(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4761702号
(P4761702)
(45)発行日　平成23年8月31日(2011.8.31)　(24)登録日　平成23年6月17日(2011.6.17)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330A
G06F 15/00 (2006.01)　　G06F 15/00 310T

請求項の数 2　(全 18 頁)

(21)出願番号　特願2003-352124(P2003-352124)
(22)出願日　平成15年10月10日(2003.10.10)
(65)公開番号　特開2005-115829(P2005-115829A)
(43)公開日　平成17年4月28日(2005.4.28)
審査請求日　平成18年9月25日(2006.9.25)

特許法第３０条第１項適用　社団法人情報処理学会、情報処理学会研究報告２００３－ＯＳ－９３（２００３年５月８日）発行　第４９～５６頁に発表

前置審査

(73)特許権者　598121341
学校法人慶應義塾
東京都港区三田二丁目１５番４５号
(73)特許権者　000152228
株式会社内田洋行
東京都中央区新川２丁目４番７号
(74)代理人　100107113
弁理士　大木　健一
(72)発明者　田丸　修平
神奈川県藤沢市遠藤５３２２　慶應義塾大学　湘南藤沢キャンパス内
(72)発明者　岩谷　晶子
神奈川県藤沢市遠藤５３２２　慶應義塾大学　湘南藤沢キャンパス内

最終頁に続く

(54)【発明の名称】プライバシを考慮したパーソナライゼーションのためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
ユビキタスコンピューティング環境においてアプリケーションを実行するときにプライバシを考慮したパーソナライゼーションを実現する、ユーザの携帯端末からユーザ個人の情報を送信することのない個人情報非送信型の方法であって、
ユーザが自己の携帯端末に、個人に関する情報であってその情報から当該個人を特定できるデータである個人情報及び前記個人情報を外部に提供する際のルールであってユーザの判断基準に基づくユーザルールを設定するステップと、
アプリケーションが稼働するホストから、少なくとも１つの解を生み出す式あるいは式の集合であり、必要な個人情報の種類、コマンド生成のための式、及び、生成されるコマンドの型を要素とするテンプレートを含むアプリケーションルールをユーザの前記携帯端末にダウンロードするステップと、
ユーザが前記携帯端末に、場所や状況に応じて適宜変化する個人情報である動的個人情報を入力するステップと、
前記携帯端末で前記ユーザルールに従って、提供する前記個人情報の粒度を変更するステップと、
前記携帯端末で前記アプリケーションルール、前記動的個人情報及び前記変更された粒度の個人情報に基づいて前記ホストでの処理を制御するための制御コマンドを生成するステップと、
前記携帯端末から前記ホストへ、前記個人情報を送信する代わりに、前記変更された粒

度及び前記アプリケーションルールに基づき変換された前記個人情報を含む前記制御コマンドを送信するステップと、
前記ホストで、予め保持するデータベース及び前記制御コマンドに含まれる前記動的個人情報並びに前記変更された粒度の個人情報に基づき、予め定められたアプリケーションを実行するステップと、を備え、
前記携帯端末は個人情報保持ホストであり、さらに前記ユーザールールを保持するものであり、
前記携帯端末から前記ホストへの送信において前記個人情報は制御コマンドの形に変換されていることを特徴とする方法。
【請求項２】
ユビキタスコンピューティング環境においてアプリケーションを実行するときにプライバシを考慮したパーソナライゼーションを実現する、ユーザの携帯端末からユーザ個人の情報を送信することのない個人情報非送信型のシステムであって、
ユーザの持つ携帯端末と、ユーザの移動先の空間に存在するアプリケーション稼動ホストとを備え、
前記携帯端末は、
個人に関する情報であってその情報から当該個人を特定できるデータである個人情報及び前記個人情報を外部に提供する際のルールであってユーザの判断基準に基づくユーザルールを設定するステップと、
アプリケーションが稼働する前記ホストから、少なくとも１つの解を生み出す式あるいは式の集合であり、必要な個人情報の種類、コマンド生成のための式、及び、生成されるコマンドの型を要素とするテンプレートを含むアプリケーションルールをダウンロードするステップと、
ユーザから、場所や状況に応じて適宜変化する個人情報である動的個人情報の入力を受けるステップと、
前記ユーザルールに従って、提供する前記個人情報の粒度を変更するステップと、
前記アプリケーションルール、前記動的個人情報及び前記変更された粒度の個人情報に基づいて前記ホストでの処理を制御するための制御コマンドを生成するステップと、
前記ホストへ、前記個人情報を送信する代わりに、前記変更された粒度及び前記アプリケーションルールに基づき変換された前記個人情報を含む前記制御コマンドを送信するステップとを実行し、
前記ホストは、
予め保持するデータベース及び前記制御コマンドに含まれる前記動的個人情報並びに前記変更された粒度の個人情報に基づき、予め定められたアプリケーションを実行するステップと、を実行し、
前記携帯端末は個人情報保持ホストであり、さらに前記ユーザールールを保持するものであり、
前記携帯端末から前記ホストへの送信において前記個人情報は制御コマンドの形に変換されていることを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明はユビキタスコンピュータ環境を実現する技術に関するものであり、特に、プライバシを考慮したパーソナライゼーションのためのシステム及び方法に関する。
【背景技術】
【０００２】
１．　ユビキタスコンピューティング環境の実現を前提としたアプリケーションが日々研究開発されている。情報機器や多様なセンサの遍在によって、ユーザにとってより快適なアプリケーションの実現が可能となる。アプリケーションがユーザの嗜好に適応するための仕組みとして、ユーザが設定した静的な値に基づいて動作する方法がある。例えば、ユ

ーザインタフエースの設定や、ホットキーの割り当てなどがある。将来的には携帯デバイスの小型化、高性能化によって多様な情報の保持が可能となり、現実世界におけるユーザの個人情報をアプリケーションが利用することが可能となる。以下の説明では、性別や年齢などの不変的な情報から、好み、アプリケーションの設定まで、ユーザの個人情報を広義に用いる。個人情報の導入によって、ユーザの性別や職業に応じてアプリケーションの挙動を変えることが可能となる。つまり、公共空間におけるアプリケーションのパーソナライゼーションの実現が可能となる。

【非特許文献１】本田良司、鈴木和弘、鳥原信一、久世和資：“アドホック・ネットワークとアクティブ電子広告版”、情報処理学会コンピュータシステム・シンポジウムNO. 13、pp. 47－52、東京（2000）、http：//www.torihara.com／wit／ap／

【非特許文献２】A. Knott and C. Mellish and J. Oberlander, and M. O'Donnell、 "Sources of Flexibility in Dynamic Hypertext Generation"、 In Proceedings of the 8th International Workshop on Natural Language Generation、 Herstmonceux Castle、 UK、 june 1996.

【非特許文献３】Davies、N. 、K. Mitchell、K. Cheverst 、and G. S. Blair、"Developing a Context Sensitive Tourist Guide"、 Technical Report Computing Department、Lancaster University. March 1998.

【非特許文献４】World Wide Web Consortium、 http://www. w3. org/

【非特許文献５】Platform for Privacy Preferences Project、http：//www. w3. org/P3p/

【非特許文献６】Anonymiser、 http : //www. anonymizer. com/

【非特許文献７】OpenSSL、http://www. openss1. org/

【０００３】

２．公共空間におけるアプリケーションのパーソナライゼーション

まず、公共空間におけるアプリケーションのパーソナライゼーションについて説明し、実現する際の問題点を指摘する。

【０００４】

２．１　個人情報への適応

ユーザは移動先に存在する様々なアプリケーションを利用する。アプリケーションはユーザの携帯端末に保持されている個人情報に適応した動作を行う。これらを実現したものとして、街頭に存在しユーザの障害に応じてインタフエースを切り替えて道案内を行う、障害者のためのナビゲーションシステムであるアクティブポスター[非特許文献１］や、美術館においてユーザの美術品に対する知識により解説内容を変更するILEX－0[非特許文献２］、観光地において旅行者に対して案内を行うPDA上で動作するブラウザであるGUIDE[非特許文献３］などがある。以上のように、多様なユーザの個人情報に適応した動作を行うことで、ユーザの入力負担の軽減と、公共空間におけるアプリケーションのパーソナライゼーションを実現することができる。

【０００５】

２．２　個人情報を用いるアプリケーションの形態

個人情報とアプリケーションは、それぞれが一対になっており、個人情報が保持されている携帯端末は、1つ以上のアプリケーションのための個人情報を保持していることを想定する。例としてデパートがユーザのより好む商品を勧めるアプリケーションを挙げると、個人情報はデパート毎に存在し、個人情報はアプリケーション単位で、各々が異なる携帯端末に保持されている可能性が有る、ということである。

【０００６】

２．３　プライバシ

上記の通り個人情報の導入によって、より利便性の高いアプリケーションを実現できる一方で、プライバシの問題が発生する。ここで述べるプライバシの問題とは、ユーザの知られたくない個人情報が意図しない他者に知られてしまうことである。例えば、ユーザの住所や電話番号などが、意図しない第三者に知られてしまうことである。公共空間におけ

るアプリケーションでは問題がより深刻になる。

【０００７】

公共空間におけるアプリケーションの中には悪意のあるものが存在する可能性がある。つまり、ユーザが意図しない第三者に、取得した個人情報を公開したり、ユーザが意図しない個人情報まで取得してしまうアプリケーションの存在である。公共空間においてはこれらのアプリケーションが遍在する。そこで、アプリケーションを信用しない、という前提で対処する必要がある。

【０００８】

また、高機能化、多機能化した携帯端末を悪意のある第三者が手にすることによって、個人情報が保持されている携帯端末とアプリケーションとの通信を傍受される危険性がより高くなる。通常、通信傍受への対応には暗号化を用いるが、前項の悪意のあるアプリケーションに対する有用性がない。

【発明の開示】

【発明が解決しようとする課題】

【０００９】

２．４　現行のプライバシ保護手法

現在広く普及しているプライバシ保護手法は通信相手、または第三者に対する依存性がある。以下、この点について例を挙げて簡単に説明する。

【００１０】

P3P

W3C[非特許文献４］が提供するP3P[非特許文献５］はWebサイト閲覧において、ユーザから取得した個人情報の利用方法及び利用範囲をユーザに開示するためのフレームワークである。ユーザへの開示が個人情報を取得した以後に行われる場合が多い。また、ユーザが長い文章を読む必要がある。さらに、P3PはWebサイトによる個人情報の利用方法及び利用範囲の保障はできない。

【００１１】

プロクシサーバ

Anonymizer[非特許文献６］などのプロクシサーバは、ユーザがプロクシサーバを経由してWeb閲覧を行うことで、ユーザが使用しているホストのIPアドレスやポート番号などをWebサイトに対して隠蔽する。これによって、プライバシの保護を達成することができるが、プロクシサーバの信頼性という問題がある。

【００１２】

暗号化

SSL[非特許文献７］などの暗号化は第3者への対応策として有効である一方で、通信相手を信用する、という前提で成り立っている。前節で述べたように悪意のあるアプリケーションの遍在する環境においては有用性がないため、暗号化に代わる手法を用いる必要がある。

【００１３】

そこで、前述の公共空間における個人情報を利用したアプリケーションを実現するための、プライバシを考慮したアプリケーションフレームワークを提案する。

【課題を解決するための手段】

【００１４】

この発明は、ユビキタスコンピューティング環境においてアプリケーションを実行するときにプライバシを考慮したパーソナライゼーションを実現するための方法であって、

個人情報を基に少なくとも１つの解を生み出す式あるいは式の集合であるアプリケーションルールをユーザの携帯端末にダウンロードするステップと（ダウンロードするものはテキストあるいはプログラムいずれでもよい）、

前記携帯端末で個人情報と前記アプリケーションルールに基づいて制御コマンドを生成するステップと、

前記携帯端末からアプリケーションが稼働するホストへ前記制御コマンドを送信するス

テップと、
前記ホストで前記制御コマンドに基づいた動作を行うステップと、を備えるものである。
さらに、ユーザが定義する個人情報開示条件であるユーザルールを基に前記アプリケーションルールに提供する個人情報粒度を変更するステップとを備えるようにしてもよい。
【００１５】
さらに、動的個人情報を入力するステップを備え、
前記制御コマンドを生成するステップにおいて、前記動的個人情報を含む個人情報と前記アプリケーションルールに基づいて制御コマンドが生成され、
前記ホストで前記制御コマンドに基づいた動作を行うステップにおいて、受信した制御コマンドから動的個人情報を生成し、当該動的個人情報に対応する動作を行うようにしてもよい。
【００１６】
この発明は、ユビキタスコンピューティング環境においてアプリケーションを実行するときにプライバシを考慮したパーソナライゼーションを実現するためのシステムであって、個人情報保持ホストとしてユーザの持つ携帯端末と、ユーザの移動先の空間に存在するアプリケーション稼動ホストとを備え、
前記アプリケーション稼動ホストは、個人情報を基に少なくとも１つの解を生み出す式あるいは式の集合であるアプリケーションルールを記憶するアプリケーションルール記憶部と、前記アプリケーションルールを送信するとともに前記携帯端末に制御コマンドを要求するコマンド要求部とを含み、
前記携帯端末は、前記アプリケーションルールに必要な個人情報を取得する個人情報管理部と、前記個人情報管理部から個人情報を受けて、前記アプリケーションルールと前記個人情報を基に制御コマンドを生成するコマンド生成部とを含む、ことを特徴とするシステムである。
【００１７】
例えば、前記アプリケーション稼働ホストのコマンド要求部が前記携帯端末へ前記アプリケーションルールを送信し、前記携帯端末のコマンド生成部が前記アプリケーションルールに従って、前記個人情報管理部に個人情報を要求し、前記個人情報管理部が必要な個人情報を取得し、前記個人情報管理部が個人情報を前記コマンド生成部に返し、前記コマンド生成部が制御コマンドを生成し、前記アプリケーション稼働ホストに制御コマンドを返し、前記アプリケーション稼働ホストが制御コマンドに基づいた動作を行う。
前記携帯端末は、さらに、ユーザルールを保持し、前記コマンド生成部にユーザルールを提供するユーザルール管理部を含んでもよい。前記ユーザルール管理部は、ユーザルールに従って個人情報の粒度を変更し、前記アプリケーションルールに提供する。
【００１８】
前記携帯端末は、動的個人情報を入力するためのモード入力部を備え、
前記携帯端末のコマンド生成部は、前記動的個人情報を含む個人情報とアプリケーションルールに基づいて制御コマンドを生成し、
前記アプリケーション稼働ホストは、受信した制御コマンドから動的個人情報を生成する動的個人情報生成部を備えるようにしてもよい。
【００１９】
プライバシを考慮した、アプリケーションが個人情報に適応的に動作するためのフレームワークを提案する。ユビキタスコンピューティング環境においては、機器の高性能化、多機能化によって、公共空間におけるアプリケーションの遍在や、携帯端末の高性能化による多様な情報の保持が可能となる。このことは公共空間におけるパーソナライゼーションを可能とする。携帯端末の高性能化によって、携帯端末に保持される情報が現実世界に即した個人情報を扱えるようになるため、プライバシを考慮したフレームワークが必要となる。本発明に係る個人情報非送信型モデルでは、個人情報の取得と、アプリケーションの動作を決定するコマンドの生成を分離することでプライバシの保護を達成する。これに

よって、プライバシの保護と個人情報への適応を両立させたアプリケーションの作成が可能となる。

【発明を実施するための最良の形態】

【００２０】

発明の実施の形態１．

説明の流れについて述べる。第３項でプライバシの保護と個人情報への適応を両立させるための手法として、個人情報非送信型モデルを提案する。第４項で設計を行い、第５項で個人情報非送信型モデルを実現するためのプロトタイプ実装であるEA－P2フレームワークについて述べる。

【００２１】

本発明の実施の形態は、前述の公共空間における個人情報を利用したアプリケーションを実現するための、プライバシを考慮したアプリケーションフレームワークに関するものである。まず、対象アプリケーションの基本動作について考察し、個人情報非送信型モデルを提案する。次にその特徴について述べ、最後に実現するための機能要件を挙げる。

【００２２】

３．１　概要

本節では、対象アプリケーションの動作を考察し、個人情報非送信型モデルを提案する。

【００２３】

（１）個人情報送信型モデル

対象アプリケーションである公共空間における個人情報に適応的なアプリケーションの基本動作について述べる。従来のモデルを、個人情報送信型モデルと呼び、アプリケーションは図１のように動作することを想定する。

１．ユーザの個人情報を取得

２．個人情報とアプリケーションルールに基づいて制御コマンドを生成

３．制御コマンドに基づいた動作

【００２４】

図１には個人情報保持ホストとアプリケーション稼働ホストが示され、個人情報保持ホストからユーザーの情報（User Info）がアプリケーション稼働ホストへ送られ（１）、アプリケーション稼働ホストで予め定められたアプリケーションルールに基づきコマンドが生成され（２）、アプリケーション稼働ホストにより所定のサービスがユーザーに提供される（３）、ことが示されている。

【００２５】

アプリケーションルールとは、個人情報を基に、１つの解を生み出す式、あるいは式の集合である。本フレームワークでは、個人情報の取得と、制御コマンドの生成を分離して捉える。

【００２６】

（２）個人情報非送信型モデル

公共空間におけるパーソナライゼーションを実現するための手法として、個人情報非送信型モデルを提案する。基本動作を図２に示す。

１．ユーザの携帯端末にアプリケーションルールをダウンロード

２．個人情報とアプリケーションルールに基づいて制御コマンドを生成

３．制御コマンドの送信

４．制御コマンドに基づいた動作

【００２７】

図２には個人情報保持ホストとアプリケーション稼働ホストが示され、アプリケーション稼働ホストから予め用意されたアプリケーションルールが送られ（１）、これと個人情報保持ホストで予め保持していた個人情報に基づきコマンドが生成され（２）、当該コマンドがアプリケーション稼働ホストに送られ（３）、当該コマンドを受けてアプリケーション稼働ホストにより所定のサービスがユーザーに提供される（４）、ことが示されてい

る。図２の手順によれば、個人情報をアプリケーション稼働ホストに送る代わりに、アプリケーション稼働ホストからアプリケーションルールを受けてコマンドを生成し、このコマンドをアプリケーション稼働ホストへ送る。したがって、図２の手順でも図１の場合と同様のサービスを受けることができるが、個人情報が送信されないのでプライバシーの点で好ましい。代わりにアプリケーションルールが送信されるが、これが傍受されたところでユーザーにとって問題は生じない。したがって図２の手順は次のような特徴を備える。

【００２８】

３．２　特徴

次に、個人情報非送信型モデルの特徴を述べる。

【００２９】

３．２．１　悪意のあるアプリケーションに対する機密性

ここで提案する個人情報非送信型モデルでは、個人情報ではなく、制御コマンドをアプリケーションに送信するため、悪意のあるアプリケーションに対して有効である。

【００３０】

３．２．２　悪意のある第3者に対する機密性

公共空間において個人情報に適応的なアプリケーションを利用する際、通信を傍受される危険性がある。個人情報非送信型モデルでは個人情報自体が通信されることはないため、個人情報を保護できる。

【００３１】

３．３　機能要件

次に、ここで提案する個人情報非送信型モデルを実現するアプリケーションフレームワークに要求される機能要件について述べる。

【００３２】

（１）個人情報の機密性

前節で述べたように、ここでは悪意のあるアプリケーションの遍在を前提とするため、アプリケーションへの個人情報の漏洩を防ぐ必要がある。

【００３３】

（２）柔軟な個人情報の記述方式

ここで提案するフレームワークは様々な個人情報に適応的なアプリケーションを前提とするため、個人情報の記述が柔軟に行われる必要がある。

【００３４】

（３）利便性

ユーザの再入力や回答の負担を軽減する、という個人情報に適応的なアプリケーションの本来の目的を損なわないため、ユーザの負担を増加させずに上記の要件を達成する必要がある。

【００３５】

４　設計

本節では、本稿で提案した個人情報非送信型モデルを実現するためのアプリケーションフレームワークの設計について述べる。

【００３６】

４．１　全体構成

本フレームワークの全体構成を図３に示す。個人情報保持ホストはユーザの持つ携帯端末であり、アプリケーション稼動ホストはユーザの移動先の公共空間に存在する。

【００３７】

ユーザは個人情報保持ホストとして携帯端末を保持し、移動先の公共空間に存在するアプリケーションを利用する。コマンド要求部はアプリケーション稼動ホスト上で動作し、コマンド生成部、個人情報管理部は個人情報保持ホスト上で動作する。

【００３８】

（１）コマンド要求部

アプリケーションルールを送信し、個人情報保持ホストに制御コマンドを要求する。

（２）個人情報管理部
アプリケーションルールに必要な個人情報を取得し、コマンド生成部に提供する。
（３）コマンド生成部
アプリケーションルールと個人情報を基に、制御コマンドを生成する。
【００３９】
４．２　基本動作
基本動作を図４に示す。
１．コマンド要求部がアプリケーションルールを送信する
２．アプリケーションルールに従って、個人情報管理部に個人情報を要求する
３．個人情報管理部が必要な個人情報を取得する
４．個人情報をコマンド生成部に返す
５．制御コマンドを生成、アプリケーションに制御コマンドを返す
６．制御コマンドに基づいた動作
【００４０】
４．３　個人情報のテンプレート
自由なアプリケーション作成のためには、アプリケーション作成者が個人情報を自由に定義できる必要がある。そのために本フレームワークではテンプレートを提供する。テンプレートには情報の種別を表す要素名を自由に定義できること、様々な値を記述できることが必要である。
【００４１】
４．４　アプリケーションルール
アプリケーションルールは個人情報同様に、アプリケーション作成者による記述の余地を残す必要がある。そこで個人情報と同様にテンプレートを提供する。テンプレートには以下の要素が必要となる。
（１）必要な個人情報の種類
（２）コマンド生成のための式
（３）生成されるコマンドの型
【００４２】
４．５　コマンド要求部
コマンド要求部は、アプリケーション稼動ホストに存在しAPIの役割を果たす。アプリケーションはコマンド要求部を経由し、アプリケーションルールを送信する。また、コマンド要求部によってアプリケーションは個人情報保持ホストから制御コマンドを取得する。
【００４３】
４．６　コマンド生成部
コマンド生成部は、アプリケーションルールを取得する。次に、アプリケーションルールが必要とする個人情報管理部に個人情報を要求し、個人情報管理部から返された値とアプリケーションルールに基づいたコマンド生成を行う。
【００４４】
４．７　個人情報管理部
個人情報管理部は、個人情報の種類を識別し、アプリケーションルールが必要とする値をコマンド生成部に返す。
【００４５】
５　実装
本節ではプロトタイプ実装であるEA－P2（Enhancing Privacy and Adapting User Information for Personalized Public Space）フレームワークについて述べる。
【００４６】
５．１　個人情報
データ記述の柔軟性の観点から、個人情報の記述形式はXMLを用いた。XMLのDTD（document type definition）を図５に示す。

アプリケーション作成者は必要な個人情報を要素dataに記述する。各要素は属性nameによって識別され、その値を属性valueによって表す。個人情報は個人情報管理部によって管理される。

【００４７】

５．２　アプリケーションルール

本フレームワークではアプリケーションルールのテンプレートとしてインタフエースを提供する。このインタフエースを実装することで、アプリケーションルールを作成できる。evaluateメソッドの引数によって必要な個人情報のXMLファイルを指定する。図６にインタフエースを示す。

【００４８】

５．３　コマンド要求部

コマンド要求部のアプリケーションルール移送の動作を図７に示す。アプリケーション作成者が実装したApplicationRuleImplオブジェクトを個人情報保持ホストに移送する。

アプリケーションからの呼び出し例を図８に示す。getCommandメソッドによって、コマンド要求を行う。返り値は制御コマンドになり、制御コマンドを基にアプリケーションは個人情報に基づいた挙動を行う。

アプリケーションの記述は1行であり、アプリケーション作成者が本フレームワークを容易に利用することを可能とした。

【００４９】

５．４　コマンド生成部

アプリケーションルールの取得を図９に示す。取得したアプリケーションルールのevaluateメソッドを用いて、コマンドを生成する。これによって、アプリケーションルールの自由な作成を実現する。

【００５０】

５．５　個人情報管理部

個人情報が記載されたXMLファイルから要素を取りだす。前節で設計した通り、携帯端末上での動作を前堤としているため、APIには比較的高速処理が可能なSAX（simple API for XML）を用いた。図１０に個人情報解析の動作を示す。

【００５１】

本発明の実施の形態に係るシステム及び方法によれば次のような効果を奏する。

（１）個人情報の機密性

個人情報はコマンドに変換されることによって、第3者からの個人情報の保護は達成される。

（２）柔軟な個人情報の記述方式

アプリケーション作成者は、DTDに従う限り、自由に個人情報の項目を設定することができる。例えば、レンタルビデオ店で本フレ「ムワークを用いて、ユーザの好む俳優の映画を紹介するアプリケーションを作成する場合、ある店では“好きな俳優”という要素を持ち、別の店では、“好きな男優”、“好きな女優”と分けることも可能であり、アプリケーションによって柔軟に対応することができる。

（３）利便性

本フレームワークによってユーザの入力回答が増加することはないため、個人情報に適応したアプリケーションの本来の目的である利便性を損なっていない。よって、利便性は達成されたといえる。

【００５２】

本発明の実施の形態に係るフレームワークを用いることで、ユーザは個人情報を保護しながら、個人情報に適応的なアプリケーションを利用することができる。一方で、アプリケーション作成者は、本フレームワークを用いることで、公共空間における個人情報に適応的なアプリケーション作成を容易に行うことができる。

【００５３】

なお、以下に述べる機能を追加してもよい。

（１）ユーザによる判断基準の導入
アプリケーション作成者の自由度は達成されたが、個人情報の機密性が十分に達成されていない。そこでユーザによるアプリケーションルールへ提供する個人情報のカスタマイズを可能にする機能を設けてもよい。
（２）個人情報の処理
個人情報の記述方式、解析方式を改良して、住所などの階層構造を持つ個人情報を扱うことができるようにする。また、個人情報の追加、削除などの情報を編集する機能を持たせる。
（３）位置情報のプライバシ
本システム及び方法での対象アプリケーションが利用できる情報として、位置情報は重要である。位置情報も考慮にいれて公共空間におけるアプリケーションのパーソナライゼーションを行うようにしてもよい。また、その際に位置情報のプライバシ保護についても盛り込むことが好ましい。
【００５４】
発明の実施の形態２．
発明の実施の形態１に係るシステム及び方法に以下の点を追加してもよい。
（１）コマンドの実行はアプリケーション稼動ホストのみで行うのではなく、コマンド生成をするノードにても行うようにする。
（２）静的個人情報に加えて動的個人情報を追加してもよい。動的個人情報とは、場所や状況に応じて適宜変化する個人情報のことである。例えば来店の目的などである。
（３）トレーサビリティを持たせるために、コマンドにコマンドを生成した時刻とGPS測位データをデータとして附随させる。
（４）コンテンツ選択・デバイス選択・表示モード選択などの表示に関するコマンドを追加する。
【００５５】
以下、具体的なシステムについて図１２及び図１３を参照して説明する。
【００５６】
図１２の各部について簡単に説明する。
１１はコマンド要求部を経由し、アプリケーションルールを送信するとともに、コマンド要求部１２によって個人情報保持ホストから制御コマンドを取得するアプリケーション処理部である。
１２はアプリケーション稼動ホストに存在しAPIの役割を果たすコマンド要求部である。
１３はアプリケーションルールを予め記憶する記憶部である。
１４はユーザの個人情報を予め記憶するデータベースである。
１５は受信したコマンドに基づき動的個人情報を生成してアプリケーション処理部１１に送る動的個人情報生成部である。
２１はアプリケーションルールを取得し、次にアプリケーションルールが必要とする個人情報を個人情報管理部２２に要求し、個人情報管理部２２から返された値とアプリケーションルールに基づいたコマンド生成を行うコマンド生成部である。
２２は個人情報の種類を識別し、アプリケーションルールが必要とする値をコマンド生成部に返す個人情報管理部である。
２２は動的個人情報を入力するためのモード入力部である。
【００５７】
（Ａ）カーデーラにおける応対システム
個人情報を個人携帯端末中に保持したお客がカーデーラに訪問したときに、当該お客に特化した情報を提供するためのシステムである。
このシステムの特徴は、データベースの保存されている静的情報のほかに、お客が行動することにより発生するイベントや情報と組み合わされることにより動的情報が発生する、という点にある。

また、個人情報保持ホストは個人携帯端末となる。
カーデーラでは、アプリケーションをアプリケーション稼働ホストに持っており、また、個人情報データベース（過去の自店での購入履歴、ローンの内容など）を、アプリケーション稼働ホストに持っている。
【００５８】
Ｓ１：アプリケーション稼働ホストは、お客が来店したことつまり個人携帯端末が通信可能範囲内に存在することを検出し、アプリケーションルールをアプリケーション稼働ホストから個人携帯端末に送信する。
【００５９】
Ｓ２：お客は店舗からの求めによって、本日の来店モード（暇つぶし、大人の暇つぶし、車の詳細を知りたい、試してみたい）を個人携帯端末に入力する。
【００６０】
Ｓ３：個人携帯端末内では、事前に常時保持している個人情報と、受信したアプリケーションの求めるルールによって、制御コマンドを生成する。
制御コマンドは、個人携帯端末内に保持された静的個人情報と、入店時に入力された来店モードを合成して生成される。
たとえは、来店モード（暇つぶし）を入店時に指示した顧客は、静的個人情報と来店モードとの組み合わせにより、子供ありの暇つぶしという制御コマンドを生成する。
来店モード（車の詳細を知りたい）を入店時に指示した顧客については、静的個人情報のセダン購入実績ありという情報と車の詳細を知りたいという情報をセットにしてコマンドを生成する。
静的個人情報のアウトドア車購入実績ありという情報と、来店モード（暇つぶし）という情報をセットにして、アウトドアでの車両の利用シーンを大型ディスプレイに表示するコマンドを生成する。
【００６１】
Ｓ４：生成された制御コマンドがカーデーラのアプリケーション稼働ホストに送信される。
【００６２】
Ｓ５：カーデーラのアプリケーション稼働ホストは、カーデーラ独自の顧客へのナビゲーションやサービスを制御コマンドに基づいて行う。
【００６３】
Ｓ６：このとき、アプリケーション稼働ホストはアプリケーション稼働ホストの事前に保持する顧客データベースと受信した制御コマンドにより、動的個人情報を生成し、先に受け取ったコマンドと合わせて、顧客へのサービスを実行する。
たとえば、来店モード（暇つぶし）を入店時に指示した顧客は、静的個人情報と来店モードとの組み合わせによるコンピュータ処理、すなわち、静的個人情報の家族構成の子供ありという情報と来店モード（暇つぶし）という情報の組み合わせによるコマンドを受け取っている。これによって、この顧客には子供の遊べるコーナーがナビゲーションされる。
来店モード（車の詳細を知りたい）を入店時に指示した顧客は、静的個人情報の購入履歴から過去セダンばかりを購入しているという情報と合わせたコマンドを受け取っている。
店舗のアプリケーション稼働ホストも顧客データベースを保持しており、顧客携帯端末の静的個人情報とコマンドにより、セダンの詳細を知りたいというコマンドを受け取っている。
【００６４】
店舗のアプリケーション稼働ホストのサービスについて説明する。
店舗のアプリケーション稼働ホストの持つ顧客データベースから生年月日を基に現在の年齢を算出し、年齢と購入履歴と来店モード（車の詳細を知りたい）を合わせて、セダンの3D表示の大画面でのサービスを、乗車の案内とともに行う。このとき、過去の購入車両

の価格ランクとローンの情報によって、対象となるセダンの価格ランクもアプリケーション稼働ホストのコンピュータにより選定される。この時、個人の購買力（年収・ローン残高）などは、コマンド表現に変換して送受信されるので、個人セキュリティが漏出することは無い。生年月日も自家用車買い替えサイクル年齢モデル（自動車販売店が案出・設定した顧客の購買モデル）に従って符牒のような言葉で表現され、年月日・実年齢がデータとして流出する恐れはない。家族構成データによってはチャイルドシートでの安全性を遡及するコンテンツが、車両の紹介に続いて、同一のディスプレイに、強調された表示モードで表示される。

この際、コンテンツの選択、表示・出力デバイスの選択、表示モードの選択などを、制御コマンドにより行う。

【００６５】

気楽な気持ちで大人の暇つぶしに来店した顧客に、執拗な商品アピールを行うことにより、再度の来店を嫌う心理を醸成したり、不快な店という印象を与えることを避けることができる。また、目的を持った顧客には、目的に合致したサービスを行うことができる。

【００６６】

（Ｂ）カーデーラにお客が、自宅のパソコンからインターネットで自家用車更新の予備知識を照会する場合。この場合、パソコンが個人携帯端末に相当する。

カーデーラでは、アプリケーションをアプリケーション稼働ホストに持っており、また、個人情報データベース（お客さんBの過去の自店での購入履歴、ローンの内容など）を、アプリケーション稼働ホストに持っている。

【００６７】

お客のカーデーラへの依頼により、カーデーラはアプリケーションルールをアプリケーション稼働ホストから個人情報保持ホスト（個人のパソコン端末）に送信する。

【００６８】

照会内容を入力する。

【００６９】

制御コマンドは、保持された静的個人情報と、照会内容を合成して生成される。お客は自家用車買い替えの予備知識の照会をするため、受信したアプリケーションに従って、興味ある車の情報をインターネットを通してカーデーラのホームページ上に求める。

たとえば静的個人情報のセダン購入実績ありという情報と、照会した車の車名をセットにしてコマンドを生成したり、過去の購入履歴の色情報とセダンの車種を組み合わせたコマンドを生成したりする。

【００７０】

カーデーラのアプリケーション稼働ホスト内では、受信した制御コマンド事前と常時保持している個人情報に基づきサービスを提供する。

【００７１】

生成された制御コマンドが送信されるが、通信中の個人情報は、制御コマンドの形に変換されて伝えられる形になっており、他人に暴露されても解読不能である。このコマンドによってお客が求めた情報のうち、特にパーソナライスされた情報の伝達と、個人情報のセキュリテイの確保が可能になる。

【００７２】

（Ｃ）家具販売システム

家具販売店舗は広く、商品の数が多く、かつ、一つ一つが高額であり、商品のカテゴリーと顧客の嗜好を組み合わせることが、来店客の購買意欲を高めるために有効である。

【００７３】

アプリケーションルールを来店した顧客の個人携帯端末に送信する。

【００７４】

携帯端末内では、保持した個人情報と受信したアプリケーションルールによって、制御コマンドを生成する。

【００７５】

この制御コマンドは、顧客の嗜好を年齢との関連で抽象してコンピュータのコマンドとして表現したものである。

生年月日から年齢が算出され、整形外科での診療項目から腰痛を持つ老人の顧客という抽象顧客プロフィールが算出される。商品カテゴリーは健康基準カテゴリーが適用され、ベッドとしてはウォーターベッド、椅子には座椅子も加えた推奨商品カテゴリーが選ばれて店内をナビゲーションするストーリーの制御コマンドが生成される。

【００７６】

生成された制御コマンドをアプリケーション稼働ホストに送信する.

【００７７】

アプリケーション稼働ホストは、受信した制御コマンドに基づいて、店舗内で嗜好をさらにカテゴリー化して、客の典型的プロフィールと対応づけ、売り場ごとに客のプロフィールに適合する商品を表示したりしてナビゲーションする。コンテンツと表示デバイス、表示モードの選択をコマンドによって行うことにより、顧客の携帯への表示や大型のディスプレイに表示なども行う。お客のイベントでの来店履歴、購買履歴などを基にお客にフィットする商品をナビゲーションしたり、さらに他店在庫商品をコンテンツとして表示したりする。

【００７８】

発明の実施の形態３.

発明の実施の形態１の最後の部分で述べた、ユーザによる判断基準の導入や個人情報の処理を実現するための方法／システムについて説明する。

【００７９】

本発明の実施の形態３の要点は、ユーザルールに基づいて、個人情報の粒度（granularity）を変更してからアプリケーションルールに個人情報を提供する、という点にある。

【００８０】

まず、ユーザルールについて説明する。

ユーザルールによって、ユーザのプライバシプロフィールを開示する際の粒度が決定される。サービスルールがユーザのホストに到着すると、要求されたプライバシプロフィールのリストが提供される。サービスルールに対して提供される要求されたプライバシプロフィールの粒度は、ユーザルールによって変えられる。

【００８１】

ユーザルールとは、ユーザ自身が定義する決まりである。上記のとおり、ユーザは、サービスの機密性に応じて構成することができる。例えば、ユーザが知らないサービスに対しては、プライバシプロフィールを粗い粒度で提供し、よく知っているサービスに対しては、細かい粒度で提供する。つまり、ユーザルールは、プライバシプロフィールの各単位別に、そして各サービス別に存在するべきである。例えば、ユーザの誕生日に関するユーザルールによって、それを広告サービスに対して開示する粒度が決定され、他の場合も同様である。

【００８２】

次に、本発明の実施の形態３の動作について説明する。

図１４には、簡単なタイムチャートが示されている。縦軸は時間を表す。矢印は行動又は動作を示す。点線の矢印は別の順序のパターンを示す。

【００８３】

Ｓ１１：ユーザは、自己のプライバシプロフィール及びユーザルールをユーザデバイスに設定する。

【００８４】

Ｓ１２：いくつかのイベント、又は要求によって、サービスが開始される。例えば、ユーザがスタートボタンを押すか、又はユーザが特定の領域に入るとサービスが開始する。サービスを運営しているホストは、直ちにサービスルールをユーザのモバイルデバイスに送る。

【００８５】

Ｓ１３：サービスルールに従って、要求されたプライバシプロフィールのリストがユーザのデバイスに存在する。

【００８６】

Ｓ１４：ユーザルールに従って、プライバシプロフィールの粒度が変更され、サービスルールに提供される。

【００８７】

Ｓ１５：サービスルール及び提供されたプライバシプロフィールの両方から、コントロールコマンドが生成される。

【００８８】

Ｓ１６：コントロールコマンドが返される。

【００８９】

次に点線の矢印の順序のパターンについて説明する。

【００９０】

Ｓ１６’：使用されるプライバシプロフィールをユーザ側で確認することができるようにする場合、ユーザにコントロールコマンドが通知される。

【００９１】

Ｓ１７：ユーザが確認する。

【００９２】

Ｓ１８：その後、コントロールコマンドが返される。

【００９３】

基本的に、コントロールコマンドは、サービスルールから生成されるからこそプライバシプロフィールの一部を示す。例えば、サービスプロバイダが、以下のようにプライバシプロフィールとコントロールコマンドの間の関係を一対一とするサービスルールを説明したとする。

【００９４】

```
if (profile = A) then command = a.
else if (profile = B) the command =b.
```

【００９５】

この説明は、もしもコントロール・コマンドが“ａ”である場合、ユーザのプロフィールは“Ａ”であり、同様のことが“ｂ”の場合に適用されることを意味する。サービスが悪意の場合は、プライバシに関する問題が発生し、サービスが悪意でない場合には、問題は起こらない。

【００９６】

よって、サービスルール自体からは具体的なプライバシプロフィールを引き出すことができないよう保証するべきである。本発明の実施の形態においては、プライバシプロフィールについて粒度という概念を紹介するため、この条件を満たす。

【００９７】

図１５の左側においては、連続したデータの場合、例えば特定の回数や、誕生日、結婚記念日等の記念日を示す。もしもユーザのプライバシ・プロフィールが“３”である場合、“１－４”又は“０－１２”に変更することができる。よって、悪意のサービスルールは、具体的なプロフィールを特定できない。例えば、ユーザが“２４才”である場合、プロフィールを“２０才代”に変更することができる。

【００９８】

図１５の右側においては、階層的なデータの場合、例えば住所や提携関係を示す。もしもユーザのプライバシプロフィールが“Ａ‐Ｂ－Ｄ”である場合、“Ａ－Ｂ”、又は“Ａ”に変更することができる。例えば、ユーザの住所が“ＸＸＸ　Ｎ．マシューズ・アベニュー、アーバナ、イリノイ州６１８０１、アメリカ合衆国”である場合、“アーバナ、イリノイ州６１８０１、アメリカ合衆国”又は“イリノイ州６１８０１、アメリカ合衆国”に変更することができる。

【００９９】

よって、悪意なサ‐ビスルールにおいて、ユーザのプライバシプロフィールとコントロールコマンドとの間に一対一の関係を構築することはできない。このように、本発明の実施の形態によって、プライバシの保護と同時に、プライバシプロフィールの適用の保護を可能とする。

【０１００】

本発明は、以上の実施の形態に限定されることなく、特許請求の範囲に記載された発明の範囲内で、種々の変更が可能であり、それらも本発明の範囲内に包含されるものであることは言うまでもない。

【図面の簡単な説明】

【０１０１】

【図１】従来の個人情報送信型モデルの説明図である。

【図２】本発明の実施の形態に係る個人情報非送信型モデルの説明図である。

【図３】本発明の実施の形態に係るシステムの概念図である。

【図４】本発明の実施の形態に係るシステムの基本動作の説明図である。

【図５】本発明の実施の形態に係る個人情報のＤＴＤの例である。

【図６】本発明の実施の形態に係るアプリケーションルールの例である。

【図７】本発明の実施の形態に係るアプリケーションルールの移送の例である。

【図８】本発明の実施の形態に係るアプリケーションによるコマンド要求部の呼び出し例である。

【図９】本発明の実施の形態に係るアプリケーションルールの取得の例である。

【図１０】本発明の実施の形態に係るＸＭＬの解析の例である。

【図１１】本発明の実施の形態に係る個人情報の記述例である。

【図１２】本発明の実施の形態２に係るシステムの概念図である。

【図１３】本発明の実施の形態２に係るシステムの基本動作の説明図である。

【図１４】本発明の実施の形態３に係るシステムの基本動作の説明図である。

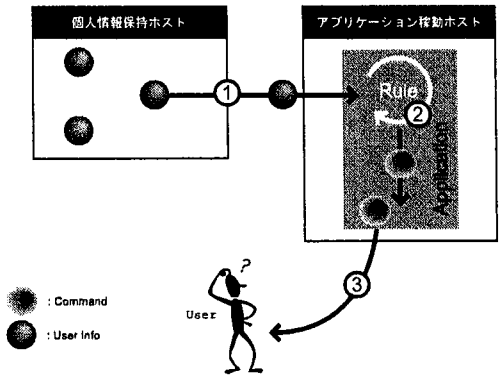
【図１５】本発明の実施の形態３に係る粒度の観念を示す図である。

【符号の説明】

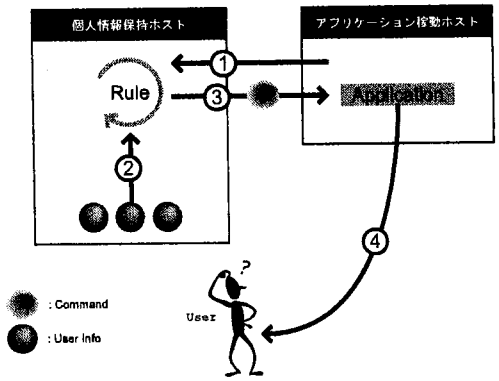
【０１０２】

１　アプリケーション稼働ホスト
１１　アプリケーション処理部
１２　コマンド要求部
１３　アプリケーションルール記憶部
１４　個人情報データベース
１５　動的個人情報生成部
２　個人情報端末
２１　コマンド生成部
２２　個人情報管理部
２３　モード入力部

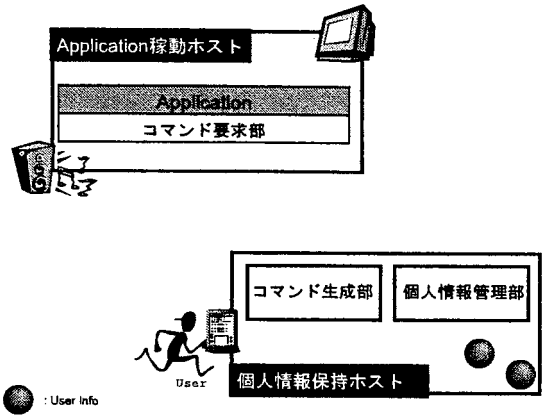
【図１】



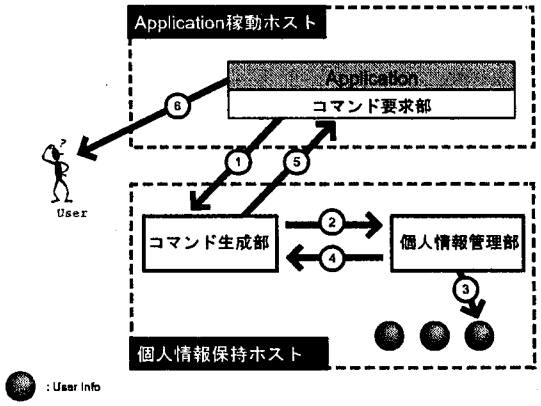
【図２】



【図３】



【図４】



【図５】

```
<?xml version="1.0" encoding="Shift_JIS"?>
<!ELEMENT userinfo (data+)*>

<!ELEMENT data EMPTY>
<!ATTLIST data name CDATA #REQUIRED>
<!ATTLIST data value CDATA #REQUIRED>
```

【図６】

```
interface EAP2ApplicationInterface{
  public char evaluate(String file);
}
```

【図７】

```
ObjectOutputStream os
 = new ObjectOutputStream
          (s.getOutputStream());
os.writeObject(new ApplicationRuleImpl());
```

【図８】

```
char command ;
UserInfoRequest ur
   = new UserInfoRequest(hostAddr,port);
command = ur.getCommand();
```

【図９】

```
ObjectInputStream ois
 = new ObjectInputStream
              (s.getInputStream());
ApplicationRule appRule
 = (ApplicationRule)ois.readObject();

command = appRule.evaluate();
```

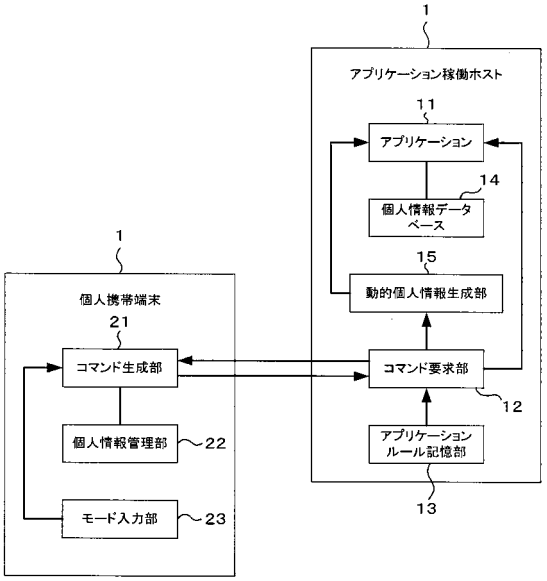
【図１０】

```
public void startElement
    (String URL,String localName,
     String qName,Attributes attrs){
 if(qName.equals("data")){
   for(int i=0;i<attrs.getLength();i++){
     data[i] = attrs.getValue(i);
   }
 ...
```

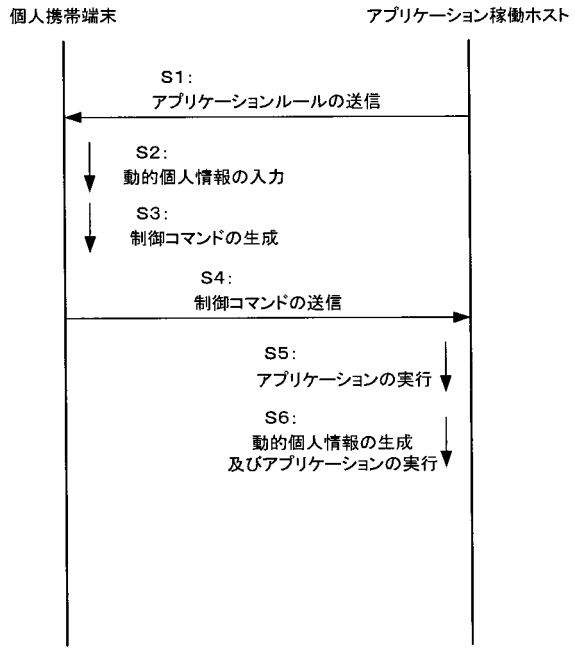
【図１１】

```
<?xml version="1.0" encoding="Shift_JIS"?>
<!DOCTYPE userinfo SYSTEM "EAP2.dtd">
<userinfo>
  <data name="age" value="23"/>
  <data name="sex" value="lady"/>
  <data name="nation" value="japan"/>
  <data name="job" value="student"/>
</userinfo>
```

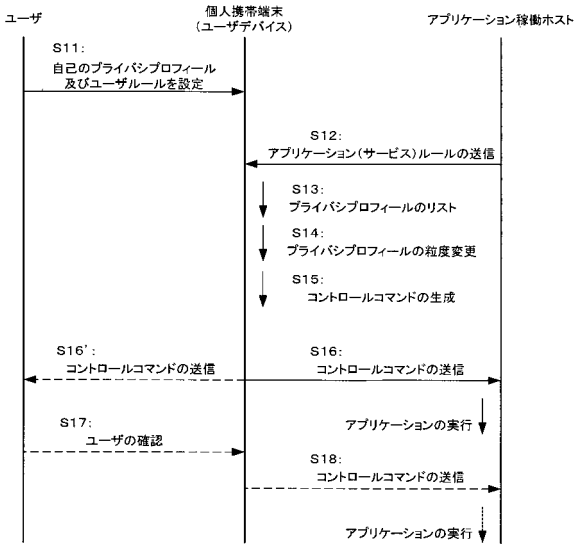
【図１２】



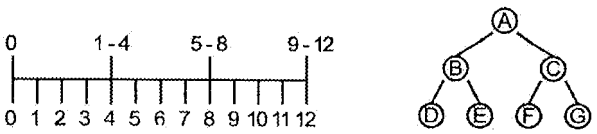
【図１３】



【図１４】



【図１５】



フロントページの続き

(72)発明者　高汐　一紀
神奈川県藤沢市遠藤５３２２　慶應義塾大学　湘南藤沢キャンパス内
(72)発明者　徳田　英幸
神奈川県藤沢市遠藤５３２２　慶應義塾大学　湘南藤沢キャンパス内
(72)発明者　村　浩二
東京都江東区潮見二丁目９番１５号　株式会社内田洋行　潮見オフィス内
(72)発明者　坪井　公載
東京都江東区潮見二丁目９番１５号　株式会社内田洋行　潮見オフィス内
(72)発明者　伊原　文子
東京都江東区潮見二丁目９番１５号　株式会社内田洋行　潮見オフィス内

審査官　辻本　泰隆

(56)参考文献　特開平０８－２２７４２５（ＪＰ，Ａ）
特開２００３－１１４８７４（ＪＰ，Ａ）
特開２００１－１０１１３１（ＪＰ，Ａ）
特開平１０－２４０８２８（ＪＰ，Ａ）
田丸修平，ユーザ情報非送信型プライバシ保護手法，慶應義塾大学環境情報学部，2002年度(平成14年度)卒業論文，２００３年　3月３１日
田丸修平　外３名，プライバシを考慮したパーソナライゼーションを実現するアプリケーションフレームワーク，情報処理学会研究報告、2003 No.42　2003-OS-93，２００３年　5月　8日

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｆ　１５／００