スマートコミュニティにおける プライバシー保護規制と対策技術

Development of Technologies Corresponding to Privacy Regulations in Smart Communities

森尻　智昭　　小島　健司
■MORIJIRI Tomoaki　■KOJIMA Kenji

スマートコミュニティでは，電気や，水，交通，物流，医療，情報などの統合的な管理と最適制御を，ICT（情報通信技術）を活用することで実現しようとしている。そのためには，住民のプライバシーに関連した多くのデータを扱う必要がある。現在，特にスマートメータからのデータ収集に関して，多くの国や地域でプライバシー保護に関する規制の制定が進められている。今後，プライバシー保護の動きは，スマートコミュニティ全体に広がっていくと考えられる。

そこで東芝グループは，スマートコミュニティを実現する様々なシステムに必要となる，プライバシー保護規制に対応するための技術を開発している。

Smart communities are aiming at the integrated management and optimized control of electric power, water, transportation, logistics, and information through the application of information and communication technologies (ICTs). As ICT systems deal with various data containing the private information of residents in a smart community, privacy protection regulations for smart meter data in particular are being enacted in many countries and regions. In the future, privacy protection regulations will expand to all types of data handled in a smart community.

With these circumstances as a background, the Toshiba group is engaged in the development of technologies for privacy protection that are necessary when an integrated system for a smart community is constructed.

1　まえがき

東芝グループでは，スマートコミュニティを，電気や，水，交通，物流，医療，情報など，あらゆるインフラの統合的な管理と最適制御を実現した次世代のコミュニティと位置づけて取り組んでいる。これにより，環境に配慮した持続可能な社会と，快適な生活との両立を目指している。

スマートコミュニティでは，行政機関，管理団体，及び関連企業が，今までと比較してより多くの住民情報を扱うようになる。その情報の中には，住民の生活パターンや経済活動など，個人のプライバシーに関連した多くの情報が含まれる可能性が指摘されている[(1)]。また，これらの情報は単一の機関や，団体，企業内にとどまっているわけではなく，都市インフラの最適化を行うため互いに交換されることになる。更に，今後は，コンピュータ資源を有効利用するために，インターネットを介したクラウドコンピューティングの利用も想定されており，プライバシー侵害への懸念がより高まっている。

健全なスマートコミュニティの導入と発展のためには，利用者が安心して各種サービスを利用できることは必須であり，プライバシーの保護は避けては通れない課題である。これに対して，現在，プライバシー保護に関する規制の検討が多くの国や地域で進められている。

東芝グループのスマートコミュニティ事業においても，このようなプライバシーを含む情報を扱うことになる。したがって，それぞれの国や地域のプライバシー保護に関する規制を理解したうえでシステム化を進めていく必要があり，規制に対応するための技術的課題を明確にして，それを解決するための技術の開発を進めている。

ここでは，まず，スマートコミュニティでのプライバシー保護に関する規制，特に世界で整備が進みつつあるスマートメータに関連した規制について整理する。続いて，それらの規制に対応するために開発を進めている技術について述べる。

2　スマートメータデータのプライバシー

スマートコミュニティの中でも，電気やガスなどのエネルギー分野は特に重要な位置を占めている。この分野では，各家庭の電気やガスの消費量を短い周期で自動収集できるスマートメータの導入と，収集した消費量を活用したサービスの検討が各国で進められている。例えば，消費量を短周期で収集することにより，直近の消費量の把握と，需要量の予測が可能になる。この値をもとに，リアルタイムに電気やガスの価格を変動させたり，住民に対して省エネの提案をしたりすることで，電気やガスの需要量の制御を行う。これにより，究極的には，エネルギー消費量を社会全体で最適化できると言われている。わが国でも，2011年のエネルギー需給安定行動計画で，スマートメータの導入率を5年後に80 %としており，今後スマートメータの普及が進むと予想される。

しかし，短周期で電力・ガス消費量を収集することにより，その家庭の生活パターンが推測できる問題が指摘されている。例えば，平日の朝に電力・ガス消費量が急激に増えれば，その時間に朝食の準備を行っていると推測でき，その家庭の起床時間も推測できる。また，平日の夕方の電力・ガス消費量を見れば，その時間に家人が在宅しているかどうか推測することができる。つまり，電気やガスの消費量データには，その家庭の生活パターンというプライバシーに関する情報が含まれていることになる。

また今までは，消費量データは基本的に電力・ガス会社だけが利用するものであった。しかしスマートコミュニティでは，電気やガスの動的な価格付けや，顧客に対する省エネ提案などを行うために，それらのサービスを行う第三者企業にも消費量データが提供される可能性がある。つまり，顧客のプライバシーを含む情報が複数の企業で利用されることになる。

これらの理由から，スマートメータによる電気やガスの消費量データの収集方法や，収集した消費量データの管理方法などに関する規制が必要になってきている。わが国では，経済産業省や総務省などが中心になり，そのための議論が始められたばかりである。しかし，既にスマートメータの導入が進んでいる国や地域では，プライバシー保護や個人情報保護を目的とした法律をベースに，より実用的で具体的な規制を定めるための議論が進められている。

3　スマートメータデータのプライバシー保護規制の比較

スマートメータから収集する消費量データの取扱いに関する規制の制定が進められている国や地域としては，米国カリフォルニア州，EU（欧州連合），英国，フランス，カナダ オンタリオ州が挙げられる。これらの国や地域では，関連した複数の規制が存在しているが，代表的なものを**表1**にまとめる。

(1)　米国カリフォルニア州　　2010年9月の州法案SB 1476（Public utilities：customer privacy：advanced metering infrastructure.）の成立を受け，2011年7月にカリフォルニア州公益事業委員会（CPUC）が，消費者のプライバシー保護のためにカリフォルニア州内の電力・ガス企業3社が従うべき規制を定めている。

(2)　EU　　個人情報保護に関するEU指令（Directive 95/46/EC)に基づいて，EU第29条データ保護作業部会（WP29）が，スマートメータからの消費量データの収集がプライバシーに与える影響を分析している。WP29は2011年に，プライバシーを保護するための推奨事項をOpinion 12/2011 on smart meteringとしてまとめた。この内容に対して，2012年6月に，欧州データ保護管理局が追加の記載を求めており，今後，それを反映した新たな推奨事項がWP29から出されると思われる。

(3)　英国　　政府が電力の送電・供給企業に対して与えている免許事項に，スマートメータから収集した消費量データの取扱いに関する規制を加えることを検討している。規制事項案に対するパブリックコメントの受付けが2012年6月に終了したため，まもなく正式な規制内容が公開されるものと思われる。

(4)　フランス　　独立行政機関である，情報と自由に関する国家委員会（CNIL）が，公共部門と民間部門に対して個人情報に関する監視と監督を行っている。2010年12月に，CNILはスマートメータの設置についてプライバシーへの影響を抑えるための推奨事項を公表した。しかし，これは(2)のEUの推奨事項より前に出されているため，今後更に改定される可能性がある。

(5)　カナダ オンタリオ州　　オンタリオ州の情報・プライバシーコミッショナーが，スマートメータの導入に関してプライバシーを保護するための7原則を提言している。これは法的な拘束力を持つものではないが，他の国や地域でスマートメータデータのプライバシーに関する規制を策定する際に参考にされる機会が多い。

それぞれの規制での記載事項や，その粒度は異なっているが，全ての規制で共通に定められている要件を**図1**に示し，その内容を次に述べる。

表1．スマートメータデータのプライバシー保護規制
Privacy regulations for smart meter data

国・地域	規制文書のタイトル	発行者
米国カリフォルニア州	Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company	カリフォルニア州公益事業委員会（CPUC）
EU	00671/11/EN WP183 Opinion 12/2011 on smart metering	EU第29条データ保護作業部会（WP29）
英国	Electricity Supply Licence Condition, Electricity Distribution Licence Condition	英国政府
フランス	Recommendations for the deployment of electric "smart meters"	情報と自由に関する国家委員会（CNIL）
カナダ オンタリオ州	Privacy by Design The 7 Foundational Principles	情報・プライバシーコミッショナー

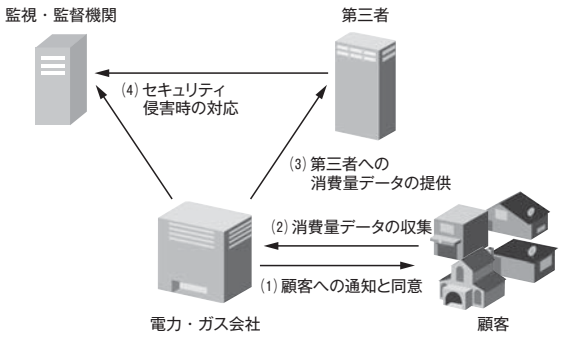

図1. スマートメータデータのプライバシー保護要件 ― スマートメータデータのプライバシー保護では，多くの国や地域の規制で4項目の要件が共通に定められている。

Requirements for privacy protection of smart meter data

(1) 顧客への通知と同意　　スマートメータによる消費量データの収集に先立って，顧客に対して文書により収集目的を通知し同意を得ておくことが，全ての規制で定められている。しかし，記載事項の粒度は，規制それぞれで異なっている。例えば，フランスでは「顧客が判断をするために必要な全ての情報を提示する」と抽象的であるのに対して，カリフォルニア州では，通知形式や，通知タイミング，通知内容，プライバシーポリシーに含める事項，利用目的に含める事項などが詳細に定められている。

また，いずれの国や地域でも，顧客が自身の消費量データについて，削除や修正を求めることを認めている。

(2) 消費量データの収集　　全ての規制で，スマートメータから収集する消費量データは，顧客に示した目的を達成するために必要最小限であることが定められている。更にカリフォルニア州と英国では，収集の目的ごとに具体的な収集周期も定められている。

(3) 第三者への消費量データの提供　　それぞれの規制で異なっている。

英国では，消費量データの収集時に同意した目的内であれば，顧客の再同意なく第三者への消費量データの開示が認められている。

フランスでは，第三者への消費量データの開示に関する規制は定められていない。しかし，個人情報保護法で，個人情報を取得する際には個人の同意が必要と定められている。そのため，消費量データの提供を受ける第三者は，顧客に対して同意を得る必要があると考えられる。

カリフォルニア州では，第三者への消費量データの開示が，電力・ガス消費量に対する課金を目的としている場合には，顧客からの再同意は必要ないとされている。しかし，課金に直接関係ない目的の場合には，顧客の再同意が必要とされている。個人の識別情報を取り除いた消費量データについては，規制の対象外とされている。

更にオンタリオ州とカリフォルニア州の規制では，消費量データの開示を受ける第三者は，データの開示元と同等か，それ以上のプライバシー保護を行うことが求められている。

(4) セキュリティ侵害時の対応　　カリフォルニア州では，セキュリティ侵害が発生した場合に，電力・ガス企業がとるべき行動や，CPUCへ報告する際の内容などについて，法律とは別に明確に定められている。

その他の国や地域では，セキュリティ侵害時の対応方法はスマートメータデータに関連した規制の中では定められていないが，個人情報保護法やデータ保護法で定められている。

4　スマートコミュニティでのプライバシー保護対応例

このようなプライバシーの問題は，前述したスマートメータに特化した問題ではなく，スマートコミュニティ全体の問題として考えなければならない。スマートコミュニティでは，電気やガス以外にも，水，交通，物流，医療など様々な領域で多くの情報が収集され，社会としての統合的な最適化が図られていく。その際には，プライバシーに配慮したシステムを構築していく必要がある。

例えば，一般家庭内での電力消費を最適制御するHEMS（Home Energy Management System）では，家庭内に設置された家電製品やセンサから，各機器の稼働状況や電力消費状況を収集する。続いて，これらのデータをもとに各機器の制御スケジュールなどを計算し，機器を制御することで，家庭内の電力消費量の最適制御を可能にしている。その際，家庭内から様々なデータを企業が収集する場合があり，これに対してはスマートメータと同様のプライバシーの問題が想定される。ここではHEMSを例に，前章の規制をベースにして，必要と考えられる対応について述べる。

(1) 顧客への通知と同意　　提供するサービスの内容や，そのために収集するデータの種類や収集周期などを，文書で顧客に通知し，同意を得ること。また，顧客に示す内容については，サービス提供地域の規制に従うこと

(2) 各種データの収集　　サービスを提供するために必要最小限のデータだけを収集すること。また，収集の周期については，サービス提供地域の規制を参考に，できるだけ粗い間隔とすること

(3) 第三者とのデータ交換　　サービス提供地域の規制に従って，第三者とのデータ交換が可能かを判断すること。また，収集したデータを第三者に開示する場合には，相手が自社以上のセキュリティ体制を保持していることを確認すること。逆に，第三者からデータ開示を受ける場合には，自社が相手以上のセキュリティ体制を保持している

ことを確認すること

(4) セキュリティ侵害時の対応　　監視・監督機関への報告など，サービス提供地域の規制に従って適切に対応すること

5 プライバシー保護規制に対応するための技術

スマートコミュニティを実現するための種々のシステムにおいて，プライバシー保護規制に対応するうえで重要になると考えられる技術について以下に述べる。

(1) システムがプライバシーに与える影響評価と対策

システムの設計にあたっては，システム内に保持しているデータの漏えいや改ざんがプライバシーに与える影響を，定性的あるいは定量的に測定するためのプライバシー影響評価手法（PIA：Privacy Impact Assessment）[2]の具体的な手順を確立する必要がある。また，システムで一貫したプライバシー保護を実現するために，設計段階でプライバシーを含む情報の収集から廃棄までを考慮するPbD（Privacy by Design）[3]の考え方を取り入れる必要がある。

PIAやPbDは，現在わが国をはじめ多くの国や地域で注目されており，今後広く普及していく可能性が高い考え方である。

(2) 情報開示先の認証　　個人情報を第三者に電子的に開示する際に，開示先と開示元が互いに正しい相手であることを，容易に確認できる技術が必要である。

また，開示先に対しては，開示元と同等以上のプライバシー保護が必要になる。様々な企業がスマートコミュニティに参加するためには，契約だけでなく，プライバシーポリシーの表現形式を定め，その内容の比較を自動的に行う技術が必要である。

(3) 目的外利用の確実な禁止　　個人情報は，基本的に顧客が同意した目的以外では使用できない。これを確実に行うためには，個人情報と利用目的をリンクさせ，目的外での利用を行えなくする技術が必要である。

(4) 個人によるアクセスと修正及び削除　　企業や組織が収集した個人情報に対して，その情報の提供元である本人がアクセスできるようにし，必要に応じて修正や削除をできるようにする必要がある。そのためには，個人情報が第三者に開示された場合でも，個人情報の所在を組織や企業を超えて追跡するための技術が必要である。

(5) データの匿名化　　個人情報を含む大量のデータから個人を識別するための情報を取り除き，統計処理などに必要なデータだけを残す，データの匿名化技術が必要である。匿名化されたデータは個人情報保護に関連した規制の範囲外となるので，多くの人が自由に利用できるようになる。これにより，様々な場面でデータ利用が容易になり，新たなサービスを創出できる可能性が高まる。

(6) 監査ログ　　監視・監督機関に報告したり，監視・監督機関からの調査に対応したりするためには，個人情報を含むデータのアクセスなどを記録するログシステムが必要になる。また，単にデータへのアクセス許可又は拒否を記録するのではなく，アクセスした際の目的なども併せて記録しておくことで，より厳密な管理が可能になる。

東芝グループは，各種のインフラシステムやデジタルプロダクツでこれまでに蓄積してきた技術を基に，これらの技術の開発を進めている。

6 あとがき

スマートコミュニティでは，行政機関や，管理団体，関連企業などが住民のプライバシーを含んだ多くのデータを扱うようになる。住民のプライバシーを保護するために一定以上のセキュリティを確保させるよう，これらの組織に対して規制が強化されていくと予想される。したがって，今後，これらの規制の動向を見極めて，必要な技術の開発を進めていく。

文　献

(1) National Institute of Standards and Technology (NIST). Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid. 2010-08, NIST IR 7628. <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf>, (accessed 2012-10-16).

(2) ISO 22307:2008. Financial services-Privacy impact assessment.

(3) Information & Privacy Commissioner, Ontario, Canada. Privacy by Design. <http://privacybydesign.ca/>, (accessed 2012-10-16).

森尻　智昭　MORIJIRI Tomoaki

東芝ソリューション（株）IT技術研究所 研究開発部研究主務。情報セキュリティ技術及び応用システムの研究・開発に従事。情報処理学会会員。

Toshiba Solutions Corp.

小島　健司　KOJIMA Kenji

東芝ソリューション（株）IT技術研究所 研究開発部研究主務。情報セキュリティ技術及び応用システムの研究・開発に従事。

Toshiba Solutions Corp.