Socio-familiar Personalized Service の提案とその応用 ——次世代ユビキタスサービスを実現するネットワークソフトウェアへ向けて——

橋本　和夫[†]　北形　元[††,†]　高橋　秀幸[††]　武田　敦志[†††]
チャクラボルティ　デバシシュ[††]　白鳥　則郎[††,†]

Socio-familiar Personalized Service and Its Application ——Towards a New Network Software for Next Generation Ubiquitous Service——

Kazuo HASHIMOTO[†], Gen KITAGATA[††,†], Hideyuki TAKAHASHI[††], Atushi TAKEDA[†††], Debasish CHAKRABORTY[††], and Norio SHIRATORI[††,†]

あらまし　現在の日本社会は，少子化による労働人口の減少と，高齢化による公的・社会的サービスへのニーズ増加という社会問題に直面しており，将来のユビキタス社会においてはこれらの問題解決の手法として，高齢者介護や働く女性の支援など，社会インフラとしての公的・社会的サービスを，よりきめ細やかにかつ経済的にも妥当なコストで実現する必要がある．これらの公的・社会的サービスを実現するための基盤となる将来のユビキタスサービスには，偏在性 (Pervasiveness) を重視するユビキタス性と Personalized Service の統合が求められる．そこで，本論文では，将来のユビキタスサービスの新たな概念として，社会性と人間性を明示的に導入する Socio-familiar Personalized Service (S-P サービス) を提案する．また，これを実現するための重要な要素技術となるスケーラブルな分散認証手法について述べる．

キーワード　次世代ユビキタスサービス，社会性・人間性，ネットワークソフトウェア，分散認証手法

1. まえがき

1.1 ユビキタスサービスの将来像

現在の日本社会は，少子化による労働人口の減少と，高齢化による公的・社会的サービスへのニーズ増加という社会問題に直面している．このため，高齢者介護や働く女性の支援など，社会インフラとしての公的・社会的サービスを，よりきめ細やかにかつ経済的にも妥当なコストで実現する要求は高い．

[†] 東北大学大学院情報科学研究科，仙台市
Graduate School of Information Sciences, Tohoku University, 6–3–09 Aoba, Aoba-ku, Sendai-shi, 980–8579, Japan
[††] 東北大学電気通信研究所，仙台市
Research Institute of Electrical Communication, Tohoku University, 2–1–1 Katahira, Aoba-ku, Sendai-shi, 980–8577, Japan
[†††] 東北学院大学教養学部情報科学科，仙台市
Faculty of Liberal Arts Department of Information Science, Tohoku Gakuin University, 2–1–1 Tenjinzawa, Izumi-ku, Sendai-shi, 981–3193 Japan

このような公的・社会的サービスの実現においては，以下の 3 点を考慮したサービス設計が大切である．

- いつでもどこでも必要なサービスを提供するユビキタス性
- 実現の容易さとコスト的な経済性
- 人間関係や社会規範など，利用者の社会的関係

一方，インターネット上での商用サービスでは，Amazon.com の推薦システムなどのように，利用者の嗜好を重視して個人ごとにカスタマイズを行う個人適応が広く行われるようになった．現在は，利用者個人の利用目的に合わせたサービス提供を行うことが重要視されているが，利用者の状況を考慮したサービス提供の観点からも重要だと考えられ，将来のユビキタスサービスにおいては，より広い意味での利用者の人間性に配慮した個人適応型サービス（Personalized Service）の高度化が求められるであろう．このような，より進化した Personalized Service の特徴としては，

- 人間の尊厳を守る

- システム側がサービスを押しつけない
- そっと支援する
- 心のこもったサービス

などが考えられる．

1.2 インターネットの利用形態の将来像

現在，インターネットの利用形態では，移動性 (Mobility) と偏在性 (Pervasiveness) の両側面でユビキタス化が進み，サービス提供環境のポータブル化が急速な展開を見せている．Mobile 化は，固有端末を個人がもち歩くことで，いつでもどこでもサービスにアクセスすることを保証するものであるが，Pervasive 化は固有端末への端末依存性を取り除くことに力点を置いている．

これまでのユビキタス化は，携帯電話や携帯端末など固有の端末がいつでもどこでもつながる Mobile 化の軸で進展してきた．計算機が様々な形で環境に埋め込まれる将来のユビキタス社会では，例えば，レストランにおけるメニューがタッチパネルで提供されたり，鉄道の駅の情報 KIOSK で観光情報が提供されたりするなど，Pervasive 化がよりいっそう加速され，利用端末に依存しない形で，誰でも容易に使えるサービスを提供することが重視されると考えられる．

このため，Pervasive 化の軸に沿ったユビキタス化の展開が期待され，個人情報を積極的に活用し，利用者のニーズをより高いレベルで満足させる Personalized Service を社会に偏在する様々な情報端末を利用する Pervasive サービスとして実現することが重要となる．

このようなサービスを多数の情報端末が混在するユビキタス社会においてスケーラブルに実現するためには，以下の 2 点の技術開発が必要になる．

- 個人情報をサービスシステムから独立させて提供するアーキテクチャ
- PKI (Public Key Infrastructure) のような集中的な機関やサーバを用いず，スケーラブルに公開鍵を管理可能とする新たなソフトウェア技術

1.3 次世代ユビキタスサービスの概念について

次世代のネットワークサービスの構成技術としては，以下の四つの方向で研究が進められており，移動性や偏在性を重視するサービスや Personalized Service などの統合については，個別事例ごとに検討が行われている．

- ネットワークサービスソフトウェア技術
- ネットワークソフトウェア基盤
- ネットワーク制御管理ソフトウェア技術
- 個々のソフトウェア要素技術

ネットワークサービスソフトウェア技術は，ユビキタスサービスやクラウドコンピューティング等，利用者が直接利用するネットワークサービスに関する技術である．ネットワークソフトウェア基盤，及びネットワーク制御管理ソフトウェア技術は，ネットワークサービスを支えるネットワークの拡張と高度化，及び安定運用のための技術である．また，個々のソフトウェア要素技術とは，エージェントや高信頼ソフトウェア技術等，ソフトウェア開発自体の効率化，及び高品質化を支える技術である．特に，利用者に直接関わるネットワークサービスソフトウェア技術においては，将来のユビキタスサービスの概念を一般化し，設計論として確立することが期待されている．

従来のユビキタスサービスは，移動性と偏在性を統合する技術として議論されてきたが，将来のユビキタスサービスは (1) のように特に Pervasive 性を重視し発展させたユビキタスサービスと高度な Personalized Service が統合される，と筆者らは予測する．

$$\begin{aligned}&\text{将来のユビキタスサービス}\\&\quad = \text{高度な } \mathit{PersonalizedService}\\&\qquad + \mathit{Pervasive} \text{ 性を重視し発展させた}\\&\qquad\quad \text{ユビキタスサービス}\end{aligned} \tag{1}$$

本論文では，将来のユビキタスサービスの新たな概念として，社会性と人間性を明示的に導入する Socio-familiar Personalized Service (S-P サービス) を提案する．また特に，これを実現するための重要な要素技術の一つとなるスケーラブルな分散認証手法について述べる．

以下，**2.** では，次世代ユビキタスサービスに関するネットワークソフトウェアについて，本論文で提案する Socio-familiar Personalized Service (S-P サービス) の実現に中核となる技術である，ユビキタスサービス，オーバレイネットワーク，P2P，エージェントに関する関連研究を中心に取り上げ現状について述べる．**3.** では，S-P サービスを提案し，具体的な事例を示す．**4.** ではこれを実現するための核技術の一つとなるスケーラブルな分散認証手法について述べる．**5.** では S-P サービスの具体例を示し，**6.** はまとめである．

2. ネットワークソフトウェアの現状

本章では，次世代ユビキタスサービスに関するネットワークソフトウェアの現状について述べる．次世

代ユビキタスサービスに関する主要な技術は，ネットワークサービスソフトウェア技術，ネットワークソフトウェア基盤，ネットワーク制御管理ソフトウェア技術，ネットワークシステム・サービスを構成するソフトウェア要素技術の四つである．本論文で提案するSocio-familiar Personalized Service (S-P サービス)の実現に中核となる技術であり，この四つの分類それぞれに対応する，ユビキタスサービス，オーバレイネットワーク，P2P，エージェントに関する関連研究を中心に取り上げ現状について述べる．

2.1 ユビキタスサービス

ユビキタスサービスは，携帯端末，家電機器，生体センサ，実空間に設置されたセンサなどがネットワークを介して連携し，時間や場所を意識させることなく利用者にサービスを提供する．現在，ナビゲーション [1]，家庭内や自然環境のモニタリング [2]，協調作業支援 [3]，医療・健康管理支援 [4], [5] などの生活支援，広告・情報配信や映像などのマルチメディアコンテンツ [6] など多岐にわたる分野への応用を想定した研究開発が行われている．ユビキタスサービスの実現のための主要な要素技術として，利用者の状況や嗜好を推定するための研究，人・環境をセンシングするための各種センサに関する研究が盛んである．具体的には，利用者の状況推定の例として，ウェアラブルセンサを用いて利用者の日常生活の行動を認識するための研究 [7] や加速度センサを用いたジェスチャの認識に関する研究 [8]，GPS と移動経路履歴に基づき利用者の訪問地等を予測する研究が行われている [9]．また，環境をセンシングする例として，室内のトイレや洗濯機などの水道の使用状況をモニタリングするシステムに関する研究開発がある [10].

現状のユビキタスサービスは，いつでもどこでもサービスが利用可能となりつつあるが，サービスの利用環境と利用者を事前に想定したものがほとんどである．また，高齢者や子供などを含む人間の尊厳を守りながらの思いやり（そっと心のこもった）サービスが不十分であり，その実現が強く期待されている．そこで，本論文ではこれらの問題を解決する新たな基本概念を **3.** で提案する．

2.2 オーバレイネットワーク，P2P（Peer-to-Peer）

オーバレイネットワークは，インターネットのルーチングを向上する方法として提案され様々な研究が行われている．アプリケーションレイヤマルチキャスト (ALM) では，あらかじめ ALM に参加するエンドホストのみでアプリケーションレベルのネットワークを形成し，そのネットワーク上の仮想リンクを用いてデータのやり取りを行う．ここで，ALM ツリー上を流れるデータは複数のエンドホストを経由するが，隣接エンドホスト間の通信はユニキャストで行われる [11]．また，ビデオ会議等の多対多マルチメディア通信の品質向上を目的とし，利用者端末によるマルチキャスト通信の配信木の構成法として，通信品質の偏りを段階的に軽減する，配信木の自律分散型構成法が提案されている [12].

Peer-to-peer (P2P) は，ネットワーク上の端末間を相互に接続し，データを送受信する通信方式である．代表的なソフトウェアとして，Napster や Gnutella, Skype などがあり，利用者間を直接接続したファイルや音声などのやり取りが可能である．P2P は，スケーラビリティ，対障害性，ネットワークの負荷分散，検索効率の向上，データの複製配置の面で優れた特徴をもつ．一方，P2P ネットワークでは，公開鍵暗号技術を用いたセキュアな通信を実現する際に，従来の公開鍵の分散管理手法ではスケーラビリティに問題があった．上記のスケーラビリティに関する問題を解決するために，信頼の輪と分散ハッシュテーブルを用いた公開鍵の分散認証手法が提案されている [13].

多様な個人情報と多数の機器を活用した将来的に期待される高度なサービスを提供するためには，利用者の多様な個人情報を安全・安心に，そして，スケーラブルな方法で管理しつつ，個人の特性・嗜好に合わせて「そっと」支援を行う技術が必要となる．このサービスで必要な個人情報は，利用者とサービスが直接やり取りすることが必須である．そのため，P2P ネットワークはこのようなサービスにとって主要な通信方式であり，詳細は **4.** で述べる．

2.3 エージェント

エージェントは，自律性などの新しい特性を備え，利用者や他のエージェントと知的に相互作用を行うソフトウェアである．次世代のネットワークサービスを構成する中核的ソフトウェアの要素技術として，国内外において盛んに研究が進められている [14]〜[16]．エージェントのもつ協調性，すなわち，人や他のエージェントと協調的に動作する特徴は，情報ネットワークのような分散処理システムと親和性が高く，また，エージェントの自律性は，ネットワークサービスに適応性や柔軟性を与え得る重要な要素の一つとして期待

できる．

2.4 共生コンピューティング

次世代ユビキタスサービスに向けた試みとして，人と機械の共生に関する二つの流れの取組みがある．一つは共生コンピューティングに関する取組みであり，もう一つはアンビエントコンピューティングに関するものである．

共生コンピューティングに関する取組みは，更に二つに分かれる．一つは，擬人化された情報システムが人間のパートナーとしてともに活動を行い，人間と共生する情報システムの実現を目指した研究 [17] や人や環境に対するしなやかさをもつ情報システム基盤の実現を目指した研究 [18] がある．二つ目として，筆者等は，1992 年より，人，社会，情報環境を総合的な協調系としてとらえ，これらが共生する世界（共生社会）の実現に向けた共生コンピューティングを提案し，研究開発を行ってきた．具体的には，現在のユビキタス情報環境において限界となっている，現実空間とディジタル空間との間の大きなギャップに着目し，この限界を克服するために 3 種類のソフトウェア，すなわち，(1) パーセプチャルウェア，(2) ソーシャルウェア，(3) ネットワークウェアの基本モデルとアーキテクチャ，及び要素技術の開発を行ってきた [19]〜[23]．

一方，アンビエントコンピューティングに関する取組みとしては，2001 年に開始した EU における IST プロジェクトがあり，Ambient Intelligence の実現を目指して，生活空間に埋め込まれたコンピュータが人々の生活を支援する仕組みに関する研究開発が行われてきた [24]．また，国内では平成 19 年度からアンビエント情報社会の実現に向けた基盤技術の研究が進められている [25]．

これらの取組みによって，次世代ユビキタスサービスに向けた要素技術や応用例が数多く開発されてきている．更に今後，高齢者や子供などの人間の尊厳を守り，心のこもった高度なサービスの提供が望まれている．そのため，このようなサービスのための新たな基本概念及び要素技術の研究開発が期待されている．

3. S-P サービスの提案

3.1 S-P サービスの概念

従来のユビキタスサービスは，移動性 (Mobility) と偏在性 (Pervasive) の二つの軸からなるサービスとして説明できる．移動性とは，無線通信能力を有する携帯端末により，利用者がどこにいてもサービスを利用できる性質である．また偏在性とは，あらゆる場所に設置される端末を利用し，利用者が端末を携帯せずとも，様々な場所でサービスを利用できる性質である．これら二つの軸により，利用者は「いつでも・どこでも」サービスを享受できるようになる．しかしながら，ユビキタスサービスが社会に広く浸透するには，子供や高齢者を含む社会全体を構成する人々が，これらのサービスを安全・安心に利用できることが求められる．

そこで本論文では，これまで個別に研究開発が進められてきた社会性と人間性に関する観点を，第 3 と第 4 の軸として考え，これらを発展させる．更に，これらの二つの軸を，従来のユビキタスサービスにおける移動性と偏在性に追加・統合することにより，図 1 に示すように，従来のいつでも・どこでもに加えて，人間の尊厳を守り「誰でも・いつものように」利用できるサービスとして「S-P サービス」（Socio-familiar Personalized Service）を提案する．

3.2 第 3 の軸：社会性

本論文における社会性とは，「人間関係や社会規範などの現実社会の仕組みをサービスに反映し，様々な利用者からなる協働作業のスムーズな遂行を支援する性質」である．社会性の例として，親子関係や師弟関係などの人間関係，また法律や慣習などの社会規範やルールなどがある．これらの社会性の実現例として，現実空間での社会的振舞いに関する研究 [26] や共生オフィスシステム [27] が挙げられる．例えば，現実社会では一般に，オフィスに入室できる人間はそのオフィスの在籍者のみであり，在籍者が誰も知らない第三者がオフィスに入室することは，不自然である．一方で，在籍者の友人や仕事相手であれば，その在籍者とともにオフィスに入室することは自然である．共生オフィスシステムの特徴は，このような現実社会の人間関係などの社会性を活用し，例えば，ある研究者が共同研究先に訪問した際に，訪問先の在籍者との”共同研究者である”という人間関係をシステムが把握し，プリンタやネットワーク等の訪問先のリソースに対する一時的な使用権限を，訪問者に自動的に貸与する点であり，これが，社会性を実現した例である．

3.3 第 4 の軸：人間性

本論文における人間性とは，「人間の尊厳を守り，システムがそっと手助けをする，心のこもった性質」である．

これまで，ヒューマンセンタードなど，人間中心の考え方や利便性の向上を目的とし，人々の生活を便利

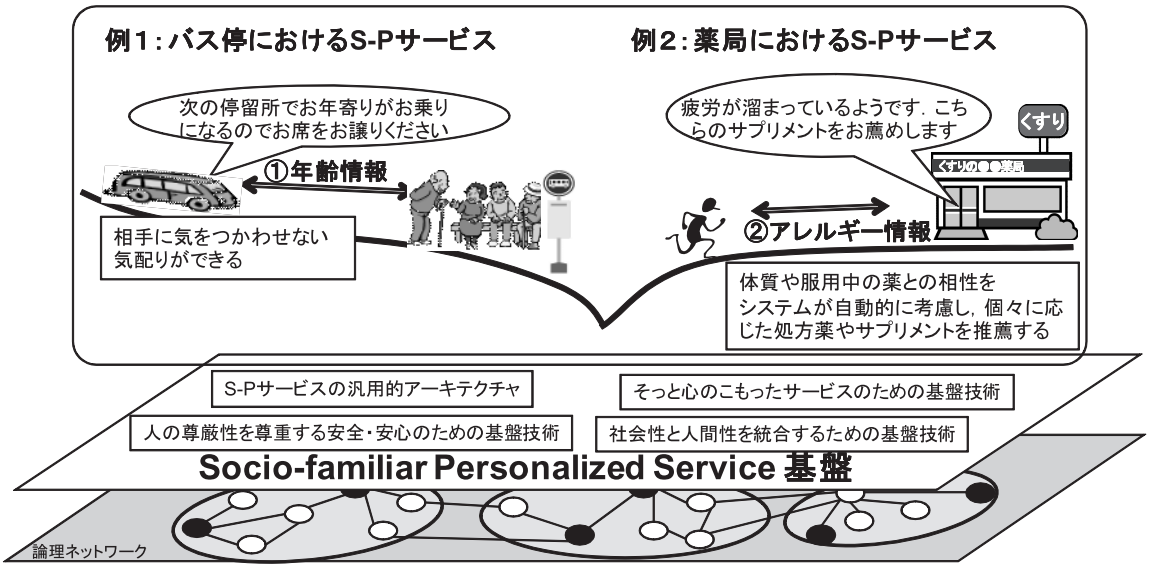

図 1　S-P サービスを実現するための基盤技術と応用
Fig. 1　Fundamental technologies and applications of Socio-familiar Personalized Service.

にする様々なサービスが提案されているが，人の尊厳やプライバシーを守るという観点からの検討が，十分ではなかった．

例えば，高齢化社会で広く関心の高いユビキタスサービスの応用事例として，高齢者が自宅で危険な状態にないか等，遠隔地から見守るシステムが挙げられる．このような従来の見守りシステムにおいては，見守られる対象である高齢者の状態によらず，常時 24 時間，映像による見守りを行い，例えば，着替え中や入浴中など，人間の尊厳性やプライバシーの保護に関して配慮が不十分である場合が多い．

人間性を積極的に考慮した具体例として，高齢者見守りシステムが挙げられる [5]．本システムは，高齢者の人間性を尊重するため，高齢者の状態や緊急度，及び見守る側との関係を考慮し，必要最小限の情報のみを伝達する機能を実現している．

3.4　第 3 の軸と第 4 の軸の統合

上述の第 3 と第 4 の軸に関する具体例においては，個人情報，すなわち，訪問者と在籍者の間の人間関係や，見守られる側の人間に対する見守る側の人間の立場などの人間関係を活用し，社会性や人間性を反映したサービスをそれぞれ実現している．しかしながら，次世代ユビキタスサービスとして，利用端末に依存しない形で誰でも容易に使えるサービスの提供を実現するには，これら第 3 と第 4 の軸を，従来のユビキタスサービスに追加・統合することが必要となる．そのためには，これまでサービスごとに個別に管理・利用されてきた利用者の個人情報を，しかるべき認証の手続きを経て，様々なサービスから共通して利用可能とするアーキテクチャの確立が不可欠となる．加えて，偏在する多数の情報端末において，様々な利用者の個人情報を安全に送受するためには，PKI のような集中的な機関やサーバを用いずに，スケーラブルに公開鍵を管理可能とする新たな分散型の認証技術が必要となる．

3.5　S-P サービスの定義と具体例

S-P サービスとは，「子供や高齢者を含む社会を構成する様々な人々が，いつでも・どこでもに加えて，誰でも・いつものように，その恩恵を意識せずに享受し，人の尊厳を守り，人がより人らしく活動できるようなそっと心のこもった思いやりサービス」である．

S-P サービスの具体例として，下記のようなサービスが挙げられる．

- レストランにおいて客が注文する際に，客のアレルギーや高血圧など，公開するのが躊躇されるような，しかしながらメニューの選択に不可欠な個人情報が，レストランに設置された情報端末からメニューシステムに伝達され，利用客の特性に即した安全・安心な心のこもったメニューを提示する．

- 同様に，薬局で薬を購入する際に，既に服用している他の薬と併飲してもよい薬だけを，そっと勧めてくれる．
- 同様に，バス停で高齢者が待っているという情報が，バス停に設置された情報端末から到着予定のバスにあらかじめ伝えられ，席を自動的に確保する．
- 同様に，タクシーに乗って「自宅まで」と伝えるだけで，自宅の住所が運転手に通知され，いつものように帰宅できる．
- 同様に，コンビニエンスストア等で宅配便を発送する際,「おばあちゃんの家まで」というだけで，いつものように，祖母の住所がコンビニエンスストアのレジに自動入力される．
- 同様に，駅のキオスクで「たばこを下さい」と注文するだけで，いつもの銘柄を購入できる．

これらの例に共通する特徴は，利用者の明示的な指示がなくとも，その人のもつ特性を反映したサービスが自然に提供されること，すなわち，初めて利用する場所でも，あたかもいつも利用しているように個人化されたサービスが提供される点である．

3.6 S-P サービスの実現に向けて

S-P サービスを実現するには，図 1 に示す，次の四つの基盤技術を確立する必要がある．

（1） S-P サービスの汎用的アーキテクチャ

（2） そっと心のこもったサービスのための基盤技術

（3） 人の尊厳性を尊重する安全・安心のための基盤技術

（4） 移動性・偏在性に社会性・人間性を統合するための基盤技術

特に，上述の（4）移動性・偏在性に社会性・人間性を統合するための基盤技術は，第 3 と第 4 の軸を統合して従来のユビキタスサービスの限界を越え，S-P サービスを実現するための根幹となる技術である．

移動性・偏在性に社会性・人間性を統合するためには，社会性・人間性の実現に不可欠な利用者の個人情報を，いつでも・どこでも，システムがアドホックに把握する技術の実現が不可欠である．これまで，利用者の個人情報は主に秘匿し保護する点に重点が置かれてきた．ここで，移動性・偏在性を有するユビキタスサービスにおいて，サービスの個人化に必要な最小限の個人情報のみを，サービスの利用者と提供者の間で安全・安心に交換することができれば，プライバシー情報を積極的に活用したサービス，すなわち S-P サービスの実現が期待できる．

これまで我々は，以上に述べた S-P サービスの実現のための根幹となる課題を解決するため，偏在する極めて多数の機器を利用した，安全かつスケーラブルな通信手段の開発を推進してきた．次の **4.** において，その基礎となる分散認証手法について概説する．

4. スケーラブルな分散認証手法

4.1 S-P サービスに向けた分散認証手法

S-P サービスでは，偏在する極めて多数の端末で利用者のプライバシー情報を扱うため，プライバシー情報を安全に送受信するためのスケーラブルな分散認証手法が必須となる．クライアント・サーバモデルで構成される従来のコンピュータネットワークでは，Public Key Infrastructure (PKI) によって安全な通信路を確保していた．PKI では，少数の認証局がすべてのサーバに対して公開鍵証明書を発行し，これらの公開鍵証明書に記述された公開鍵を利用して暗号通信を行うことにより，クライアント・サーバ間の安全な通信を実現する．一方，S-P サービスを提供するためのコンピュータネットワークでは，携帯端末やセンサ端末などの端末が直接通信を行うため，これらのすべての端末に対して公開鍵証明書を発行しなければならない．しかし，PKI では少数の認証局がすべての公開鍵証明書を管理しているため，S-P サービスで使用するすべての端末に対して公開鍵証明書を発行することは難しい．すなわち，S-P サービスを実現するためには，新たにスケーラブルな分散認証手法を開発することが必須となる．

すべての端末が直接通信を行うスケーラブルなネットワークとして，様々な構造型オーバレイネットワークが提案されている [28]〜[31]．これらの構造型オーバレイネットワークは，それぞれの端末がデータを効率的に分散管理するため，スケーラビリティや耐故障性に優れている．しかし，従来のオーバレイネットワークはファイルデータや動画データの分散管理を目的としているため，各端末間の通信の安全性については考慮されていない．そこで，我々は，構造型オーバレイネットワーク上の各端末が相互に認証することにより，各端末間の安全で確実な通信を可能とするスケーラブルな分散認証手法：Hash-based Distributed Authentication Method (HDAM) を提案してきた [13]．本論文では，HDAM を発展させた方式として，構造型オーバレイネットワーク上での相互認証に冗長性をもた

せることにより，より安全な端末間通信を実現するスケーラブルな分散認証手法：Hash-based Distributed Public Key Infrastructure (HDPKI) を提案する．

HDPKI は，分散ハッシュテーブルの概念を利用することにより，スケーラブルな分散認証を実現する手法である．HDPKI では，Chord [28] と同様のリング状の構造型オーバレイネットワークを構成し，このオーバレイネットワークで公開鍵証明書を分散管理をすることにより，各端末間の確実で安全な通信を実現する．従来の分散ハッシュテーブルでも公開鍵証明書を分散管理することは可能である．しかし，従来手法は悪意のある端末や不正動作を行う端末からの攻撃に対する防御メカニズムをもたないため，公開鍵証明書を安全に管理することができない．一方，HDPKI では，以下の攻撃に対する防御メカニズムを導入することにより，公開鍵証明書の安全な分散管理を実現している．

（1） HDPKI で端末間で送受信されるすべてのメッセージに対して，公開鍵暗号による暗号化と署名を行う．これにより，HDPKI に参加していない端末からの攻撃があったとしても，正しい公開鍵証明書の取得が可能となる．

（2） HDPKI では，1 個の公開鍵証明書を複数の端末で管理する．また，1 個の公開鍵証明書を取得するために複数の通信経路を利用する．これにより，HDPKI に不正動作する端末が参加していたとしでも，正しい公開鍵証明書の取得が可能となる．

本章では，分散認証手法 HDPKI の仕組みとスケーラビリティについて述べる．

4.2 HDPKI の仕組み

図 2 に，HDPKI における公開鍵証明書の分散管理の例を示す．ここで，A，B，M，P_n，S_n は端末を示し，C_k は端末 k の公開鍵証明書を示す．HDPKI では，それぞれの端末識別子から一方向ハッシュ関数で求めたハッシュ値に基づいて，1 から N までの指標を円形に配置したリング状の仮想ネットワークを構成する．ここで，N はハッシュ値の最大値であり，通常は 2^{128} などの大きな値となる．そして，各端末は自身の位置から正の方向に隣接している r 個の端末と負の方向に隣接している r 個の端末の公開鍵証明書を管理する．ここで，r は HDPKI の冗長度であり，HDPKI では 1 個の端末の公開鍵証明書を $2r$ 個の端末が分散管理する．図 2 の場合，端末 A は正の方向に隣接している 3 個の端末 S_{A1}，S_{A2}，S_{A3} の公開鍵証明書を管理している．また，端末 S_{A1}，S_{A2}，S_{A3} は負の方向に位置しており距離が 3 以内の端末である端末 A の公開鍵証明書を管理している．

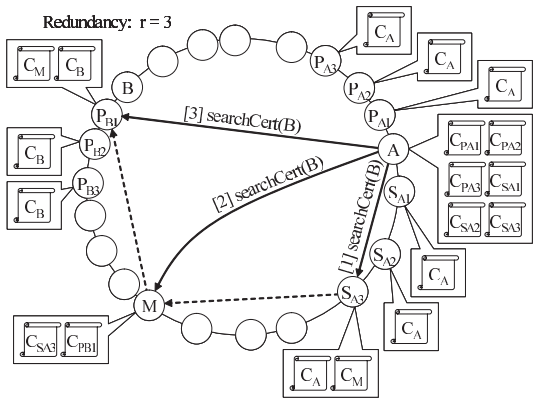

図 2 公開鍵証明書の分散管理
Fig. 2 Distributed management of public key certificates.

HDPKI において公開鍵証明書を検索する場合，公開鍵暗号を用いた安全な通信が可能な端末を介して新たな公開鍵証明書を取得する動作を繰り返すことにより，任意の公開鍵証明書を取得する．図 2 において，端末 A が端末 B の公開鍵証明書を検索するための手順は以下のとおりである．

（1） 端末 A は，端末 A と端末 B の間に存在する端末の中で公開鍵暗号を用いたセキュアな通信が可能な端末 S_{A3} に対して，端末 B の公開鍵証明書 C_B を要求する．

（2） 端末 S_{A3} は端末 B の公開鍵証明書 C_B を管理していないので，端末 S_{A3} と端末 B の間にある端末 M を端末 A に紹介する．このとき，端末 S_{A3} は端末 M の公開鍵証明書を端末 A に送信し，端末 A の公開鍵証明書を端末 M に送信する．これにより，端末 A と端末 M は公開鍵暗号を用いた安全な通信が可能となる．

（3） 端末 A は端末 M に端末 B の公開鍵証明書 C_B を要求する．端末 M は公開鍵証明書 C_B を管理していないため，端末 M と端末 B の間にある端末 P_{B1} を端末 A に紹介する．このとき，端末 M は端末 P_{B1} の公開鍵証明書を端末 A に送信し，端末 A の公開鍵証明書を端末 P_{B1} に送信する．

（4） 端末 A は端末 P_{B1} より公開鍵証明書 C_B を取得する．

このとき，すべての送受信メッセージに対して公開鍵

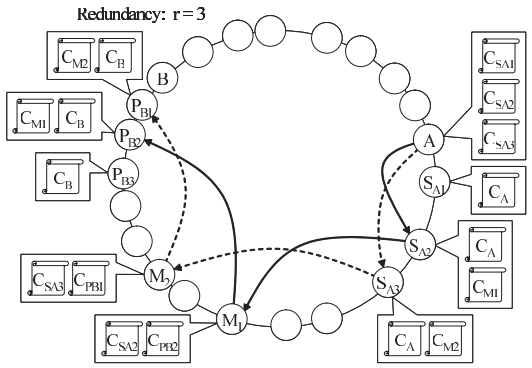

図 3　複数の経路を経由した公開鍵証明書の検索
Fig. 3　Multi-path for searching a public key certificate.

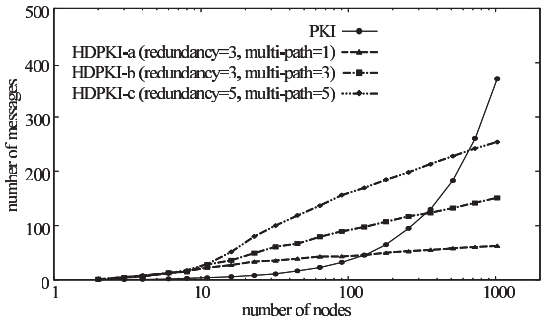

図 4　公開鍵証明書の管理に必要な通信データ量
Fig. 4　Communicatino overhead for managing public key certificates.

暗号による暗号化と署名が行われる．また，メッセージを受信した端末は必ず電子署名の検証を行う．そのため，HDPKI に参加していない端末による攻撃があったとしても，上記手順により正しい公開鍵証明書を取得することができる．

HDPKI では，複数の端末を経由して公開鍵証明書を検索するため，公開鍵証明書検索の経路上の端末の中に不正動作を行う攻撃者が含まれている場合は正しい公開鍵証明書を取得できない可能性がある．そこで，HDPKI では複数の経路を経由して 1 個の公開鍵証明書を検索する仕組みを導入している．図 3 に，複数の経路を使用した 1 個の公開鍵証明書の検索の例を示す．この例では，端末 A が，端末 M_1 を経由する経路と端末 M_2 を経由する経路を使用して公開鍵証明書 C_B を取得している．そのため，端末 M_1 が不正な動作をする攻撃端末であるとしても，端末 M_2 を経由する経路から正しい公開鍵証明書 C_B を取得可能である．複数経路を経由して 1 個の公開鍵証明書を検索する仕組みにより，HDPKI に不正動作をする端末が参加していたとしても正しい公開鍵証明書の取得が可能となる．ただし，HDPKI に参加している端末の多くが不正動作を行う攻撃者の端末である場合，正しい公開鍵証明書を取得することは難しい．そのため，HDPKI を運用するためには，Sybil Attack のような多数ノードによる攻撃を防ぐための運用上の仕組みが必要である．

4.3　HDPKI のスケーラビリティ

HDPKI では，Chord と同様に，リング状の仮想ネットワーク上に配置された各端末が Finger Table を作成し，Finger Table に登録された端末の公開鍵証明書を保持する．これにより，公開鍵証明書を検索するための経路のホップ数は $O(\log n)$（n は端末数）となり，公開鍵証明書の検索・端末の参加・端末の離脱のために各端末が送受信する通信データ量は $O(\log n)$ となる．図 4 に HDPKI で公開鍵証明書を管理するために各端末が送受信する通信データ量を示す．また，比較対象として，1 個の認証局が公開鍵証明書を発行する PKI において認証局が送受信する通信データ量を同時に示す．ここで，公開鍵証明書の管理に必要な通信データ量とは，公開鍵証明書の検索・端末の参加・端末の離脱に必要な通信データ量の合計である．PKI では公開鍵証明書を検索する必要はないが，HDPKI では公開鍵証明書を検索するために端末間で通信する必要がある．HDPKI で公開鍵証明書を検索するときに各端末で送受信される通信データ量は $O(\log n)$ となる．一方，PKI では端末の参加・端末の離脱のときの通信データが認証局に集中するが，HDPKI では端末の参加・端末の離脱のときの通信データは各端末に分散される．PKI で端末の参加・端末の離脱のときに認証局で送受信される通信データ量は $O(n)$ であるのに対し，HDPKI で公開鍵証明書の端末の参加・端末の離脱のときに各端末で送受信される通信データ量は $O(\log n)$ である．そのため，参加端末数が十分に多い場合，HDPKI が公開鍵証明書の管理のための各端末で送受信される通信データ量は PKI の認証局が送受信する通信データ量より少ない．以上より，従来手法である PKI と比べて，HDPKI はスケーラブルな分散認証手法であるといえる．

5.　S-P サービスの具体例

前述の分散認証手法を用いることで，個人情報を有効に活用したサービスを実現できる．ここでは例とし

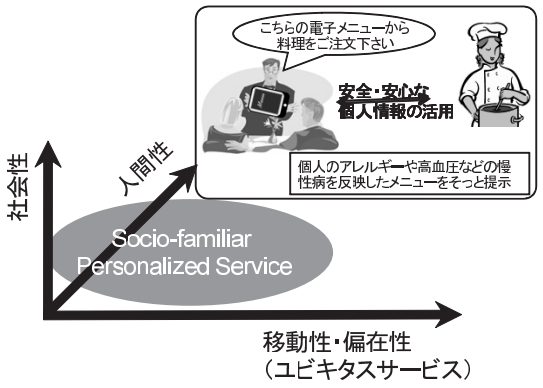

図 5　S-P サービスの概念と具体例
Fig. 5　Concept and examples of Socio-familiar Personalized Service.

て，図 5 に示すように，ボブが取引先のアリスをレストランのディナーに招待しメニューを選択するシーンを想定し，席への案内とメニューの推薦において，個人情報に配慮した S-P サービスの具体例を述べる．

まず，ボブとアリスには，それぞれ公に知られたくない，下記のような条件がある．

- ボブは高血圧であり，塩分の少ないメニューが好ましい．
- ボブが服用している血圧降下剤は，グレープフルーツと相性が悪い．
- アリスの昼食はパスタだったので，パスタ以外のものが食べたい．
- アリスは卵アレルギーであり，卵を摂取できない．
- ボブは，使用可能な接待費の範囲内で，できるだけ豪華なメニューを選びたい．

実際にボブとアリスがレストランに入ると，まず，喫煙の有無等，2 人の個人情報が，前述の分散認証手法を用いて，安全・安心にレストラン側のシステムに送信され，ボブとアリスがレストランのウェイターに口頭で明示的に伝えることなく,「そっと」禁煙席に案内される．続いて 2 人が座席に着くと，単に嗜好だけではなく，上述のような互いに公にしたくないが，メニュー選択に必要な条件を，口頭で伝えることなくシステムが自動的に考慮し,「人間の尊厳を守り」お薦めメニューを選択・提示する．

すなわち，従来の協調フィルタリングや利用履歴に基づく推薦システムでは実現が難しかった，アレルギーや健康状態など，個人情報を積極的に活用したきめ細かい条件を配慮した「心のこもった」メニュー推薦を可能とする．

6. むすび

将来のユビキタスサービスが，偏在性 (Pervasiveness) を重視するユビキタス性と高度な Personalized Service の統合によって構成されることが期待される．本論文では，そのサービスの実現へ向けた新たな概念として，社会性と人間性を明示的に導入する Socio-familiar Personalized Service (S-P サービス) を提案し，その具体例を示した．

S-P サービスを実現するには，次の四つの基盤技術を確立する必要がある．(1) S-P サービスの汎用的アーキテクチャ．(2) そっと心のこもったサービスのための基盤技術．(3) 人の尊厳性を尊重する安全・安心のための基盤技術．(4) 移動性・偏在性に社会性・人間性を統合するための基盤技術．本論文では，主に (4) について議論した．今後の課題として，(1)〜(3) の研究開発が残されている．

謝辞　本研究の一部は，情報通信研究機構 (NICT) の委託研究「ダイナミックネットワーク技術の研究開発」の助成を受けて実施したものである．

文　献

[1] M. Arikawa, S, Konomi, and K. Ohnishi, “Navitime: Supporting pedestrian navigation in the real world,” IEEE Pervasive Computing, vol.6, no.3, pp.21–29, July-Sept. 2007.
[2] H. Esaki and H. Sunahara, “Live E! project; Sensing the earth with Internet weather stations,” The 2007 International Symposium on Applications and the Internet (SAINT2007), Jan. 2007.
[3] D.C. McFarlane and S.M. Wilder, “Interactive dirt: Increasing mobile work performance with a wearable projector-camera system,” Proc. 11th international conference on Ubiquitous computing (UbiComp2009), pp.205–214, Sept.-Oct. 2009.
[4] J.H. Kim, R. Haw, E.J. Cho, C.S. Hong, and J. Choe, “Design and implementation of NEMO based ZigBee mobile router for healthcare system,” Proc. 10th Annual International Symposium on Applications and the Internet (SAINT2010), pp.77–83, July 2010.
[5] S. Izumi, K. Yamanaka, Y. Tokairin, H. Takahashi, T. Suganuma, and N. Shiratori, “Ubiquitous supervisory system based on social contexts using ontology,” Mobile Information Systems (MIS), vol.5, no.2, pp.141–163, 2009.
[6] S. Imai, A. Takeda, T. Suganuma, and N. Shiratori, “Effective ubiquitous service provisioning based on knowledge circulation framework,” Int. J. Business

Intelligence and Data Mining, vol.4, no.1, pp.78–98, May 2009.

[7] T. Maekawa, Y. Yanagisawa, Y. Kishino, K. Ishiguro, K. Kamei, Y. Sakurai, and T. Okadome, “Object-based activity recognition with heterogeneous sensors on wrist,” Proc. 8th International Conference on Pervasive Computing (Pervasive 2010), LNCS 6030, pp.246–264, May 2010.

[8] J. Liu, Z. Wang, L. Zhong, J. Wickramasuriya, and V. Vasudevan, “uWave: Accelerometer-based personalized gesture recognition and its applications,” Proc. 7th IEEE International Conference on Pervasive Computing and Communications (PerCom 2009), pp.1–9, March 2009.

[9] C. Zhou, D. Frankowski, P. Ludford, S. Shekhar, and L. Terveen, “Discovering personally meaningful places: An interactive clustering approach,” ACM Trans. Inf. Syst., vol.25, no.3, pp.1–31, July 2007.

[10] J. Froehlich, E. Larson, T. Campbell, C. Haggerty, J. Fogarty, and S.N. Patel, “HydroSense: infrastructure-mediated single-point sensing of whole-home water activity,” Proc. 11th International Conference on Ubiquitous Computing (UbiComp2009), pp.235–244, Sept.-Oct. 2009.

[11] M. Hosseini, D.T. Ahmed, S. Shirmohammadi, and N.D. Georganas, “A survey of application-layer multicast protocols,” IEEE Commun. Surveys & Tutorials, 3rd Quarter 2007, vol.9, no.3, pp.58–74, 2007.

[12] D. Chakraborty, J. Makishi, T. Osada, G. Kitagata, A. Takeda, K. Hashimoto, and N. Shiratori, “Construction of overlay application layer multicast tree for efficient multi-source multimedia communication,” Proc. 4th International Conference on Intelligent Computing and Information Systems (ICICIS 2009), March 2009.

[13] A. Takeda, D. Chakraborty, G. Kitagata, K. Hashimoto, and N. Shiratori, “Proposal and performance evaluation of hash-based authentication method for P2P networks,” J. Inf. Process., vol.17, pp.59–71, Feb. 2009.

[14] T. Uchiya, T. Maemura, H. Hara, K. Sugawara, and T. Kinoshita, “Interactive design method of agent system for symbiotic computing,” Int. J. Cognitive Informatics and Natural Intelligence, vol.3, no.1, pp.57–74, 2009.

[15] S. Abar, S. Konno, and T. Kinoshita, “Autonomous network monitoring system based on agent-mediated network information,” Int. J. Computer Science and Network Security, vol.8, no.2, pp.326–333, 2008.

[16] I. Legrand, H. Newman, R. Voicu, C. Cirstoiu, C. Grigoras, C. Dobre, A. Muraru, A. Costan, M. Dediu, and C. Stratan “MonALISA: An agent based, dynamic service system to monitor, control and optimize distributed systems,” Comput. Physi. Commun., vol.180, no.12, pp.2472–2498, 2009.

[17] 松山隆司，川嶋宏彰，鷲見和彦，“人間と共生する情報システムの実現を目指して,” 情報処理，vol.47, no.8, pp.851–858, Aug. 2006.

[18] 原　良憲，山田敬嗣，“情報システム基盤における Symbiotic Computing,” 情報処理，vol.47, no.8, pp.844–850, Aug. 2006.

[19] 白鳥則郎，“ポスト・モダン分散システム,” 2010 年マルチメディア通信と高速・知能・分散・協調コンピューティングシンポジウム論文集（情報処理学会），pp.1–7, 1994. 情報処理，vol.36, no.9, pp.811–814, Sept. 1995.

[20] S. Fujita, K. Sugawara, T. Kinoshita, and N. Shiratori, “An approach to developing human-agent symbiotic space,” Proc. 2nd Joint Conference on Knowledge-based Software, pp.11–18, 1996.

[21] 白鳥則郎，菅原研次，菅沼拓夫，藤田　茂，小出和秀，“Symbiotic Computing -ポスト・ユビキタス情報環境へ向けて,” 情報処理，vol.47, no.8, pp.811–816, Aug. 2006.

[22] T. Suganuma, K. Sugawara, and N. Shiratori, “Symbiotic computing: Concept, architecture and its applications,” Proc. 4th International Conference on Ubiquitous Intelligence and Computing (UIC2007), pp.1034–1045, July 2007.

[23] T. Suganuma, K. Sugawara, T. Kinoshita, F. Hattori, and N. Shiratori, “Concept of symbiotic computing and its agent-based application to a ubiquitous care-support service,” Int. J. Cognitive Informatics and Natural Intelligence (IJCINI), vol.3, no.1, pp.34–56, 2009.

[24] M. Vallee, F. Ramparany, and L. Vercouter, “A multi-agent system for dynamic composition in ambient intelligence environments,” Proc. 3rd International Conference on Pervasive Computing (Pervasive 2005), pp.175–182, May 2005.

[25] http://www.ist.osaka-u.ac.jp/GlobalCOE

[26] 小川悟史，ラデスク　ジョルジュ　シェルバン，魏　文鵬，北形　元，武田敦志，白鳥則郎，“現実空間での社会的振舞を活用した柔軟かつ安全なアクセス制御方式,” 信学技報，IN2007-67，Sept. 2007.

[27] G. Kitagata, D. Chakraborty, S. Ogawa, A. Takeda, K. Hashimoto, and N. Shiratori, “Visitor access control scheme utilizing social relationship in the realworld,” Trust Management IV : Proc. 4th IFIP WG 11.11 International Conference (IFIPTM2010), pp.95–107, June 2010.

[28] I. Stoica, R. Morris, D. Liben-Nowell, D.R. Karger, M.F. Kaashoek, F. Dabek, and H. Balakrishnan, “Chord: A scalable peer-to-peer lookup protocol for internet applications,” IEEE/ACM Trans. Netw., vol.11, no.1, pp.17–32, 2003.

[29] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, “A scalable content-addressable network,” Proc. ACM SIGCOMM, pp.161–172, 2001.

[30] A. Rowstron and P. Druschel, “Pastry: Scalable, decentralized object location, and routing for large-

scale peer-to-peer systems," Proc. IFIP/ACM International Conference on Distributed Systems Platforms, pp.329–350, 2001.
[31] J. Aspnes and G. Shah, "Skip graphs," ACM Trans. Algorithms, vol.3, no.4, pp.37:1–37:35, 2007.

（平成 22 年 9 月 2 日受付，11 月 9 日再受付）

橋本　和夫　（正員）

1979 東北大学大学院修士課程了．同年国際電信電話（株）入社．2006 東北大学大学院情報科学研究科教授．ネットワークセキュリティ，データマイニング，マルチメディア情報検索を統合する Web コミュニケーションの研究に従事．博士（情報科学）．1999 人工知能学会研究奨励賞，2001 本会論文賞，2002 電波功績賞，各賞受賞．情報処理学会，人工知能学会，AAAI，IEEE 各会員．

北形　　元　（正員）

2002 東北大学大学院情報科学研究科博士後期課程了．現在，東北大学電気通信研究所准教授．博士（情報科学）．エージェント指向コンピューティング，やわらかい情報システム，ネットワーク管理の研究に従事．情報処理学会，会員．

高橋　秀幸

2008 東北大学大学院情報科学研究科博士後期課程了．現在，東北大学電気通信研究所産学官連携研究員．博士（情報科学）．ユビキタスコンピューティング，エージェント指向コンピューティング，グリーン ICT の研究に従事．情報処理学会会員．

武田　敦志

2005 東北大学大学院情報科学研究科博士後期課程了．現在，東北学院大学教養学部情報科学科講師．博士（情報科学）．オーバレイネットワーク，ネットワークセキュリティの研究に従事．情報処理学会会員．

チャクラボルティ　デバシシュ

1999 東北大学大学院情報科学研究科博士後期課程了．現在，東北大学電気通信研究所客員准教授．博士（情報科学）．オーバレイネットワーク，アドホックネットワーク，ネットワーク管理の研究に従事．

白鳥　則郎　（正員：フェロー）

1977 東北大学大学院博士課程了．1990 同大工学部教授を経て 1993 同電気通信研究所教授．2010 同大客員教授・名誉教授，公立はこだて未来大学理事．博士（工学）．人と情報環境の共生などの研究に従事．文部科学大臣表彰「研究部門」，情報処理学会功績賞，本会業績賞など受賞．情報処理学会フェロー，IEEE フェロー，情報処理学会会長．