

EUにおける「モノのインターネット」(IoT)をめぐる政策動向

一般財団法人 マルチメディア振興センター 電波利用調査部

副主席研究員 木賊智昭

1 IoTに関する欧州委員会の取り組み

携帯電話サービス市場が世界的に成熟化しつつある移動体通信分野において、今後の新しい通信サービスの一つとして、センサー/機器/装置/設備等が直接通信し相互に情報交換する「モノのインターネット」(Internet of Things : IoT) あるいは「M2M」(Machine to Machine) の成長が期待されている。例えば、シスコ (Cisco) 社は、2013年2月に発表した「Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017」において、世界のM2Mのデータトラフィック(月平均)は、2012年の24ペタバイトから2017年には563ペタバイトへと、24倍に増加すると予想しており、また世界の各地域の中で西欧地域におけるM2Mトラフィックが同期間において最も伸びるものと予想している¹。

欧州連合(EU)も、IoT²を、交通、エネルギー、医療、教育、小売物流、製造業等の幅広い産業分野において、経済的・社会的利益をもたらす新技術・アプリケーションとして位置付けている。政策面でも、2009年に欧州委員会が、「モノのインターネット：欧州のアクション・プラン」と題する(COM(2009) 0278 final) コミュニケーションを発表(2009年6月18日)し、これに基づき、研究開発や普及の促進を図る施策の実施や、伝送されるデータに関するセキュリティやプライバシー保護などのルールづくり等が検討されている(後述)。

元来、IoTに関する政策議論は、RFIDに関する政策上の戦略を検討するところを端緒にしている。市民によるRFID利用を促進するために、2007年3月に欧州委員会が、プライバシーと個人データ保護が十分に確保されることが不可欠であるとの方針を公表し³、2009年には、「個人情報処理と電子通信部門におけるプライバシー保護に関する指令」(e プライバシー指令)(2002/58/EC)で規定している、①ネットワーク上で伝送される個人データに関するセキュリティ確保、②データ内容の秘匿性の確保、③ロケーションデータの利用に関する事前の本人同意の義務付け等を、RFIDにも適用するよう同指令を改

¹ http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf

² IoTとM2Mの関係について、欧州委員会「モノのインターネット：欧州のアクション・プラン」では、IoTは、通信形態に従い「モノとヒト」(things-to-person)と「モノとモノ」(thing to thing)の通信で構成され、M2Mは後者に属するものと位置付けられている。

³ http://www.iot-visitthefuture.eu/fileadmin/documents/the_roadmap/Documents/150307_Press_Release_CeBIT_Brussels_Hannover.pdf

正している⁴。

その後、RFID という分野にとどまらず、医療、交通、エネルギーなど幅広い分野において「モノとヒト」及び「モノとモノ」を結ぶ新しい IoT 技術の開発・普及が注目されるに伴い、改めて IoT の枠組みの下で規制と振興に関する政策方針が検討され、2009 年に IoT のアクション・プランがまとめられるに至った。同アクション・プランでは、欧州委員会が今後取り組むべき課題として、IoT の管理ルールや制度づくり、研究開発、普及促進など、14 項目が挙げられている。

図表 1 IoT に関する欧州委員会のアクション・プラン

1. ガバナンス	欧州委員会は、IoT のガバナンスに必要な原則を策定する。また、分散型管理アーキテクチャの設計に取り組む。
2. プライバシーとデータ保護	欧州委員会は、IoT へのデータ保護の法的規定の適用に関して継続的にモニターを実施する。
3. 「チップの沈黙」(Silence of Chips) への権利	欧州委員会は、個人が、いかなる時でもネットワーク接続から解除されることを保証するための技術及び法的根拠を検討する。
4. 出現するリスク	欧州委員会は、IoT の信頼性、社会受容、セキュリティの確保に必要とされる課題を明らかにし、効果的な措置を講じる。
5. 不可欠な資源	欧州委員会は、IoT を域内の経済や社会にとって不可欠な (Vital) 資源として位置付け、サイバーアタック等への対応措置を講じる。
6. 標準	欧州委員会は、適宜、IoT に関する標準の作成を域内の標準化機関に要請 (mandate) する。
7. 研究開発	欧州委員会は、第 7 次研究開発枠組みプログラムにおいて IoT 分野の研究開発プロジェクトの資金援助を行う。
8. パブリック・プライベート・パートナーシップ (PPP)	欧州委員会は、製造業、エネルギー管理、エコカー、インターネット高度化の 4 分野において利用される IoT 技術の開発を、官民パートナーシップ (PPP) 形式で進める。
9. 技術革新	欧州委員会は、Competitiveness and Innovation Framework Programme(CIP)を通じて、eヘルス、気候変動、デジタルデバイスに対応する IoT アプリケーションのパイロット・プロジェクトを開始する。
10. 関連機関における認識の深化	欧州委員会は、IoT の開発状況に関して、欧州議会、欧州理事会、欧州経済社会委員会、個人データ保護指令第 29 条作業部会 (Article 29 Data Protection WG) 等に定期的に報告を行う。
11. 国際的対話	欧州委員会は、IoT に関する情報共有や共同事業の推進のため、国際的なパートナー機関と積極的に対話を行う。
12. 環境	欧州委員会は、RFID タグのリサイクルの可能性や廃棄物一般のリサイクルに関して RFID 利用の利点を検討する。
13. 統計	欧州統計局 (Eurostat) は、RFID 利用の統計報告を作成する。
14. 進展状況の評価	欧州委員会は、欧州の代表的なステークホルダーとの会合を開催し、IoT の進展状況を把握する。

出所：European Commission, Internet of Things — An action plan for Europe (COM(2009) 278 final) より作成

⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF>

このアクションプランを踏まえて、2013年夏に欧州委員会の勧告書が発表される予定であり、その後、同勧告に従って政策が具体化される見通しである。現在、勧告内容の検討が進められているが、特に、IoT分野におけるプライバシーとデータ保護、セキュリティと安全、倫理、相互運用性、ガバナンスに関しては、2012年4月～6月にコンサルテーションが実施され、以下の事項の意見を、企業・団体、政府機関、個人から求めるなどしている。

① プライバシーとデータ保護

- ・IoTアプリケーションを利用する際のデータ保護に関する特定の施策の必要性。

② セキュリティとセーフティ

- ・IoTにおけるセキュリティと個人の安全を確保するための特定のガイドラインと基準の必要性。

③ IoTインフラのセキュリティ

- ・クリティカル・インフラストラクチャ（critical infrastructure）として、より厳しい／強制力を有する政策措置の必要性。

④ 倫理：倫理上の問題

- ・IoTによる倫理への影響。
- ・倫理面の問題の特定と制度整備の必要性。

⑤ オブジェクト識別子（OID）と相互運用性

- ・相互運用性を確保するための最小の要件。

⑥ ガバナンス：IoTガバナンスに関するスコープ

- ・プライバシー、セキュリティ、倫理、相互運用性のほか、ガバナンスに係る検討事項。
- ・IoTガバナンスの枠組み、組織、実施方法。

コンサルテーションでは、多様なステークホルダーからの意見が寄せられ、IoTの政策・制度の在り方に関する欧州内のコンセンサスを見出すことは難しい状況にあることが明らかになった。プライバシーやデータ保護、セキュリティ確保のためのガイドラインやルール制定の必要については、大半の回答者が認めているものの、政府介入の範囲や度合いについての意見は多様であり、産業界からは、揺籃期にあるIoTの成長を妨げるような過度の規制を回避するべきとの意見が出され、消費者団体や個人からは、データ保護やセキュリティ確保を重視する意見が出されるなど⁵、今後の政策議論を通じて利害の調整が図られることが期待されている。

また、個人データ保護については、元来、「欧州連合基本権憲章」（Charter of Fundamental Rights of the European Union）第8条において基本的人権として保障され

⁵ http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746

ているが⁶、そのほか、1995年にEUで制定された「個人データ保護指令」に代わる「個人データ保護規則（案）」⁷が、2012年1月に提出されており、IoT分野の個人情報データの管理ルールは、同規則案の内容を考慮したものになると見込まれる。

図表2 個人データ保護規則（案）の主な規定

- ・個人データ保護ルールの簡素化（1国内でのデータ保護の承認の他国への適用など）
- ・個人データを利用する際に本人に対し明示的（exploit）な同意を取得することを義務化。
- ・本人が要求した場合や、同意されたデータ保有期限を過ぎた場合、本人データを消去する「忘れられる権利（Right to be forgotten）」を保障。
- ・利用者が他事業者へサービスを切り替える際に、元事業者から個人データを入手する「データ・ポータビリティの権利」を保障。
- ・サービスを導入する際に、設計段階から予めプライバシー対策を講じる「プライバシー・バイ・デザイン」原則を導入。

出所：European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012) 11 final) より作成

2 IoT関連の振興施策

IoTアプリケーションは、交通、エネルギー、医療、小売、物流など幅広い産業分野で、その普及が期待されているが、エネルギーや交通分野では、欧州委員会による政策的な取り組みが、それら分野におけるIoT普及を促す役割を果たしている。

①エネルギー分野

家庭やオフィスの電力の消費量を一定間隔で自動検針し、その情報を電力会社へ伝送するとともに、当該家庭・オフィスの情報端末で可視化するスマートメーターの設置が進んでいる。EUでは、2009年に欧州委員会が発出した電気指令（2009/72/EC）により、2020年までに域内の80%のカスタマに対しスマートメーターの設置が目指されている。欧州各国でもスマートメーター普及政策が策定されており、スウェーデンでは、2003年に国内の全世帯でスマートメーターの設置が法制化され、2009年に達成している。また、他の主要国でも、スマートメーターの設置政策が進められている。

- ・英国：国内3000万需要家（世帯・オフィス）へのスマートメーター設置を2019年までに達成することとされている。

⁶ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:FULL:EN:PDF>

⁷ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

- ・フランス：2012年以降、電力メータはスマートメーターとすることが義務化されており、2014年までに700万台、2018年までに更に2800万台の追加設置が目標とされている。
- ・ドイツ：2010年以降、新規ビル及び建て替えビルにスマートメーターを設置することとされている。
- ・イタリア：2006年にスマートメーターの設置が義務化され、スマートメーターの設置比率を2008年25%、2009年65%、2010年90%、2011年95%と定めている。
- ・スペイン：2007年にスマートメーター設置を法制化し、目標を2010年30%、2012年50%、2015年70%、2018年100%と定めている。

②車両・ロケーション

欧州では、EUが2012年6月のeCall決議により、2015年までにEU諸国内の全ての新しい自動車に、事故車からの緊急信号を発することができる携帯電話とGPS等の通信機能の組み込みを義務付けている。事故が発生した場合、車内に設置されたセンサーが事故を感知し、自動的に緊急通報番号112（emergency call：eCall）を発信、これを受けてGPSや移動電話位置システムが発動して事故現場の位置を特定し、最寄りの緊急通話センター（Public Safety Answering Point：PSAP）へ車両の位置、進行方向、車両タイプ等の情報が伝送される。PSAPとドライバーとの通話セッションも設定され、収集された情報に基づき最適な緊急サービス（救急、消防、警察等）を迅速に提供することで被害を最小限に抑えることが出来る⁸。交通分野において通信システムを活用するテレマティクスの一つであるが、交通安全政策の一環として、このようなテレマティクスの利用が義務化されることで、EU諸国におけるIoTの普及が一層進むものと予想される。

3 まとめ

IoTのアプリケーション等の開発と普及について、欧州委員会は、あくまでも民間部門が主導で進めるべきとの立場にあるが、同時に、IoTが経済や社会に与える影響が大きいことが予想される中で、①ネットワークに接続されるモノの識別子（ID）の形態と割当て、②情報セキュリティ確保と個人データ保護、③サービス提供／利用に係る利害関係者の責任の明確化など、IoTの管理体制（ガバナンス）に関するEUの方針を明確にする、としている。特に個人データ保護に関しては、IoTの場合、アプリケーションの内容に応じて、医療情報、消費行動、生活パターン、位置情報など個人に固有する情報データが自動収集・加工される利用ケースが頻繁化・常態化する傾向になるため、個人情報データのネットワーク上の扱いに関するルール作りが、特に重視されていると言える。

半面、IoTのサービス市場は初期段階にあるため、IoTの市場形成を促す配慮が求められているところでもあり、今後開発されるであろう将来のIoT関連技術やアプリケーション

⁸ http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm#eCall_Recommendation

ンに個別に対応する柔軟な管理体制の整備も欧州委員会の検討課題の一つとなっている。**IoT** の政策をめぐっては、**IoT** 市場の成長とデータ保護／セキュリティを調和させた施策の形成が目指されることが期待されているところであり、今後の欧州委員会の動向が注目されている。