ベネディクト・ブフナー

ユビキタス・コンピューティング時代におけるプライバシー

村 上 康 二 郎 (訳)

本稿は,「ユビキタス・コンピューティング」におけるプライバシーの意義について論じたものである。本稿の第一部では,私は,ユビキタス・コンピューティングを定義する。すなわち,この形態のコンピューティングにおいて,特別なものは何かということである。第二部では,ユビキタス・コンピューティングのデータ・プライバシー法に対する特別な影響に焦点を当てる。最後に,第三部では,データ・プラバシー法がユビキタス・コンピューティングの影響にどのように対応していくことができるのかという問題について,解答することを試みる。

A. ユビキタス・コンピューティングの定義

「ユビキタス・コンピューティング」は,90年代初頭に,Xerox PARCのコンピュータサイエンス・ラボにいたマーク・ワイザーによって,はじめて提唱されたものである。ワイザーは,21世紀に向けて,科学技術は目に見えなくなる方向に進むものと予測した。すなわち,どこでもコンピューターである。彼は,この新しい形態のコンピューティングを「ユビキタス・コンピューティング」と呼び,次のように定義した。「目に見えない,どこでもコンピューターであり,それはどんな種類のパーソナルデバイスの中にもなく,どこにでもある木製品の中にある」[1),と。ユビキ

タス・コンピューティングは，コンピューターの世界における「第三の波」を表している。第一の波においては，一つの (大型) コンピューターが多数の人々によって共有され，第二の波 (パーソナル・コンピューターの時代) においては，各人が自分のコンピューターを所有するようになる。これに対して，今，我々は第三の波 (ユビキタス・コンピューティングの時代) に突入しようとしており，そこでは，一人の人が，生活の環境の中にとけ込んでしまった多数のコンピューターに囲まれることになるのである。

今のところ，我々の身の回りにあるほとんどのコンピューターは，目に見えるものであり，コントロール可能なものである。例えば，私のラップトップ PC，PDA，携帯電話などがそうである。そのような技術的なデバイスを異なった種類のネットワーク (オンライン・ワールド，携帯通信ネットワークなど) に入るために利用するかどうかを判断するのは私である。そして，それらのネットワークから離れ，現実世界に戻るために，「ログオフ」するかどうか，そしていつ「ログオフ」するのかを判断するのも，私である。しかし，コンピューターはさらに拡散し，コントロール不可能なものになる。携帯電話がよい例である。携帯電話は，はじめは，誰か他の人と時々話すための道具として使われていたが，今日では，次第に，様々な種類のネットワークと常に接続するためのゲートウェイに発展してきている。携帯電話によって，インターネットに接続するし，携帯電話によって，メッセージを受信したり，送信したりするし，携帯電話によって，リアルタイムの全地球測位システム (GPS) に接続する。携帯電話によって，私はそれら全ての異なったネットワークのメンバーになるのであり，それらのネットワークの中を動き回り，それらと常に接続していることになる。しかしながら，携帯電話は，ユビキタス・コンピューティングの典型例ではない。というのは，我々は，現在でも携帯電話をコミュニケーションの道具と受けとめており，意識的にそのようなものとして利用しているからである。むしろ，ユビキタス・コンピューティングの時代

においては，コミュニケーションの道具は小型化し，実際には目に見えないものになる。すでに今日においても，コンピューターは，デスクトップPCの中にあるだけではなく，至るところに存在している。例えば，電気製品，家，自動車，基本的なインフラ施設などである。このようなコンピューター製品の小型化および進歩は，今後も続いていくことになる。さらに進むと，それらのコンピューターは，腕時計，衣服，食品の包装，値札などの我々の日常生活における身の回りのものにも埋め込まれるようになるであろう[2)]。それらのコンピューター製品が知覚できない，目に見えないものになればなるほど，我々は，それらが自分の個人情報を他者に伝達しているのかどうか，またどのように伝達しているのかということに，気づかなくなるのである。

ユビキタス・コンピューティングの典型例は，RFID（radio frequency identification）タグである。RFIDタグは，超小型のタグであり，情報を発信するが，この情報は離れたところからRFIDリーダーによって読みとることができる。これらのタグは，より小さくなり，また製造コストが安くなってきているので，広範囲にわたる製品において，周りの環境と情報をやりとりすることを可能にするために，利用されるようになっている。現在用いられているRFIDタグの具体例としては，以下のようなものがある[3)]。

— パスポート内のRFIDタグ（パスポートに記載してある情報だけではなく，例えば旅行履歴のようなものも記録している）
— 公共交通料支払のためのRFIDタグ（例えば，公共交通用の定期券に埋め込まれており，この定期券が有効かどうか，またいつまで有効かという情報を発信する）
— 在庫管理や商品トレーサビリティ確保のためのRFIDタグ
— 動物をID管理するためのRFIDタグ

データ・プライバシーの観点からは，その所持者に関する個人情報を送

信するような類の RFID が特に関心事となる。しばしば言及される例としては，ショッピングカード (frequent shopper cards) に埋め込まれる RFID タグがある。RFID タグは，私がスーパーマーケットの建物に入るとすぐに，ショッピングカードが，その建物内の RFID リーダーと「交信」することを可能にする。RFID のおかげで，スーパーマーケットは，いつ私が店内に入り，いつ出たのかを知るだけではなく，私が売り場の中のどこを通ったのかということや，どのような商品を見て，購入したのかということまで知ることになる。これら全ての個人情報の伝達は，私に通知ないし予告無しになされることになる。これが，RFID をラップトップ PC や携帯電話と異なったものにするのである。ラップトップ PC をインターネットに接続させる場合，私は自分がサイバースペースに入るということに気づいている。携帯電話のスイッチを入れる場合，私は遠距離通信のネットワークに接続するということに気づいている。それに対して，RFID を装着したショッピングカードをスーパーマーケットの RFID リーダーに接続させるためには，何らの積極的な行動を必要としない。私は自分のカードの「スイッチを入れる」のではなく，単に売り場に入って歩き回るだけである。

このようなコミュニケーション・プロセスの意識的な開始の欠如は，ユビキタス・コンピューティングに共通した特徴である。コミュニケーションの道具として受けとめられていない我々の日常生活における身の回りのものも，コミュニケーションを自動的に開始するようになる。ショッピングカードだけではない。「スマート冷蔵庫」は，自動的にその中身をチェックし，新鮮な牛乳を注文するし，「スマート衣服」は，心臓を頻繁にチェックして，そのデータを健康管理センターに送信する。あるいは，子供の腕時計の中にある GPS チップは，常にその位置を「児童追跡」サービスステーションに伝達するのである。

B．ユビキタス・コンピューティングと データ・プライバシーへの影響

これまで述べてきたようなユビキタス・コンピューティングの特殊な性格は，データ・プライバシーに対する特別な影響を生じさせる。

I．データ処理の量

第一に，ユビキタス・コンピューティングは，より多くの個人データを作り出す。これまでは，私がスーパーマーケットに入る場合に，ほとんど誰も，私が誰であり，どこから来て，何を買ったのかということに気づかなかった。私が現金で支払ったとすれば，実際に私が残す個人データは，全く存在しないことになる。ユビキタス・コンピューティングの時代においては，私は，大量のデータのトラックを作り出し，そして残すことになるであろう。RFIDタグを埋め込んだショッピングカードのおかげで，スーパーマーケットは，私が店内に入るとすぐに私のことを識別することになる。スーパーマーケットにおいて私が行った全ての歩みおよび行動は，ショッピングカードのRFIDと常に通信するRFIDリーダーによって記録されうる。いつスーパーマーケットに入ったのか，お店のお酒売り場でどれぐらいの時間を費やしたのか，お店の中のどの道を通ったのか，何を購入し，いくらのお金を使ったのか，そのような全ての情報は，もはや匿名のものではなくなり，記録され，そして私個人と結びつけられることになる。

この種のデータの処理が買い物をより快適なものにすることは疑いがない。支払いのためにレジに並んで待つ必要はなくなるのである。買い物かごに入れた全てのものは，直ちに記録されることになる。というのは，シッピングカードの中のRFIDタグおよび買い物かごに入れられた商品の中にあるRFIDタグと，スーパーマーケットのRFIDリーダーが「交信」

することになるからである。このようにして，お店を出るときには，レジで支払いをする代わりに，全てのものが自動的にクレジットカードの取引額に加算されることになる。また，RFID のおかげで，買い物はより，当該個人に特化したものになる。というのは，スーパーマーケットは，私がする全ての買い物によって，私および私の好みをよりよく知るようになるからである。そして，スーパーマーケットが私のことをよく知れば知るほど，その情報およびマーケティングは，私個人に特化したものになる。しかしながら，まさにこのデータ処理の増大が，データ・プライバシーに対する大きなリスクを生じさせることになる。私の買い物の完全なパターンを私が気に入っているお店に知られたとしても，おそらく私は気にしないであろう。このお店が，長期間にわたって，私の買い物の特徴に関する詳細で完全なプロフィールを保有することになったとしても，おそらく私は気にしないであろう。しかし，私の買い物に関する個人的なプロフィールを他の会社に売られてしまうとなると，どうであろうか。私の健康保険会社や雇用者が私のニコチンやアルコールの消費量に関心を持ったとしたら，どうであろうか。

II. データ処理の質

ユビキタス・コンピューティングは，個人データの量を増大させるだけではなく，データの質を高める。これは特に，位置情報に当てはまる。伝統的なインターネットと異なり，ユビキタス・コンピューティングの領域では，ユビキタス・コンピューターの物質への埋め込みという観点から，物質空間 (physical space) が重要となる。ユビキタス・コンピューティングは，今現在の位置に関する情報に基づいた，多様な位置サービスを作り出す (あるいはすでに作り出している)。位置サービスの典型例は，位置に基づく情報サービスである。例えば，特定の高速道路の出口に向かって車を運転している際の，レストランやガソリンスタンドなど，近くの「興味のある場所」に関する情報である。それら全ての位置サービスは，

行動に関する広範な追跡と記録を伴うものであり，これは詳細な「行動履歴」という形で残ることになる。これについても，私は，私のサービス提供者がこれら全ての情報を保有するということを気にしない。しかし，この情報が他の販売会社に売られてしまったとしたら，どうであろうか。警察や税務署が私の行動履歴に興味を持ったとしたら，どうであろうか。

iii. データ処理の不可視性

最終的に，ユビキタス・コンピューティングに特徴的な問題は，処理されるデータの量および質だけではない。我々が，自分の個人データが処理されることに気がつくかどうか，またどのように気がつくのか，ということも問題となる。ユビキタス・コンピューティングは，個人データの処理が日常の出来事になるということを意味する。データの処理は，日常生活における「正常」かつ不可欠な一部分となる。必然的に，我々はこの毎日行われることに慣れてしまい，もはや人間性および独立性に対するリスクに気がつかなくなるであろう。データの処理がより普及し，データ処理の装置がより小型化して，目に見えないものになればなるほど，我々は，自分の個人データが記録され，処理されることに気がつかなくなるであろう。ユビキタス・コンピューティングの「父」であるマーク・ワイザーは，「コンピューターを埋め込み，そのものに適合させ，自然なものにすることによって，我々がそれについて考えることなしに使えるようにする」ということが，ユビキタス・コンピューティングの最高の理想であるとしている。データ・プライバシーの観点からは，このことは，我々が自分の個人データの処理について考えなくなるということを意味する。

C．データ・プライバシー法による対応

データ・プライバシー法は，これまで述べてきたような影響に対して，どのように対応すべきなのだろうか。我々は，データ・プライバシーに関

する新しい法律および新しいコンセプトを必要とするのであろうか，それとも現在のプライバシー法で，十分なのだろうか。

Ⅰ. ユビキタス・コンピューティングに関する特別な法律

現在のデータ・プライバシー法が，ユビキタス・コンピューティングの特別な影響に対して，十分に対応できるかどうかは，まず何よりも，データ・プライバシー法の基本的なコンセプトにかかっている。この基本的なコンセプトは，我々が対象とする法体系によって異なっている。ヨーロッパのデータ・プライバシー法の基本的なコンセプトは，個人データの処理は，法によって許容されるか，データ主体が同意を与えた場合を除いて，禁止されるというものである[4)]。このように，ヨーロッパのデータ・プライバシー法の出発点は，彼または彼女が明確に同意をしていない個人データの処理から，個人を保護するということである。これは，ユビキタス・コンピューティングにも当てはまる。従って，ヨーロッパの立法者がさらなる行動を起こすかどうかにかかわらず，プライバシーの基本的なレベルは保障されることになる。

これに対して，アメリカのデータ・プライバシー法の出発点は，個人データを含むデータの自由な流通にある。データ処理者は，データの処理が法によって禁止されていない限り，個人データを自由に収集し，利用し，移転させることができる。従って，これまで述べてきた新しい形態のデータの処理が，データ・プライバシーに対する新しいリスクを生じさせると考えるのであれば，ユビキタス・コンピューティングの特別な影響に対応する追加的な立法措置がより強く必要とされることになる。現在，アメリカ合衆国の様々な州が，ユビキタス・コンピューティングとりわけ RFID 技術に関する問題を規律するための法律を導入しようとしているか，もしくはすでに導入している。特に，これらの法律は，ID カードへの RFID の装着[5)]，RFID によるトラッキングまたは識別[6)]，人体への RFID の埋め込み[7)]，商品およびその包装への RFID の装着について[8)]，規律してい

る。これらのプライバシー法案が用いている法的手段は多様であるが，おおむね共通しているのは，以下の点である[9]。

— RFID の使用を開示する必要性
— RFID タグが「私的な領域」に入る前に，RFID タグを除去するかまたは無効化する必要性
— 個人を識別しうる情報が，RFID によって収集されたデータと照合され，保存される前に，データ主体から書面による同意を取得する必要性
— RFID データと個人情報をリンクすることの禁止
— 人体への埋め込みのような RFID のその他の利用の禁止

II. 一般的なデータ・プライバシー法

アメリカ合衆国の法律と異なり，ヨーロッパの法律は，ユビキタス・コンピューティングの影響に対する対応については，なお一般的なデータ・プライバシー法に依存している。しかし，このことは，ヨーロッパの立法者が，ユビキタス・コンピューティングの問題に気がついていないということを意味しない。むしろ，現在では，RFID 技術は注目の的になっている。欧州委員会にとっては，RFID に関するプライバシー問題についてヨーロッパで共通した対応を確認する明確な必要性が存在する[10]。欧州委員会によって進められている審議および交渉の結果次第では，委員会の立場から，さらなる立法による介入が必要とされるかもしれないし，あるいは現存する法的枠組みの明確化が必要とされるかもしれない。

1. 同意の役割

ユビキタス・コンピューティングについて，現在，議論の中心となっている問題の一つは，将来における同意の役割である。これまでは，個人の同意は，個人データの処理のための主たる正当化根拠の一つであった。同

意は，個人の自由および自主性を表している。彼または彼女の個人データが処理されてよいかどうか，またどのように処理されてよいのかを判断するのは，国家ではなく，当該個人である。同意は，関係者がデータ処理の仕方を判断することを可能にする。

しかしながら，同意による正当化は，批判を浴びている。プライバシー学者は，同意は単なる擬制に過ぎないと主張している。というのは，ほとんどの場合において，当該個人は，通知を受けていないし，個人データの処理について同意をするかどうか，そしてどのように同意をするかということについて，自主的に判断する自由を有していないからである。さらに，個人は，しばしば，自らの個人データの処理について同意を与えているということにすら気づいていない。これは，とりわけ，同意が日常の行為の一部としてなされる場合に当てはまる。特に，後者の問題は，ユビキタス・コンピューティングにおいても基本的な課題となる。ユビキタス・コンピューティングの特殊な性格は，それが日常生活において，頻繁に生じるということである。身の回りにある全ての「スマート」な装置のおかげで，我々は常にネットワーク環境に接続され，そして同時に自分の個人データが常に外部とやりとりされることになる。このようにして，同意をデータ処理の主たる正当化根拠として用いるということは，我々が頻繁に無数のデータ処理行為に対して同意を与えなければならないということを意味することになってしまう。結論は，もはや実現不可能であることを理由に同意による正当化を止めるか，もしくは，同意による正当化を継続しつつ，我々が何をしているのかを通知するのをやめ，次第にそして無意識のうちにプライバシーを失うかのどちらかである。

2. 包括的なプライバシー規定は選択肢としてありうるか？

他方で，同意よりも適切な選択肢が存在するとは思えない。もちろん，ユビキタス・コンピューティングに特化した包括的なプライバシー規定を設けるということも可能である。しかし，包括的な規定は，プライバシー

法において，これまで必ずしも成功した方法ではなかった。個別の規定によって，データ処理のあらゆる側面を網羅するのは，実際上は不可能である。それゆえ，立法者が予測できないか，または詳細に規定することができない全ての事実を規律することを目的とするある種の包括的規定が常に存在している。代表例は，ヨーロッパのデータ保護指令（Data Protection Directive）7条の中にある一般的利益のための規定である。7条fによれば，「管理者によって追求される正当な利益のために処理が必要とされる場合には，個人データは処理されうる。……ただし，データ主体の基本的な権利および自由のための利益が優先する場合には，この限りではない」。現実問題としては，包括的規定は，データ処理者が自らの裁量によって，個人データを収集，利用，移転することに対して，扉を大きく開けることになる。従って，最終的には，これらの包括的規定は，他のより詳細なプライバシー規定によって設定される限界を無意味にしてしまうことになる。

3. 正当な同意の要件

最終的に，私は，同意の有効性に関する厳格な要件が満たされる限りにおいて，ユビキタス・コンピューティングの領域においても，同意がデータ処理のための主たる正当化根拠とされるべきであると主張したい。有効な同意となるためには，以下の4つの要件が満たされていなければならない。同意は，任意になされなければならない。同意は，明確なものでなければならない。同意は，通知がなされた上で与えられなければならない。同意は，撤回可能なものでなければならない。

任意性：同意は，任意になされたものでなければならない。ユビキタス・コンピューティングが広まれば広まるほど，個人がネットワーク環境に参加することを欲するかどうかを完全に自由に判断しうるということが重要になる。直接的であるか，間接的であるかを問わず，何人も，ネットワークに参加し，そして彼または彼女の個人データを共有することを強制

されてはならない。任意性の原則は，以下のことも要請する。すなわち，データ処理者は，商品またはサービスを取得する他の手段が個人に提供されないか，または合理的に提供されない場合に，個人の同意を条件として商品またはサービスを提供することをしてはならないということである。

明確性：同意は，明確なものでなければならず，あいまいさを残さずに与えられなければならない。RFID が備えられたスーパーマーケットの例では，例え RFID 技術の存在が売り場の入り口で明確に示されたとしても，単に顧客がそのようなスーパーマーケットに入ったという事実だけでは，特定のデータ処理の形態に対して黙示的に同意を与えたということはできない。そうではなく，顧客が特定のデータ処理の方法に対して明示的に同意を与えた場合にのみ，同意の存在が認められる。他方で，同意がデータ処理の一つ一つに対して個別的に与えられる必要はない。むしろ，一般的な形態の同意は，一つの共通した種類のデータ処理行為を包含するものとして与えられる。RFID が備えられたスーパーマーケットの例では，この一般的な同意は，そのスーパーマーケット内で行われる全てのデータ処理行為を包含することができる。

通知：全ての同意は，事前に通知がなされている場合にのみ有効である。RFID が備えられたスーパーマーケットにおけるデータ処理に対して同意を与える顧客は，当該データが収集されるという事実を通知されるだけでは不十分である。それだけではなく，どのような種類のデータが収集されるのか，どのような目的のためにデータが収集されるのか，どれぐらいの期間データが保存されるのか，データが第三者と共有されるのか，データが他のデータと結合されるのかについても，通知がなされなければならない。通知される情報は，包括的なだけではなく，理解可能なものでなければならない。

撤回可能性：最後に，とりわけ，同意はいつでも撤回可能なものでなければならない。撤回は，異なった形態が想定されうる。明示的に通知することもできるし，あるいは，技術的手段を用いて表示することもできる。

例えば,RFIDタグの無効化・除去や,いわゆるRFIDブロッカーの利用などである。

D.結　論:「ログオン」および「ログオフ」する自由に対する保障としての同意

ユビキタス・コンピューティングの大きな脅威は,我々がもはや「ログオフ」することができないということである。なぜなら,我々は,自分と自分の情報を交換するスマート・オブジェクトおよびネットワーク環境によって接続され,取り囲まれることによって,常に「ログオン」することになるからである。このユビキタス・コンピューティングによる影響に対して,我々は,どのように対応することができるのであろうか。また,この遍在性(ubiquity)を,どのように限界づけることができるのであろうか。法的限界を設定する有効な方法は,個人の同意である。同意が,データ処理のあらゆる行為について要求されるのであれば,データ処理は,もはや目に見えないものではありえないし,拡散したものにもなりえない。なぜなら,常に,当該個人による何らかの積極的な行動が必要とされるからである。

理論的には,ユビキタス・コンピューティングは,「どこでも」という「一つ」の包括的なコンピューティング環境であると考えられている。しかしながら,現実には,ユビキタス・コンピューティングは多数の異なった部分または「仕切られた空間(zoned rooms)」から構成されており,それゆえ容易に認識し,管理することができるものである。RFIDが備えられたスーパーマーケットは,「仕切られた空間」として見ることができる。自由かつ通知がなされた上での同意がデータ・プライバシー法の中核にあるとするならば,私がこの空間に入るかどうか,そして私の個人データが処理されてよい(「ログイン」)のかどうかは,私の自主的な判断による。そして,(同意が撤回可能であるならば)私が,この「仕切られた空間」

を再び去り，私の個人データの処理を終了させる（「ログオフ」）のかどうかについても，同様に私の判断による。従って，同意は，ユビキタス・コンピューティングの影響に対して対応するための，データ・プライバシー法における実現可能な手段であると思われる。

1) *Xerox Palo Alto Research Center*, Ubiquitous Computing (no pages); available at www.ubiq.com/hypertext/weiser/UbiHome.html.
2) *Kang/Cuff*, Pervasive Computing: Embedding the Public Sphere, 62 Wash. & Lee L. Rev. 93 (2005), 93 (97).
3) これらの全ての具体例については，http://en.wikipedia.org/wiki/RFID を参照。
4) See Art. 7 of the European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data (95/46/EC) of 1995.
5) 例えば，カリフォルニア州上院法案（California Senate Bill）768は，高感度で大衆向けの州発行 ID カード（運転免許証，K-12学生 ID カード，政府健康保険証，公共図書カード）に装備される RFID タグについて，プライバシー保護およびセキュリティ対策を要求している。
6) 例えば，ロードアイランド州下院法案（Rhode Island House Bill）5929は，州または市の機関に対して，給付またはサービスを付与する条件として，従業者，学生，顧客の行動および身元を追跡することを禁止している。
7) 例えば，南ダコタ州下院法案（South Dakota House Bill）1114は，RFID 技術の人体における利用を制限している。
8) 例えば，ネバダ州下院法案（Nevada Assembly Bill）264は，RFID タグを装着した商品の購買者に対して通知を行うことを要求している。
9) See *National Conference of Senate Legislatures*, 2005 Privacy Legislation Related to Radio Frequency Identification (RFID); http:// www. ncsl. org/ programs/ lis/pivacy/ rfid05.htm.
10) *European Commission*, Radio Frequency Identification Devices (RFID): Frequently Asked Questions on the Commission's Public Consultation, MEMO/06/378 of October 2006.

［訳者後記］

本稿は，2007年２月21日に立命館大学において行われた，2006年度第３回法政研究会におけるベネディクト・ブフナー博士の講演原稿（Privacy in the Age of Ubiquitous Computing）を翻訳したものである。ブフナー博士は，ミュンヘン大学，アウグスブルク大学で法律学を学ばれ，2002年にはカリフォルニア大学ロサンゼルス校（UCLA）で LL. M を取得されている。現在は，ブレーメン大学の講

師である。もともとは，国際私法，国際民事訴訟法などを研究されていたが，最近は，情報法など科学技術に関する法律問題を精力的に研究されている。

講演会当日は，指宿信教授(立命館大学)が司会をされたほか，夏井高人教授(明治大学)，渡辺惺之教授(立命館大学)などが参加され，活発な議論がなされた。講演では触れられなかったが，プライバシーについては，米国の9.11テロ以降に，ホームランドセキュリティが強調され，方向性が大きく変わったように，セキュリティや安全性の要請とのバランスをいかにしてはかっていくのかが問題になるという指摘があった。また，講演では，RFIDを中心に議論がなされていたのに対して，将来のユビキタス社会では，RFIDだけではなく，ビデオカメラやセンサネットワークなどが至るところに設置されるようになるが，これによって生じるプライバシー問題をどのように考えるのかといった指摘がなされた。

本稿でも述べられているように，ユビキタス・コンピューティングでは，超小型のマイクロコンピューターを身の回りのあらゆるものに埋め込むということが目指されている。目に見えない超小型のコンピューターやセンサを張り巡らし，個人に関する情報をできるだけ多く取得することによって，当該個人に特化した，当該個人に最適なサービスを提供しようというものである。これによって利便性は増すが，同時にプライバシーが危機にさらされることになる。このようなユビキタス・コンピューティングにおけるプライバシー問題について，著者は，本人同意の取得を重視すべきであるとしている。基本的には妥当な方向性を示しているものと考えられるが，厳密な意味での本人同意を常に要求することが，技術的に実現可能なのかどうか，またユビキタスの本来の理念に反しているところがないか，課題は多く残されている。利便性，プライバシー保護，安全性といった矛盾した要求をいかに調和していくのか，多方面からの議論が必要であると考えられる。

最後に，本翻訳の機会を与えていただいた指宿信教授に，この場を借りて感謝申し上げる次第である。