社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－MBL－36（2）
2006－UBI－10（2）
2006／2／16

Wonder 発見・共有の為の体感的ナビゲーション

田中 英里香[*1]　西木 健哉[*1]　宮本 洋[*2]　黒澤 雄一[*2]　玉山 尚太朗[*2]
[*1]日立製作所システム開発研究所　[*2]日立製作所デザイン本部

概要：情報機器や無線通信技術の進歩に伴い,いつでも,どこからでも情報にアクセスできるユビキタス環境が整ってきた．しかし利用者にとって安全で快適なユビキタスネットワーク社会を実現する為には,ユビキタス環境に適したセキュリティ管理を行うこと,利用者の意思を反映し利用者をサポートすることが重要である．本稿では,ユーザの位置情報やサービス利用場所の状況等に応じて認証・認可ポリシを適用する「状況依存型認証・アクセス制御機能」を持つ認証制御エージェントと,易しい端末操作でユーザの興味・意思(ポリシ)をシステムに反映し,サービスの存在を近接ユーザに通知する「気づきコミュニケーション」システムを提案する．

Real navigation for “Wonder” discovery and sharing

Erika Tanaka[*1]　Kenya Nishiki[*1]　Yoh Miyamoto[*2]　Yuuichi Kurosawa[*2]　Shotaro Tamayama[*2]
[*1] Hitachi, Ltd., Systems Development Laboratory　[*2] Hitachi, Ltd., Design Division

Abstract：As the advance of information instruments and the wireless communication technology, the ubiquitous environment that we can access information at any time, from anywhere is in order. The security management that suit for an ubiquitous environment and to reflect user’s intention and to support the user is important for realization the safe and a comfortable ubiquitous network society for the user. In this paper, we propose the authentication and access control agent that has “Context-Aware authentication and access control” function can authenticate and access control based on user’s location data and the situation of the place that provides service, and the “Communications using awareness” system that reflects user’s interest and policy by an easy terminal operation and notifies the existence of service to the adjacent user.

1．はじめに

情報機器や無線通信技術の進歩に伴い,いつでも,どこからでもネットワークを利用して,あらゆる情報やコンテンツにアクセスできるユビキタス環境が整ってきた．ユビキタスネットワーク社会では,例えば会社から訪問先へと出張する際,電車やタクシーといった移動手段の中や街角のホットスポットからでも自分のオフィスにリモートアクセスできたり,訪問先のネットワークやプリンタなどのデバイスが利用できたりということが実現しつつある．この様な自由で使いやすいネットワーク環境が発達する一方で,通信内容の漏洩や不正な情報へのアクセスによってユーザのプライバシが侵害されたり,データの改竄が行われたりするなどの危険性が増加している．これらの危険性から利用者を守り,利用者にとって安全にサービスを提供できるユビキタスネットワーク社会を実現するためのサービスプラットフォームの整備が必要である．ユビキタスネットワーク環境の特徴は,人が絶えず動きながらサービスを利用し,その環境の変化が激しいことである．そのため,ユビキタス環境におけるセキュリティに対する考え方は従来と大きく異なると考えられ,単に強固な認証を実現するだけでは不十分であり,セキュリティとユーザ利便性やプライバシ保護との両立が必要である．すなわち,セキュリティの確保が簡単なユーザ操作によること,異なるネットワークや機器に跨って運用ポリシの統一性があること,場所や環境が変わっても継続して安全性が確保されること等がユビ

キタスサービスプラットフォームに期待されており，新たな研究開発が必要である[1]．

本稿では，従来の中央集中サーバで認証を処理する形ではなく，分散配置されたエージェントがサービスを提供する場の状況に適した認証・認可を行う分散連携型アーキテクチャを提案する．これにより，大量のユーザのアクセスや移動が発生しても充分なスケーラビリティを確保し，またセキュリティポリシの設定も柔軟に変更が可能なため，コンテキスト・アウェアなサービスを迅速に提供できる．また，ユーザの意思や好みをシステムに反映し，サービスの存在を近接ユーザに通知するシステムを提案する．これにより容易な端末操作でユーザ主導でのサービス利用を実現できる．

2. ユビキタス認証制御プラットフォーム

2-1. 分散認証ネットワーク

ユビキタスネットワーク環境においては，ユーザや端末が移動を伴いながらアプリケーションやサービスを利用する．このような場合，従来の認証システムでは，セキュリティポリシが異なるドメイン間をユーザが移動し，サービスを利用する度に新たな認証やセキュリティの設定を行う必要があり，ユーザにとっては負担となる問題がある．ユビキタス環境を利用するユーザには，ユーザに負担なく高度なセキュリティを提供しながら，シームレスな移動が可能なシステムであることが望まれている．そこで，図1のような認証及び鍵交換処理を統一的に行えるモデルを提案する．認証制御エージェントは，ローカルなネットワークドメイン毎に分散配置することにより，状況変化に合わせて自律的にドメイン毎のセキュリティポリシを変更することが可能となる．また，認証制御エージェントの導入により，別のドメインのエージェント，あるいは連携インターフェースを備えた既存の認証システムとユーザの認証情報を交換し，エンドツーエンドで認証が完了するように構成することも可能なモデルである．そのため，ユーザは一度の認証でドメイン移動後も再認証の必要なく，サービスを利用できる．

2-2. 状況依存型認証・アクセス制御技術

ユビキタスネットワーク環境に存在するリソースへの適切なアクセス制御を行い，ユーザが即座にサービスを享受できるようにするセキュリティを提供することが重要であるが，リソースの種類や数量が膨大になれば，ユーザ毎に状況に応じた異なるアクセス制御ルールを管理者が事前設定することは困難である．

この課題を解決するため，認証制御エージェントは状況に応じて適切なセキュリティポリシを自立的

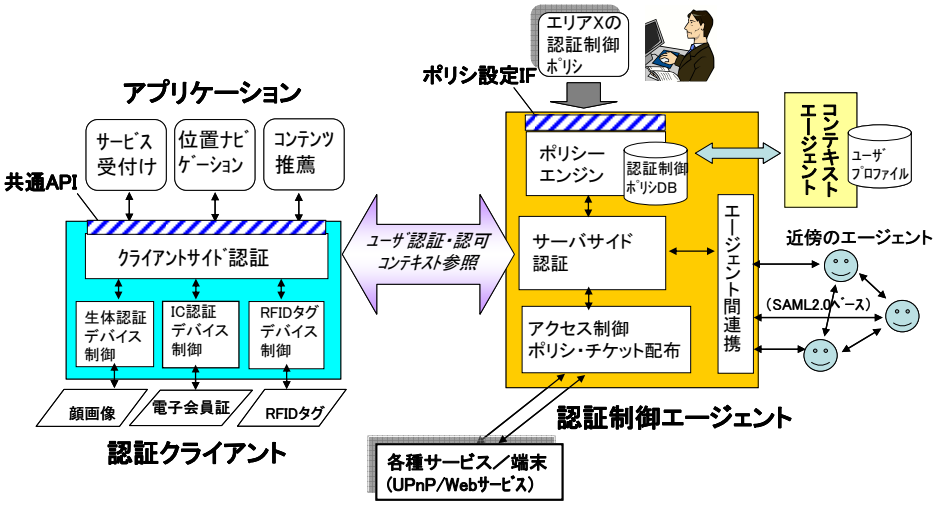

図 1　認証制御プラットフォームの基本構成

に選択可能なポリシーエンジンを有している．認証クライアントからのアクセス要求を受けると,ポリシに基づきユーザを認証して認証チケットを作成し,サービスへのアクセス認可を行う．無線LANの認証で使用されているEAP(Extensible Authentication Protocol)[2]を拡張し,クライアントとエージェントの間で認証方法のネゴシエーションを行う．エージェント同士は信頼関係を構築し,認証情報やコンテキスト情報を交換する．すでに認証済みのユーザがネットワークドメインを移動した場合は,移動後のエージェントが移動前のエージェントから認証チケットを取得し,有効性を確認したらアクセスを許可する．認証クライアントを認証した後は,各種サービスへのアクセス認可制御を行うため,ユーザのコンテキスト情報を管理しているコンテキストエージェントと連携し,ユーザの属性情報やコンテキスト情報を基にしてアプリケーションやデバイスへのアクセス制御ルールを生成して配布する．

認証クライアントはユーザ端末で動作し,認証制御エージェントの指示に従って認証処理を行う．各種認証手段をサポートしており状況に応じた認証方法での認証が可能である．認証制御エージェントから取得した認証チケットを管理し,ユーザ移動時のシングルサインオンや再認証要求に利用する．

本モデルでは,認証・認可のための共通 API やセキュリティポリシ設定 IF を提供することにより,アプリケーションやサービスの開発を容易にしている．人や端末の移動によりエリア内の状況やネットワークを構成する要素が刻々と変化する環境においては,全ての状況を予め想定してポリシを設定しておくことは難しく,ルールベースのセキュリティポリシでは必要なセキュリティレベルを保つことができない．そこで,ポリシーエンジンでは内部に状態遷移マシン及び状態遷移表をベースにXMLで書かれたルール定義ファイルを有している(図 2,図 3)．

図 3のように, 環境内に設置された各種センサ等からコンテキストを収集し, コンテキストに変化が

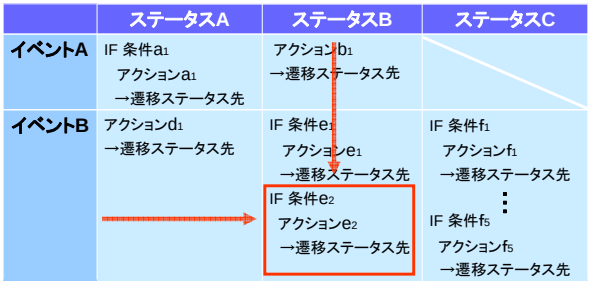

図 2 状態遷移表を用いたルール定義の形式

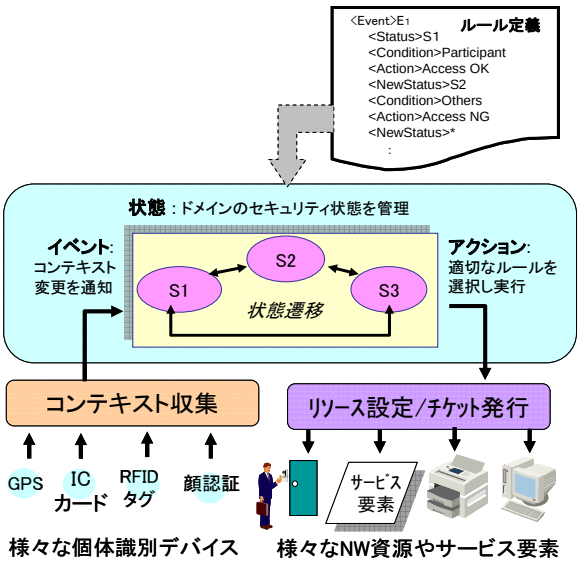

図 3 状況適応型認証制御エージェントシステム

生じるとそれがイベントとしてポリシーエンジンに通知される．ポリシーエンジンは, 図 2のように, 受け取ったイベントの内容とその時のエリアのステータス情報を基に, ルール定義ファイルからルールを選択し, アクションを決定する. また必要に応じてステータスを変化させる. これにより, 状況の変化に対応可能なポリシ選択機能を実現している．

3. 気づきコミュニケーションシステム

3-1. 気づきを支えるコンテキストエージェント

情報過多の現在,ユーザに通知される多くの情報を全て受信しなくてはならない状況は,ユーザにとって負担になりかねない．しかし,まず情報の存在とその重要性を知らせることができれば,ユーザに情報の取捨選択の自由を与えることにより,情報過多のストレスからユーザを救うことが出来る．逆にユーザが気づいていないサービスやコンテンツの存在を通知し,利用可能な場所に誘導することにより,ユ

ーザに新たな発見を与えることができる.

気づきコミュニケーションシステムでは2種類の「気づき」をポイントとしており,1つはシステムからの通知によってユーザにサービスやコンテンツの存在を「気づかせる」こと,もう 1 つは,ユーザが気に入った,おもしろいと思ったものや人に「気づく」ことである. この、ユーザがふと発見した興味の惹かれる対象をWonderと呼ぶ。見本システムでは,ユーザのWonderへの気づきを検知し,それをWonderListやバディリストとしてユーザコンテキストエージェントが管理し,これらをもとに,ユーザに推薦すべきサービスやコンテンツがあった場合や,バディからの呼び出しがあった場合に,ユーザコンテキストエージェントはユーザに通知を行い,ユーザにサービス等の存在を気づかせることができる(図 4).

図 4 気づきコミュニケーションシステム構成

3-2. 体感的マスコット端末の試作

3-1 節のサービスを提供するためには,容易な操作でユーザの気づきをシステムに反映し,システムからの通知を受けてユーザに気づきを与えることが必要である. また,ユーザ主導型のサービスを実現するためには,2 章で述べたようにシステム管理者がセキュリティポリシを設定するのみならず,サービスを利用するユーザ自身が自分のプロファイル情報を公開するかどうか,どのようなサービスを利用したいかなどのユーザの意思やポリシをシステムに反映することも必要である. 従来ではPCなどを用いてWeb画面等から設定する必要があるが,より簡単でかつ直感的な操作でユーザの意思を汲み,気づきを支えることができる端末を試作した（図 5).

図 5 マスコット端末

端末に要求される機能としては,ユーザを識別すること,ユーザの位置を検出すること,システムからの通知をユーザに気づかせること,ユーザの気づきをシステムに反映することである. 試作したこのマスコット端末には,パッシブ型RFID,アクティブ型RFIDが付けられており,端末の固体識別や位置情報の取得が可能である. また微弱無線受信部,モータ,LED,スピーカが搭載されており,サーバから通知を受けるとモータの振動,LEDの発光,音声の発生などでユーザに気づきを与えることができる. 他にも赤外線送受信機能を有しており,図 6のようなボックスから赤外線通信によってIDを受信する.

図 6 Wonder ID 発信機との通信

状況適応型認証制御エージェントシステムと本マスコット端末を用いて,ショッピングモールを想定した「ユビキタスショッピングナビゲーションシステム」の試作を行った.

4. ﾕﾋﾞｷﾀｽｼｮｯﾋﾟﾝｸﾞﾅﾋﾞｹﾞｰｼｮﾝの開発

総務省委託研究グループであるNTT,大阪大学と連携し,ユビキタスショッピングナビゲーションシステムを構築した. このシステムは日立の上記の認

証技術・気づきコミュニケーションシステム,NTTのサービス合成技術,大阪大学のコンテンツ推薦技術を連携させたものであり（図 7）,マスコット端末を利用したお気に入り商品のブックマークや個人向けのコンテンツ推薦が行えることが特徴である.

ショッピングモール内において認証制御エージェントが複数のゾーンに分散してアクセスを制御している. 受付にてユーザ登録を済ませたユーザにマスコット端末（ワンダーキャッチャー）を貸し出す. マスコット端末に備えられたアクティブタグとエリア毎に置かれたリーダによってユーザの位置情報を検出し,ユーザがエリア内に移動してきたことが検出されると,認証制御エージェントはエージェント間で引き継いだ認証情報を基に作成したサービスチケットを合成エンジンに渡しシングルサインオンを可能にする.

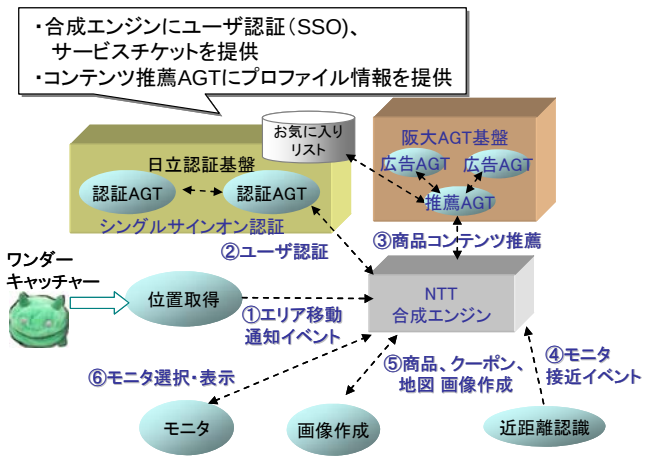

図 7 「ﾕﾋﾞｷﾀｽｼｮｯﾋﾟﾝｸﾞﾅﾋﾞｹﾞｰｼｮﾝ」システム構成

また同時にコンテンツ推薦エージェントにユーザのプロファイル情報を渡し,これをもとに推薦エージェントがそのユーザに適したコンテンツを検索する. そのエリア内で推薦するコンテンツがある場合, マスコット端末に通知され,ユーザに「気づき」を与える. 通知されたユーザは,近くのディスプレイ等の表示デバイスでコンテンツを確認できる.

またWonder ID発信機が各商品を紐付けられており,ユーザが気に入ったりブックマークしておきたいと思った商品(Wonder)を見つけた場合,その Wonder ID発信機をマスコットでくわえるだけで（図 8）,商品IDをキャッチすることができ,そのユーザのためのWonder List(お気に入りリスト)が作成される. そのWonder List を参照しコンテンツが推薦されるため,ユーザの好みにより適したサービスが通知されるという双方向システムである.

ショッピングナビゲーションの拡張として,ワンダーシェアサービス,今どこサービス,My Groupサービスを試作した（図 9）.

図 8 パンプスの Wonder ID をキャッチ

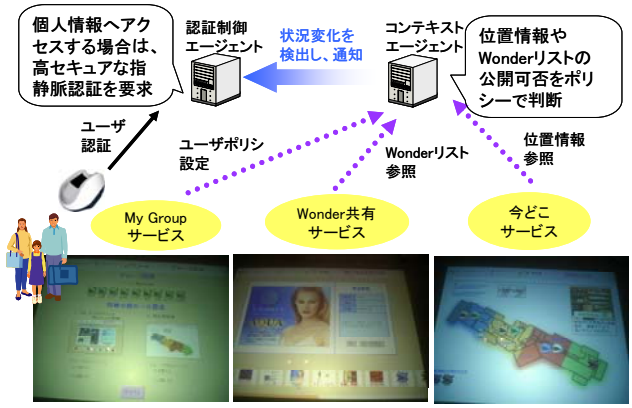

図 9 気づきを支えるｺﾐｭﾆｹｰｼｮﾝｻｰﾋﾞｽ

ワンダーシェアサービスとは,マスコット ID を送信し合うことで,その場で簡単にグループを作ることができるのだが,そのバディ同士で Wonder List を交換し合えるコミュニケーションサービスである. また今どこサービスとは,同じくバディが今どこにいるのかを確認することができるサービスであり, 位置情報はアクティブタグを検出することで得ている. My Group サービスとは,バディリストを確認できると共に,バディに対して Wonder List や位置情報を公開する否かのポリシをユーザ自身で設定できるサービスである. これら WonderList,バディリスト,位置情報,ポリシといったコンテキストをユーザ

コンテキストエージェントが管理しており,適切なアクセス制御を行う．また認証制御エージェントにおいてサービスに応じたセキュリティレベルを管理しており,自分の Wonder List を参照する場合はマスコット端末が認証された際に発券されるサービスチケットがあればよいが,バディの Wonder List や位置情報といったプライバシに関わる情報にアクセスする場合は,生体認証等の高レベルの認証方法で認証されないとアクセス出来ないようにし,セキュリティを確保している.

4. 考察

4-1. 状況依存型認証・アクセス制御に関する考察

今回のユビキタスショッピングナビゲーションシステムでは,認証制御エージェントの役割としてはユーザ認証の要・不要を判断し,シングルサインオンを実現すること,推薦エージェントに対してユーザのプロファイル情報を渡すことにとどまっており,状況に応じた認証やアクセス制御を十分に行えていない．しかしながら,そのようなアクセス制御を行った場合には,ユーザに対してより細やかなサービスが提供できると思われる．例えば,ショッピングモール内での音楽配信サービスを提供する際にも,一般のユーザに対しては今流れている曲やそれが購入できるお店の情報を提供するだけだが,モールの会員やゴールド会員には,その曲の PV をダウンロード可能にしたり,コンサートチケットの優先予約券を発券したりといったように提供するサービスに違いを出したい場合がある．音楽配信サービスに限らずコンテンツに応じて異なるサービスを提供したい場合に,認証制御エージェントがユーザを認証し,利用者の属性等のコンテキストに応じてサービスチケットを発券することによって,サービス提供サーバにおいてはそのチケットに従ってサービスを許可すればよく,サーバ毎でユーザ管理や細かな設定を行う必要がなくなる．このような柔軟なサービスを提供する際にも本提案手法は有効である.

4-2. マスコット端末の他端末との比較

本マスコット端末は,バイブレータや音声でユーザに通知する機能,無線通信機能,商品等の情報を記憶する機能を有している．これらの機能は携帯電話や PDA によっても実現可能であるが,本稿においてマスコット端末を提案した理由は,ユーザに温かみを与えられる端末であると考えた為である．本章において,携帯電話・PDA と比較し本マスコット端末の長所および欠点について述べる.

マスコット端末の長所

- WonderID 発信機をくわえるという単純な操作の為,情報機器に不慣れな人にも容易に使え,自分の意思や興味をシステムに反映できる
- ユーザに楽しさ・面白さを与えられる温かみのある端末である
- 室内においても位置検出が可能である

マスコット端末の欠点

- 表示機能を持たない為,ユーザに情報が伝わり難い,提供できる情報量が少ない

5. 今後の予定

本稿では, ユビキタス環境において場のコンテキストに適した柔軟なユーザ認証とアクセス制御を実現する認証制御プラットフォームおよびサービス支援システムについて述べた. 今後は, 実証実験により評価を進める. まずは 2006 年 2 月から 1 ヶ月間青森県のショッピングモールにおいて実証実験を行う.

謝辞

本研究の一部は, 平成 15-17 年度総務省「ユビキタスネットワーク認証・ エージェント技術の研究開発」の研究助成によるものである.

参考文献

［1］ 情報処理学会研究報告, ユビキタスコンピューティングシステム, IPSJ-UBI04005012 , Vol.2004 No.66, 西木 健哉, 坂田 匡通, 田中 英里香
[2] Extensible Authentication Protocol, http://www.ietf.org /internet-drafts/draft-ietf-eap-rfc2284bis-09.txt
[3] SAINT Workshops 2005: 200－203, Authentication and Access Control Agent Framework for Context-Aware Services, Kenya Nishiki, Erika Tanaka