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

2004－ＤＰＳ－117　(36)
2004－CSEC－　24　(36)
2004／3／5

オペレータによる属性情報の安全な提供方法

各務　健太郎　　小栗　伸幸　　関野　公彦

株式会社NTTドコモ　マルチメディア開発部

携帯電話によるモバイルインターネットサービスの普及に伴い，多くのコンテンツが提供されている．オペレータの持つ契約者に紐付く多くの情報を利用者の意思によって提供することが可能であれば，利用者の省力化やサービスの多様化を実現することができる．本稿では，オペレータとの利用契約に基づいた契約者に紐付く情報を，オペレータが利用者の許諾に基づいて提供を行う方式について示す．オペレータが属性情報を提供する上での必須条件とオペレータの管理する属性の定義を行い，携帯電話から要求を行うPush方式とコンテンツプロバイダから要求を行うPull方式についてシステム構成と動作概要を示す．また，利用者の意思を反映することのできるプライバシコントロールの概念と実現方式について示す．

Secure Attribution Providing Method by the Communication Operator

Kentaro KAKAMI　Nobuyuki OGURI　Kimihiko SEKINO

Multimedia Development Department, NTT DoCoMo Inc.

With the popularity of mobile internet service for mobile phones, wide range of contents is becoming available. Information tied to the contractor and which is held by the communication operator can increase convenience for the user and variation of services. In this paper, we propose a method to provide attributes on behalf of the user. We define essential conditions of providing attributes and types of attributes held by the operator. We also show the system structures and the providing sequence of the two methods called “the push method”, requested by the mobile phone, and “the pull method”, requested by the contents provider. Moreover we show the basis and the operation method of the privacy control by which the user can reflect his/her own policy of providing attributes.

1．はじめに

携帯電話によるモバイルインターネットに一般のネットワーク技術が適用されることも多くなっているが，その一つにPKI技術に代表されるセキュリティ関連技術が挙げられる．携帯電話によるオンラインでの決済技術などへの発展により，高度な通信路の安全性や通信対象への信頼性の確保など，モバイルにおいてもセキュリティに関する需要が高まり，現状においても通信の暗号化・サーバの正当性保証を行うSSLサーバ認証は一般の携帯電話によるモバイルインターネットの標準サービスとなり，またNTTドコモのFOMAには，さらにクライアントである携帯電話の認証を行うSSLクライアント認証を行うFirstPassサービス[1]が提供されている．

一方，携帯電話を利用するためには，オペレータと利用者による利用契約が締結され，オペレータは利用者の多くの情報を保持している．携帯電話に対して何らかのサービスを提供するコンテンツプロバイダにとって必要な情報はオペレータが保持している情報と重複することが多い．当然ながら，契約者に関する情報はむやみやたらに第三者に対して漏洩してはならないものであるが，コンテンツプロバイダがサービス提供を行う利用者に関する情報を，利用者の許諾の意思を確実に確認した上でオペレータから属性情報として得ることができれば，利用者がオペレータに対して通知した情報を二重にコンテンツプロバイダに通知を行わなければならない煩雑さや，利用者の入力によって発生しうる誤入力の問題をなくし，利用者の省力化を実現することが可能となる．また，オペレータのみが取り扱うことのできる，利用者の持つ携帯電話の位置情報などのリアルタイム情報を属性情報として得ることができれば，より高度なサービスをより確度の高い情報によって利用者に提供することが可能となる．

本稿では，オペレータが保持している，オペレータと利用者の利用契約に基づく利用者に紐付く情報を属性

情報として扱い，利用者あるいはコンテンツプロバイダからの要求に応じて，利用者の意思を正確に反映した上で，コンテンツプロバイダに対してオペレータが属性情報を提供する方式について示す．

以降，2.において，携帯電話における情報の提供について触れ，3.において，オペレータが利用者に代わって属性を提供するための条件と，移動体通信網において提供されうる属性の種類を示す．4.において，要求のメッセージの送信元によって分けられる2つの実現モデルを中心に携帯電話の利用者に対応する属性情報の提供方式について説明し，さらに属性情報の提供において必須となる利用者の意思を反映させるためのプライバシコントロールの方式について説明する．5.において，結論を述べる．

2. 携帯電話における情報の提供

携帯電話において，利用者に関連する情報が第三者に提供されている例としては，利用者の識別や，携帯電話の現在位置を推定するエリア情報・位置情報などがある．

2.1. 利用者の識別

コンテンツプロバイダなどがサービスを利用者に提供する際に，利用者を何らかの方法によって識別してパーソナライズする必要性が生じるコンテンツが多い．特に，一つの携帯電話からのアクセスは一人の利用者によるアクセスであることがほぼ確定できるため，ランダムな文字入力が難しいといった機器上の制約もあり，一般的な利用者識別方法であるID・パスワード入力よりも，単純なアクセスのみで識別子を通知できる方式を採用した方が利用者の利便性も上がるといったメリットがある．ただし，プライバシの面から，利用者がコンテンツプロバイダを信頼する仕組みである必要がある．

現在，オペレータによって提供されている利用者の識別方法は，以下のように分類される．

- **オペレータ内部網による識別子の付加**
  携帯電話によるコンテンツプロバイダへのアクセスはオペレータの管理する通信網を通過する．その際に，電話番号と一対一に対応する識別子を付加する方法である．オペレータによって公認されかつ利用者によって利用登録を行われたコンテンツプロバイダにのみ識別子の付加が行われるなど，利用者・オペレータ双方の信頼がコンテンツプロバイダに必要である．
- **携帯電話の端末情報の送信**
  携帯電話の端末や内部に格納されたUIMの製造番号など，通信を行う機器を特定する情報を利用者の承諾を得て送信する方法である．利用者のみの操作で送信可能なためコンテンツプロバイダを問わないが，機器が変わってしまうと契約が継続していても同一利用者であることを認識できない．
- **クライアント証明書による相互認証**
  オペレータが認証局を運用し，携帯電話に対しクライアント証明書を発行して，コンテンツプロバイダとのアクセスでSSLサーバ・クライアント認証を行ってクライアント証明書を利用者の意思の下でコンテンツプロバイダに送信する方法である．

2.2. エリア情報・位置情報

携帯電話の現在位置をコンテンツプロバイダに送信して位置に応じたコンテンツを取得する方法として，携帯電話の交信している基地局の設置位置から携帯電話の現在位置を類推し，大まかなエリアとして送信する方法や，携帯電話に搭載したGPSによって位置を測位して送信する方法がある．

双方とも，利用者の同意なしでは位置を表す情報をコンテンツプロバイダに送信することはできず，また第三者からの位置情報要求によって携帯電話上のGPSに測位を行わせる場合には，利用者によって測位の可否の意思を事前かつ測位中に示すことが可能とすることによって，利用者のプライバシに配慮するといった対応がとられている．

3. オペレータによる属性情報の提供

3.1. 属性情報提供を行うための必須条件

オペレータは契約者に関する多くのユーザ情報を持っているが，それを第三者であるコンテンツプロバイダに対して提供するためには，何らかのセキュリティポリシーを定めておかなければならない．満たさなければならない条件を以下に示した．

- **属性情報はあくまで利用者に所有権があり，オペレータは利用者の代行としてコンテンツプロバイダに提供するという前提であること**
  属性情報には個人情報保護法[2]でいう「個人情報」に含まれる情報があり，契約時の利用目的を超えた利用や第三者への提供を契約者に無断で行うことを禁じている．また，電気通信事業法[3]により，電気通信事業者は「通信の秘密」を侵してはならず，通信を行う上でオペレータが知りうる情報を無断で

第三者に提供することはできない.

属性情報の提供をサービスとして実施するには，契約者と改めて契約を締結するか契約内容の変更を行うことによって，オペレータの持つ属性情報はすべて利用者に所有権が存在する情報であり便宜上オペレータからコンテンツプロバイダに利用者の代行の意思を持って提供が行われるという前提を相互で確認し，属性情報提供の実システムにおいてもこの前提が遵守されるものでなくてはならない.

- **属性情報の提供に際して，利用者が必ず提供に対してのイニシアチブを取ること**

  利用者の認知できる範囲外で，オペレータとコンテンツプロバイダだけで属性情報のやりとりを行うことは，利用者のプライバシを大きく損なうことに直結する. そこで，属性情報の提供を行う際には，携帯電話側から意識的に属性情報を提供できるような方式をとることが望ましい. 具体的な方法としては，携帯電話からコンテンツプロバイダに向かう通信が発生した際にのみコンテンツプロバイダに対して属性情報を提供することが可能であることとし，また携帯電話の利用者に対して当該通信の発生によって属性情報をコンテンツプロバイダに提供するということを認知させることとする.

  コンテンツプロバイダ側からのトリガによって属性を要求する方法もサービスによってはあり得るが，事前のコンテンツプロバイダ・オペレータ・利用者の三者間による合意が必須であり，かつ実際の属性提供時には利用者に対して属性を提供することを認知させることが必要である.

- **利用者によって提供の意思を示すことが可能であること**

  オペレータが提供できる属性の中でも，利用者が提供を望むものと望まないものが存在したり，また提供を行うコンテンツプロバイダ毎に提供の可否を判断したいという利用者の要望がある. 事前に提供可否リストを登録したり，逐次確認を行ったりするなど，提供時に利用者の意思を確認し，正確に反映できる仕組みを用意する必要がある.

- **利用者が開示する属性情報について知ることが可能であること**

  利用者の希望に応じて，コンテンツプロバイダに対して提供される属性情報について，携帯電話の画面上に表示するなどの方法で確認することができ，提供の可否を判断する一つの材料とすることができるようにする.

3.2. オペレータが持つ契約者に関する属性の種類

オペレータが携帯電話を所持する利用者に対し，所有する移動体通信網の利用を行わせるための契約を締結し，利用者が実際に携帯電話を利用することにより，オペレータは以下のような情報を契約者に紐付いた情報として取得することが可能となる. プライバシの問題など技術面以外の障壁も大きいが，オペレータは提供を行おうと思えば，利用者の許諾を得た上で以下の情報を属性情報としてコンテンツプロバイダに提供することが可能となる.

- **契約を維持するために必要な情報**

  利用契約の締結の際に，オペレータは契約者の名前・住所・電話番号・生年月日・性別などの個人情報を契約者から取得し，これをデータベース化して，契約者に対して利用料金の請求やカスタマサービスなどを行っている.

  このような情報は，コンテンツプロバイダにとっても携帯電話の利用者とのコンテンツ提供契約を行う際に必要であったり，懸賞などオフラインでの特典提供やサポートを行う際に用いることがある. また，個人の嗜好を性別・年齢・居住地などからパターンに分類してそれぞれに異なるコンテンツを提供するといった使い方も可能となる.

  ただし，利用者とオペレータという二者間の契約によって取り交わされた情報はプライバシの問題に大きく関わり，悪用される可能性が高い情報である. そのため，取り扱いには細心の注意が必要となる.

- **移動体通信網の利用によって知りうる情報**

  利用者は，オペレータが運用する移動体通信網を利用して携帯電話による通話・通信を行っている. この際に，携帯電話が交信している移動体基地局の情報（基地局の設置位置などから，携帯電話の大まかな位置を推測することが可能）・通信状態（待受状態／音声通話中／テレビ電話中／パケット通信中など）・在圏情報（圏内／圏外）など，携帯電話としての機能を提供するために網側で保持している状態をリアルタイムな属性情報として位置づけることもできる.

  ただし，これらは通信の秘密に関わる情報が多いため，契約時の情報と同様に取り扱いや提供には十分な注意を要する.

- **オペレータ提供サービスのユーザ情報**

  オペレータによって，メールサービスやGPSによる位置情報サービスなど，オペレータが運用し基本契約に付随して契約する付加サービスが存在する.

その付加サービスの管理するユーザデータベースと連携し，メールアドレスや携帯電話の位置情報などを取得して属性情報として提供することにより，利用者に対してより多くの属性を持たせることができ，また提供インタフェースの統一により効率的な情報の提供が可能となる．

各付加サービスの利用に際して，基本の回線契約とは別の契約を締結しており，それらのユーザ情報の利用に関してはその契約によって拘束される．

4. 属性情報の提供を行うシステム・方式とプライバシコントロール

4.1. 属性情報提供手法のシステム構成

図1に，オペレータによって利用者の属性情報を提供するシステムの構成を示す．携帯電話はコンテンツプロバイダにゲートウェイを通じてアクセスしている．携帯電話－ゲートウェイ間には基地局までの無線区間が含まれる．ゲートウェイはコンテンツプロバイダと網内部の属性機関と接続している．

携帯電話内にはオペレータから発行されたクライアント証明書をUIM内に格納しており，利用者の正当性をSSLクライアント認証によって確認する．また，証明書内に記述された識別子によって，オペレータ網内の属性機関のみが契約者との紐付けを行うことができる．

属性機関はオペレータ網にある複数のデータベースにアクセスを行い，契約者に対応する情報を抽出することができる．

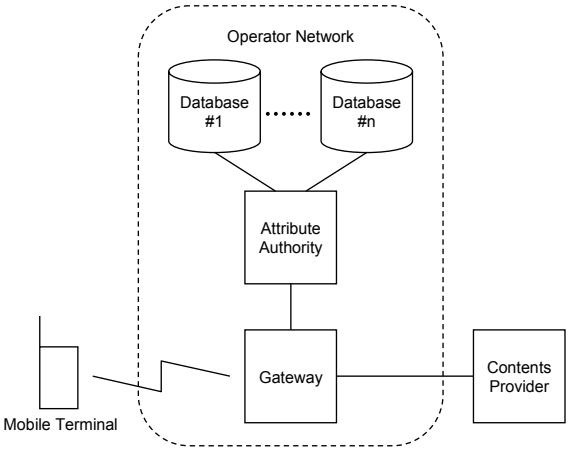

図1：システム構成

4.2. 属性情報の基本的な提供手法

オペレータが契約者に紐付く属性情報を上記システム構成で提供する手法として，以下の2通りがある．なお，本稿では携帯電話側から属性要求のトリガが発せられることを前提とした方式のみを対象とし，携帯電話が属性要求に関して関知しないコンテンツプロバイダ側からのトリガによる属性要求は対象としない．

- **携帯電話から要求が行われる方式（Push方式）**
  実際の属性提供要求メッセージがクライアント証明書と共に携帯電話から発出され，通信網によってその要求を受け取り，属性情報を網内から取得し，コンテンツプロバイダに送信される方式．
- **コンテンツプロバイダから要求が行われる方式（Pull方式）**
  携帯電話からコンテンツプロバイダへのSSLクライアント認証によるアクセスをトリガとして，実際の属性提供要求メッセージがコンテンツプロバイダから発出され，通信網によってその要求を受け取り，属性情報を網内から取得し，コンテンツプロバイダに送信される方式．

4.2.1. Push方式

図2に，携帯電話から実際の属性要求が行われるPush方式について，その動作の概要をシーケンス図にて示す．

携帯電話からゲートウェイに対して，必要な属性情報の提供を指示する要求が含まれた，コンテンツプロバイダに対してのコンテンツ要求がクライアント証明書と共に送信される．コンテンツ要求がゲートウェイによって受信されると，クライアント証明書から契約者を識別する契約者識別子を取り出し，契約者識別子と要求された属性が記述された属性クエリを生成し，属性機関に対して送信される．属性機関は要求された属性の値を該当するデータベースから取得し，属性情報としてゲートウェイに送信する．ゲートウェイはコンテンツ要求に受信した属性情報を付加してコンテンツプロバイダに送信する．コンテンツプロバイダは送信されたコンテンツ要求と属性情報を元にコンテンツを生成して，携帯電話に対して送信する．

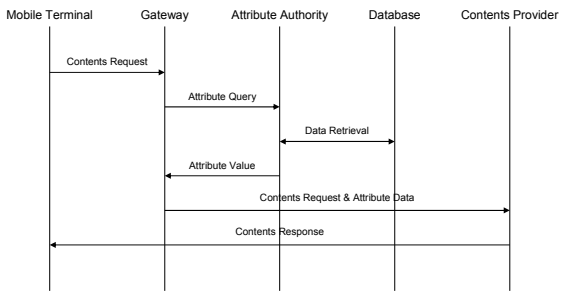

図2：Push方式 シーケンス

4.2.2. Pull方式

図3に，コンテンツプロバイダから実際の属性要求が行われるPull方式について，その動作の概要をシーケンス図にて示す．

クライアント証明書を含む携帯電話からのコンテンツ要求はゲートウェイを介してコンテンツプロバイダに送信される．コンテンツプロバイダは，要求されたコンテンツに属性情報が必要である場合に，クライアント証明書から契約者識別子を取り出し，契約者識別子と要求する属性を記述した属性クエリを生成して，ゲートウェイ経由で属性機関に送信する．属性機関はPush方式と同様に要求された属性に対して属性値を網内のデータベースから取得し，属性情報としてゲートウェイ経由でコンテンツプロバイダに送信する．コンテンツプロバイダは受信した属性情報を元にコンテンツを生成して携帯電話に送信する．

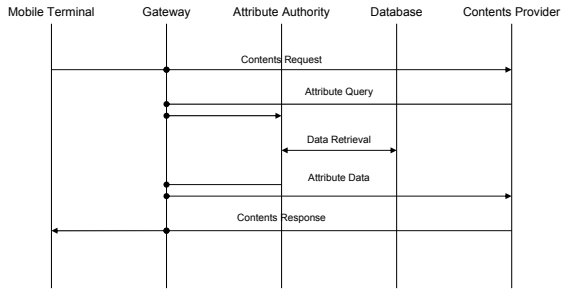

図3：Pull方式 シーケンス

4.3. 利用者意思を反映するプライバシコントロール

4.3.1. プライバシコントロールの必要性

4.2. で示した基本的な属性情報提供手法において，3.1. で示した属性情報の提供に関する必須条件を満たすためには，利用者が全面的にコンテンツプロバイダを信頼することを前提としている．Push方式においては携帯電話から発出されるコンテンツ要求に属性要求も含まれていることを，Pull方式においてはコンテンツ要求によってコンテンツプロバイダが属性要求を行うことがあることを，コンテンツプロバイダが事前に認知させる必要がある．

しかし，コンテンツプロバイダが属性情報を要求する際に利用者に認知させた属性以外の属性を要求したり，また利用者に認知させずに勝手に属性要求を行ったりする可能性は否定できず，4.2. で示した手法においては，コンテンツプロバイダによる上記のような不正を看破する手段をオペレータは利用者に提供できていない．

属性情報をコンテンツプロバイダに提供する際に，利用者の「このコンテンツプロバイダに対しては，この種類の属性は提供してもよい」といった，自身の意思を正確に提供の可否といった形で反映するために，属性機関が提供要求を受けた際に利用者が事前に登録したポリシーに従って，必要ならば携帯電話に対して直接アクセスすることによって，提供の可否を決定することのできるプライバシコントロールの機構を備えることが必要となる．

4.3.2. 利用者の設定するポリシー

本方式におけるプライバシコントロールは，属性機関が属性情報の取得を要求する属性クエリを受信した際に，あらかじめ利用者によって設定され，データベースとして管理されたポリシーを参照して実行される．

ポリシー管理データベースの構造の一例を表1に示す．利用者識別子・コンテンツプロバイダ・属性項目に対応するポリシーが設定されることになる．

ポリシーは属性を開示するコンテンツプロバイダ・属性項目ごとに利用者が携帯電話によって設定することが可能とする．ポリシーの設定を行うユーザインタフェースは，属性機関によって提供される．

設定を行うコンテンツプロバイダ・属性項目の数が増加すると，設定が煩雑となりプライバシコントロールの意義が薄れる危険性を持つため，属性項目を種類毎にグルーピングしたり，全属性項目に対するコンテンツプロバイダ毎一括設定・全コンテンツプロバイダに対する属性項目／グループ毎一括設定などのような設定方式をユーザインタフェースに追加することによって，設定の便宜を図ることが可能である．

表1：ポリシー管理データベースの構造の一例

利用者識別子	コンテンツプロバイダ	属性項目	ポリシー
ABC012	X	a	無条件提供
ABC012	X	b	通知後提供
:	:	:	:
ABC012	Y	a	無条件非提供
ABC012	Y	b	無条件非提供
:	:	:	:
DEF345	X	a	許可後提供
:	:	:	:

利用者がプライバシコントロールにおいてコンテンツプロバイダ・属性項目ごとに設定可能なポリシーは以下の4つである．属性機関はポリシーに従い，必要ならば携帯電話に対して直接アクセスを行って，提供／非提供を決定する．利用者がポリシーを設定する前のデフォルト値としては，いかなるコンテンツプロバイダ・属性項目の組み合わせにおいても無条件非提供とし，利用者

の設定なしに属性情報が提供される危険を防ぐ.

- **無条件提供**
  利用者へのアクションをとらずに，当該コンテンツプロバイダに対する当該属性の提供を常に許可し，即時に提供を行う.
- **通知後提供**
  属性を提供する前に，携帯電話に提供先のコンテンツプロバイダ名・属性項目名を明示し，提供を行うことをダイアログ／Webページなどで通知する. 利用者が確認を表すボタンを押下すると，属性機関は実際に属性をコンテンツプロバイダに対して提供する.
- **許可後提供**
  属性を提供する前に，携帯電話に提供先のコンテンツプロバイダ名・属性項目名を明示し，提供を行ってよいかどうかの許可を求めるダイアログ／Webページなどを表示する. 利用者が許可を表すボタンを押下すると，属性機関は実際に属性をコンテンツプロバイダに対して提供する. 拒否を表すボタンを押下すると，属性機関は属性提供を行わず，利用者の意思により提供不可であることをコンテンツプロバイダに通知する.
- **無条件非提供**
  利用者へのアクションをとらずに，当該コンテンツプロバイダに対する当該属性の提供を常に行わず，利用者の意思により提供不可であることをコンテンツプロバイダに通知する.

4.3.3. プライバシコントロールの実現方式

プライバシコントロールを4.2. で示した各属性情報開示方式に導入した際のシーケンスを，Push方式は図4，Pull方式は図5に示す.

属性機関は，内部にプライバシコントロールの状態を格納したポリシー管理データベースを持ち，利用者は属性機関によって提供されたユーザインタフェースを通してあらかじめポリシーを設定する. 属性機関が属性クエリを受信した際に，属性要求対象の利用者を表す利用者識別子・属性提供先のコンテンツプロバイダ・提供を要求された属性項目からポリシーを内部データベースから読み出し，ポリシーに従って必要ならば携帯電話に対する提供通知／提供確認を行って提供／非提供を決定する.

属性提供すると決定されたならば，属性クエリの送信元に対して属性情報を送信する. 属性を提供しないと決定されたならば，利用者の意思によって提供不可であることを属性クエリの送信元に通知する.

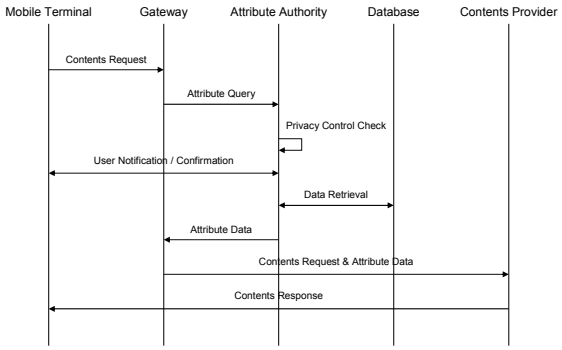

図4：プライバシコントロールを行うPush方式シーケンス

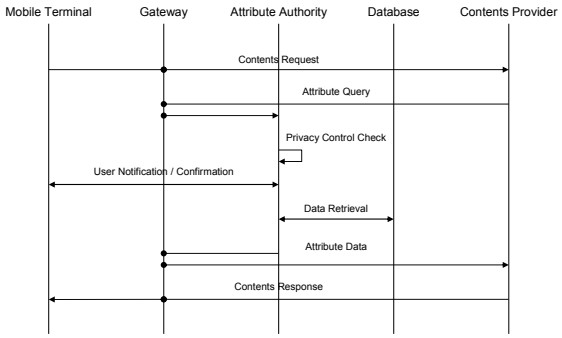

図5：プライバシコントロールを行うPull方式シーケンス

5. おわりに

本稿では，オペレータの持つ契約者に紐付く情報を属性情報として扱い，利用者の意思を反映することができるプライバシコントロールの制御下で，利用者またはコンテンツプロバイダからの要求に基づいて属性情報をコンテンツプロバイダに対して提供する方式について示した.

今後は，属性情報に対する証明の方式や証明を行うプレイヤについて，また属性証明書[4]やSAML[5]など，証明を伴った属性情報の出力の形態についての検討を行っていく予定である.

参考文献

[1] FirstPass, http://www.nttdocomo.co.jp/p_s/firstpass/
[2] 個人情報保護法, http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/030307houan.html
[3] 電気通信事業法, http://www.soumu.go.jp/joho_tsusin/policyreports/japanese/laws/telecom/index-re9908.html
[4] An Internet Attribute Certificate Profile for Authorization, *RFC 3281*.
[5] Security Assertion Markup Language(SAML) v.1.1, http://www.oasis-open.org/specs/index.php#samlv.1.1