2011/4/1	2012/3/31

4.2 アクセスポリシーに基づく権限有無判定の実装方式

要件②では，アプリケーションへの提供候補となる実世界情報の件数によって権限有無判定の処理のためのリソースが大幅に増加しないことが求められている．そこで提案方式では，アクセスポリシーを基にした SQL(Structured Query Language)を生成し，それを実行することで実世界情報を SC 基盤内部の RDBMS(Relational DataBase Management System)にてフィルタリングし，そのフィルタリングの結果に対してアプリケーションが指定した検索条件に基づく検索を実行することとする．これにより，権限有無判定の処理を RDBMS 内にて実施することとなり，SC 基盤の独自処理として権限有無判定の処理を行う必要がなくなる．RDBMS 内での処理であれば，インデックスの定義により処理高速化が可能であるため，処理時間を抑制することができる．

以上の方針に基づき，前節で提案したアクセス権限定義の実装方式について説明する．アプリケーションから参照要求があった場合の SC 基盤の処理のフローチャートを図 4 に記す．

① 参照要求を受信したら，参照要求を送信したアプリケーションの識別子を基に関係情報を検索する．該当するロールがあった場合，以降の処理手順では権限付与対象に取得したロールを指定する．ない場合は要求元のアプリケーションの識別子を権限付与対象とする．
② 権限付与対象を基にアクセスポリシーを検索し，該当するアクセス権限・アクセス条件を取得する．
③ ②で取得した内容を基にフィルタリング用の SQL(WHERE 句部分)を作成することが可能になる．作成する SQL の WHERE 句の内容を図 5 に記す．
④ アプリケーションが送信してきた検索条件に基づく SQL(WHERE 句部分)を作成する．
⑤ ③で作成した SQL の WHERE 句と，④で作成した SQL の WHERE 句とを AND 条件で組み合わせ，それを RDBMS に対して実行することにより，アプリケーションが付与された権限の範囲内に限定されたデータの中で，指定の検索条件に該当するデータを取得できる．
⑥ ⑤で取得したデータを要求元のアプリケーションにレスポンスとして返信することで，参照アクセス制御を実現する．

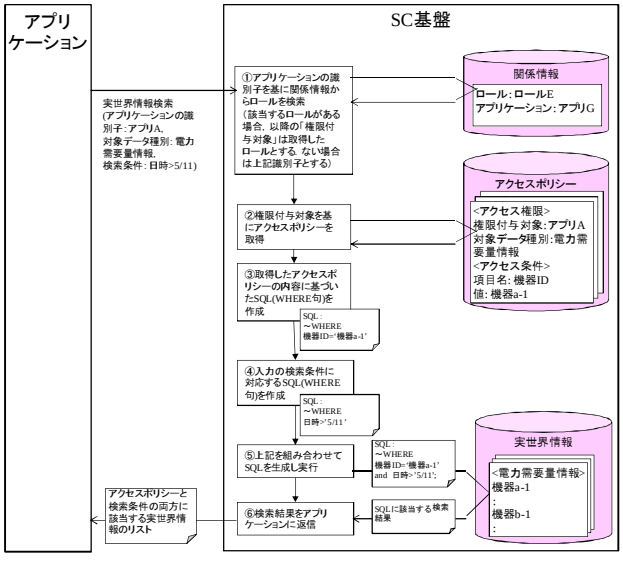

図 4　実世界情報参照時の処理のフローチャート

Vol.2012-DPS-152 No.28
Vol.2012-GN-85 No.28
Vol.2012-EIP-57 No.28
2012/9/14

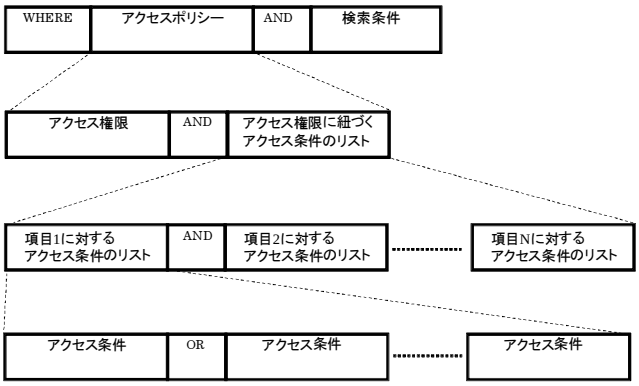

図 5　アクセスポリシーに基づく SQL(WHERE 句部分)

5. 電力需要量情報管理への適用

5.1 提案方式の適用と考察

前章で述べた提案方式を，電力需要量情報の管理に適用した場合を例に説明する．この場合，SC 基盤は機器の電力需要量情報を収集・管理し，これらのデータを利活用する 2.2(1)に記載のアプリケーションに提供する．各アプリケーションとデータ所有者との契約内容は以下のとおりである．

- 電力需給調整アプリ A

契約期間内において，機器種別が「スマートメータ」に一致する全ての需要家の電力需要量情報が参照可能．

- 電力消費量見える化アプリ B

契約期間内において，契約している需要家の契約上指定された機器の電力需要量情報が参照可能．

- 使用者遠隔見守りアプリ C

契約期間内において，契約している需要家の契約上指定された機器の契約期間中の日時の電力需要量情報のみ参照可能．

上記の契約内容に基づいたアクセスポリシーの定義内容を表 5，表 6，表 7 に示す．

アプリ A は全ての需要家のデータが参照可能であるため，表 7 の関係情報にてロール D を定義し，そのロールにアプリ A を紐付ける．関係期間はアプリ A とデータ所有者(SC 基盤運用者)との契約期間を指定する．ロール D は機器種別が「スマートメータ」に一致する電力需要量情報の参照が可能な契約であるため，表 5 のアクセス権限の権限 ID が「1」のレコードにて権限内容に「参照」を，対象データ種別に「電力需要量情報」を指定する．有効期間にはそのロールを有効とする期間を指定する．また，機器種別が「スマートメータ」に一致するデータは参照可能な契約であるため，表 6 のアクセス条件にて権限 ID に「1」，項目名に「機器種別」，値に「スマートメータ」と指定する．これらの定義により，全ての需要家のスマートメータの電力需要量情報が参照できる．

アプリ B は契約する需要家 a の，契約上指定された機器「機器 a-1」「機器 a-2」の電力需要量情報が参照可能であるため，ロール D の場合と同様に表 5 のアクセス権限の権限 ID「2」のレコードにて権限内容に「参照」，対象データ種別に「電力需要量情報」，有効期間にその契約期間を指定する．表 6 のアクセス条件の権限 ID に「2」，項目名に「機器 ID」，値に「機器 a-1」，さらに権限 ID と項目名は同じで値に「機器 a-2」となる 2 つのレコードを定義する．この定義により，アプリ B と契約する需要家 a の 2 つの機器については電力需要量情報の参照が可能である．

アプリ C は契約期間中の日時の電力需要量情報のみ参照可能な契約であるため，表 5 のアクセス権限の権限 ID「3」のレコードにて有効期間，権限内容，対象データ種別の指定のほか，データ登録期間に契約期間を指定する．また，契約している需要家の特定機器（機器 c-1，機器 e-2）の電力需要量情報の参照が可能な契約であるため，アプリ B の場合と同様に表 6 のアクセス条件の権限 ID「3」のレコードとして項目名に「機器 ID」，値に「機器 c-1」，「機器 e-2」を指定する．この定義により，アプリ C は契約している需要家の特定機器の契約期間中の日時の電力需要量情報のみ参照可能となる．

以上により，上記の 3 つのアプリケーションのアクセス制御を実現可能である．この結果から，電力需要量情報管理にて想定する一部アプリケーションについて提案方式は 2.3 に記載の要件①を満たす．

表 5　アクセス権限の定義例

権限 ID	ロール	権限付与対象	有効期間（開始）	有効期間（終了）	権限内容	対象データ種別	データ登録期間（開始）	データ登録期間（終了）
1	true	ロールD	2012/4/1		参照	電力需要量情報		
2	false	アプリB	2012/4/1		参照	電力需要量情報		
3	false	アプリC	2012/4/15	2012/7/31	参照	電力需要量情報	2012/4/15	2012/7/31

表 6　アクセス条件の定義例

権限ID	項目名	値
1	機器種別	スマートメータ
2	機器ID	機器a-1
2	機器ID	機器a-2
3	機器ID	機器c-1
3	機器ID	機器e-2

表 7　関係情報の例

ロール	アプリケーション	関係期間（開始）	関係期間（終了）
ロールD	アプリA	2012/4/1	

また，要件③について，表 8 に記す汎用的な検索 I/F を用意し，実際にデータアクセス制御が定義どおりに動作するかを確認した．

Vol.2012-DPS-152 No.28
Vol.2012-GN-85 No.28
Vol.2012-EIP-57 No.28
2012/9/14

表 8　検索 I/F の例

I/F 名	実世界情報検索
引数	アプリケーションの識別子
	対象データ種別
	検索条件リスト(複数指定の場合は AND)
	検索条件
	検索条件指定項目 検索条件の対象となるデータ項目名
	対象境界値リスト(複数指定の場合は OR)
	対象境界値 検索条件指定項目で指定する項目に対する境界値
	対象境界値条件 対象境界値で指定する値に対する条件.”一致”,”以上”,”以下”,”未満”,”より大きい”のいずれかを指定する.
戻り値	検索条件に該当する実世界情報リスト
	実世界情報

実際に上記の検索 I/F を Java で実装し電力需要量情報の検索処理を実行したところ，引数で指定のアプリケーションに付与された参照権限の範囲のデータのみ戻り値のデータに含まれていることを確認した．これにより，提案方式は 2.3 に記載の要件③を満たしている．

2.3 に記載の要件②については，前章にて述べたように検索条件とアクセスポリシーに該当するデータの検索はいずれも SQL にて実施するため，SC 基盤の中の RDBMS よりも上位のレイヤで権限有無判定処理を実施することによる処理時間の増大は回避できるが，最終的な性能は RDBMS に依存することになる．性能向上のためインデックスの定義等によるチューニングにて対応することが必要になると考えられる．

5.2 今後の課題

前節にて述べたように，要件②に対応する RDBMS のチューニング方法について検討する必要がある．ただし性能向上のための具体的なチューニング方法は採用する RDBMS 製品によって異なるため，実システムにて実証する必要がある．

また，提案方式によるアクセスポリシーの定義では少なくとも以下の制限が存在することが分かっている．

- アクセス条件に指定のデータ項目が同一の場合は OR 条件，異なる場合は AND 条件となる．従って，仮に実世界情報が保持する異なる項目間で OR 条件となる契約が存在する場合は現状の実装方式では対応できない．
- 関係情報にロールが割り当てられたアプリケーションは，そのロールに対し定義されたアクセスポリシーのみが有効となる．

上記の制限により定義できないアクセスポリシーが存在するが，現時点の検討の範囲においては上記の制限が問題となるアプリケーションは見つかっていない．

また，本報告では実世界情報の参照に関するデータアクセス制御のみについて論じたが，需要家や機器に対する計画や制御指示などをアプリケーション側から SC 基盤に登録するケースについてもアクセス制御方式を検討する必要がある．

6. おわりに

本報告ではスマートシティ向け情報管理基盤のデータアクセス制御について 3 つの要件を整理し，従来技術として RBAC を適用した場合の問題点について述べるとともに，それらの要件を満たすデータアクセス制御方式を提案した．提案方式では，実世界情報の内容とは無関係の契約内容を保持するアクセス権限と，実世界情報の内容に関する契約内容を保持するアクセス条件の 2 つでアクセスポリシーを構成することで，ロールに基づくデータアクセス制御では不十分であったアクセス権限付与対象とデータ所有者との個々の契約内容に対応するアクセス権限の定義を可能とする．また，アクセス権限判定処理ではアクセスポリシーに該当する実世界情報のフィルタリングを RDBMS 内で実施することで，権限判定処理時間の大幅な増加を回避する．

今後は，前章で述べた課題への対応を必要性も含めて検討するとともに，提案方式を適用した実システムの実証実験等により提案方式の妥当性，十分性について評価を進めていく．

参考文献

1) M.Naphade, G.Banavar, C.Harrison, J.Paraszczak and R.Morris, Smarter Cities and Their Innovation Challenges, IEEE Computer, 44(6), pp.32-39,(2011).
2) S.Karnouskos, Demand Side Management via Prosumer Interactions in a Smart City Energy Marketplace, Proceedings of IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies(ISGT Europe), pp.1-7,(2011).
3) J.Lee, S.Baik and C.Lee, Building an Integrated Service Management Platform for Ubiquitous Ecological Cities, IEEE Computer, 44(6), pp.56-63, (2011).
4) National Institute of Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, (2010)
5) R.S. Sandhu, E.J.Coyne, H.L.Feinstein, and C.E.Youman, Role-Based Access Control Models, IEEE Computer, 29(2), pp.38-47 (1996).
6) 水野善弘，矢野浩仁，大河内一弥，真下祐一，社会インフラを支える IT 基盤，日立評論，Vol.93，No.12，pp.58-63 (2011).