プライバシアウェアなユビキタス環境構築のためのシステム
－個人情報の利用内容をユーザ自ら制御－

1. 背景

無線通信技術の発達や計算機の小型高性能化により計算機は日常空間に埋め込まれるようになり，やがてその存在が空気のように当たり前で透明な存在になることが期待される．このような環境はユビキタス環境と呼ばれ，1990 年代初頭より研究されてきた．このような環境下では，空間に張り巡らされたセンサやアクチュエータの連携により，状況に依存した空間やデバイス機能の再構成などが可能になり，人間とコンピュータの新たな関係が期待される．これを実現する技術はコンテクストアウェアネス（Context-awareness）と呼ばれ，近年研究が盛んである．しかしながら従来は，コンテクストとそれに応じた振る舞いはセンサから得られた情報をもとに開発者により決定されており，利用者の真の要望との乖離を招くことがあった．

特に，コンテクストアウェアネスを実現する上で必要不可欠である個人のプライバシに関わる情報（プライバシ情報）については，享受するサービスレベルと提供する情報の重要性との間には個人毎にトレードオフが存在すると考えている．

2. 目的

このような背景から本プロジェクトでは真に実用的なシステムを提供するために，適応に関する個人の嗜好（プレファレンス）を反映した適応を実現する機構を構築することを目的とする．特にシステムが適応動作をとるにあたり，個人が提供を許可する個人情報および情報の取得方法をプレファレンスとして扱うこととする．これにより，利用者とサービス提供者間でプライバシ情報の扱い方に関するコンセンサスを確立し，なおかつ与えられた情報に応じた適応動作をすることで安心感と快適さの双方を提供することを目的とする．

なお，このようなシステムはプライバシ情報を意識していることからプライバシアウェア(Privacy-aware)であると呼ぶことにする．

3. 開発の内容

本プロジェクトでは，ユビキタス環境におけるサービス提供時に必要となる，ユーザ自身によるプライバシ情報提供制御を行うための基盤ソフトウェア PENATES（ローマ神話における家庭の守り神）; Privacy protEctioN Architecture for contexT-aware EnvironmentS）およびこれを使用した実証アプリケーションを開発した．

基盤ソフトウェアとしては，１）サービス提供者側の個人情報利用ポリシ（以下，ポリシ）と利用者側の個人情報提供ポリシ（以下，プレファレンス）の比較機能，２）比較結果に応じた情報提供機能，３）利用者への実行時問い合わせ機能，４）サービス提供領域への利用者侵入を契機として当該空間で提供されているサービスのポリシを利用者所有の端末に対して配信し，１）～３）の処理の後に得られた情

報をアプリケーションに配信するサービスビーコン機能，５）アプリケーションとサービスビーコンの連携フレームワーク，で構成される．なお，１）～３）の機能を担うソフトウェアエンティティをプライバシエージェントと呼ぶ．

ポリシには，収集情報・収集目的・使用期限・使用者といった情報を記述する．また，情報の収集目的をあらわす要素に対して，それがサービス提供のために必須のものか，付加価値を与えるものかを指定する属性）を記述する．一方，プレファレンスには受入れることができる（できない）ポリシと，該当するポリシが存在したときの処理を記述することができる．該当ポリシが存在した場合の処理としては，１）常に提供または拒否，２）常に利用者に扱いを問い合わせる，がある．

実証アプリケーションとしては，１）Context-aware Trash box，２）Context scheduler の２種類を開発した．これらは，いずれも与えるプライバシ情報によって利用者に提供するサービスレベルが変化するものである．１）は，ゴミ箱に対して提供する情報（名前，年齢，廃棄場所）の量に応じて「リサイクル協力ポイント」として加算される得点が変わるというものである．２）は，グループウェアの一種であり，コミュニティ内で提供する情報（特定空間の現在の在室状況，スケジュール（在室退室予定））の量に応じて閲覧できる他者のスケジュール情報と付加サービスの種類が変化するというものである．

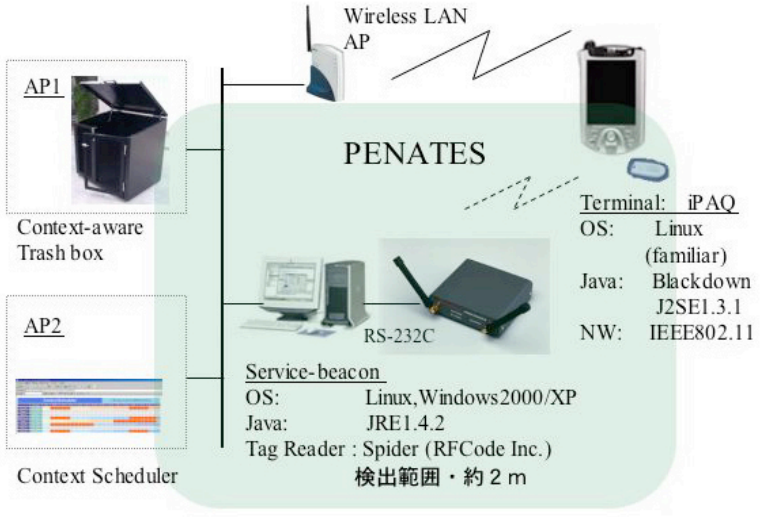

図１：システム構成

図１にシステム構成を示す．メッシュがけがしてある部分は PENATES が関与する部分である．サービスビーコンには RF タグ読み取り器が接続され， RFCode 社の Spider を用いた．2 メートル程度の検出範囲を持ち，端末に取り付けられたタグを検出する．ユーザ端末としては PDA を想定し，HP 社 iPAQ を用いた．OS には Linux を用い，プログラムは Java で開発した．ユーザ端末は無線 LAN による接続が確立されているという前提で，サービスビーコンが検出したタグ ID を持つ端末に対してのみポリシの URL を通知する．これによりサービス提供領域付近の端末にのみ

配信することを可能としている．アプリケーションは，必ずしもサービスビーコンと同一 LAN 上に存在する必要はなく，インターネットを介していても良い．

図２にプレファレンス設定により，情報の提供可否を常に問い合わせるとした場合の問い合わせ画面を示す（この場合は，user.address で表される住所）．YES または NO を明示的に指定することでその瞬間の利用者の情報の扱われ方についてのコンセンサスが得られたものとして扱うことが出来る．なお，プレファレンス上で常時提供可または拒否の指定をした場合にはこのような画面は表示されない．

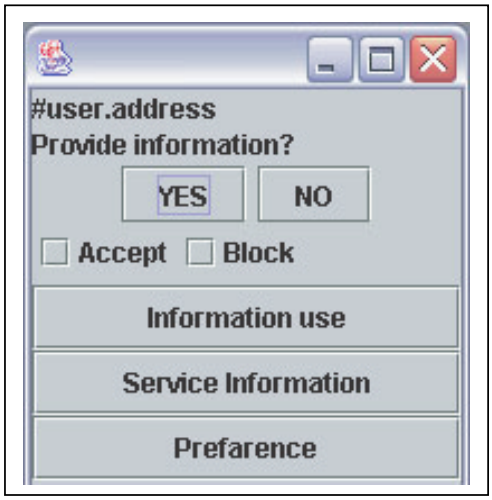

図２：利用者に情報の扱いを問い合わせる際の GUI

4.　従来技術との相違

プライバシ制御技術の標準動向（P3P）：本開発におけるポリシおよびプレファレンスの記述は P3P（The Platform for Privacy Preferences Project）をベースとした．P3P は Web サイトによるプライバシ情報の扱い方（プライバシポリシ）に関する標準として W3C 勧告となった．P3P では，従来，各サイトが自然言語で“プライバシポリシ”として記述し利用者に読ませてきたものを，利用者側のエージェント・ソフトウェアが利用者の基準と照合して自動的に処理することを可能とする．一方 P3P のサブプロジェクトとして，利用者のプライバシポリシに応じた情報提供の嗜好を記述する言語である APPEL（A P3P Preference Exchange Language）がある．

P3P が提供するポリシおよびプレファレンス記述の仕様を用いることでサービス享受と個人情報提供のトレードオフ解決を利用者を交えてシステマティックに実現することが可能になると考えられるが，P3P ではトレードオフ解決の機構までは規定していないため，我々が規定した．

多様な個人関連情報の利用：従来，P3P を用いたアプリケーションの例としてはインターネットを利用したオンラインショッピングなどが挙げられてきた．しかしながら，構築した２つのアプリケーションに見られるように，名前や年齢といった一般的に使用される情報の他に，スケジュール情報やネットワーク情報，ゴミの廃棄場所（ゴミ箱設置場所），空間内の在室情報といった情報も用いられる．特に，位置情報のような物理空間情報はユビキタス環境におけるサービスでは重要な要素であり，多様な情報を扱えることを示した．また，携帯端末に接続されたウェアラブルセンサや環境側に配置されたセンサに対する拡張機構を設けたため，さらに物理空間に依存したサービスにわずかな拡張で展開することが可能であると考える．

5. 期待される効果

個人関連情報の扱いを本人に委ねることに関して：本システム（PENATES）を用いることで，サービス提供者にとってはビジネスチャンスを逃すことが少なくなると考えられる．つまり，個人適応的なサービスを提供する際に必要となる個人関連情報の扱いについてユーザが意思を表示でき，提供されるサービスはそのコンセンサスがとれたものであることから，従来，情報漏洩などを懸念して敬遠していたユーザを取り込むことが出来ると考える．これまでもインターネット上のオンラインショッピングサイトなどでは個人情報の提供可否を問い合わせることはあった．しかし，情報の使用目的や使用者，使用期間などのポリシに相当する情報に関しては包括的で一般ユーザには理解しがたい．このため，享受できるサービス以上に情報を求められていると判断したユーザはサービス利用を中断していた．

本システムでは，提供する情報の扱いをユーザの意思で事前にあるいは実行時に決定し，それに応じて適切なレベルのサービスが提供されることで，ギブアンドテイクの関係を作り出すことが出来ると考える．

6. 普及の見通し

普及に向けての課題および新規サービス提供に関する作業は次のようなものがある．

ポリシおよびプレファレンスのエディタ：これらは，P3P で規定されたスキーマに基づき XML にて記述されるが，サービス提供者や一般利用者が容易に記述するのは困難である．そこで，記述を支援するためのエディタが必要となる．

サービス提供者とサービスビーコン運営者との連携：ショッピングモールなどでの利用の場合，モールの入り口などにサービスビーコンを配置し，これを第三者（サービスビーコン運営者）が運営することになる．サービス提供業者は，プライバシポリシを制定（記述）し，本プロジェクトで開発したアプリケーションフレームワークに則り新規開発あるいは既存部分とのアダプタを開発する．その後，ビーコン運営者との間で登録手続きをするが，現状ではこの過程を手動で行う必要があるため，オンラインで容易に追加変更が出来るようになることが望まれる．

ポリシに則った適正な情報利用の担保：本システムはサービス提供側が正直にポリシファイルを作成しており，定義通りの動作を行うという事が前提となっている．しかし，実際に個人情報が取り扱われる過程においては何の保証もしていない．そこで，今後は個人情報収集側がポリシファイルの定義した通りの動作を行っているかどうかを如何に検証し，保証するかという事が課題となる．

7. 開発者名

- 藤波香織（早稲田大学大学院理工学研究科；fujinami@dcl.info.waseda.ac.jp）
- 正寺朋子（同上；tomo@dcl.info.waseda.ac.jp）
- 中村暢芳（同上；nobusp@dcl.info.waseda.ac.jp）
- 山邉哲生（同上；yamabe@dcl.info.waseda.ac.jp）