

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4666878号
(P4666878)

(45) 発行日 平成23年4月6日(2011.4.6)

(24) 登録日 平成23年1月21日(2011.1.21)

(51) Int. Cl.		F I			
G06F 21/20	(2006.01)	G06F	15/00	330B	
G09C 1/00	(2006.01)	G06F	15/00	330G	
H04L 9/32	(2006.01)	G09C	1/00	660A	
		H04L	9/00	673A	

請求項の数 14 (全 15 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)
 (65) 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)
 審査請求日 平成17年12月12日(2005.12.12)
 審判番号 不服2008-30061 (P2008-30061/J1)
 審判請求日 平成20年11月26日(2008.11.26)

特許法第30条第1項適用 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

特許法第30条第1項適用 2002年9月26日九州大学大学院システム情報科学研究院発行の刊行物「九州大学大学院システム情報科学紀要第7巻第2号」に発表

(73) 特許権者 504145342
 国立大学法人九州大学
 福岡県福岡市東区箱崎六丁目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

合議体
 審判長 赤川 誠一
 審判官 田中 秀人
 審判官 富吉 伸弥

最終頁に続く

(54) 【発明の名称】 認証方法および認証システム

(57) 【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。

10

20

【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、前記ユーザが前記ユーザの 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。

10

【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。

20

【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を配置し、

30

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 11】

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、

40

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 12】

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 11 記載の認証システム。

【請求項 13】

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、前記ユーザが前記ユーザの 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

50

ことにより行う構成とした請求項 10 から 12 のいずれかに記載の認証システム。

【請求項 14】

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 10 から 12 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認証システムに 10 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。 20

【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。) 30

【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。 40

【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認証システムを提供することを目的と 50

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。

10

【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。

20

【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。

30

【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。

40

【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。

50

【 0 0 1 7 】

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。

【 0 0 1 8 】

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。

10

【 0 0 1 9 】

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。

【 0 0 2 0 】

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。

20

【 0 0 2 1 】

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。

【 0 0 2 2 】

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。

30

【 0 0 2 3 】

【 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。

40

【 0 0 2 4 】

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I

50

D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

10

20

30

40

50

者は、発行者から s u b P I D 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。s u b P I D とユーザの本人性については、発行者が保証する。

【 0 0 3 3 】

以上のプロセスにより、サービス提供者はユーザの s u b P I D 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 s u b P I D 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 1 4 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、P I D を保持し、なおかつ s u b P I D 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 s u b P I D のみを保持している。

10

【 0 0 3 4 】

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 P I D (s u b P I D) とサービス提供者が端末 3 に保持する s u b P I D 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。

【 0 0 3 5 】

また、前述のように、ユーザの P I D 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 P I D の全体ではなくその一部である s u b P I D により認証するため、仮にこの s u b P I D が何らかの形で漏洩した場合であっても、ユーザの P I D 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、P I D 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。

20

【 0 0 3 6 】

なお、s u b P I D 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。

【 0 0 3 7 】

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。

30

【 0 0 3 8 】

(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 s u b P I D を発行者から発行してもらう必要がある。s u b P I D 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 s u b P I D を用いてユーザ A , B との間でサービス提供を行う。s u b P I D は各ユーザによって異なるので、一人のユーザの s u b P I D に事故があっても、他のユーザには影響がない。

40

【 0 0 3 9 】

(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 s u b P I D を取得する手順は前述と同様であるが、発行者の s u b P I D の発行方法に三つの特徴がある。これは P I D が長いビット列であるという特性に基づいている。

【 0 0 4 0 】

一つ目は、各 s u b P I D が、他の s u b P I D と重複しないように発行するという方法である。P I D は長いビット列であり、s u b P I D はその一部である。例えば、図 9 に

50

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 P I D からそれぞれ s u b P I D を発行する場合、お互いが重複しないように提供する。各 s u b P I D は互いに独立しているため、何らかの形で一つの s u b P I D 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。

【 0 0 4 1 】

二つ目は、図 1 0 に示すように、各 s u b P I D 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 s u b P I D が漏洩した場合、前述した各 s u b P I D 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 s u b P I D と一部重複した部分の s u b P I D 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十分に確保できる。このような s u b P I D の発行方法は、簡易的なサービスを 10
提供する場合や、同一サービス提供者による複数の s u b P I D 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。

【 0 0 4 2 】

三つ目は、発行する s u b P I D 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 s u b P I D 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 s u b P I D 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 s u b P I D を発行しているの、図 9 のサービス提供者の中では一番高い安全性を 20
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。

【 0 0 4 3 】

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 1 1 は一人のユーザが三つの発行者 X, Y, Z からそれぞれ P I D 2 0, 3 0, 4 0 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。

【 0 0 4 4 】

図 1 1 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 s u b P I D 2 1, 4 1 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 s u b P I D 2 2, 3 1, 4 2 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 s u b P I D 2 1, 4 1 を用いて認証し、サービス提供者 Q との間においては s u b P I D 2 2, 3 1, 4 2 を用いて 30
認証する。

【 0 0 4 5 】

図 1 2 に示すように、発行者 Y のセキュリティが破られ、P I D 3 0 が漏洩した場合、ユーザは発行者 Y からの s u b P I D 3 1 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 P I D 3 0 の s u b P I D 3 1 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 s u b P I D 2 2, 4 2 が必要であるため、サービス提供者 Q への影響もない。

【 0 0 4 6 】

また、図 1 3 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、s u b P I D 2 1, 4 1 が漏洩した場合、サービス提供者 Q との間で利用する s u b P I D 2 2, 3 1, 4 1 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 s u b P I D が漏洩しても、他のサービス提供者の s u b P I D 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。 40

【 0 0 4 7 】

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 s u b P I D を用いる場合には、たとえ一つの発行者からの P I D 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 P I D ある 50

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。

10

【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みえる。

20

【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。

30

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。

40

【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。

50

(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

10

20

30

40

50

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

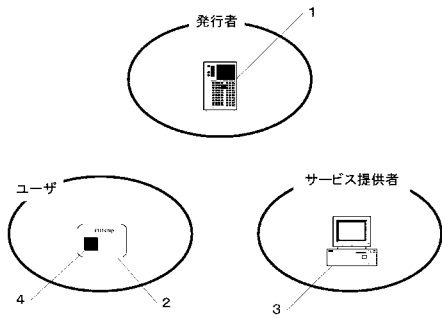
10

20

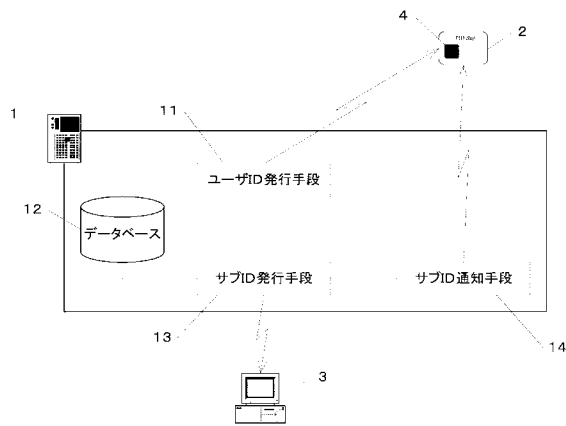
30

40

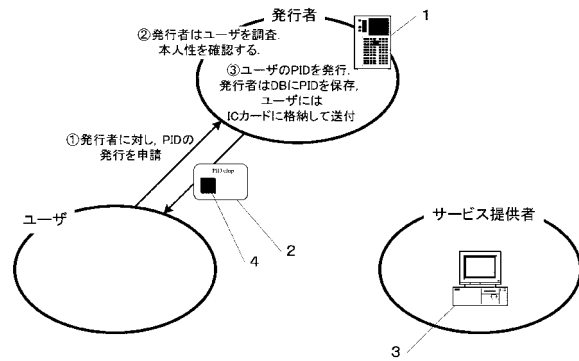
【図1】



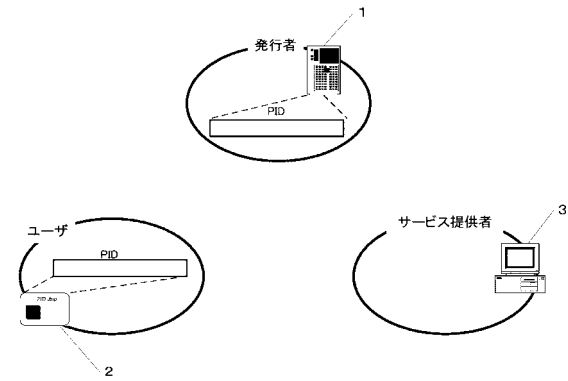
【図2】



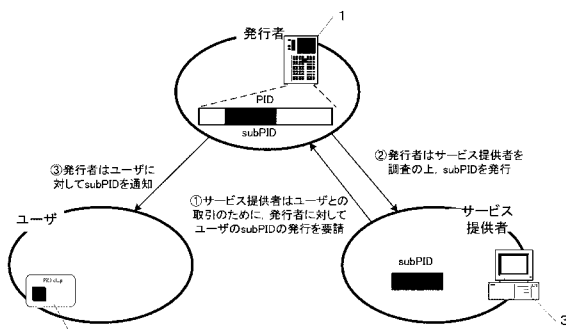
【図3】



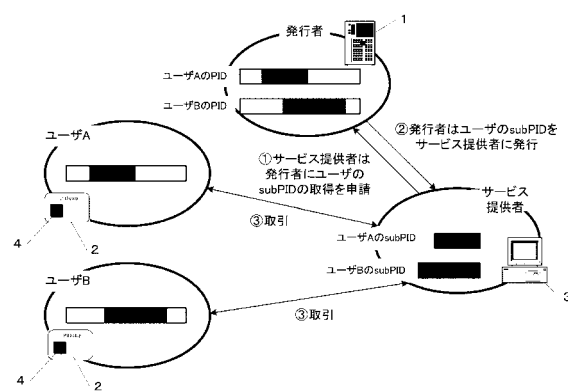
【図4】



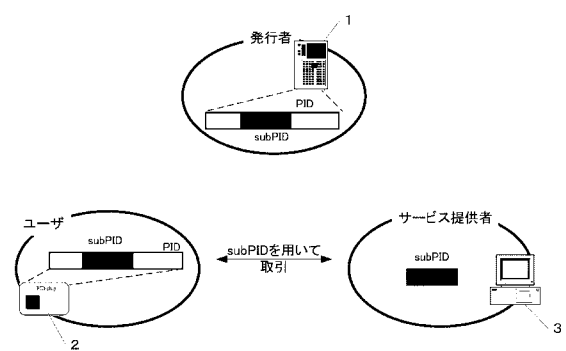
【図5】



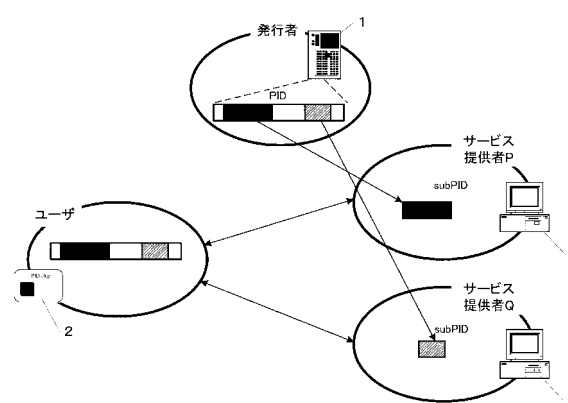
【図7】



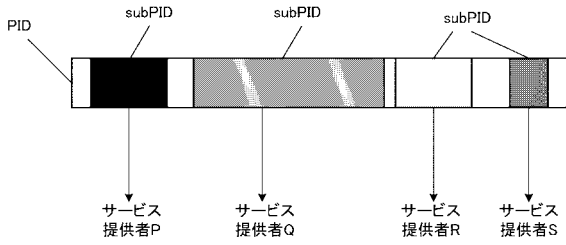
【図6】



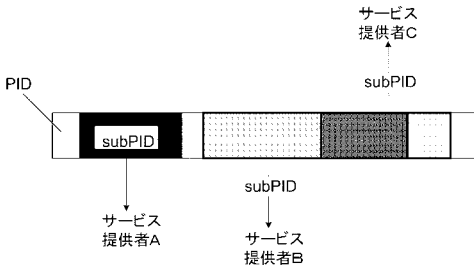
【図8】



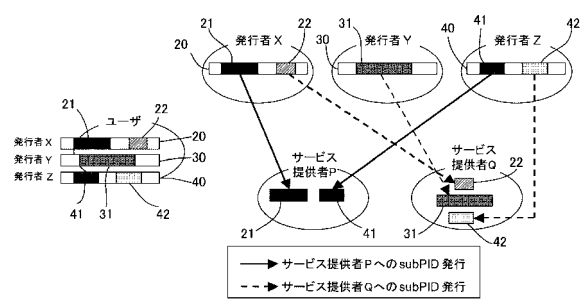
【図9】



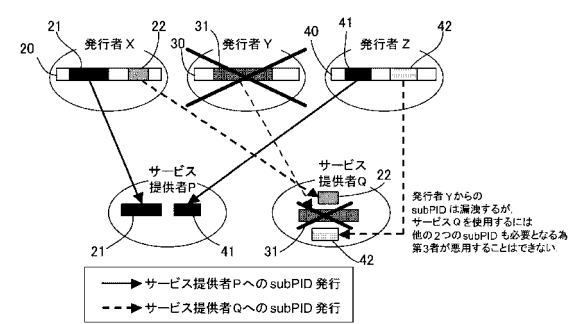
【図10】



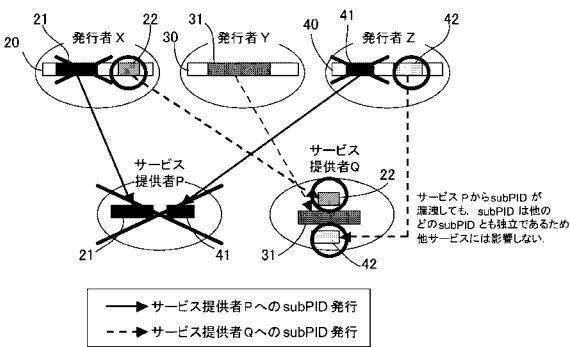
【図11】



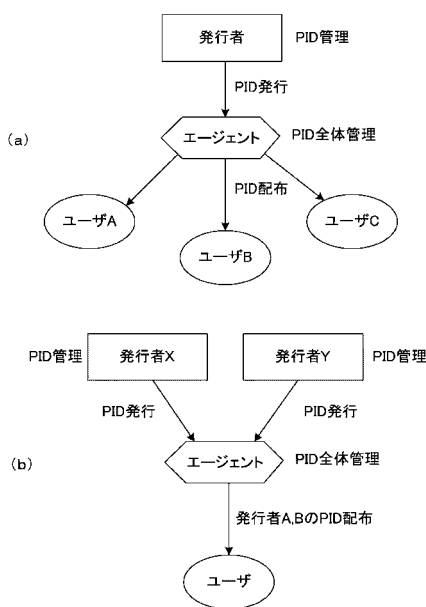
【図12】



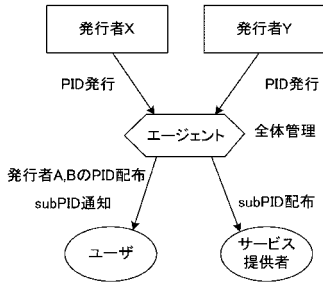
【図13】



【図14】

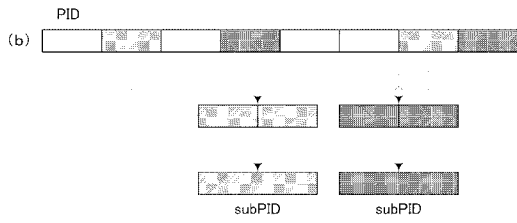


【図15】



【図16】

(a) PID 011100111110101010100101110100101



フロントページの続き

(56)参考文献 特開2001-344205号公報(JP, A)
特開2001-312565号公報(JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 15/00 330B, G06F 15/00 330G, G09C 1/00 660A, H04L 9/00 673A