情報処理学会論文誌 Vol.53 No.7 1807–1820 (July 2012)

安心安全なユビキタス環境実現のための人にやさしいリモートアクセス方式の提案

小林 透[1,a)] 上野 正巳[2] 多田 好克[3]

受付日 2011年10月19日, 採録日 2012年4月2日

概要：IT 機器を使い慣れていない人々でも，安心，安全に外出先の環境を利用して，会社や家庭の環境にアクセス可能とする人にやさしいリモートアクセス方式を提案する．関連研究では，“安心・安全” を実現するうえで重要な利用者の認証と公共の環境におけるコンピューティング資源そのものの認証に関する問題の議論が十分でなかった．そこで，提案する方式は，利用者やコンピューティング資源に関するアクセス制御ポリシが記述された電子的な利用権を用いて，コンピューティング資源利用時の認証認可機構をベースとしたリモートアクセス機構を提供している．さらに，ロケーションを越えて資源が提供するサービスの合成を可能としている．これにより，オンデマンドで安全に外出先の環境を利用して，煩雑な手続きを要さずに会社や家庭のコンピューティング資源にリモートアクセスすることが可能となる．実験システムを用いた評価により提案する方式が達成すべき要件面，セキュリティ面，性能面において優位であることを示す．

キーワード：ユビキタスコンピューティング，アクセス制御，リモートアクセス，IC カード

A Proposal of Human-centered Remote Access Method for Realizing Ubiquitous Environment

Toru Kobayashi[1,a)] Masami Ueno[2] Yoshikatsu Tada[3]

Received: October 19, 2011, Accepted: April 2, 2012

Abstract: We propose a human-centered remote access method for realizing ubiquitous environment without anxiety. It gives users conditional on-demand access to computing resources such as computing or network devices located in open environments, e.g., Internet cafes or hotels. It also provides users combined services among computing resources in open and closed environments such as those of the office or home. In order to establish this usage environment, we introduced an electronic ticket called a “Use-right Policy” that includes policies relating to user attributes or computing-resource attributes. Using this Use-right Policy, we are aiming to realize the secure on-demand usage of local computing environment and also the secure remote access and combination of remote computing environment without needing special knowledge or complicated procedures. We describe the system configuration and its advantages in terms of user requirements, security and performance.

Keywords: ubiquitous computing, access control, remote access, smart cards

1. はじめに

近年,「新たな情報通信技術戦略」などの国家政策 [1] により政府主導で IT 技術を広く国民のインフラとすべく各種の取り組みがなされている．それにともない，BlueTooth [2] や無線 LAN などのネットワーク関連技術や Linux ボックスなどの組込み技術の普及・展開が進められている．このような状況変化により，これまで会社や家庭などの限定さ

[1] NTT サイバーソリューション研究所
NTT Cyber Solutions Laboratories, Yokosuka, Kanagawa 239–0847, Japan
[2] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, Musashino, Tokyo 180–8585, Japan
[3] 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[a)] kobayashi.toru@lab.ntt.co.jp

れた空間での利用が中心だったコンピューティング環境が駅，空港，カフェなどの公共空間へ広がりつつある．このような環境の変化により，外出先の環境をオンデマンドに利用して，会社や家庭などのホーム環境に安全にかつ簡単にアクセスしたいというニーズが高まっている．本稿では，このような広域に分散されたコンピューティング資源の利用環境をユビキタス環境と呼ぶ．

一方，近年日本をはじめとする一部の先進国では，少子高齢化という問題が台頭してきている．このような状況において，社会を活性化していくためには，専業主婦や高齢者などこれまで社会に出ていなかった人々が積極的に社会で活躍することが望まれる．このような人々が安心して社会で活躍できるようにするためには，身体的，精神的負担をかけずにふだんの生活とのつながりを維持しながら，いつでもどこでも仕事ができる環境が必要である．つまり，このような人々が仮にどこにいても，特別の IT 機器を携帯しなくても，その場の環境を利用して安心，安全に仕事ができ，家庭の様子を確認できる環境の実現が求められる．

しかし，実際には，PC などの高機能 IT 機器を携帯する必要があったり，外出先の環境を利用できたとしても，事前にサービス利用契約が必要であったりする．また，一時的な利用が可能でも，半日単位や 1 日単位などが多く，必要なときに必要なだけ利用することは難しい．無線 LAN の一時利用サービスなどはその好例である．さらに，その環境から安全に会社や家庭の環境にアクセスするには，認証のための ID，パスワードの設定や暗号通信路構築のための証明書のインストールなどが必要である．そのため，煩雑な手続きや専門的な知識が必要となり，特に IT 機器を使い慣れていない人々にとっては，大きな障害となっている．

そこで，本研究の狙いは，IT 機器を使い慣れていない人々でも，安心，安全に外出先の環境を利用して，その人々のホーム環境にアクセス可能とすることである．ユビキタスコンピューティングに関する関連研究では，“安心・安全” を実現するうえで重要な利用者の認証と公共の環境におけるコンピューティング資源そのものの認証に関する問題の議論が十分でなかった．そこで，本稿では，コンピューティング資源利用時の認証認可に着目し，外出先の環境から安心・安全にホーム環境にアクセス可能とする人にやさしいリモートアクセス方式を提案する [3], [4]．提案する方式は，電子的な利用権を用いて，広域に分散されたコンピューティング資源利用時の利用者と資源の認証認可機構をベースとしたリモートアクセス機構を提供する．さらに，ロケーションを越えて資源が提供するサービスの合成を可能としている．

以下，2 章において，想定する利用シーンと関連研究から，従来の一時利用サービスや関連研究との違いを示す．3 章で提案方式実現のための要件と基本モデル，4 章に基本モデルの実現方式を示す．そして，5 章で実験システムとその動作検証結果を，6 章で要件の検証結果やセキュリティ，性能に関する考察を述べる．

2. 想定する利用シーンと関連研究

2.1 想定する利用シーン

利用者は，会社のドキュメントサーバと自宅の Web カメラにアクセスできる利用権が格納された IC カードを携帯している．そして，必要に応じて，外出先のカフェのインターネット端末を利用できる利用権を取得（購入）する．

利用者は，その IC カードを外出先のインターネット端末のカード R/W に提示する．それにより，インターネット端末を利用して，会社のドキュメントサーバ上の資料を編集したり，自宅の被介護者の様子を確認したりできる．この際，利用者や資源の属性に応じて，インターネット端末の利用可能時間が可変となる．ここで，利用者属性や資源属性とは，利用者が，外出先で利用しようとしているインターネット端末のサービス事業者と提携関係がある ISP（Internet Service Provider）の会員であるとか，利用する機器が大画面モニタ付きであるとかといったことを指す．たとえば，利用者がインターネット端末のサービス事業者と提携関係がある ISP の会員の場合は，そうでない場合よりも利用可能時間が長くなる．

この利用シーンでは，IC カードという軽く使い慣れたデバイスを持ち運ぶことを前提としている．そのうえで，以下の 3 つのポイントが従来の一時利用サービスと異なる．

- 外出先コンピューティング資源を利用する際，利用者やコンピューティング資源の属性に合わせたサービスを提供できること
- IC カードの提示だけで，外出先コンピューティング資源の利用と会社や家庭のコンピューティング資源へのリモートアクセスができること
- 外出先コンピューティング資源の提供するサービスと会社や家庭のコンピューティング資源が提供するサービスを合成することができること

なお，本稿でのコンピューティング資源（以下，資源と呼ぶ，特に物理的に利用者の身近にある資源をローカル資源，遠隔にある資源をリモート資源と呼ぶ）とは，会社のドキュメントサーバや自宅の Web カメラ，外出先のインターネット端末など，プロセッサが埋め込まれた機器全般を指している．また，これらの資源を提供することをサービスといい，その資源を管理しサービスを提供する人をサービス提供者と呼ぶ．

2.2 関連研究

複数の資源を利用することで，個々の利用者に最適なサービス提供を目指すユビキタスコンピューティングの研究 [5] は，これまでも多く提案されている．これらの研究の

多くは，適用する環境や対象とする利用者によって3つのグループに分けられる．ここで，適用する環境とは，会社や家庭などのclosedな特定の環境と駅や空港などのopenな公共の環境を指す．また，利用者は，サービス提供者と事前契約関係のある特定の利用者と事前契約関係のない不特定の利用者を指す．

- 第1のグループ：特定の環境において，特定の利用者を対象にしたもの
- 第2のグループ：公共の環境において，特定の利用者を対象にしたもの
- 第3のグループ：公共の環境において，不特定の利用者を対象にしたもの

以下，これら3つのグループにおいて，具体的な関連研究をあげながら，利用者認証，資源認証，リモートアクセス，およびサービス合成の各観点における対応状況を示す．ここで，利用者認証とは，悪意のある利用者を排除したり，利用者に提供するサービスを決定したりするために行われる利用者の本人性や属性の認証行為を指す．資源認証とは，資源を管理する悪意のあるサービス提供者を排除したり，資源が提供するサービスレベルを保証したりするために行われる資源の真正性や属性の認証行為を指す．リモートアクセスとは，特定の環境や公共の環境から異なるロケーションの特定の環境へネットワークを利用してアクセスし，利用者の権限に応じてアクセス先の資源を利用することを指す．また，サービス合成とは，利用者の要求に応じて個々の資源の受付可能な入力や出力の型を判定し，それらを動的にバインドさせることで，複数の資源を連携させたサービスの提供を意味する．公共の環境では，対象資源の安全性や享受できるサービスレベルの保証が，安心・安全なユビキタス環境の実現のために重要と考えた．そこで，利用者認証だけでなく，上で定義した資源認証も比較の観点とした．

利用者の位置情報を利用して環境に遍在するデバイスの利用制御を行うEasy Living [6]や環境に埋め込まれたコンピュータを利用して，人の状況を認識し収納物の探索支援などが可能なThe Aware Home [7]が提案されている．また，病院内の位置情報と医師などの利用者属性によって利用できるデバイスを制御するContext-aware user authentication [8]などが提案されている．これらは，第1のグループに属する．第1のグループでは，特定の利用者を対象としているため，RFIDやICカードなどによる利用者認証を前提としている．また，特定の環境を前提としているため，その環境内の資源そのものの認証や異なるロケーションの環境へのリモートアクセスは考慮されていない．サービス合成に関しては，特定の環境内の資源が提供するものに限られている．

VNC [9]，MetaFrame，Sun Rayといったサーバベースコンピューティング [10]が提案されている．これらは，アプリケーションをサーバ上で実行する形態をとっており，そのサーバ配下のクライアントであれば，どこからでもサーバ上のアプリケーションを実行できる．アプリケーションそのものを外出先のPCで実行することができるPC環境ローミング技術 [11]が提案されている．これは，ICカードなどによる利用者認証に基づいて，暗号化されたコンピューティング環境を専用サーバから外出先のPCにダウンロードする．それにより，あたかも外出先のPCに自分のPC環境がローミングされたかのような作業環境を実現するものである．携帯電話を利用した利用者認証に基づき，遠隔地，たとえば友人宅から，自宅のホームネットワークにアクセスする情報家電サービス利用方式 [12]が提案されている．これは，DLNAプロトコル [13]により遠隔からコンテンツの視聴などを可能にするものである．さらに，携帯電話を用いて自宅のホームネットワークに接続された情報家電の制御が可能なサービスゲートウェイ [14]が提案されている．これらは，第2のグループに属する．第2のグループは，特定の利用者を対象としているため，ICカードや携帯電話などによる利用者認証を前提としている．また，公共の環境を前提としているが，公共の環境におけるPCや家電などの資源に関しては専用端末か，その利用が暗黙に了解されている場合（友人宅のTVの場合など）を想定している．つまり，資源自体の認証は考慮されていない．さらに，これらの研究は，そもそもリモートアクセスを目的としているものが多く，複数サービスの合成は視野に入っていない．

自動登録された資源を名前解決によって発見した後，それらを動的にバインドして利用者の置かれた環境の中で最適なサービスを提供するものとして，Hive [15]，STONE [16]，DANSE [17]，Ninja [18]などが提案されている．また，個々のサービスをジグソーパズルのピースに見立てて，それらを利用者が合成させることができる“Playing with the Bits” [19]が提案されている．これらは，第3のグループに属する．第3のグループは，不特定の利用者を対象としている．サービス合成のためには，個々の利用者を識別する認証認可機構との協調が必要であるが，認証認可を前提として議論しているものが多い．これは，第1，第2グループが特定の利用者が対象であるのに対して，第3のグループでは不特定の利用者が対象であることが認証認可の問題を難しくしているといえる．また，公共の環境を前提にしているにもかかわらず，環境内の資源そのものの認証は考慮されていない．さらに，これらの研究は，サービス合成に重きをおいており，リモートアクセスはフォーカスされていない．

一方，本研究では，公共の環境において，不特定の利用者を対象としたものである．つまり，第3のグループに属する．そして，関連研究では議論が十分でなかった利用者の認証と公共の環境における資源そのものの認証に関する問題に取り組んでいる．そして，利用者と資源の認証機

表 1 関連研究と提案方式の比較
Table 1 Related work and proposed method.

グループ	対象環境	対象利用者	利用者認証	資源認証	リモートアクセス	サービス合成
1	特定	特定	○	×	×	○
2			○	×	○	×
3	公共	不特定	×	×	×	○
提案方式			○	○	○	○

構をベースとしたリモートアクセス機構を提供し，ロケーションを越えた資源が提供するサービス合成を可能としている．以上述べた関連研究と本研究の違いを表 1 に整理する．

3. 人にやさしいリモートアクセス方式

3.1 要求条件

2 章で示した想定する利用シーンにおける既存サービスとの違いや関連研究との違いを明確化し，人にやさしいリモートアクセス方式を実現するための要件を以下のように整理する．

【要件 1】利用者と資源の認証とその認証結果に合わせたサービス提供が可能なこと

公共の資源を不特定の利用者が利用する場合でも利用者や資源の認証が可能で，認証された本人性（資源の場合は真正性）や属性に合わせたサービスを提供できる必要がある．

【要件 2】利用者に負担をかけずにリモートアクセスが可能なこと

特別な IT 機器が不要で，煩雑な手順をふまなくてもリモートアクセスが可能である必要がある．

【要件 3】ロケーションを越えたサービス合成が可能なこと

専門知識がなくてもローカル資源とリモート資源が提供するサービスの合成が可能である必要がある．

【要件 4】直感的な操作でリモートアクセスやサービス合成が可能なこと

グラフィックとタッチセンスを用いた直観的な UI によりその利用者のアクセス可能範囲を可視化でき，直感的な操作を可能とする必要がある．

特に本研究では，上記の要件に関して，改ざんが不可能な IC カードの利用を想定している．ここで想定している IC カードは，ISO/IEC7816 や 14443TypeB に準拠したカード [20] である．

3.2 基本モデル

公共の資源を不特定の利用者が利用する場合には，これまでのような個々の資源が個別に利用者ごとのアクセス制御ポリシを管理し，個別に利用者認証する方式は適用できない．これは，いつだれがどこの資源を利用するのかを予測することができないことに起因する．そこで，【要件 1】を満足するための方式として，電子権利流通技術に着目した．具体的には，外出先の資源や会社や家庭などの特定の環境の資源を利用できる電子的な権利（利用権）を導入した．詳細は 4 章で説明するが，利用権には，資源利用の条件として，利用者や資源に関連する条件（アクセス制御ポリシ）が記述されている．利用者は，必要に応じてサービス提供者から利用権を入手する．この場合のサービス提供者は，外出先資源をビジネスとして提供する事業者や会社のネットワーク管理者，家庭の場合はホームネットワーク管理者などを指す．このようにアクセス制御ポリシを個々の資源から分離し，利用権の形にして流通させることで，【要件 1】を満足させることができる．

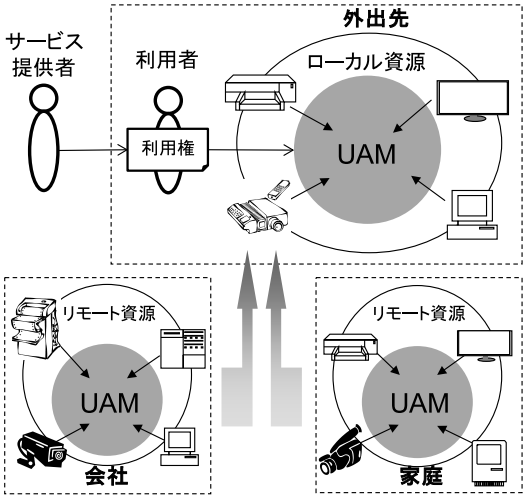


図 1 基本モデル
Fig. 1 Basic model.

さらに，【要件 2】，【要件 3】を満足させるために，オーバレイネットワーク技術に着目した．具体的には，外出先や会社などの各ロケーションに，オーバレイネットワーク機能として UAM（Ubiquitous Area Manager）からなる基本モデルを考えた（図 1）．この基本モデルでは，利用者は，IC カードに複数の利用権を格納して持ち歩く．利用者が利用権を格納した IC カードを外出先の UAM（ローカル UAM）に提示すると，ローカル UAM は，利用権に記述された権利情報を解析し，他のロケーションの UAM（リモート UAM）と協調しながら最終的にローカル資源とリモート資源のそれぞれの提供サービスを合成し，利用者に提供する．つまり，利用者は，外出先の環境に利用権を提示するだけでよく，資源利用の認証認可からリモートアクセス処理，サービス合成まで利用者に代わってシステムが実行する利用権ドリブンなオーバレイネットワークを可能としている．

4. 基本モデルの実現方式

3 章で示した基本モデルを実現するための課題とその解決方法を示す．

4.1 課題の定義

基本モデルを実現するための課題とその定義を以下に示す．

① 利用権を用いた利用者認証・資源認証方法
公共の資源の一時利用に際して，不特定の利用者であってもその利用者，資源の本人性（真正性），属性の認証が可能となる方法が課題である．

② 利用権によるリモートアクセス制御方法
特定の環境や公共の環境から不特定の利用者がリモートアクセス先を柔軟に選択してリモートアクセスできる方法が課題である．

③ サービス合成，合成サービス実行制御方法
個々の資源の受付可能な入力や出力の型を判定し，それらを動的にバインドさせることで，複数の資源を連携させたサービスをその開始から終了まで制御する方法が課題である．

④ UAM アーキテクチャ
基本モデルの構成要素である UAM をオーバレイネットワーク機能としてヘテロジニアスなネットワーク環境上に適用可能なアーキテクチャが課題である．

⑤ UAM のシステム構成とサービスコンポーネント間の連携方法
UAM アーキテクチャをシステム化するための実際のシステム構成と UAM を構成する各サービスコンポーネント間の具体的な連携方法が課題である．

⑥ GUI デザイン
【要件 4】を満足するユーザインタフェースをどのようにデザインするかが課題である．

①～③ の課題は，3.2 節で述べたように基本モデルを実現するうえで必要な機能的な課題である．これらは，2.2 節で示したように関連研究で解決できていない課題でもある．④～⑥ の課題は，機能的課題の解決方法をどのように UAM として構成するかというシステム化に向けた課題である．以下，それぞれの課題に対する解決方法を示す．

4.2 機能的課題の解決方法

(1) 利用権を用いた利用者認証・資源認証方法

図 2 に利用権を用いた利用者と資源の認証機能である分散認証認可方式を示す [21]．利用権には，利用権をユニークに識別可能で，対象となる資源の設置ロケーションや種別の識別が可能な利用権 ID と利用者や資源に関連するアクセス制御ポリシである利用者ポリシと資源ポリシが記述されている．利用者は，IC カードに利用者属性を格納し，必要に応じて利用権を取得（購入）する．資源利用時には，利用者ポリシは利用者属性が格納された IC カード内（利用者ポリシ判定）で，資源ポリシは資源属性が格納された資源内（資源ポリシ判定）で分散して判定される．そして，それぞれの判定結果として，利用権 ID が含まれる利用者ポリシアサーションと資源ポリシアサーションが生成され，サービス認可装置に送付される．サービス認可装置では，双方の判定結果により対象資源の一時利用が認可判定され，サービスが提供される．これらの処理プロセスは，SAML フレームワーク [22] に準拠しており，新たに定義した信頼モデルにより判定結果の信頼性を担保している．この信頼モデルは，利用者属性を管理し利用者ポリシ判定に責任を持つ利用者認証ドメインと資源属性を管理し資源ポリシ判定に責任を持つ資源認証ドメイン，利用権を発行し資源利用を利用者に認可することに責任を持つサービス認可ドメイン（サービス提供者はこれに含まれる）からなる．このような独立した 3 者モデルを前提とした認証認可方式を用いることで，不特定の利用者であってもその利用者，資源の本人性（真正性），属性の認証結果の正しさが保証される．

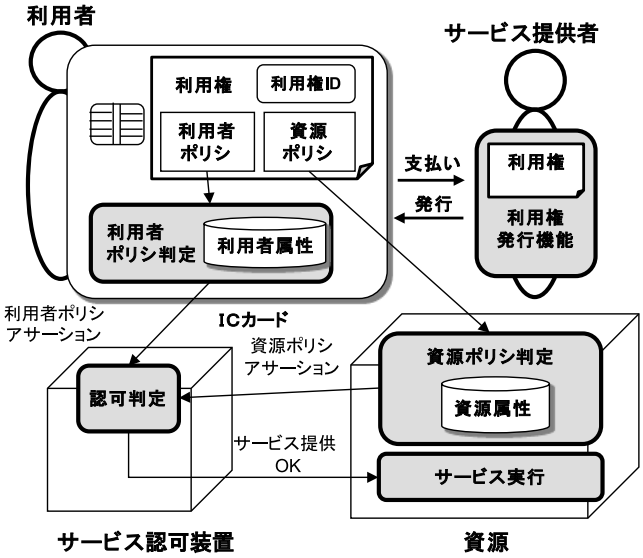


図 2 分散認証認可方式
Fig. 2 Distribution authentication authorization method.

(2) 利用権によるリモートアクセス制御方法

分散認証認可方式では，利用権に記述された利用者ポリシに基づき，利用者の認証結果である利用者ポリシアサーションが生成される．もしこの利用権がその利用権 ID からリモートアクセス先の資源のものであると判明した場合，この利用者ポリシアサーションは，その利用者がそのリモート資源にアクセスできることを証明するものとなる．さらに利用権 ID から資源の設置ロケーションが判別できる．これにより，対象資源が所属する UAM に対して利用者ポリシアサーションを送付しリモート資源に対するアクセス制御を依頼することができる．2.2 節で示した第 2 のグループに属する関連研究でも，リモートアクセスのために，IC カードや携帯電話を利用して認証情報をリモートアクセス先に通知している．しかしながら，これらの関連研究では，リモートアクセス先が固定的であり，事前契約に基づく利用者の事前登録を前提としている．本提案方

表 2 資源の役割定義
Table 2 Computing resource role definition.

役割	役割定義	具体例
Client	特定のプロトコルに対応し，クライアントとしての機能を持つ資源	コンテンツプレーヤー
Local – server	クライアントと同じロケーションにあり，特定のプロトコルに対応し，サーバとしての機能を持つ資源．．	ローカルコンテンツストリーミングサーバ，ローカルWebカメラ
Remote-server	クライアントと異なるロケーションにあり，特定のプロトコルに対応し，サーバとしての機能を持つ資源．．	リモートコンテンツストリーミングサーバ，リモートWebカメラ
Through	プロトコルによらず情報を伝送する資源	IPフィルタリングのようなネットワークアクセス制御資源

法では，必要に応じてサービス提供者から利用者ポリシが記述された利用権を入手することで，利用者ポリシアサーションがICカード内で動的に生成される．それによりリモートアクセスが可能となる．これは，利用者の事前登録が不要であるばかりでなく，リモートアクセス先を柔軟に選択できるという点でメリットがある．

(3) サービス合成，合成サービス実行制御方法

サービス合成のために資源の受付可能な入力や出力の型を判定するためには，該当する資源が，同一のプロトコル，同一のデータフォーマットをサポートしているかどうかを検証する必要がある．これについては，ICANN管理のwell-known port名称 [23] とMIME type [24] が同一かどうかをチェックすることを考えた．さらに，資源ごとに**表 2** に示したような役割を定義した．表2に定義した資源間で合成が可能なのは，client-server，client-through，server-throughの3パターンとした．これにより，資源間の情報伝達のコリジョンなどを防ぐことができる．さらに資源のロケーション情報により異なるロケーションの資源を合成させる場合は，かならずthroughの役割の資源が必要とした．

合成サービス実行制御は，最終的に合成したサービスの開始，終了などの実行制御を司る機能である．サービス開始にあたっては，複数の資源が関わるため資源の起動順序を制御する必要がある．資源の起動順序については，through，server，clientとした．これは，たとえば，ストリーミングコンテンツを利用する場合は，clientの役割を持つコンテンツプレーヤからserverの役割を持つストリーミングサーバに対して送信要求が出される．そのため，その前にthroughの役割を持つネットワークアクセスとストリーミングサーバをready状態にしておく必要があるためである．サービス終了時には，開始時の逆の順番で資源を終了させる．さらに，サービス終了時には，異常終了も考慮した後処理を漏れなく実施する必要がある．そこで，これら一連のサービス合成，合成サービス実行制御に関する状態遷移（**図 3**）を明らかにし，それに基づいた制御機能を設計した．これは，上述した資源どうしの合成（合成待ち）やそれらの実行制御（サービス実行），実行後の利用

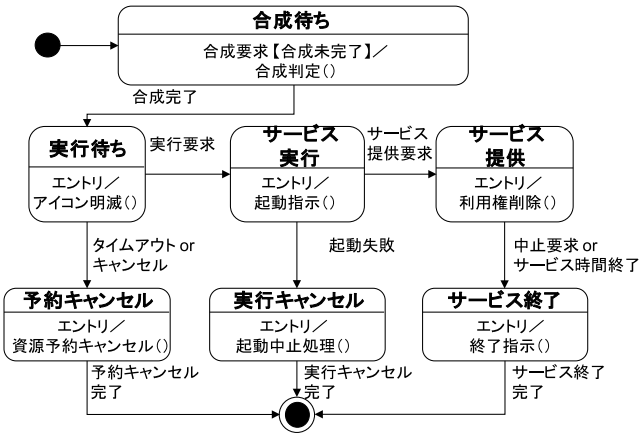


図 3 サービス合成，合成サービス実行制御に関する状態遷移図
Fig. 3 State transition diagram of service combine and execution control.

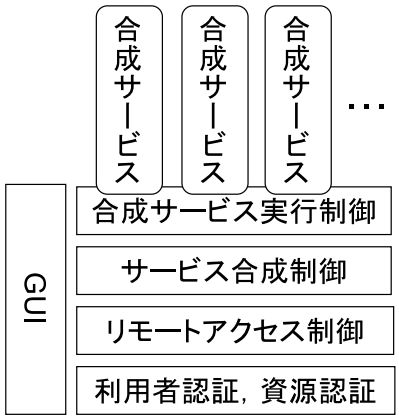


図 4 UAM アーキテクチャ
Fig. 4 UAM architecture.

権削除（サービス提供）まで，異常系も考慮したものである．これにより，例え異常終了しても，ローカル資源上のキャッシュデータなどの一時データの削除などの後処理が漏れなく完了できる．

4.3 システム化に向けた課題の解決方法

(1) UAM アーキテクチャ

UAMアーキテクチャは，SOA（Service Oriented Architecture）の考えに沿って構成した（**図 4**）．具体的には，4.2節で説明した課題の解決方法に対応する機能をサービスコンポーネントとして定義した．具体的なサービスコンポーネントは，利用者認証・資源認証，リモートアクセス制御，サービス合成制御，合成サービス実行制御の4つである．個々の合成サービスは，この合成サービス実行制御の管理下において，それぞれ独立に実行される．また，【要件4】を満足するために，4つのサービスコンポーネントに対して1つのGUIを用意し，UAMの持つサービスコンポーネントを統一的に操作可能な構成とした．

提案するUAMアーキテクチャは，人にやさしいリモートアクセスを実現するサービスコンポーネント群とその上

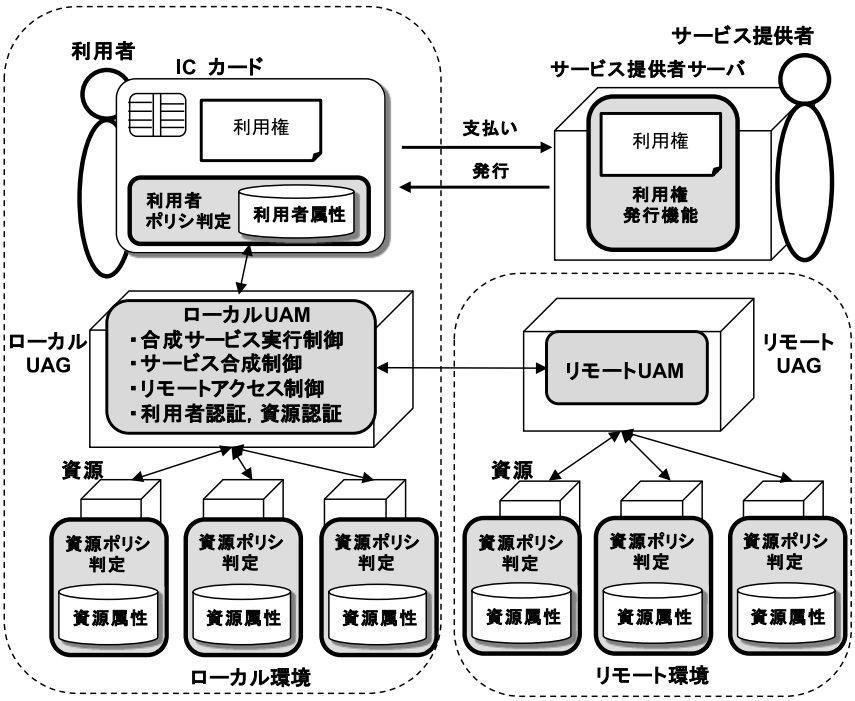


図 5 UAM システム構成
Fig. 5 UAM system structure.

で稼働する個々の合成サービスから構成される点が特徴である．これにより，個々の合成サービスは，サービス提供にあたって認証認可などの機能を個別に考慮する必要がなくなり，対象サービスのバリエーションの広がりを期待できる．また，UAM アーキテクチャは，そもそも SOA としてのメリットである機能の拡張性や実装上の柔軟性を有する．

(2) UAM のシステム構成とサービスコンポーネント間の連携方法

図 5 に UAM のシステム構成を示す．UAM を実装する装置を UAG（Ubiquitous Area Gateway）と呼ぶ．UAG は，インターネットカフェなど，ロケーションごとに 1 つ設置され，その場所の複数の資源を管理することを想定している．ここで，管理するとは，資源のその環境へのプラグイン，プラグアウトの検知によりその資源が利用可能であるか否かの情報を保持していることを指す．さらに，左側の点線で囲んだ領域が利用者の存在するローカル環境を表し，右側の点線で囲んだ領域が会社や家庭などのリモート環境を表す．

図 5 の中で，UAM アーキテクチャのサービスコンポーネントに含まれないのは，図右上のサービス提供者サーバ内の利用権発行機能である．サービス提供者サーバとは，外出先資源を提供する事業者や会社のネットワーク管理者，ホームネットワーク管理者などのサービス提供者が運用するサーバを想定している．図 5 のシステム構成において，図 4 で定義した各サービスコンポーネントや利用権発行機能がどのように連携するのかを，全体の処理プロセス（**図 6**）の流れに沿って説明する．なお，提案する処理プロセスは，次の (3) で述べる統一的な GUI を通した利用者の操作により動作することを前提としている．

A．利用権発行

サービス提供者サーバと IC カード間で，オンデマンドに暗号通信路を構築する．それにより利用権が IC カードに配送される（①）．利用権内の利用者ポリシのみが IC カード内で判定されて，利用者ポリシアサーションが作成される．利用権発行時に利用者ポリシアサーションを作成しておくのは，後の各処理プロセスを高速に行うためである．利用権が発行される契機は，外出先でサービス提供者サーバからそのつど取得するケースと事前に会社のネットワーク管理者などから取得するケースが考えられる．いずれにしても，本プロセスは，以下の外出先資源を利用したリモートアクセスに関する処理プロセスとは独立したプロセスとなる．IC カード単体では，サービス提供者サーバとの間で暗号通信路を構築することができない．そのため，ここでは，IC カードとサービス提供者サーバとのインタフェース機能を有する操作端末（IC カード R/W 付きの PC）の利用を前提としている．本操作端末は，プロセス B 以降の IC カードと UAG とのインタフェース機能も有する．

B．資源表示

利用権が格納された IC カードを操作端末のカード R/W に載せると利用権 ID が読み込まれる．そして，該当する資源のアイコンが操作端末上に表示される．

C．リモートアクセス可否判定

利用者からの指示により，資源ポリシのみが含まれた利用権と利用者ポリシアサーションのセットがローカル UAG

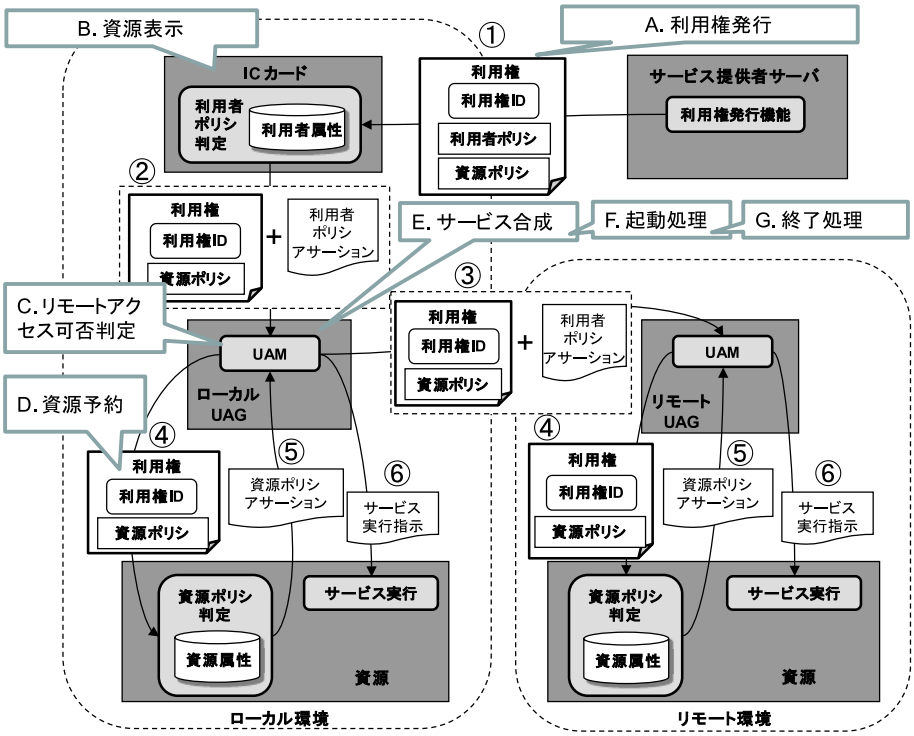


図 6 処理プロセス
Fig. 6 Process sequence.

に提示される（②）．その利用権 ID から該当する資源の設置ロケーションを判別する．他ロケーションの場合は，該当するリモート UAG にそのセットが転送される（③）．利用権と利用者ポリシアサーションのセットを受け取ったリモート UAG では，利用者ポリシアサーションに基づき利用者認証を実施し，リモートアクセス可否の判定を行う．

D．資源予約

利用権と利用者ポリシアサーションのセットを受け取った UAG は，該当する資源に対して，資源ポリシの判定を依頼（④）する．その結果として資源ポリシアサーションを受け取る（⑤）．利用者ポリシアサーションと資源ポリシアサーションから資源の利用可否を判定し，その資源の予約を完了する．この場合，対象資源のポリシの判定結果のほかに，その資源が利用可能であることが前提となる．複数の資源を利用する場合は，C，D が繰り返される．

E．サービス合成

UAG は，4.2 節で示した方法によりサービス合成の判定を行い，その結果に基づきサービスを合成する．

F．起動処理

4.2 節で示した方法により資源の起動順を制御する（⑥）．正常にサービスが開始された段階で，該当する利用権の削除処理などの後処理を実施する．

G．終了処理

既定時間の経過や利用者の指示により途中でサービスを終了する場合，サービス終了にともなう後処理を実施する．また，利用者が IC カードを操作端末のカード R/W から

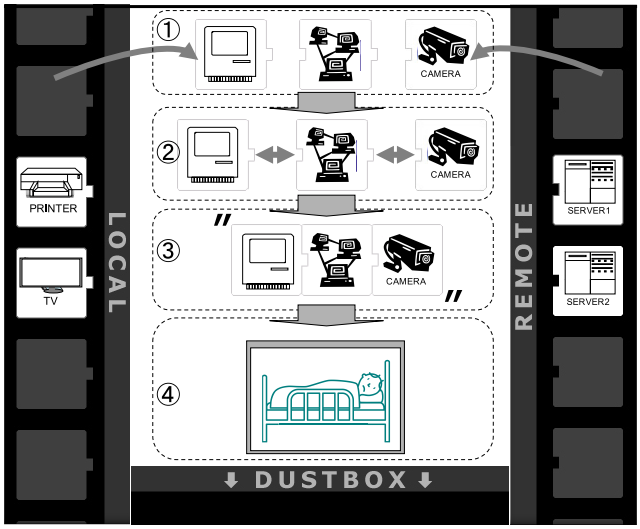


図 7 GUI
Fig. 7 Graphical user interface.

取り去ると，資源アイコンの消去とともに，利用権に関する情報はすべて操作端末上から削除される．

(3) GUI デザイン

4.3 節 (2) に示したようにプロセス A は，外出先資源を利用したリモートアクセスに関する処理プロセスとは独立したプロセスである．そのため，プロセス B 以降の GUI を説明する．この GUI の特徴は，各資源を操作端末のタッチパネル上にアイコン表示し，それらを指でパズルのピースのように合成させることができるという点である（図 7）．これにより，利用者のアクセス可能範囲が可視化でき，直

感的な操作が可能となる．以下に GUI の操作手順を示す．

- 4.3 節 (2) で示したプロセス B により，ローカル資源が画面左側に，リモート資源が画面右側に表示される．
- 利用したい資源をそれぞれ中央の場にドラッグ&ドロップする（①）．この際，プロセス C，D が実行される．認証認可が正常に完了すれば，アイコンはその場に残る．そうでない場合は，アイコンは元の場所に自動的に戻る．いったん，場に出したアイコンをキャンセルしたい場合は，画面下の DUSTBOX にドラッグ&ドロップすることで可能である．
- 合成させたい資源のアイコンを重ね合わせる（②）とプロセス E が実行される．合成判定が合格した場合のみ，複数のアイコンが連結される．判定が不合格の場合は，個々のアイコンが反発し合い連結されない．
- 最終的に資源の合成が完了すると，そのアイコン全体がブリンクする．それにより，実行可能状態であることを知らせる（③）．
- ブリンクしたアイコンをダブルタップすると，サービスが開始される（④）．図 7 の例では，タッチパネルを有した操作端末そのものと，インターネット接続，自宅のカメラを合成させている．それにより，操作端末のブラウザ上に自宅の被介護者の様子が表示される．

5. 実験システム

5.1 実験システムの実装

図 8 に今回開発した実験システムの構成図を示す．外出先の資源としてインターネットカフェの資源を利用して，会社や家庭の資源にリモートアクセスすることを想定した実験システムである．実験システムでは，IC カード，サービス提供者サーバ，UAG（ローカル，リモート），ローカル資源としての操作端末，大画面 TV，IP フィルタリング AP，リモート資源としてのドキュメントサーバ，ストリーミングコンテンツサーバ，Web カメラがその構成機器となっている．各資源が提供するサービスは以下のとおりである．

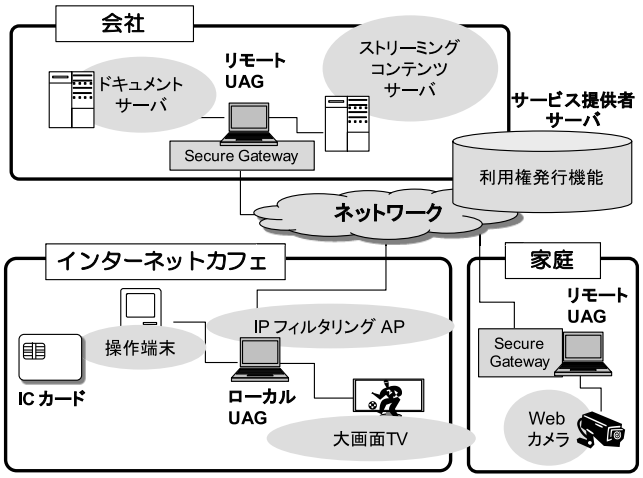


図 8 実験システム
Fig. 8 Demonstration systems.

- 操作端末・大画面 TV：Web ブラウザによるコンテンツ表示サービス
- IP フィルタリング AP：他ロケーションへのパケット通信制御サービス．実際の環境では，外部インターネットへの接続制御を行うサービスに該当
- ドキュメントサーバ：文書，画像などのファイル共有サービス
- ストリーミングコンテンツサーバ：動画像配信サービス

本研究では，UAG はグローバルアドレスを持つルータに統合され UAG 相互に直接通信できるものという前提をおいている．つまり，ルータに統合されている UAG が NAT 機能を持って各構成機器に付与されたプライベートアドレスのアドレス変換を行うこととしている．しかし，実験システムでは，クローズドな実験環境内の同一の LAN 上に，想定するロケーションごとにサブネットを割り当てて構成しており，UAG に NAT 機能までは実装していない．これは，本研究が提案する基本モデル実現のための各方式の実現性評価に主眼をおいたためである．現実のネットワーク環境に本提案システムを実装する際の制約や課題については，別途 5.3 節で論じる．

以下に各構成機器への実装結果を示す．

(1) IC カード

IC カードは，TypeB の非接触 I/F を持つ大容量マルチアプリケーション IC カードである ELWISE [25] を用いた．本 IC カードの Native OS 上に C 言語を用いて利用者ポリシ判定機能を実装した．IC カードの発行機能や IC カードへのアプリケーションダウンロード機能などについては，マルチアプリケーション IC カード管理プラットフォームである NICE [26] を用いた．

(2) サービス提供者サーバ

サービス提供者サーバに利用権発行機能を Linux OS 上に Java で実装した．本来ならインターネットカフェ，会社，家庭の資源の利用権は，それぞれ異なるサービス提供者サーバが発行するのが普通である．しかし，今回は，実験システムということもありインターネットカフェの資源の利用権発行機能のみを実装した．今回実装しなかった会社や家庭の資源の利用権発行機能のフィージビリティについては，別途 6.1 節で議論する．

(3) UAG

利用者認証・資源認証，リモートアクセス制御，サービス合成制御，合成サービス実行制御の 4 つの機能を持つ UAG は，Linux OS 上に C 言語および Java を用いて実装した．リモート UAG には，外部ネットワークからの不正なアクセスを防御する機能が求められる．本実験システムでは，そのための「リモートアクセス可否判定」を実現する Secure Gateway をリモート UAG に実装した．

表 3 装置スペック
Table 3 Experimental equipment specification.

	OS	CPU		メモリ
サービス提供者サーバ，UAG	FedoraCore2	Pentium M	1.6GHz	1GB
資源代行PC，操作端末	Windows XP	Pentium 3	1.1GHz	392MB
ドキュメントサーバ，ストリーミングコンテンツサーバ	Windows XP	Pentium 4	2.8GHz	392MB

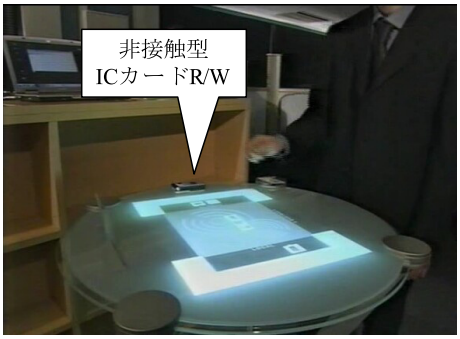


図 9 操作端末の操作イメージ
Fig. 9 Operation image.

Mizuno らは，UPnP を利用したゼロコンフィグレーション機能と外部利用者の認証に基づき動的に FireWall を制御する機能を持つ Home-Use Gateway [27] を提案している．Home-Use Gateway における外部利用者の認証については，Home-Use Gateway 上に公開されたポータルページに SSL を使ってアクセスし，ユーザ名とパスワードを入力することで実現していた．今回，このユーザ名とパスワードによる認証を，ローカル UAG から送付された利用者ポリシアサーションに置き換えて検証できるように改造することで Secure Gateway を実現した．

(4) 資源

各対象資源には，図 6 に示したように資源ポリシ判定やサービス実行を制御する機能を実装した．ただし，実験で利用した大画面 TV と Web カメラそのものにはプログラミングによりこれらの機能を付加することができなかった．そのため，これらの資源に接続した PC でその機能を代行させた（資源代行 PC）．非接触型 IC カード R/W が付属した操作端末には，他の資源にはない機能としてサービス提供者サーバや UAG とのインタフェース機能を実装した．さらに，タッチパネル上で資源の合成を利用者が直接的に操作可能とする GUI 機能を Flash で実装した．操作端末の実機操作イメージを図 9 に示す．以上の機能は Window OS 上に C++，Java を用いて実装した．また，他ロケーションとの間でパケットをフィルタリングする IP フィルタリング AP については，ローカル UAG が稼動する同一のサーバ上に実装した．

上述した機能を実装し実験に利用した各構成機器の装置スペックを表 3 に示す．

5.2 動作検証

以下に示すシチュエーション，前提条件下で，4 つのシナリオを実験システム上で動作検証した．

＜シチュエーション＞

利用者 A は，図 8 で示したインターネットカフェにおり，カフェの操作端末や大画面 TV を一時利用して，会社や家庭にリモートアクセスしようとしている．

＜前提条件＞

- 利用者 A の持つ IC カード内の利用者判定ポリシには，“ISP X の会員” という利用者属性が，操作端末内の資源ポリシ判定には，“画面サイズ 20 インチ”，大画面 TV 内（実際には資源代行 PC）の資源ポリシ判定には，“画面サイズ 40 インチ” という資源属性が格納されている．
- 利用者 A は，IC カード内に会社のドキュメントサーバとストリーミングコンテンツサーバにアクセスできる利用権と家庭の Web カメラにアクセスできる利用権を所持している．
- 利用者 A は，インターネットカフェで “ISP X の会員が 20 インチ以上の操作端末を使用して 1 時間インターネットアクセスが利用可能” という利用権と，“ISP X の会員が 40 インチ以上の大画面 TV を使用して 1 時間インターネットアクセスが利用可能” という利用権を取得する．

＜動作シナリオ＞

共通動作シナリオとして，利用者 A が所持する IC カードを操作端末の IC カード R/W 上に載せると，図 7 で示した GUI の左側にインターネットカフェの操作端末と大画面 TV のアイコンが表示される．同様に右側には，会社のドキュメントサーバとストリーミングコンテンツサーバ，家庭の Web カメラのアイコンが表示される．その後，利用者 A は，GUI を操作することで，以下の 4 つのシナリオを実行する．

(1) インターネットカフェの操作端末とネットワークアクセスを一時利用し，会社のドキュメントサーバを参照する．

(2) インターネットカフェの操作端末とネットワークアクセスを一時利用し，自宅の Web カメラの映像を見る．
(3) インターネットカフェの操作端末とネットワークアクセスを一時利用し，会社のストリーミングコンテンツサーバから配信される映像コンテンツを視聴する．
(4) インターネットカフェの大画面 TV とネットワークアクセスを一時利用し，会社のストリーミングコンテンツサーバから配信される映像コンテンツを視聴する．

前提条件で示した利用者 A の属性から，それぞれのシナリオにおいて，ローカル資源を用いて 1 時間のリモートアクセスが可能であることが確かめられた．

5.3 提案システムの制約と課題

今回，実験システムは，実際のネットワーク環境上ではなく，クローズドな実験環境内に構築した．また，ローカル資源である操作端末や大画面 TV のサービスとしては Web ブラウザによるコンテンツ表示サービスのみを対象とした．そのため，ここでは，実際の利用環境や利用シーンを想定した場合の提案システムの制約と課題を論じる．具体的には，提案システムを現実のネットワーク環境に実装するという観点とローカル資源上の多様なアプリケーションを利用するという観点での制約と課題を取り上げる．

(1) 提案システムを現実のネットワーク環境に実装するという観点での制約と課題

5.1 節に示したように，UAG は，グローバルアドレスを持つことを前提としている．そのため，UAG をグローバルアドレスが付与されたルータに統合できることが条件となる．そのため，既存ルータへの統合方法を検討する必要がある．また，今後のネットワーク環境の進展によりこの前提が満たされなくなる可能性もあるため，ネットワーク環境の進展に合わせて実装方法を検討する必要がある．

提案システムでは，利用権 ID から該当する資源の設置ロケーションを判別することとしている．実装した実験システムでは，会社と家庭の 2 つのロケーションのみを判別できればよかった．しかし，提案システムを現実のネットワーク環境に適用するためには，別途，設置ロケーション判別のための名前（利用権 ID）解決システムが必要である．

(2) ローカル資源上の多様なアプリケーションを利用する観点での制約と課題

現状，クラウドコンピューティングが進展し，Web ブラウザを利用することで，単なる情報の参照だけでなく加工，編集も可能になってきている．また，HTML5 [28] に代表される Open Web Platform の台頭により多くの情報機器に Web ブラウザが搭載されるようになってきている．そのため，ローカル資源で提供するサービスは Web ブラウザのみという制約をおいたとしても 2.1 節で示した “外出先で資料を編集する” という利用シーンを阻害するものではない．しかし，今後のアプリケーション開発技術の高度化を考えると，Web ブラウザだけでなく，個別のアプリケーションを利用することで，より利用者に対してバラエティに富んだサービスを提供できる可能性がある．

そこで，提案システムにおいて，ローカル資源上での Web ブラウザ以外のアプリケーションを利用する際の課題を論じる．具体的には，利用者がローカル資源上でアプリケーションを利用する際，その利用前，利用時，利用後の契機に分けて，それぞれ現状考えられる課題とその実現可能性を示す．

- 利用前：利用者に対してアプリケーションを認知させる方法

通常，利用者は利用するローカル資源上でどのようなアプリケーションが利用可能かを知りえない．これは，想定する利用シーンから利用者がそのローカル資源をはじめて利用するケースが多いと考えられるためである．そのため，その認知方法が課題である．提案システムでは，操作端末や大画面 TV といったローカル資源単位でアイコンを表示している．これを，“ローカル資源＋アプリケーション” という単位でアイコン表示する．これにより，利用者に対して，どのローカル資源でどのアプリケーションが利用可能なのかを認知させることができる可能性がある．ただし，この際，“ローカル資源＋アプリケーション” という単位で利用権を発行することが条件である．

- 利用時：利用者の属性に応じてアプリケーションの提供する機能を制御する方法

アプリケーションの提供する機能により利用するローカル資源のリソースが異なる可能性がある．通常の PC 利用の場合は，たとえば，パスワードによる管理者権限の確認などにより，特定のリソースにアクセスすることを可能としている．しかし，本研究では，不特定の利用者を対象にしているため，このような対処方法は適用できない．一方，提案システムでは，利用者属性に応じた利用者ポリシ判定により資源の利用可否を判定している．そのため，この機能を利用することで，利用者の属性に応じてアプリケーションの提供する機能を制御できる可能性がある．

- 利用後：アプリケーション終了後の後処理方法

アプリケーション終了後，アクセスした情報が残留してしまうのを防ぐ必要がある．これは，公共の資源を利用する場合のセキュリティに関する一般的な課題でもある．そこで，この課題の対応方法については，6.2 節で示す．

6. 考察

本研究の目的は，人にやさしいリモートアクセスの実現である．そこで，そのための要件の検証結果と要件の検証を行ううえでの前提条件である利用権発行機能の実現性を議論する．また，実用化にあたっては，セキュリティと性能のフィージビリティが重要となるためこれらの評価結果を合わせて示す．

6.1 要件の検証結果とその前提条件の実現性について

5.2 節に示したように，前提とするシチュエーション，条件下で 4 つのリモートアクセスにかかわるシナリオが実現できることを確認した．それぞれのシナリオにおけるローカル資源の利用認可にあたっては，利用者の属性と資源の属性に合わせたサービス提供が可能であり【要件 1】を満足している．会社や家庭へのリモートアクセスに関しては，IC カードの携帯と提示，および直感的な GUI による操作のみで可能であり【要件 2】を満たす．ロケーションを越えたサービス合成についても，直感的な GUI による操作で可能であり，専門知識が不要であるため【要件 3】を満足する．また，これらのことは，GUI の要件である【要件 4】を満たしている．

ただし，これらの【要件】を達成するためには，利用者は利用者の IC カードに必要に応じて，あるいは前もってローカル資源やリモート資源の利用権を取得することが必要である．そのため，利用権の取得にあたって技術的困難性や利用者への負担がある場合は問題となる．著者らの先行研究 [21] や本研究では，ローカル資源の利用権発行機能を実装し，必要に応じた利用権取得に関するフィージビリティを確認している．そこで，ここでは，会社や家庭の資源に対する利用権の発行機能を取り上げる．

まず，会社の資源に対する利用権発行機能に関して説明する．通常固有の社内ネットワークを持つ会社では，ネットワーク上の資源のアクセス権限が組織や職位などによって決められている．また，社内 OA システムなどの利用にあたっては，通常，ID やパスワード，社員証によるアクセス認証が行われている．したがって，個人認証とそれに紐づくアクセス権限の情報をもとに，容易に利用権発行機能を実装することが可能であると考える．

次に，家庭の資源に対する利用権発行機能に関して説明する．家庭の場合，ホームネットワークが敷設されていたとしても，会社のように厳密な個人認証やアクセス権限管理が行われていないことが多い．5.1 節で示した Home-Use Gateway のゼロコンフィグレーション機能では，ホームネットワークに新たに接続された UPnP 対応の家電を自動的にリストアップする．さらにそれだけでなく，Home-Use Gateway の設定ページに Web ブラウザでアクセスすることで，家電ごとに家族の誰にアクセス権を与えるかを設定できる．この際，市販のブラウザ内蔵テレビの画面を見ながら，テレビ番組を予約するような感覚でリモコン操作により設定できる．このように簡易にアクセス権限を設定できる Home-Use Gateway に，その設定内容を利用権の形で発行できる機能を追加することで，家庭内の資源に対する利用権の発行が現実的になると考える．

以上より，会社や家庭における具体的な利用権発行形態は，今後検討する必要があるが，既存システムや既存技術を応用することで，技術面，利用者負担軽減の観点で実現性があると考える．さらに，本研究では言及していないが，先行文献 [29] などから利用権の流通を可能とすることもできる．これにより，たとえば，友達や親せきの家庭の資源の利用権を入手しリモートアクセスするなど，利用権をベースにすることにより新しいユースケースも実現可能となると考える．

6.2 セキュリティ

著者らの先行研究では，資源利用認証認可に利用権を用いることによるセキュリティ脅威を抽出し議論している．そのため，本稿では，それ以外の部分，すなわち利用権入手後，利用権の入った IC カードを携帯し，外出先の資源を利用して合成サービスを利用するまでのセキュリティ脅威全般について議論する．具体的には以下の点である．

(1) 外出先資源を利用するまでの IC カード紛失などによるセキュリティ脅威
(2) 外出先資源を利用した合成サービス実行までのセキュリティ脅威
(3) 外出先資源を利用した合成サービスの実行中，実行後のセキュリティ脅威

(1) については，紛失した IC カードを悪用される脅威が考えられる．現状，指紋認証などの生体認証機能を持つ IC カードが市販されている．利用者は，外出先資源を利用した合成サービスを利用する直前に，指紋認証により IC カード機能をアクティベートする．これを前提とすれば，他の認証要素，たとえば，PIN コード入力などの他の認証行為を利用者に強要することなく IC カードの悪用を防止できる．

(2) については，外出先の操作端末に付属した IC カード R/W にスキミング機能が付けられてしまうケース，外出先操作端末や UAM が改ざんされてしまうケース，合成サービス利用までに異常終了し，利用権情報などが UAM に残ってしまうケースが考えられる．スキミングについては，完全に排除することはできないが，そもそもスキミング機能が付けられない形状にする，あるいは，付けられてもその不自然さから容易に気づくような形状に設計することで防止可能であると考える．外出先操作端末や UAM の改ざんについては，各操作端末や UAG にセキュリティチップを搭載し，インテグリティの観測によりハードウェアやソフトウェアが改ざんされていないかをチェックすることが可能である．たとえば，TCG（Trusted Computing Group）[30] が仕様化しているセキュリティチップである TPM（Trusted Platform Module）を利用することが考えられる．サービス開始に至る前に異常終了した場合は，図 3 で示した状態遷移に基づく制御機能がそれを検知し，利用権情報などを削除する後処理を実行する．

(3) については，たとえば，外出先の資源で社内の機密情報にアクセスした際，そのサービス中に漏えいしたり，

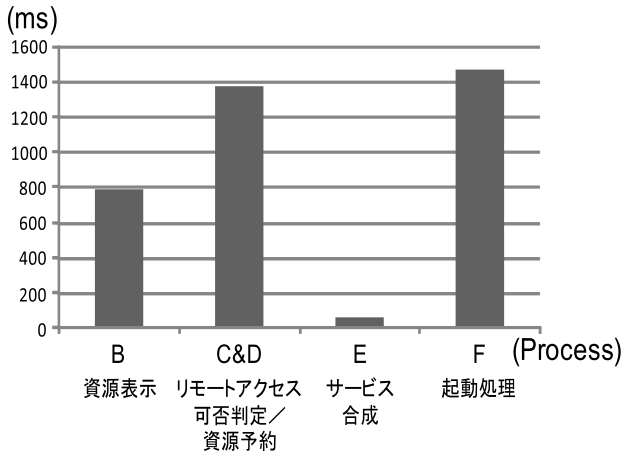


図 10 性能評価結果
Fig. 10 Performance evaluation results.

あるいはサービス終了後にアクセスした情報が残留したりしてしまうことを指す．サービス提供中の情報漏えいに関しては，サービス依存であり，本稿の対象外であるが，サービスを提供するリモートサーバ側で，HTTPS によるアクセスを前提とするなどにより解決可能である．また，サービス後の情報残留については，4.2 節で示したように終了処理において，操作端末などに残されたキャッシュデータなどのサービス利用にともなう一時データはすべて消去される．しかし，より厳密に利用者の作業領域を消去し，利用前の状態に自動的に復元するためには，市販のドライブシールド [31] を組み込むことが有効であると考える．ドライブシールドは，ファイルの新規作成や変更，削除など，レジストリやシステムフォルダへの変更操作を行っても，コンピュータを再起動するだけでそれらの操作は無効になり元の状態に戻るという機能を備えている．5.3 節で示したようにローカル資源上で提供するサービスを Web ブラウザ以外のアプリケーションにまで拡張する場合，すべてのアプリケーションの動作を検証して後処理を施すことは現実的でない．そのため，そのような場合特に有効であると考える．

6.3 性能

5.2 節で示したシナリオ (1) における処理プロセス B，C&D，E，F の性能測定結果を図 **10** に示す．処理プロセス B，C&D，E，F とは，図 6 で定義した各処理プロセスを指す．それぞれのプロセスを 5 回実行しその平均を求めた．会社や家庭などのリモート環境での処理と連携が必要な「リモートアクセス可否判定/資源予約」「起動処理」がそれぞれ 1 秒以上かかっているが，それでも全体で見ると，ぞれぞれのプロセスは 1 秒前後で完了しており，ストレスなく実行できることが分かった．

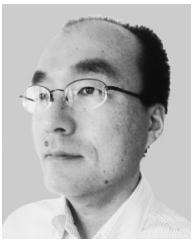
7. おわりに

コンピューティング資源利用時の認証認可に着目し，外出先の環境から安心・安全にホーム環境にアクセス可能とする人にやさしいリモートアクセス方式を提案した．提案方式では，外出先の資源をオンデマンドに利用し，会社や家庭などのホーム環境にセキュアにリモートアクセスできることを示した．また，実験システムの評価により達成すべき要件面やセキュリティ面，性能面でその有効性を示した．今後は，利用権発行機能の具体化，セキュリティに関する残された課題に取り組むとともに，UAM 機能の既存ルータへの実装など既存ネットワーク装置へのマイグレーション方式を検討する．また，並行して「人にやさしい」という観点での評価実験を行いユーザインタフェースの改良を進める．それにより，提案方式をオーバレイネットワークとして実用化することを目指す．

参考文献

[1] 首相官邸，高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）：新たな情報通信技術戦略，入手先 ⟨http://www.kantei.go.jp/jp/singi/it2/dai52/gijisidai.html⟩.
[2] IEEE 802.15, Working Group for WPAN, available from ⟨http://www.ieee802.org/15/⟩.
[3] Kobayashi, T., Ueno, M. and Tada, Y.: Overlay Network for Personalized Ubiquitous Environment Roaming, ICADIWT 2011, *The 4th International Conference on the Applications of Digital Information and Web Technologies*, pp.87–93 (2011).
[4] 小林 透，上野正巳，多田好克：ユビキタス環境ローミングアーキテクチャ：PURE の提案，信学技報，Vol.110, No.374, pp.87–92 (2011).
[5] Weiser, M.: Some Computer Science Issues in Ubiquitous Computing, *Comm. ACM*, Vol.36, No.7, pp.74–83 (1993).
[6] Brumitt, B., Meyers, B., Krumm, J., Kern, A. and Shafer, S.: Easy Living: Technologies for Intelligent Environments, *Proc. Handheld and Ubiquitous Computing*, Vol.1927 of Lecture Notes in Computer Science, pp.12–29 (2000).
[7] Kidd, C.D., Orr, R.J., Abowd, G.D., Atkeson, C.G., Essa, I.A., MacIntyre, B., Mynatt, E., Starner, T.E. and Newstetter, W.: The Aware Home: A living laboratory for ubiquitous computing research, *Proc. 2nd International Workshop on Cooperative Buildings, Integrating Information, Organization, and Architecture*, pp.191–198 (1999).
[8] Bardram, J.E., Kjaer, R.E. and Pedersen, M.Ø.: Context-aware user authentication — supporting proximity-based login in pervasive computing, *Proc. 5th International Conference on Ubiquitous Computing*, pp.107–122 (2003).
[9] VNC, available from ⟨http://www.realvnc.com/⟩.
[10] 岡田潤之，河東 勇，清水茂樹：サーバベースコンピューティング（SBC）ソリューション，三菱電機技報，Vol.77, No.4, pp.263–266 (2003).
[11] Iizuka, S., Uwazumi, K., Nakahama, K., Nakajima S. and Ogawa, K.: Secure PC environment roaming technology for ubiquitous office, *2nd Workshop on Security in Ubiquitous Computing 2003*, pp.799–804 (2003).
[12] Mizuno, S., Haruyama, T., Yamada, K. and Mizuno, O.: A mobile phone based authentication service for

home appliances, *4th IEEE Consumer Communications and Networking Conference* (*CCNC2007*), pp.1168–1169 (2007).
[13] DLNA, available from ⟨http://www.dlna.org/⟩.
[14] 吉原貴仁，茂木信二，堀内浩規：ユビキタス・ネットワーク実現に向けたサービスゲートウェイの実装と評価，情報処理学会論文誌，Vol.44, No.12, pp.3038–3049 (2003).
[15] Minar, N., Gray, M., Roup, O., Krikorian, R. and Maes, P.: Hive: Distributed Agents for Networking Things, *Proc. ASA/MA'99, the 1st International Symposium on Agent Systems and Application and 3rd International Symposium on Mobile Agents* (1999).
[16] 南 正輝，杉田 馨，森川博之，青山友紀：ユビキタス環境に向けたインターネットアプリケーションプラットホーム，電子情報通信学会論文誌（B），Vol.J85-B, No.12, pp.2313–2330 (2002).
[17] 板生知子，松尾真人：適応型ネットワーキングサービス環境 DANSE，電子情報通信学会論文誌（B），Vol.J82-B, No.5, pp.730–739 (1999).
[18] Gribble, S.D.: The Ninja Architecture for Robust Internet-Scale Systems and Services, *Special Issue of Computer Networks on Pervasive Computing* (2000).
[19] Humble, J., Crabtree, A., Hemmings, T., Åkesson, K.P., Koleva, B., Rodden T. and Hansson, P.: "Playing with the Bits" User-Configuration of Ubiquitous Domestic Environments, *UbiComp 2003*, Lecture Notes in Computer Science, Vol.2864/2003, pp.256–263 (2003).
[20] International Organization for Standardization, available from ⟨http://www.iso.org/iso/home.htm⟩.
[21] 小林 透，近藤好次，高橋健司，鶴岡行雄，多田好克：ユビキタス環境における資源利用のための分散認証認可方式の提案，信学論（D），Vol.J93-D, No.11, pp.2390–2402 (2010).
[22] OASIS, available from ⟨http://www.oasis-open.org/committees/security/⟩.
[23] Service Name and Transport Protocol Port Number Registry, available from ⟨http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml⟩.
[24] MIME Media Types, available from ⟨http://www.iana.org/assignments/media-types/index.html⟩.
[25] Yoshizawa, M., Unno, H., Fukunaga, T. and Ban, H.: ELWISE — A super multi-purpose smart card, *NTT Review*, Vol.14, No.1, pp.23–27 (2002).
[26] Toji, R., Wada, Y., Hirata, S. and Suzuki, K.: A network-based platform for multi-application smart cards, *Proc. 5th IEEE International Enterprise Distributed Object Computing Conference*, pp.34–45 (2001).
[27] Mizuno, S., Matsuura, K., Yamada, K. and Takahashi, K.: A New Remote Configurable Firewall System for Home-Use Gateways, *Proc. CCNC'05*, 4-P01-17.pdf (2005).
[28] HTML Working Group, available from ⟨http://www.w3.org/html/wg/⟩.
[29] 寺田雅之，花舘蔵之，藤村 考，関根 純：電子権利流通基盤のための汎用的な原本性保証方式，情報処理学会論文誌，Vol.42, No.8, pp.2017–2029 (2001).
[30] Trusted Computing Group, available from ⟨http://www.trustedcomputinggroup.org/⟩.
[31] ドライブシールド，入手先 ⟨http://www.idk.co.jp/products/driveshield/ss.html⟩.



小林 透 （正会員）

1985 年東北大学工学部精密機械工学科卒業．1987 年同大学大学院工学研究科修士課程修了．同年 NTT 入社．以来，ソフトウェア生産技術，ユビキタスコンピューティング等の研究開発に従事．現在，NTT サイバーソリューション研究所主幹研究員．IEEE，電子情報通信学会各会員．博士（工学）．

上野 正巳 （正会員）

1991 年山梨大学工学部計算機科学科卒業．1993 年同大学大学院工学研究科修士課程修了．同年 NTT 入社．以来，要求分析手法，権利流通プラットフォーム等の研究開発に従事．現在，NTT セキュアプラットフォーム研究所主任研究員．

多田 好克 （正会員）

1985 年東京大学大学院工学系研究科情報工学専門課程博士課程修了．工学博士．同年電気通信大学電気通信学部電子情報学科着任．現在，情報システム学研究科情報システム基盤学専攻教授．並列・分散システムの記述法に興味を持ち，OS やシステムソフトウェアの実現法に関する研究に従事．ACM 会員．