MC-03

ID 連携スキームガイドライン

平成 22 年 7 月 15 日　　1.0 版

社団法人電波産業会
高度無線通信研究委員会
モバイルコマース部会

本文書は、モバイル IT フォーラムモバイルコマース部会平成 18 年活動報告書（平成 19 年 5 月 8 日付）に記載されていた「ID 連携スキームガイドライン」を抜粋、再編集した文書である。

本文書は、社団法人電波産業会高度無線通信研究委員会モバイルコマース部会の承認を経て、ここに開示するものである。

ID 連携スキームガイドライン

目次

1　はじめに

1.1 スコープ

本ガイドラインは、ポータル、サービスプロバイダおよび端末に対して、ポータル間の ID 連携スキームにおけるインターオペラビリティ確保のための指針を示す。

本ガイドラインは、携帯電話会社や各ポータル事業者および利用者、サービス提供者のいずれに対しても、強制力や責務を負わせるものではない。

1.2　目的

現在、多様なポータルが開設・運営されている。同一ユーザが複数のポータルを利用する場合、そのユーザはそれぞれのポータルに独立したアカウントを保有することになる。これらの異なるアカウントを同一ユーザとして紐付けることができれば、各ポータルの長所を生かし、短所を互いに補えるものと考えられる。

携帯ポータルと他ポータルのアカウント同士が連携する際、携帯ポータルによって ID 情報の提供方法が異なると、他ポータルにとって、それぞれで異なる対応が必要となる。そこで、携帯ポータルの ID 連携スキームの共通化を目的とし、本ガイドラインを定める。

なお以下では、他ポータルとして、TV ポータルに着目し、携帯ポータルと TV ポータルの間での ID 連携について議論を進める。

> 《ID 情報とは》
>
> 本ガイドラインにおいて、ID 情報とは、各ポータルで保持されるアカウント内の情報であり、システムにおけるユーザのアイデンティティを表す。具体的には認証結果を表す情報、ユーザの属性情報を指す。なお、ID 連携とは、アプリケーションレイヤにおいて、異なるポータルが保持するアカウント同士を、紐付けることを指す。

1.3 想定モデル

本ガイドラインにおける想定モデルを図 1 に示す。登場するプレイヤは、ユーザ、端末、TV ポータル、携帯ポータル、サービスプロバイダであり、矢印はプレイヤ間の通信接続を示す。

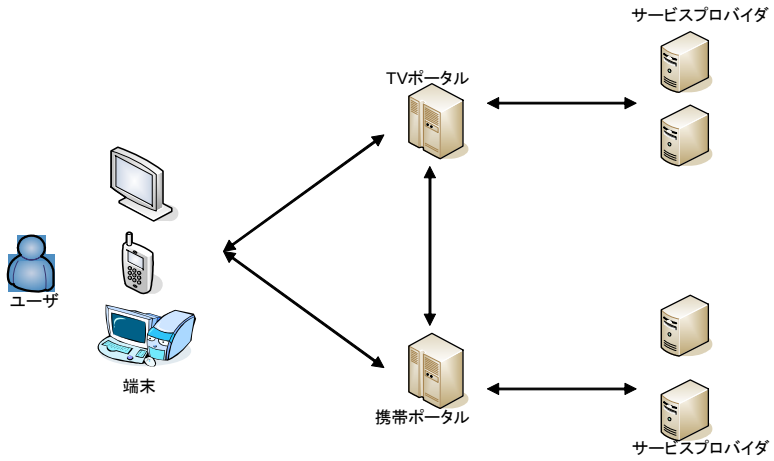

図 1： 想定モデル

各プレイヤについて以下に説明する。

◆ ユーザ：

携帯ポータル及びTVポータルにアカウントをもつ個人。必ずしもアクセスしている本人とは限らない。

◆ 端末：

ユーザがポータルへのアクセスや、サービスプロバイダからサービスを享受するために利用する機器。携帯電話、デジタルテレビ、PCなどが対象となる。

◆ TVポータル：

家電事業者や通信事業者、放送事業者が運営するポータルである。機器IDによる認証や、B-CAS等のICカードによる認証、およびログイン名/パスワードによる認証などの認証機能をもつ。少なくともデジタルテレビからアクセス可能であるが、アクセスできる端末が固定されていない場合も想定される。

（解説）機器IDによる認証では、個人ではなく、世帯を認証する場合がある。TVポータルが世帯に対応するアカウントしかもたない場合はそのアカウントがポータル間におけるアカウント紐付けの対象となる。一方、他に個人に対応するアカウントをもつ場合は、個人に対応するアカウントがポータル間におけるアカウント紐付けの対象となる。

◆ 携帯ポータル：

携帯電話事業者が運営するポータルである。UICC等のICカードに基づく認証やログイン名/パスワードによる認証などの認証機能をもつ。少なくとも携帯電話からアクセス可能であるが、アクセスできる端末が固定されていない場合も想定される。

◆ サービスプロバイダ：

ユーザにサービスや商品を提供するウェブサイト。携帯ポータル、あるいはTVポータルとID連携されていることを前提とする。携帯ポータルとID連携しているサービスプロバイダは、携帯ポータルにアクセスできる端末からのみアクセス可能とする。TVポータルとID連携しているサービスプロバイダは、TVポータルにアクセスできる端末からのみアクセス可能とする。

1.4 規定範囲

本ガイドラインでは、以下について規定する。

◆ ポータル間でのアカウント紐付け登録・解除の方法

◆ ポータル間でのID情報（認証情報・属性情報）の共有方法

◆ 携帯ポータルから提供するID情報（認証情報・属性情報）の表現方法

また、以下は規定範囲外とする。

◆ 携帯ポータルにおけるユーザの認証方法

◆ TVポータルにおけるユーザの認証方法

◆ 携帯ポータルとサービスプロバイダ間のID連携方法

◆ TVポータルとサービスプロバイダ間のID連携方法

◆ 同一ポータル内に同一ユーザがもつ、複数の異なるアカウント間のID連携方法

1.5 Reference Documents

【SAMLCore】
Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0

【SAMLProfiles】
Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0

【SAMLAuthnContext】
Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0

【LibertyWSFDST】
Liberty ID-WSF Data Service Template V2.0

【LibertySISPP】
Liberty ID-SIS Personal Profile

【LibertySISEP】
Liberty ID-SIS Employee Profile

【LibertySISGL】
Liberty ID-SIS Geolocation Service

【LibertyInteraction】
Liberty ID-WSF Interaction Service Specification

【SAMLToken】
Web Service Security: SAML Token Profile

2　要求条件

本章では、ポータル間でのアカウント紐付け、解除、および ID 情報の交換に関する要求条件について、ユースケースの実現フローをもとに抽出する。なお、要求条件は、アカウント紐付けに関するもの、認証情報の共有に関するもの、属性情報の共有に関するものに対し、それぞれ ID、AH、AT を頭文字とする通番（例：AT-1）で示す。

2.1 ユースケース

2.1.1　携帯電話を使って TV ポータルの登録情報を更新する

2.1.1.1　概要

TV ポータルに登録されているユーザ情報（例：e メールアドレス）が変更になった場合、その情報の更新はデジタルテレビからリモコンを使って行うことができる。しかし、リモコンによる文字入力は操作が煩雑である。本ユースケースでは、デジタルテレビの登録情報に携帯電話の登録情報をコピーすることでユーザのリモコンを使ったデジタルテレビへの文字入力の手間を省くことができる。

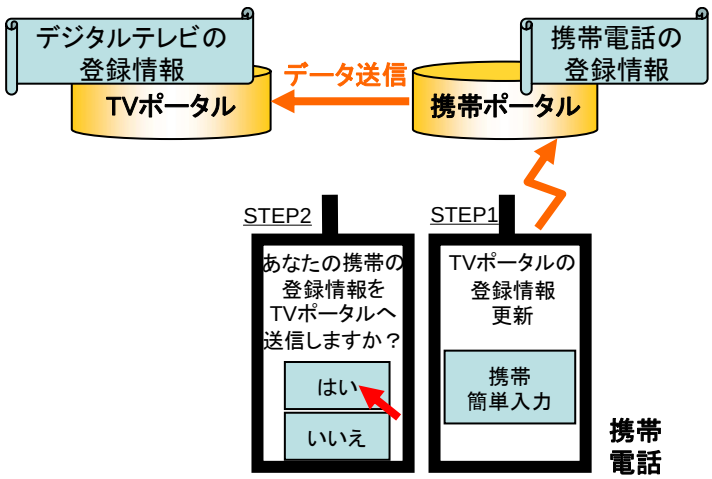

図 2： 携帯電話を使って TV ポータルの登録情報を更新する

2.1.1.2　プレイヤ

- ユーザ
- 携帯ポータル
- TV ポータル
- 携帯電話

2.1.1.3　事前条件

- TV ポータルの事業者と携帯ポータルの事業者は、ID 情報を交換する契約が成立している
- ユーザは携帯ポータルと TV ポータルからアカウントを取得している
- ユーザは携帯電話とデジタルテレビを所有している
- ユーザは携帯ポータルのアカウントにより携帯ポータルにログインしている
- 携帯ポータルの登録情報は更新されているが、TV ポータルの登録情報は更新されていない

2.1.1.4　事後条件

- TV ポータルの登録情報が更新される

2.1.1.5　実現フロー

① ユーザは携帯電話から携帯ポータルにアクセスする
② 携帯ポータルは登録情報更新画面を表示する
③ ユーザは「携帯電話の登録情報をデジタルテレビの登録情報にコピーすること」を携帯ポータルへ通知する
④ 携帯ポータルから TV ポータルへ登録情報が送られ、TV ポータルは携帯電話の登録情報をコピーする。
(AT-1)　携帯ポータルから利用者に登録情報のコピーに対する承諾を得ること
(AT-2)　ポータル間で、登録情報が共通的な形式で共有されること
⑤ 携帯電話の画面に、登録情報のコピー完了画面が表示される

なお、本ユースケースで事前にアカウント紐付けが行なわれていない場合は、③の後に以下が行なわれ、④に復帰する。ここで、アカウント紐付けは、携帯ポータルと TV ポータルがアクセスできる端末をそれぞれ携帯電話とデジタルテレビに固定している場合（端末固定）と、そうでない場合（端末非固定）に分けられるため、要求条件の抽出では双方の場合を考察する。

③’-(1) 携帯ポータルは紐付け可能なポータル一覧を表示し、ユーザにアカウント紐付けすることを促す

（ID-1）TV ポータル及び携帯ポータルで紐付け可能なポータル URL を管理すること

③’-(2) ユーザは携帯電話から携帯ポータルへ TV ポータルと紐付けすることを通知する

③’-(3) TV ポータルと携帯ポータルとの間でアカウント紐付けが行われる

（ID-2）携帯ポータルが生成する情報を基に、TV ポータルとアカウント紐付けできること
（端末非固定の場合のみでなく、端末固定の場合においても紐付けできること）

（ID-3）TV ポータルからユーザに対するアカウント紐付けの承認確認できること
（端末非固定の場合のみでなく、端末固定の場合においても承認確認できること）

（ID-4）一度アカウントが紐付けされると、解除を行わない限り紐付けは保持されること

③’-(4) 携帯ポータルは携帯電話へアカウント紐付け完了画面を表示する

また、本ユースケースで携帯ポータルが登録情報を開示する際に、TV ポータルの認証結果が携帯ポータルで必要とされる認証レベルを満たさない場合は、以下の要求条件を満たす処理が行われる。

（AH-1）ポータルは必要に応じて認証情報の取得要求を連携先ポータルに対して送信し、連携先ポータルは、それに対して共通的な形式で認証情報を開示する

2.1.2　デジタルテレビを使って TV ポータルの登録情報を追加する

2.1.2.1　概要

本ユースケースでは、デジタルテレビに登録されていない登録情報（例：電話番号）を携帯電話の登録情報からコピーすることでユーザのリモコンを使ったデジタルテレビへの文字入力の手間を省くことができる。

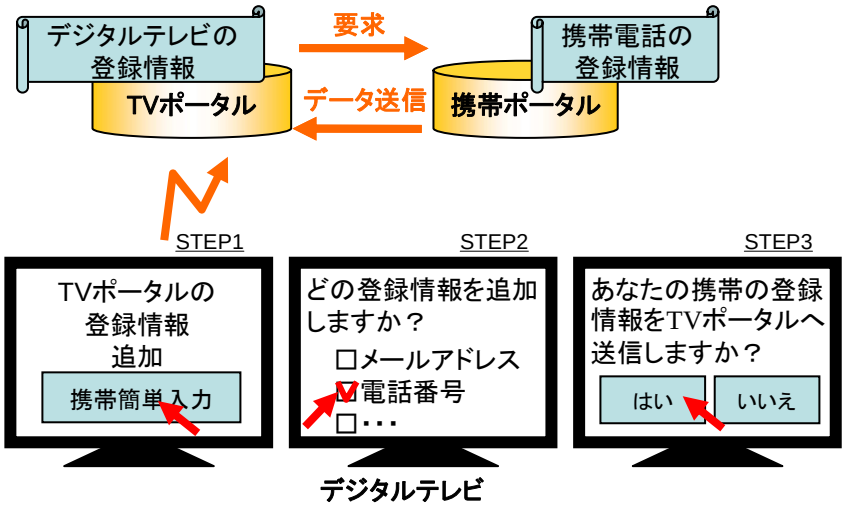

図 3　デジタルテレビを使って TV ポータルの登録情報を追加する

2.1.2.2　プレイヤ

- ユーザ
- 携帯ポータル
- TV ポータル
- デジタルテレビ

2.1.2.3　事前条件

◆ TV ポータルの事業者と携帯ポータルの事業者は、ID 情報を交換する契約が成立している
◆ ユーザは携帯ポータルと TV ポータルからアカウントを取得している
◆ ユーザは携帯電話とデジタルテレビを所有している
◆ ユーザは TV ポータルのアカウントにより TV ポータルにログインしている
◆ 携帯ポータルに登録されているユーザ情報（例：電話番号）が TV ポータルには登録されていない。

2.1.2.4　事後条件

◆ 携帯電話の登録情報がデジタルテレビの登録情報にコピーされる

2.1.2.5　実現フロー

① ユーザはデジタルテレビから TV ポータルにアクセスする
② TV ポータルは登録情報追加画面を表示する
③ ユーザは「携帯電話の登録情報をデジタルテレビの追加を必要とする登録情報にコピーすること」を TV ポータルへ通知する
④ TV ポータルは追加を必要とする登録情報を携帯ポータルに要求する
⑤ TV ポータルは携帯ポータルから送られた登録情報をコピーする
　（AT-1）TV ポータルから利用者に登録情報のコピーに対する承諾を得ること
　（AT-2）ポータル間で、登録情報が共通的な形式で共有されること
⑥ デジタルテレビの画面に、登録情報のコピー完了画面が表示される

なお、本ユースケースで事前にアカウント紐付けが行なわれていない場合は、③の後に以下が行なわれ、④に復帰する。また、要求条件の抽出では端末固定と非固定の場合を考察する。

③'-(1) TV ポータルは紐付け可能なポータル一覧を表示し、ユーザにアカウント紐付けすることを促す
　（ID-1）TV ポータル及び携帯ポータルで紐付け可能なポータル URL を管理すること
③'-(2) ユーザはデジタルテレビから TV ポータルへ携帯ポータルと紐付けすることを通知する
③'-(3) 携帯ポータルと TV ポータルとの間でアカウント紐付けが行われる
　（ID-5）TV ポータルが生成する情報を基に、携帯ポータルとアカウント紐付けできること
　　（端末非固定の場合のみでなく、端末固定の場合においても紐付けできること）
　（ID-6）携帯ポータルからユーザに対するアカウント紐付けの承認確認できること
　　（端末非固定の場合のみでなく、端末固定の場合においても承認確認できること）
　（ID-4）一度アカウントが紐付けされると、解除を行わない限り紐付けは保持されること
③'-(4) TV ポータルはデジタルテレビへアカウント紐付け完了画面を表示する

また、本ユースケースで携帯ポータルが登録情報を開示する際に、TV ポータルの認証結果が携帯ポータルで必要とされる認証レベルを満たさない場合は、要求条件（AH-1）を満たす処理が行われる。

2.1.3　デジタルテレビによる有料コンテンツ購入において携帯決済を利用する

2.1.3.1　概要

通常、ユーザが TV ポータルで有料コンテンツを購入する場合は、TV ポータルで決済方法を選択する。本ユースケースでは、TV ポータルと携帯ポータルのアカウントを紐付けることによって、決

済方法の選択肢に携帯決済を加えることができる。

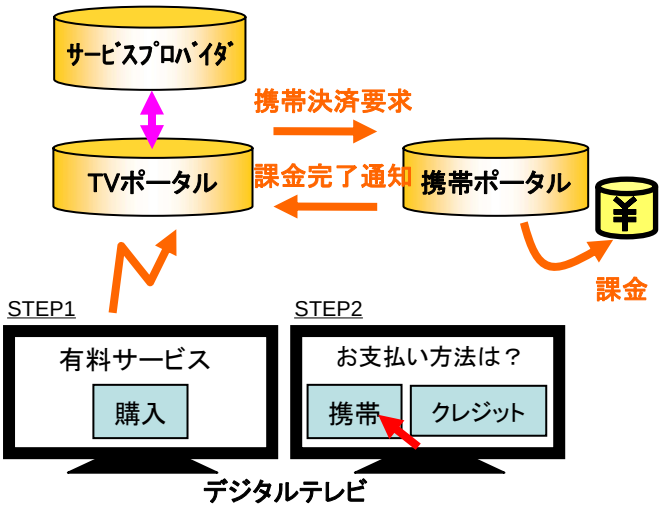

図 4： デジタルテレビによる有料コンテンツ購入において携帯決済を利用する

2.1.3.2　プレイヤ

- ◆ ユーザ
- ◆ 携帯ポータル
- ◆ TV ポータル
- ◆ デジタルテレビ
- ◆ TV ポータルのサービスプロバイダ（SP）

2.1.3.3　事前条件

- ◆ TV ポータルの事業者と携帯ポータルの事業者は、ID 情報を交換する契約が成立している
- ◆ ユーザは携帯ポータルと TV ポータルからアカウントを取得している
- ◆ ユーザは携帯電話とデジタルテレビを所有している
- ◆ ユーザは TV ポータルのアカウントにより TV ポータルにログインしている
- ◆ ユーザは SP からアカウントを取得している
- ◆ TV ポータルのアカウントは SP のアカウントと紐付けられている

2.1.3.4　事後条件

- ◆ 購入したコンテンツ料金が携帯電話に課金される

2.1.3.5　実現フロー

① ユーザはデジタルテレビから TV ポータルにアクセスし、有料コンテンツを購入する
② TV ポータルは決済方法選択画面を表示する
③ ユーザは携帯決済を TV ポータルへ通知する
④ TV ポータルは携帯決済を携帯ポータルに要求する
⑤ 携帯ポータルはコンテンツ料金をユーザの所有する携帯電話に課金し、課金完了を TV ポータルへ通知する
　※ ポータル間で交換する携帯決済要求や課金完了通知については、ID 連携スキーム上で動作するアプリケーションに依存するため、要求条件として抽出しない。
⑥ TV ポータルは課金完了画面を表示する

なお、本ユースケースで事前にアカウント紐付けが行なわれていない場合は、③の後に 2.1.2 の実現フロー③'-(1)～(4)が行なわれ、④に復帰する。

また、本ユースケースで携帯ポータルが課金する際に、TV ポータルの認証結果が携帯ポータルで必要とされる認証レベルを満たさない場合は、要求条件（AH-1）を満たす処理が行われる。

2.1.4 アカウント紐付けを解除する

2.1.4.1 アカウント紐付けを解除するポータルが携帯ポータルの場合

ユーザは携帯ポータルへアクセスし、対話形式で解除手続きを行う場合では、ユーザが自らアカウント紐付けを解除する。また、以下に示すユースケースでは、ポータルがアカウント紐付けを解除する。

- ◆ ユーザは携帯電話を解約、もしくは休止する
- ◆ 利用規約に違反したユーザのアカウントを強制的に失効する

2.1.4.2 アカウント紐付けを解除するポータルが TV ポータルの場合

ユーザは TV ポータルへアクセスし、対話形式で解除手続きを行う場合では、ユーザが自らアカウント紐付けを解除する。また、以下に示すユースケースでは、ポータルがアカウント紐付けを解除することが想定される。

- ◆ ユーザは TV ポータルサービスを解約する
- ◆ ユーザはデジタルテレビを買い換える

2.2 要求条件

2.2.1 アカウント紐付け

2.2.1.1 携帯ポータルからアカウント紐付けを行なう場合

要求条件番号	要求条件
ID-1	TV ポータル及び携帯ポータルで紐付け可能なポータル URL を管理すること
ID-2	携帯ポータルが生成する情報を基に、TV ポータルとアカウント紐付けできること （端末非固定の場合のみでなく、端末固定の場合においても紐付けできること）
ID-3	TV ポータルからユーザに対するアカウント紐付けの承認確認できること （端末非固定の場合のみでなく、端末固定の場合においても承認確認できること）
ID-4	一度アカウントが紐付けされると、解除を行わない限り紐付けは保持されること

2.2.1.2 TV ポータルからアカウント紐付けを行なう場合

要求条件番号	要求条件
ID-1	TV ポータル及び携帯ポータルで紐付け可能なポータル URL を管理すること
ID-5	TV ポータルが生成する情報を基に、携帯ポータルとアカウント紐付けできること （端末非固定の場合のみでなく、端末固定の場合においても紐付けできること）
ID-6	携帯ポータルからユーザに対するアカウント紐付けの承認確認できること （端末非固定の場合のみでなく、端末固定の場合においても承認確認できること）
ID-4	一度アカウントが紐付けされると、解除を行わない限り紐付けは保持されること

2.2.2 アカウント紐付け解除

要求条件番号	要求条件
ID-7	携帯ポータルが生成する情報を基に、TV ポータルとアカウントの紐付け解除ができること （端末非固定の場合のみでなく、端末固定の場合においても紐付け解除できること）
ID-8	TV ポータルからユーザに対するアカウント紐付け解除の承認確認できること （端末非固定の場合のみでなく、端末固定の場合においても承認確認できること）

2.2.3 認証結果の共有

要求条件番号	要求条件
AH-1	ポータルは必要に応じて認証情報の取得要求を連携先ポータルに対して送信し、連携先ポータルは、それに対して共通的な形式で認証情報を開示する

2.2.4 属性情報の共有

要求条件番号	要求条件
AT-1	携帯ポータルから利用者に登録情報のコピーに対する承諾を得ること
AT-2	ポータル間で、登録情報が共通的な形式で共有されること

3 ID 連携スキーム

3.1 基本方針

本ガイドラインでは、基本的には SAML2.0、Liberty ID-WSF2.0 および Liberty ID-SIS1.0 のプロファイリングを行い、最小限の規定をすることとする。上記に際しては、2 章の要求条件を満たすこと、国内モバイル環境での実現性を考慮することとする。
なお、2 章の要求条件と 3 章での記載内容の対応関係は 3.9 に示す。

3.2 アカウント紐付け方法

アカウント紐付け登録のパターンは、2 章の要求条件に基づき、アカウント紐付けが開始されるポータルアカウント（起点アカウント）及び端末とポータルの関係から以下のように分類できる。

- ◆ 起点アカウント
  - ➢ 携帯アカウント
  - ➢ TV アカウント
- ◆ 端末とポータルの関係
  - ➢ 端末固定
  - ➢ 端末非固定

さらに、アカウント紐付けに用いる識別子（共有識別子）を発行するポータルにより分類できる。

- ◆ 共有識別子を発行するポータル
  - ➢ 携帯ポータル

- TV ポータル
- 双方のポータル

全 12 パターンのアカウント紐付け方法に分類できるが、携帯ポータルが共有識別子を発行する 4 パターン及び TV アカウント起点において TV ポータルが共有識別子を発行する 2 パターンのみ規定する（表 1)。

表 1：アカウント紐付け方法パターン

起点アカウント	端末とポータルの関係	共有識別子を発行するポータル	規定する内容
携帯アカウント	端末固定	携帯ポータル	①
		TV ポータル	×
		双方のポータル	×
	端末非固定	携帯ポータル	②
		TV ポータル	×
		双方のポータル	×
TV アカウント	端末固定	携帯ポータル	③
		TV ポータル	④
		双方のポータル	×
	端末非固定	携帯ポータル	⑤
		TV ポータル	⑥
		双方のポータル	×

3.2.1 共有識別子

個人情報保護の観点から、携帯ポータルがポータル間で共有するアカウント識別子（共有識別子）を発行する場合は、アカウント識別子として仮名を用いることを推奨する。TV ポータルが共有識別子を発行する場合は、実アカウント、仮名のどちらでもかまわないものとする。

3.2.2 アカウント紐付けフロー

【SAMLProfiles】の *4.1Web Browser SSO Profile* に従って、各パターンのアカウント紐付け登録フローを規定する。

3.2.2.1 携帯アカウントが起点・端末固定・携帯ポータルが共有識別子を発行する場合（①）

この場合のアカウント紐付け方法を以下のように定める。なお、【SAMLProfiles】の *4.1 Web Browser SSO Profile* における Identity Provider が携帯ポータル、Service Provider が TV ポータル、User Agent は、携帯ポータルと通信しているときは携帯電話、TV ポータルと通信しているときはデジタルテレビに相当する。

◆ フローの開始点

- フローは[SAMLProfiles]の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* からスタートするものとする。

  （解説）[SAMLProfiles]の *4.1.3 Profile Description* の分類において、Identity Provider から開始されるプロファイルに相当するため。

◆ユーザ端末を経由するメッセージ

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* において、携帯ポータルから TV ポータルへ認証情報を渡すための<Response>メッセージとして HTTP Artifact binding を用いることを推奨する。

  （解説）携帯電話の処理能力を考慮すると、認証情報本体は署名を含む場合が多いため、Artifact を用いることが望ましい。

◆ 端末固定の場合に特有の処理手順

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Sertive Provider* において、携帯ポータルから TV ポータルへ認証情報を渡すための<Response>メッセージは、携帯電話において保存可能な形式で携帯ポータルから携帯電話に対して送信されるものとする。

  （解説）携帯ポータルにアクセスする User Agent は携帯電話、TV ポータルにアクセスする User Agent はデジタルテレビであるため、Identity Provider から User Agent を経由して Service Provider へ<Response>メッセージが渡されるには 2 種類の User Agent 間で携帯ポータルが送信した<Response>メッセージをやりとりする必要がある。User Agent 間で<Response>メッセージをやりとりするためのフロー例を以下に示す。また、このフローを含む全体フローを図 5 に示す。

  ①携帯ポータルは携帯電話に対して、認証アサーションもしくは Artifact をデータとして送信する。

  ②携帯電話からデジタルテレビに対して、認証アサーションもしくは Artifact が任意の方法で渡される。

  ③デジタルテレビから TV ポータルに対して、認証アサーションもしくは Artifact に基づいてアクセスする。

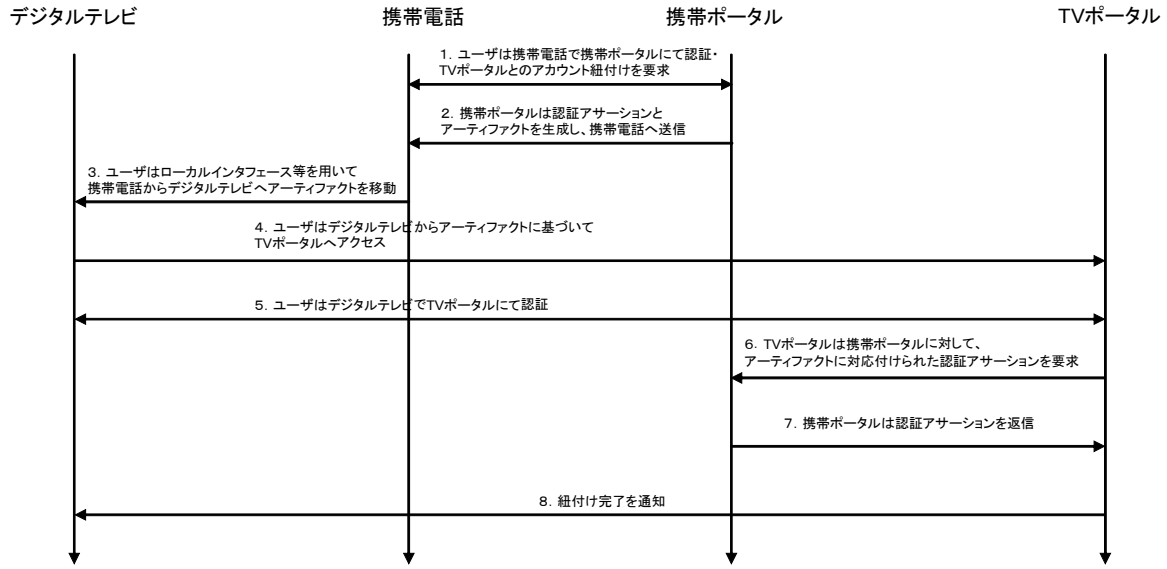

図 5：携帯ポータルから TV ポータルに対してアカウント紐付けを行う場合のフロー

3.2.2.2　携帯アカウントが起点・端末非固定・携帯ポータルが共有識別子を発行する場合(②)

この場合のアカウント紐付け方法について次のように定める。なお、【SAMLProfiles】の *4.1 Web Browser SSO Profile* における Identity Provider が携帯ポータル、Service Provider が TV ポータルに相当し、User Agent は、携帯電話、デジタルテレビのどちらかに相当する。。

◆ フローの開始点

- フローは[SAMLProfiles]の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* からスタートするものとする。

  （解説）[SAMLProfiles]の *4.1.3 Profile Description* の分類において、Identity Provider から開始されるプロファイルに相当するため。

◆ ユーザ端末を経由するメッセージ

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* において、携帯ポータルから TV ポータルへ認証情報を渡すための<Response>メッセージとして HTTP Artifact binding を用いることを推奨する。

  （解説）携帯電話の処理能力を考慮すると、認証情報本体は署名を含む場合が多いため、Artifact を用いることが望ましい。

3.2.2.3　TV アカウントが起点・端末固定・携帯ポータルが共有識別子を発行する場合（③）

この場合のアカウント紐付け方法について次のように定める。なお、【SAMLProfiles】の *4.1 Web Browser SSO Profile* における Identity Provider が携帯ポータル、Service Provider が TV ポータル、User Agent は、携帯ポータルと通信しているときは携帯電話、TV ポータルと通信しているときはデジタルテレビに相当する。

◆ フローの開始点

- フローは[SAMLProfiles]の *4.1 Web Browser SSO Profile* に示されたフローの最初からスタートするものとする。

  （解説）[SAMLProfiles]の *4.1.3 Profile Description* の分類において、Service Provider から開始されるプロファイルに相当するため。

◆ 連携先ポータル情報の取得方法

- 【SAMLProfiles】の *4.1.3.2 Service Provider Determines Identity Provider* において、TV ポータルは連携可能なポータルのリストをユーザに提供することを推奨する。

  （解説）連携先ポータルをユーザが指定できるようにするため。

◆ ユーザ端末を経由するメッセージ

- 【SAMLProfiles】の *4.1.3.3 <AuthnRequest> Is Issued by Service Provider to Identity Provider* において、TV ポータルは携帯ポータルに共有識別子の発行を要求するための<AuthnRequest>メッセージとして HTTP POST binding もしくは HTTP Artifact binding を用い、TV ポータルの URI を追加情報として付加することを推奨する。
- 【SAMLProfiles】の *4.1.3.3 <AuthnRequest> Is Issued by Service Provider to Identity Provider* において、<AuthnRequest>に付加された TV ポータルの URI は、*4.1.3.5 Identity Provider Issues <Response> to Sertive Provider* において、携帯ポータルは TV ポータルに認証情報を渡すための<Response>メッセージの宛先として用いることとする。

  （解説）端末固定の場合は HTML の Referer ヘッダを利用できないため。
- 【SAML Profiles】の *4.1.3.3 <AuthnRequest> Is Issued by Service Provider to Identity Provider* において、TV ポータルから携帯ポータルに共有識別子の発行を要求するための<AuthnRequest>メッセージに署名が付与されている場合は、TV ポータルは HTTP Artifact binding を用いることを推奨する。

  （解説）携帯電話の処理能力を考慮すると、<AuthnRequest>メッセージに署名が含まれる場合は Artifact を用いることが望ましい。

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* において、携帯ポータルから TV ポータルへ認証情報を渡すための<Response>メッセージとして HTTP Artifact binding を用いることを推奨する。

  （解説）携帯電話の処理能力を考慮すると、認証情報本体は署名を含む場合が多いため、Artifact を用いることが望ましい。

◆ 端末固定の場合に特有の処理手順

- 【SAMLProfiles】の *4.1.3.3 <AuthnRequest> Is Issued by Service Provider to Identity Provider* において、TV ポータルから携帯ポータルに共有識別子の発行を要求するための<AuthnRequest>メッセージは、デジタルテレビにおいて保存可能な形式で TV ポータルからデジタルテレビに対して送信されるものとする。

  （解説）携帯ポータルにアクセスする User Agent は携帯電話、TV ポータルにアクセスする User Agent はデジタルテレビであるため、Service Provider から User Agent を経由して Identity Provider へ<AuthnRequest>メッセージが渡されるには 2 種類の User Agent 間でTVポータルが送信した<AuthnRequest>メッセージをやりとりする必要がある。User Agent 間で<AuthnRequest>メッセージをやりとりするためのフロー例を以下に示す。

  ① TV ポータルはデジタルテレビに対して、<AuthnRequest>メッセージをデータとして送信する。

  ② デジタルテレビから携帯電話に対して、<AuthnRequest>メッセージが任意の方法で渡される。

  ③ 携帯電話から携帯ポータルに対して、<AuthnRequest>メッセージに基づいてアクセスする。

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* において、携帯ポータルから TV ポータルに共有識別子を渡すための<Response>メッセージは、携帯電話において保存可能な気式で携帯ポータルから携帯電話に対して送信されるものとする。

  （解説）携帯ポータルにアクセスする User Agent は携帯電話、TV ポータルにアクセスする User Agent はデジタルテレビであるため、Identity Provider から User Agent を経由して Service Provider へ<Response>メッセージが渡されるには 2 種類の User Agent 間で携帯ポータルが送信した<Response>メッセージをやりとりする必要がある。User Agent 間で<Response>メッセージをやりとりするためのフロー例を以下に示す。

  ① 携帯ポータルは携帯電話に対して、認証アサーションもしくは Artifact をデータとして送信する。

  ② 携帯電話からデジタルテレビに対して、認証アサーションもしくは Artifact が任意の方法で渡される。

  ③ デジタルテレビから TV ポータルに対して、認証アサーションもしくは Artifact に基づいてアクセスする。

3.2.2.4　TV アカウントが起点・端末固定・TV ポータルが共有識別子を発行する場合（④）

この場合のアカウント紐付け方法について次のように定める。なお、【SAMLProfiles】*4.1 Web Browser SSO Profile* における Identity Provider が TV ポータル、Service Provider が携帯ポータル、User Agent は、携帯ポータルと通信しているときは携帯電話、TV ポータルと通信しているときはデジタルテレビに相当する。

◆ フローの開始点

- フローは[SAMLProfiles]の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* からスタートするものとする。

  （解説）[SAMLProfiles]の *4.1.3 Profile Description* の分類において、Identity Provider から開始されるプロファイルに相当するため。

◆ ユーザ端末を経由するメッセージ

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* において、携帯ポータルから TV ポータルへ認証情報を渡すための<Response>メッセージとして HTTP Artifact binding を用いることを推奨する。

  （解説）携帯電話の処理能力を考慮すると、認証情報本体は署名を含む場合が多いため、Artifact を用いることが望ましい。

◆ 端末固定の場合に特有の処理手順

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* において、TV ポータルから携帯ポータルに共有識別子を渡すための<Response>メッセージは、携帯電話において保存可能な気式で携帯ポータルから携帯電話に対して送信されるものとする。

  （解説）携帯ポータルにアクセスする User Agent は携帯電話、TV ポータルにアクセスする User Agent はデジタルテレビであるため、Identity Provider から User Agent を経由して Service Provider へ<Response>メッセージが渡されるには 2 種類の User Agent 間で携帯ポータルが送信した<Response>メッセージをやりとりする必要がある。User Agent 間で<Response>メッセージをやりとりするためのフロー例を以下に示す。

  ① TV ポータルはデジタルテレビに対して、認証アサーションもしくは Artifact をデータとして送信する。

  ② デジタルテレビから携帯電話に対して、認証アサーションもしくは Artifact が任意の方法で渡される。

  ③ 携帯電話から携帯ポータルに対して、認証アサーションもしくは Artifact に基づいてアクセスする。

3.2.2.5　TV アカウントが起点・端末非固定・携帯ポータルが共有識別子を発行する場合（⑤）

この場合のアカウント紐付け方法について次のように定める。なお、【SAMLProfiles】*4.1 Web Browser SSO Profile* における Identity Provider が携帯ポータル、Service Provider が TV ポータルに相当し、User Agent は、携帯電話、デジタルテレビのどちらかに相当する。

◆ フローの開始点

- フローは[SAMLProfiles]の *4.1 Web Browser SSO Profile* に示されたフローの最初からスタートするものとする。

  （解説）[SAMLProfiles]の *4.1.3 Profile Description* の分類において、Service Provider から開始されるプロファイルに相当するため。

◆ 連携先ポータル情報の取得方法

- 【SAMLProfiles】の *4.1.3.2 Service Provider Determines Identity Provider* において、TV ポータルは連携可能なポータルのリストをユーザに提供することを推奨する。

  （解説）連携先ポータルをユーザが指定できるようにするため。

◆ ユーザ端末を経由するメッセージ

- 【SAML Profiles】の *4.1.3.3 <AuthnRequest> Is Issued by Service Provider to Identity Provider* において、TV ポータルから携帯ポータルに共有識別子の発行を要求するための <AuthnRequest>メッセージに署名が付与されている場合は、TV ポータルは HTTP Artifact binding を用いることを推奨する。

  （解説）携帯電話の処理能力を考慮すると、<AuthnRequest>メッセージに署名が含まれる場合は Artifact を用いることが望ましい。

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* において、携帯ポータルから TV ポータルへ認証情報を渡すための<Response>メッセージとして HTTP Artifact binding を用いることを推奨する。

  （解説）携帯電話の処理能力を考慮すると、認証情報本体は署名を含む場合が多いため、Artifact を用いることが望ましい。

3.2.2.6　TV アカウントが起点・端末非固定・TV ポータルが共有識別子を発行する場合（⑥）

この場合のアカウント紐付け方法について次のように定める。なお、【SAMLProfiles】*4.1 Web Browser SSO Profile* における Identity Provider が TV ポータル、Service Provider が携帯ポータルに相当し、User Agent は、携帯電話、デジタルテレビのどちらかに相当する。

◆ フローの開始点

- フローは[SAMLProfiles]の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* からスタートするものとする。

  （解説）[SAMLProfiles]の *4.1.3 Profile Description* の分類において、Identity Provider から開始されるプロファイルに相当するため。

◆ ユーザ端末を経由するメッセージ

- 【SAMLProfiles】の *4.1.3.5 Identity Provider Issues <Response> to Service Provider* において、TV ポータルから携帯ポータルへ認証情報を渡すための<Response>メッセージとして HTTP Artifact binding を用いることを推奨する。

  （解説）携帯電話の処理能力を考慮すると、認証情報本体は署名を含む場合が多いため、Artifact を用いることが望ましい。

3.3 アカウント紐付け解除の方法

2.1.4 のユースケースに対応する。【SAMLProfiles】の *4.5 Name Identifier Management Profile* に従って紐付け解除を行うものとする。

3.4 認証情報の共有方法

2.1.1～2.1.3 のユースケースに対応する。認証情報を要求するポータルは、【SAMLProfiles】の *6 Assertion Query/Request Profile* に従って認証情報を要求するものとする。また、処理を要求するポータルが、【SAMLToken】に従い、あらかじめ要求メッセージに認証情報を埋め込んで送ることも可能とする。

3.5 属性情報の共有方法

2.1.1、2.1.2 のユースケースに対応する。ポータル間での属性情報の共有は、あらかじめ同一ユーザのアカウントを紐付けしているポータル同士でのみ行われ、【LibertyWSFDST】に従い、属性情報をポータル間でやりとりするものとする。

3.6 URL 長

携帯電話に機能制限がある場合を考慮して、携帯電話を経由してポータル間でやりとりされる、<AuthenRequest>メッセージや<Response>メッセージにおける URL 長は、256byte までとする。

3.7 ユーザ承認の確認

本ガイドラインでは、アカウント紐付け・解除を行う場合、ユーザのブラウザ上に承認を求める画面を表示し、ユーザの同意が得られたときのみアカウント紐付け・解除を実行することを推奨する。

（解説）SAML2.0 ではアカウント紐付け・解除におけるユーザ承認確認は規定されていないが、個人情報がやりとりされる可能性のある処理であるため。

また、ポータル間で属性情報を交換する際は、【LibertyInteraction】に従ってユーザ承認を確認するものとする。【LibertyInteraction】の *2 Overview* において属性情報を提供するポータル(WSP : Web Service Provider に相当)がユーザとインタラクションするための 4 通りの方法を整理しているが、端末非固定の場合は 4 種類のうちいずれかを用いてユーザ承認を確認するものとする。一方、端末固定の場合は、情報を提供するポータルが、そのポータルにアクセス可能な端末を介してユーザ承認を確認することが望ましい。そのため、【LibertyInteraction】の *Figure 1* で示される、属性情報を提供するポータル自身がユーザとインタラクションを行う方法を推奨する。なお端末固定の場合、【LibertyInteraction】の *Figure 1* において、HTTP リダイレクトを行うステップでは、本ガイドライン 3.2.2 の①③④と同様の方法を用いて、ユーザが端末間で情報を移動させなければならない。

3.8 携帯ポータルから提供する ID 情報の表現方法

本節では、認証アサーション、属性アサーションおよびアーティファクトに関して、日本のモバイル環境を考慮した、記述等に関する指針を示す。なお、ここで触れない部分に関しては【SAMLCore】に従うものとする。

3.8.1　認証情報の表現方法

3.8.1.1　携帯ポータルにおける主な認証方式

携帯ポータルにおける主な認証方式として、以下に挙げる方式の概要と特徴をまとめる。

（1）通信回線に基づく認証
（2）公開鍵証明書（携帯電話加入者証明書）に基づく認証
（3）パスワードに基づく認証
（4）携帯電話に固有な識別情報通知に基づく認証

（1）通信回線に基づく認証

携帯事業者は、発信先の携帯電話番号（通信回線）を特定するために、UIM 等の通信情報を用いて認証を行っている。携帯ポータルを提供する通信事業者では、この通信回線の認証を基に利用者を特定することが可能となる。

◆ 特徴
- 通信の安全性に基づく認証であり、なりすましなどが困難。
- 利用者は認証操作を意識する必要がない。

（2）公開鍵証明書（携帯電話加入者証明書）に基づく認証

携帯電話が携帯電話加入者証明書（2002 年度・認証 WG 報告書参照）を保持している場合、携帯ポータルでは携帯電話加入者証明書に記載のあるモバイル ID の認証を基に利用者を特定することが可能となる。

◆ 特徴

- SSL/TLS 等の標準的な認証プロトコルで認証できる。
- 秘密鍵の安全な管理と公開鍵暗号の強度に基づき、なりすましが困難。
- PIN 等と組み合わせ認証できる。
- 利用者が証明書を取得している必要がある。

（3）パスワードに基づく認証

携帯ポータルがパスワードを管理している場合、利用者が携帯ポータルに接続する際や携帯ポータル内の特定サービス利用時に、携帯電話番号等のログイン名とパスワードを求めることで、利用者を特定することが可能となる。

◆ 特徴

- 通信経路や利用者端末に依存しない。
- 利用者はパスワードを覚え、入力する必要がある。

（4）携帯電話に固有な識別情報通知に基づく認証

携帯電話から通知される、携帯電話が固有に所持する製造番号などの識別情報に基づき、利用者を特定することが可能となる。

◆ 特徴

- 機種変更に伴い識別情報が変更するため、アカウントの再設定が必要となる。
- なりすまし防止のためには、他の認証方式と組み合わせる必要がある。

3.8.1.2　認証結果の表現方法

携帯ポータルから提供される認証結果として、【SAMLCore】で規定する認証アサーションで表現することとする。

認証アサーションの記載事項として以下を定める。

◆ Subject

アカウント紐付けの項において規定した共有識別子を記載することとする

◆ AuthnContext

表 2 に記載した認証方式のいずれかで表現することを推奨する。

なお、表 2 では、前項でまとめた携帯ポータルにおける主な認証方式に基づき、【SAMLAuthnContext】において定義する認証方式を整理している。

表 2：携帯ポータルから提供する認証方式

認証方式	概要
MobileOneFactorContract	モバイルデバイス（登録手続きあり）。 通信回線に基づく認証が該当。
MobileTwoFactorContract	モバイルデバイスの所持と PIN 等の組合せ（登録手続きあり）。 携帯電話加入者証明書に基づく認証が該当。
MobileOneFactorUnregistered	モバイルデバイスのみ（登録手続きなし）。 携帯電話に固有な識別情報通知に基づく認証が該当。
Password	パスワード確認。 パスワードに基づく認証が該当。
Public Key – X.509	公開鍵証明書利用。 携帯電話加入者証明書に基づく認証が該当。
Smartcard	スマートカード利用。 通信回線に基づく認証（但，3G のみ）及び携帯電話加入者証明書に基づく認証が該当。

3.8.2　属性情報の表現方法

3.8.2.1　属性情報の定義

本ガイドラインでは、携帯ポータルで扱う属性情報として、2005 年度認証 WG 報告書に整理されている属性情報の表現方法を定義する。

3.8.2.2　属性情報の表現方法

携帯ポータルと他ポータル間で交換される属性情報は、【SAMLCore】で規定される属性アサーションによって表現される。

属性アサーションの記載事項として以下を定める。

- ◆ Subject 要素
  アカウント紐付けの項において規定した共有識別子を記載することとする。
- ◆ Attribute 要素
  本要素の子要素である AttributeValue 要素は、3.8.2.1 で定義した属性情報で表現する。
  AttributeValue 要素の XML のスキーマ定義を表 3 に示す。なお、XML 文書例については、「付録」を参照されたい。

表 3：XML スキーマ定義一覧

通番	項目名称	要素名	表記方針	表記例	制約	スキーマ既定方針
1	名前	LLegalName	全角	属性　太郎		【LibertySISPP】LegalIdentity に従う
2	住所	AddressCard	全角	東京都属性区青坂1－2－3日本青坂ビル10F		【LibertySISPP】AddressCard に従う
3	生年月日	DOB	半角数字	2005-08-15	日付表記（yyyy-mm-dd）	【LibertySISPP】LegalIdentity に従う
4	性別	Gender	半角英字	m		【LibertySISPP】LegalIdentity に従う
5	携帯電話番号	MsgContact	半角数字	01234XX7890		【LibertySISPP】MsgContact に従う
6	携帯メールアドレス	MsgContact	半角英数字記号	aaXXa@doXXmo.ne.jp		【LibertySISPP】MsgContact に従う
7	自宅電話番号	MsgContact	半角数字	0344XX5555		【LibertySISPP】MsgContact に従う
8	自宅 FAX 番号	MsgContact	半角数字	036XX67777		【LibertySISPP】MsgContact に従う
9	自宅メールアドレス	MsgContact	半角英数字記号	bbXXb@ccc.moXXra.ne.jp		【LibertySISPP】MsgContact に従う
10	職種	Occupation	全角	会社員、公務員、学生、主婦、自営業、パート・アルバイト、その他等		新規に定義する
11	所属組織	LOU	全角	株式会社属性商事法人営業本部、属性大学大学院理工学研究科等		【LibertySISEP】LOU に従う
12	所属組織住所	AddressCard	全角	東京都属性区青坂1－2－3日本青坂ビル10F		【LibertySISPP】AddressCard に従う
13	所属組織電話番号	MsgContact	半角数字	0344XX5555		【LibertySISPP】MsgContact に従う
14	所属組織役職	LInternalJobTitle	全角	課長、部長、社長等		【LibertySISEP】LInternalJobTitle に従う
15	所属識別子（社員番号、会員番号等）	EmployeeID	半角英数字	BD73KF82905		【LibertySISEP】EmployeeID に従う
16	サービス提供組織	serviceProviderName	全角	TUTUYA、JTA、等		新規に定義する
17	サービス提供組織住所	serviceProviderAddress	全角	東京都属性区青坂1－2－3日本青坂ビル10F		新規に定義する
18	サービス提供組織電話番号	serviceProviderNumber	半角数字	0344XX5555		新規に定義する
19	会員役職	Role	全角	シルバー、ゴールド等		新規に定義する
20	会員識別子	memberAccount	半角英数字	BD73KF82905		新規に定義する
21	身長	Length	半角数字	198.5	0.5 単位の cm	新規に定義する
22	体重	Weight	半角数字	128.5	0.5 単位の kg	新規に定義する
23	スリーサイズ	bwhSize	半角数字	78.5,55.5,75.5	0.5 単位の cm	新規に定義する
24	フットサイズ	footSize	半角数字	28.5	0.5 単位の cm	新規に定義する
25	血液型	Bloodtype	半角英字	A		新規に定義する
26	既婚・未婚	Marriage	全角	既婚		新規に定義する
27	子供の有無	Children	全角	有		新規に定義する
28	趣味・嗜好	Interest	全角	映画，読書，テニス等		新規に定義する
29	記憶認証情報	Password	半角英数字記号	zokusei,rdovipocri		新規に定義する
30	生体認証情報	Biometrics	jpg ファイル	顔写真情報等		新規に定義する
31	クレジットカード番号	creditCardNumber	半角数字	11112222XXXX4444		新規に定義する
32	クレジットカード有効期限	creditCardValidity	半角数字	1205	日付表記（mmyy）	新規に定義する
33	デビットカード番号	debitCardNumber	半角数字	銀行番号＋店番号＋口座番号		新規に定義する

				00003331234567		
34	運転免許証 ID	driverLicenseID	半角数字	0123XXXX8901		新規に定義する
35	支払い証明証	paymentEvidence	半角数字	2,000,000		新規に定義する
36	所有物名称	itemName	全角	パソコン、キーホルダー等		新規に定義する
37	所有物 UID	possessionUniqueIdentifier	半角英数字	BD73KF82905		新規に定義する
38	所有物 Type	itemType	全角	携帯端末、文房具等		新規に定義する
39	GPS 情報	Coord	半角英数字	様々な表現手法があるため、例示なし		【LibertySISGL】coord に従う
40	ID-Tag 情報	IDTagInformation	半角英数字	BD73KF82905		新規に定義する
41	時刻情報	Time	半角数字	20051018103010.3450	24H 表記（YYYYMMDDHHMMSS.SSSS）	新規に定義する
42	利用サービス名称	serviceName	全角	XX マート、TSUXXYA 等		新規に定義する
43	利用サービス UID	serviceUID	半角英数字	BD73KF82905		新規に定義する

3.9 要求条件との対応関係

要求条件番号	要求条件	対応関係
ID-1	TV ポータル及び携帯ポータルで紐付け可能なポータル URL を管理すること	3.2 アカウント紐付け方法
ID-2	携帯ポータルが生成する情報を基に、TV ポータルとアカウント紐付けできること（端末非固定の場合のみでなく、端末固定の場合においても紐付けできること）	
ID-3	TV ポータルからユーザに対するアカウント紐付けの承認確認できること（端末非固定の場合のみでなく、端末固定の場合においても承認確認できること）	3.7 ユーザ承認の確認
ID-4	一度アカウントが紐付けされると、解除を行わない限り紐付けは保持されること	3.2 アカウント紐付け方法
ID-5	TV ポータルが生成する情報を基に、携帯ポータルとアカウント紐付けできること（端末非固定の場合のみでなく、端末固定の場合においても紐付けできること）	
ID-6	携帯ポータルからユーザに対するアカウント紐付けの承認確認できること（端末非固定の場合のみでなく、端末固定の場合においても承認確認できること）	3.7 ユーザ承認の確認
ID-7	携帯ポータルが生成する情報を基に、TV ポータルとアカウントの紐付け解除ができること（端末非固定の場合のみでなく、端末固定の場合においても紐付け解除できること）	3.3 アカウント紐付け解除の方法
ID-8	TV ポータルからユーザに対するアカウント紐付け解除の承認確認できること（端末非固定の場合のみでなく、端末固定の場合においても承認確認できること）	3.7 ユーザ承認の確認

AH-1	ポータルは必要に応じて認証情報の取得要求を連携先ポータルに対して送信し、連携先ポータルは、それに対して共通的な形式で認証情報を開示する	3.4 認証情報の共有方法 3.8.1 認証情報の表現方法
AT-1	携帯ポータルから利用者に登録情報のコピーに対する承諾を得ること	3.7 ユーザ承認の確認
AT-2	ポータル間で、登録情報が共通的な形式で共有されること	3.5 属性情報の共有方法 3.8.2 属性情報の表現方法

【付録】　属性情報の XML 文書例

```
<?xml version="1.0" encoding="UTF-8"?>
<AttributeValue xmlns:pp="urn:liberty:id-sis-pp:2005-05" xmlns:ep="urn:liberty:id-sis-ep:2005-05"
xmlns:gl="urn:liberty:id-sis-gl:2005-02">
  <pp:LLegalName xml:lang="jp">属性　太郎</pp:LLegalName>
  <pp:AddressCard>
    <pp:AddrType>urn:liberty:id-sis-pp:addrType:domicile</pp:AddrType>
    <pp:Address>
      <pp:LPostalAddress xml:lang="jp">青坂１－２－３日本青坂ビル１０Ｆ</pp:LPostalAddress>
      <pp:LL xml:lang="jp">属性区</pp:LL>
      <pp:LSt xml:lang="jp">東京都</pp:LSt>
    </pp:Address>
  </pp:AddressCard>
  <pp:DOB>2005-08-15</pp:DOB>
  <pp:Gender>urn:liberty:id-sis-pp:gender: m</pp:Gender>
  <pp:MsgContact>
    <pp:MsgType>urn:liberty:id-sis-pp:msgType:mobile</pp:MsgType>
    <pp:MsgMethod>urn:liberty:id-sis-pp:msgMethod:voice</pp:MsgMethod>
    <pp:MsgAccount>01234XX7890</pp:MsgAccount>
  </pp:MsgContact>
  <pp:MsgContact>
    <pp:MsgType>urn:liberty:id-sis-pp:msgType:mobile</pp:MsgType>
    <pp:MsgMethod>urn:liberty:id-sis-pp:msgMethod:email</pp:MsgMethod>
    <pp:MsgAccount>aaXXa@doXXmo.ne.jp</pp:MsgAccount>
  </pp:MsgContact>
  <pp:MsgContact>
    <pp:MsgType>urn:liberty:id-sis-pp:msgType:personal</pp:MsgType>
    <pp:MsgMethod>urn:liberty:id-sis-pp:msgMethod:voice</pp:MsgMethod>
    <pp:MsgAccount>0344XX5555</pp:MsgAccount>
  </pp:MsgContact>
  <pp:MsgContact>
    <pp:MsgType>urn:liberty:id-sis-pp:msgType:personal</pp:MsgType>
    <pp:MsgMethod>urn:liberty:id-sis-pp:msgMethod:fax</pp:MsgMethod>
    <pp:MsgAccount>036XX67777</pp:MsgAccount>
  </pp:MsgContact>
  <pp:MsgContact>
    <pp:MsgType>urn:liberty:id-sis-pp:msgType:personal</pp:MsgType>
    <pp:MsgMethod>urn:liberty:id-sis-pp:msgMethod:email</pp:MsgMethod>
    <pp:MsgAccount>aaXXa@ccc.moXXra.ne.jp</pp:MsgAccount>
  </pp:MsgContact>
  <occupation>会社員</occupation>
  <ep:LOU>株式会社属性商事法人営業部</ep:LOU>
  <pp:AddressCard>
    <pp:AddrType>urn:liberty:id-sis-pp:addrType:work</pp:AddrType>
```

```
    <pp:Address>
      <pp:LPostalAddress xml:lang="jp">青坂１－２－３日本青坂ビル１０Ｆ</pp:LPostalAddress>
      <pp:LL xml:lang="jp">属性区</pp:LL>
      <pp:LSt xml:lang="jp">東京都</pp:LSt>
    </pp:Address>
  </pp:AddressCard>
  <pp:MsgContact>
    <pp:MsgType>urn:liberty:id-sis-pp:msgType:work</pp:MsgType>
    <pp:MsgMethod>urn:liberty:id-sis-pp:msgMethod:voice</pp:MsgMethod>
    <pp:MsgAccount>0344XX5555</pp:MsgAccount>
  </pp:MsgContact>
  <ep:LInternalJobTitle xml:lang="jp">課長</ep:LInternalJobTitle>
  <ep:EmployeeID>BD73KF82905</ep:EmployeeID>
  <serviceProviderName>ＴＵＴＵＹＡ</serviceProviderName>
  <serviceProviderAddress>東京都属性区青坂１－２－３日本青坂ビル１０Ｆ</serviceProviderAddress>
  <serviceProviderNumber>0344XX5555</serviceProviderNumber>
  <role>シルバー</role>
  <memberAccount>BD73KF82905</memberAccount>
  <length unit=”cm”>198.5</length>
  <weight unit=”kg”>128.5</weight>
  <bwhSize unit=”cm”>78.5,55.5,75.5</bwhSize>
  <footSize unit=”cm”>28.5</footSize>
  <bloodType>A</bloodType>
  <marriage>既婚</marriage>
  <children>有</children>
  <interest>映画</interest>
  <password>zokusei,rdovipocri</password>
  <biometrics>http://www.ddXd.ne.jp/XXXX/eeXe.jpg</biometrics>
  <creditCardNumber>11112222XXXX4444</creditCardNumber>
  <creditCardValidity>1205</creditCardValidity>
  <debitCardNumber>00003331234567</debitCardNumber>
  <driverLicenseID>0123XXXX8901</driverLicenseID>
  <paymentEvidence>2,000,000</paymentEvidence>
  <itemName>パソコン</itemName>
  <possessionUniqueIdentifier>BD73KF82905</possessionUniqueIdentifier>
  <itemType>携帯端末</itemType>
  <gl:coode>
    <gl:x>30 16 28.312N</gl:x>
    <gl:y>45 15 33.431E</gl:y>
  </gl:coord>
  <IDTagInformation>BD73KF82905</IDTagInformation>
  <time>20051018103010.3450</time>
  <serviceName>ＸＸマート</serviceName>
  <serviceUID>BD73KF82905</serviceUID>
</AttributeValue>
```

ID 連携スキームガイドライン

MC-03　1.0 版

平成 22 年 7 月　1.0 版第 1 刷発行

発　行　所

社団法人　電　　波　　産　　業　　会
高度無線通信研究委員会モバイルコマース部会
〒100-0013　東京都千代田区霞が関１－４－１
日土地ビル１１階
電　話　03-5510-8594
ＦＡＸ　03-3592-1103