携帯端末上でのID管理技術に関する検討

渡辺　龍[†]　仲野　有登[†]　田中　俊昭[†]

† （株）KDDI研究所　〒356–8502 埼玉県ふじみ野市大原 2–1–15

あらまし　近年、携帯端末の高度化に伴いその利用も進んでいる。これら端末のさらなる利便性の向上としては、利用状況、状態に応じた端末切り替え、ネットワークのサービス同士が連携した高度なサービス提供などがあげられる。こうした端末側、ネットワーク側での安全な連携のためには、端末の安全性確認や、認証の一元化や利用者情報の収受などの技術が必要となり、そのためのプラットフォームの構築が不可欠である。こうした背景のもと、本論文では、ネットワーク側での利用者の認証について着目し、携帯端末の一つとして想定される携帯電話でのシングルサインオンと属性情報の取り扱いを行うID管理技術の検討について述べる。具体的には、携帯電話を利用し、携帯電話上でのシングルサインオンと属性情報の管理についてユースケースをもとに方式検討を行った。検討に基づいて実装されたシステムの評価についても併せて述べる。

A Study for Identity Management Technique on Mobile Terminals

Ryu Watanabe[†], Yuto Nakano[†], and Toshiaki Tanaka[†]

† KDDI R&D Laboratories, Inc.　2–1–15 Ohara, Fujimino-shi, Saitama, 356–8502 Japan

Abstract　Thanks to the high spec of mobile terminals, the use of them becomes widespread. Moreover, if a terminal is selected depending on the user environment such as in train or bus, at office, etc., usability will be improved greatly. In addition, the federation of individual services also encourages providing efficient and convenient services for users. In order to realize such services, however, many functions have to be provided on both terminal and network side such as authentication, authorization, securing terminals, and so on. Therefore, especially on network side, a platform for multiple terminals is required. In this paper, we focus on the Identity management scheme on network side for mobile terminals. Based on our investigation, we implemented the proto system with cellular phone. The evaluation of the system also described in this paper.

1　はじめに

近年、携帯型端末技術の進展に伴い、PDAのような小型の端末が多機能化している。また、ネットワークインフラの整備も進み、屋外、移動時での端末利用が増加している。しかしながらこうした小型の端末では、画面やキーなどの、入出力デバイスが小さく、見づらい、入力しづらいなどの欠点がある。このため、移動中は携帯端末を利用していても、目的地に着いたならば、PCのような大きなディスプレイのある端末にサービスを切り替えるなど、端末の環境に応じて適切なサービス適用が必要とされる。また、複数のサービスが協力して一つのサービスを提供するケースや、関連する複数サービスの連続利用など、ネットワーク側でのサービス連携を行うことで、サービスの向上につながる。こうした一方で、ノートPCなどの持ち運び可能な端末からの情報漏洩などのインシデントも増加しており、対策が求められている。サービスを継続しながらの端末切り替えのためには、端末環境の安全な確認・構築に加えて、利用継続のための端末を介した安全性の確認、端末移行のために必要な情報の安全な授受、サービスセッションの適切な管理技術などが必要である。この他、ネットワーク側でのサービスの連携、およびそのサービス利用の利便性のためには、認証の一元化、利用者の属性情報の適切なやり取りなどの管理技術およびサービスの連携技術が必要となる。

端末のためのプラットフォーム技術

前述の端末の切り替え及びサービスの連携のためには、端末、サービス双方の機能改良だけではなく、ネットワーク側に位置し、端末、サービスをサポートする機能を提供するプラットフォームが必要となる。こうしたプラットフォームの機能としては、端末の管理、サービス利用のための利用者の認証、サービスの継続のためのセッションの管理、サービス連携のための情報管理など多く

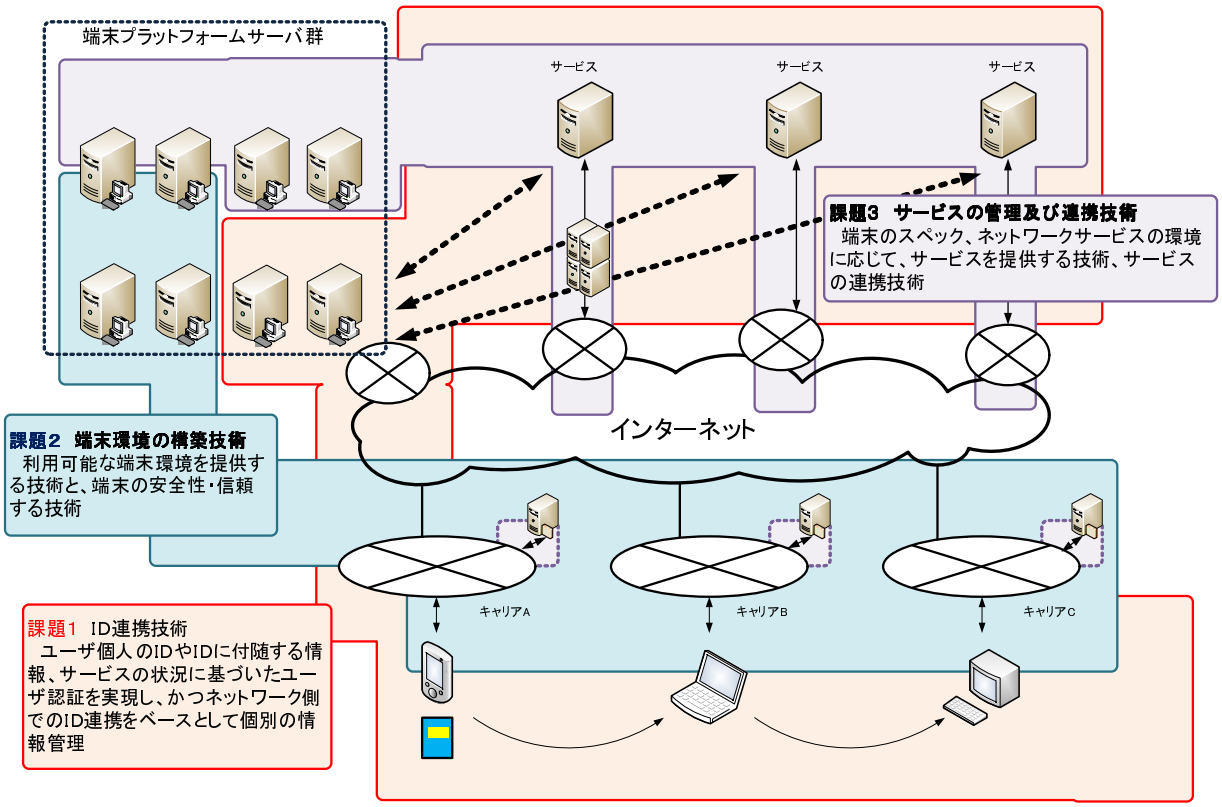

図 1　システムの基本モデル

の機能が想定できる。機能の整備として、必要となる要素技術は大きく分けて、3 つの課題に分類できる。

(1) ID 連携技術
(2) 端末環境の構築技術
(3) サービスの管理及び連携技術

1. の ID 連携技術は、ネットワークやサービスが利用者を識別するための ID や、ID に属する情報を取り扱う技術であり、利用者の ID や情報を適切に管理する技術である。本技術を適用することで、これら情報に基づき、利用者の端末環境に最適なネットワークやサービスを利用可能となるものである。

2. の端末環境の構築技術は、利用者が利用する端末の状態について取り扱う技術であり、利用者がある端末を利用するにあたり、端末の安全性と信頼性を確保し、目的とするサービスを利用する環境を構築するための技術である。

3. のサービスの管理及び連携技術は、利用する端末の能力や端末の付帯状況・環境を把握した上で、異なるサービスを連携させ、利用者および端末の状態に併せて適合するサービスを提供するサービス側の技術である。

各課題の技術を構築することで、プラットフォームが構築される。図 1 にシステムの基本モデルを示す。本モデルでは、プラットフォームの各機能を提供するサーバを端末プラットフォームサーバ群と本稿では呼ぶこととする。

また、個々の課題は、さらに複数の要素技術に分割することが可能である。1. の ID 連携技術は、異なる端末を状況に併せて切り替えるために必要なる端末側での ID 情報の連携技術と、端末プラットフォームを構成するサーバとサービスが端末に対して機能やサービスを提供するための技術である ID 連携技術に大別することができる。ID 管理技術は既にいくつかの仕様や実装があるものの、携帯電話での利用に特化していない。そこで、本稿では携帯電話上での ID 管理について着目し、その検討と実装について述べる。

2　関 連 研 究

2.1　ID 管理技術

ID 管理技術とは、利用者の情報（認証のための情報、識別子、属性情報）などを適切に管理する技術である。利用者の認証情報を適切に取り扱うことで、サービス利用時の利便性を向上するためのシングルサインオンの機能なども提供される。シングルサインオンとは、一度の認証で複数のサービス利用を実現する技術である。一度認証を受けたならば、異なるサービスを認証なしで利用できるようになるため利便性の向上につながる。唯一の ID とパスワードが漏洩した場合は、全てのサービスに被害が及ぶものの、逆に言えば、この ID とパスワードだけを保護すればよいため、多くの ID とパスワードをメモに書き留めたりする必要がなくセキュリティの向上にもつながる。このシングル

サインオンを含むID管理を実現する技術・技術仕様として、Liberty Alliance Project (LAP) [2] [7] 仕様、SAML [3]、OpenID [1]、Microsoft 社の ID メタシステムなどがあげられる。

2.1.1 SAML

SAML は、標準化団体である OASIS が制定した、SSO、ID 管理を実現するための XML 技術仕様である。SAML を利用した場合、トラストサークルと呼ぶグループに属し、信頼関係にあるサービスサイト（サービスプロバイダ：SP Service Provider）と認証サービス（IDP：Identity provider）は双方のローカル ID を仮名（ハンドル）と呼ばれるサービスサイトごとに異なる別の識別子を利用して ID を連携させる。すべての情報のやりとりは、このハンドルを通じて行われるため、リンカビリティの問題は解決されている。

2.1.2 OpenID

OpenID は、SSO、ID 管理を実現する認証システムのひとつである（現状の仕様は 2.0 [4]）。OpenID での利用者識別子はインターネットとの親和性が高く、その利用が広がっている。OpenID では、SAML のように、サービスプロバイダ（OpenID 上では、RP: Relying Party と呼ぶ）と、認証サーバである OP 間において、双方のローカル ID を連携させるという仕組みを利用しない。RP はローカル側に ID を持つ必要がなく、OP から通知された ID を利用者の識別子として利用することができる。

3 方 式 検 討

3.1 利用者の端末

プラットフォームを利用する利用者の端末としては、次の 3 つが想定できる。ノート PC、PDA、携帯電話は移動時、移動先での利用、デスクトップはオフィスや自宅での利用となる。

(1) ノート PC、PDA
(2) 携帯電話
(3) 公共端末

ノート PC、PDA はデスクトップ PC に比べると端末のリソースは非力ではあるものの、近年ではモニタやキーボードなどの入出力の部分以外は、それほど遜色がないといえる。また公共端末は、公共の場所や店舗に設置され多数の利用者が共用する類の端末であり、基本的にはデスクトップの PC であるといえる。

一方で、携帯電話は上記 2 種の PC とは異なる。日本の携帯電話は大変多機能であり、E-mail や SMS(Short Message Service) の通信機能に加えて、高画質カメラ、ワンセグ TV 放送の視聴など、電話本来の機能である通話でない機能についても非常に充実している。その一つとして、インターネットサイトの閲覧の機能があり、専用のブラウザが存在する。先に述べたシングルサインオンを実現する ID 管理の実装では、現状携帯電話専用のブラウザでの利用はあまり検討されておらず利用・実装にあたっては工夫が必要となる。

3.2 携帯電話における認証時の利便性

携帯電話利用時の問題の一つは、入力の問題である。アルファベット、日本語ともに入力可能であるが、認証時の際に、認証サイトにおいて ID とパスワードを毎回入力することは手間のかかる作業である。シングルサインオンが実現されるため個々のサイトでの入力はなくなってはいるが、この入力の手間の低減について検討する。この入力の手間の低減手法の一つに、公開鍵証明書の利用があげられる。認証にあたり、ID/password 代わり、PKI に基づく、公開鍵証明書を利用するものである。すなわち、ID の代わりに携帯電話に保持された公開鍵証明書を選択し、パスワードの代わりに、利用のための PIN 入力を行うことで、認証が実現される。また、携帯電話上の公開鍵証明書を利用することで、認証の安全性も高めることが可能である。

3.2.1 携帯電話上での公開鍵証明書サービス

前述のとおり日本の携帯電話は多機能であり、その一つとして、携帯電話上の公開鍵証明書サービスがある。このサービスは、携帯電話会社 2 社より提供されている [5] [6]。これらのサービスは携帯電話会社が CA となり、端末認証を実施した上で公開鍵証明書を発行する。発行された公開鍵証明書は、端末内の領域に安全に格納され、主として携帯サイトでの認証で利用される。どちらの場合も、銀行などの金融系のサイトの認証などで利用され、利用者の利便性と安全性の向上に貢献している。この公開鍵証明書のサービスの一つが Security Pass である。Security Pass では au の携帯電話利用者ごとに固有な公開鍵証明書（au 証明書）を発行する。利用者は公開鍵証明書のダウンロードサーバにアクセスし証明書の発行を要求する。要求を受けたダウンロードサーバは端末認証を経た上で、証明書を発行する。この証明書の CN (common name) 値は証明書ごとに固有な値であり、KDDI の認証局側で加入者の番号と紐づいて管理されている。

3.3 属性情報の管理

情報の管理についての検討を示す。例えば、サービスサイトが、オンラインショッピングの場合には、送付先や連絡先などの情報を提出することとなるが、オンラインのストリーミングサービスの場合にはこうした情報は必要なく、課金のための情報などのみが必要である。従って、こうしたサイトが必要とする情報を適切に管理することも重要である。また、サイト利用のためのチケットのような形式の権利情報の管理することが必要な場合がある。例えば、サービスが連携するようなユースケースを想定する。ショッピングサイトで特典付きの CD などを購入した場合にのみ、ストリーミング配信サービスで特典映像が限定配信されるような場合である。ショッピングサイトは、購入に基づいて権利情報を利用者に付与する。利

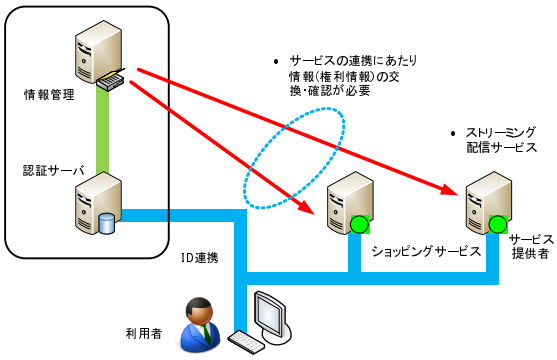

図 2　サービスの連携

表 1　管理情報

タイプ rank	説明	例
1	固定的な情報。アカウント登録時に管理側が確認して登録する。利用者が変更する場合にはオフラインの手続きを必要とする。	名前、性別、生年月日
2	ユーザ自身が情報を自由に登録ができるもの。ユーザが直接変更できる。	ニックネーム、プリファレンス
3	サービスの利用により変化する内容。利用者が意図せず変化することもある。	利用履歴
4	権利に関する情報。利用者が確認できるが変更はできない。	利用チケット、権利情報

用者はこの権利を行使しないという選択はできるが、不正にこうした情報を入手し付与することができてはならないこととなる（図 2）。

これらの情報の場合は、利用者自身が提出を管理することとは別に、適切なサイト利用のためにその内容を変更できないことが必要となる。すなわち、利用者の属性情報については、いくつかのタイプがあることとなる。こうした情報管理について利用形態に基づいて検討した結果、表 1 に示す 4 つの項目（ランク）に分類して管理することとした。

4　実装と評価

携帯電話上での ID 管理およびシングルサインオンの実現と利便性の確認のため、実際にプロトタイムを構築し評価試験を行った。

4.1　実　　装

ID 管理とシングルサインオンの本実装にあたっては、実装モジュールとして OpenSSO [8] を利用した。OpenSSO は通常の PC での利用を前提としているため携帯電話での利用のためにはいくつかの改造が必要となる。また、OpenSSO では認証手法として、通常 ID/password での認証を想定している。携帯電話の公開鍵証明書サービスには対応していない。従って実装にあたってこの 2 点への対応を目的として改造を行った。この結果、シングルサインオンの認証シーケンスは、図 6 のように修正されている。また、携帯電話のブラウザでは、URL の文字数制限から、認証情報となるアサーションを URL 引数として直接取り扱うことができない。このため、アサーションの場所を示す情報となるアーティファクト（図中番号-14）を送付する手法を選択した。

rank	属性名	説明
1	本名	利用者の本名
	性別	利用者の性別　男性/女性
	生年月日	利用者の生年月日　1900年以降
	住所	都道府県 市町村
2	ニックネーム	利用者の任意の仮名
	メールアドレス	利用者のメールアドレス
	電話番号	利用者の電話番号
	配送先	ショッピングサイトでの配送先　複数登録可能
3	利用履歴	サービスごとの利用履歴
4	ポイント	サービスで利用可能なポイント(電子マネー的なイメージ)
	利用回数	サービス利用のためのチケットのイメージ

図 3　設定した属性とランク

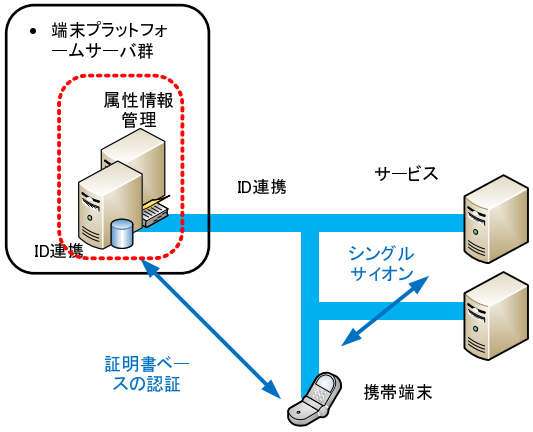

図 4　実装構成

また、設定した属性情報とそのランクを表に示す。模擬的な住所や、ポイントなどは、模擬的なショッピングサービスでのサービス利用の際に利用者の情報として利用した。

実装された機能は、ID 連携機能、シングルサインオン機能、情報管理機能である。また、実装の構成を図 4 に示す。各サーバには、CPU: Intel core duo2 U2400 1.06GHz、メモリ 1GByte の PC を、またプラットフォームには Fedora 9 を利用した。また、この他の実装条件を以下に示す。

- サービスとして模擬的にブログとショッピングのサイトを構築した。
- 認証を担うサーバと情報管理のサーバは便宜的に同一の PC 上に構築した。
- 基本的に端末は携帯電話を利用する（但し、PC からの利用も可能）。
- 携帯電話からの認証には、公開鍵証明書サービスを利用する（ID/password の利用も可能）。

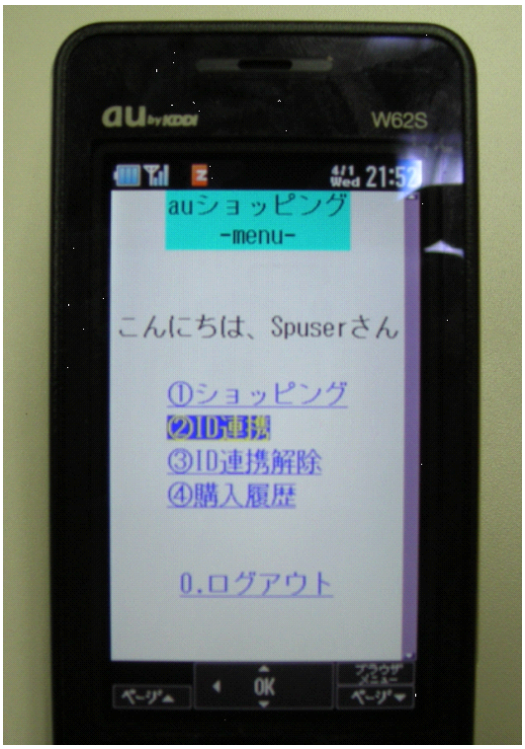

図 5　携帯電話画面サンプル

図 5 にシステム利用時の携帯電話の画面サンプルを示す。これはショッピングサイトの画面である。認証サーバとの連携のため機能、またすでに連携している場合に解除を行うためのボタンなどがトップ画面に表示されている。

4.2　評　　価

4.2.1　動 作 検 証

実装された各機能の評価には、端末を利用して各種機能が正しく動作するかを確認し、シングルサインオンによる認証、ID 連携、ID 連携の解除、各種属性情報の認証サーバからサービスへの受け渡し、証明書を利用した認証サーバでの認証が正しく動作することを確認した。また各種属性情報については、ランクに関して所定の動作を行うことが確認された。但し、サービス間連携については今回実装を行わなかった。

4.2.2　性 能 評 価

本システムの性能評価として、シングルサインオン機能を利用した場合の認証に要する時間について計測を行った。認証サーバとサービスのサーバでの内部処理の時間を測定している。その際、端末上で選択してボタンを押すなどの人の手が介在する部分についてはシステム性能に依存しないため測定から排除している。図 6 に各サーバでの測定ポイントを示す。

また、表 2、表 3 に認証サーバ、サービスのサーバでの処理時間を示す。各値は 10 回の試行の平均値である。

表から示されるとおり、認証サーバでの処理は、2.4 秒程度、サービスでのサーバの処理は 0.8 秒程

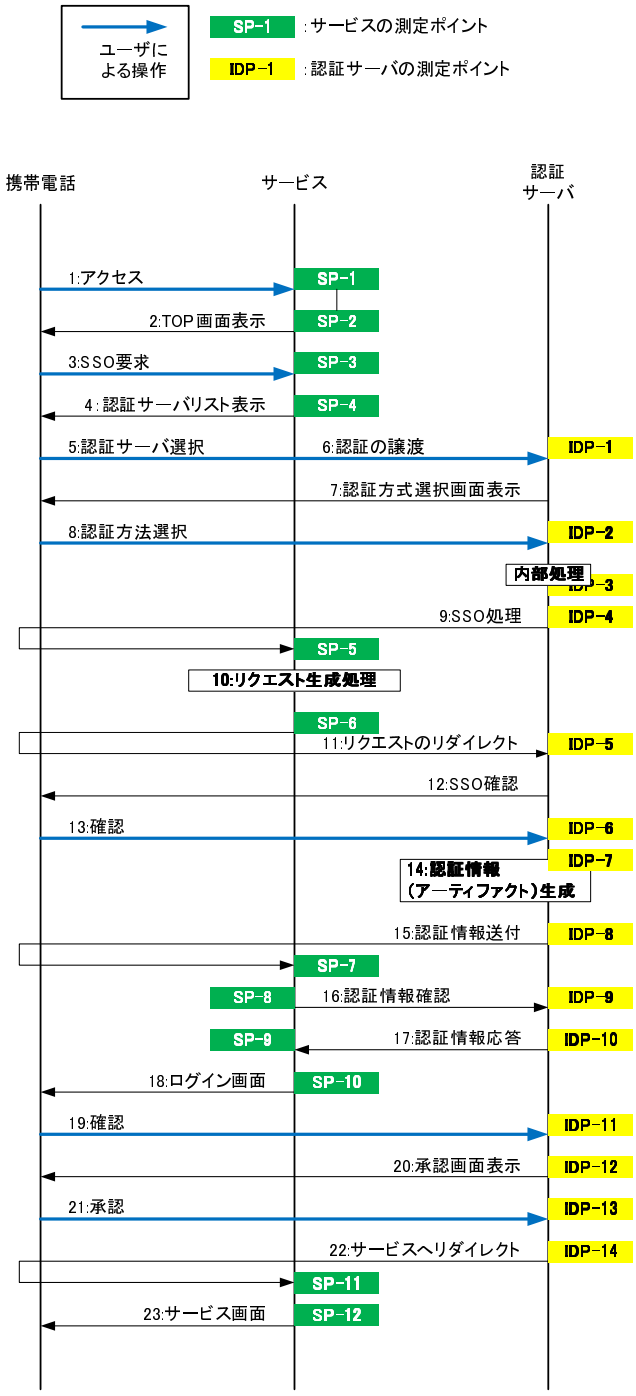

図 6　シーケンスと測定ポイント

度と、合計 3.2 秒程度であった。認証サーバ内部の処理では、項番 2 の “シングルサインオンの処理” に大きく時間がかかることが確認された。これは処理を進めるにあたり一度リダイレクトの処理が発生しているためであり、処理の構成を修正することで時間の削減ができると考えられる。また、サービスのサーバにおいては、ハンドルの確認に時間を要していることが確認された。内部の処理とは別に、実際には利用者のオペレーションと通信時間等が加わるためもう少し時間を要する

表 2　認証サーバでの処理

項番	開始	終了	説明	時間 (msec)
1	IDP-1	IDP-2	画面表示	2
2	IDP-3	IDP-5	SSOの処理	1832
3	IDP-6	IDP-7	リクエスト処理	414
4	IDP-8	IDP-10	アーティファクト生成・送付	5
5	IDP-11	IDP-12	アーティファクト処理	3
6	IDP-13	IDP-14	画面処理	24
7	IDP-15	IDP-16	画面処理	139
合計				2.41sec

表 3　サービスのサーバでの処理

項番	開始	終了	説明	時間 (msec)
1	SP-1	SP-2	画面表示	1.3
2	SP-3	SP-4	画面表示	1.8
3	SP-5	SP-6	リクエスト生成	3.1
4	SP-7	SP-8	アーティファクトのリレー	3.1
5	SP-9	SP-10	ハンドルの確認	817
6	SP-11	SP-12	画面処理	2.1
合計				0.83sec

こととなるが、内部の処理としては比較的短時間で終了できることが確認された。

5 ま と め

本稿では、携帯端末での ID 管理技術の検討として、携帯電話上の公開鍵証明書サービスを用いた認証と利用者情報の管理についての方式検討し、実装とその利便性の向上を図った。また、検討に基づいた実装を用いて評価試験を行った。シングルサインオンの認証の処理に要する内部処理での時間は 3.2 秒程度であることが評価により確認され、高速に動作することが確認された。

謝　　辞

本研究は、独立行政法人情報通信研究機構（NiCT）からの委託研究「端末プラットフォーム技術に関する研究開発」の成果である。関係各位に深謝する。

文　　献

[1] OpenID, http://openid.net/
[2] Liberty Alliance Project: http://www.projectliberty.org/
[3] OASIS SAML V2.0: http://www.oasis-open.org/specs/index.php#samlv2.0
[4] “OpenID Authentication 2.0 - Final”, 2007.
[5] Security Pass, KDDI, http://www.kddi.com/business/security_pass/index.html
[6] First Pass, docomo, http://www.docomo.biz/html/product/firstpass/
[7] B. Pfitzmann, “Privacy in Enterprise Identity Federation - Policies for Liberty Single Signon -”, In proceedings of 3rd workshop on privacy enhancing technology (PET 2003), 2003.
[8] OpenSSO V1 Build 4.5, https://opensso.dev.java.net/public/use/