(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-192487
(P2004-192487A)
(43)公開日　平成16年7月8日(2004.7.8)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330B	5B085
G09C 1/00	G06F	15/00	330G	5J104
H04L 9/32	G09C	1/00	660A	
	H04L	9/00	673A	

審査請求 未請求　請求項の数 16　ＯＬ　（全 14 頁）

(21)出願番号　特願2002-361637(P2002-361637)
(22)出願日　平成14年12月13日(2002.12.13)

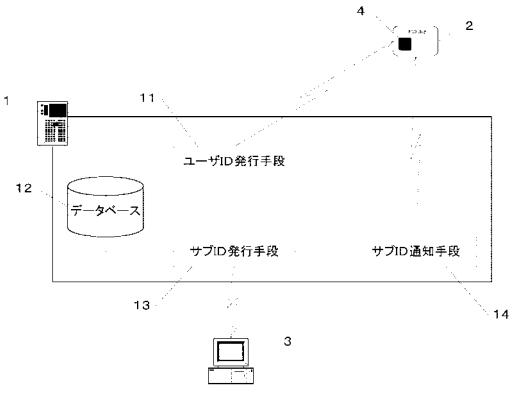
特許法第３０条第１項適用申請有り　２００２年７月３日　社団法人情報処理学会発行の「情報処理学会シンポジウムシリーズ　Ｖｏｌ．２００２　Ｎｏ．９」に発表

(71)出願人　800000035
株式会社産学連携機構九州
福岡県福岡市東区箱崎６丁目１０番１号
(74)代理人　100099508
弁理士　加藤　久
(72)発明者　浜崎　陽一郎
福岡県福岡市東区馬出６丁目１３－２２－６０５

Ｆターム(参考)　5B085 AE02 AE04 AE11
5J104 AA07 KA01 NA36

(54)【発明の名称】認証方法および保証装置並びにこれを用いた認証システム

(57)【要約】
【課題】一つのＩＤで多くのサービスの提供を受けるに際して、ＩＤの漏洩に対する安全性を向上させる。
【解決手段】発行者のサーバ１は、ユーザＩＤ発行手段１１により各ユーザに対してそれぞれ一つのユーザＩＤを発行し、データベース１２に記録、保管する。発行されたユーザＩＤは、各ユーザのＩＤカード２のＩＣチップ４に記録、保存する。また、発行者のサーバ１は、サブＩＤ発行手段１３により各サービス提供者に対してユーザＩＤの一部を抽出してサブＩＤとして発行し、サブＩＤ通知手段１４により各ユーザに対してこの発行したサブＩＤを通知する。これにより、ユーザとサービス提供者との間でサブＩＤを用いて安全に認証することができる。
【選択図】　図２



【特許請求の範囲】
【請求項１】
発行者のサーバからユーザのＩＤ保持体に対して一つのユーザＩＤを発行し、
前記発行者のサーバは、サービス提供者の端末に対して前記ユーザＩＤの一部を抽出してサブＩＤとして発行し、
前記ユーザのＩＤ保持体とサービス提供者の端末との間で前記サブＩＤを用いて認証することを特徴とする認証方法。
【請求項２】
複数の発行者のサーバからユーザのＩＤ保持体に対してそれぞれ一つずつユーザＩＤを発行し、
前記複数の発行者のサーバは、サービス提供者の端末に対して、それぞれ前記ユーザのＩＤ保持体に対して発行したユーザＩＤの一部を抽出してサブＩＤとして発行し、
前記ユーザのＩＤ保持体とサービス提供者の端末との間で前記複数の発行者のサーバがそれぞれ発行した複数のサブＩＤを用いて認証する
ことを特徴とする認証方法。
【請求項３】
前記複数の発行者のサーバによりそれぞれ発行されたユーザＩＤまたはサブＩＤは、仲介機関のサーバが一括して前記ユーザのＩＤ保持体または前記サービス提供者の端末へ引き渡すことを特徴とする請求項２記載の認証方法。
【請求項４】
前記ユーザのＩＤ保持体とサービス提供者の端末との間の認証は、前記ユーザのＩＤ保持体上のユーザＩＤと前記サービス提供者の端末上のサブＩＤとを照合することにより行うことを特徴とする請求項１から３のいずれかに記載の認証方法。
【請求項５】
前記発行者のサーバは、前記ユーザのＩＤ保持体に対して前記サービス提供者の端末に発行したサブＩＤを通知し、
前記ユーザのＩＤ保持体とサービス提供者の端末との間の認証は、前記ユーザのＩＤ保持体上のサブＩＤと前記サービス提供者の端末上のサブＩＤとを照合することにより行うことを特徴とする請求項１から３のいずれかに記載の認証方法。
【請求項６】
前記ユーザのＩＤ保持体は、前記サブＩＤが前記ユーザＩＤ上のどの部分から抽出されたものであるかを示すサブＩＤ抽出情報を含めて保持することを特徴とする請求項５に記載の認証方法。
【請求項７】
前記ユーザのＩＤ保持体は、前記サブＩＤが前記ユーザＩＤ上のどの部分から抽出されたものであるかを示すサブＩＤ抽出情報を前記ユーザＩＤとは別に保持することを特徴とする請求項５に記載の認証方法。
【請求項８】
前記ユーザのＩＤ保持体は、前記サブＩＤが前記ユーザＩＤ上のどの部分から抽出されたものであるかを示すサブＩＤ抽出情報を保持せず、前記サービス提供者の端末が、前記サブＩＤ抽出情報を前記サブＩＤとともに保持することを特徴とする請求項５に記載の認証方法。
【請求項９】
前記サブＩＤの発行は、前記ユーザＩＤから連続的または不連続的に抽出することにより行うことを特徴とする請求項１から８のいずれかに記載の認証方法。
【請求項１０】
ユーザのＩＤ保持体に対して一つのユーザＩＤを発行する手段と、
サービス提供者の端末に対して前記ユーザＩＤの一部を抽出してサブＩＤとして発行する手段と
を備えた保証装置。

【請求項１１】
前記ユーザのＩＤ保持体に対して前記サービス提供者に発行したサブＩＤを通知する手段を備えた請求項１０記載の保証装置。
【請求項１２】
請求項１０または１１に記載の保証装置を配置し、
前記ユーザのＩＤ保持体とサービス提供者の端末との間で、前記サブＩＤを用いて認証する構成とした認証システム。
【請求項１３】
請求項１０または１１に記載の保証装置を複数配置し、
前記複数の保証装置から前記ユーザのＩＤ保持体に対してそれぞれ一つずつユーザＩＤを発行し、
前記複数の保証装置は、前記サービス提供者の端末に対して、それぞれ前記ユーザのＩＤ保持体に対して発行したユーザＩＤの一部を抽出してサブＩＤとしてそれぞれ発行し、
前記ユーザのＩＤ保持体とサービス提供者の端末との間で前記複数の保証装置がそれぞれ発行した複数のサブＩＤを用いて認証する
構成とした認証システム。
【請求項１４】
前記複数の保証装置によりそれぞれ発行されたユーザＩＤまたはサブＩＤを、一括して前記ユーザのＩＤ保持体または前記サービス提供者の端末へ引き渡す仲介機関のサーバを配置した請求項１２記載の認証システム。
【請求項１５】
前記ユーザのＩＤ保持体とサービス提供者の端末との間の認証は、前記ユーザのＩＤ保持体上のユーザＩＤと前記サービス提供者の端末上のサブＩＤとを照合することにより行う構成とした請求項１２から１４のいずれかに記載の認証システム。
【請求項１６】
前記ユーザのＩＤ保持体とサービス提供者の端末との間の認証は、前記ユーザのＩＤ保持体上のサブＩＤと前記サービス提供者の端末上のサブＩＤとを照合することにより行う構成とした請求項１２から１４のいずれかに記載の認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ユーザとサービス提供者との間でＩＤ（Identification）コード（本明細書中において「ＩＤ」と称す。）を用いて認証を行うための認証方法および保証装置並びにこれを用いた認証システムに関する。
【０００２】
【従来の技術】
インターネットを始めとするネットワークの急速な普及を背景に、様々なサービスの電子化が着々と進んでいる。電子情報を利用するサービスは、例えば、従来紙ベースで行っていた情報提供をネットワークを通じて電子ベースで行ったり、ネットワーク上で商取引を行ったり、ネットワーク上で金融サービスを行ったり等、多岐に渡り、我々の身近な生活に大きな影響を与えている。
【０００３】
これらの電子情報を利用したサービスの導入により、我々の生活はより便利に、より効率的になるものと思われる。近年では、一つのＩＤ（識別符号）に情報を集積することにより利便性を追求したもの（例えば、住民基本台帳ネットワークなど）も提案されている。近い将来、一つのＩＤで多くのサービス提供を受けることが可能になることが予想される。
【０００４】
しかしその反面、電子的であるがために発生する安全性の問題も大きな課題である。痕跡を残さない改ざん、なりすましや盗聴など、数々の驚異が存在する。従来、ネットワーク

上で流通する電子情報の安全性を保つための研究は盛んに行われているが、これらは主に認証、完全性、秘匿性といった電子情報を保護するという観点からアプローチするものが多い（例えば、非特許文献１を参照。）

【０００５】

【非特許文献１】

カーライル・アダムズ、スティーブ・ロイド著，鈴木優一訳，「ＰＫＩ　公開鍵インフラストラクチャの概念、標準、展開」，初版，株式会社ピアソン・エデュケーション，２０００年７月１５日，ｐ．４１－５２

【０００６】

【発明が解決しようとする課題】

ところが、将来、一つのＩＤで多くのサービス提供を受けるようになった場合、仮にそのＩＤが漏洩すると、その被害は絶大なものとなることが予想される。そのＩＤ一つですべてのサービスが盗用可能となるためである。今後、我々が留意しなければならないのはこれらの点であり、被害を最小限に止めるためのシステムを構築することが重要である。

【０００７】

上記従来の電子情報の保護といった観点からのアプローチだけでは、このような漏洩に対しては対応することができない。従来の方法によりシステム上で電子情報を完璧に保護しても、第三者による盗聴の危険性は拭えない。サービスに対する内部または外部からの攻撃によるＩＤの漏洩の危険性があり、また、サービス提供者が悪意を持てば簡単にＩＤは漏洩してしまうためである。

【０００８】

そこで、本発明においては、一つのＩＤで多くのサービスの提供を受けるに際して、ＩＤの漏洩に対する安全性を向上した認証方法および保証装置並びにこれを用いた認証システムを提供することを目的とする。

【０００９】

【課題を解決するための手段】

本発明の認証方法は、発行者のサーバからユーザのＩＤ保持体に対して一つのユーザＩＤを発行し、発行者のサーバは、サービス提供者の端末に対してユーザＩＤの一部を抽出してサブＩＤとして発行し、ユーザのＩＤ保持体とサービス提供者の端末との間でサブＩＤを用いて認証することを特徴とする。

【００１０】

ここで、ユーザとは、サービス提供者と取引を行う主体である。発行者とは、一般社会において社会的に認知された集団（社会的集団）を代表するものである。ユーザは発行者に属する。社会的集団とは、市や学校といった公共団体、企業やサークルといった私的団体を問わず、社会的に団体あるいは集団として認知された集団を指す。サービス提供者とは、ユーザにサービスを提供する主体である。なお、本明細書中においてサービスの提供とは、純粋な役務の提供の他、物質的生産物（商品）の提供を含むものとする。

【００１１】

ユーザＩＤとは、各ユーザを識別するための各ユーザ固有の識別符号である。ＩＤ保持体とは、このユーザＩＤを記録し、保持するフラッシュメモリ、ＩＣチップ、ハードディスク、フレキシブルディスク、光磁気ディスク、光ディスク、磁気テープなどの記録媒体を指す。

【００１２】

上記本発明の認証方法によれば、発行者のサーバはユーザのＩＤ保持体に対して一つのユーザＩＤを発行し、サービス提供者の端末に対してはユーザのＩＤ保持体に発行したユーザＩＤの全部ではなくその一部をサブＩＤとして発行するため、サービス提供者の端末はこのユーザＩＤのうちサブＩＤの部分のみを保持する。そして、このサブＩＤを用いてユーザのＩＤ保持体とサービス提供者の端末との間で認証を行うことができる。

【００１３】

また、発行者のサーバが複数存在する場合の認証方法は、複数の発行者のサーバからユー

ザのＩＤ保持体に対してそれぞれ一つずつユーザＩＤを発行し、複数の発行者のサーバは、サービス提供者の端末に対して、それぞれユーザのＩＤ保持体に対して発行したユーザＩＤの一部を抽出してサブＩＤとして発行し、ユーザのＩＤ保持体とサービス提供者の端末との間で複数の発行者のサーバがそれぞれ発行した複数のサブＩＤを用いて認証することを特徴とする。

【００１４】

この認証方法によれば、複数の発行者のサーバから一つのユーザのＩＤ保持体に対してそれぞれ一つずつユーザＩＤを発行し、サービス提供者の端末に対してはユーザのＩＤ保持体にそれぞれ発行したユーザＩＤの全部ではなくそれぞれの一部をサブＩＤとして発行するため、サービス提供者の端末はこのユーザＩＤのうちサブＩＤの部分のみを保持する。そして、このサブＩＤを用いてユーザのＩＤ保持体とサービス提供者の端末との間で認証を行うことができる。

【００１５】

このとき、複数の発行者のサーバによりそれぞれ発行されたユーザＩＤまたはサブＩＤは、仲介機関のサーバが一括してユーザのＩＤ保持体またはサービス提供者の端末へ引き渡すことも可能である。これにより、複数の発行者のサーバによりそれぞれ発行されたユーザＩＤ、サブＩＤの管理、発行を仲介機関のサーバによって一括して行うことができる。

【００１６】

ユーザのＩＤ保持体とサービス提供者の端末との間の認証は、ユーザのＩＤ保持体上のユーザＩＤとサービス提供者の端末上のサブＩＤとを照合することにより行うことができる。あるいは、発行者のサーバが、ユーザのＩＤ保持体に対してサービス提供者の端末に発行したサブＩＤを通知するものとし、ユーザのＩＤ保持体上のサブＩＤとサービス提供者の端末上のサブＩＤとを照合することにより行うことができる。

【００１７】

ユーザのＩＤ保持体にサブＩＤが通知された場合、ユーザのＩＤ保持体は、サブＩＤがユーザＩＤ上のどの部分から抽出されたものであるかを示すサブＩＤ抽出情報を含めて保持することができる。あるいは、ユーザのＩＤ保持体が、このサブＩＤ抽出情報をユーザＩＤとは別に保持する構成とすることもできる。さらに、ユーザのＩＤ保持体は、サブＩＤ抽出情報を保持せず、サービス提供者の端末が、サブＩＤ抽出情報をサブＩＤとともに保持する構成とすることもできる。

【００１８】

発行者のサーバは、サブＩＤの発行を、ユーザＩＤから連続的または不連続的に抽出することにより行うことができる。なお、連続的または不連続的な抽出は、規則的に行っても不規則的に行ってもよい。

【００１９】

上記本発明の認証方法に係る発行者のサーバは、ユーザのＩＤ保持体に対して一つのユーザＩＤを発行する手段と、サービス提供者の端末に対してユーザＩＤの一部を抽出してサブＩＤとして発行する手段とを備えた保証装置として構成することができる。この保証装置を配置した認証システムは、ユーザのＩＤ保持体とサービス提供者の端末との間で、サブＩＤを用いて認証する構成とすることができる。

【００２０】

また、この保証装置を複数配置した認証システムは、複数の保証装置からユーザのＩＤ保持体に対してそれぞれ一つずつユーザＩＤを発行し、複数の保証装置は、サービス提供者の端末に対して、それぞれユーザのＩＤ保持体に対して発行したユーザＩＤの一部を抽出してサブＩＤとしてそれぞれ発行し、ユーザのＩＤ保持体とサービス提供者の端末との間で複数の保証装置がそれぞれ発行した複数のサブＩＤを用いて認証する構成とすることができる。

【００２１】

また、複数の発行者の保証装置によりそれぞれ発行されたユーザＩＤ、サブＩＤの管理、発行を仲介機関によって一括して行う場合には、複数の保証装置によりそれぞれ発行され

たユーザＩＤまたはサブＩＤを、一括してユーザのＩＤ保持体またはサービス提供者の端末へ引き渡す仲介機関のサーバを配置することにより実現可能である。

【００２２】

なお、この認証システムにおいて行うユーザのＩＤ保持体とサービス提供者の端末との間の認証は、本発明の認証方法と同様に、ユーザのＩＤ保持体上のユーザＩＤとサービス提供者の端末上のサブＩＤとを照合することにより行うことができる。あるいは、保証装置が、ユーザのＩＤ保持体に対してサービス提供者の端末に発行したサブＩＤを通知する手段を備えるものとし、ユーザのＩＤ保持体上のサブＩＤとサービス提供者の端末上のサブＩＤとを照合することにより行うことができる。

【００２３】

【発明の実施の形態】

図１は本発明の実施の形態における認証システムの概略構成図である。

図１において、本実施形態における認証システムは、各ユーザに固有のユーザＩＤ（以下、「ＰＩＤ」と称す。）を発行する発行者のサーバ１、各ユーザが所有するＩＤカード２、および、各ユーザに対して様々なサービスの提供を行うサービス提供者の端末３により構成される。ＩＤカード２は、ＩＤ保持体としてのＩＣチップ４を内蔵する。ＩＤカード２は、例えば、クレジットカード、キャッシュカード、学生証や会員証等として用いられる。

【００２４】

図２は図１のサーバ１の機能構成を示すブロック図である。

図２に示すように、サーバ１は、各ユーザに対してそれぞれ一つのユーザＩＤを発行するユーザＩＤ発行手段１１と、各ユーザのユーザＩＤを記録、保管するデータベース１２と、各サービス提供者に対してユーザＩＤの一部を抽出してサブＩＤとして発行するサブＩＤ発行手段１３と、各ユーザに対して各サービス提供者に発行したサブＩＤを通知するサブＩＤ通知手段１４とを備える。

【００２５】

ＰＩＤは発行者が各ユーザに対して割り当てる長いビット列である。ユーザＩＤ発行手段１１によって発行されたＰＩＤは、サーバ１のデータベース１２内に保管されるとともに、各ユーザのＩＤカード２に引き渡され、各ＩＤカード２のＩＣチップ４に記録、保持される。ＰＩＤの発行者は、一般的にＩＤ発行を行っている組織に準ずる者であり、例えば、学生や職員などにＩＤを発行する学校（厳密には学校長）、社員や顧客などにＩＤを発行する企業、レンタルショップやクレジット会社等である。

【００２６】

また、発行者は、各ユーザがサービスの提供を受けるサービス提供者に対して、各ユーザのＰＩＤの一部を抽出してサブＩＤ（以下、「ｓｕｂＰＩＤ」と称す。）として発行する。サブＩＤ発行手段１３によって発行されたｓｕｂＰＩＤは、発行者のサーバ１からサービス提供者の端末３に引き渡され、各サービス提供者の端末３の記憶装置（図示せず。）に記録、保持される。また、このｓｕｂＰＩＤは、サブＩＤ通知手段１４によって各ユーザのＩＤカード２に通知される。

【００２７】

なお、本実施形態における発行者は、従来のＴＴＰ（Trusted Third Party）と呼ばれる二つの主体の間に立つ公正・中立な第三者機関とは大きく異なる。上の定義からも分かる通り、発行者とはユーザが属する集団の長である。よって、発行者は各ユーザの権利の保護や利益の拡大を行うのが義務であり、各ユーザを保護する立場にある者であることに留意する。

【００２８】

以下、ユーザとサービス提供者との間で安全にサービス提供に対する認証を行う手順について説明する。

【００２９】

最初は、ユーザが発行者からＰＩＤを取得するプロセスである（図３参照。）。ユーザは

、発行者（自分が属する社会的集団あるいは自分が属したいと思う社会的集団）に対して、名前や住所といった個人情報を提供する。この情報を元に発行者はユーザの本人性を確認し、そのユーザに対してＰＩＤを発行する。実際には、ＰＩＤは発行者のサーバ１のユーザＩＤ発行手段１１により発行され、この発行されたＰＩＤはユーザのＩＤカード２のＩＣチップ４に記録、保存される。この発行されたＰＩＤは、厳重に管理されたサーバ１のデータベース１２に記録、保存される。

【００３０】

以上のプロセスにより、ユーザはＰＩＤを取得することができる。図４に示すように、この時点で、ユーザはＩＤカード２に保存された形でＰＩＤを保持し、発行者はデータベース１２にユーザのＰＩＤを保持している状態である。なお、図４に示すように、この時点では、サービス提供者はユーザのＰＩＤに関して何も情報を持っていない。

【００３１】

次は、サービス提供者がユーザに対してサービス提供を行うプロセスである（図５を参照。）。まず、サービス提供者は、ユーザと直接取引する前に、発行者に許可を得る必要がある。

【００３２】

サービス提供者がユーザにサービスを行いたい場合、サービス提供者はそのユーザの属する集団の発行者に対して、ユーザとの取引を打診する。発行者は、調査の結果、このサービス提供者がユーザに不利益をもたらさないと判断し、ユーザとの取引を認めると、サービス提供者に対してユーザのＰＩＤの一部を提供する。このＰＩＤの一部がｓｕｂＰＩＤである。実際には、ｓｕｂＰＩＤは発行者のサーバ１のサブＩＤ発行手段１３により発行され、サービス提供者の端末３に引き渡される。サービス提供者は、こうして取得したユーザのｓｕｂＰＩＤを端末３に記録、保存する。なお、図５に示すように、サービス提供者は、発行者からｓｕｂＰＩＤ以外のユーザに関する情報は一切受け取ることができない。ｓｕｂＰＩＤとユーザの本人性については、発行者が保証する。

【００３３】

以上のプロセスにより、サービス提供者はユーザのｓｕｂＰＩＤを取得することができる。また、本実施形態においては、発行者はサービス提供者に発行したｓｕｂＰＩＤをユーザに対して通知する。実際には、発行者のサーバ１のサブＩＤ通知手段１４によってユーザのＩＤカード２に通知され、ＩＤカード２のＩＣチップ４に記録、保存される。図６に示すように、この時点で、ユーザおよび発行者は、ＰＩＤを保持し、なおかつｓｕｂＰＩＤの情報も保持している。サービス提供者は、発行者から発行されたｓｕｂＰＩＤのみを保持している。

【００３４】

これにより、ユーザがＩＤカード２のＩＣチップ４に保持するＰＩＤ（ｓｕｂＰＩＤ）とサービス提供者が端末３に保持するｓｕｂＰＩＤとを照合することにより認証を行うことができ、認証後はサービス提供の取引を行うことが可能となる。このとき、ユーザ側からみれば、サービス提供者の安全性は発行者によって保証されている。一方、サービス提供者側からみれば、ユーザの信用度は発行者に依存していることになる。すなわち、発行者のサーバ１は、ユーザおよびサービス提供者を相互に保証する保証装置として機能するものである。

【００３５】

また、前述のように、ユーザのＰＩＤおよび個人情報（住所など）は、サービス提供者側に知られることはない。すなわち、ユーザがサービス提供者からサービスの提供を受ける際、ユーザとサービス提供者との間の認証をＰＩＤの全体ではなくその一部であるｓｕｂＰＩＤにより認証するため、仮にこのｓｕｂＰＩＤが何らかの形で漏洩した場合であっても、ユーザのＰＩＤの全部が漏洩することはない。したがって、本実施形態における認証システムは、ＰＩＤ漏洩に対する安全性が極めて高い堅牢なシステムであるといえる。

【００３６】

なお、ｓｕｂＰＩＤを用いて、ユーザのＩＤカード２とサービス提供者の端末３との間で

、どのようなプロトコルで具体的な認証を行うかは自由である。ワンタイムパスワードや共通鍵暗号の利用などの種々の方法が考えられる。

【００３７】

ところで、現実の社会においては、（ａ）複数のユーザが同一のサービス提供者のサービスを受ける場合や、（ｂ）一人のユーザが複数のサービス提供者のサービスを受ける場合などが考えられる。以下、それぞれの場合について詳細に説明する。

【００３８】

（ａ）複数のユーザが同一のサービスの提供を受ける場合

同じ発行者に属する複数のユーザＡ，Ｂが同一のサービス提供者のサービスを受ける場合（図７参照。）、サービス提供者はそれぞれのユーザＡ，ＢのｓｕｂＰＩＤを発行者から発行してもらう必要がある。ｓｕｂＰＩＤは、それぞれのユーザＡ，Ｂについて前述の手順を踏んで得られる。サービス提供者は、発行されたそれぞれのｓｕｂＰＩＤを用いてユーザＡ，Ｂとの間でサービス提供を行う。ｓｕｂＰＩＤは各ユーザによって異なるので、一人のユーザのｓｕｂＰＩＤに事故があっても、他のユーザには影響がない。

【００３９】

（ｂ）一人のユーザが複数のサービスの提供を受ける場合

一人のユーザが複数のサービス提供者Ｐ，Ｑのサービスを受ける場合（図８参照。）、サービス提供者が発行者からユーザのｓｕｂＰＩＤを取得する手順は前述と同様であるが、発行者のｓｕｂＰＩＤの発行方法に三つの特徴がある。これはＰＩＤが長いビット列であるという特性に基づいている。

【００４０】

一つ目は、各ｓｕｂＰＩＤが、他のｓｕｂＰＩＤと重複しないように発行するという方法である。ＰＩＤは長いビット列であり、ｓｕｂＰＩＤはその一部である。例えば、図９に示すように、四つのサービス提供者Ｐ，Ｑ，Ｒ，Ｓに同一のユーザのＰＩＤからそれぞれｓｕｂＰＩＤを発行する場合、お互いが重複しないように提供する。各ｓｕｂＰＩＤは互いに独立しているため、何らかの形で一つのｓｕｂＰＩＤが漏洩しても他のサービス提供者との認証に影響が出ることはない。

【００４１】

二つ目は、図１０に示すように、各ｓｕｂＰＩＤが重複しても構わないという発行の方法である。重複している部分のどちらかのｓｕｂＰＩＤが漏洩した場合、前述した各ｓｕｂＰＩＤが重複しない場合のような安全性を得ることはできないが、漏洩したｓｕｂＰＩＤと一部重複した部分のｓｕｂＰＩＤだけでは認証することができないため、漏洩に対する安全性は充分に確保できる。このようなｓｕｂＰＩＤの発行方法は、簡易的なサービスを提供する場合や、同一サービス提供者による複数のｓｕｂＰＩＤ取得の場合などに好適であり、簡便で、経済性に優れるという利点がある。

【００４２】

三つ目は、発行するｓｕｂＰＩＤのビット長により安全性の度合いを調整することが可能であるということである。サービス提供者が安全性の高い取引を望む場合、発行者はｓｕｂＰＩＤのビット長を長くして発行する。逆にそれほど高い安全性が必要でない場合は、短いビット長のｓｕｂＰＩＤを発行する。図９において、サービス提供者Ｑに対して一番長いｓｕｂＰＩＤを発行しているので、図９のサービス提供者の中では一番高い安全性を要求していることになる。逆にサービス提供者Ｄは要求する安全性が最も低い。

【００４３】

ところで、本実施形態の認証システムにおいて発行者を複数配置すると、ユーザ、サービス提供者、発行者のいずれにとってもセキュリティのリスクが大きく低減される。図１１は一人のユーザが三つの発行者Ｘ，Ｙ，Ｚからそれぞれ ＰＩＤ２０，３０，４０を発行され、二つのサービス提供者Ｐ，Ｑとそれぞれ取引を行う例を示している。

【００４４】

図１１に示すように、サービス提供者Ｐは、発行者Ｘおよび発行者Ｚからそれぞれサービス提供の対象となるユーザのｓｕｂＰＩＤ２１，４１を取得する。同様に、サービス提供

者Ｑは、発行者Ｘ、発行者Ｙおよび発行者ＺからそれぞれｓｕｂＰＩＤ２２，３１，４２を取得する。ユーザは、サービス提供者Ｐとの間においてはｓｕｂＰＩＤ２１，４１を用いて認証し、サービス提供者Ｑとの間においてはｓｕｂＰＩＤ２２，３１，４２を用いて認証する。

【００４５】

図１２に示すように、発行者Ｙのセキュリティが破られ、ＰＩＤ３０が漏洩した場合、ユーザは発行者ＹからのｓｕｂＰＩＤ３１を受け取っているサービス提供者Ｑのサービスは利用できなくなるが、サービス提供者Ｐのサービスの利用には影響しない。一方、サービス提供者側からみた場合、サービス提供者Ｑのサービスを利用するには、漏洩したＰＩＤ３０のｓｕｂＰＩＤ３１だけでなく、他の発行者Ｘ，Ｚによりそれぞれ発行された二つのｓｕｂＰＩＤ２２，４２が必要であるため、サービス提供者Ｑへの影響もない。

【００４６】

また、図１３に示すように、サービス提供者Ｐのセキュリティが破られ、ｓｕｂＰＩＤ２１，４１が漏洩した場合、サービス提供者Ｑとの間で利用するｓｕｂＰＩＤ２２，３１，４１とは独立しているため、サービス提供者Ｑの利用には影響がない。すなわち、サービス提供者側からみれば、自身のセキュリティが破られてｓｕｂＰＩＤが漏洩しても、他のサービス提供者のｓｕｂＰＩＤとは独立しているため、他サービス提供者への影響はない。

【００４７】

このように、発行者を複数にし、なおかつユーザがサービス提供者との取引において、複数の発行者により発行されたｓｕｂＰＩＤを用いる場合には、たとえ一つの発行者からのＰＩＤが漏洩しても、他人がサービスをなりすまして受けるには不十分である。すなわち、他人がそのユーザになりすましてサービスを受けるためには、他の発行者のＰＩＤあるいはｓｕｂＰＩＤが必要になるため、サービスを悪用することはできない。

【００４８】

なお、本実施形態においては、発行者のサーバ１により発行されたＰＩＤおよびｓｕｂＰＩＤは、発行者のサーバ１からユーザのＩＤカード２またはサービス提供者の端末３へそれぞれ直接配布する構成としているが、サーバ１が直接配布するのではなく第三者機関としての仲介機関（エージェント）を介して配布する構成とすることも可能である。

【００４９】

図１４は発行者とユーザとの間にエージェントを配置した例を示しており、（ａ）は発行者が一つの場合の例を、（ｂ）は発行者が複数の場合の例をそれぞれ示している。この場合、発行者のサーバ１はＰＩＤおよびｓｕｂＰＩＤの発行のみを行い、ＰＩＤおよびｓｕｂＰＩＤの配布などはエージェントの仲介サーバ（図示せず。）が行う。

【００５０】

このようなエージェントを置く目的としては、図１４（ｂ）に示すように、複数の発行者Ｘ，ＹからＰＩＤ等が発行された場合、それらのＰＩＤ等の全体を一括して配布・管理する方が運用上効率的な場合があるからである。また、図１４（ａ）に示すように、発行者が一つの場合でも、ＰＩＤの管理をエージェントにより行うことでサーバ１の負荷を分散することができるので、運用上の利点がある。

【００５１】

図１５はより具体的なエージェントの運用例を示す図である。図１５に示すように、複数の発行者Ｘ，Ｙが存在する場合、複数の発行者Ｘ，Ｙから一人のユーザに対して複数のＰＩＤが発行される。発行者Ｘ，Ｙはそれぞれが発行したＰＩＤを管理し、エージェントはすべてのＰＩＤを管理する。また、ユーザおよびサービス提供者へのｓｕｂＰＩＤの発行に際しては、場合に応じて複数のＰＩＤから一つのｓｕｂＰＩＤを割り当てる作業をエージェントが代行する。この場合、エージェントが発行者の一部の機能を担っているともいえる。

【００５２】

ところで、ＰＩＤの生成方法には、例えば以下の三通りが考えられる。

（ａ）発行されたＩＤそのものをＰＩＤとして使用する。
（ｂ）発行されたＩＤを伸張あるいは圧縮して、それをＰＩＤとする。
（ｃ）発行されたＩＤとは別にＰＩＤを用意する。
この場合、（ａ）の方法は、ＩＤ＝ＰＩＤであり、（ｂ）の方法は、ＩＤ＋ＰＩＤ（ＩＤとの関連性有り）であり、（ｃ）の方法は、ＩＤ＋ＰＩＤ（ＩＤとの関連性なし）という形になる。いずれを採用するかは、実際に運用する場合に依る。
【００５３】
また、生成されたＰＩＤからどのようにｓｕｂＰＩＤを抽出して発行するかについては、例えば次の二通りの方法が考えられる。
（ａ）連続的にｓｕｂＰＩＤを抽出する方法。
（ｂ）不連続的（ランダム）にｓｕｂＰＩＤを抽出する方法。
【００５４】
図１６はｓｕｂＰＩＤの抽出方法の例を示している。同図（ａ）に示すように、連続的に抽出する場合は、抽出が容易なうえ、管理が簡便になるという利点がある。一方、同図（ｂ）に示すように、不連続的に抽出する場合は、予めＰＩＤに区切りを入れておき、その中からランダムにｓｕｂＰＩＤの一部を取り出し、それらを結合させてｓｕｂＰＩＤとする方法が考えられる。
【００５５】
ところで、ｓｕｂＰＩＤ情報の保持方法については、例えば次の三つの方法が考えられる。
（ａ）ｓｕｂＰＩＤに関する情報も含めてＰＩＤ上にすべて格納する。
（ｂ）ｓｕｂＰＩＤに関する情報はＰＩＤとは別にユーザ保有のデータベースなどに格納する。
（ｃ）ユーザはｓｕｂＰＩＤに関する情報を一切持たず、各サービス提供者がｓｕｂＰＩＤに関する情報も含めて各ｓｕｂＰＩＤを分散して保持する。
【００５６】
ここで、ｓｕｂＰＩＤに関する情報とは、ｓｕｂＰＩＤがＰＩＤ上のどの部分から抽出されたものであるかを示す情報（以下、「ｓｕｂＰＩＤ抽出情報」と称す。）をいう。ｓｕｂＰＩＤ抽出情報は、例えば、ＰＩＤ上のｓｕｂＰＩＤの位置を示すアドレス等である。
【００５７】
（ａ），（ｂ）については、ユーザがすべての情報を保持しておく形態である。この場合、ユーザはＩＤカード２のＩＣチップ４上のＰＩＤからサブＩＤ抽出情報に基づいてｓｕｂＰＩＤを特定し、取引の対象であるサービス提供者の端末３とこのｓｕｂＰＩＤをやり取りすることで認証を行う。（ａ）の場合、ユーザがＩＤカード２以外にデータベース等を保有する必要がなく、簡単な構成で安全な認証システムを構築することができる。（ｂ）の場合、ＰＩＤとｓｕｂＰＩＤ抽出情報とを別々に保持することで、一方の情報が漏洩してもそれだけでは利用できないため、悪用を防ぐことができる。
【００５８】
（ｃ）については、ユーザはＰＩＤ以外の情報をまったく持たない形態である。この場合、ユーザは、サービス提供者の端末３から提供されるｓｕｂＰＩＤとｓｕｂＰＩＤ抽出情報に基づいて、ＩＣチップ４上のＰＩＤからｓｕｂＰＩＤを特定し、認証を行う。このように、ユーザがｓｕｂＰＩＤ抽出情報を持たないことによって、ユーザのＰＩＤが漏洩しても、他人はそのＰＩＤのみではどのようにｓｕｂＰＩＤが構成されているか分からないため、悪用することは不可能である。
【００５９】
【発明の効果】
本発明により、以下の効果を奏することができる。
【００６０】
（１）発行者のサーバからユーザのＩＤ保持体に対して一つのユーザＩＤを発行し、発行者のサーバは、サービス提供者の端末に対してユーザＩＤの一部を抽出してサブＩＤとし

て発行し、ユーザのＩＤ保持体とサービス提供者の端末との間でサブＩＤを用いて認証する構成により、ユーザがサービス提供者からサービスの提供を受ける際、ユーザとサービス提供者との間の認証をユーザＩＤの全部ではなくその一部であるサブＩＤにより認証するため、仮にこのサブＩＤが漏洩した場合であっても、ユーザＩＤの全部が漏洩することがなく、ユーザＩＤの漏洩に対する安全性が向上する。

【００６１】

（２）複数の発行者のサーバからユーザのＩＤ保持体に対してそれぞれ一つずつユーザＩＤを発行し、複数の発行者のサーバは、サービス提供者の端末に対して、それぞれユーザのＩＤ保持体に対して発行したユーザＩＤの一部を抽出してサブＩＤとして発行し、ユーザのＩＤ保持体とサービス提供者の端末との間で複数の発行者のサーバがそれぞれ発行した複数のサブＩＤを用いて認証する構成により、ユーザがサービス提供者からサービスの提供を受ける際、ユーザとサービス提供者との間の認証を複数の発行者のサーバから発行されたユーザＩＤの全部ではなく、それぞれの一部を抽出して発行された複数のサブＩＤにより認証するため、仮に一つのサブＩＤが漏洩した場合であっても、他のサブＩＤまですべて漏洩しなければ悪用することはできず、さらに安全性が向上する。

【００６２】

（３）複数の発行者のサーバによりそれぞれ発行されたユーザＩＤまたはサブＩＤを、仲介機関のサーバが一括してユーザのＩＤ保持体またはサービス提供者の端末へ引き渡す構成により、複数の発行者のサーバによりそれぞれ発行されたユーザＩＤ、サブＩＤの管理、発行を効率良く行うことが可能となる。

【００６３】

（４）ユーザのＩＤ保持体が、サブＩＤがユーザＩＤ上のどの部分から抽出されたものであるかを示すサブＩＤ抽出情報を含めて保持する構成によって、簡単な構成により上記安全な認証システムを構築することができる。

【００６４】

（５）ユーザのＩＤ保持体が、サブＩＤがサブＩＤ抽出情報をユーザＩＤとは別に保持する構成によって、一方の情報が漏洩した場合であっても他人により悪用されるのを防止することができる。

【００６５】

（６）ユーザのＩＤ保持体は、サブＩＤ抽出情報を保持せず、サービス提供者の端末が、サブＩＤ抽出情報をサブＩＤとともに保持する構成によって、ユーザからユーザＩＤが漏洩した場合であっても他人により悪用されるのを防止することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態における認証システムの概略構成図である。

【図２】図１のサーバの機能構成を示すブロック図である。

【図３】ユーザが発行者からＰＩＤを取得するプロセスを示す説明図である。

【図４】ＰＩＤの保持状態を示す説明図である。

【図５】サービス提供者がユーザに対してサービス提供を行うプロセスを示す説明図である。

【図６】ＰＩＤおよびｓｕｂＰＩＤの保持状態を示す説明図である。

【図７】複数のユーザが同一のサービスの提供を受ける場合の例を示す説明図である。

【図８】一人のユーザが複数のサービスの提供を受ける場合の例を示す説明図である。

【図９】複数のサービス提供者に互いに重複しないｓｕｂＰＩＤを発行する例を示す説明図である。

【図１０】複数のサービス提供者に重複を許してｓｕｂＰＩＤを発行する例を示す説明図である。

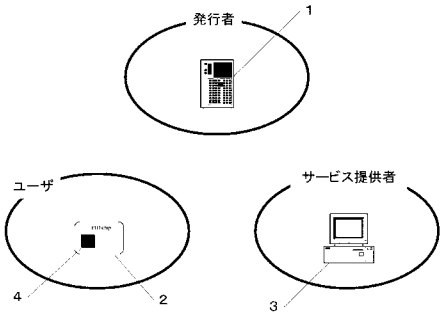
【図１１】一人のユーザが複数の発行者からＰＩＤを発行され、複数のサービス提供者と取引を行う例を示す説明図である。

【図１２】発行者の一つからＰＩＤが漏洩した場合の例を示す説明図である。

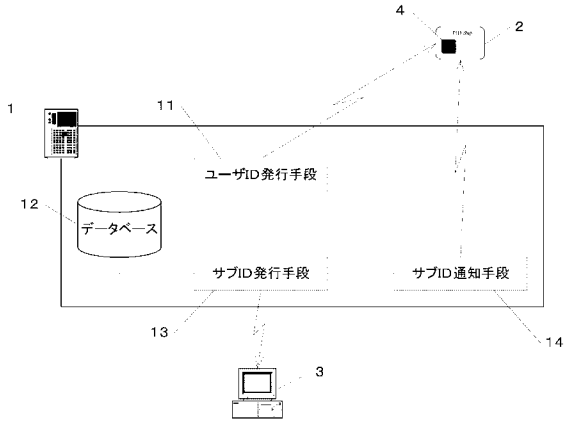
【図１３】サービス提供者の一つからｓｕｂＰＩＤが漏洩した場合の例を示す説明図であ

る。
【図１４】発行者とユーザとの間にエージェントを配置した例を示す説明図である。
【図１５】具体的なエージェントの運用例を示す説明図である。
【図１６】ｓｕｂＰＩＤの抽出方法の例を示す説明図である。
【符号の説明】
１　サーバ
２　ＩＤカード
３　端末
４　ＩＣチップ
１１　ユーザＩＤ発行手段
１２　データベース
１３　サブＩＤ発行手段
１４　サブＩＤ通知手段
２０，３０，４０　ＰＩＤ
２１，２２，３１，４１，４２　ｓｕｂＰＩＤ

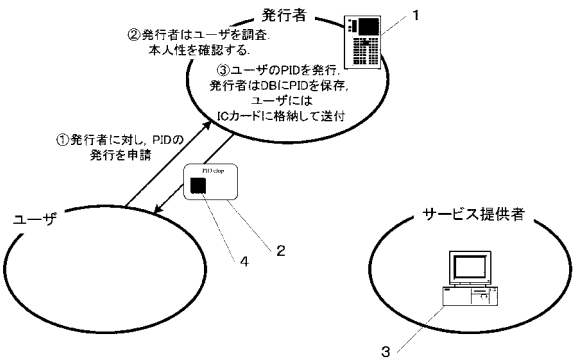
【図１】



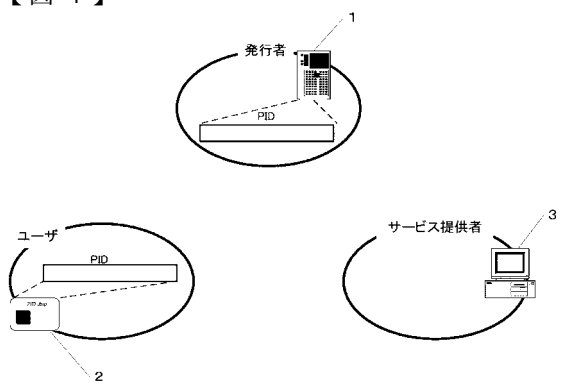
【図２】



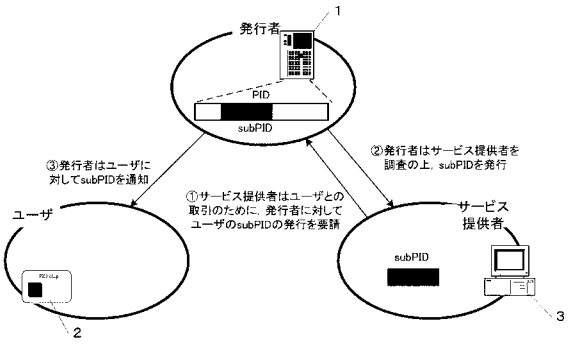
【図３】



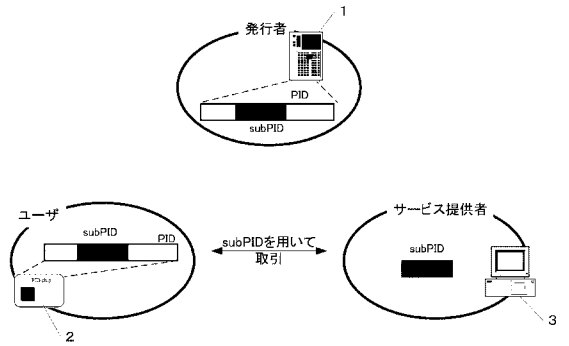
【図４】



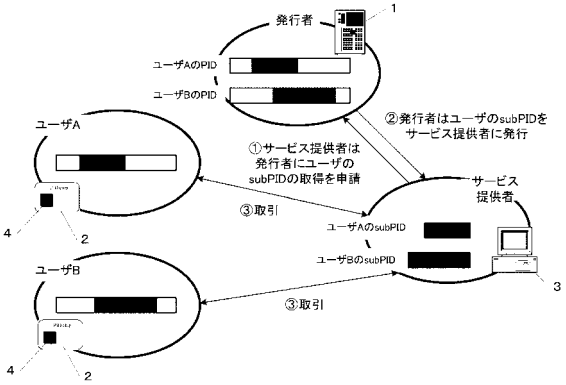
【図５】



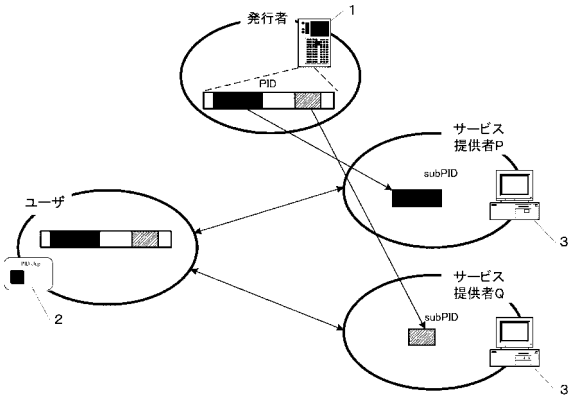
【図６】



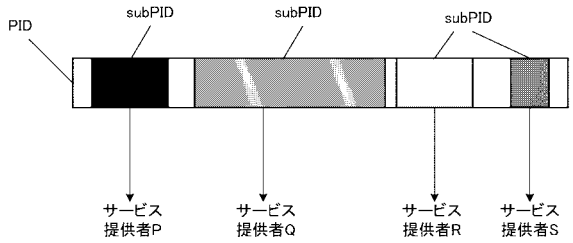
【図７】



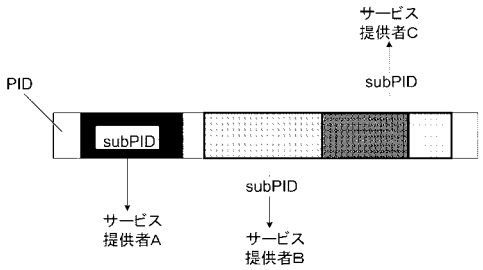
【図８】



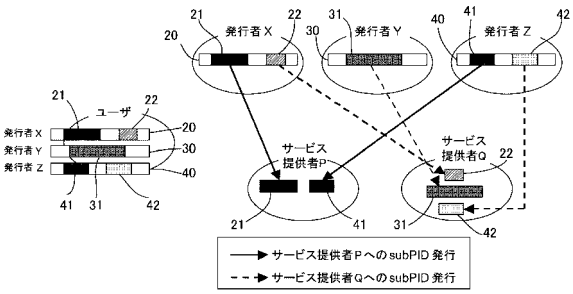
【図９】



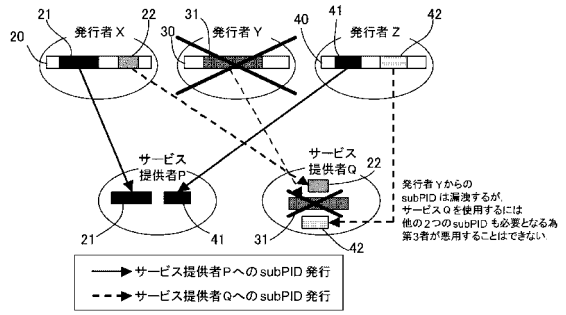
【図１０】



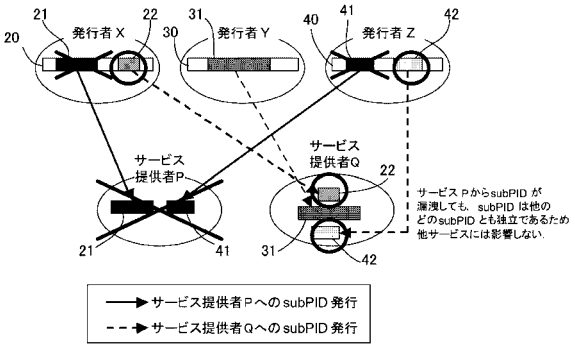
【図１１】



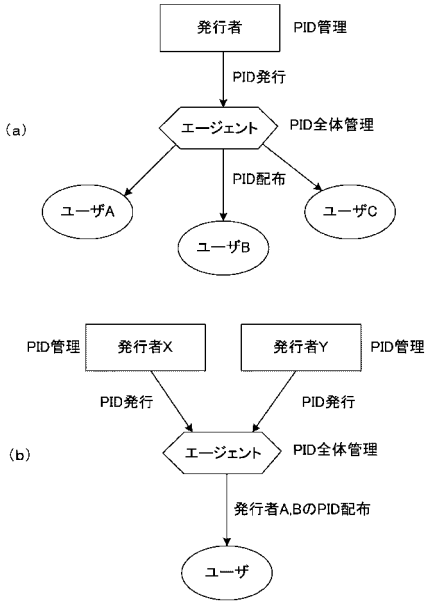
【図１２】



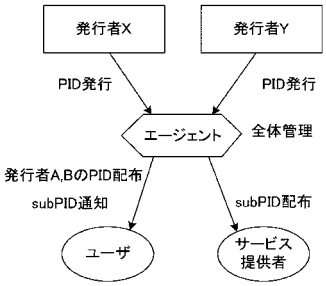
【図１３】



【図１４】



【図１５】



【図１６】