

スマートメーターの法的課題

著者名(日)	湯浅 壱道
雑誌名	社会文化研究所紀要
巻	69
ページ	35-51
発行年	2012-03
URL	http://id.nii.ac.jp/1265/00000421/

スマートメーターの法的課題

湯 淺 壘 道

1. はじめに
2. スマートメーターとプライバシー
 - 2.1. 技術的可能性
 - 2.2. 技術的可能性
 - 2.2.1. 個人の行動パターン
 - 2.2.2. リアルタイムの行動調査
 - 2.2.3. 微細情報の集積
 - 2.2.4. 物理的な侵入
 - 2.2.5. プラグインハイブリッドカー
3. スマートメーターのデータの利用
 - 3.1. 利用目的
 - 3.2. 利用主体
4. プライバシー保護の方法
 - 4.1. 公開に関する同意
 - 4.2. 関税表モデル
 - 4.3. 消費者への通知
5. おわりに

1. はじめに

近年、わが国でもスマートグリッドが大きな注目を浴びるようになっていく。スマートグリッドとは、一般に発電所や送電網と、家庭や工場などの電力消費地をネットワークで接続し、電力技術とICT技術を利用して効率良く電気を供給することとされている。東日本大震災の後の大津波によって発生した

福島第一原子力発電所の事故の後、電力消費量の抑制が求められるようになっており、これまでエネルギー源の電力への転換を中心としてきたきらいのあった低炭素社会化への取り組みとの関連においても、スマートグリッドが脚光を浴びるようになってきている。

スマートグリッドにおいては、既存の電力計の代わりにスマートメーターと称する新たな電力計を家庭やオフィスなどの電力消費地に設置する¹。スマートメーターは、単に積算消費量や月間消費量だけではなく、ネットワーク回線を使用して消費電力などの情報をリアルタイムで電力会社にリアルタイムに転送する。スマートメーターを用いたシステムを活用することにより、電力会社は個々の家庭や工場、さらには供給先地域全体の詳細な電力消費量をリアルタイムで把握することができる。アメリカでは、IBMがアイオワ州のDubuqueという人口6万人の自治体で1,000家庭にスマートメーターを導入する実証実験を行ったところ、11%の電力消費量の削減に成功したという実証実験結果もある²。

これまでも先進的な環境政策を展開してきた北九州市は、政府の新成長戦略に位置づけられる日本型スマートグリッドの構築と海外展開を実現するための取組みである「次世代エネルギー・社会システム実証」を行う地域の公募に対して応募し、平成22年4月に公募に応じた20地域の中から全国で横浜市、豊田市、京都府（けいはんな学研都市）と並んで北九州市が選定された³。平成22年8月には提案に基づいて「北九州スマートコミュニティ創造事業」のマスタープラン⁴が策定され、平成22年度から26年度までの5年間に、市内の標準街区と比較して、2014年までに2005年比50%のCo2を削減するという目的を掲げている。

マスタープランにおいては、スマートメーターの大量導入が実証事項の一つとされており、実証の仮説として、「地域エネルギーマネジメントの考えの下に標準化されたスマートメーターを開発、導入することにより、街区全体の構成者が、地域エネルギーマネジメントに参加している社会が構築できる。スマートメーターには、従来の計量機能に加え、双方向通信による自動検針、情報表示機能を備え、また、需要家ゲートウェイによる直接機器制御

を行う。」としている⁵。また、実証内容として「富士電機システムズ(株)が、スマートシステムのゲートウェイとして、標準化を念頭においた適切なAMI (Advanced Metering Infrastructure) を備えたスマートメーターを開発し、70社、200世帯に導入する。スマートメーターには、従来の電力量を計測する機能に加えて、天候・電力料金・各種ガイダンス・エコポイント積算機能、デマンドレスポンス対応機能、BEMS や HEMS と連携した直接機器制御機能等の様々な機能を付加する。制御対象としては、需要家側PV、蓄電システム、EV、燃料電池、温水器、家電などを対象とする。エネルギー消費情報の計測は、10秒から30分の間で行い、最適な計測間隔を検証する。スマートメーターに最適な通信方法を検討するとともに、スマートメーターの使いやすさ、有効性、経済性を検証する。」とされている⁶。

一方、アメリカにおいてはオバマ政権がスマートグリッドを「グリーンニューディール」政策の一環に位置づけて推進している。アメリカにおけるスマートグリッド構想は、ブッシュ政権に発端をさかのぼることができるが⁷、本格化したのはオバマ政権によるアメリカ復興・再投資法 (American Recovery and Reinvestment Act of 2009)⁸の制定以降である。

アメリカ復興・再投資法は、オバマ政権の経済政策の中核となるものであり、クリーンで効率的なエネルギー開発、科学技術に基づく経済への転換、道路・橋梁・交通・水路の近代化、21世紀に向けた教育、雇用創出減税、医療費削減、失業者支援、公共部門の雇用確保など多くの内容を含む包括的な法律となっている。カリフォルニア州を初めとする州政府によってもスマートグリッドは推進されており、スマートメーターの普及も進んでいる⁹。たとえばカリフォルニア州では、2010年6月の時点で600万台をこえるスマートメーターが導入された¹⁰。

しかしスマートメーターに関しては、プライバシーに関する懸念も表明されており、2011年6月にホワイトハウスが公表した報告書¹¹の中ではプライバシー保護と消費者保護の必要性が明記されるに至った¹²。

そこで本稿では、スマートメーターの普及が先行しているアメリカにおけるスマートメーターとプライバシーに関する議論について検討し、わが国におけ

るスマートメーター普及に向けた若干の考察を行うことにしたい。

2. スマートメーターとプライバシー

2.1. 技術的可能性

スマートメーターは、各工場や家庭に取り付けることによって、電気使用量の変化を詳しく把握できるという特徴を持つ。このようなスマートメーターによって得られたデータが、なぜプライバシー侵害の危険性を包含するのであるうか。

それは、スマートメーターによって得られた電気使用量の変動を知ることによって、各家庭がいつ外出しているかとか、いつ就寝しているかという生活スタイルをある程度把握することが可能となるという特徴があるからである。このため、2001年の時点で、すでに研究者からはスマートメーターの導入によるプライバシー侵害の危険性が指摘されていた¹³。

家庭やオフィスで用いられる各種の電気製品は、その瞬間的な消費電力量に特有の特徴と傾向を示すから、瞬間的な消費電力量を計測し続け、その消費電力量のデータを詳細に分析すれば、ある瞬間に家庭やオフィスにおいてどのような電気製品を使用したのかをかなりの精度で推定することができるとされる(図1)。図1はさまざまな文献で引用されることが多いが、この家庭ではkettle(湯沸かし)の使用頻度が高いことから、おそらくお茶を頻繁に飲むことが多いのではないかと推測されるという¹⁴。

もっとも、ある瞬間に家庭やオフィスにおいてどのような電気製品を使用したかがわかったからといって、ただちにそれが個人情報やプライバシー侵害を発生させるとは限らない。しかし、ある家庭においてどの程度の頻度で電子レンジを使用しているか、ある家庭においてどの時間帯にどの程度テレビを視聴しているか(それによって、視聴しているテレビ番組の内容も把握できる)、いつシャワーを浴びているか、といった行動について、電力供給事業者はある程度把握することが可能となる。

さらに、このようなデータを集積して分析することで、家庭における家族の行動の様子についても、通常時とは異なる変化を看取することができる。たと

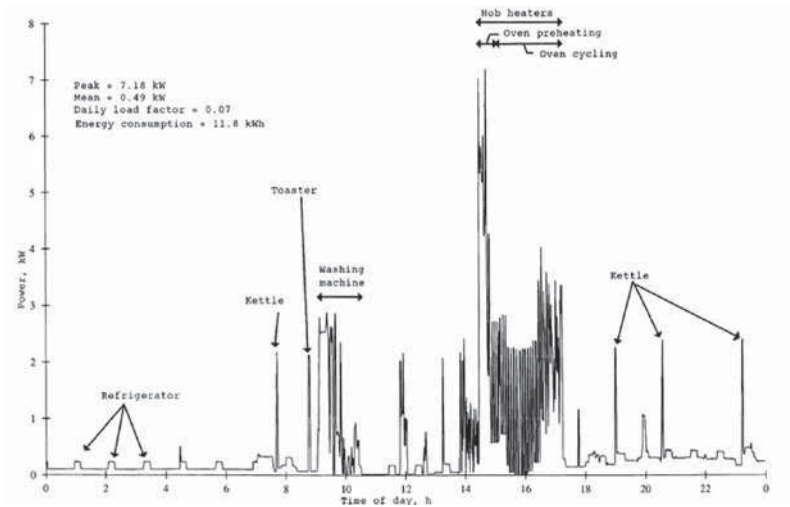


図1 計測した家庭の電力消費量から推定される電気製品の使用¹⁵

えば、深夜に毎晩長時間テレビを視聴し、ほとんど外出していないというようなデータからは、その家庭の家族の運動不足による肥満を予想させるし、病気に罹患する確率も高いであろうことを推測させる。電子レンジの使用頻度が高く、キッチンで他の電気製品を使うことが少ない家庭は、冷凍食品などの出来合いの食品を購入して調理しているのではないかとと思われるし、コーヒーマーカーの使用頻度が高い家庭ではコーヒーが愛飲されていることがわかる。

このことから、スマートメーターから収集されるデータは、従来の積算消費量や月間消費量のデータとは異なり、プライバシーとしての性質を強く有することになる¹⁶。また、長期間にわたってこれらのデータを蓄積することにより、スマートメーターから収集されたデータはライフログ¹⁷としての性質も帯びることになり、匿名化処理を行う必要も指摘されている。

ただし、スマートメーターの導入は後述するようにプライバシー保護強化の側面も有することには注意を向ける必要がある。スマートメーターを導入することにより、物理的な電力計を家庭に設置する必要がなくなる。このため、従来のように検針員が各家庭の敷地内に立ち入って（往々にしてそれは家庭の家

族が不在であっても行われる) 検針することがなくなり、検針員を装った不審者の侵入を防ぐことにも役立つことになる。

2. 2. 技術的可能性

スマートメーターによるデータ収集によってプライバシー侵害が生じる恐れは、次のように類型化することができる¹⁸。

2. 2. 1. 個人の行動パターン

高い精度で計測される電気使用量のデータからは、家庭の特定の電気製品の使用を認識することを通じて個人の行動パターンを推測することができる。たとえばどの時間帯に調理し、テレビを視聴し、シャワーを浴びているかということが容易に把握できる。

2. 2. 2. リアルタイムの行動調査

スマートメーターはリアルタイムで電気使用量のデータを収集することができるため、個人の行動パターンの推測をリアルタイムで行うことができる。バッテリーへの充電などのデータからは、これから外出するのではないかということも予測できる。

2. 2. 3. 微細情報の集積

消費者は、電子商取引や日常の買い物などにおいて、微細な個人情報を生成させ、放置している。これらの情報一つ一つが有する価値は小さいが、集積させることによって、個人の行動パターンの分析に利用することができる。スマートメーターによって収集されたデータを第三者に提供することが可能となった場合には、集積情報の価値を大きくすることに寄与すると思われる。

2. 2. 4. 物理的な侵入

物理的な侵入の恐れは、偶発的なものと意図的なものとに分類される。

偶発的な侵入は、スマートメーターの導入によって減少する。物理的な電力

計を家庭に設置する必要がなくなるから、検針員が各家庭の敷地内に立ち入って検針することがなくなり、検針員を装った不審者の侵入を防ぐことにもなる。

しかし、スマートメーターのデータによって意図的な侵入が増加する恐れもある。ある家庭の不在や外出のパターンが明らかになるので、空き巣や強盗などの犯罪者にとってはターゲットを特定しやすくなるからである。このため、スマートメーターのデータの第三者提供や漏洩が特に問題となる。反面で、スマートメーターのデータを警察や警備会社等が利用することが可能になれば、空き巣や強盗に狙われやすい家庭や地域を特定して警備警戒することができるという特質も有している。

2. 2. 5. プラグインハイブリッドカー

近年、直接コンセントから充電できるタイプのハイブリッドカーであるプラグインハイブリッドカー(PHV = Plug-in Hybrid Vehicle)が、トヨタ自動車、ゼネラルモーターズ等の各自動車会社から発売されるようになった。

PHVも、スマートメーターによるプライバシー侵害の恐れの原因となる。というのは、通常はPHVは家庭の電気契約に登録し、家庭で充電することが多いからである。このため、PHVの充電を通じてスマートメーターは各家庭の自動車の利用パターンを収集することが可能となる¹⁹。充電時に車載コンピュータのデータとリンクすることが可能となれば、詳細な走行パターンまでもが収集されることになる。

3. スマートメーターのデータの利用

3. 1. 利用目的

スマートメーターによって収集される電力消費量のデータは、電力消費量の削減にとどまらず、次のようにさまざまな目的に使用可能である²⁰。

表1 電力消費量データの利用目的の例

カテゴリー	内容
供給効率サービス	漏電検出、漏電箇所把握、修復・修理
	盗電検知
	リモート接続、切断
	財産管理
	電気料金のリアルタイム通知
	電力供給状況モニタリング
	電力消費量と負荷の予測
エッジ・サービス	電力消費の効率性分析
	家庭の電気製品の効率性モニタリング
	家庭の電力消費量と負荷の予測、ウェブポータルやソフトウェアを通じた管理・情報提供サービス
	家庭の電気製品のネットワーク化
その他の目的	火災保険等
	マーケティング、マーケティング調査
	国家安全保障、刑事捜査

3.2. 利用主体

スマートメーターによって収集される電力消費量のデータを利用する主体は、これまでのように電力事業者には限定されない。前述したように、スマートメーターのデータはさまざまな目的に使用可能だからである。

スマートメーターのデータの利用主体としては、次のような例が考えられる。

表2 スマートメーターのデータ利用主体の例²¹

利用主体	利用形態の例
電力事業者	電力消費、負荷のモニタリング、料金決定
電力利用助言事業者	エネルギーの効率的な利用とコスト削減
生命保険会社	家庭・個人の行動履歴の把握による健康状況の予測、特異な行動パターンからの事故や事件の予測
営業	行動ターゲティング広告への利用
警察等	犯罪行為や違法行為の察知、捜査
民事訴訟弁護士	財産権侵害等の察知、証拠
土地等所有者	賃貸借契約の遵守状況の確認
投資者	事件、事故発生の察知
報道関係者	著名人に関する情報収集
信販業者	カード破産の事前予知
犯罪者	犯行の適切な日時決定、犯罪を行う場所の物色

4. プライバシー保護の方法

アメリカにおいては、連邦法では包括的な個人情報保護法が存在せず、個別の領域においてプライバシー保護に関する約30の法律が制定され²²、連邦政府や民間事業者に対して各種の義務を課している²³。また、州法においても、各州が独自にプライバシーや個人情報の保護に関する法律を制定している。総じていえば、保護の水準は州法のほうが高い傾向にある（ただし、すべての州でプライバシー保護や個人情報保護に関する厳しい州法が制定されているわけではない）。

このような状況にあるので、スマートメーターに関しても、アメリカでは連邦法と州法という二本立てによってプライバシー保護が図られる仕組みとなっている。すでに連邦レベルではアメリカ国立技術標準局(NIST = National Institute of Standards and Technology)がガイドラインを定めている²⁴。ただし、プライバシー保護の方法については、連邦法であるか州法であるかと問わず、次のような論点が存在する。

4. 1. 公開に関する同意

スマートメーターのプライバシーの最大の問題は、スマートメーターのデータにアクセスできる当事者をどのようにして限定するかという点である。

コロラド州をはじめとする数州の州法では、スマートメーターの設置に関して、オプトイン又はオプトアウト型によりデータの利用について消費者の同意を得ることを求めている。しかし、オプトイン・オプトアウト型については、常にいずれのほうが適切であるか、また有効であるかという点が問題となっている。厳格なオプトイン型を採用すれば、スマートメーターの利用可能性が日進月歩で高まるたびに消費者に同意を取り直す必要が生じ、技術進歩に萎縮効果を与えかねない。その一方で、オプトアウト型は消費者の目の届かないところで予想もしなかったようなデータ利用がなされるという帰結を招くことにもなりかねない。

4. 2. 関税表モデル

一方、プライバシー保護の方法としては「関税表(tariff)モデル」も提案されている。このモデルは、スマートメーターを設置した消費者は、スマートメーターのデータの利用の制限を自分で選択することができる一方で、スマートメーターのデータ利用許容度に応じて料金率を変えるというものである。利用を制限すればするほど、電気代に荷重料金が課せられる仕組みであり、逆に利用を許容すればするほど料金が割引となる。

この方法は、消費者に対しても選択肢を与えることができると同時に、新たな技術進歩等についても柔軟に対処できるという利点がある。

4. 3. 消費者への通知

アメリカにおいては、プライバシーや個人情報の保護に関して大きな論点となっているのは、プライバシーに関する情報や個人情報に関するインシデントが発生した場合、それを本人に通知することを事業者に義務づけることの是非である。

クレジットカードのナンバー等の個人情報が事業者から漏洩してしまった

場合、事業者等に、影響を受ける個人に対する通知を行う義務を定めているのは、連邦法では一部の領域だけである。アメリカ復興・再投資法の一部をなすものとして制定された経済的・客観的な健康情報技術に関する法律²⁵では、健康保険ポータビリティ及び説明責任法(Health Insurance Portability and Accountability Act)²⁶のプライバシー基準及びセキュリティ基準を強化する形で、セキュリティ侵害の通知に関する規定を具体的に置き、健康情報への侵害(breach)が発生した場合、または「保護される健康情報がセキュアでない(unsecured protected health information)」状態になった場合の通知・公表義務を規定している²⁷。またグラム・リーチ・ブライリー法(Gramm Leach Bliley Act)²⁸でも、2003年に連邦取引委員会によって金融機関等に適用されるグラム・リーチ・ブライリー・セーフガード規則²⁹が制定され、顧客情報への不正アクセスに対する対処と顧客への通知プログラム(Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice)³⁰がもりこまれた。

これに対して、州法においては、2011年12月時点で46州において、個人情報を含むセキュリティ漏洩事案が発生した場合には当該個人に通知することを義務づける法律が制定されている。逆にこのような法律をもたないのは、アラバマ、ケンタッキー、ニューメキシコ及びサウスダコタの4州だけである。また、コロンビア特別区、プエルト・リコ準州及び米領ヴァージン諸島においても同様の法律が制定されている。このような州法制定のうごきを先導したのはカリフォルニア州で、2002年、全米で最初にデータセキュリティ侵害通知法を制定し、個人情報の漏洩等のインシデントが発生した場合の公表義務と本人への通知義務を定めた³¹。

カリフォルニア州法は、個人情報の漏洩等のインシデントが発生した場合の公表義務について次のように規定している³²。

1798.29(a)

いかなる個人情報を含むコンピュータ化されたデータを所有する又は権限を有するものも、カリフォルニアの居住者の暗号化されていない個人情報を含

む又は含むと合理的に推定されるデータのセキュリティ侵害が発生したときには、システムのセキュリティの侵害を公表しなければならない。当該公表は、可能な限りの最も好都合な時間に、かつ不当な遅延なしで行われるものとする。ただし、(c)に定める合法的な法執行の必要性または侵害範囲を決定して、データ・システムの合理的な完全性を復元するのに必要な措置と矛盾なく行われるものとする。

また本人への通知義務については、次のように定めている。

1798.82(a)

いかなるカリフォルニアで事業を行う個人または団体であって個人情報を含むコンピュータ化されたデータを所有する又は権限を有するものも、カリフォルニアの居住者の暗号化されていない個人情報を含む又は含むと合理的に推定されるデータを権限のないものが取得してセキュリティ侵害が発生したときには、システムのセキュリティの侵害を公表するか、通知しなければならない。

(b)

いかなる個人または団体であって当該個人又は団体が所有していない個人情報を含むコンピュータ化されたデータを運用するものも、カリフォルニアの居住者の暗号化されていない個人情報を含む又は含むと合理的に推定されるデータを権限のないものが取得してセキュリティ侵害が発生したときには、システムのセキュリティの侵害を公表するか、通知しなければならない。

漏洩等のセキュリティ侵害が発生した場合に公表・通知義務を負うことになる個人情報の種類を問わず、義務を負う者の業種等も問わないので、およそカリフォルニアで事業を行おうとする場合、個人情報の漏洩を引き起こした場合には公表・通知義務を負うということになる。

スマートメーターに関しても、現時点では上記のような州法が制定されている州では、通知義務が適用されるのかどうか問題になると思われる。スマー

トメーターは、一般的には各世帯に1台設置されるため、単身世帯の場合にはスマートメーターのデータは個人に関する情報であるということになるが、複数人で構成される世帯の場合は、個人に関する情報が集積・混合した形でデータを構成することになる。しかし、そのことを理由としてスマートメーターに関する情報が上記の通知法制の適用から除外されることになれば、消費者からは不安や不満が生じることになる。

5. おわりに

上述したように、スマートメーターで収集される電気使用量のデータは、従来のデータとは全く異なる性質を有している。

今後、わが国でもスマートメーターの導入が進むと考えられるが、リアルタイムで電気使用量を把握できるため、スマートメーターから収集される電気使用量のデータが漏洩したり盗聴されたりした場合には、各家庭の生活状況もリアルタイムに把握できることになり、防犯・セキュリティ上の問題が生じる。また、スマートメーターから収集されるデータが電力会社によって集中的に管理されることになるので、電力会社は収集したデータの管理についてきわめて大きな責任を負うことになるほか、収集したデータを電力の効率的活用以外の目的で利活用してもよいかという問題も生じる。

また、スマートメーターによって収集されるデータは、世帯単位であることにも難しさがある。単身世帯の場合は、世帯のプロファイルに関するデータはそのまま個人に関するデータであるとみなしうる。しかし、複数の家族によって構成されている世帯のデータについては、ただちにそこから家族の誰の行動であるかをプロファイルすることは困難であると考えられる。したがって、「個人」を保護の基礎としているわが国の個人情報法制の下では、同じように収集されるデータでありながら、個人情報に関する法が適用される場合と適用されない場合が生じる可能性があり、世帯単位の個人情報の保護という観点からの検討が必要である³³。

このように、スマートメーターの導入については、多くの法的な問題がある。これらの諸問題について、わが国においては前述した北九州市の実証実験など

の経験をもとにしながら、現行のプライバシー保護に関する法制度及び個人情報保護に関する法制度の下でのデータの取扱いの検討を進める必要があるだろう。

※本稿は、科学技術振興機構「環境モデル都市における既存市街地の低炭素化モデル研究」（代表：宮崎昭・九州国際大学教授）の研究成果の一部である。

注

- 1 スマートメーターについては、スマートメーター制度検討会「スマートメーター制度検討会報告書」（2011年）http://www.meti.go.jp/committee/summary/0004668/report_001_01_00.pdf参照。
- 2 James Niccolai, Residents *Cut Energy Bills 11% in Smart Meter Test: IBM is Running a Test in Dubuque, Iowa, to Get Residents Engaged with Their Smart Meter Data*, available at http://www.computerworld.com/s/article/9219520/Residents_cut_energy_bills_11_in_smart_meter_test?taxonomyId=14&pageNumber=1, (last visited Jan, 30, 2012).
- 3 経済産業省「[次世代エネルギー・社会システム実証地域]の選定結果について」（2010年）。<http://www.meti.go.jp/press/20100408003/20100408003-1.pdf>
- 4 北九州市「北九州スマートコミュニティ創造事業マスタープラン」（2010年）。<http://www.city.kitakyushu.lg.jp/files/000041577.pdf>
- 5 北九州市、前注4、19頁。
- 6 北九州市、前注4、19頁。
- 7 村瀬・佐藤、前注9、978頁。
- 8 P.L. 111-5, codified at 2 U.S.C. 661 et seq.
- 9 アメリカのスマートグリッド政策については、村瀬一郎・佐藤明男「米国を中心としたスマートグリッドの動向」情報処理51巻8号（2010年）978-985頁参照。
- 10 Joey Peters, *Consumers Wary of Smart Meters*, available at <http://www.stateline.org/live/details/story?contentId=500546> (last visited Jan, 30, 2012).
- 11 Executive Office of the President, *A Policy Framework for The 21st Century Grid: Enabling Our Secure Energy Future*, available at <http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf> (last visited Jan, 30, 2012).
- 12 Executive Office of the President, *supra* note 11, 46-48.
- 13 Alan Leo, *The Measure of Power: Non-Intrusive Load Monitoring Gives*

- Detailed Views of Where Power is Going, With Payoffs for Utilities, Consumers, and maybe Big Brother*, available at <http://www.technologyreview.com/energy/12466/> (last visited Jan, 30, 2012).
- 14 Ariel Bleicher, *Privacy on the Smart Grid*, IEEE Spectrum, available at <http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid> (last visited Jan, 30, 2012).
- 15 出典：M. Newborough & P. Augood, *Demand-side Management Opportunities for the UK Domestic Sector*, IEE Proceedings of Generation Transmission and Distribution 146 (3) (1999) 283-293.
- 16 藤井秀之・山口健介「スマートグリッドとプライバシー・個人情報の保護: プライバシー影響評価(PIA)からの検討」電子情報通信学会技術研究報告 SITE技術と社会・倫理110巻231号 (2010年) 35-40頁。
- 17 ライフログの法的定義と問題点については、石井夏生利「ライフログをめぐる法的諸問題の検討」情報ネットワークロー・レビュー9巻1号 (2010年) 1-14頁、新保史生「ライフログの定義と法的責任：個人の行動履歴を営利目的で利用することの妥当性」情報管理53巻6号 (2010年) 295-310頁、生貝直人「オンライン・プライバシーと自主規制: 欧米における行動ターゲティング広告への対応」情報通信学会誌28巻3号 (2010年) 105-113頁などを参照。
- 18 Elias Leake Quinn, *Smart Metering and Privacy: Existing Law and Competing Policy, A report for the Colorado Public Utilities Commission*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1462285 (last visited Jan, 30, 2012).
- 19 Cheryl Balough, *Privacy Implications of Smart Meters*, 86 Chicago Kent L. Rev. 161, 167-168 (2011).
- 20 Quinn, *supra* note 18.
- 21 出典：National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid: Vol. 2, Privacy and the Smart Grid*, NISTIR 7628 (2010)より作成。
- 22 主要なものとして、Administrative Procedure Act, 5 U.S.C. § 551, 554-558, Cable Communication Policy Act, 47 U.S.C. § 551, Census Confidential Statute, 13 U.S.C. § 9, Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501, Communications Assistant for Law Enforcement Statute, 47 U.S.C. § 1001, Computer Security Act, 40 U.S.C. § 1441, Consumer Credit Reform Act of 1996, Pub. L. 104-208, Criminal Justice Information System Statute, 42 U.S.C. § 3789G,

Customer Proprietary Network Information Statute, 47 U.S.C. § 222, Driver's Privacy Protection Act, 18 U.S.C. § 2721, Drug and Alcoholism Abuse Confidentiality Statute, 21 U.S.C. § 290dd-3, Electronic Communication Privacy Act, 18 U.S.C. § 2701, Electronic Funds Transfer Act, 15 U.S.C. § 1693, Employee Polygraph Protection Act, 29 U.S.C. § 2001, Employee Retirement Security Act, 29 U.S.C. § 1025, Equal Credit Opportunity Act, 15 U.S.C. § 1691, Equal Employment Opportunity Act, 42 U.S.C. § 2000E, Fair Credit Billing Act, 15 U.S.C. § 1666, Fair Credit Reporting Act, 15 U.S.C. § 1681, Fair Debt Collection Practices Act, 15 U.S.C. § 1692, Fair Housing Act, 42 U.S.C. § 3604, Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, Freedom of Information Act, 5 U.S.C. § 552, Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Health Insurance Portability and Accountability Act, Pub. L. 104-191, Health Research Data Statute, 42 U.S.C. § 242m, Mail Privacy Statute, 39 U.S.C. § 3623, Paperwork Reduction Act of 1980, 44 U.S.C. § 3501, Privacy Act, 5 U.S.C. § 552a, Privacy Protection Act, 42 U.S.C. § 2000aa, Right of Financial Privacy Act, 12 U.S.C. § 3401, Tax Reform Act, 26 U.S.C. § 6103, Telephone Consumer Protection Act, 47 U.S.C. § 227, Video Privacy Protection Act, 18 U.S.C. § 2710, Wiretap Statutes, 18 U.S.C. § 2510.

- 23 内容の詳細については、牧田潤一郎「アメリカのプライバシー保護法制の日本への示唆」Law and Practice 4号（2010年）185-218頁。
- 24 NIST Smart Grid Interoperability Panel Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security vol. 1, Smart Grid Cyber Security Strategy. Tech. rep., National Institute of Standards and Technology*, July 2010.
- 25 The Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as Title XIII of Division A (§ § 13001-13424) and Title IV of Division B (§ § 4001-4302) of the American Recovery and Reinvestment Act of 2009 (ARRA), P.L. 111-5.
- 26 P.L. 104-191, 110 Stat. 1936 (1996), codified in part at 42 U.S.C. § § 1320d et seq.
- 27 P.L. 111-5, § § 13402, 13407.
- 28 Pub.L. 106-102, 113 Stat. 1338.
- 29 16 CFR Part 314.
- 30 セキュリティガイドラインにおいては、顧客情報の漏洩による実際の被害は「センシティブな顧客情報（顧客の氏名、住所、電話番号、社会保障番号、運転免許証番号、口座番号、クレジットカード番号等）」の不正使用によって引き起こされるとし、金融機関等からの顧客情報の漏洩・流出が発生した場合には顧客に通

知することを勧告しているほか、顧客の情報の不正使用が発生したか、発生する可能性が高い場合には、漏洩・流出について公表することを求めている。ただし、捜査機関が顧客への通知や情報公開が操作の妨げになると判断した場合には、通知を遅らせることができるとしている。Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), Supplement A to Appendix D-2, at 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), 70 Fed. Reg. 15736-15754 (March 29, 2005).

31 Cal. Civ. Code 1798. 82 and 1798. 29.

32 Cal. Civ. Code 1798. 82 and 1798. 29.

33 給付型の社会福祉行政における同様の問題点を指摘するものとして、渥美由喜・瀧口樹良「個人情報保護法の施行に伴う介護事業者の課題」富士通総研経済研究所研究レポート268号（2006年）8-9頁。