(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5920891号
(P5920891)
(45)発行日　平成28年5月18日(2016.5.18)　(24)登録日　平成28年4月22日(2016.4.22)

(51)Int.Cl.　　F I
G06F 21/41 (2013.01)　G06F 21/41
H04W 12/06 (2009.01)　H04W 12/06
H04W 92/24 (2009.01)　H04W 92/24

請求項の数 8　(全 17 頁)

(21)出願番号　特願2013-23141(P2013-23141)
(22)出願日　平成25年2月8日(2013.2.8)
(65)公開番号　特開2014-153917(P2014-153917A)
(43)公開日　平成26年8月25日(2014.8.25)
審査請求日　平成27年2月10日(2015.2.10)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　110001863
特許業務法人アテンダ国際特許事務所
(72)発明者　馬場　宏基
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　河村　憲一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　安川　正祥
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】通信サービス認証・接続システム及びその方法

(57)【特許請求の範囲】
【請求項１】
第１通信網に接続された端末から第２通信網に対応する認証情報を用いてWebサービスにアクセスしたときに、該Webサービスが前記第１通信網のID提供サーバに前記端末に対するID発行を依頼し、該ID提供サーバは前記第１通信網のID連携プロファイルサーバにID発行条件を要求し、前記ID提供サーバが前記ID連携プロファイルサーバからID発行条件を得られたときに前記端末の前記Webサービスへのアクセスが可能となる通信サービス認証・接続システムにおいて、
複数の通信網の前記ID連携プロファイルサーバに接続可能なプロファイル連携プロキシを設け、
前記プロファイル連携プロキシは、
前記複数の通信網におけるID連携プロファイルサーバ間でID発行条件を流通する機能と、
前記第１通信網のID連携プロファイルサーバからの前記ID発行条件の問い合わせを解析して、前記認証情報を発行した問い合わせ対象となる前記第２通信網のID連携プロファイルサーバを解析する機能と、
前記問い合わせ対象となる第２通信網のID連携プロファイルサーバに対してID発行条件を問い合わせる機能と、
前記問い合わせ対象となる第２通信網のID連携プロファイルサーバから受信したID発行条件を問い合わせ元の前記ID連携プロファイルサーバに送信する機能とを備え、

前記第１通信網のID提供サーバは、
前記Webサービスから前記端末に対するID発行依頼を受けたときに、前記第１通信網のID連携プロファイルサーバと前記プロファイル連携プロキシとを介して前記第２通信網のID連携プロファイルサーバから前記端末のID発行条件を取得することにより、前記端末のシングルサインオンを確立する機能を備えている
ことを特徴とする通信サービス認証・接続システム。
【請求項２】
前記プロファイル連携プロキシは、
前記ID発行条件の問い合わせの要求・応答の信号の中継時に、問い合わせ元通信網及び問い合わせ先通信網のポリシーによって信号内容を変換する
ことを特徴とする請求項１に記載の通信サービス認証・接続システム。
【請求項３】
前記プロファイル連携プロキシは、問い合わせ先となる複数の通信網のID連携プロファイルサーバの宛先情報を保持する機能を有する
ことを特徴とする請求項１又は２に記載の通信サービス認証・接続システム。
【請求項４】
前記プロファイル連携プロキシは、複数のモバイル通信網に接続された固定通信網に配備されている
ことを特徴とする請求項１乃至３の何れかに記載の通信サービス認証・接続システム。
【請求項５】
前記プロファイル連携プロキシは、固定通信網とモバイル通信網に接続された第三者の仲介事業者の通信網に配備されている
ことを特徴とする請求項１乃至３の何れかに記載の通信サービス認証・接続システム。
【請求項６】
第１通信網に接続された端末から第２通信網に対応する認証情報を用いてWebサービスにアクセスしたときに、該Webサービスが前記第１通信網のID提供サーバにID発行を依頼し、該ID提供サーバは前記第１通信網のID連携プロファイルサーバにID発行条件を要求し、前記ID提供サーバが前記ID連携プロファイルサーバからID発行条件を得られたときに前記端末の前記Webサービスへのアクセスを可能にする通信サービス認証・接続方法において、
複数の通信網の前記ID連携プロファイルサーバに接続可能なプロファイル連携プロキシを設け、
前記プロファイル連携プロキシは、
前記複数の通信網におけるID連携プロファイルサーバ間でID発行条件を流通し、
前記第１通信網のID連携プロファイルサーバからの前記ID発行条件の問い合わせを解析して、前記認証情報を発行した問い合わせ対象となる前記第２通信網のID連携プロファイルサーバを解析し、
前記問い合わせ対象となる第２通信網のID連携プロファイルサーバに対してID発行条件の問い合わせを行い、
前記問い合わせ対象となる第２通信網のID連携プロファイルサーバから受信したID発行条件を問い合わせ元の前記ID連携プロファイルサーバに送信し、
前記第１通信網のID提供サーバは、前記Webサービスから前記端末に対するID発行依頼を受けたときに、前記第１通信網のID連携プロファイルサーバと前記プロファイル連携プロキシとを介して前記第２通信網のID連携プロファイルサーバから前記端末のID発行条件を取得することにより、前記端末のシングルサインオンを確立する
ことを特徴とする通信サービス認証・接続方法。
【請求項７】
前記プロファイル連携プロキシは、前記ID発行条件の問い合わせの要求・応答の信号の中継時に、問い合わせ元通信網及び問い合わせ先通信網のポリシーによって信号内容を変換する

ことを特徴とする請求項６に記載の通信サービス認証・接続方法。
【請求項８】
前記プロファイル連携プロキシは、問い合わせ先となる複数の通信網のID連携プロファイルサーバの宛先情報を保持する
ことを特徴とする請求項６又は７に記載の通信サービス認証・接続方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数の通信網を介した通信サービス利用時のユーザ認証・接続に関し、特に、固定網やモバイル網への接続時の認証・接続を行う通信サービス認証・接続システム及びその方法に関するものである。
【背景技術】
【０００２】
移動体端末の認証に用いられるUICC（Universal Integrated Circuit Card：SIM（Subscriber Identity Module） カード）は、セキュリティ機能の高さから広く用いられている。さらに、SIMカードの認証結果を基にして上位のサービス（Webサービス）に対してシングルサインオンを実現するため、3GPP（Third Generation Partnership Project）ではGBA（Generalized Bootstrapping Architecture, 非特許文献１ TS33.220）によるアプリケーションレベルでのSIM認証技術や、１つのユーザーIDで複数のWebサイトを使える認証技術であるOpenIDとの連携技術が検討されている。（非特許文献２ 3GPP TR33.980、非特許文献３、非特許文献４）
IEEE 802.1XはLAN接続時に使用する認証技術であり、あらかじめ決められた端末機器以外がコンピュータ・ネットワークに参加しないように認証によって接続を規制する規格である。また、EAP-AKAは、EAP(Extensible Authentication Protorol)上でSIMを使ったAKA認証を実施するプロトコルである。
【０００３】
例えば、802.1X(EAP-AKA)による通信では、図４に示すように、通信が行われる。すなわち、端末(801)と公衆WiFi(802)の接続時に端末(801)から認証要求が送信される(901)と、固定網(804)のWiFi AP(802)はEAP-SIMによる認証を要求する(902)。端末(801)はＳＩＭカード内に保存されたID情報をEAP応答に含めて送信する(903)。
【０００４】
WiFi AP(802)はID情報を固定網(804)の認証サーバ((AAA)サーバ)(803)に送信する(904)。AAAサーバ(803)はEAP-AKA認証の開始を要求する(905)。
【０００５】
WiFI AP(802)は端末(801)にEAP-AKA認証開始要求を送信する(906)。
【０００６】
端末(801)はWiFi AP(802)にEAP-AKA認証開始要求に対する応答を送信する(907)。WiFi AP(802)はEAP-AKA認証開始要求への応答をAAAサーバ(803)に送信する(908)。
【０００７】
AAAサーバ(803)は移動網(809)のHSS(807)から認証データ（認証ベクトル）を取得する(909,910)。
【０００８】
AAAサーバ(803)はAKA認証のチャレンジをWiFi AP(802)に送信し(911)、WiFi AP(802)は端末(801)にチャレンジを送信する(912)。
【０００９】
端末(801)はチャレンジにあったレスポンス値を計算し、WiFi AP(802)経由でAAAサーバ(803)に送信する(913.914)。
【００１０】
AAAサーバ(803)はチャレンジとレスポンス値の関係が正しければ認証を完了し、接続を許可するようにWiFi AP(802)に通知する(915)。

【００１１】
WiFi AP(802)は当該端末(801)の通信を許可するようMACアドレス等の端末情報を接続許可リストに登録し、端末(801)に認証完了を通知する(916)。
【００１２】
また、GBAは移動体網のネットワーク接続時に用いるSIM認証をHTTPベースのサービスにおいても利用する技術である。図４における移動網(809)のNAF(Network Application Function)(805)は、実際にアプリケーションを提供する機能であり、移動網(809)のBSF(Bootstrapping function)(808)は、HTTPを使ってSIM認証を行う機能である。
【００１３】
GBAを用いた通信では、まず端末(801)からNAF(805)へ接続を要求する(931)とNAF(805)は認証処理を端末に要求する(932)。
【００１４】
端末(801)は指定されたBSF(808)にユーザIDを含む認証要求を送信する(933)。
【００１５】
BSF(808)はHSS(807)から当該ユーザのAKA認証データ(認証ベクトル)を取得する(934,935)。
【００１６】
BSF(808)は認証データをもとにしてチャレンジを端末(801)に送信する(936)。
【００１７】
端末(801)はチャレンジに対するレスポンスを計算し、認証応答としてBSF(808)に送信する(937)。
【００１８】
BSF(808)はチャレンジに対するレスポンスの関係が正しいかを検証し、正しい場合には認証を完了し、端末(801)に認証成功を通知する(938)。このとき、Bootstrapping Transaction Identifier(B-TID)を付与する。
【００１９】
端末(801)はB-TIDを以ってNAF(805)に再度アクセスする(939)。
【００２０】
NAF(805)は送信されたB-TIDが本当にBSFによって払い出されたものかを検証するため、B-TIDの検証をBSF(808)に依頼する(940)。
【００２１】
BSF(808)は検証結果をNAF(805)に通知して(941)、NAF(805)は端末(801)の認証を完了し(942)、セッションを確立する(943)。
【００２２】
また、3GPP TR33.980ではGBAを使ったアプリケーションレベルのSIM認証とOpenID/SAMLを連動して、シングルサインオンの技術を検討している。GBA-OpenID/SAML連携を用いた通信では、図５に示すように、 端末(801)からWebサービス(810)にHTTPでのシングルサインオンを用いた接続を要求する(961)。
【００２３】
Webサービス(810)は、端末(801)に対してIdP/NAF(811)と認証するようにリダイレクトする(962)。
【００２４】
端末(801)がIdP/NAF(811)に認証を要求する(963)と、IdP/NAF(811)は、BSF(808)とSIM認証するようにリダイレクトする(964)。
【００２５】
端末(801)はBSF(808)にHTTPでSIMカードに記録されたユーザIDを送信して認証を要求し(965)、以降はGBAのメカニズムでHTTPによるSIM認証実施し、B-TIDを生成し、端末(801)に送付する。IdP/NAF(811)がBSF(808)にB-TIDの正当性を検証して(972,973)、端末(801)とIdP/NAF(811)間の認証が完了して、セッションが確立される(974)。
【００２６】

IdP/NAF(811)は認証が完了すると、それを示すトークンを端末(801)に払い出す(975)。

【００２７】

端末(801)はそのトークンを以てWebサービス(810)に再度アクセスする(976)。

【００２８】

Webサービス(810)はトークンがIdP/NAF(811)によって発行されたかどうかを検証し(977)、正当性が確認できれば(978)、Webサービス(810)と端末(801)間の認証が完了して、セッションが確立される(979)。そして、Webサービス(810)は、端末(801)に対してHTTPの応答を行う(980)。

【００２９】

次に、3GPP TR33.980の概要を図６を参照して説明する。

【００３０】

図６において、モバイル網（移動網）(101)におけるIdP(102)は、ユーザの認証と属性情報を提供する機能であり、ユーザがWebサービス(103)にアクセスすると、Webサービス(103)はIdP(102)にアクセスをリダイレクトする。IdP(102)はこれを受けてSIMを用いた端末認証を行う。また、IdP(102)はユーザのCookieを確認して、既に認証済みである場合は、２回目以降のユーザに対する認証は行わず、シングルサインオンを実施する。また、IdP(102)はユーザに関してWebサービス(103)が要求する属性情報を、DBから取得して、Webサービスに送信する。この際、サービスに情報を送信して良いかどうか、ポリシーを確認する。

【００３１】

HSS(104)は、加入者データベースサーバであり、ユーザのNW（ネットワーク）接続に関する認証情報、ネットワークサービス加入属性情報を管理する。

【００３２】

ID連携プロファイルサーバ(105)は、IdP(102)がIDを発行する際にWebサービス(103)に対して認証情報や属性情報の提供をして良いか否かの情報であるID発行条件を、ユーザ毎に管理するサーバである。

【００３３】

上記構成のシステムにおいては、次のように端末とWebサービスとの間の認証か行われる。

【００３４】

端末(106)がWebサービス(103)を利用するためアクセスする。

【００３５】

Webサービス(103)はユーザの認証を要求し、IdP(102)と通信するように端末(106)からのアクセスをリダイレクトする。

【００３６】

端末(106)とIdP(102)の間でSIMカードを使った認証を実行する（認証(SIM)）。

【００３７】

IdP(102)はID連携プロファイルサーバ(105) にID発行条件を問い合わせ、ID連携プロファイルサーバ(105)はID発行条件を応答する（プロファイル確認）。

【００３８】

Webサービス(103)はIdP(102)に対して当該のアクセスに対する認証をIdP(102)に依頼し、当該ユーザのIDの検証を要求する（ＩＤ検証要求）。

【００３９】

IdP(102)からWebサービス(103)にID検証結果を通知する（ＩＤ検証結果）。

【００４０】

端末(106)とWebサービス(103)の認証が完了する（認証完了）。

【先行技術文献】

【非特許文献】

【００４１】

【非特許文献１】3GPP TR33.980 V11.4.0(2012-09)

【非特許文献２】3GPP TR33.980 V11.0.0(2012-09)
【非特許文献３】Andreas Leicher, Andreas U. Schmidt, and Yogendra Shah, “SmartOpenID: A Smart Card Based OpenID Protocol,” SEC 2012, IFIP AICT 376, pp. 75-86, 2012, IFIP International Federation for Information Processing 2012
【非特許文献４】Charlott Lorentzen, Markus Fiedler, and Peter Lorentzen, “Decisive Factors for Quality of Experience of OpenID Authentication Using EAP,” ADVANCES IN ELECTRONICS AND TELECOMMUNICATIONS, VOL. 2, NO. 3, SEPTEMBER 2011
【発明の概要】
【発明が解決しようとする課題】
【００４２】
しかしながら、前述した従来のシステムにおいては、ID提供サーバ（IdP：Identity Provider）(102)は、端末が認証を要求してきたサービスに対して、SIMカードを使った認証結果を提供する機能である。また、IdP(102)は、本来単一の通信網事業者が管理・運用するものであったが、異なるネットワーク（通信網）間で同一IDに基づいた認証情報をWebサービス事業者に提供する場合、IDの払い出し条件が統一できない。
【００４３】
上記課題に関して図７を参照して詳細に説明する。
【００４４】
図７において、前述した図６と同一構成部分は同一符号をもって表す。
【００４５】
AAAサーバ(204)は、固定網(201)においてモバイル網(101)を運営する移動体事業者のSIMカードを使ってネットワークに接続するための認証サーバであり、認証データの問い合わせのため、モバイル網(101)のHSS(104)にSIMによる認証に必要な認証情報を問い合わせる。
【００４６】
ここでは固定網(201)でもIdP機能を持ち、移動体端末(106)が固定網(201)にWiFi等で移動体事業者のSIMカードを使って接続し、WebサービスにSIMの認証データを提供するケースを想定して説明する。
【００４７】
図４を参照して説明したEAP-AKAと同様に、端末(106)は固定網(201)にSIM認証による認証後、固定網(201)に接続する。
【００４８】
端末(106)からWebサービス(103A,103B)にアクセスする。
【００４９】
Webサービス(103A,103B)は端末を認証のためIdP(202)にリダイレクトして、ID発行を依頼する。
【００５０】
端末(106)とIdP(202)の間でSIM認証手続きを実施する。
【００５１】
IdP(202)はSIM認証に用いる認証データを取得するためAAAサーバ(204)を介してHSS(104)からSIM認証データを取得する。
【００５２】
認証完了後、IdP(202)はID連携プロファイルサーバ(203)にID発行条件を要求する。
【００５３】
このとき、固定網(201)のID連携プロファイルサーバ(203)は当該のユーザに対応したID発行条件を持っていないため、IdP(202)において認可を要求してきたWebサービス(103A,103B)に対してID情報を提供してよいのか判断できない。
【００５４】
本発明は上記の問題点に鑑み、固定網やモバイル網などの通信網の違いによらずSIM等を用いるネットワーク認証を使ったシングルサインオンが可能であり、端末がアクセスす

るネットワーク（通信網）の違いによりWebサービス側でSIM認証が使えなくなることがない通信サービスの認証・接続システム、及びその方法を提供することである。

【課題を解決するための手段】

【００５５】

本発明は上記の目的を達成するために、第１通信網に接続された端末から第２通信網に対応する認証情報を用いてWebサービスにアクセスしたときに、該Webサービスが前記第１通信網のID提供サーバに前記端末に対するID発行を依頼し、該ID提供サーバは前記第１通信網のID連携プロファイルサーバにID発行条件を要求し、前記ID提供サーバが前記ID連携プロファイルサーバからID発行条件を得られたときに前記端末の前記Webサービスへのアクセスが可能となる通信サービス認証・接続システムにおいて、複数の通信網の前記ID連携プロファイルサーバに接続可能なプロファイル連携プロキシを設け、前記プロファイル連携プロキシは、前記複数の通信網におけるID連携プロファイルサーバ間でID発行条件を流通する機能と、前記第１通信網のID連携プロファイルサーバからの前記ID発行条件の問い合わせを解析して、前記認証情報を発行した問い合わせ対象となる前記第２通信網のID連携プロファイルサーバを解析する機能と、前記問い合わせ対象となる第２通信網のID連携プロファイルサーバに対してID発行条件を問い合わせる機能と、前記問い合わせ対象となる第２通信網のID連携プロファイルサーバから受信したID発行条件を問い合わせ元の前記ID連携プロファイルサーバに送信する機能とを備え、前記第１通信網のID提供サーバは、前記Webサービスから前記端末に対するID発行依頼を受けたときに、前記第１通信網のID連携プロファイルサーバと前記プロファイル連携プロキシとを介して前記第２通信網のID連携プロファイルサーバから前記端末のID発行条件を取得することにより、前記端末のシングルサインオンを確立する機能を備えていることを特徴とする通信サービス認証・接続システムを提案する。

【００５６】

さらに、本発明は上記の目的を達成するために、第１通信網に接続された端末から第２通信網に対応する認証情報を用いてWebサービスにアクセスしたときに、該Webサービスが前記第１通信網のID提供サーバにID発行を依頼し、該ID提供サーバは前記第１通信網のID連携プロファイルサーバにID発行条件を要求し、前記ID提供サーバが前記ID連携プロファイルサーバからID発行条件を得られたときに前記端末の前記Webサービスへのアクセスを可能にする通信サービス認証・接続方法において、複数の通信網の前記ID連携プロファイルサーバに接続可能なプロファイル連携プロキシを設け、前記プロファイル連携プロキシは、前記複数の通信網におけるID連携プロファイルサーバ間でID発行条件を流通し、前記第１通信網のID連携プロファイルサーバからの前記ID発行条件の問い合わせを解析して、前記認証情報を発行した問い合わせ対象となる前記第２通信網のID連携プロファイルサーバを解析し、前記問い合わせ対象となる第２通信網のID連携プロファイルサーバに対してID発行条件の問い合わせを行い、前記問い合わせ対象となる第２通信網のID連携プロファイルサーバから受信したID発行条件を問い合わせ元の前記ID連携プロファイルサーバに送信し、前記第１通信網のID提供サーバは、前記Webサービスから前記端末に対するID発行依頼を受けたときに、前記第１通信網のID連携プロファイルサーバと前記プロファイル連携プロキシとを介して前記第２通信網のID連携プロファイルサーバから前記端末のID発行条件を取得することにより、前記端末のシングルサインオンを確立することを特徴とする通信サービス認証・接続方法を提案する。

【発明の効果】

【００５７】

本発明の通信サービス認証・接続システム及びその方法によれば、固定網やモバイル網などの通信網の違いによらずSIM等の認証情報を用いるネットワーク認証を使ったシングルサインオンが可能となり、端末がアクセスする通信網の違いによりWebサービス側で認証情報が使えなくなることがない。

【図面の簡単な説明】

【００５８】

【図１】本発明の通信サービス認証・接続システムの概要を説明する図
【図２】本発明の一実施形態における通信サービス認証・接続システムを示す構成図
【図３】本発明の一実施形態における通信サービス認証・接続システムの通信の詳細を説明する図
【図４】802.1X(EAP-AKA)による通信を説明する図
【図５】GBA-OpenID/SAML連携(3GPP 33.980)を用いた通信を説明する図
【図６】従来例の3GPP TR33.980の概要を説明する図
【図７】従来例の通信サービス認証・接続システムにおける課題を説明する図
【発明を実施するための形態】
【００５９】
本発明はネットワーク（通信網）間においてシングルサインオン可能なサイト情報の交換機能を配備することで、ユーザがシングルサインオンにより認証する登録サイト情報を交換し、異なるネットワークにアクセスしてもSIMカード等による認証を可能とし、同一の条件で共通IDによってサービスへの認証・接続を行う技術である。
【００６０】
以下に、その一実施形態の詳細を説明する。
【００６１】
なお、本実施形態では、固定網(201)においてモバイル網(101)を運営する移動体事業者のSIM認証カードを使って接続する場合に関して説明する。
【００６２】
まず、図１を参照して、本発明の通信サービス認証・接続システムの概要を説明する。なお、以下の説明においては、固定通信網を固定網、モバイル通信網をモバイル網と称する。
【００６３】
図１において、前述した従来例と同一構成部分は同一符号をもって表す。
【００６４】
モバイル網（移動網）(101)におけるIdP（ID提供サーバ：Identity Provider）(102)は、ユーザの認証と属性情報を提供する機能を有し、ユーザがモバイル網(101)を介して端末(106)によってWebサービス(103A,103B)にアクセスすると、Webサービス(103A,103B)はIdP(102)にアクセスをリダイレクトする。IdP(102)はこれを受けてSIMを用いた端末認証を行う。
【００６５】
また、IdP(102)はCookie等を利用してユーザ認証状態を確認して、既に認証済みである場合は、２回目以降のユーザに対する認証は行わず、シングルサインオン機能を実現する。また、IdP(102)はユーザに関してWebサービス(103A,103B)が要求する属性情報を、データベースから取得して、Webサービス(103A,103B)に送信する。この際、サービスに情報を送信して良いかどうかのポリシーを確認する。
【００６６】
HSS(104)は、加入者データベースサーバであり、ユーザのモバイル網（ネットワーク）(101)への接続に関する認証情報とネットワークサービス加入属性情報などを管理する。
【００６７】
ID連携プロファイルサーバ(105)は、IdP(102)がIDを発行する際にWebサービス(103A,103B)に対して認証情報や属性情報の提供をして良いか否かの情報であるID発行条件を、ユーザ毎に管理するサーバである。
【００６８】
IdP(202)は、ユーザの認証情報と属性情報を提供する機能を有し、ユーザが端末(106)によって固定網(201)を介してWebサービス(103A,103B)にアクセスすると、Webサービス(103A,103B)はIdP(202)にアクセスをリダイレクトする。IdP(202)はこれを受けてSIMを用いた端末認証を行う。

【００６９】
また、IdP(202)はCookie等を利用してユーザの認証状態を確認して、既に認証済みである場合は、２回目以降のユーザに対する認証は行わず、シングルサインオン機能を実現する。また、IdP(202)はユーザに関してWebサービス(103A,103B)が要求する属性情報を、データベースから取得して、Webサービス(103A,103B)に送信する。この際、サービスに情報を送信して良いかどうかポリシー、すなわちID発行条件を確認する。
【００７０】
ID連携プロファイルサーバ(203)は、IdP(202)がIDを発行する際にWebサービス(103A,103B)に対して認証情報や属性情報の提供をして良いか否かの情報であるID発行条件を、ユーザ毎に管理するサーバである。
【００７１】
AAAサーバ(204)は、固定網(201)においてモバイル網(101)を運営する移動体事業者のSIMカードを使って接続するための認証サーバであり、認証データの問い合わせのため、モバイル網(101)のHSS(104)にSIMによる認証データを問い合わせる。
【００７２】
プロファイル連携プロキシ(300)は、ネットワークサービス事業者間、ここでは固定網(201)とモバイル網(101)との間でユーザIDの発行事業者が管理しているID情報のWebサービス(103A,103B)へのID発行条件を管理流通するために、ID発行条件の取得・回答を行う機能を有する。
【００７３】
なお、プロファイル連携プロキシ(300)の配備については２つのモデルが考えられる。１つは、固定網(201)に配備して、固定網(201)が複数のモバイル網のモバイルネットワーク事業者とIDを連携する場合に各モバイル網に問い合わせるために中継するモデルである。他方は、固定網(201)でもなく、モバイル網(101)でもなく、固定網(201)とモバイル網(101)の接続可能な第三者の仲介事業者の通信網にプロファイル連携プロキシ(300)を配備し、第三者の仲介事業者が固定網(201)とモバイル網(101)の事業者間のID連携を仲介するモデルである。この場合、固定網(201)でもモバイル網(101)でもない第三のネットワーク（インターネットも含む）にプロファイル連携プロキシ(300)が配備されることになる。プロファイル連携プロキシはサーバであるので、ネットワークに接続したコンピュータ上のソフトウェア機能になる。
【００７４】
次に、図１に示す構成からなる通信サービス認証・接続システムの動作を説明する。
【００７５】
端末(106)は固定網(201)にSIM認証による認証後、固定網(201)に接続する。
【００７６】
端末(106)からWebサービス(103A,103B)にアクセスする。
【００７７】
Webサービス(103A,103B)はIdP(202)にID発行を依頼する。
【００７８】
端末(106)とIdP(202)の間でSIM認証手続きを実施する。
【００７９】
IdP(202)はSIM認証に用いる認証データを取得するためAAAサーバか(204)らSIM認証データを取得する。
【００８０】
認証完了後、IdP(202)はID連携プロファイルサーバ(203)にID発行条件を要求する。
【００８１】
ID連携プロファイルサーバ(203)は、モバイル網(101)の事業者が発行したユーザIDであることをキーとして発行元にID情報の発行条件を問い合わせるため、プロファイル連携プロキシ(300)に問い合わせる。
【００８２】

プロファイル連携プロキシ(300)は、要求されたユーザIDの発行元の通信網事業者を特定し、当該通信網事業者のID連携プロファイルサーバ(105)からID発行条件を取得し、固定網(201)のID連携プロファイルサーバ(203)に応答する。

【００８３】

ID連携プロファイルサーバ(203)は、IdP(202)にID発行条件を応答する。

【００８４】

以上の処理によって、移動体事業者が発行したIDの発行条件に沿って固定網(201)のIdP(202)でもユーザIDの発行を制御することが可能となる。

【００８５】

次に、本実施形態におけるプロファイル連携プロキシの詳細を図２及び図３を参照して説明する。図２は構成図であり、図３は通信の詳細を説明する図である。

【００８６】

図２に示すように、固定網(201)のIdP(202)はID発行部(202A)と認証処理部(202B)とID発行条件確認部(202C)を備えてる。

【００８７】

ID発行部(202A)は、Webサービス(103A,103B)に対してIdP(202)が認証したユーザのID情報を発行する機能を有する。

【００８８】

認証処理部(202B)は、端末(106)と通信して、SIM認証要求をAAAサーバ(204)に送信し、AAAサーバ(204)でSIM認証が完了するとAAAサーバ(204)に認可情報を要求する機能を有する。

【００８９】

ID発行条件確認部(202C)は、ID連携プロファイルサーバ(203)と通信してユーザのID連携に関する属性情報であるID発行条件を取得する機能を有する。

【００９０】

ID連携プロファイルサーバ(203)は、IdP(202)に対してユーザのID連携属性情報であるID発行条件を提供する機能を有する。具体的には、Webサービスごとにユーザが ID連携機能によって認証することを登録しているかどうかなどの情報を送信する。このとき、IDを自網で発行した場合には、ID連携プロファイルサーバ(203)内のユーザ属性情報DB(203B)のデータを参照する。他の事業者が発行するIDの場合は、他事業者のIDに関するID発行条件を取得するため、プロファイル連携プロキシ(300)にサービス登録状況を要求する。

【００９１】

また、固定網(201)のID連携プロファイルサーバ(203)はサービス登録状況判定部(203A)と認可事業者識別部(203C)、他事業者認可条件判定部(203D)を備え、サービス登録状況判定部(203A)はユーザ属性情報DB(203B)有する。

【００９２】

サービス登録状況判定部(203A)は、自社が発行したIDについてユーザ毎にID連携対象として登録されたサービスの一覧を管理するユーザ属性情報DB(203B)を有し、ID連携サービスに登録しているユーザについて、登録された属性を管理し、IdP(202)からの問い合わせに応じてユーザ毎のサービス登録状況を確認し、ID連携可否情報であるID発行条件をIdPに応答するとともに、IdP(202)からのID発行条件の要求に応じてユーザ属性情報DB(203B)から当該ユーザのID発行条件を取り出して応答する機能を有する。

【００９３】

また、サービス登録状況判定部(203A)は、特定ユーザの特定サービスへの登録状況を確認し、登録状態を応答する機能も持つ。このため、サービス登録状況判定部(203A)は、ユーザ属性情報データベース(203B)によりユーザのID発行条件を保存する。

【００９４】

認可事業者識別部(203C)は、IdP(202)から問い合わせを受けたユーザの各サービスへの登録状況の問い合わせに対して、問い合わせ対象のユーザIDのドメイン情報等からID発行元である通信網事業者を特定し、他の通信網事業者かどうかを判定し、自社ユーザについ

てはサービス登録状況判定部(203A)に問い合わせ、他の通信網事業者のユーザについては他の通信網事業者の認可条件判定部(203D)によってプロファイル連携プロキシ(300)に対して他通信網事業者IDによるサービス登録状況を問い合わせるように振り分け処理を行う機能を有する。

【００９５】

他の通信網事業者の認可条件判定部(203D)は、認可事業者識別部(203C)で振り分けた要求を受信し、認可事業者識別部(203C)において他の通信網事業者のユーザと判定された場合に、プロファイル連携プロキシ(300)を介して他の通信網事業者のID連携プロファイルサーバ(105)に対してサービス登録状況を問い合わせ、ID連携可否情報であるID発行条件をIdP(202)に応答する機能を有する。

【００９６】

プロファイル連携プロキシ(300)は、サービス登録状況要求受信部(311)、サービス登録状況要求送信部(312)、サービス登録状況応答受信部(313)、サービス登録状況応答送信部(314)、リクエスト生成・管理部(315)を備えている。

【００９７】

サービス登録状況要求受信部(311) および送信部(312)は、サービス登録状況の要求を送受信する機能を有する。

【００９８】

サービス登録状況応答受信部(313) および送信部(314)は、サービス登録状況の応答を送受信する機能を有する。

【００９９】

また、リクエスト生成・管理部(315)は、宛先事業者判定機能(315A)と、リクエストID対応生成機能(315B)、リクエスト生成元事業者判定機能(315C)、リクエストID対応確認・復元機能(315D)を備えている。

【０１００】

リクエスト生成・管理部(315)は、ID発行元の通信網事業者を識別し、管理用のIDを付与して認可条件の取得に必要な信号を生成し、ID発行元のID連携プロファイルサーバに問い合わせる機能を有する。このため、リクエスト生成・管理部(315)は、宛先となる通信網事業者の判定機能(315A)と、受信した応答とリクエストの対応関係を管理するためのリクエストIDの生成機能(315A)、リクエスト生成元の通信網事業者の判定機能(315C)、リクエストID対応確認・復元機能(315D)を備え、要求送信元と要求送信先の通信網事業者へのID発行条件の送受信に必要な信号の変換機能(プロトコル、ヘッダ情報の生成、削除等)を有する。

【０１０１】

これにより、プロファイル連携プロキシ(300)は、複数の通信網の事業者間でID発行条件の流通を可能とする機能と、所定通信網のID連携プロファイルサーバからのID発行条件の問い合わせを解析し、端末(106)が送信した認証情報を発行した問い合わせ対象の通信網事業者のID連携プロファイルサーバを解析する機能と、問い合わせ対象となる通信網事業者のID連携プロファイルサーバにID発行条件を問い合わせる機能と、問い合わせ対象のID連携プロファイルサーバから受信したID発行条件を問い合わせ元のID連携プロファイルサーバに送信する機能とを持つ。

【０１０２】

すなわち、プロファイル連携プロキシ(300)は、通信網事業者間でID連携プロファイルを交換する際に、問い合わせ対象のユーザIDからIDの発行元通信網事業者を特定し、当該通信網事業者のID連携プロファイルサーバの宛先を解決し、宛先通信網事業者に対応した要求信号に整形してリクエストを転送し、その応答として受信したID連携可否情報を変形してリクエスト送信元の通信網事業者のID連携プロファイルサーバに返送する。この際、ID発行条件の問い合わせの要求・応答の信号の中継時に、問い合わせ元通信網事業者及び問い合わせ先通信網事業者のポリシーによって信号内容を変換（情報の削除・置換等）することにより、通信網事業者間で流通すべきでない情報を隠ぺい可能とする。

【０１０３】
このため、プロファイル連携プロキシ(300)は、問い合わせ先となる各通信網事業者のID連携プロファイルサーバの宛先情報(ホスト名、アドレス、接続プロトコル、信号条件(パラメータ等)、等)を保持する。
【０１０４】
次に、端末(106)が固定網(201)を介してWebサービス１(103A)に接続する際の具体的な動作を説明する。
【０１０５】
固定網(201)のIdP(202)のID発行部(202A)は、認可要求をWebサービス１(103A)から受信し、それを受けて認証処理部(202B)から認証トークン#1を取得し、認証トークン#1をWebサービス１(103A)に送信する。
【０１０６】
認証処理部(202B)は、端末(106)から当該の認証トークン#1による認証要求を受信し、GBA等の技術を使って端末(106)のSIMカード等により認証処理を行う。さらに、認証処理部(202B)は、認証が成功すると、当該ユーザのIDをWebサービス１(103A)に発行可能か確認するため、ID発行条件確認部(202C)に問い合わせる。
【０１０７】
ID発行条件確認部(202C)は、ID連携プロファイルサーバ(203)に認証されたユーザIDとID要求元のWebサービス１(103A)の情報を送信し、ID発行条件を要求する。
【０１０８】
ID連携プロファイルサーバ(203)の認可事業者識別部(203C)はユーザIDから認可元の通信網事業者を割り出して、自社のユーザであればWebサービス１(103A)の情報とともにサービス登録状況判定部(203A)にID発行条件の確認を要求する。他の通信網事業者のユーザであれば、Webサービス１(103A)の情報とともに他の通信網事業者のID発行条件判定部(203D)にID発行条件の確認を要求する。以下では他の通信網事業者のユーザである場合の処理の流れを述べる。
【０１０９】
他の通信網事業者のID発行条件判定部(203D)はプロファイル連携プロキシ(300)に対してユーザIDと要求元Webサービス事業者の情報でID発行条件確認要求を送信する。
【０１１０】
プロファイル連携プロキシ(300)は、ID発行条件確認要求の受信後、ユーザIDから宛先となる通信網事業者を識別して、ID連携プロファイルサーバ(203)のユーザ属性情報DB(203B)内から当該のユーザIDを発行する通信網事業者のID連携プロファイルサーバ(105)に接続するために必要な情報（ホスト名、アドレス、接続プロトコル、信号条件（パラメータ等）、等）を取得する。この情報をもとに、接続先のID連携プロファイルサーバ(105)に対して、ID発行条件の確認を要求する。
【０１１１】
ID連携プロファイルサーバ(203)は、ID発行条件を含んだサービス登録状況応答を生成し、プロファイル連携プロキシ(300)に応答する。
【０１１２】
プロファイル連携プロキシ(300)は、応答に含まれる識別IDから対応する要求信号を特定し、固定網(201)から送信された要求の応答として、受信した応答に含まれるサービス登録状況応答を送信する。
【０１１３】
固定網(201)のID連携プロファイルサーバ(203)は、応答を受信するとそこに含まれるID発行条件を参照し、IdP(202)に対して、対象のWebサービス１(103A)へのID発行条件を含む応答を送信する。
【０１１４】
次に、図３を参照して、本実施形態の通信サービス認証・接続システムにおいて、端末(106)が固定網(201)を介してWebサービス１(103A)に接続する際の具体的な通信に関して

説明する。

【０１１５】

ユーザが端末(106)から固定網(201)を通じてWebサービス１(103A)へアクセスし(401)、Webサービス(103)上で認証を行う際に固定網(201)が払い出すIDにより認証することを選択した場合、Webサービス１(103A)から固定網(201)のIdP(202)に対して認証要求が行われる(402)。

【０１１６】

IdP(202)はどのサービスのどの認証要求に対してトークンを払い出すのかを識別するために、Webサービス１(103A)に認証要求識別ID#1を払い出し、Webサービス１(103A)に通知する(403)。

【０１１７】

Webサービス１(103A)は認証要求識別ID#1を端末(106)に通知し固定網(201)のIdPサーバ(202)と認証するように端末(106)をリダイレクトする(404)。

【０１１８】

端末(106)は、IdP(202)に対して認証要求識別ID#1を通知して認証を開始する(405)。

【０１１９】

IdP(202)は端末(106)をSIMにより認証するため、固定網(201)のAAAサーバ(204)に対してSIM認証要求を行う(406)。

【０１２０】

AAAサーバ(204)はIdP(202)に対してどのIdP(202,102)の認証要求へのトークンを払い出すのかを識別するため、SIM認証要求識別ID#2をIdP(202)に通知する(407)。

【０１２１】

IdP(202)はSIM認証要求識別ID#2を端末(106)に通知するとともに、AAAサーバ(204)とSIM認証を行うように端末(106)からの信号をリダイレクトする(408)。

【０１２２】

端末(106)は、AAAサーバ(204)に対してSIM認証要求識別ID#2により認証要求を行う(409)。

【０１２３】

AAAサーバ(204)は認証情報をモバイル網(101)のHSS（Home Subscriber Server）(104)から取得し、端末(106)との間でSIM等を使った認証を行う(410,411)。認証が完了した(412)後、AAAサーバ(204)は端末(106)に対して認証されたことを示すSIM認証トークン#2を発行する(413)。

【０１２４】

端末(106)はAAAサーバ(204)から受け取ったSIM認証要求識別IDとSIM認証トークンをIdP(202)に送信し、認証処理を要求する(414)。

【０１２５】

IdP(202)はSIM認証の結果をAAAサーバ(204)に問い合わせるため、SIM認証要求識別ID#2をAAAサーバ(204)に送信する(415)。

【０１２６】

AAAサーバ(204)はSIM認証結果をもとに、SIM認証トークン#2をIdP(202)に送信する(416)。

【０１２７】

IdP(202)は端末(106)とAAAサーバ(204)から送られたSIM認証トークンの一致を確認し、IdP(202)は要求元のWebサービス１(103A)が認証代行することを登録されているか否かを確認するため、ID発行条件の要求を固定網(201)のID連携プロファイルサーバ(203)に送信する(417)。

【０１２８】

ID連携プロファイルサーバ(203)は、受信したID発行条件要求をプロファイル連携プロキシ(300)に送信する(418)。

【０１２９】

これを受けた、プロファイル連携プロキシ(300)は、要求元の通信網と、ID、サービス等の情報から適切な事業者のID連携プロファイルサーバ(105)に対してユーザとサービスの対応からID発行条件を問い合わせる(419)。

【０１３０】

ID連携プロファイルサーバ(105)は、ユーザとサービスの情報からID発行条件を確認し、プロファイル連携プロキシ(300)を介して、固定網(201)のID連携プロファイルサーバ(203)にID発行条件を送信し(420,421)、ＩＤ連携プロファイルサーバ(203)はIdP(202)にID発行条件を送信する(422)。

【０１３１】

IdP(202)はID発行条件の情報をもとに、端末(106)に対してWebサービス１(103A)への認証用トークン#1を通知する(423)。

【０１３２】

端末(106)は認証要求識別ID#1とトークン#1の組をWebサービス１(103A)に送信し、認証処理を要求する(424)。

【０１３３】

Webサービス１(103A)は認証要求識別ID#1によりIdP(202)から認可情報を問い合わせ(425)、トークン#1を取得し(426)、端末(106)が送信したトークンと比較して認証処理を完了し、シングルサインオンが実現される(427)。

【０１３４】

上記実施形態の通信サービス認証・接続システムによれば、固定網(201)やモバイル網(101)などの通信網の違いによらずSIMを用いるネットワーク認証を使ったシングルサインオンが可能となり、従来のような問題すなわち端末(106)がアクセスするネットワーク（通信網）の違いによりWebサービス側でSIM認証情報が使えなくなるという問題を解消することができる。

【産業上の利用可能性】

【０１３５】

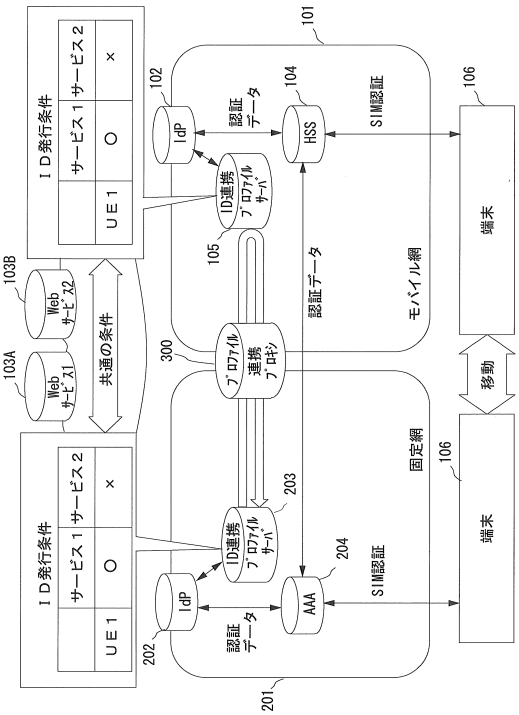
固定網やモバイル網などの通信網の違いによらずSIM等を用いるネットワーク認証を使ったシングルサインオンが可能となり、端末(106)がアクセスするネットワーク（通信網）の違いによりWebサービス側で認証情報が使えなくなることがない通信サービス認証・接続システム及びその方法を提供することができる。

【符号の説明】

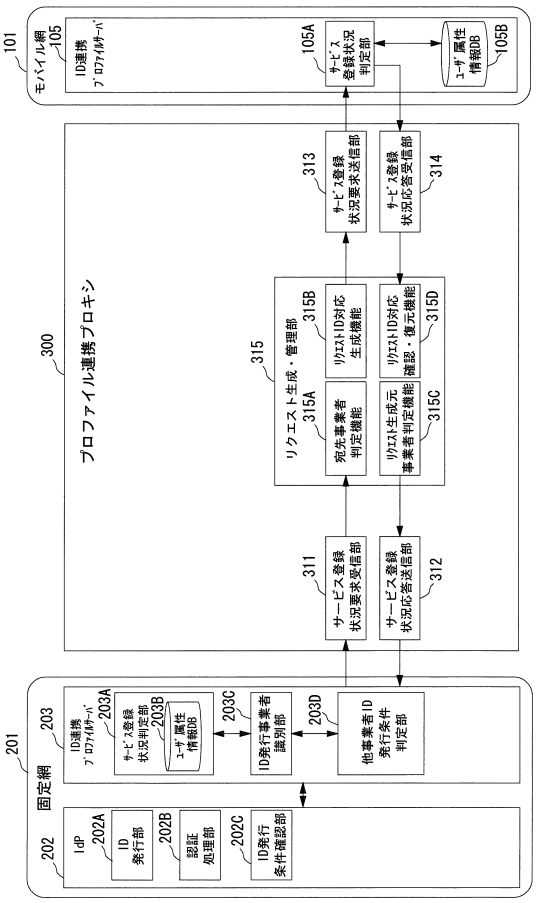
【０１３６】

101…モバイル網、102…IdP、103A,103B…Webサービス、104…HSS、105…ID連携プロファイルサーバ、106…端末、201…固定網、202…IdP、203…ID連携プロファイルサーバ、204…AAAサーバ（認証サーバ）、300…プロファイル連携プロキシ、311…サービス登録状況要求受信部、312…サービス登録状況要求送信部、313…サービス登録状況応答受信部、314…サービス登録状況応答送信部、315…リクエスト生成・管理部、315A…宛先事業者判定機能、315B…リクエストID対応生成機能、315C…リクエスト生成元事業者判定機能、315D…リクエストID対応確認・復元機能。

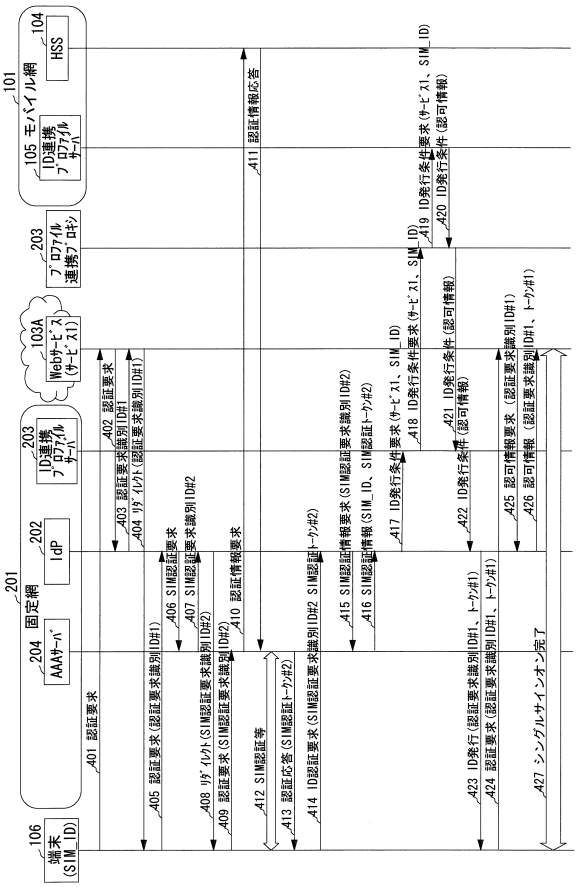
【図１】


ＩＤ発行条件
ＵＥ１
サービス１
サービス２
○
×
共通の条件
Web サービス１
Web サービス２
IdP
ID連携 プロファイル サーバ
プロファイル 連携プロキシ
AAA
HSS
認証データ
認証データ
SIM認証
SIM認証
認証データ
端末
端末
移動
固定網
モバイル網
101
102
103A
103B
104
105
106
201
202
203
204

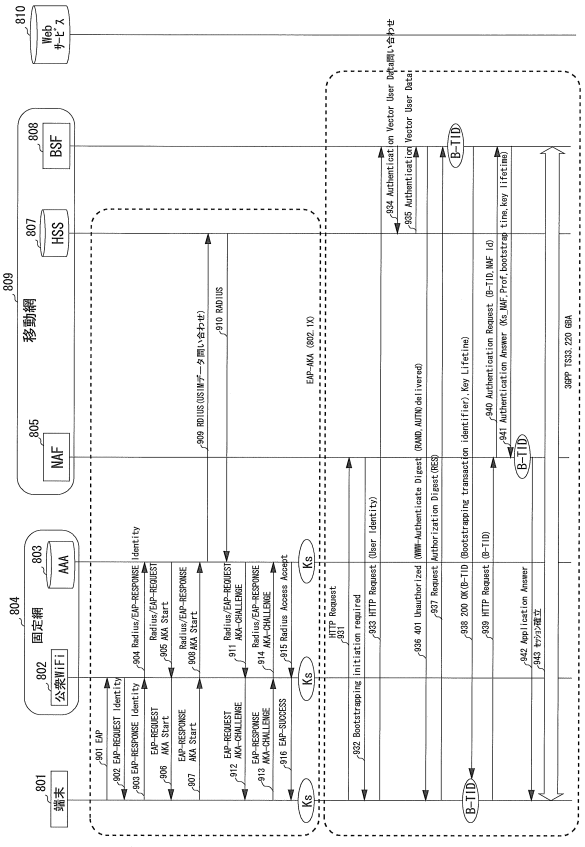
【図２】


101
モバイル網
105
ID連携 プロファイルサーバ
105A
サービス登録状況判定部
105B
ユーザ属性情報DB
300
プロファイル連携プロキシ
311
サービス登録状況要求受信部
312
サービス登録状況応答送信部
313
サービス登録状況要求送信部
314
サービス登録状況応答受信部
315
リクエスト生成・管理部
315A
発生事業者判定機能
315B
リクエストID対応生成機能
315C
リクエスト生成元事業者判定機能
315D
リクエストID対応確認・復元機能
201
固定網
203
ID連携プロファイルサーバ
203A
サービス登録状況判定部
203B
ユーザ属性情報DB
203C
ID発行事業者識別部
203D
他事業者ID発行条件判定部
202
IdP
202A
ID発行部
202B
認証処理部
202C
ID発行条件確認部

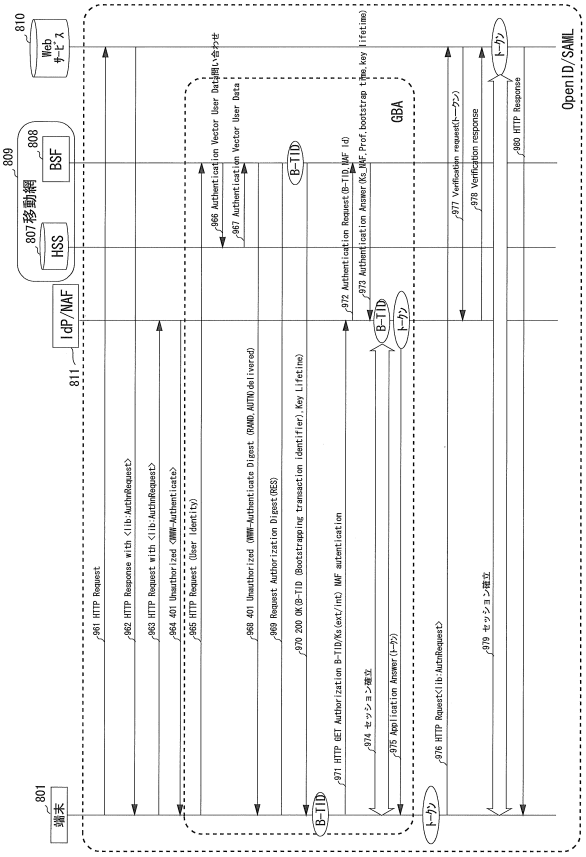
【図３】


106
端末 (SIM_ID)
201
固定網
204
AAAサーバ
202
IdP
203
ID連携 プロファイル サーバ
103A
Webサービス (サービス1)
203
プロファイル連携プロキシ
105
ID連携 プロファイル サーバ
101
モバイル網
104
HSS
401 認証要求
402 認証要求
403 認証要求識別ID#1
404 リダイレクト(認証要求識別ID#1)
405 認証要求(認証要求識別ID#1)
406 SIM認証要求
407 SIM認証要求識別ID#2
408 リダイレクト(SIM認証要求識別ID#2)
409 認証要求(SIM認証要求識別ID#2)
410 認証情報要求
411 認証情報応答
412 SIM認証等
413 認証応答(SIM認証トークン#2)
414 ID認証要求(SIM認証要求識別ID#2 SIM認証トークン#2)
415 SIM認証情報要求(SIM認証要求識別ID#2)
416 SIM認証情報(SIM_ID、SIM認証トークン#2)
417 ID発行条件処理要求(SIM_ID、SIM認証トークン#2)
418 ID発行条件要求(サービス1、SIM_ID)
419 ID発行条件要求(サービス1、SIM_ID)
420 ID発行条件(認可情報)
421 ID発行条件(認可情報)
422 ID発行条件(認可情報)
423 ID発行(認証要求識別ID#1、トークン#1)
424 認証要求(認証要求識別ID#1、トークン#1)
425 認可情報要求(認証要求識別ID#1)
426 認可情報(認証要求識別ID#1、トークン#1)
427 シングルサインオン完了

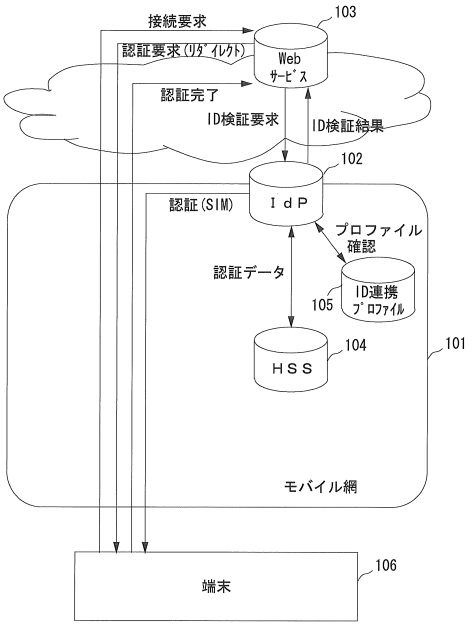
【図４】


801 端末
802 公衆WiFi
803 AAA
804 固定網
805 NAF
807 HSS
808 BSF
809 移動網
810 Webサービス
801 IAP
802 EAP-REQUEST Identity
803 EAP-RESPONSE Identity
804 Radius/EAP-RESPONSE Identity
805 EAP-REQUEST AKA Start
806 Radius/EAP-REQUEST AKA Start
807 EAP-RESPONSE AKA Start
808 Radius/EAP-RESPONSE AKA Start
809 RADIUS(USIMデータ問い合わせ)
810 RADIUS
811 EAP-REQUEST AKA-CHALLENGE
812 Radius/EAP-REQUEST AKA-CHALLENGE
813 EAP-RESPONSE AKA-CHALLENGE
814 Radius/EAP-RESPONSE AKA-CHALLENGE
815 Radius Access Accept
816 EAP-SUCCESS
EAP-AKA' (800-1X)
Ks
Ks
Ks
821 HTTP Request
822 Bootstrapping Initiation required
823 HTTP Request (User Identity)
824 Authentication Vector (User Identity)
825 Authentication Vector (User Data)
826 401 Unauthorized (WWW-Authenticate Digest (RAND, AUTN)delivered)
827 Request Authorization Digest(RES)
828 200 OK(B-TID (Bootstrapping transaction identifier), Key Lifetime)
829 HTTP Request (B-TID)
840 Authentication Request (B-TID, NAF ID)
841 Authentication Answer (Ks_NAF, Prof, bootstrapping time, key lifetime)
842 Application Answer
843 セッション確立
3GPP TS33.220 GBA
B-TID
B-TID
B-TID

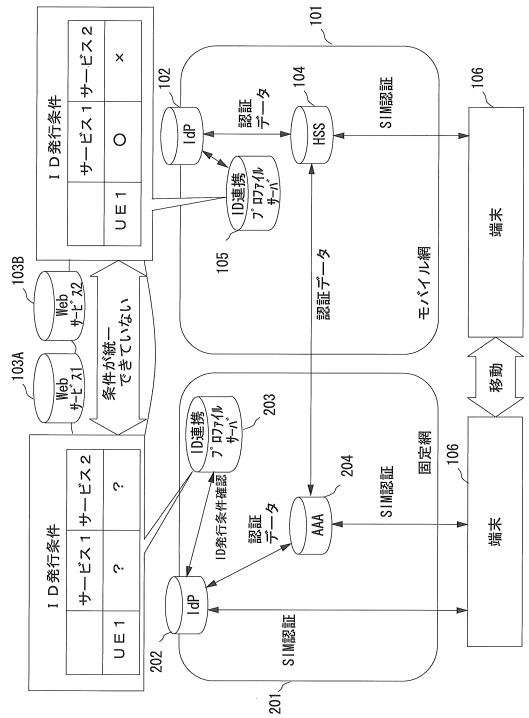
【図５】


Webサービス
BSF
HSS
移動網
IdP/NAF
端末
OpenID/SAML
GBA
B-TID
トークン
S61 HTTP Request
S62 HTTP Response with <Ub-AuthnRequest>
S63 HTTP Request with <Ub-AuthnRequest>
S64 401 Unauthorized (WWW-Authenticate)
S65 HTTP Request (User Identity)
S66 Authentication Vector User Data要求
S67 Authentication Vector User Data
S68 401 Unauthorized (WWW-Authenticate Digest, RAND, AUTN delivered)
S69 Request Authorization Digest (RES)
S70 200 OK (B-TID (Bootstrapping transaction Identifier), Key Lifetime)
S71 HTTP GET Authorization B-TID/Ks(ext/int) NAF authentication
S72 Authentication Request (B-TID, NAF Id)
S73 Authentication Answer (Ks_NAF, Prof. bootstrap time, key lifetime)
S74 セッション確立
S75 Application Answer (トークン)
S76 HTTP Request <Ub-AuthRequest>
S77 Verification request (トークン)
S78 Verification response
S79 セッション確立
S80 HTTP Response

【図６】


接続要求
認証要求(リダイレクト)
認証完了
ID検証要求
ID検証結果
Web サービス
103
102
IdP
認証(SIM)
プロファイル確認
認証データ
105
ID連携 プロファイル
104
HSS
101
モバイル網
106
端末

【図７】


ID発行条件
サービス1 サービス2
UE1 ○ ×
Webサービス2
Webサービス1
条件が統一できていない
ID発行条件
サービス1 サービス2
UE1 ? ?
101
102
IdP
認証データ
104
HSS
SIM認証
106
端末
ID連携プロファイルサーバ
105
モバイル網
認証データ
移動
203
204
AAA
固定網
ID発行条件確認
202
201

フロントページの続き

(72)発明者　則武　克誌
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　金沢　史明

(56)参考文献　特開２０１３－０３０１２４（ＪＰ，Ａ）
特表２００６－５１２６４８（ＪＰ，Ａ）
特表２００８－５３８２４７（ＪＰ，Ａ）
特表２００８－５０６１３９（ＪＰ，Ａ）
国際公開第２０１２／０６２９１５（WO，Ａ１）
国際公開第２０１１／０３６４８４（WO，Ａ１）
米国特許出願公開第２０１０／０２８１５３０（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４１