(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2006-128873
(P2006-128873A)
(43)公開日　平成18年5月18日(2006.5.18)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104

審査請求 未請求　請求項の数 7　ＯＬ　（全 14 頁）

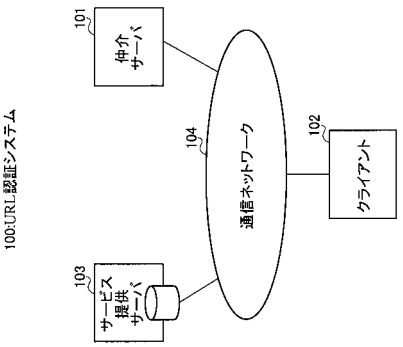
(21)出願番号　特願2004-312084 (P2004-312084)
(22)出願日　平成16年10月27日 (2004.10.27)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　青山　恭弘
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内
(72)発明者　鬼頭　勉
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内

最終頁に続く

(54)【発明の名称】ＵＲＬ認証システム及びＵＲＬ認証方法

(57)【要約】
【課題】　ＯＴＵの発行者とＯＴＵの受付者が物理的に異なる場合でも、ＯＴＵの偽造又は改竄による不正アクセスを防止するＵＲＬ認証システム及びＵＲＬ認証方法を提供する。
【解決手段】　サービス提供サーバ１０３が仲介サーバ１０１に接続方法を通知し、仲介サーバ１０１がサービス提供サーバ１０３に共通鍵Ｋｃを通知する。クライアント１０２が仲介サーバ１０１にサービス提供サーバ１０３への接続要求を通知すると、仲介サーバ１０１が共通鍵Ｋｃを用いて認証コードを生成し、生成した認証コードをＵＲＬに付加したＯＴＵを発行する。クライアント１０２はＯＴＵを辿ることにより、サービス提供サーバ１０３に接続し、サービス提供サーバ１０３は、クライアント１０２から提示されたＯＴＵの正当性を共通鍵Ｋｃによって確認し、ＯＴＵの正当性を確認すると、クライアント１０２にサービスを提供する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
自サーバとは異なる他のサーバへの接続を誘導するOne Time URLにOne Time URL自体の正当性を証明する認証コードを含め、認証コードを含むOne Time URLを発行する仲介サーバと、
前記仲介サーバによって発行されたOne Time URLを取得し、取得したOne Time URLを辿ることにより、前記仲介サーバとは異なる他のサーバに接続するクライアントと、
前記クライアントが接続に用いたOne Time URLの正当性を確認し、One Time URLの正当性が確認されたクライアントにサービスを提供する、前記仲介サーバとは異なる他のサーバとしてのサービス提供サーバと、
を具備することを特徴とするＵＲＬ認証システム。
【請求項２】
前記サービス提供サーバは、前記仲介サーバが認証コードの生成に用いる暗号鍵を共有し、共有した暗号鍵を用いて認証コードの正当性を確認することを特徴とする請求項１に記載のＵＲＬ認証システム。
【請求項３】
前記仲介サーバと前記サービス提供サーバとの間にセキュアな通信路を備え、前記通信路を介して前記暗号鍵を共有することを特徴とする請求項２に記載のＵＲＬ認証システム。
【請求項４】
自サーバとは異なる他のサーバへの接続を誘導するOne Time URLにOne Time URL自体の正当性を証明する認証コードを公開鍵暗号方式に基づく鍵対の一方である秘密鍵を用いて生成し、生成した認証コードを含むOne Time URLを発行する仲介サーバと、
前記仲介サーバによって発行されたOne Time URLを取得し、取得したOne Time URLを辿ることにより、前記仲介サーバとは異なる他のサーバに接続するクライアントと、
前記クライアントが接続に用いたOne Time URLの認証コードに前記秘密鍵と鍵対をなす公開鍵を用いてOne Time URLの正当性を確認し、One Time URLの正当性が確認されたクライアントにサービスを提供する、前記仲介サーバとは異なる他のサーバとしてのサービス提供サーバと、
を具備することを特徴とするＵＲＬ認証システム。
【請求項５】
自サーバとは異なる他のサーバへの接続を誘導するOne Time URLの正当性を証明する認証コードの生成に第１暗号鍵を用いる認証コード生成手段と、
前記認証コード生成手段によって生成された認証コードを含めたOne Time URLを生成するOne Time URL生成手段と、
前記認証コード生成手段で用いられた第１暗号鍵に応じた第２暗号鍵を前記自サーバとは異なる他のサーバに通知する通知手段と、
を具備することを特徴とする仲介サーバ。
【請求項６】
請求項５に記載の仲介サーバから通知された第２暗号鍵を用いて、クライアントが接続に用いたOne Time URLの正当性を検証するOne Time URL検証手段と、
前記One Time URL検証手段によってOne Time URLの正当性が検証されたクライアントにサービスを提供するサービス提供手段と、
を具備することを特徴とするサービス提供サーバ。
【請求項７】
仲介サーバが、自サーバとは異なる他のサーバへの接続を誘導するOne Time URLにOne Time URL自体の正当性を証明する認証コードを含め、認証コードを含むOne Time URLを発行し、
クライアントが、前記仲介サーバによって発行されたOne Time URLを取得し、取得したOne Time URLを辿ることにより、前記仲介サーバとは異なる他のサーバに接続し、

前記仲介サーバとは異なる他のサーバとしてのサービス提供サーバが、前記クライアントが接続に用いたOne Time URLの正当性を確認し、One Time URLの正当性が確認されたクライアントにサービスを提供する
ことを特徴とするＵＲＬ認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＵＲＬ認証システム及びＵＲＬ認証方法に関し、特に、One Time URLの認証を行うＵＲＬ認証システム及びＵＲＬ認証方法に関する。
【背景技術】
【０００２】
一般に、One Time URL（以下、「ＯＴＵ」と省略する）は、ユーザが公衆ネットワーク上の特定コンテンツにアクセスしようとする度に異なるＵＲＬを発行してコンテンツを視聴させる仕組であり、一旦ＵＲＬが使用された場合、あるいは一定時間が経過した場合は発行済みＵＲＬが無効となる。また、有料コンテンツなど利用者を限定するコンテンツを提供する場合、既に行っている認証システムと連動させて不正アクセスの防止を補完する（例えば、特許文献１参照）。例えば、コンサートライブストリーミングに事前に申し込みをしておくと、開演直前にユーザ毎に異なるＵＲＬを発行する。このようなＯＴＵの特徴により、特定のユーザを特定のＷｅｂページに誘導したり、ＵＲＬを取得していること自体が本人認証を兼ねることから簡易なユーザ認証機能を実現したり、特定Ｗｅｂページへのアクセス回数やアクセス期間等を制限したりすることができる。
【０００３】
特に、ＯＴＵは、ユーザ認証の補完的意味合いで用いられることが多い。ＯＴＵはＷｅｂサーバが特定ユーザに対して必要に応じて随時発行するという性質のものであるため、それを知っていること、すなわち、そのＯＴＵを辿って特定のＷｅｂページに到達できるということ自体がそのまま認証的な機能を実現することになり、このような用い方が一般的である。例えば、昨今の会員登録制Ｗｅｂサービスでは、ユーザ登録情報の変更の際に予め登録していたメールアドレスへＯＴＵが送信され、そのユーザ固有の登録情報変更画面へユーザを誘導するという例が多く見られる。具体的には、ユーザ情報変更のためのフロントページでユーザＩＤとパスワードを入力するとユーザ情報変更用メインページのＯＴＵがメールで送られてくるというものである。
【０００４】
図５は、ＯＴＵの一例を示す図である。この図において、“http://server.¯php”のＡ１部分が位置情報（接続される装置、アクセス用ＴＣＰポート番号（図では8080）及びアクセス対象とするサーバ上のコンテンツ情報）を示しており、“Param1¯ZZZZ”のＡ２部分がＵＲＬパラメータといわれ、ＨＴＴＰプロトコルによるアクセス時にクライアントからサーバに渡されるパラメータ群である。このＵＲＬの構成は一般にインターネットで使用されるＵＲＬのデータ構造そのものであり、インターネットを構成するＩＰネットワークは、ＯＴＵの前半部分Ａ１から接続すべきサーバの位置を把握し、クライアントからサーバへのパケット伝達経路の自立解決を図る。
【０００５】
ＯＴＵの一般的な使用方法としては、図５のXXXやYYYYにはアクセス制限情報（ユーザ情報やアクセス制限数等）を記載し、ZZZZには暗号化した認証コードを記載するといった形態が多く見られる。ここで、ZZZZはＯＴＵの信憑性を証明するための文字列であり、ＯＴＵ全体から“ADM=ZZZZ”を除いた文字列（図５のＡ３部分）に対して、サーバが保持する秘密鍵を用いてハッシュ演算を行った結果である。
【０００６】
なお、ここでは、One Time URLという表現を用いているが、一般的に同種のＵＲＬの使用制限はサーバ側の設定に依存するものであり、その使用が１回のみに限定される場合もあれば、一定期限内に複数回の使用が許可される場合もあり得る。

【０００７】
次に、上述したＯＴＵを用いたサーバ、クライアント間の接続処理について図６を用いて説明する。図６において、サーバはクライアントからサービス提供の要求（ＯＴＵ発行要求）を受けると、ＵＲＬパラメータを選択し、選択したＵＲＬパラメータを図５に示したＯＴＵのＡ１部分に付加する。そして、ＯＴＵのＡ３部分に共通鍵Ｋｃでハッシュ演算を行うことにより得られる認証コードZZZZをＯＴＵのＡ３部分に付加し、クライアントにＯＴＵが発行される。
【０００８】
クライアントは、サーバから発行されたＯＴＵを取得し、取得したＯＴＵにてサーバにアクセスする。クライアントからＯＴＵにてアクセスを受けたサーバは、ＯＴＵのＡ３部分に共通鍵Ｋｃでハッシュ演算を行って認証コードGGGGを計算する。最後に、認証コードGGGGとＯＴＵに付加されていたZZZZが同一であることを認識して、アクセスに用いられたＯＴＵが偽造及び改竄されたものではないこと、すなわち、ＯＴＵの正当性を認識する。このように、ＯＴＵの発行と受け付けは、通常、物理的に同一のサーバで行うものである。
【０００９】
ところで、近年、インターネットの常時接続環境の普及が進み、ＤＶＤレコーダ、ネットワークカメラ、白物家電といった様々な電化機器（以下、「宅内機器」という）がネットワークに接続するようになってきた。企業や家庭におけるこれらのネットワーク環境（以下、「宅内ローカルネットワーク」という）は、ＮＡＴ（Network Address Translation）あるいはＮＡＰＴ（Network Address Port Translation）機能を有するルータによってインターネットに接続しているのが一般的である。
【００１０】
このため、宅外から特定の宅内機器への接続を想定した場合、ＩＰトラバーサルの問題、いわゆるＮＡＴ越えの問題を解消する必要がある。すなわち、宅内機器の大部分はローカルアドレス空間に設置されているため、位置情報（ＩＰアドレス）のみを指定しても宅外から特定の宅内機器への経路を決定することができず、位置情報とポート番号の双方を指定する必要がある。
【００１１】
一方、ＮＡＴ越しにアクセスする際のポート番号を宅外から知得することは困難であり、このため、図７に示すように、常に宅内機器（サービス提供サーバ）と同期しながらポート番号を把握する接続仲介者（仲介サーバ）が必要となる。
【００１２】
このようなシステムにおいて、位置情報とポート番号の双方を明示的に用いて、簡便に接続のリダイレクトが可能なＯＴＵが用いられている。例えば、宅内のＨＤＤプレイヤ（宅内機器）に蓄積された映像コンテンツを宅外の携帯電話（クライアント）で視聴しようとするユーザは、特定サービスＡＳＰ（仲介サーバ）と契約を行い、ＡＳＰ管理の仲介サーバにＨＤＤプレイヤへの接続方法（接続用ＯＴＵ）を動的に管理・発行させる。
【特許文献１】特開２００３－１５０４９２号公報
【発明の開示】
【発明が解決しようとする課題】
【００１３】
しかしながら、ＯＴＵの発行者（ＯＴＵを発行する装置）とＯＴＵの受付者（ＯＴＵにてアクセスされる装置）が物理的に異なる場合、ＯＴＵそれ自体の正当性、すなわち、当該ＯＴＵが正しい発行者のもとで作られたことの証明、及び、当該ＯＴＵの一部が改竄されていないことの証明、すなわち、ＯＴＵの正当性を確認する手立てが確立されていない。
【００１４】
本発明はかかる点に鑑みてなされたものであり、ＯＴＵの発行者とＯＴＵの受付者が物理的に異なる場合でも、ＯＴＵの偽造又は改竄による不正アクセスを防止するＵＲＬ認証

システム及びＵＲＬ認証方法を提供することを目的とする。
【課題を解決するための手段】
【００１５】
本発明の第１の態様は、自サーバとは異なる他のサーバへの接続を誘導するOne Time URLにOne Time URL自体の正当性を証明する認証コードを含め、認証コードを含むOne Time URLを発行する仲介サーバと、前記仲介サーバによって発行されたOne Time URLを取得し、取得したOne Time URLを辿ることにより、前記仲介サーバとは異なる他のサーバに接続するクライアントと、前記クライアントが接続に用いたOne Time URLの正当性を確認し、One Time URLの正当性が確認されたクライアントにサービスを提供する、前記仲介サーバとは異なる他のサーバとしてのサービス提供サーバと、を具備するＵＲＬ認証システムである。
【００１６】
本発明の第２の態様は、上記態様において、前記サービス提供サーバが、前記仲介サーバが認証コードの生成に用いる暗号鍵を共有し、共有した暗号鍵を用いて認証コードの正当性を確認するＵＲＬ認証システムである。
【００１７】
これらの構成によれば、クライアントが仲介サーバによって発行されたOne Time URLを辿ることにより仲介サーバとは異なる他のサービス提供サーバに接続し、サービス提供サーバがOne Time URLの正当性が確認されたクライアントにサービスを提供することにより、One Time URLの発行者とOne Time URLの受付者が物理的に異なる場合でも、One Time URLの偽造又は改竄による不正アクセスを防止することができる。
【００１８】
本発明の第３の態様は、上記態様において、前記仲介サーバと前記サービス提供サーバとの間にセキュアな通信路を備え、前記通信路を介して前記暗号鍵を共有するＵＲＬ認証システムである。
【００１９】
この構成によれば、仲介サーバとサービス提供サーバとの間に備えられたセキュアな通信路を介して暗号鍵を共有することにより、暗号鍵の漏洩を防止することができる。
【００２０】
本発明の第４の態様は、自サーバとは異なる他のサーバへの接続を誘導するOne Time URLにOne Time URL自体の正当性を証明する認証コードを公開鍵暗号方式に基づく鍵対の一方である秘密鍵を用いて生成し、生成した認証コードを含むOne Time URLを発行する仲介サーバと、前記仲介サーバによって発行されたOne Time URLを取得し、取得したOne Time URLを辿ることにより、前記仲介サーバとは異なる他のサーバに接続するクライアントと、前記クライアントが接続に用いたOne Time URLの認証コードに前記秘密鍵と鍵対をなす公開鍵を用いてOne Time URLの正当性を確認し、One Time URLの正当性が確認されたクライアントにサービスを提供する、前記仲介サーバとは異なる他のサーバとしてのサービス提供サーバと、を具備するＵＲＬ認証システムである。
【００２１】
この構成によれば、クライアントが仲介サーバによって発行されたOne Time URLを辿ることにより仲介サーバとは異なる他のサービス提供サーバに接続し、サービス提供サーバがOne Time URLの正当性が確認されたクライアントにサービスを提供することにより、One Time URLの発行者とOne Time URLの受付者が物理的に異なる場合でも、One Time URLの偽造又は改竄による不正アクセスを防止することができる。
【００２２】
本発明の第５の態様は、自サーバとは異なる他のサーバへの接続を誘導するOne Time URLの正当性を証明する認証コードの生成に第１暗号鍵を用いる認証コード生成手段と、前記認証コード生成手段によって生成された認証コードを含めたOne Time URLを生成するOne Time URL生成手段と、前記認証コード生成手段で用いられた第１暗号鍵に応じた第２暗号鍵を前記自サーバとは異なる他のサーバに通知する通知手段と、を具備する仲介サーバ

である。
【００２３】
この構成によれば、認証コードの生成に用いられた第１暗号鍵に応じた第２暗号鍵を仲介サーバとは異なる他のサーバに通知することにより、他のサーバは仲介サーバで生成されたOne Time URLの正当性を仲介サーバから通知された第２暗号鍵を用いて確認することができる。
【００２４】
本発明の第６の態様は、上記態様の仲介サーバから通知された第２暗号鍵を用いて、クライアントが接続に用いたOne Time URLの正当性を検証するOne Time URL検証手段と、前記One Time URL検証手段によってOne Time URLの正当性が検証されたクライアントにサービスを提供するサービス提供手段と、を具備するサービス提供サーバである。
【００２５】
この構成によれば、One Time URLの正当性を検証されたクライアントにサービスを提供することにより、仲介サーバから発行されたOne Time URLを辿って接続したクライアントに対してのみサービスを提供することになるので、One Time URLの偽造又は改竄による不正アクセスを防止することができる。
【００２６】
本発明の第７の態様は、仲介サーバが、自サーバとは異なる他のサーバへの接続を誘導するOne Time URLにOne Time URL自体の正当性を証明する認証コードを含め、認証コードを含むOne Time URLを発行し、クライアントが、前記仲介サーバによって発行されたOne Time URLを取得し、取得したOne Time URLを辿ることにより、前記仲介サーバとは異なる他のサーバに接続し、前記仲介サーバとは異なる他のサーバとしてのサービス提供サーバが、前記クライアントが接続に用いたOne Time URLの正当性を確認し、One Time URLの正当性が確認されたクライアントにサービスを提供するＵＲＬ認証方法である。
【００２７】
この方法によれば、クライアントが仲介サーバによって発行されたOne Time URLを辿ることにより仲介サーバとは異なる他のサービス提供サーバに接続し、サービス提供サーバがOne Time URLの正当性が確認されたクライアントにサービスを提供することにより、One Time URLの発行者とOne Time URLの受付者が物理的に異なる場合でも、One Time URLの偽造又は改竄による不正アクセスを防止することができる。
【発明の効果】
【００２８】
本発明によれば、サービスを提供するサーバとは異なる仲介サーバがＯＴＵ自体の正当性を証明する認証コードを含むＯＴＵを発行し、サービス提供サーバがＯＴＵの正当性を検証することにより、ＯＴＵの発行者とＯＴＵの受付者が物理的に異なる場合でも、ＯＴＵの偽造又は改竄による不正アクセスを防止するＵＲＬ認証システム及びＵＲＬ認証方法を提供することができる。
【発明を実施するための最良の形態】
【００２９】
以下、本発明の実施の形態について、図面を参照して詳細に説明する。
【００３０】
（実施の形態１）
図１は、本発明の実施の形態１に係るＵＲＬ認証システム１００の構成を示すブロック図である。この図において、仲介サーバ１０１、クライアント１０２及びサービス提供サーバ１０３は、それぞれ一般的な公衆ＩＰネットワークであるインターネット等の通信ネットワーク１０４に接続されている。
【００３１】
仲介サーバ１０１は、サービス提供サーバ１０３と定期的に接続及び情報交換を行うことにより、サービス提供サーバ１０３への接続方法を把握し、把握した接続方法をOne Time URL（以下、「ＯＴＵ」と省略する）にてクライアント１０２に通知する。

【００３２】
クライアント１０２は、仲介サーバ１０１からＯＴＵを取得し、取得したＯＴＵを辿ることによりサービス提供サーバ１０３に接続し、ＨＴＴＰプロトコルを介してサービス提供サーバ１０３からコンテンツを受信したり、サービス提供サーバ１０３に特定の処理を実行させたりする。
【００３３】
サービス提供サーバ１０３は、例えば、ＨＤＤプレイヤ等の宅内機器であり、クライアント１０２から提示されたＯＴＵの認証コード部分を検証することにより、ＯＴＵの正当性を確認し、クライアント１０２へのコンテンツの提供、あるいはクライアント１０２からの指示に応じた特定の処理を実行するなどのサービスを提供する。
【００３４】
図２は、仲介サーバ１０１、クライアント１０２及びサービス提供サーバ１０３の内部構成を示すブロック図である。まず、仲介サーバ１０１について説明する。図２において、サーバ間通信部１１１は、通信ネットワーク１０４を介してサービス提供サーバ１０３のサーバ間通信部１３１と接続し、サービス提供サーバ１０３から定期的にアドレス情報（サービス提供サーバのアドレス情報及びアクセス用ＴＣＰポート番号）の通知を受け、通知されたアドレス情報を情報記憶部１１２に出力する。また、情報記憶部１１２に記憶されている共通鍵Ｋｃをサービス提供サーバ１０３に通知する。
【００３５】
情報記憶部１１２は、サーバ間通信部１１１から出力されたアドレス情報を記憶すると共に、共通鍵Ｋｃを記憶している。
【００３６】
ＨＴＴＰサーバ機能部１１３は、通信ネットワーク１０４を介してクライアント１０２のＨＴＴＰクライアント機能部１２１と接続し、クライアント１０２からのアクセスを受ける。ＨＴＴＰサーバ機能部１１３は、クライアント１０２からのアクセスを受けるとクライアント認証を行い、認証が正しければ、クライアント１０２からサービス提供サーバ１０３への接続要求を受ける。また、後述するＯＴＵ生成部１１４で生成されたＯＴＵをＨＴＭＬページ上の情報として、クライアント１０２側のＨＴＴＰクライアント機能部１２１で直接認識できるようにクライアント１０２に通知する。
【００３７】
ＯＴＵ生成部１１４は、クライアント１０２から受けた接続要求に従って、情報記憶部１１２に記憶されたサービス提供サーバのアドレス情報と、サービスメニュー等のサービス制約条件とからサービス提供サーバ接続用のＵＲＬを生成し、生成したＵＲＬをハッシュ演算部１１５に出力する。また、後述するハッシュ演算部１１５で生成された認証コードをサービス提供サーバ接続用のＵＲＬに付加することによりＯＴＵを生成し、生成したＯＴＵをＨＴＴＰサーバ機能部１１３に通知する。
【００３８】
ハッシュ演算部１１５は、ＯＴＵ生成部１１４から出力されたＵＲＬに対して情報記憶部１１２に記憶された共通鍵Ｋｃを用いてハッシュ演算を行い、認証コードを生成する。生成された認証コードはＯＴＵ生成部１１４に出力される。なお、ハッシュ演算部１１５は認証コード生成手段として機能する。
【００３９】
次に、クライアント１０２について説明する。図２において、ＨＴＴＰクライアント機能部１２１は、通信ネットワーク１０４を介して仲介サーバ１０１のＨＴＴＰサーバ機能部１１３及びサービス提供サーバ１０３のＨＴＴＰサーバ機能部１３３に接続し、仲介サーバ１０１にアクセスすると、クライアント１０２は仲介サーバ１０１からクライアント認証を受ける。クライアント認証は、ＨＴＭＬメニューに従ってユーザＩＤ及びパスワードを入力することにより行われる。そして、クライアント１０２は接続先のサービス提供サーバ１０３及びサービスメニュー等の選択を行う。また、仲介サーバ１０１から通知されたサービス提供サーバ接続用のＯＴＵを情報記憶部１２２に記憶させる。さらに、情報

記憶部１２２に記憶したＯＴＵを用いて、サービス提供サーバ１０３にアクセスする。

【００４０】

次に、サービス提供サーバ１０３について説明する。図２において、サーバ間通信部１３１は、定期的にアドレス情報を仲介サーバ１０１に通知する一方、仲介サーバ１０１から共通鍵Ｋｃを取得し、取得した共通鍵Ｋｃを情報記憶部１３２に記憶させる。

【００４１】

サービス提供サーバ１０３のＨＴＴＰサーバ機能部１３３は、クライアント１０２からのアクセスに応じて、アクセスに用いられたＯＴＵをＯＴＵ検証部１３４に通知する。

【００４２】

ＯＴＵ検証部１３４は、ＨＴＴＰサーバ機能部１３３から通知されたＯＴＵの認証コード以外の部分をハッシュ演算部１３５に出力し、後述するハッシュ演算部１３５から通知された結果（ハッシュ値）がＯＴＵに付加されている認証コードと一致するか否かを確認する。

【００４３】

ハッシュ演算部１３５は、ＯＴＵの認証コード以外の部分に対して、情報記憶部１３２に記憶された共通鍵Ｋｃを用いてハッシュ演算を行い、その結果（ハッシュ値）をＯＴＵ検証部１３４に出力する。なお、ＯＴＵ検証部１３４及びハッシュ演算部１３５はOne Time URL検証手段として機能する。

【００４４】

ＯＴＵ検証部１３４において、ハッシュ値がＯＴＵに付加されている認証コードと一致しないと確認された場合、ＨＴＴＰサーバ機能部１３３はクライアントからのＨＴＴＰアクセスを拒否する。一方、ハッシュ値がＯＴＵに付加されている認証コードと一致すると確認された場合、ＨＴＴＰサーバ機能部１３３はクライアントからＨＴＴＰアクセスを許可し、情報記憶部１３２に記憶されたＨＴＴＰサーバ提供コンテンツをクライアントに提供する。なお、ＨＴＴＰサーバ機能部１３３はサービス提供手段として機能する。

【００４５】

次に、上記構成を有する仲介サーバ１０１、クライアント１０２及びサービス提供サーバ１０３の動作について図３を用いて説明する。図３において、ステップ（以下、「ＳＴ」と省略する）１４１では、サービス提供サーバ１０３が仲介サーバ１０１に定期的（例えば、５秒間隔）に通信パケットを送出（キープアライブ通信）することにより、サービス提供サーバ１０３が稼動状態であることと、サービス提供サーバ１０３の接続方法（ＩＰアドレスやアクセスポート番号等）を通知する。

【００４６】

ＳＴ１４２では、仲介サーバ１０１がサービス開始当初の所定のタイミングでサービス提供サーバ１０３にＯＴＵの認証コード生成及び認証コード検証に用いる共通鍵Ｋｃを通知する。これにより、仲介サーバ１０１とサービス提供サーバ１０３は同一の共通鍵Ｋｃを有することになる。なお、共通鍵Ｋｃの通知はサーバ間に別途設けるセキュアな通信路で行うことにより、共通鍵Ｋｃの漏洩を防止することが望ましい。

【００４７】

ＳＴ１４３では、クライアント１０２が仲介サーバ１０１の固定アドレスにアクセスし、サービス提供サーバ１０３への接続要求を通知し、ＳＴ１４４では、仲介サーバ１０１がサービスメニュー又はユーザの要望に応じたアクセス制限情報をＵＲＬパラメータとして図５に示すＡ１部分のＵＲＬに付加し、共通鍵Ｋｃを用いて認証コードを生成し、認証コードを図５に示すＡ３部分に付加する。

【００４８】

ＳＴ１４５では、仲介サーバ１０１がパスワード等の所望のクライアント認証を行った後、ＯＴＵにてサービス提供サーバ１０３への接続方法をクライアント１０２に通知する。このとき、ＯＴＵの通知方法は、予め仲介サーバ１０１が把握するクライアント１０２のメールアドレス宛に電子メールで通知してもよいし、ＨＴＴＰプロトコル上でＨＴＭＬページ上の情報として通知してもよい。

【００４９】
ＳＴ１４６では、仲介サーバ１０１から通知されたＯＴＵをクライアント１０２が辿ることにより、サービス提供サーバ１０３に接続する。通常、この接続はウェブブラウザ又はメーラ上でＵＲＬリンク部分をクリックするだけの簡便なユーザインタフェースにより実現される。
【００５０】
ＳＴ１４７では、サービス提供サーバ１０３がクライアント１０２から提示されたＯＴＵの認証コード部分を共通鍵Ｋｃで検証することにより、ＯＴＵの正当性を確認し、ＳＴ１４８では、クライアント１０２が所望するサービス提供サーバ１０３へのＨＴＴＰアクセスを実現する。
【００５１】
このように実施の形態１によれば、サービス提供サーバとは異なる別の仲介サーバを設け、仲介サーバがサービス提供サーバのアドレス情報を定期的に取得し、サービス提供サーバのアドレス情報からＯＴＵ用の認証コードを生成する際に用いる暗号鍵をサービス提供サーバが共有し、サービス提供サーバは、共有する暗号鍵を用いて認証コードの正当性を確認することにより、ＯＴＵの発行者とＯＴＵの受付者が物理的に異なる場合でも、ＯＴＵの偽造又は改竄による不正アクセスを防止することができる。
【００５２】
なお、本実施の形態では、ＯＴＵの発行方法をＨＴＭＬ上で直接通知することにより行っているが、本発明はこれに限らず、電子メールによる通知、携帯電話のショートメッセージサービスによる通知、ＰＣ端末のインスタントメッセージングによる通知、さらには、口頭伝達等のオフラインによる通知でもよい。
【００５３】
また、本実施の形態では、ＨＴＴＰプロトコルによるサーバアクセスを前提にしているが、本発明はこれに限らず、ＵＲＬによるロケーションの指定はＨＴＴＰＳプロトコル又はＦＴＰプロトコルを用いてもよい。
【００５４】
また、本実施の形態におけるハッシュ演算関数は、不可逆な一方向性関数であればその種別は問わず、また、ＵＲＬのハッシュ演算対象範囲も任意に設定してよい。ただし、ＵＲＬのハッシュ演算対象範囲はサービス提供サーバと仲介サーバとで一致させなければならない。
【００５５】
また、本実施の形態では、クライアントが仲介サーバに接続する際に、ユーザＩＤ及びパスワードによるライアント認証を行っているが、本発明はこれに限らず、クライアント認証を行うか否かを任意に選択可能であり、クライアント認証を行う場合にはその認証方法の種別は問わない。
【００５６】
（実施の形態２）
図４は、本発明の実施の形態２に係るクライアント、仲介サーバ及びサービス提供サーバの内部構成を示すブロック図である。ただし、図４が図２と共通する部分には図２と同一の符号を付し、その詳しい説明は省略する。
【００５７】
まず、仲介サーバ１０１について説明する。図４において、鍵対生成部１５１は、予め公開鍵暗号方式に基づく鍵対を生成し、一方を秘密鍵Ｋｓ、他方を公開鍵Ｋｐとして情報記憶部１５２に記憶させる。
【００５８】
サーバ間通信部１５３は、情報記憶部１５２に記憶されている共通鍵Ｋｃ及び公開鍵Ｋｐを通信ネットワーク１０４を介してサービス提供サーバ１０３のサーバ間通信部１６１に通知する。
【００５９】

暗号化処理部１５４は、ハッシュ演算部１１５で共通鍵Ｋｃを用いて得られたハッシュ演算結果に対し、情報記憶部１５２に記憶された秘密鍵Ｋｓを用いて暗号化処理を行い、暗号化処理結果を認証コードとしてＯＴＵ生成部１５５に出力する。

【００６０】

ＯＴＵ生成部１５５は、暗号化処理部１５４から出力された認証コードをサービス提供サーバ接続用のＵＲＬに付加することによりＯＴＵを生成し、生成したＯＴＵをＨＴＴＰサーバ機能部１１３に通知する。なお、ハッシュ演算部１１５及び暗号化処理部１５４は認証コード生成手段として機能する。

【００６１】

次に、サービス提供サーバ１０３について説明する。図４において、サーバ間通信部１６１は、仲介サーバ１０１から共通鍵Ｋｃ及び公開鍵Ｋｐを取得し、取得した共通鍵Ｋｃ及び公開鍵Ｋｐを情報記憶部１６２に記憶させる。ここで、サービス提供サーバ１０３は、公開鍵暗号方式に基づく公開鍵Ｋｐを仲介サーバ１０１から取得するため、実施の形態１で説明したようなサーバ間のセキュアな通信路を設ける必要がない。

【００６２】

復号化処理部１６３は、後述するＯＴＵ検証部１６４からＯＴＵに記載された認証コードを取得し、取得した認証コードに対して、情報記憶部１６２に記憶された公開鍵Ｋｐを用いて復号化処理を行い、復号化処理結果をＯＴＵ検証部１６４に通知する。

【００６３】

ＯＴＵ検証部１６４は、ＨＴＴＰサーバ機能部１３３から通知されたＯＴＵの認証コード以外の部分ハッシュ演算部１３５に出力し、ハッシュ演算部１３５において情報記憶部１６２に記憶された共通鍵Ｋｃを用いて行われたハッシュ演算結果（ハッシュ値）を取得し、演算結果（ハッシュ値）が復号化処理部１６３から通知された認証コードの復号処理結果と一致するか否かを確認する。

【００６４】

ハッシュ値が認証コードの復号処理結果と一致しない場合、ＨＴＴＰサーバ機能部１３３はクライアント１０２からのＨＴＴＰアクセスを拒否する。これは、秘密鍵Ｋｓを知り得る仲介サーバ１０１でなければ正しい認証コードを生成することができず、サービス提供サーバ１０３においてＯＴＵの正当性が確認されない場合、第三者によってＯＴＵが改竄されたか、仲介サーバ１０１に関する詐称（なりすまし）攻撃があったとみなすことができるためである。

【００６５】

一方、ハッシュ値がＯＴＵに付加されている認証コードと一致する場合、ＨＴＴＰサーバ機能部１３３はクライアント１０２からＨＴＴＰアクセスを許可し、情報記憶部１６２に記憶されたＨＴＴＰサーバ提供コンテンツをクライアントに提供する。

【００６６】

このように実施の形態２によれば、サービス提供サーバとは異なる別の仲介サーバを設け、仲介サーバがサービス提供サーバから定期的に取得したアドレス情報に対して共通鍵でハッシュ演算を行い、公開鍵暗号方式に利用可能な鍵対の一方である秘密鍵を用いてハッシュ演算結果を暗号化処理してＯＴＵ用の認証コードを生成し、サービス提供サーバは、仲介サーバと共有する共通鍵を用いてＯＴＵの認証コード以外の部分に対してハッシュ演算を行うと共に、仲介サーバが暗号化処理に用いた秘密鍵と鍵対をなす公開鍵を用いて認証コードを復号化処理し、ハッシュ演算結果と復号化処理結果とを比較して認証コードの正当性を確認することにより、ＯＴＵの発行者とＯＴＵの受付者が物理的に異なる場合でも、ＯＴＵの偽造又は改竄による不正アクセスを防止することができる。

【００６７】

なお、本実施の形態では、公開鍵の配信方法として、仲介サーバからサービス提供サーバへ直接通知する方法を採用しているが、本発明はこれに限らず、一般的な公開鍵の流布機構としてＰＫＩプロトコルで定義されている第三者機関によって間接的に配信する方法でもよく、要は、公開鍵が仲介サーバからサービス提供サーバに配信されればどんな方法

でもよい。

【００６８】

また、本実施の形態における公開鍵暗号方式は、非対称暗号鍵対を用いる暗号方式であれば、その種別は問わない。

【産業上の利用可能性】

【００６９】

本発明にかかるＵＲＬ認証システム及びＵＲＬ認証方法は、ＯＴＵの発行者とＯＴＵの受付者が物理的に異なる場合でも、ＯＴＵの偽造又は改竄による不正アクセスを防止するという効果を有し、例えば、宅内ローカルネットワーク内の宅内機器及び携帯電話等の携帯端末に適用することができる。

【図面の簡単な説明】

【００７０】

【図１】本発明の実施の形態１に係るＵＲＬ認証システムの構成を示すブロック図

【図２】図１に示す仲介サーバ、クライアント及びサービス提供サーバの内部構成を示すブロック図

【図３】図１に示す仲介サーバ、クライアント、及びサービス提供サーバの動作を示すシーケンス図

【図４】本発明の実施の形態２に係る仲介サーバ、クライアント及びサービス提供サーバの内部構成を示すブロック図

【図５】ＯＴＵの一例を示す図

【図６】ＯＴＵを用いたサーバ、クライアント間の接続処理の説明に供する図

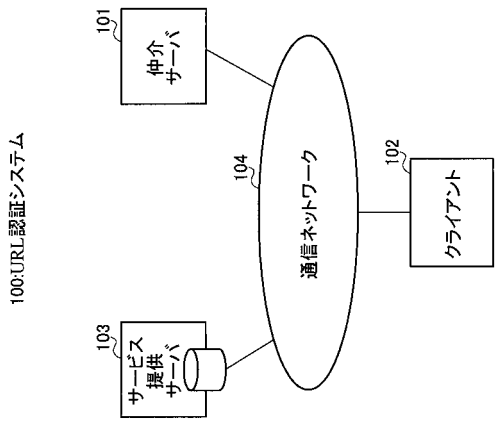
【図７】仲介サーバを備えた通信システムの構成を示すブロック図

【符号の説明】

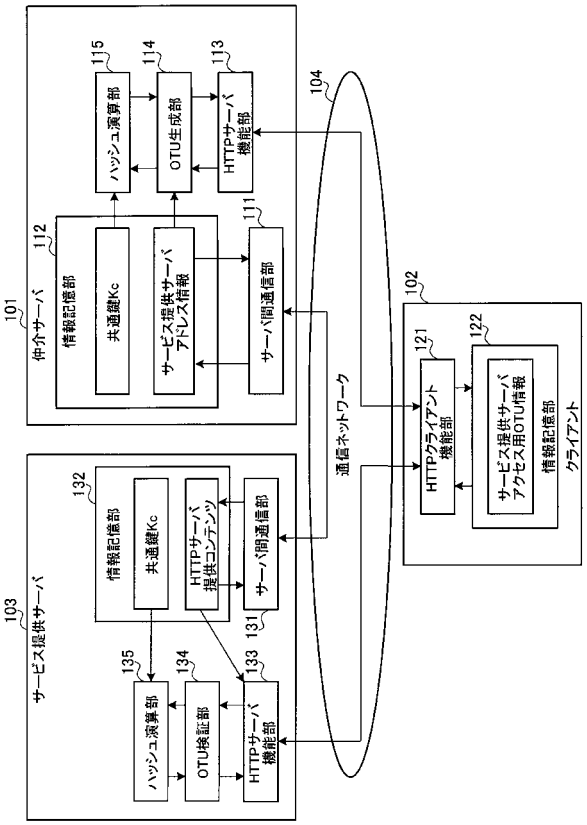
【００７１】

１０１　仲介サーバ
１０２　クライアント
１０３　サービス提供サーバ
１０４　通信ネットワーク
１１１、１３１、１５３、１６１　サーバ間通信部
１１２、１２２、１３２、１５２、１６２　情報記憶部
１１３、１３３　ＨＴＴＰサーバ機能部
１１４、１５５　ＯＴＵ生成部
１１５、１３５　ハッシュ演算部
１２１　ＨＴＴＰクライアント機能部
１３４、１６４　ＯＴＵ検証部
１５１　鍵対生成部
１５４　暗号化処理部
１６３　復号化処理部

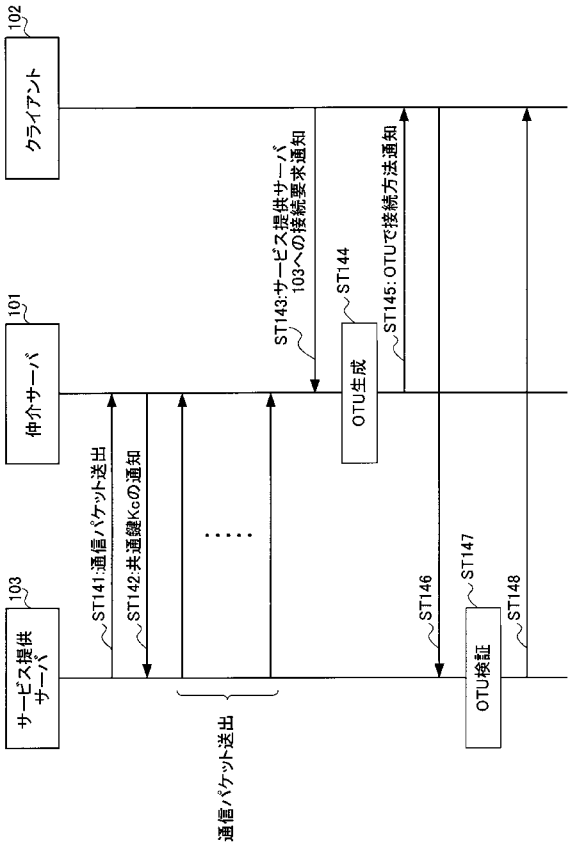
【図１】


100:URL認証システム
101
仲介サーバ
104
通信ネットワーク
102
クライアント
103
サービス提供サーバ

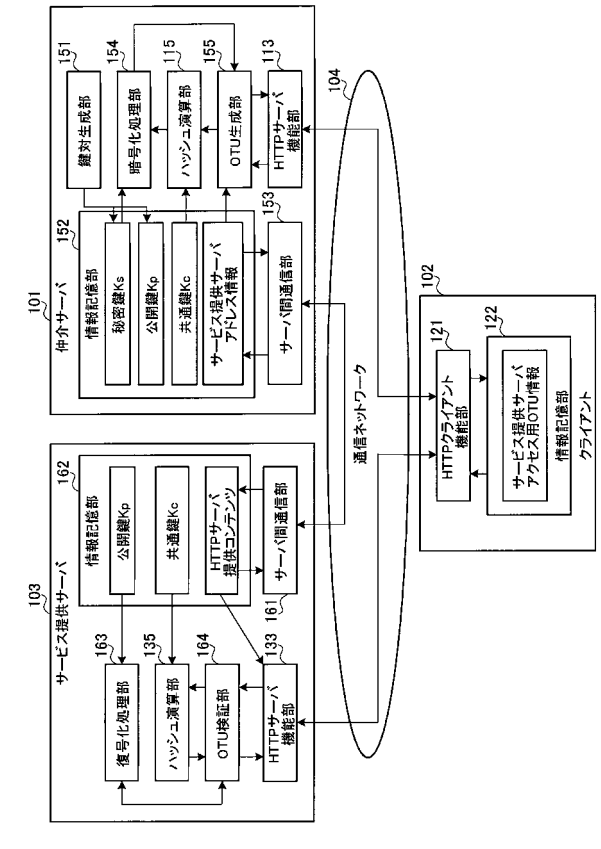
【図２】


101
仲介サーバ
112
情報記憶部
共通鍵Kc
サービス提供サーバアドレス情報
111
サーバ間通信部
115
ハッシュ演算部
114
OTU生成部
113
HTTPサーバ機能部
104
通信ネットワーク
102
121
HTTPクライアント機能部
122
サービス提供サーバアクセス用OTU情報
情報記憶部
クライアント
103
サービス提供サーバ
132
情報記憶部
共通鍵Kc
HTTPサーバ提供コンテンツ
131
サーバ間通信部
135
ハッシュ演算部
134
OTU検証部
133
HTTPサーバ機能部

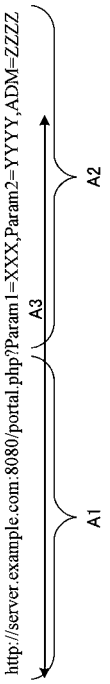
【図３】


102
クライアント
101
仲介サーバ
103
サービス提供サーバ
ST141:通信パケット送出
ST142:共通鍵Kcの通知
ST143:サービス提供サーバ103への接続要求通知
ST144
OTU生成
ST145:OTUで接続方法通知
ST146
ST147
OTU検証
ST148
通信パケット送出

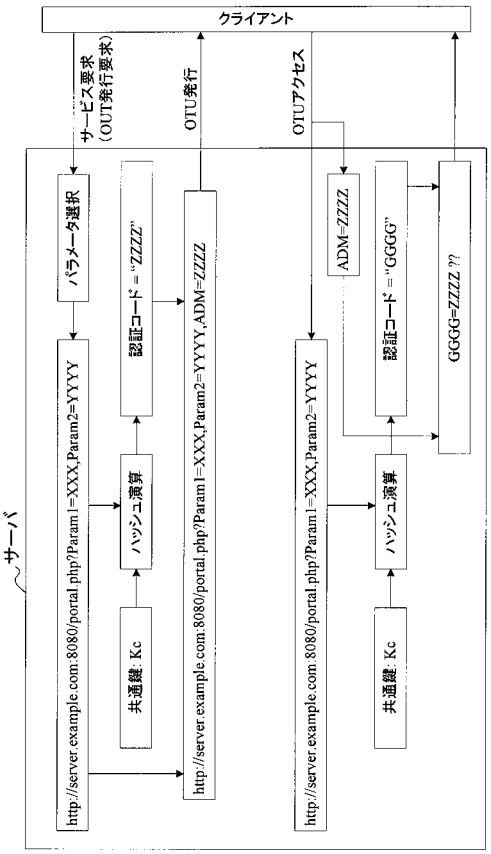
【図４】


101
仲介サーバ
151
鍵対生成部
154
暗号化処理部
115
ハッシュ演算部
155
OTU生成部
113
HTTPサーバ機能部
152
情報記憶部
秘密鍵Ks
公開鍵Kp
共通鍵Kc
サービス提供サーバアドレス情報
153
サーバ間通信部
104
通信ネットワーク
102
121
HTTPクライアント機能部
122
サービス提供サーバアクセス用OTU情報
情報記憶部
クライアント
103
サービス提供サーバ
162
情報記憶部
公開鍵Kp
共通鍵Kc
HTTPサーバ提供コンテンツ
161
サーバ間通信部
163
復号化処理部
135
ハッシュ演算部
164
OTU検証部
133
HTTPサーバ機能部

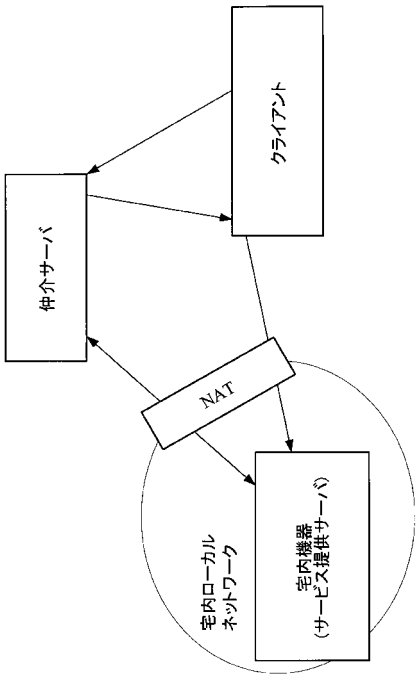
【図５】


http://server.example.com:8080/portal.php?Param1=XXX,Param2=YYYY,ADM=ZZZZ
A1
A3
A2

【図６】


クライアント
サーバ
サービス要求
（OUT発行要求）
パラメータ選択
http://server.example.com:8080/portal.php?Param1=XXX,Param2=YYYY
共通鍵：Kc
ハッシュ演算
認証コード＝"ZZZZ"
OTU発行
http://server.example.com:8080/portal.php?Param1=XXX,Param2=YYYY,ADM=ZZZZ
OTUアクセス
http://server.example.com:8080/portal.php?Param1=XXX,Param2=YYYY
共通鍵：Kc
ハッシュ演算
ADM=ZZZZ
認証コード＝"GGGG"
GGGG=ZZZZ ??

【図７】


仲介サーバ
クライアント
NAT
宅内ローカル
ネットワーク
宅内機器
（サービス提供サーバ）

フロントページの続き

(72)発明者　金子　友晴
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内
(72)発明者　岩間　智大
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内

Ｆターム(参考) 5J104 AA07　KA01　KA06　PA07　PA08