情報処理学会論文誌 Vol. 50 No. 4 1334–1346 (Apr. 2009)

推薦論文

仮名認証に基づいた地域交通支援システムのための位置情報プライバシ保護フレームワーク

山崎 重一郎[†1]

個人の日々の活動の中で生み出される個人情報を活用する Web 企業の成功によって，個人情報の有用性が再認識されるようになった．個人情報はビジネスだけではなく都市交通などの公共サービスにおいても有用な情報であるが，個々の企業や組織の責任と費用負担で個人情報を安全に管理することは一般に困難がともなう．我々は，個人情報の安全な有効活用を目的とする統合的個人情報管理システム「アイデンティティ・シェルタ」の研究開発を行っている．アイデンティティ・シェルタは，アプリケーションサービスから共通的に利用できるプライバシ保護のための社会情報基盤の 1 つになることを目的としている．アイデンティティ・シェルタの主な特長は，(1) アプリケーション中立的な認証認可機構，(2) 仮名認証によるアイデンティティの隠蔽，(3) 利用者中心型の個人情報管理，(4) Place Agent モデルによる匿名化通信，(5) Place Agent モデルによる個人情報流通範囲の限定とアクセス記録の保持である．本論文では，アイデンティティ・シェルタの概説とロケーションプライバシの既存研究からの要件分析を行ったうえで，前半においてアイデンティティ・シェルタの公共サービスへの応用例として，利用者の位置や目的地情報をプライバシを保護しつつ流通させることによって地域の交通資源に対する需要と供給を最適化する地域交通支援システムを提案する．後半で提案した地域交通支援システムのプロトタイプを利用した実験について報告する

A Pseudo Identity Based Location Privacy Framework for Local Traffic Support Systems

Shigeichiro Yamasaki[†1]

Recent years, many succeeded web companies shows that the personal information such as histories of searching or histories of purchasing of a person is valuable. Such kinds of personal information is also valuable for various public services like a local traffic control system. However, it is difficult to manage personal information safely for ordinal private companies or organizations. We have been developing an integrated personal information management system which we call 'Identity Shelter.' We intend for our Identity Shelter to be a kind of the social information infrastructure for privacy protection. The peculiar features of our Identity Shelter are (1) application independent authentication and authorization, (2) identity protection by pseudo identity based authentication and authorization, (3) user centric private information control, (4) anonymous communication with Place and Agent model, (5) Limitation of distribution of the personal information and logging of access history with Place and Agent model. In the former part of this paper, we explain the overview of Identity Shelter and our traffic control system for a local area which requires the location and the destination information of passengers as an application of Identity Shelter. In the latter part of this paper, we report the results of the experimentation with a prototype of our local traffic control system.

1. はじめに

個人情報保護法が施行された当初，多くの企業や組織は個人情報の収集や活用を制限し情報管理義務を回避しようとしたが，近年では個人情報の有用性が再認識されている．たとえば，SNS や検索エンジンマーケティングや顧客の購買履歴に基づくマーケティングなど Web によるサービスで成功している企業の多くは個人が日々の活動の中で生み出す情報を合法的な手段で収集しビジネスに活用している．そしてこのような個人情報は，ビジネスだけでなく公共サービスの効率化においても価値の高いものである．その一例が都市交通における交通資源の需要と供給の最適化である．

日々の暮らしの中で都市の中を移動する人々の位置情報や目的地などの情報を正確に利用できれば，都市の交通需要を高精度で把握することが可能になり，交通資源の供給制御の効率化などが期待できる．特に，路線バスの廃止などで，交通資源の減少に悩む地方都市にとって，都市の限られた交通資源の効率的な供給制御の実現は切実な要求である．

しかし，個人情報の漏洩や不正使用などの事故が発生すると企業や組織の信用が大きく傷つくため，個人情報の有効利用の実現には安全な情報管理体制の整備が前提となる．そして

†1 近畿大学
Kinki University
本論文の内容は 2007 年 7 月のマルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウムにて報告され，コンピュータセキュリティ研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

個々の企業や組織の責任と費用負担でそれを実現することは一般に困難がともなう．

本研究の目的は，個人情報の安全な管理と有効活用を両立させるプライバシ保護システムを，電子認証基盤などと同様の一種の社会情報基盤として提案することである．

2. アイデンティティ・シェルタの概要

我々は，個人情報の安全な有効活用を目的とする統合的個人情報管理システム「アイデンティティ・シェルタ」[12] の研究開発を行っている．我々は，アイデンティティ・シェルタを多様なアプリケーションサービスから共通的に利用できるプライバシ保護のための社会情報基盤の 1 つとすることを目指している．

アイデンティティ・シェルタの特長は，次の 5 点である．

(1)　アプリケーション中立的な認証認可機能
(2)　仮名認証によるアイデンティティの隠蔽
(3)　利用者中心型の個人情報管理
(4)　Place Agent モデルによる匿名化通信
(5)　Place Agent モデルによる個人情報流通範囲の限定とアクセス記録の保持

図 1 は，アイデンティティ・シェルタの構成を概念的に表したものである．以下にこの 5 つの特長について説明する．

2.1 アプリケーション中立的な認証認可機能

現在の多くの Web ベースのアプリケーションサービスでは，それぞれのサイトで利用者登録を実施し，それぞれが利用者認証機能および認可機能を持ち，それぞれにおいて個人情報の蓄積を行っている．

しかし，近年では，ブログ記事へのコメントスパム対策を目的としたコメント書き込み者の認証やマッシュアップ型サービスを利用するための認証などの要求から，外部組織の認証結果を相互利用する技術が普及しはじめている．

このようなアプリケーション中立的な認証認可機構としては，元来はシングルサインオンを目的に OASIS によって標準化が進められてきた SAML [1] や MicroSoft によって推進されている CardSpace [2] や OpenID Foundation による OpenID [3] などがある．現在の我々のアイデンティティ・シェルタの実装では，OpenID およびその属性交換に関する仕様である OpenID AX [4] をそれぞれ認証と認可システムに利用している．

上記のようなアプリケーション中立的な認証認可機構では，本人確認を意味する「認証」と本人に対する権限付与を意味する「認可」のそれぞれに対して独立した 2 つのトークンを利用する．本論文では，これらをそれぞれ「認証トークン」と「認可トークン」と呼ぶことにする．

図 2 は，アプリケーション中立的な認証認可機構の典型的なログインシーケンスである．以下にこのログインシーケンスを説明する．

(1)　アプリケーションサービスにログインしようとすると，HTTP Redirection を利用して自動的に認証サービスにリダイレクトされる．

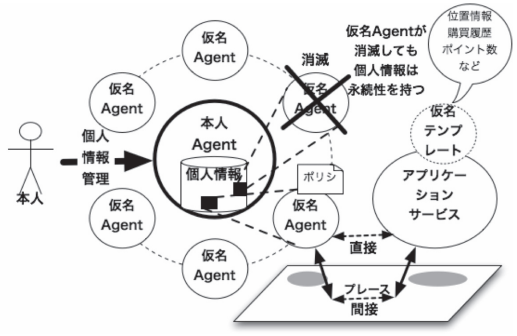

図 1　アイデンティティ・シェルタの概念図
Fig. 1　Conceptual design of Identity Shelter.

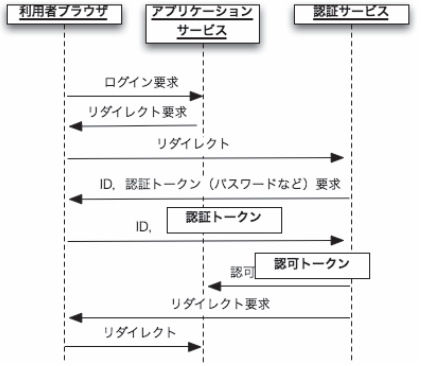

図 2　アプリケーション中立的な認証認可機構における認証トークンと認可トークン
Fig. 2　ID token and authorization token for the application independent authentication and authorization.

(2)　認証サービスから利用者に向けて ID と認証トークン（パスワードなどの本人確認のための情報）が要求される．
(3)　利用者が認証サービスに対して自分の ID と認証トークンを送信する．
(4)　認証サービスは，利用者から受け取った ID と認証トークンを検証する．検証が成功した場合，ポリシに基づいて認可トークンをアプリケーションサービスに送信する．
(5)　認証サービスは，HTTP Redirection を利用して利用者の接続先を元のアプリケーションサービスへリダイレクトする．

我々のアイデンティティ・シェルタは，この 2 つのトークンを使用する認証プロトコルを仮名認証によるアイデンティティの隠蔽に利用している．

2.2　仮名認証によるアイデンティティの隠蔽

個人を特定可能な本名などのアイデンティティをアプリケーションサービスに対して適切に隠蔽されることはプライバシ保護の基本的要件である．

図 2 のアプリケーション中立的な認証認可機構の典型的なログインシーケンスを観察すると，利用者はアプリケーションサービスに対して直接的には ID も認証トークンも渡していないことが分かる．認証サービスからアプリケーションサービスに渡される認可トークンの中に利用者を識別可能な名前や ID が含まれなければアイデンティティ隠蔽のプライバシ要件が満たされる．

しかし，アプリケーションサービスは，コンテクストを持ったサービスの提供やポイント数などの属性の連続性を判別するために何らかの利用者の識別子を必要とする．我々は，本人のアイデンティティを隠蔽するために用いる識別子として「仮名」という概念を導入し「匿名」の概念と区別する．

2.2.1　仮名（pseudo identity）

我々が導入する「仮名」の概念は，現実の本人の属性や権限の正確な射影につけられた識別名であり，識別名以外には虚偽の情報を含まないものとする．そして，その内容の正確さは，信頼できる第三者によって保証され，何らかの技術的な手段でその信頼性が検証可能なものとする．

仮名は，それが信頼できる用途の範囲で，投票，決済，通報，取引などの行為を行う権限と責務を持つことや与信を受けることができる．また仮名は，個人が持つ様々な社会的な人格の 1 つを代表するものであるともいえる．たとえば，アイデンティティ・シェルタでは，アプリケーションサービスから顧客に与えられるクーポンやポイントなどは，仮名によって識別される個人の 1 つの人格が対象になる．

EU の PRIME プロジェクト[15] においても，通報や投票の秘密を守りつつ「匿名」とは異なる責任ある個人を識別するために「pseudo identity」という概念に注目し様々なプライバシ要件の分析に用いているが，この pseudo identity と我々の仮名の概念はほぼ同じであるといってよい．ただし，PRIME プロジェクトにおける pseudo identity の概念が，電子プライバシに関する法理論的な用語であるのに対して，我々の「仮名」はより限定された技術的用語である．

2.3　利用者中心型の個人情報管理

図 1 に示したように，アイデンティティ・シェルタの中核は本人 Agent であり，その中にはその個人の情報を集約的に管理するデータベースサービスが存在している．本人 Agent によるデータベースサービスは，外部のシステムに対してサーバとしてもクライアントとしても機能する自律的なプロセスなので「Agent」という用語を用いている．ただし，本人 Agent は，本人以外の外部システムとは直接的に通信を行うのではなく，必ず「仮名 Agent」と呼ぶプロキシを介して通信する．

通常の Web アプリケーションサービスは，それぞれのサービスごとに利用者の購買履歴やポイント数などを管理するが，アイデンティティ・シェルタでは，このような情報も本人 Agent のデータベースで管理することを基本とする．

個人情報は本人が管理するという方針がアイデンティティ・シェルタの設計の基本的な考え方となっており，我々はこれを「利用者中心型の個人情報管理」と呼んでいる．

関連する研究として，Bagues らによる User-Centric Privacy Framework[7] がある．この研究は，ユビキタス環境における個人のコンテクストを保護する手段を「Transformations」と「Foreign Constraints」という 2 つの概念で抽象化している．「Transformations」は，本人が自ら定義した方法で個人情報を変換することによって情報の露出を防ぐ方法の一般化であり，「Foreign Constraints」は本人を取り巻く他者を介した情報漏洩に対する制約を一般化したものである．後に示すように，我々の利用者中心型の個人情報管理も，このフレームワークの実現方法の一例ということができる．

利用者中心型の個人情報管理の実現方法の特長は次の 2 点である．

(1)　仮名テンプレート
(2)　個人情報の永続性

2.3.1　仮名テンプレート

図 1 に記載されているように，アプリケーションサービスは，それぞれのアプリケーションが必要とする個人情報のテンプレートを持つものとしている．たとえば，書籍販売のサー

図 3　アイデンティティ・シェルタに組み込まれた仮名テンプレート
Fig. 3　A template of pseudo identity.

ビスであれば，購買履歴，郵送先住所，ポイントの蓄積数などの構造がテンプレートになり，SNS であれば友人のリスト，日記のリストなどがテンプレートになる．

実際の購買履歴や郵送先住所やポイント蓄積数などは，アプリケーションサービス側ではなく，仮名 Agent を介して本人 Agent のデータベースの内部に蓄積される．仮名 Agent は，アプリケーションサービスから提供された仮名テンプレートに基づいて生成され，仮名 Agent を介して蓄積されるデータの構造を決定する．

図 3 は，アイデンティティ・シェルタに組み込まれた仮名テンプレートの例である．この図のように，アプリケーションサービスを利用するとき，どの仮名人格を利用するか選択することができる．また，事前にアプリケーションサービスごとに利用する仮名 Agent を設定しておけば，自動的にサービスを提供することもできる．

2.3.2　個人情報の永続性

我々の利用者中心型の個人情報管理におけるの設計方針のもう 1 つの柱は，個人情報の永続性である．個人情報を管理する本人 Agent は，アプリケーションサービスとは独立に本人が存在を希望する限り永続的に存続する．これに対して仮名 Agent は，特定のアプリケーションサービスを利用している間だけ利用者を代理するものである．したがって，仮名 Agent の寿命は一般に本人 Agent よりも短い．特に匿名性を重視するサービスでは，仮名

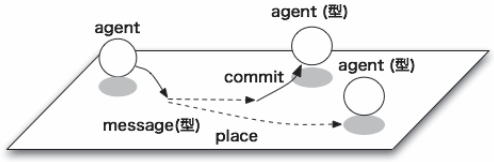

図 4　Place Agent モデル
Fig. 4　The Place and agent model.

Agent を短期間で消滅させては別の仮名 Agent を新規に生成して処理を引き継ぐという方法を使うことさえある．しかし，仮名 Agent が消滅してもそれを通じて本人 Agent の内部に蓄積された個人情報は消えることなく永続的に保持される．さらにすべての記録は時間軸と利用したアプリケーションサービスの識別にそって一貫性を持って保持される．

2.4　Place Agent モデルによる匿名化通信

アイデンティティ・シェルタは，アプリケーションサービスに対して本人 Agent が保持している個人情報を仮名 Agent を介して提供するために自律的に動作するサーバとして機能する．また，アプリケーションサービスの側は，クライアントとしてアイデンティティ・シェルタの仮名 Agent に個人情報を要求する．

2.4.1　Place Agent モデル

Place とは，Agent どうしがコミュニケーションを行う場である．Place 自身も URI を持つ 1 つの自律的なサーバシステムである．Place に参加する Agent は，それぞれ一定の型を持つ．

Place 内の Agent 間のコミュニケーションは，Place を介して行われる．**図 4** は，Place に参加している Agent 群が Place を介して他の Agent とコミュニケーションを行う様子を概念化したものである．より具体的には，次のようにしてメッセージの交換が行われる．

(1)　メッセージ送信者の Agent が，メッセージの受信者 Agent の型とメッセージの内容の対として構成されたデータを Place に渡す．
(2)　Place に参加しているすべての Agent は，その Place に渡されたメッセージを検出する．
(3)　メッセージ受信者 Agent の型が適合する Agent 群のうち，だた 1 つの Agent だけがそのメッセージにコミットし，メッセージを受け取る．
(4)　メッセージを受け取った Agent が処理を行い，その応答を Place に返す．
(5)　メッセージ送信者の Agent は，Place からメッセージの応答を受け取る

たとえば，バスの乗客のコミュニティを意味する Place があり，そこに複数の「乗客型」の Agent が参加していた場合，乗客型 Agent 宛のメッセージは，Place 宛に送信され，それを受け取るのは，Place に参加している乗客型 Agent のうちそのメッセージにコミットしたただ 1 つの Agent である．

アプリケーションサービスがアイデンティティ・シェルタの仮名 Agent にアクセスする方法には次の 2 種類がある．

(1)　仮名 Agent の URI を利用してアクセスする．

(2)　仮名 Agent が参加しているコミュニティの Place の URL を使って間接的にアクセスする．

仮名 Agent の URI を利用する方法は，通常の Web サーバへのアクセスと変わりはない．仮名の利用によって本人のアイデンティティは隠蔽されているが，仮名としてのアイデンティティの露出や履歴情報や属性情報の露出は避けることができない．一方，Place の URI を利用する場合は，宛先 Agent の型とその Place に参加している Agent であることは分かるが，具体的にどの Agent であるかということはメッセージの送信側には分からない．

たとえば，バスの乗客のコミュニティを意味する Place の場合，「乗客型」Agent の現在位置や目的地などの個人情報を問い合わせて応答を得ることができるが，それに答えたのがどの「乗客」であるかは分からない．

2.5　個人情報に対する流通範囲の限定とアクセス記録の保持

個人情報の活用の視点で見ると，情報の流通範囲が限定されていることは重要な特性となる．Place Agent モデルの利点の 1 つは，情報流通範囲を同じ Place に参加している Agent 群のみに限定できることである．Agent が新規に Place に参加するには，認証と認可を経ることが必要であり，一定の権限を持った Agent のみが Place に参加できる．したがって，Place は一種のプライベートネットワークであるということができる．

Place のもう 1 つの機能として，メッセージへのアクセス記録の保持がある．これは，Place 内でメッセージにアクセスした主体の記録を時間軸にそって保持できるという機能である．多くの SNS で実装されている「足跡機能」と同様のものであり，個人情報の不正な利用が疑われた場合には，この記録を用いて立件や追求などが可能になる．

3.　ロケーションプライバシの既存研究と要件

現在位置や目的地など位置情報に関連した個人情報には独特の特性と要件があり，これをロケーションプライバシと呼ばれている．ここでは，ロケーションプライバシの関連研究と要件について述べる．

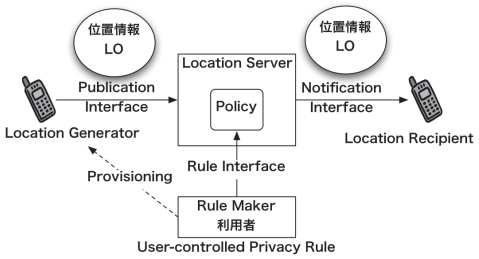

図 5　IETF Geopriv の基本モデル
Fig. 5　The basic model of IETF Geopriv.

3.1　ロケーションプライバシの目的

ロケーションプライバシの目的は，意図しない第三者に自分の位置情報を知られてしまうことを防止することである．

3.2　ロケーションプライバシの関連研究

ロケーションプライバシの研究としては，ロケーションプライバシアーキテクチャに関する研究と位置情報や行動履歴などの匿名化の手法に関する研究が代表的である．前者としては，IETF Geopriv WG[14] における成果や Langheinrich のユビキタスシステムプライバシの 6 原則[13] をあげることができる．また後者の研究としては，中西らによる人口密度に応じた位置情報粒度の変更による匿名性の保持の研究[16] や貴戸らによる移動軌跡の追跡可能性の評価指標とダミー情報の挿入による匿名性の研究[17] などをあげることができる．

3.2.1　IETF Geopriv WG

IETF の Geopriv WG は，位置情報を扱うサービスの一般的アーキテクチャ標準を RFC3693 などの文書で提案している．**図 5** は Geopriv の基本モデルを示したものである．

Geopriv WG のアーキテクチャは，ルールに基づいた LO（Location Object）の流通に関するセキュリティの定義を基本としている．LG（Location Generator）で発生した LO が LS（Location Server）を経由して最終的に LR（Location Recipient）に到達するという情報流通を基本としている．

Geopriv には多くの原則があるが，特に利用者中心のルール作成と運用や合理的理由がない限り LO とアイデンティティはリンクされるべきでないとしている．

3.2.2　Langheinrich のユビキタスプライバシの 6 原則

Langheinrich は，ユビキタスプライバシの原則として次の 6 つをあげている[13]．

通知の原則　データ収集側は使用目的，使用者，データ保持期間などを記述したプライバシポリシをデータ提供側に伝え，両者の条件を満足したときのみデータが提供される．

同意の原則　ユーザによるデータ提供への同意は明示的に行われる．

匿名と仮名の原則　明示的な同意が困難な場合は匿名化や仮名化ができること．

局所化の原則　データの収集はユーザの近傍に限られ，ユーザがサービスの利用を終了するとデータ収集は止められる．

セキュリティの原則　適切なセキュリティがかかっていること．

請求権の原則　使用履歴などで自分のデータへのアクセス状況が分かるようにしていること．

4. アイデンティティ・シェルタの地域交通支援システムへの応用

次に，アイデンティティ・シェルタの応用例として実際にこのシステムに基づいてロケーションプライバシの要件を満足する地域交通支援システムを構成する．

4.1 地域交通問題における個人情報収集の必要性

全国の地方都市でバス路線の廃止による交通空白地域の拡大や高齢化にともなう運転免許返上による交通弱者の増加が社会問題になっている[8]．この困難な問題に対処するには，都市内の交通需要の正確な把握を行ったうえで，地域に残っているあらゆる交通資源を需要の高い時間と場所に的確に供給できるようにする必要がある[9)–11)]．都市を移動する市民の現在位置や目的地などの情報を安全に収集することができれば，交通需要の正確な把握が可能になる．

4.2 提案する地域交通支援システム

我々は，福岡県飯塚市の地域交通を対象として地域交通支援システム開発のための調査と試作を行った．飯塚市は 2006 年 3 月に旧飯塚市・穂波町・筑穂町・庄内町・頴田町が合併して誕生した，面積 214.13 km^2 人口密度 629 人/km^2，55,723 世帯，人口 134,602 人の都市である．飯塚市は急速な高齢化と人口減少が進行している日本の典型的な地方都市であり，飯塚市で機能する地域交通支援システムは他の多くの日本の地方都市にも適用可能である可能性が高い．

4.2.1 デマンド交通の情報化と利用者の行動予測

都市の交通資源の供給管理を実現する方法の 1 つとして，利用者からの要求に応じてバスや乗り合いタクシなどの運行を行うデマンド交通という形態がある．

デマンド交通は，予約という形で利用者から情報が登録されるので，この情報を活用することによって交通需要を正確に知ることができる．デマンド交通の一形態として，予約のないバス停や経路をスキップして運行されるフレックスルートバスというものがある．フレックスルートバス通常のフレックスルートバスの運用では，電話予約で前日までに予約するという形が普通だが，情報端末を利用した情報化を進めることによってよりリアルタイムに近い予約が可能になる．さらに利用者の最終目的地などの情報を収集することによってより効率的なデマンド交通が構成可能になる．さらに，デマンド交通の利用者が乗り継ぎなどを経て到達しようとする最終目的地などの情報が収集できれば，より大域的な交通需要についての予測情報を得ることができる．

4.2.2 提案する地域交通支援システムの基本構成

我々が提案する地域交通支援システムは，利用者のためのデマンド交通予約システムとデマンド交通事業者支援システムの 2 つのシステムから構成される．

利用者のためのデマンド交通予約システムは，同時にあいのりコミュニティ生成および参加システムになっている．このシステムは一種のコミュニティ機能を備えた地域 SNS であり，ここに利用者の位置情報や最終目的地や到着希望時刻などの情報を登録する．

交通事業者向けシステムは配車オペレータと運転者に，デマンド交通のバス停ごとの予約の受付けと大域的な地域交通の正確な需要予測情報を提供するシステムである．

4.2.3 デマンド交通予約システム

我々が提案するデマンド交通予約システムは，あいのりする仲間を募ることを目的としたシステムであり，自分が利用する予定のバス停と最終目的地および到着希望時刻および希望運賃を入力することによってバスの予約を行う．これを以降「あいのりコミュニティシステム」と呼ぶことにする．

図 6 は，デマンド交通の予約画面の例である．あいのりコミュニティシステムの利用者がログイン後に，既存のあいのりコミュニティに参加することで予約が可能になる．また，必要に応じて自ら新しいコミュニティを生成することもできる．図 6 の例は，病院の待合室に予約用の端末を設置して，次の移動先までの交通手段の予約するシナリオに基づいて設計したものである．

4.2.4 デマンド交通事業者支援システム

図 7 は，デマンド交通事業者支援システムのオペレータ用画面である．デマンド交通事業者支援システムは，各路線ごとの現時点での交通需要やあいのりコミュニティで予約している利用者の地図上の位置情報などを見ることができる．

4.2.5 プライバシポリシ設定とアクセス記録のチェック

あいのりコミュニティシステムでは，利用者が自ら自分の位置情報に関するプライバシポ

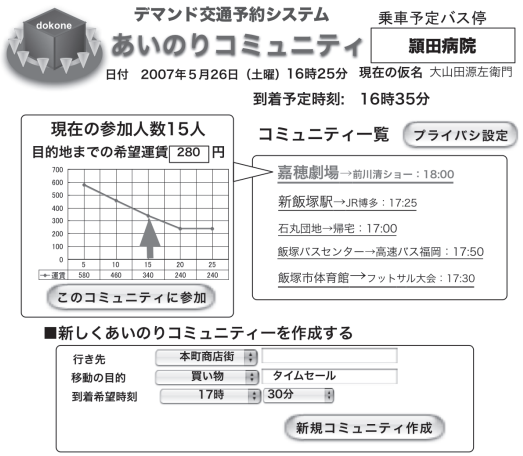

図 6　デマンド交通予約画面
Fig. 6　The demand bus reservation system.

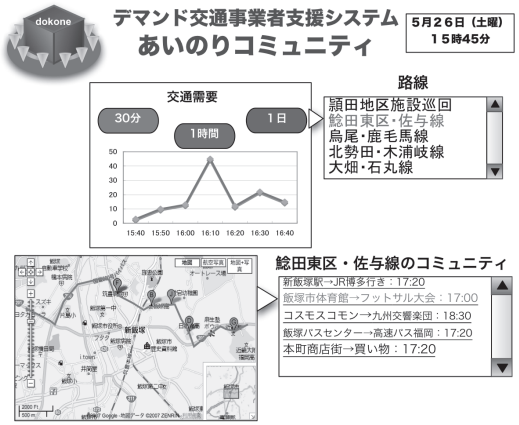

図 7　デマンド交通事業者支援システム
Fig. 7　Demand bus provider's system.

リシの設定ができる．このポリシには，個人情報を開示する相手と使用目的，位置情報や移動目的の開示をするかどうか，仮名の自動再生成の条件などの指定が含まれる．

さらに，このシステムにはアクセス記録のチェックを行う機構を備えている．これは，Place のアクセス記録保持機能を利用したもので，SNS などにおける「足跡機能」と同様に，自分の個人情報にどのような主体がいつアクセスしたかという記録を本人がチェックできる．

4.3　地域交通支援システムの実装

地域交通支援システムの実装について次の 3 つの構成要素の実装方法を中心に説明する．

(1)　アイデンティティ・シェルタの実装方法
(2)　Place Agent モデルの実装方法
(3)　仮名 Agent および仮名テンプレートの実装方法

4.3.1　アイデンティティ・シェルタの実装方法

アイデンティティ・シェルタは，本人 Agent と複数の仮名 Agent 群から構成される．

本人 Agent　本人 Agent は，本人の属性，人間関係，記憶，行動履歴などのすべての本人の個人情報を永続的に保存するデータベースである．Ruby on Rails の動的特性を利用して，新しい仮名テンプレートが登録されたときに，モデルの拡張が行えるようになっている．本人 Agent へのアクセスできるのは本人のみに限定されており，外部システムとは仮名 Agent を介してコミュニケートする．MVC モデルの観点では，外部システムに対するビューやコントロールは仮名 Agent のみにあるが，モデルは仮名 Agent のモデルが本人 Agent のモデルに埋め込まれている．

仮名 Agent　仮名 Agent は，外部システムに対する本人の社会的立場，人間関係，行使権限などを代表するインタフェースである．仮名 Agent は，仮名テンプレートから生成される．仮名 Agent は，自律的に動作するプロセスであり，ログインによって認証認可手続きが成立したアプリケーションサービスや Place に対して自動的に利用者の個人情報を提供する．仮名 Agent に対する個人情報開示ポリシは，利用者本人が設定を行う．利用者本人は，いつでも仮名 Agent を停止させ消去できる．仮名 Agent が停止すると，それを用いて接続されていたすべてのセッションが強制的に終了する．仮名 Agent とのセッションが終了すると Place は，その時点で残存していた仮名 Agent のメッセージをすべて削除する．仮名 Agent の停止後も Place はアクセスログの収集を継続する．

図 8 は，利用者がアプリケーションサービスや Place に参加するときのログインシーケンスである．

(1)　アイデンティティ・シェルタは，アプリケーション独立型認証機構であるため，利用者は，アプリケーションサービスや Place に自分の ID や認証トークンを開示することなく認証処理を行う．
(2)　認証サービスによる本人確認と利用者による仮名人格の選択が完了すると，アイデン

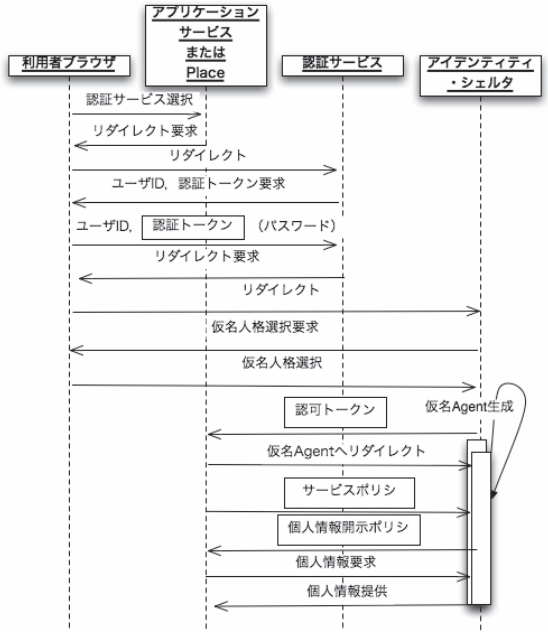

図 8　アイデンティティ・シェルタへのログインシーケンス
Fig. 8　Login sequence for Identity Shelter.

ティティ・シェルタからアプリケーションサービスや Place に対して認可トークンを発行すると同時に仮名 Agent を生成する．

(3)　アイデンティティ・シェルタは，認可が完了すると，利用者のブラウザにリダイレクトする代わりに生成した仮名 Agent に接続先をリダイレクトする．

(4)　アプリケーションサービスや Place は，仮名 Agent に対して，それが要求するサービスポリシを提示する．その中には，個人情報開示の最低条件などが含まれる．

(5)　仮名 Agent がサービスポリシに合意した場合，自分の個人情報開示ポリシをアプリケーションサービスや Place に返す．

(6)　自律的に動作する仮名 Agent は，利用者本人の代理として，アプリケーションサービスや Place からの個人情報の要求に応えて個人情報を提供するサーバとして機能する．

4.3.2　Place Agent モデルの実装方法

Place Agent モデルにおける Agent の実体は個人情報を提供するサーバ群である．また，Place は，複数の Agent 群が協調動作しながらメッセージの交換を行う環境を実現するサービスである．したがって，多数の Agent 群が参加する Place の実装方法として，並列分散処理におけるメッセージ交換システムを利用することが自然である．

我々は，このような機能を実現する手段として，Carriero らが 1980 年代に開発した Linda [19] を採用した．正確には，Linda の Ruby 言語による実装である Rinda を利用している．Rinda では，タプルスペースと呼ばれるプロセス間メッセージ交換の場と write，take（Linda では in，out）などの単純なメッセージ操作によって実現されている．また，メッセージは，タプルと呼ばれる変数を含まない配列である．タプルの例は次のようなものである．我々の Agent 間コミュニケーションの実装では，Agent の型，コントローラ，アクション，パラメータのリストを意味する 4 要素からなるタプルを Place へのメッセージの基本構造としている．ただし，ここでパラメータのリストは，URL の形式でエンコードされた 1 つの文字列とする．

```
tuple = [{type}, {controller}, {action}, {params}]
```

4.3.3　仮名 Agent および仮名テンプレートの実装方法

アイデンティティ・シェルタの仮名 Agent は，個人情報をアプリケーションサービスに提供するサーバとして機能する．提供する個人情報の構造や API を定義するのが仮名テンプレートである．

アイデンティティ・シェルタは，新しいアプリケーションサービスと連携を開始するときに，仮名テンプレートを要求する．アイデンティティ・シェルタのアプリケーションサービスへのインタフェースとなる仮名 Agent は，この仮名テンプレートから生成される．

現在の仮名テンプレートの個人属性は，OpenID の AX の仕様を利用して名前空間や構造を定義している．以下に，仮名テンプレートから生成された仮名 Agent の構造の例を示す．

Agent 型：`openid.ax.type.agent=passenger`
仮名：`openid.ax.value.psudo_identity=4423`
緯度：`openid.ax.value.location.lat=32.1234`
経度：`openid.ax.value.location.lng=135.1234`
目的地：`openid.ax.value.destination=kahogekijo`
到着時刻：`openid.ax.value.time_of_arrival=14:00`

上記の例は，「乗客」型の Agent が持つ属性として，仮名，緯度，経度，目的地，到着時

刻を持つケースを OpneID の AX で記述したものである．

仮名 Agent は，Ruby on Rails のフレームワークを利用して実装している．Ruby on Rails は，MVC フレームワークで構成されており，メッセージは “ホスト名/コントローラ名/アクション名/パラメータ” という URI の構造にそってコントローラの処理にルーティングされる．

前述したように，タプルスペースとしての Place に対するメッセージのタプルも同じ構造になっているので，Place に流されたメッセージにコミットした仮名 Agent は，受け取ったタプル形式のメッセージを URI に変換するだけでコントローラやアクションを判別して自然に処理を行うことができる．

また，仮名テンプレートは，Ruby on Rails の枠組みにそって仮名 Agent のモデルおよび本人 Agent のモデルになり，データベーススキーマとして既存の本人 Agent のデータベースのスキーマに追加される．

4.4　Place Agent モデルによる地域交通支援システムの構成

地域交通支援システムを次のような方針で Place Agent モデルに基づいて構成した．

(1)　あいのりコミュニティ，交通事業者のコミュニティを 1 つの Place とする．
(2)　これらの Place の情報を集約し相互に連絡するするために集約 Agent という中継用 Agent を作成した．
(3)　集約 Agent どうしが相互にコミュニケーションを行う集約 Place を設け，2 階層 Place の構造とした．

図 9 は，地域交通支援システムを Place Agent モデルで構成した例である．

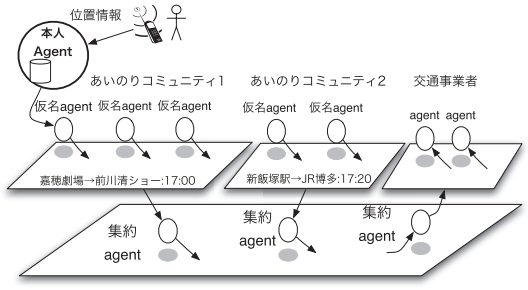

図 9　Place Agent モデルに基づいた地域交通支援システム
Fig. 9　The local traffic support system over the Place and agent model.

4.5　集約 Agent による個人情報の流通制御

Place は，個人情報の流通範囲を限定する．しかし集約 Agent を経由してルーティングすることによって，個人情報は別の Place に伝播させる．したがって，集約 Agent は，個人情報の流通を制御する要となる．

集約 Agent による個人情報の流通制御は次の 2 種類のものがある．

(1)　個人情報の流通ポリシに基づくルーティング
(2)　統計化や抽象化に基づく非個人情報への変換

個人情報の流通ポリシに基づくルーティングは，個人情報の一部を一定の事前に合意されたルールのもとで別の Place に流すことである．

統計化や抽象化に基づく非個人情報への変換とは，個人を特定可能な情報から，Place に参加するエージェント群の統計的なデータなどへの変換によって個人と特定不可能なデータへ変換したうえで他の Place に情報を流すことである．

5.　地域交通支援システムの適合性検証

提案した地域交通支援システムがロケーションプライバシのフレームワークになっていることを，Geopriv（RFC3603）のロケーションプライバシモデルとの整合性の観点と，Langheinrich のユビキタスプライバシの 6 原則との整合性の観点から検証する．

5.1　地域交通支援システムの GeoPriv モデルによる位置情報の流通

GeoPriv のモデルは，**図 10** に示すような対応によって我々の提案システムに対応づけることができる．

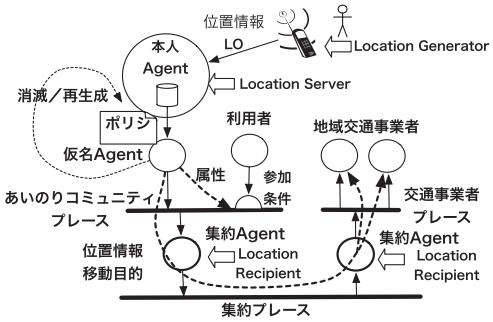

図 10　Place 間の位置情報の流通
Fig. 10　Private message object exchange.

LG（Location Generator） GPS 携帯による位置情報収集端末

LS（Location Server） 本人 Agent と仮名 Agent

LR（情報開示の相手） 同じあいのりコミュニティPlace 参加者および地域交通事業者 Place 参加者

利用者中心のルール適用 仮名 Agent に対して利用者本人が設定する個人情報開示ポリシ．また，Place やアプリケーションサービスが提示するサービスポリシに対する仮名 Agent による合意もこれに含まれる．

以上の対応付けにより，実アイデンティティと LO の分離や利用者中心のルール運用を含めて我々のモデルと整合することが分かる．

5.2 Langheinrich のユビキタスプライバシの 6 原則との整合性

提案したフレームワークは，ユビキタスプライバシの 6 原則と次のように整合する．

通知の原則 Place やアプリケーションサービスにログインするときに，Place やアプリケーションサービスのサービスポリシを通知し仮名 Agent が合意したときのみコミュニティに参加する．

同意の原則 仮名 Agent に対する本人の個人情報開示ポリシの登録がこれにあたる．ひとたび設定されると，仮名 Agent が本人に代わって自動的に同意を行うことがある．

匿名と仮名の原則 仮名については仮名 Agent によって実現されている．匿名性については，Place を用いた匿名コミュニケーション．集約 Agent を用いた個人情報の非個人情報化変換などがあげられる．

局所化の原則 仮名 Agent の消滅によるセッションの強制終了．

セキュリティの原則 アイデンティティ・シェルタおよび集約 Agent と集約 Place は信頼できる組織が安全に管理する．

請求権の原則 集約 Agent は Place が消滅するまでその Place で発生した個人情報に対して誰がいつアクセスしたかというアクセス履歴を管理する．

以上のように，提案モデルがすべての原則を充足可能であることが分かる．

6. 実 証 実 験

内閣府都市再生モデル事業の一環として，飯塚市のコミュニティバスの利用実態を測定するために，本システムのプロトタイプによる実験調査を行った[21]．

この実験の目的は，飯塚市における交通需要の測定である．この目的のために，まず飯塚市民 2,000 世帯を対象にアンケート調査を行った．また，主要地点 50 カ所の施設に対して実地調査を行い利用者数など，交通需要の基礎データも収集した．

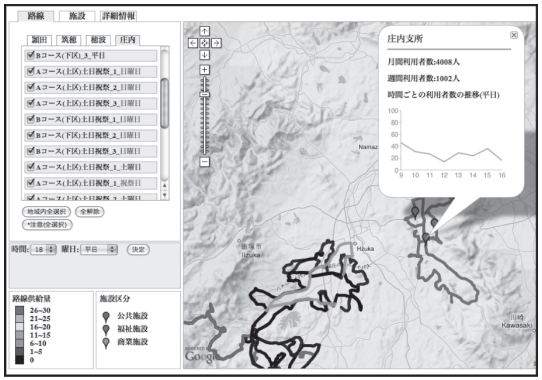

図 11 コミュニティバスの経路と主要地点の交通需要
Fig. 11 Routes of community bus and demand of traffic for principal points.

6.1 コミュニティバスの運行実態の調査

我々が提案する地域交通支援システムは，デマンド交通を対象にすることによる個人の位置情報や目的地の情報の取得が大きな特長になっている．しかし，今回の実験では，実際の利用者の参加によるデマンド交通の実験は実現できなかった．

しかし，これに代わるものとして，地域交通支援システムのプロトタイプを用いて，飯塚市全域のコミュニティバスの運行実態調査に用いた．実験の実施は，市民ではなく実験補助員が乗客の代理として携帯電話の GPS で取得した位置情報を発信するシステムを操作した．実施対象は，飯塚市を走るコミュニティバス全路線である．

市民が実際に予約端末を操作する実験ではないが，コミュニティバスという 1 つの交通手段に関するすべての利用者の位置情報を収集したという意味では，都市の規模を持つ公的な個人情報の収集と活用を行うシステムであるといえる．

図 11 は，現在の飯塚市のコミュニティバスの路線と時刻表の一部である．実験に使用した GPS 携帯電話と調査端末を**図 12** に示す．

6.2 コミュニティバス Place を用いた個人情報収集の匿名化

図 13 は，実際にコミュニティバスを利用した利用者の行動履歴を携帯電話の GPS 機能を使って収集した結果である．図 13 の中で太い線は，乗車人数が多い区間を表し，細い線は乗車人数が少ない区間を表している．

図 12　GPS 携帯携帯と調査端末
Fig. 12　Cellphone with GPS and the terminal for investigation.

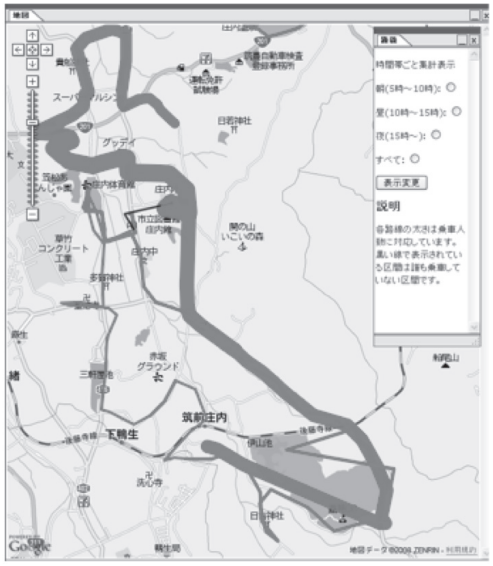

図 13　コミュニティバス乗客の行動履歴
Fig. 13　Trace of passengers of community bus.

この例では，それぞれのコースを走るコミュニティバスが Place になり，乗車中の乗客が Agent になる．乗客の Agent は乗車の時点で自動的にコミュニティバス Place に参加し，あいのりコミュニティを形成する．あいのりコミュニティに参加した利用者は，携帯電話の GPS 機能によって 10 秒ごとにの自分の位置情報をあいのりコミュニティの Place に伝える．

しかし位置情報は，同じコミュニティバス Place 内にそれぞれ仮名で伝えられるので，同じ Place に属する他の Agent からも，それが誰から送信されたメッセージなのか直接的には分からないという弱い匿名化が実現される．またコミュニティバス Place に参加していない外部の Agent からは Place 内の情報は隠蔽される．

6.3　集約 Agent による個人情報の非個人情報化

集約 Agent は，個人情報を非個人情報化変換する役割を持っている．あいのりコミュニティ Place の集約 Agent は，収集した個人の位置情報をその時点のその場所における乗客数という個人を特定しにくい情報に変換した後に交通事業者 Place にルーティングするが，これが集約 Agent による個人情報の非個人情報化にあたる．

7. ま と め

個人情報の安全な有効活用を目的とする統合的個人情報管理システムである「アイデンティティ・シェルタ」と，これを利用するシステムの例として地域交通支援システムを提案した．また，このシステムの検討の中で位置情報プライバシフレームワークについて検討と実現方法の提案を行った．

アイデンティティ・シェルタの主な特長は，(1) アプリケーション中立的な認証認可機構，(2) 仮名認証によるアイデンティティの隠蔽，(3) 利用者中心型の個人情報管理，(4) Place Agent モデルによる匿名化通信，(5) Place Agent モデルによる個人情報流通範囲の限定とアクセス記録の保持の 5 点である．

また，我々が提案する地域交通支援システムの特長は，(1) 2 階層の Place による個人情報の流通範囲のコントロール，(2) 集約 Agent による収集した個人情報の非個人情報化変換の 2 点である．

提案システムのプロトタイプを使った飯塚市の地域交通実態調査における実証実験を通じて，コミュニティバスの乗客などの多数の個人の位置情報を自動的に統計量などの非個人情報化変換を行うことにより一定の実用性を持つ安全な個人情報収集手段として利用可能なことを示すことができた．

我々は，ビジネスにおいても公共的分野においても個人情報を安全に有効活用できるようにするためには統合的なプライバシ保護フレームワークが必要であると考えている．その提案の具体例であるアイデンティティ・シェルタの実用化を目指して今後も研究開発を推進したい．

謝辞　本研究は，内閣府による「地域再生モデル調査事業」の一環として実施された．飯塚市における地域交通の実験はNPO法人住学共同機構筑豊地域づくりセンターのご協力の下に実施した．

参 考 文 献

1) Gelernter, D.: Security Assertion Markup Language V2.0 (2005). http://www.aosis-open.org/communities/#documents, as of 9/1/
2) Cameron, K. and Jones, M.B.: Design Rationale behind the Identity Metasystem Architecture (Jan. 2006).
3) OpenID Foundation: OpenID Authentication 2.0 – Final. http://openid.net/specs/openid-authentication-2_0.html
4) OpenID Foundation: OpenID Attribute Exchange 1.0. http://openid.net/specs/openid-attribute-exchange-1_0.html
5) OAuth Core 1.0. http://oauth.net/core/1.0/
6) OpenID Foundation: OpenID Simple Registration Extension 1.0. http://openid.net/specs/openid-simple-registration-extension-1_0.html
7) Bagues, S.A., Zeidler, A., Valdivielso, C.F. and Matias, I.R.: User-Centric Privacy Framework for Pervasive Environments, *Ecture Notes in Computer Science*, Vol.4278 (2006).
8) 国土交通省自動車交通局旅客課：地域住民との協働による地域交通のあり方に関する懇談会 (2006).
9) MPEC研究会（編）：MPECにもとづく交通・地域政策分析，勁草書房 (2003).
10) 土井靖範：交通政策の未来戦略—まちづくりと交通権保障とで脱「クルマ社会」の実現を，文理閣 (2007).
11) 河上省吾，松井　寛：交通工学，森北出版 (2004).
12) 山崎重一郎，宮川祥子：人間関係に基づいた情報提供システムのためのプライバシ保護フレームワーク，情報処理学会マルチメディア分散協調とモーバイルシンポジウム（DICOMO2006）論文集，pp.197–200 (2006).
13) Langheinrich, M.: Privacy by design? principles of privacy-aware ubiquitous systems, *Proc. Ubicomp 2001*, Abowd, G.D., Brumitt, B. and Shafer, S. (Eds.), Vol.2201 of Lecture Notes in Computer Science, pp.273–291, Springer (2001).
14) Mulligan, D., Cuellar, J. and Morris, J.: Request for comments: 3693 geopriv requirements (2004). http://www.ietf.org/rfc/rfc3693.txt
15) Hansen, M. and Krasemann, H.: Privacy and Identity Management for Europe, PRIME White Paper (2005). http://www.prime-project.eu.org/
16) 中西健一，高汐一紀，徳田英幸：粒度の動的変更による位置匿名性についての考察，情報処理学会論文誌，Vol.46, No.9, pp.2260–2268 (2005).
17) 貴戸秀年，柳沢　豊，佐藤哲司：位置情報サービスにおけるユーザの位置追跡可能性の評価手法，第13回マルチメディア通信と分散処理ワークショップ論文集（DPSWS 2005），pp.442–446 (2005).
18) Burr, W.E., Dodson, D.F. and Polk, W.T.: NIST SP800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology (June 2004).
19) Carriero, N. and Gelernter, D.: Linda in context, *Comm. ACM*, Vol.32, No.4, pp.444–458 (1989).
20) Thomas, D. and Hansson, D.H.: *Agile Web Development with Rails*, Pragmatic Bookshelf (2005).
21) 山崎重一郎，大塚洋一，金井洋文，仙波大和，田辺健太，具志　敦，瀬上剛玄，久保勇介：多様なタイプの地域の交通資源を効率的に連携させ，高齢化の時代にも地域のすみずみまで交通弱者のない活気ある地域であるための地域交通支援情報センター実現にむけた実証的調査報告書，平成19年度都市再生プロジェクト推進調査費，国土交通省九州地方整備局 (2008).

(平成20年1月7日受付)
(平成21年1月7日採録)

推 薦 文

地方都市の地域交通を支援するための情報共有システムと利用者の位置に関するプライバシ保護フレームワークを提案している．後者には，著者が研究開発を行っているアイデンティティシェルタ（仮名認証を利用した統合的個人情報管理システム）が実用に即して有効に活用されており，興味深い．特に，実システムへのセキュリティ技術と運用方法の適用を明確に示している点，しかも，属性管理，ユーザインタフェース，利便性など，実システムとして多面的に考察がなされている点，システム考察の根底にある地域格差と年齢格差（ならびに高齢化）を（セキュリティ技術を含めた）情報技術により埋めるという観点は，多くの本学会会員に有益となると考えられることから推薦する．

（コンピュータセキュリティ研究会主査　寺田真敏）

山崎重一郎（正会員）

昭和 32 年生．昭和 57 年東京理科大学理工学部数学科卒業．平成 14 年九州大学大学院システム情報科学研究科情報工学専攻博士後期課程．博士（情報科学）．昭和 57 年富士通株式会社入社．昭和 62 年株式会社富士通研究所へ移籍．平成 11 年より 13 年まで財団法人九州システム情報技術研究所研究員として出向．Telescript 言語入門編訳．平成 15 年より近畿大学産業理工学部情報学科教授．社会情報基盤，電子認証，電子マネー，プライバシ保護技術．