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

2004－UBI－5　(12)
2004／6／21

位置関係に基づく動体認証及びアクセス制御機構

西木　健哉　　坂田　匡通　　田中　英里香

日立製作所　システム開発研究所

概要：いつでも、どこでも自由に接続できるユビキタスネットワークの普及とともに、アイデンティティの窃盗やサービスの不正利用の脅威が増している。本稿では、ネットワークに接続するユーザ・端末数が飛躍的に増大しても高速かつ信頼性の高い認証を実現するため、認証制御エージェントによる分散処理アーキテクチャを提案した。その特徴は、ユーザの位置関係等のコンテキストに応じて最適な認証・認可ポリシーを適用するコンテキスト・アウェア認証機能、ユーザの移動時に再認証の手間なくサービスを継続する異種ドメイン間認証連携機能などであり、機能試作により有効性を確認した。

Location-based Authentication and Access Control Mechanism for Ubiquitous Mobile Nodes

Kenya Nishiki　　Masayuki Sakata　　Erika Tanaka

Systems Development Laboratory, Hitachi, Ltd.

Abstract: With the recent advances of ubiquitous network infrastructure, theft of personal identity and illegal use of services have become serious problems. In this paper, we propose distributed system architecture based on authentication control agent in order to construct the high performance and high reliable platform. Authentication control agent provides context-aware authentication function which enables selection of adequate security policy in response to the present context and inter-domain authentication function which enables service roaming without re-authentication.

1 はじめに

近年、無線技術やフォトニック技術の進展とともに、地球上のあらゆる場所までネットワークが張り巡らされ、遠隔のユーザ同士が自由に会話したり、大容量の映像コンテンツを簡単に視聴できるようになる。一方これに伴い、個人情報への不正なアクセスや機密データの漏洩によって、ユーザのプライバシーが侵害されたり、データの遺失が発生したりする危険性が増加しており、これらの危険性を排除し、安心してコミュニケーションや電子商取引を行える信頼性の高いサービスプラットホームの整備が急務である。

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る。単に強固な認証や暗号化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ー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、接続するネットワークや使用機

器の詳細な知識を要求されないこと、異なるネットワークや機器に跨って運用ポリシーの統一性があること、ユーザの利用や行動を過度に監視しないこと、認証や暗号化のための処理遅延を最小限にとどめること、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ホームに期待されており、新たな研究開発が必要である[1]。

本報告では、従来の中央集中サーバで画一的に認証を処理するのではなく、ローカルに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最適な認証・認可を行う分散連携型アーキテクチャを提案した。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ーの設定も柔軟に変更が可能なため、コンテキスト・アウエアなサービスを迅速に提供できる。

2 ユビキタス環境におけるセキュリティの課題とアプローチ

本章では、モバイルユーザや機器の認証、その移動における認証の連携、及びサービスに対するアクセス制御について技術課題を述べる。

2.1 モバイル認証技術に関する課題

ユビキタス環境下では機器レベルからネットワークレベル、アプリケーション・コンテンツレベルにいたるまで様々なセキュリティを必要とするが、複数の認証方法や暗号化方法を組み合わせて常に高いセキュリティを得ようとする従来のアプローチでは、多くの計算機資源が必要となり、ユーザは煩雑な操作を強いられる傾向が強い。ユビキタスネットワークに利用される小型の端末やセンサーノードにはパワーおよびストレージは充分備わっていない。そのため、ユビキタス環境で利用できる限られたリソースにあわせた、セキュリティソリューションを考えなければならない。

そこで認証時にモバイルユーザやモバイル機器の位置・時間・環境などに関するリアルタイム情報を収集することにより、コンテキストに最適な認証方法を選択させたり、認証に必要となる秘密情報（クレデンシャル）を効率的に管理することが可能な認証プラットホームを実現する。そのためには、既存の認証システムとのシームレスな連携が必要であり、また認証手段の特性を考慮したモバイル端末向けの柔軟な認証プロトコルの開発が必要である。

2.2 移動ユーザに対する認証連携技術に関する課題

ユーザや端末が移動しながらアプリケーションやサービスを利用する場合、セキュリティコンテキストを移動先のドメインに転送し、新たな認証やセキュリティの設定を行う必要が生じる。しかしユビキタス環境を利用するユーザはあまり目立たないシステムを求めている。「目立たない」という意味は、ユーザに何度もパスワードを要求したり、あらゆる所でバイオメトリックス機器が照合を要求したりしないシステムのことである。個人にとって、高度なサービスと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。

そこでインターネット上で管理されている個人のＩＤ情報とRFIDタグ等で識別可能な実世界のＩＤ情報との関係付けを管理し、 従来レイヤ毎に提供されていた認証情報を一元的に管理し、 セキュリティポリシーの異なるドメイン間で認証関連情報を安全に交換しシングルサインオンを行うことが可能な認証プラットホームを実現する。ユーザや端末が移動した場合に再認証を必要とせずにサービスやアプリケーションを継続して利用できるようにするためには、ユーザの移動（位置）をリアルタイムにトラッキングして認証状態の引継ぎを短時間で効率良く行うことが必要である。さらに、個人情報をインターネット上で管理し交換する場合には高いセキュリティが必要であり、認証プラットホーム自身が不正アクセスやサービス不能攻撃に対するロバスト性や、ネットワーク構成の変化に柔軟に対応可能な自律性を持たなければならない。また、プライバシー保護の観点からは、ユーザの同意に基く情報開示コントロールやユーザの属性やコンテキスト基づいて匿名アクセスを実現する必要がある。

2.3 アクセス制御技術に関する課題

ユビキタス環境下の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“Place and Play”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になり、ユーザが持ち込んだ情報機器へのアクセスに関しても不正なアクセスを防ぐ手段を提供する必要がある。

そこでデータの暗号化、情報機器間の連携、複数ユーザ間の競合解消等を行うための制御ルールを自動生成し、対象機器にリアルタイムに設定・実行可能であり、前記の利用者認証技術と協調させることにより、移動時や構成変更時にも適切なセキュリティを確保可能なプラットホームを実現する。そのためには、システムの構成や状況が常時変化し、同時に確保するべきセキュリティレベルも変動することを前提にして、セキュリティレベルをリアルタイムに把握することが課題となる。ネットワークに接続された端末・機器を自動検出し、多数のセンサー情報を収集してコンテキスト情報として統合していくことや、システムの構成や状況に応じたセキュリティポリシーを管理者や利用者が簡単に定義・変更できるユーザインターフェースも必要である。

3　認証制御プラットホーム

前章で述べた課題を解決するために、認証処理やアクセス制御処理をエージェントが代行する分散連携型アーキテクチャを開発した。

3.1 基本アーキテクチャ

従来モデル（図１）では、ユーザ認証・クライアント端末認証をサーバ毎に独立して行っており、その認証手段や鍵交換方法は統一されていない。従って通常は、無線 LAN 接続時にパスワード認証を行い、VPN 接続時に IC カードの電子証明書により認証し、さらに業務アプリケーションへのアクセス時に生体認証を行うというように複数回の操作を要求されることになる。どの認証手段をサポートするかはプロトコルや実装に依存しているため、すべてのサーバで共通化することも容易ではない。

提案モデル（図２）は、ユーザ（クライアント）とサーバの双方が信頼するTrusted 3rd Party（TTP）を導入して、認証及び鍵交換処理を統一的に行わせるモデルである。このTTPを認証制御エージェントと呼ぶことにする。認証制御エージェントは、ユーザ情報やセキュリティ権限を管理することになるため、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、情報管理リスクを下げるとともに、状況変化に合わせてセキュリティポリシーを変更することも自律的に行うことが可能になる。ユーザは、利用サービスをその場で選択すれば、それに必要な認証を一度行えば済むようにしたい。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（デレゲーション）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。

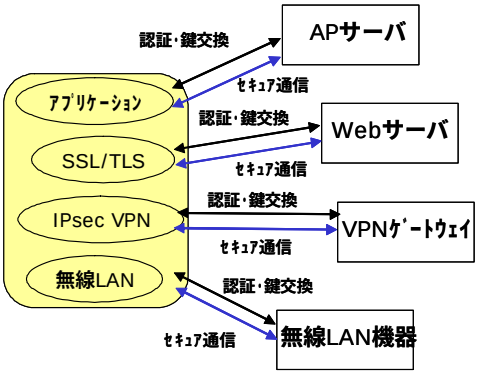

図１　サーバ独立認証モデル

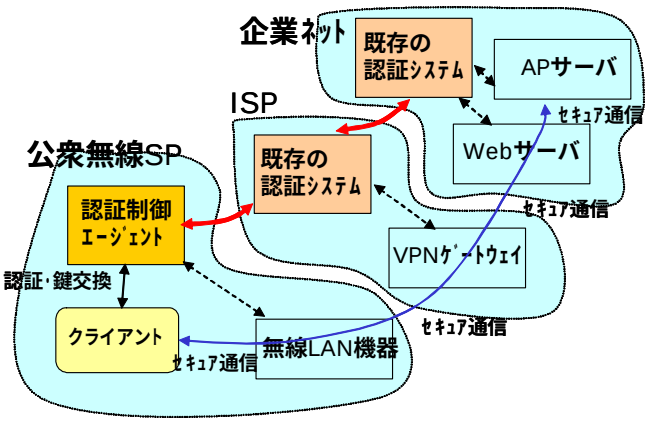

図２　ＴＴＰ認証モデル

図３に認証制御プラットホームの構成を示す。

(i)　認証制御エージェント

特定のネットワークドメイン内の認証をポリシーに基づき制御する。認証クライアントからのアクセス要求を受けてユーザを認証し、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。

認証されたユーザに対しては、さらに、ユーザのコンテキスト情報（所持している端末やトークンの ID 情報、ユーザの位置情報など）も管理する。

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、配布を行う。

(ii)　認証制御クライアント

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インタラクティブに認証処理を行う。認証手段として、ＩＤ・パスワード認証だけでなく IC カード、RFID 等物理トークンを用いた認証や、各種生体センサーデバイスによる認証をサポートする。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。

(iii)　アプリケーション

認証制御プラットホームは、クライアントアプリケーションに対して認証・認可用の共通 API を提供し、サーバアプリケーションに対してアクセス制御ポリシー設定用の共通 API を提供する。アプリケーションに依存する部分は個別に実装する必要があり、今回は以下のモジュールを開発した。

・JXTA グループ管理モジュール

P2Pプラットホームのひとつである JXTA[3]上で動作する、音声／ビデオチャット、コンテンツ共有等のコラボレーションアプリケーションに対して、認証やアクセス制御等のセキュリティ機能を提供する。

・UPnP コントローラモジュール

UPnP[4]対応デバイスを利用するアプリケーションに対して、認証やアクセス制御等のセキュリティ機能を提供する。

・UPnP 対応デバイス制御モジュール

認証制御エージェントから配布されたアクセス制御ポリシーに基づいて、情報機器に対するアクセス制御機能を提供する。

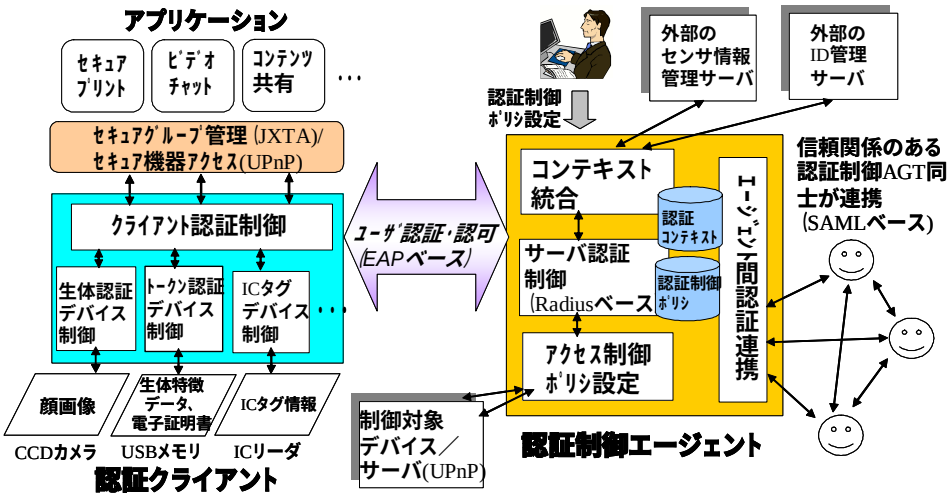

図３　認証制御プラットホームの基本構成

3.2 認証制御エージェント機能

以下にエージェント機能の詳細を述べる。

（1） コンテキスト・アウェア認証機能

場所の種別や許容できる利用人数、ユーザの属性（所属・役務・優先対象かどうか）や振る舞い、端末の種類などの状況をエージェントが判断して最適な認証・認可を実行する機能である。ローカルに分散配置された認証制御エージェントが、従来は端末とサービスの間で独立に行っていた認証を一括して代行する。

離れたドメインにある端末同士がセッションを確立する場合も、それぞれがローカルの認証制御エージェントで認証した後、エージェント同士が連携してセキュア通信を行う。その際、認証データのトラフィックはユーザデータのトラフィックと分離可能とし、高速かつセキュリティの高い認証を実現する。

ICカード等の物理トークンを用いた認証後に一時的に有効な認証チケットやアクセスチケットを発行し、物理トークンを端末に装着することにより可搬なサービスを実現する。ここで認証チケットは、Webサービスセキュリティの標準仕様であるSAML(Security Assertion Markup Language)[5]をベースとし、エージェントの収集したコンテキスト情報を扱えるようにタグを定義した。

さらに、IC タグリーダーを備えた端末により、サービスエリア内に設置された IC タグを読み取ることにより、サービスや場所に関連するコンテキストを収集し、これを用いてサービスや場所に適した認証方法を選択可能とすることにより、サービスに適した認証を実現する。

（2）異種レイヤ/ドメイン間認証連携機能

ユーザが異なるネットワークを移動時に、エージェントがユーザの現在位置を把握し、シングルサインオン認証によりサービスを継続する機能である。

認証制御エージェントが、サービスの利用に必要なリソース（ネットワーク接続や情報機器）を仮想的に統合し、レイヤ間での認証関連情報の伝達を行う。現状は、ネットワーク/アプリケーションレイヤ毎に個別設定や認証処理が必要なためユーザにとって負担が大きく、コンテキスト（誰が、いつ、どこから、何に対してアクセス）に応じたセキュリティの動的確保が困難である。そこで端末側に認証制御エージェントとの間でレイヤ横断的にユーザ認証及び鍵交換を実行する認証クライアントを載せることにより、ユーザは制御された一度の認証で複数のレイヤのセキュリティを確保できるようになる。また、認証クライアントは多様な認証手段をサポートし、新たな拡張が可能な方法で実装する。

ドメイン間で認証制御エージェントが連携する場合には、移動先のドメインのコンテキストやセキュリティレベルによって連携可否を判断し、また相互に同意したプライバシポリシに従って ID 情報の交換・共有を行う。

（3）アクセス制御ポリシー自動構成機能

Plug&Play で接続されたサーバや情報機器に対して、エージェントが動的にアクセス制御ポリシーを設定し、ユーザに一時的な利用を許可する機能である。

ユーザ認証結果や位置情報を含むコンテキスト情報を基に、アクセスインターフェースを持つ情報機器サーバ（プリンター、プロジェクタ、ネットワークカメラ等）やネットワーク機器に対する制御ルールを生成し、設定を行う。機器の自動発見、コマンド実行等には UPnP を拡張したプロトコルを使用する。

ユーザは要求時にアクセスチケットを提示し、アクセスされた機器はアクセスチケットと配布された制御ルールを照らし合わせてアクセス可否を決定する。

4 位置関係に基づく認証及びアクセス制御方法

前章で述べたコンテキストに基づく認証及びアクセス制御は、静的なルールを当てはめるのではなく、場の安全度及び信頼度を求め動的に判断することが特徴である。まず、サービスエリアの種別、システムの構成要素の種別、参加者の役職や責任などの情報を収集してシステムに要求される安全度を数値で求め、実際に利用するユーザの所属、アクセスしている場所、アクセスの過去の履歴などの情報を収集して

ユーザの信頼度を数値で求める。サービスエリアの管理者は、安全度及び信頼度の組に対してあらかじめ認証レベルを設定し、それを参照して最適な認証・認可処理を実行する。サービスエリアに参加（ログイン）あるいは離脱（ログアウト）したユーザ/機器の情報は、システムの状態にフィードバックされる。

このようにして単に本人確認を行う認証ではなく、状況に応じてきめ細かいセキュリティポリシーを適用しようとすると従来よりも認証処理の負荷が増えることになる。ネットワークに接続するユーザ・端末の数が飛躍的に増大した場合でも、効率的に処理し、ユーザの利便性を低下させないようにしたい。例えば、団体旅行ツアーが空港内での様々な手続き（チェックイン～保安検査～搭乗チェック～機内サービス）であるとか、観光地での施設の利用を行う場合に、ツアーの責任者あるいは案内人が代表して認証を受け、同じツアー参加者は認証された責任者の監督下でサービスを受けることを想定する。

まず代表して本人認証を行うユーザ（主管ユーザと呼ぶ）と、主管ユーザが存在する場所でサービス利用を許可されるユーザあるいはデバイス（従属ユーザ/デバイスと呼ぶ）で構成されるグループを決定する。ユーザは全て位置を識別可能な無線型物理トークン（ＩＣカード、ＲＦＩＤタグ等）を所持する。認証制御エージェントは次のように動作する（図４）。

（i）主管ユーザを通常の方法で認証する。

（ii）グループメンバに、最寄りの位置リーダに所持するトークンを提示させ、位置リーダから収集したトークンＩＤ及び位置情報のリストを受け取る。

（iii）主管ユーザの認証結果と通知されたトークンの位置情報リストを対応付ける。

（iv）ユーザがサーバにアクセスする時に、所持しているトークンを読み取り、エージェントにアクセス可否を問合せる。

（v）エージェントは認可ポリシーを参照して、サーバにアクセス可否を応答する。

認可ポリシーは、主管ユーザの位置と従属ユーザの位置の関係を用いて様々なポリシーを定義できる。例えば、

- 主管ユーザが同一サービスエリアに存在する場合のみ、従属ユーザのアクセスを許可
- 主管ユーザの存在が確認されない場合は従属ユーザによる再認証によりアクセスを許可
- 主管ユーザの存在が確認されない場合でも一定時間はサービスの継続を許可

さらにアクセスの可否を判定するだけでなく、主管ユーザのアクセス権限を従属ユーザも引き継ぐこともできる。従属ユーザは、再認証を要求されない限り位置登録のみ行えばよいので、認証処理の負荷を軽減することができる。一方、位置制約によって主管ユーザが従属ユーザの管理・監視を行えない状況での利用を排除・制限することにより、一定のセキュリティレベルを維持することが可能と考えられる。

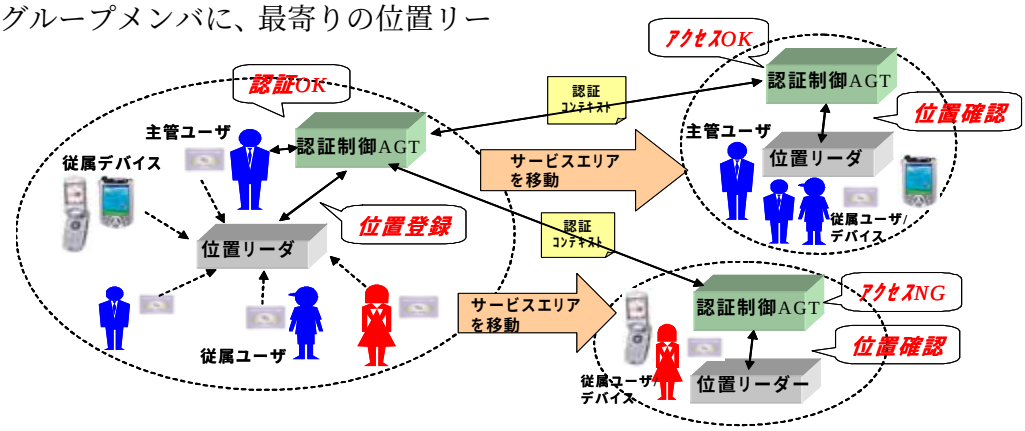

図４　位置制約条件を用いた認証・認可

5　実装例

提案アーキテクチャに基づいて認証制御エージェント及び認証クライアントを実装し、複数のネットワークドメインにまたがってサービスを利用するシナリオで評価した。図４は、ＩＣカード等の物理トークンを利用したシングルサインオンのシナリオの一例を示す。

（i）認証制御エージェント#1 のログイン要求に対してユーザ認証情報及び物理トークンの ID を送る。

（ii）認証が OK ならば、電子署名付き認証チケットを発行し、チケットをトークンに格納。

（iii）ユーザがドメインを移動後、エージェント#2 のログイン要求に対してトークンに格納された認証チケットを送る。

（iv）エージェント＃2 は認証元（エージェント#1）から必要なユーザ情報を取得する。

（v）認証チケットの署名及び有効期限を確認し、ログイン OK ならば、ユーザ端末に対して署名付きアクセスチケットを発行する。

（vi）サーバ機器に対してアクセス要求を送る。

（vii）サーバ機器はアクセスチケットを確認し、アクセスを許可する。

以上は物理トークンが認証チケットを格納できる場合であるが、認証チケットを格納できない RFID タグを利用する場合に、エージェントにおいてタグ毎に認証チケットを管理し、移動時にエージェント間で認証チケットを転送することでシングルサインオンが可能なことも確認した。

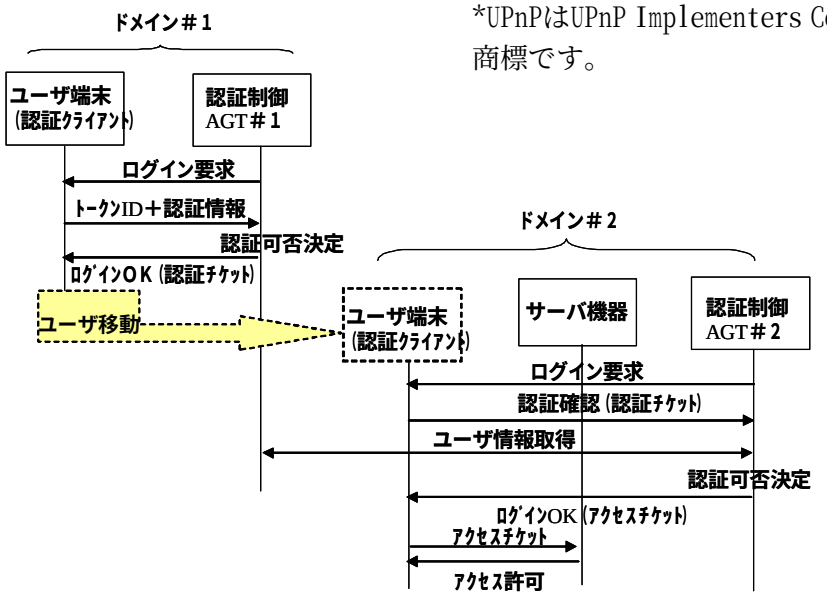

図５　物理トークンを利用した認証連携

6　おわりに

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ホームについて述べた。今後、より大規模なネットワーク環境での実験評価を進める。

謝辞

本研究の一部は、平成 15 及び 16 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] A BOOK OF DOKODEMO NETWORK, ユビキタスネットワーキングフォーラム, 2004 年

[2] Extensible Authentication Protocol, http://www.ietf.org/internet-drafts/draft-ietf-eap-rfc2284bis-09.txt

[3] JXTA, http://www.jxta.org

[4] UPnP Forum, http://www.upnp.org

[5] Security Assertion Markup Language, http://www.oasis-open.org/committees/security