コンテキスト：ユビキタス社会の“見えない”個人情報

下畑　光夫

ユビキタスサービスの特徴の一つに現実世界の状況（コンテキスト）を取得してサービスに活用することが挙げられる。このコンテキストには、気温や交通情報といった環境の情報も含まれるが、特定個人の位置や購入履歴、体温・心拍数といった個人情報に該当するものも含まれる。個人情報に該当するコンテキストを改めて考えると、氏名や住所といった事項を記述するタイプの個人情報と比べて情報取得と得られる情報の質において“見えない”という性質がある。

本論文では、この見えない個人情報としてのコンテキストを従来の個人情報と対比させてその問題点を指摘する。そして、コンテキスト利用に対してプライバシー侵害への懸念が根強い中、コンテキストの利活用に理解を求める方策について述べる。

1　ユビキタスサービス学の論点としてのプライバシー

東京大学大学院・情報学環では2007年4月にOKIからの寄付を受けて「OKIユビキタスサービス学」寄付講座が設立された。本講座はユビキタスサービス普及のための課題を取り上げ、体系的、学術的に探っていくことを目的としている。このユビキタスサービス普及のための論点の一つとしてプライバシーの問題が挙げられる。

実際、プライバシー侵害への懸念でユビキタスサービスが中止に追い込まれている例は多い。2003年にベネトンが商品にRFIDタグを貼付しようという計画を発表したが、プライバシー保護団体の反対を受けて中止に追い込まれている。ベネトン側では、タグを貼付することで盗難と偽造の防止に役立つという点と、タグ付きの服を着て来店した客のさまざまな活動が分かるという点を導入効果としている。しかし、客にしてみれば意識されない形で購入履歴さらには来店履歴というコンテキストを取得されることに対して反発があったのである。

2005年にはカリフォルニア州の小学校で児童にICカードを所持させて読み取り機にかざさせることで教室の入退出をチェックするという実証実験が行われたが、プライバシーを侵害するという反発を受けて中止となっている[1)]。導入効果として正確な出欠確認、教師の手間軽減、セキュリティ向上が挙げられていた。しかし、児童の入退出というコンテキストを取得することが児童の監視につながっているとされたのである。ただし、同様のシステムが本格導入されている学校もあり、状況はさまざまではある。

コンテキスト以外の個人情報ではこれほど大きな争点となることは少ない。前者の事例でいえば、ベネトンにもしロイヤリティカード（俗にいうポイントカード）があったとすると、それを使うことで氏名と購入履歴の情報が収集されることになる。また、後者の例では、学校に対して氏名や住所の個人情報は渡していると考えられる。しかし、ロイヤリティカードや学校への個人情報提出は大きな問題とはされていない。なぜコンテキストの取得がプライバシー侵害として大きく取り上げられるのか。そのカギはコンテキストの持つ“見えない”性質にあると考えている。

以下、本論文ではコンテキストの背景知識として2節で技術的背景、3節でプライバシー権、4節で個人情報について述べる。5節ではコンテキストと項目記述型の個人情報を比較し、コンテキストの“見えない”性質について述べる。6節ではコンテキストを“見える”ようにすることで、その利活用を促進する方策について述べる。

2　コンテキスト取得・利用の技術的背景

近年、コンテキストを利用したユビキタスサービスが徐々に拡大している。GPS機能を利用した位置情報サービス、RFIDによるモニタリング、またネットでの行動履歴を利用した行動ターゲティング広告もその範疇に入るであろう。これは、コンテキスト利用における導入・運用コストの低下や性能の向上といった技術の発達に支えられている。特に進展が目覚ましいのが、コンテキスト取得装置、解析技術、データマイニングの3つである。以

下、それらについて述べる。

(1) コンテキスト取得装置

コンテキストを取得する装置の代表例としてRFID、携帯端末が挙げられる。RFID（Radio Frequency IDentification）は電磁界や電波を用いて無線で個体識別情報などを送受信する技術である。機能や数量にも大きく依存するが概して言えばタグは1個100円程度に下がってきている。使い捨てとするにはまだ高い価格であるが、再利用する形で、交通カード、製造現場、資産管理などでの利用が拡大している。

また、コンテキスト取得装置として日本では携帯電話がクローズアップされてきている。元々は通信機器であり、それ自身ではコンテキスト取得機能が低かったが、GPS機能、2次元バーコード読み取り機能、ICカード機能が装備され、コンテキストを活用したサービス端末としての機能が高まってきている。Webマーケティングガイドの調査によれば、2007年におけるGPS機能付き携帯電話の保有率は44.1%となっている。欧米ではGPSによる位置情報取得装置としては、パーソナルナビゲーションデバイス（PND）の普及が目覚ましい。

(2) 解析技術

コンテキストとして取得された初期段階（解析が施されていない）の情報は、体温や血圧の様に解析を必要とせずに利用できるものもあるが、多くの場合は解析を施して利用しやすい形へ変換する必要がある。

位置情報の場合では、緯度・経度といった低次の位置情報と地図とのマッピングや住所情報に変換する技術（逆ジオコーディング）が一般的に利用可能となってきている。

また、監視カメラに映った画像もコンテキストであるが、画像から特定の対象物を認識する画像認識技術がある。画像認識技術は光学式文字認識（OCR）を発端とし、実環境画像における文字読み取り、さらには顔画像認識も実用レベルになってきている。実際、日本の高速道路では自動車ナンバー自動読取システムが稼働している。また、今や公共空間や交通機関や空港などの至る所に監視カメラ（CCTV）が設置されている。これらのカメラには顔認識処理が組み込まれているものも多く、犯罪捜査などに利用されている。

(3) データマイニング

コンテキストは時々刻々と増加する情報であり、これを多種、多人数について集計すると膨大なデータ量となる。これを解析し、共通するパターンを発掘するためにデータマイニングがある。効率的なアルゴリズムの開発とコンピュータパワーの増大により、膨大なデータであってもデータマイニングの適用は現実的に可能となってきている。

主な分析領域としては、頻出パターン抽出（データ集合中で高頻度に現れるパターンを抽出）、クラス分類（分類情報のついたデータから分類方法を獲得し、未知のデータを分類）、クラスタリング（データ集合をクラスタと呼ばれる類似性の高いグループに分類）などがある。

3 プライバシー権

プライバシーに関する権利は、大別すると伝統的プライバシー権と現代的プライバシー権に分けられるが、本論文では情報化社会を想定した現代的プライバシー権を対象とする。

なお、伝統的プライバシーとは私的な事柄をみだりに公表されない権利を表している。1890年にウォーレンとブランダイスによる論文で提唱されており、この論文で用いられている「独りにしてもらう権利」（right to be let alone）がその定義としてよく知られている。

現代的プライバシーの概念は1960年代のアメリカで誕生している。この頃、コンピュータ技術が飛躍的に発達し、個人の情報を大量に記録して処理することが可能となってきた。これにより、個人の権利がコンピュータ管理者によって左右されるという危機感が生まれてきた。このような状況を背景としてプライバシー権を新たに定義する動きが現れた。アラン・ウェスティンは1967年の「プライバシーと自由」という著作において「プライバシー（権）とは、個人、グループまたは組織が、自己に関する情報を、いつ、どのように、また、どの程度に他人に伝えるかを自ら決定できる権利である」と定義している。これは伝統的プライバシー権にあるような「独りにしてもらう権利」というような受動的なものでなく、他人が持つ自己に関する情報の利用に干渉できるという能動的な定義となっている。個人にとって自分に関する情報とは自分のものであり、その流れをコントロールする権利が保障されているとも表現できる。

そして、ヨーロッパ各国でも同様の状況が到来したことを背景として個人情報保護法制が整備されていく中、個人情報は国を越えて活用されうるということから国際的な個人情報保護のルール作りが要請されるようになった。これを受けて、1980年に経済協力開発機構（OECD）が「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」を採択し、プライバシー

に関するガイドラインとして以下の8原則が発表された。

① **目的明確化の原則**：収集目的を明確にし、データ利用は収集目的に合致するべきである。
② **利用制限の原則**：データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない
③ **収集制限の原則**：適法・公正な手段により、かつ情報主体に通知または同意を得て収集されるべき。
④ **データ内容の原則**：利用目的に沿ったもので、かつ、正確、完全、最新であるべきである。
⑤ **安全保護の原則**：合理的安全保護措置により、紛失・破壊・使用・修正・開示などから保護するべき。
⑥ **公開の原則**：データ収集の実施方針などを公開し、データの存在、利用目的、管理者などを明示するべきである。
⑦ **個人参加の原則**：自己に関するデータの所在および内容を確認させ、また異議申し立てを保証すべきである。
⑧ **責任の原則**：管理者は諸原則実施の責任を有する。

この8原則は現代的プライバシー保護を表すものとしてよく知られており、日本の個人情報保護法にも強い影響を与えている。

とはいえ、この原則は個人情報のITへの依存度が比較的小さい時代に策定されたものである。ITによって管理される個人情報が極めて多岐に渡り、かつこれらがネットワークで接続された膨大な情報機器上で運用される現代では、これに厳密に従うことは困難である。たとえば、ウェブブラウザを利用した時に用いられるクッキーが挙げられる[2)]。クッキーは利用端末を識別するIDを自動的（非明示的）に付与するものであり、利用者に通知を行わず、引いては同意も得ていないという点で議論となっている。

4　個人情報

個人情報はJIS Q 15001によれば『個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述、または個人別に付けられた番号、記号その他の符号、画像若しくは音声によって当該個人を識別できるもの（当該情報だけでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む。）』と定義されている。簡単にいえば個人を識別しうる情報であり、その例として氏名、住所、年齢、電話番号、写真、職歴、資産状況などが該当する。

この個人情報の定義によればコンテキストも（個人を特定するIDなどが付与されてないとしても）個人情報に該当する。たとえば携帯電話は基地局と定期的に交信しており、交信している基地局によりおおよその位置を知ることができる。この位置情報はコンテキストに相当する。「電気通信事業における個人情報保護に関するガイドライン」では、携帯電話の位置情報は利用者の同意や法令によるものを除いて他人に提供しないとある。ネット上での行動履歴も仮想世界でのコンテキストであるが、ネットサービス事業者が公開している個人情報保護規約によれば、多くのサービス事業者がネットでの行動履歴を個人情報と解釈している。つまり、一般的にはコンテキストは個人情報として認識されていると考えてよい。

また、機微な情報についても触れておく。JIS Q15001:2006では個人情報においても特にプライバシー性が高いとされる「機微（センシティブ）な個人情報」という部類を定めている。これには保健医療、宗教、人種、犯罪歴、財務などが該当する。この機微な個人情報については収集は原則として禁止されている。（明示的な情報主体の同意、法令に特別の規定がある場合、司法手続上必要不可欠な場合は除かれる）

5　“見えない”コンテキスト

氏名や住所といった事項を記述するタイプの個人情報とコンテキストとでは性質が異なる。その対比を**表1**に示す。表中、1次情報とは当該個人情報が取得された段階での情報を指し、2次情報とは蓄積された1次情報を分析することにより新たに獲得される情報を指す。コンテキストの特徴を簡潔にいえば、（1）情報取得、（2）得られる情報の質、が見えないことにある。以下、この2点について述べる。

（1）情報取得

事項記述型の個人情報の場合、紙や端末を入力手段として情報を記載する。そのような取得プロセスからすれば、利用者は個人情報を提供する段階において情報提供という行動が意識できると共に、その際にサービス事業者の個人情報保護方針を確認することもできる。提供されるサービスと登録する個人情報の両者のバランスによっては、その場でサービス利用を中止するという判断もできる。

一方、コンテキストはその情報取得が潜在的である。最初にサービスの利用登録をする段階では利用者から承諾を得たり、個人情報保護方針を提示することも可能であるが、その時点では取得した具体的情報がなく、情報の

表1　事項記述型個人情報とコンテキストの比較

	例	情報取得	1次情報	2次情報
事項記述型 個人情報	氏名 (山田太郎)	情報を記述して登録 （明示的）	更新型 （または追記）	固定的 推測可能
コンテキスト （断片蓄積型）	位置 (13:10、東京駅)	装置が取得して記録 （潜在的）	蓄積型	漸増的 推測困難

確認ができない。そして、コンテキストの具体的情報の取得は利用者の意識を喚起しない形で行われる。これには2つの意味がある。一つは取得動作そのものが利用者に意識させず行われるというものである。このような例としては監視カメラやクッキー、Webビーコンなどが挙げられる。また、アクティブ型やUHF帯のRFIDタグも数メートル離れての交信が可能であるため、タグをリーダーにかざすという動作が不要となり、読み取りを意識させないことができる。

もう一つは利用者が取得に関与しているものの、それが個人情報の提供と意識されにくいというものである。その例として近接型ICカードが挙げられる。近接型ICカードは交通カードや電子キーとして広く利用されているが、読み取り距離が10cm程度であるためリーダーにかざす必要がある。リーダーにかざすという能動的動作を行っている時に、改札処理や解錠処理をしているという意識はあっても、活動情報としての個人情報が記録されていると意識することは少ない。

(2) 得られる情報の質

コンテキストとして得られる情報（1次情報と2次情報の両方において）がどのような重要性を持つかは、推測が難しい。位置情報で考えてみよう。収集された位置情報の秘匿性がどの程度かということは、人・時間・場所に依存し、一概にはいえない。ほとんどの場合において位置情報は特に秘匿すべきものではないかもしれないが、時々秘匿性の高い位置情報が発生する。そうすると、位置情報として蓄積された1次情報の中に秘匿性の高いものと低いものが混在する状態となる。事項記述型の場合には、事項ごとに秘匿性が高いか否かを判定することができ、しかもその秘匿性が時期によって変わるということはほとんど起きない。

また、1次情報を解析することにより獲得できる2次情報において、コンテキストはより高度な情報が導けるという大きな特徴がある。位置情報でいえば、ある人の位置情報を長期間にわたって取得することで、その人の住所、勤務地、通勤経路を推測することができる。頻繁にいく場所によってはその人の趣味・嗜好も推測できる。また、他の人との位置情報と照合することで、いつからどのくらいどこで会っていたかも推測できる。コンテキストにおける2次情報は1次情報の蓄積量に比例してその質・量・確度が拡大していく。

さらには機微な個人情報に相当するものも取得することができる。たとえば、特定の医療機関によく行くことが分かれば保険医療に関する情報が推測できる。よく利用する店によっては資産・所得状況も推測できる。4節で述べたようにこれらの情報は同意なしには取得できない情報である。

事項記述型の情報でいえば、それ自体から2次的に引き出せる情報は多くはない。たとえば、氏名から派生的に引き出せる情報としては性別ぐらいである。また、機微でない事項情報から機微な事項情報を導くことはほとんどできない。

2次情報の質は2節で述べた解析技術によっても変わる。監視カメラを例に考えてみよう。監視カメラが単に映像を記録するだけの機能しか有していない場合、特定個人がカメラの前を通過したという情報は記録映像に潜在しているものの、それを顕在化するためには人手による解析が必要となる。恒常的に人手による解析を実施するのは多大なコストがかかるため、特定の人が通ったかどうかという情報は現実的には2次情報としては得られないことになる。しかし、監視カメラに顔認識処理が組み込まれたとすると、顔画像を登録すれば特定の人が通ったかどうかという情報が常時かつ低コストに得られることになる。つまり顔認識処理という解析技術が2次情報を拡大するのである。また、位置情報の場合でも、位置情報取得が機能するエリアや検出する位置の精度によって2次情報の質が変わってくる。

この得られる情報の質が定まらないという点は、利用

者だけでなくサービス事業者にとっても悩ましい問題である。個人情報保護法第16条で「利用目的の達成に必要な範囲を超えて取り扱ってはならない」という最小限原則が定められている。昨今の個人情報の利用においても、不要な個人情報は積極的に破棄するという運用が見られる。しかし、コンテキストの場合にはどこからどこまでが十分な量かという判断が難しい。また、元々の利用目的のためには不足しているが、目的外の情報が取得されてしまったという事態も考えられる。これらの情報の管理の手間や漏洩した場合のことを考えるとサービス事業者にとっても扱いが難しい。

6　コンテキスト活用への方策

ユビキタスを提唱したマークワイザーの論文“The Computer for the 21st Century”は、“The most profound technologies are those that disappear.”（最も深遠なる技術は見えなくなる技術である）という文から始まる。[3] 奇しくもコンテキストの特徴とはこの見えなくなる点にある。見えないという特徴は人に無用な注意を喚起しないという意味では優れている。しかし、人の活動に関する詳細な情報を知らないうちに取得するという点においては人にプライバシー侵害の危惧を抱かせてしまう。この危惧はしばしば“監視社会”という呼び方で表現される。

コンテキストによるプライバシー侵害への危惧は根強く、欧米においてはRFIDに対する利活用を用途別に制限しようという動きが見られる。欧州議会の科学技術評価会議（STOA）が2006年に発表したレポートによれば[4]、RFIDを利用したサービスでは現在までのところプライバシーを侵害する重大な事件は起きていないと報告されている。しかし、社員の入退室にICカードを用いたり、来場者にICタグを持たせてトラッキングするサービスは現実に稼働しており、しかも監視されている方にはそのことがあまり意識されていない。得られたデータを濫用する事件はこの先起こりうると指摘している。

また、カリフォルニア州の上院では運転免許証へのRFIDタグの搭載および公立学校などが生徒の活動を記録するRFIDの使用を3年間禁止する法案が2007年に採択されている[5]。

コンテキストを活用したサービスとそれに対するプライバシー侵害の懸念が共に拡大している現在、何らかの事件が起こればコンテキストの利用を抑制する方向へ一気に傾くこともありうる。コンテキスト活用を順調に拡大させるために、以下の3つの方策を提案する。

（1）コンテキストのプライバシーポリシーの詳細化

コンテキストを含めて個人情報の取り扱いはプライバシーポリシーで利用者に公開されている。しかし、詳細に記述されているものはほとんどなく、サービス事業者がどのような情報を得て、どのように利用しているかの詳細が不明である。このような状態では、プライバシー侵害の懸念を払拭することは難しい。

サービス事業者はコンテキストの取得・利用について詳しくかつ分かりやすく説明する必要がある。1次情報については、取得間隔、精度、蓄積期間、個人を特定する情報が付随しているかなどについて説明する必要がある。2次情報についても、適用する解析技術、他人のコンテキストと照合するかどうか、などについて説明することが必要である。

（2）コンテキスト取得の制御

コンテキストから得られる2次情報は利用者とサービス事業者の双方にとって予測できない。そうであれば、不要なコンテキストは取得しないよう制御するべきである。たとえば、サービスがある地域やある時間帯だけを対象としているのであれば、サービス外でのコンテキストは取得しない。また、必要がなければ個人を識別する情報と結びつけないことが挙げられる。

また、利用者がコンテキストの提供を望まない条件があるならば、それを手動もしくは自動で容易に実行できる仕組みを備えておくことも必要である。

（3）利用者への直接的便益の提示

プライバシーは、個人情報と便益のバランスが重要である。コンテキストが持つ情報は大きいため、サービス事業者はコンテキストの価値に見合う便益を提示する必要がある。

アメリカのマーケティング会社が行ったRFIDに関する調査[6] によれば、利用者は直接的便益が明確な応用事例に対して肯定的であるとの結果が出ている。肯定的な応用分野としては、パスポート・免許証への貼付、高齢者監視、薬品の真正証明が挙げられている。総じて言えば、これらは安全という直接的便益を実現している。また、プライバシー侵害が議論となりながらも普及が拡大している監視カメラも、安全という便益をもたらしている。（ただし、監視カメラは捜査能力が高いことを示しているものの、犯罪抑止効果については明確に証明されていない）一方でこの調査では商品へのRFIDタグ貼付は利用者への直接的便益が明確でないために否定的であったと報告されている。この用途はサービス事業者にとっての便益が

主目的となっており、利用者への便益がおざなりになっている感がある。サービス事業者だけの便益だけでは利用者からの理解は得られない。

7 ま と め

コンテキストは、ユビキタス技術の発展に伴ってその利用が可能となってきた個人情報であり、ユビキタスサービスの基盤となる重要な情報である。しかもコンテキストの持つ情報は従来の個人情報と比較すると非常に大きく、これを活用した社会的便益の高いサービスが期待されている。また、現在の技術ではコンテキストを低コストで常時取得することも可能となってきている。

しかし、コンテキストは利用者にとって詳細が見えない個人情報である。この見えなさが利用者からプライバシー侵害の懸念を生じさせているといってよいであろう。サービス事業者は、事項記述型の個人情報より慎重にコンテキストを取り扱う必要がある。

寄付講座では、コンテキストを利用したユビキタスサービスの普及を促進するための方策についてさらに詳細に追究していきたいと考えている。 ◆◆

■参考文献

1）青柳武彦：“サイバー監視社会”，電気通信振興会，2006年
2）岡村久道，新保史生：“電子ネットワークと個人情報保護”，経済産業調査会，2002年
3）http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html
4）http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf
5）http://www.aclunc.org/issues/technology/blog/california_rfid_bill_signed_into_law_today_by_governor.shtml
6）http://www.rfidjournal.com/article/articleview/1491/

●筆者紹介

下畑光夫：Mitsuo Shimohata. 東京大学大学院情報学環客員准教授