2003－MBL－26　(7)
2003／9／26

ユビキタスコンピューティングにおけるプライバシ保護方式 EMAPP の提案

三田貴子[†]　山田茂樹[‡]　上岡英史[‡]

ユーザがいつでもどこでも移動しながら通信サービスを受ける事が可能なユビキタス環境では、ユーザのプライバシに関わるパーソナルデータを用いてサービスを行うため、このパーソナルデータのしっかりとした管理が求められる。本論文ではこのパーソナルデータを管理する新しい方法として EMAPP（Encapsulated data and Mobile Agent based Privacy Protection）を提案する。EMAPP はユーザのパーソナルデータとプライバシプリファレンスをユーザ管理下の閉じられた空間で管理し、外部に収集させない事、更にサービスを受ける場合には Mobile Agent を送り込ませ、処理結果だけを外部に出す事という 2 つの特徴により、強固なプライバシ保護を可能にする。

Proposal for a method of privacy protection in ubiquitous computing environments

Takako Sanda[†], Shigeki Yamada[‡] and Eiji Kamioka[‡]

Ubiquitous computing will enable mobile users to take communication services anytime and anywhere. However, as this new technology utilizes user's personal data related to his/her privacy to provide those services, a robust management for personal data is required. This paper proposes a new method, named *EMAPP (Encapsulated data and Mobile Agent based Privacy Protection)*, to manage personal data. EMAPP has two characteristics, it protects user's personal data and privacy preferences within closed space where only the user can controls, and keeps them from being collected by outside parties. When the user requires to take a service, a mobile agent sent by a service provider executes instructions for the service within the closed space and only generated results are sent to outside. This method provides a new robust privacy protection.

1. はじめに

近年注目を集めているユビキタスコンピューティング技術は、いつでもどこでもコンピュータを使う事を可能にするばかりでなく、遍在するコンピュータ同士が自律的に動作し、ユーザのコンテクストを取得・学習する事により、ユーザがコンピュータの存在を意識する事なく、必要な時に必要なサービスを得る事を可能にする[1]。しかしながら、このユーザのコンテクストには、プライバシに関わるパーソナルデータが含まれる。

[†] 総合研究大学院大学 数物科学研究科
The Graduate University for Advanced Studies
[‡] 国立情報学研究所
National Institute of Informatics

紙や音声ベースのデータのやりとりと異なり、コンピュータ同士がデータをやりとりするネットワークにおいては、データは電子化され、容易にコピー, 送受信される事から、このパーソナルデータの管理が重要な課題である事は言うまでもない。

これまでインターネットやセルラネットワークにおいて、ユーザのパーソナルデータ管理はそのネットワークを提供するサービスプロバイダや企業内 LAN と言った、閉じられた環境をターゲットに研究され、提供されてきた。しかしながらユビキタスコンピューティングにおいて、パーソナルデータはいたる所に遍在するセンサ, セルラネットワーク, 無線 LAN などといった、プロバイダもセキュリティ技術も異なるネットワークを通じて収集, 活用される可能性がある。また

ユーザの移動に伴い接続先ネットワークが自動的に変化するケースも考えられる。つまりユビキタス環境においては、動的に変化するどのような接続網に対しても満足できるようなパーソナルデータの管理方法が必要となる。

本論文では、このようなパーソナルデータの管理を実現するための方法として、EMAPP（Encapsulated data and Mobile Agent based Privacy Protection）を提案する。

EMAPP には 2 つの特徴がある。1 つはパーソナルデータを自分の管理下の閉じられた空間（Encapsulated Space）に置き、このデータに対するユーザのプライバシプレファレンスと一緒に管理する。この事によりパーソナルデータを外から隠す事ができる。

2 つ目はパーソナルデータを利用したサービスを受ける際、パーソナルデータをサービスプロバイダに提供するのではなく、サービスプロバイダからサービスを受けるためのプログラム（Mobile Agent）を Encapsulated Space 内に送り込ませ、必要とされている結果のみを外に出す。この事によりパーソナルデータそのものを外に出す事を防ぐ事ができる。Mobile Agent を送り込ませる際には Encapsulated Space 側で認証を行い、更にサービスプロバイダのプライバシポリシと、ユーザのプライバシプリファレンスを照らし合わせる事により、その Mobile Agent を受け入れ可能かどうか判断する。

尚 EMAPP で扱う「パーソナルデータ」とは、そのデータにより個人を特定できるかできないかに関わらず、個人に関わる全てのデータの事を意味する。

2. プライバシ管理に関する研究

ここでは EMAPP の考えの元ともなっている、これまでのプライバシ管理に関する研究を紹介する。

2.1 情報の流れの不均衡の最少化（Principle of Minimum Asymmetry）

カリフォルニア大学バークレー校の X. Jiang 氏等は彼らの論文[4]の中で、ユビキタス環境におけるプライバシデータのライフサイクルには、収集（collection），アクセス（access），2 次使用（second use）の 3 段階があると考え、ユーザがサービスプロバイダ側にパーソナルデータを提供する一方向の流れのみではなく、収集されたデータに対するアクセス，2 次使用権限の設定をユーザが行えるようにする事、またデータが誰によってどのように使用されたかをユーザが知り得る事によって逆方向の情報の流れを作り、情報の流れの不均衡を最小限に抑える方法を提案している。

例として次のようなシナリオを挙げている。

アリスは外国の町を旅行した際、ボブ社の旅行ガイド電子システムを借りる。アリスの位置情報はボブ社の中央サーバに記憶され（収集）、アリスが旅行ガイドシステムのサービスを受けるために使用される（アクセス）。次にアリスと別行動をしている友人キャロルが、アリスが自分の近くに居るかどうかという情報を知るために、ボブ社の中央サーバにアクセスし、認証されると、アリスの位置データは中央サーバからキャロルに送られる（２次使用）。

このような一方向の情報の流れを防ぐために、アリスがキャロルに自分のデータへアクセスする事を許すかどうか設定しておいたり、「アリスのデータが中央サーバから流出した場合アリスに知らせる」ポリシを設定しておいたりする事が考えられている。

同時に彼らは、収集，アクセス，２次使用の各段階におけるデータ保護に対し、防止（prevention），回避（avoidance），検出（detection）の３つの対応が必要であると述べている。

図 2.1 は各段階でパーソナルデータを保護するための既存技術を示している。

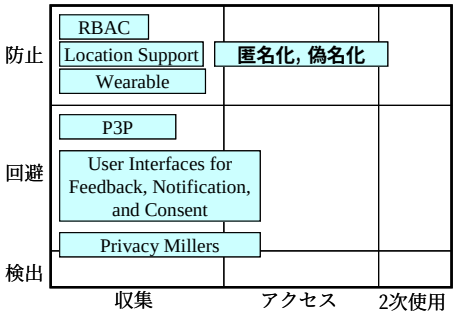

図 2.1: パーソナルデータのライフサイクルと保護技術

2.2 P3P と pawS

P3P（The Platform for Privacy Preferences Project）[2]は W3C 勧告であり、Web サイトを利用する際のプライバシポリシを XML に基づいて自動的に確認できるようにする仕組みである。

Web サイト提供側は、そのサイトのプライバシポリシとして、プライバシデータの収集者（Web サイトの提供者）は誰か，どのようなプライバシデータをどのような目的で収集するか，収集されたデータの保持期間はどの位か，第３者機関がこのポリシを保証しているかなどを XML 形式で記述する。一方ユーザ側は P3P 対応の Web ブラウザで自分のプライバシプリファレンスを設定しておけば、Web サイトを訪問した際に、そのサイトのプライバシポリシに自動的に照会され、自分のプライバシプリファレンスを満足する場合にのみそのサイトにアクセスする事を許す。また満足しない場合はユーザの画面上に警告メッセージを表示し、処理を続行するかどうかを確認する事により、例外処理に対応できるようにしている。

しかしこの P3P は、ユーザが自分のプライバシプリファレンスを設定した特定のブラウザから Web サイトにアクセスする時にのみ有用な技術で、ユビキタス環境には適応できない。

そこでこの手法をユビキタス環境に適応させたのが pawS[3]である。

pawS ではプライバシデータを収集している環境にユーザが入ると、プライバシビーコンが各サービスのプライバシポリシが置いてあるサービスプロキシの URI を知らせる。ユーザ（ユーザのプライバシアシスタント）はその URI を、ユーザのプリファレンスが置いてあるパーソナルプロキシに送り、パーソナルプロキシ経由でプリファレンスとポリシの比較を行う。結果が満足であれば P3P の場合と同様に、サービスを開始させる。

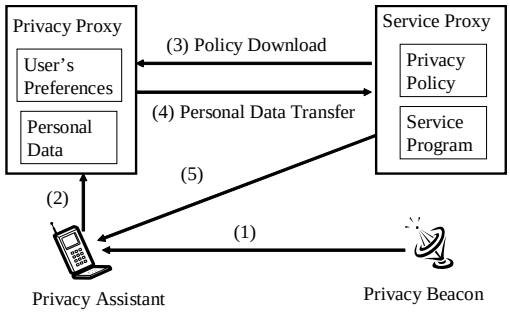

図 2.2: pawS の手順

しかしながら、この P3P や pawS は 2.1 の場合と同様、パーソナルデータをサービスプロバイダに収集させるという手法なので、この収集されたデータに対する保護対策は、データのオーナであるユーザ本人は行う事ができず、収集した側であるサービスプロバイダの管理に任せる事になる。たとえ収集する側のプライバシポリシにユーザのデータが流出した場合のペナルティが記述されていたとしても、一旦流出してしまったパーソナルデータを回収する事は極めて困難であり、ユーザが受けるであろう被害や精神的苦痛は計り知れない。

これに対して、我々の提案する EMAPP は、ユーザのパーソナルデータをサービスプロバイダに収集させる事なくサービスを受けるための手法を提供する。

3. EMAPP を用いたプライバシ保護

2 章で紹介した技術は、データをどのように収集するか，又は収集されたデータをどのように保護・管理するかが論点であった。しかしながら冒頭でも述べた通り、電子化されたデータはコピーや送受信が容易であり、またユーザの移動に伴う接続先ネットワークの変化によりユーザのパーソナルデータが安全に収集・保護されるという保証は得がたくなる。

我々が提案する EMAPP はこのような問題点を解決し、より強固なプライバシ保護を可能にする。

3.1 EMAPP の構成要素と処理手順

EMAPP はプライバシポリシとプライバシプリファレンスを比較するという点では P3P や pawS と同様であるが、次のような 2 つの特徴を持っている。

1 つ目の特徴は、ユーザのパーソナルデータとユーザのプライバシプリファレンスが Encapsulated Space と呼ばれるユーザ管理下の閉じられた空間に一体となって存在し、外からは見えないと言う点である。この Encapsulated Space はユーザの携帯端末やホームサーバのようなものであり、ユーザは自分の日々のスケジュールや位置データ，嗜好などといったパーソナルデータを、この Encapsulated Space 内で管理する。またこのパーソナルデータの扱い，誰にどのような形でパーソナルインフォメーションを提供する事ができるか、などが記述されたユーザのプライバシプリファレンスも Encapsulated Space 内に存在する。

ここで、“パーソナルデータ”と“パーソナルインフォメーション”という用語の違いであるが、パーソナルデータは生のデータそのものを指し、パーソナルインフォメーションとは何かしらの目的のためにパーソナルデータを加工したものを指すとする。例えば位置情報であれば、パーソナルデータとは今居る地点の緯度，経度の事であり、パーソナルインフォメーションとは緯度，経度のデータを元にした地図上の位置（地図の縮尺は任意）や、地名（ビル名まで特定する場合もあれば、○○県○○市程度までの場合もある）などの事を指す。この例から分かるようにデータをインフォメーションとして加工する事により、情報の精度を調整する事ができる。

2 つ目の特徴は、パーソナルデータそのものをサービスプロバイダ等に収集させ、インフォメーションして加工させるのではなく、サービスプロバイダ側から Mobile Agent を Encapsulated Space 内に送り込んでもらい、その Agent が必要な範囲でデータをインフォメーションへ加工した結果のみを外に出すという点である。これにより生のデータが外部に流れ、不正に処理される事を防ぐ事ができる。

Mobile Agent を送り込ませる際には Encapsulated Space の入り口で充分な認証や権限のチェックを行い、更にプロバイダ側のプライバシポリシと Encapsulated Space 内のプライバシプリファレンスを比較する事により、Mobile Agent 受け入れ可能かどうかを判断する。

送り込まれた Mobile Agent は必要な処理が終了した後は削除され、Encapsulated Space 内に存在し続ける事はない。これによってパーソナルデータにアクセスすることができる Encapsulated Space に Mobile Agent がいても、そのデータを持ち帰ることができず、２次使用されることはない。

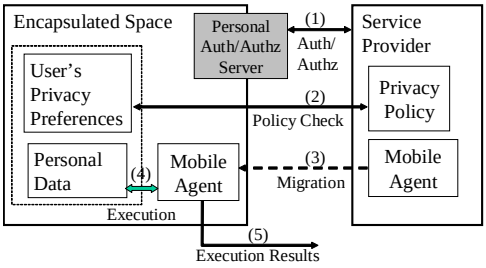

図 3.1: EMAPP の手順

次に具体例を挙げて、EMAPP の手順と有用性を説明する。

尚、サービスプロバイダのシステムを、Encapsulated Space に直接触れさせないようにするため、また Encapsulated Space の場所を隠すために、これらの処理をユーザのパーソナルアシスタントのようなものを介して間接的に行わせる方法なども考えられる。しかしサービスプロバイダ側のシステムからは、直接 Encapsulated Space とやり取りしているように見えるため、パーソナルアシスタントのような中間ノードに関しては記述せず、直接のやりとりとして説明する。

3.2 EMAPP の応用例

ここでは単一の Mobile Agent が Encapsulated Space に送り込まれ処理を行う場合と、複数の Mobile Agent が複数の Encapsulated Space に送り込まれ、それぞ

れが連動して処理を行う場合の 2 つの例を説明する。

3.2.1 単一の Mobile Agent が処理を行う場合

2.1 節の旅行ガイド電子システムの例に EMAPP を適応させたケースを考えてみる。2.1 節ではボブ社の中央サーバに収集・記憶されたアリスの位置データを使って旅行ガイド等を行うという手順であったが、EMAPP ではボブ社のシステムがアリスの Encapsulated Space に Mobile Agent を送り込む事によりサービスを行う。

手順は次の通りとなる。

1. ボブ社のシステムはアリスの Encapsulated Space の入り口にある Personal 認証サーバで認証と権限のチェックを受ける。
2. 認証が OK であれば、アリスの Encapsulated Space は、会社側が送り込もうとしている Mobile Agent のポリシと自分のプリファレンスを付き合わせる
3. 条件を満足する事が確認されたら、アリスの Encapsulated Space は Mobile Agent 受け入れ可能である事をボブ社のシステムに返す。
4. ボブ社のシステムは Mobile Agent をアリスの Encapsulated Space に送り込む
5. 送り込まれた Mobile Agent はアリスの現在位置データや嗜好データ、スケジュールデータなどを元に、周辺の店の情報などアリスにとって役立つと思われる情報を旅行ガイドシステムの画面に表示する。
6. 処理が終わったら（生存時間が過ぎたら）Mobile Agent は自動削除される。

この手順を図 3.2 に示す。

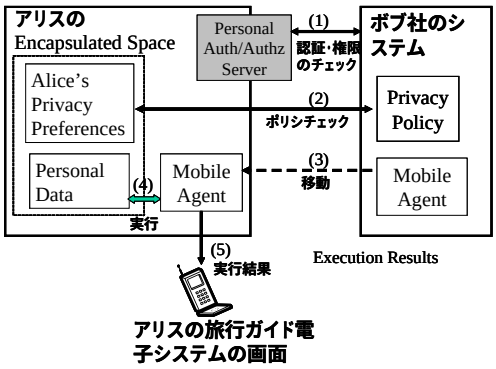

図 3.2: アリスが旅行ガイドサービスを受ける場合の手順

3.2.2 複数の Mobile Agent が連動して処理を行う場合

「家の中に誰も居なくなった事が確認されると、留守番電話が自動的にセットされる。」というシナリオを例に考える。

ここではいかにして家族全員の位置情データを外部に出す事なく、家の中に誰も居なくなったかを知るかという事が論点となる。

例としてアリスとボブの２人暮らしの家庭の場合を考え、以下にその手順を述べる。

0. アリスかボブ、どちらかが外出したのをトリガにして（ここではボブとする）、ボブの Encapsulated Space 側からサービスプロキシにサービスをスタートさせる要求を出しに行く。
1. サービスプロキシは、アリスとボブそれぞれ Encapsulated Space に対し、認証及びポリシチェックの処理を行う。
2. それぞれの Encapsulated Space で条件を満足する事が確認されたら、Mobile Agent 受け入れ可能である事をそれぞれサービスプロキシに返す。ここでアリス, ボブのどちらか一方でも受け入れ可能とならなかった場合は、処理はここで終了する。
3. サービスプロキシはそれぞれ連動して働く Mobile Agent をアリスとボブの Encapsulated Space に送る。
4. アリスに送られた Mobile Agent は、自分が不在であるかどうかの情報をボブの Mobile Agent に対して送る。
5. ボブの Mobile Agent は、アリスが不在

の場合、留守番電話をセットしに行く。

6. 処理終了後、Mobile Agent は自動削除される。

この手順を図 3.3 に示す

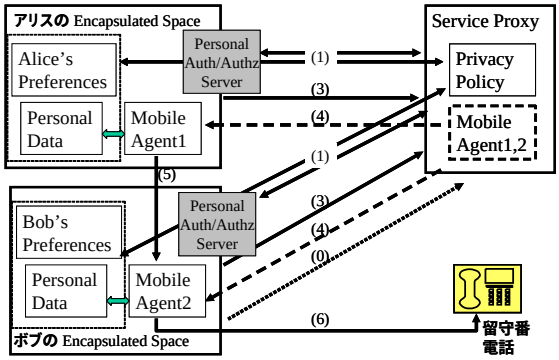

図 3.3: 留守番電話自動セットの手順

このように Mobile Agent 同士が必要な情報を交換し、自動的に留守番電話をセットしに行くので、アリスとボブは自分の位置情報や家に居るか否かという情報すら相手に知られる事なく留守番電話自動セットサービスを受ける事ができる。

ここで、ボブがサービスプロキシにサービスを要求しに行った時に、要求している相手がボブである事をサービスプロキシが確認する事や、アリスが「相手があればこのサービスを提供してもよいが、他の人には提供しない」というプリファレンスを持っておく事、Mobile Agent 同士はセキュアに通信し合う事など、多くの要求条件が考えられるが、どのように実現するかにに関しては現在検討中である。

3.2.3 EMAPP の利点

EMAPP ではプロバイダがパーソナルデータの収集を行うという事をしないため、ユーザは自分の Encapsulated Space 内のパーソナルデータを管理する事だけを考えれば良い。

図 2.1 の従来技術と比較した時、EMAPP はパーソナルデータを一切外に出さないため、この 2 次使用を防止している事になる。また、Mobile Agent が Encapsulated Space の内部でパーソナルデータを収集した結果、データがインフォメーションとして加工されて外に出ていると考えた場合でも、Mobile Agent 受け入れの際に認証・権限のチェックやポリシとの比較を行っているので、収集に対しても防止・回避を行っているといえる。

EMAPP はユビキタス環境に適した強固なプライバシ保護を可能にする。

4. 今後の検討課題

EMAPP をより確実な技術にするために、次のような検討すべき点や改善すべき点がある。

- J. J. Borking 氏等が論文[6]の中で述べているように、Mobile Agent のような知的ソフトウエアエージェント技術が逆にプライバシに対しての脅威になる事も起こりうる。これに対し Mobile Agent が Encapsulated Space 内のデータを処理する段階、更に処理結果を送信する段階両方で対策をとらなければならない。同論文中に述べられているように、Mobile Agent が信頼できるものであるかの確認、電子署名や証明書などの採用、Mobile Agent の作業ログのチェック、送受信の際の暗号化などを徹底すると共に不足している部分を補っていかなければならない。また Encapsulation Space そのものに対する攻撃には Frank Stajano 氏等の再生子ガモのセキュリティモデル[5]などを参考にしていきたい。

- ユビキタス環境ではサービスのリアルタイム性が要求される。接続しているネットワークの通信能力や Mobile Agent が実行されるハードウエアの処理能力などを考慮し、リアルタイム性に応えられるようなシステムを作成しなければならない。

- EMAPP では P3P や pawS のようにプライバシポリシとプライバシプリファレンスの比較を行っている。しかし P3P や pawS がデータの収集に対するポリシとプレファレンスであるのに対し、EMAPP は Mobile Agent 受け入れに対するものである。ポリシ側には誰からのどのような要求で、どのような目的のた

めに、どのデータをどのように加工するか、などの細かい記述が必要であり、プリファレンスにはこれらをフィルタリングするような記述が必要である。このようなポリシやプリファレンスをうまく生成する方法を検討する必要がある。

- プリファレンスの設定や、条件を満足しない Mobile Agent に対する処理、また各 Mobile Agent に対する権限の設定などは、ユーザの手動による方法が考えられているが、これはユビキタスの不可視性の概念に反する。できるだけユーザの手動設定に頼らない方法を検討しなければならない。

- EMAPP ではユーザのパーソナルデータを Encapsulated Spacen 内に隠したままサービスを受ける方法を提案し、3 章に例も示した。しかし本当に全てのサービスをこの方法で受ける事ができるのかを検討すると共に、それらに対する解決策を考えていかなければならない。

5. まとめ

この論文では EMAPP という新しいプライバシ保護方式を提案した。この方式は自分のパーソナルデータを Encapsulated Space と呼ばれる自分の管理下の閉じられた空間に置き、外部から隠す事、サービスプロバイダに Mobile Agent を送り込ませ、処理結果のみを外に出す事により、
パーソナルデータを不必要に収集させる事なく、サービスを受ける事を可能にする。

従来ではサービスプロバイダがユーザのパーソナルデータを収集する事によりサービスを行っていたので、これに続いて発生するアクセスや２次使用に対するプライバシ保護方法がサービスプロバイダ毎に必要であった。本方式ではこのような煩雑な手順を解決し、より確実なプライバシ保護をユビキタス環境上に実現する事を可能にしている。

参考文献

[1] Mark Weiser, “Some Computer Science Problems in Ubiquitous Computing,” Communications of the ACM,, Vol. 36, No. 7, pp.74-83, July 1993.

[2] http://www.w3.org/P3P/.

[3] M. Langheinrich: A Privacy Awareness System for Ubiquitous Computing Environments International Conference on Ubiquitous Computing 2002 (UbiComp 2002), pp. 237-245, LNCS2498 (September 2002).

[4] X. Jiang, J. I. Hong, and J. A. Landy: Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing, Proceedings of International Conference on Ubiquitous Computing 2002 (UbiComp 2002), pp. 176-193, LNCS2201 (September 2002).

[5] Frank Stajano, Security for Ubiquitous Computing, WILEY, ISBN 0470-84493-0, 2002.

[6] J.J. Borking, B.M.A. van Eck, P. Siepel: Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector, Information and Privacy Commissioner Ontario (Canada) and Registratiekamer (The Netherlands), April 1999.