(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4558387号
(P4558387)
(45)発行日　平成22年10月6日(2010.10.6)　(24)登録日　平成22年7月30日(2010.7.30)

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

請求項の数 4　(全 10 頁)

(21)出願番号　特願2004-179448(P2004-179448)
(22)出願日　平成16年6月17日(2004.6.17)
(65)公開番号　特開2006-4149(P2006-4149A)
(43)公開日　平成18年1月5日(2006.1.5)
審査請求日　平成19年3月8日(2007.3.8)

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100106909
弁理士　棚井　澄雄
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(72)発明者　清本　晋作
埼玉県上福岡市大原２丁目１番１５号　株式会社ＫＤＤＩ研究所内
(72)発明者　田中　俊昭
埼玉県上福岡市大原２丁目１番１５号　株式会社ＫＤＤＩ研究所内
最終頁に続く

(54)【発明の名称】利用者認証システムおよび方法

(57)【特許請求の範囲】
【請求項１】
利用者端末と前記利用者端末から通信接続される認証装置とを備えた利用者認証システムであって、
前記認証装置は、
前記利用者端末からの要求に基づき、利用者固有のマスタテンポラリ識別情報を生成する手段と、
前記マスタテンポラリ識別情報から一方向性変換関数を１回又は複数回繰り返し使用してサブテンポラリ識別情報を作成する手段と、
利用者ごとに１つの前記マスタテンポラリ識別情報と前記一方向性変換関数の最大使用回数とを管理するデータベース手段と、
被認証者の使い捨てテンポラリ情報の検証要求に基づき、当該使い捨てテンポラリ情報を検証する検証手段とを有し、
前記利用者端末は、
前記マスタテンポラリ識別情報から前記一方向性変換関数を１回又は複数回繰り返し使用してサブテンポラリ識別情報を作成する手段と、
前記作成したサブテンポラリ識別情報および当該作成時における前記一方向性変換関数の使用回数を含む使い捨てテンポラリ情報を作成する手段とを有し、
前記検証手段は、
前記検証要求された被認証者に対応する利用者の管理データを前記データベース手段か

ら検索する手段と、
前記検索した管理データ中のマスタテンポラリ識別情報と被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数とから、サブテンポラリ識別情報を再現し、被認証者の使い捨てテンポラリ情報を検証する手段と、
被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数が、前記検索した管理データ中の最大使用回数以下であることを確認する手段と、を有する
ことを特徴とする利用者認証システム。
【請求項２】
前記利用者端末は、前記サブテンポラリ識別情報作成時における前記一方向性変換関数の使用回数を保存する記憶手段を備え、同じ前記マスタテンポラリ識別情報から前記サブテンポラリ識別情報を再度作成する場合、前回の一方向性変換関数の使用回数よりも少ない使用回数とし、
前記認証装置のデータベース手段は、被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数を、該被認証者に係る最大使用回数の更新データとして格納する
ことを特徴とする請求項１に記載の利用者認証システム。
【請求項３】
利用者端末と前記利用者端末から通信接続される認証装置とを備えた利用者認証システムにおける利用者認証方法であって、
前記認証装置が、
前記利用者端末からの要求に基づき、利用者固有のマスタテンポラリ識別情報を生成する過程と、
利用者ごとに１つの前記マスタテンポラリ識別情報と前記一方向性変換関数の最大使用回数とをデータベース管理する過程と、
前記利用者端末が、
前記マスタテンポラリ識別情報から前記一方向性変換関数を１回又は複数回繰り返し使用してサブテンポラリ識別情報を作成する過程と、
前記作成したサブテンポラリ識別情報および当該作成時における前記一方向性変換関数の使用回数を含む使い捨てテンポラリ情報を作成する過程と、
前記認証装置が、
被認証者の使い捨てテンポラリ情報の検証要求に基づき、検証要求された被認証者に対応する利用者の管理データをデータベース検索する過程と、
前記検索した管理データ中のマスタテンポラリ識別情報と被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数とから、サブテンポラリ識別情報を再現し、被認証者の使い捨てテンポラリ情報を検証する過程と、
被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数が、前記検索した管理データ中の最大使用回数以下であることを確認する過程と、
を含むことを特徴とする利用者認証方法。
【請求項４】
前記利用者端末が、前記サブテンポラリ識別情報作成時における前記一方向性変換関数の使用回数を記憶手段に保存し、同じ前記マスタテンポラリ識別情報から前記サブテンポラリ識別情報を再度作成する場合、前回の一方向性変換関数の使用回数よりも少ない使用回数とし、
前記認証装置が、被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数を、該被認証者に係る最大使用回数の更新データとしてデータベースに格納する
ことを特徴とする請求項３に記載の利用者認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、利用者認証システムおよび方法に関する。
【背景技術】

【０００２】
近年、携帯電話端末からインターネット経由で各種サービス提供者のサーバにアクセス可能であり、携帯電話端末の利用者は様々なサービスを享受することができるようになっている。それら複数のサービスを利用する際には、サービス利用者に固有のＩＤ（識別情報）、例えば携帯電話番号が使用されている。
【０００３】
上述した利用者固有のＩＤを用いたサービスの一例として、異なる通信方式の複数の携帯電話端末を利用する利用者に対して一つのＩＤを発行し、このＩＤを各携帯電話端末に登録し、各携帯電話端末の利用料金を該共通のＩＤに基づき一元化し集計し、該当利用者に課金するシステムが知られている（例えば、特許文献１参照）。
【特許文献１】特許第３３７９５１７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかし、上述した従来の技術では、利用者に固有のＩＤを用いて各種サービスが提供されるので、第三者によってＩＤに基づき、特定利用者がどのようなサービスを利用しているのかを追跡されるおそれがある。
【０００５】
このような理由から、使い捨て可能なテンポラリなＩＤを用いることができれば、ＩＤから利用者を特定することはほぼ不可能となるので、テンポラリＩＤによる利用者認証システムの実現が要望されている。しかしながら、テンポラリＩＤによって利用者を識別するために、発行済みのテンポラリＩＤを利用者毎に全て記録管理すると、管理データ量が増大する。
【０００６】
本発明は、このような事情を考慮してなされたもので、その目的は、使い捨て可能なＩＤを使用して利用者認証を行うとともに管理データの削減を図ることができる利用者認証システムおよび方法を提供することにある。
【課題を解決するための手段】
【０００７】
上記の課題を解決するために、本発明に係る利用者認証システムは、利用者端末と前記利用者端末から通信接続される認証装置とを備えた利用者認証システムであって、前記認証装置は、前記利用者端末からの要求に基づき、利用者固有のマスタテンポラリ識別情報を生成する手段と、前記マスタテンポラリ識別情報から一方向性変換関数を１回又は複数回繰り返し使用してサブテンポラリ識別情報を作成する手段と、利用者ごとに１つの前記マスタテンポラリ識別情報と前記一方向性変換関数の最大使用回数とを管理するデータベース手段と、被認証者の使い捨てテンポラリ情報の検証要求に基づき、当該使い捨てテンポラリ情報を検証する検証手段とを有し、前記利用者端末は、前記マスタテンポラリ識別情報から前記一方向性変換関数を１回又は複数回繰り返し使用してサブテンポラリ識別情報を作成する手段と、前記作成したサブテンポラリ識別情報および当該作成時における前記一方向性変換関数の使用回数を含む使い捨てテンポラリ情報を作成する手段とを有し、前記検証手段は、前記検証要求された被認証者に対応する利用者の管理データを前記データベース手段から検索する手段と、前記検索した管理データ中のマスタテンポラリ識別情報と被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数とから、サブテンポラリ識別情報を再現し、被認証者の使い捨てテンポラリ情報を検証する手段と、被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数が、前記検索した管理データ中の最大使用回数以下であることを確認する手段と、を有することを特徴としている。
【０００８】
本発明に係る利用者認証システムにおいては、前記利用者端末は、前記サブテンポラリ識別情報作成時における前記一方向性変換関数の使用回数を保存する記憶手段を備え、同

じ前記マスタテンポラリ識別情報から前記サブテンポラリ識別情報を再度作成する場合、前回の一方向性変換関数の使用回数よりも少ない使用回数とし、前記認証装置のデータベース手段は、被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数を、該被認証者に係る最大使用回数の更新データとして格納することを特徴とする。

【０００９】

本発明に係る利用者認証システムにおいては、前記認証装置は、利用者ごとに前記一方向性変換関数の使用回数をデータベース管理し、前記一方向性変換関数の使用回数により、前記マスタテンポラリ識別情報の使用回数を制限することを特徴とする。

【００１０】

本発明に係る利用者認証方法は、利用者端末と前記利用者端末から通信接続される認証装置とを備えた利用者認証システムにおける利用者認証方法であって、前記認証装置が、前記利用者端末からの要求に基づき、利用者固有のマスタテンポラリ識別情報を生成する過程と、利用者ごとに１つの前記マスタテンポラリ識別情報と前記一方向性変換関数の最大使用回数とをデータベース管理する過程と、前記利用者端末が、前記マスタテンポラリ識別情報から前記一方向性変換関数を１回又は複数回繰り返し使用してサブテンポラリ識別情報を作成する過程と、前記作成したサブテンポラリ識別情報および当該作成時における前記一方向性変換関数の使用回数を含む使い捨てテンポラリ情報を作成する過程と、前記認証装置が、被認証者の使い捨てテンポラリ情報の検証要求に基づき、検証要求された被認証者に対応する利用者の管理データをデータベース検索する過程と、前記検索した管理データ中のマスタテンポラリ識別情報と被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数とから、サブテンポラリ識別情報を再現し、被認証者の使い捨てテンポラリ情報を検証する過程と、被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数が、前記検索した管理データ中の最大使用回数以下であることを確認する過程と、を含むことを特徴としている。

【００１１】

本発明に係る利用者認証方法においては、前記利用者端末が、前記サブテンポラリ識別情報作成時における前記一方向性変換関数の使用回数を記憶手段に保存し、同じ前記マスタテンポラリ識別情報から前記サブテンポラリ識別情報を再度作成する場合、前回の一方向性変換関数の使用回数よりも少ない使用回数とし、前記認証装置が、被認証者の使い捨てテンポラリ情報中の一方向性変換関数の使用回数を、該被認証者に係る最大使用回数の更新データとしてデータベースに格納することを特徴とする。

【００１２】

本発明に係る利用者認証方法においては、前記認証装置が、利用者ごとに前記一方向性変換関数の使用回数をデータベース管理する過程と、前記一方向性変換関数の使用回数により、前記マスタテンポラリ識別情報の使用回数を制限する過程とをさらに含むことを特徴とする。

【発明の効果】

【００１３】

本発明によれば、使い捨て可能なマスタテンポラリ識別情報を使用して利用者認証を行うことができる。さらに、マスタテンポラリ識別情報から一方向性変換関数を１回又は複数回繰り返し使用してサブテンポラリ識別情報を作成することにより、マスタテンポラリ識別情報と一方向性変換関数の使用回数のみからサブテンポラリＩＤを一意に特定することができる。これにより、一利用者に対して一つのマスタテンポラリ識別情報および一方向性変換関数の使用回数のみを管理すればよいので、管理データの削減を図ることができる。

【発明を実施するための最良の形態】

【００１４】

以下、図面を参照し、本発明の一実施形態について説明する。

図１は、本発明の一実施形態に係る利用者認証システムの構成を示すブロック図である。図１において、携帯電話端末１は携帯電話通信網２の加入端末である。携帯電話端末１

は、無線通信により携帯電話通信網２を介して音声通話及びデータ通信を行う機能を有する。携帯電話通信網２はインターネット５に接続している。携帯電話端末１は、携帯電話通信網２を介してインターネット５に接続し、インターネット５上の各種のサービス提供者サーバ６にアクセスすることができる。

【００１５】

通信事業者サーバ３は、携帯電話通信網２の事業者のサーバであり、携帯電話通信網２およびインターネット５に通信接続されている。通信事業者サーバ３は、テンポラリＩＤを用いた利用者認証を行うための機能を有する。携帯電話端末１は、携帯電話通信網２を介して通信事業者サーバ３にアクセスすることができる。ＩＤ管理データベース４は、携帯電話通信網２の加入者のＩＤ管理データを蓄積しており、携帯電話通信網２の事業者によって管理されている。通信事業者サーバ３は、ＩＤ管理データベース４に通信によりアクセスし、ＩＤ管理データの検索及び取得を行うことができる。

【００１６】

次に、図２を参照して、図１の利用者認証システムに係る動作を説明する。

図２は、図１に示す利用者認証システムにおける利用者認証処理の流れを示すシーケンスチャートである。

初めに、利用者が、認証情報（パスワード、指紋等）を携帯電話端末１に入力して当該携帯電話端末１を使用可能な状態にする。そして、携帯電話端末１を操作してマスタテンポラリＩＤ発行のためのソフトウェアを起動する。これにより、携帯電話端末１は、通信事業者サーバ３にアクセスし、通信事業者サーバ３との間で端末認証処理を行う（ステップＳ１）。この認証の結果、アクセスが許可されると、携帯電話端末１は、通信事業者サーバ３にマスタテンポラリＩＤの要求を行う（ステップＳ２）。

【００１７】

次いで、通信事業者サーバ３は、携帯電話端末１からのマスタテンポラリＩＤ要求に基づき、マスタテンポラリＩＤ（ｍＴ－ＩＤ）を生成する（ステップＳ３）。マスタテンポラリＩＤは、乱数等を用いて生成し、他の加入者間で重複しないようにする。また、通信事業者サーバ３は、マスタテンポラリＩＤの最大使用回数および有効期限を設定する。そして、マスタテンポラリＩＤ、最大使用回数および有効期限情報を当該加入者のＩＤ管理データに含めてＩＤ管理データベース４に格納する。ここで、最大使用回数はカウンタ値Ｖの初期値として格納する。また、ＩＤ管理データは当該加入者のＩＤ（Ｕ－ＩＤ）を含んでいる。

【００１８】

次いで、通信事業者サーバ３は、マスタテンポラリＩＤ（ｍＴ－ＩＤ）、最大使用回数および有効期限情報を携帯電話端末１へ送信する（ステップＳ４）。この送信データは暗号化等により安全性を確保する。次いで、携帯電話端末１は、通信事業者サーバ３から受信した各情報をメモリに保存する（ステップＳ５）。上記マスタテンポラリＩＤ（ｍＴ－ＩＤ）は、利用者からの要求に応じて変更可能であり、使い捨て可能なＩＤである。

【００１９】

次いで、利用者は、所望のサービスを利用する際、携帯電話端末１を操作して該当するサービス提供者サーバ６にアクセスし、サービス提供の要求を行う（ステップＳ６）。なお、必要であれば、サービス提供者サーバ６の認証を行い、安全な通信路を確保する。

【００２０】

次いで、サービス提供者サーバ６は、携帯電話端末１からのサービス提供要求に応じて、サービス提供の条件（課金情報等）およびサービス提供者の識別子（サービス提供者ＩＤ、ＵＲＬ、公開鍵証明書等）を返信する（ステップＳ７）。次いで、携帯電話端末１は、使い捨て用のテンポラリ情報（以下、使い捨てテンポラリ情報と称する）を作成するためのソフトウェアを起動し、使い捨てテンポラリ情報を作成する処理を行う（ステップＳ８）。

【００２１】

ここで、図３を参照して、ステップＳ８の使い捨てテンポラリ情報作成処理を説明する

。図３は、使い捨てテンポラリ情報１００のデータ構造および使い捨てテンポラリ情報１００の作成手順を説明するための説明図である。

【００２２】

先ず、携帯電話端末１内に保存されているマスタテンポラリＩＤ（ｍＴ－ＩＤ）から一方向性の変換関数を使用して、サブテンポラリＩＤ（ＮＴ－ＩＤ）を作成する。本実施例では、一方向性の変換関数の一例として一方向性ハッシュ関数を使用する。具体的には、マスタテンポラリＩＤ（ｍＴ－ＩＤ）を一方向性ハッシュ関数に入力して変換値（１Ｔ－ＩＤ）を得る。さらに、この変換値（１Ｔ－ＩＤ）を再度一方向性ハッシュ関数に入力して変換値（２Ｔ－ＩＤ）を得る。この変換動作をＮ回繰り返して変換値（ＮＴ－ＩＤ）を求め、サブテンポラリＩＤ（ＮＴ－ＩＤ）とする（図３のステップＳ１０１）。

上記Ｎは、携帯電話端末１内に保存されている最大使用回数以下の任意の自然数である。但し、同じマスタテンポラリＩＤ（ｍＴ－ＩＤ）から再度サブテンポラリＩＤ（ＮＴ－ＩＤ）を作成する場合は、前回のＮの値よりも小さい値を使用する。このため、今回使用したＮの値は、携帯電話端末１のメモリに保存する。

【００２３】

次いで、サブテンポラリＩＤ（ＮＴ－ＩＤ）とＮを連結して連結データＴを作成する。次いで、マスタテンポラリＩＤ（ｍＴ－ＩＤ）と連結データＴを公開鍵Ｐｕ＿Ｃで暗号化して暗号データＥｎｃ（ｍＴ－ＩＤ｜Ｔ）を作成する。

上記公開鍵Ｐｕ＿Ｃは、携帯電話通信網２の事業者の公開鍵であり、携帯電話端末１のメモリに予め記録されている。

【００２４】

次いで、連結データＴと鍵Ｋをメッセージ認証子作成関数（ＨＭＡＣ等が利用可能）に入力し、テンポラリな鍵ＮＫを得る（図３のステップＳ１０２）。

上記鍵Ｋは、携帯電話端末１の利用者に固有の鍵であり、携帯電話端末１のメモリに予め記録されている。

【００２５】

次いで、暗号データＥｎｃ（ｍＴ－ＩＤ｜Ｔ）、サービス提供者サーバ６から受信したサービス提供条件（課金情報等）およびサービス提供者識別子を連結して連結データＩｎｆｏを作成する。次いで、連結データＩｎｆｏを鍵ＮＫで暗号化し、この暗号データをメッセージ認証子作成関数に入力し、メッセージ認証子Ｍａｃ（Ｉｎｆｏ）を作成する（図３のステップＳ１０３）。次いで、連結データＩｎｆｏとメッセージ認証子Ｍａｃ（Ｉｎｆｏ）を連結して使い捨てテンポラリ情報１００を作成する。

【００２６】

説明を図２に戻す。次いで、携帯電話端末１は、使い捨てテンポラリ情報をサービス提供者サーバ６に送信する（ステップＳ９）。次いで、サービス提供者サーバ６は、携帯電話端末１から受信した使い捨てテンポラリ情報を通信事業者サーバ３へ送信し、検証を要求する（ステップＳ１０）。なお、必要であれば、サービス提供者サーバ６と通信事業者サーバ３間で相互認証を行い、安全な通信路を確保する。

次いで、通信事業者サーバ３は、サービス提供者サーバ６からの要求に基づき、受信した使い捨てテンポラリ情報の検証処理を行う（ステップＳ１１）。

【００２７】

ここで、図３の使い捨てテンポラリ情報１００を例にしてステップＳ１１の使い捨てテンポラリ情報検証処理を説明する。

先ず、使い捨てテンポラリ情報１００から連結データＩｎｆｏを抽出し、連結データＩｎｆｏから暗号データＥｎｃ（ｍＴ－ＩＤ｜Ｔ）を抽出する。次いで、暗号データＥｎｃ（ｍＴ－ＩＤ｜Ｔ）を携帯電話通信網２の事業者の秘密鍵で復号して、マスタテンポラリＩＤ（ｍＴ－ＩＤ）と連結データＴを得る。

【００２８】

次いで、マスタテンポラリＩＤ（ｍＴ－ＩＤ）を検索キーとして、ＩＤ管理データベース４からＩＤ管理データを検索する。この検索結果、マスタテンポラリＩＤ（ｍＴ－ＩＤ

）を含むＩＤ管理データが発見されたならば、当該ＩＤ管理データ中から、Ｕ－ＩＤ、カウンタ値Ｖおよび有効期限情報などを取り出す。そして、この有効期限情報に基づき、当該マスタテンポラリＩＤ（ｍＴ－ＩＤ）の有効期限を確認する（第１の検証）。また、連結データＴからＮを抽出し、Ｎがカウンタ値Ｖ以下であることを確認する（第２の検証）。また、図３のステップＳ１０１と同様に、マスタテンポラリＩＤ（ｍＴ－ＩＤ）を一方向性ハッシュ関数によりＮ回繰り返して変換し、この変換値（サブテンポラリＩＤ（ＮＴ－ＩＤ）の再現データ）と連結データＴから抽出したサブテンポラリＩＤ（ＮＴ－ＩＤ）とが一致することを確認する（第３の検証）。

【００２９】

なお、上記第３の検証でサブテンポラリＩＤ（ＮＴ－ＩＤ）の再現に使用するマスタテンポラリＩＤ（ｍＴ－ＩＤ）は、ＩＤ管理データベース４から検索されたＩＤ管理データ中のマスタテンポラリＩＤ（ｍＴ－ＩＤ）とするのが原則である。但し、本実施例では使い捨てテンポラリ情報中のマスタテンポラリＩＤ（ｍＴ－ＩＤ）を検索キーとしてＩＤ管理データを検索しているので、使い捨てテンポラリ情報中のマスタテンポラリＩＤと検索結果のＩＤ管理データ中のマスタテンポラリＩＤとは同一であり、いずれのマスタテンポラリＩＤを使用してサブテンポラリＩＤを再現しても実質的に問題はない。

【００３０】

次いで、図３のステップＳ１０２と同様に、連結データＴと鍵Ｋから鍵ＮＫを作成する。この鍵Ｋは、携帯電話通信網２の事業者に固有の鍵ｍＫと、Ｕ－ＩＤから生成してもよく、或いはＩＤ管理データに予め含めておいてもよい。次いで、図３のステップＳ１０３と同様に、鍵ＮＫと連結データＩｎｆｏからメッセージ認証子を作成し、使い捨てテンポラリ情報１００から抽出したメッセージ認証子Ｍａｃ（Ｉｎｆｏ）と一致することを確認する（第４の検証）。

【００３１】

上記第１～４の検証が全て成功した場合に、当該使い捨てテンポラリ情報の検証が成功する。

【００３２】

次いで、通信事業者サーバ３は、連結データＩｎｆｏ中の課金情報などの情報を当該加入者のＵ－ＩＤと関連付けて加入者データベース（図示せず）に格納する。次いで、通信事業者サーバ３は、使い捨てテンポラリ情報中から得たＮをカウンタ値Ｖの更新データとして当該加入者のＩＤ管理データに含めてＩＤ管理データベース４に格納する。なお、Ｎが１であった場合、当該マスタテンポラリＩＤ（ｍＴ－ＩＤ）は使用回数制限に達したので、無効とする処理を行う。例えば、ＩＤ管理データ中から当該マスタテンポラリＩＤ（ｍＴ－ＩＤ）を削除する。

【００３３】

説明を図２に戻す。次いで、通信事業者サーバ３は、使い捨てテンポラリ情報の検証結果をサービス提供者サーバ６に送信する（ステップＳ１２）。次いで、サービス提供者サーバ６は、通信事業者サーバ３から受信した検証結果に基づき、検証成功ならば携帯電話端末１に対してサービスの提供を開始する（ステップＳ１３）。なお、必要ならば、今回のサービス提供用の利用者ＩＤとして、サブテンポラリＩＤ（ＮＴ－ＩＤ）を使用することが可能である。

【００３４】

上述した実施形態によれば、使い捨て可能なマスタテンポラリＩＤを使用して利用者認証を行うことができる。さらに、マスタテンポラリＩＤから一方向性変換関数を１回又は複数回繰り返し使用してサブテンポラリＩＤを作成することにより、マスタテンポラリＩＤと一方向性変換関数の使用回数（Ｎ）のみからサブテンポラリＩＤを一意に特定することができる。これにより、一利用者に対して一つのマスタテンポラリＩＤおよび一方向性変換関数の使用回数（Ｎ）のみを管理すればよいので、ＩＤ管理データの削減を図ることができる。

【００３５】

以上、本発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。

例えば、マスタテンポラリＩＤの最大使用回数は、利用者が決定し設定してもよい。この場合、マスタテンポラリＩＤ（ｍＴ－ＩＤ）から一方向性の変換関数を使用して、最初にサブテンポラリＩＤ（ＮＴ－ＩＤ）を作成するときのＮが、最大使用回数に相当する。

【００３６】

また、暗号データＥｎｃ（ｍＴ－ＩＤ｜Ｔ）の代わりに、Ｕ－ＩＤを用いた暗号データＥｎｃ（Ｕ－ＩＤ｜Ｔ）を作成し用いてもよい。つまり、被認証者を識別可能な情報を暗号化して用いればよい。この場合、通信事業者サーバ３では、Ｕ－ＩＤによりＩＤ管理データベース４を検索し、発見したＩＤ管理データ中のマスタテンポラリＩＤ（ｍＴ－ＩＤ）を用いてサブテンポラリＩＤ（ＮＴ－ＩＤ）を再現し、使い捨てテンポラリ情報中のサブテンポラリＩＤ（ＮＴ－ＩＤ）と比較することにより、上記第３の検証を行う。

【００３７】

なお、本発明に係る利用者認証システムは、サービスプロバイダのサイトの認証や課金代行サービスなどに適用可能である。また、上記した実施形態では、携帯電話端末が携帯電話通信網経由でインターネット上のサービス提供者サーバにアクセスしたが、ローカル通信によってサービス提供者装置にアクセスしてもよい。例えば、赤外線通信や近距離無線通信、或いは通信ケーブルを用いた有線通信により、サービス提供者サーバにアクセスするものであってもよい。

【００３８】

また、認証装置は通信事業者のサーバに限定されない。また、利用者端末は、携帯電話端末等の携帯通信端末に限定されず、固定電話網等の有線通信網に接続し、認証装置にアクセスするものであってもよい。

【図面の簡単な説明】

【００３９】

【図１】本発明の一実施形態に係る利用者認証システムの構成を示すブロック図である。

【図２】図１に示す利用者認証システムにおける利用者認証処理の流れを示すシーケンスチャートである。

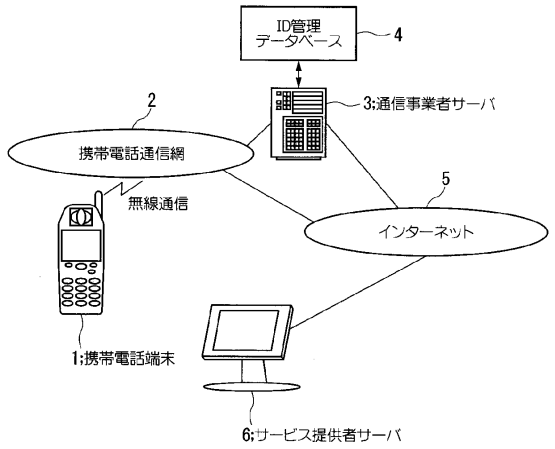
【図３】使い捨てテンポラリ情報１００のデータ構造および使い捨てテンポラリ情報１００の作成手順を説明するための説明図である。

【符号の説明】

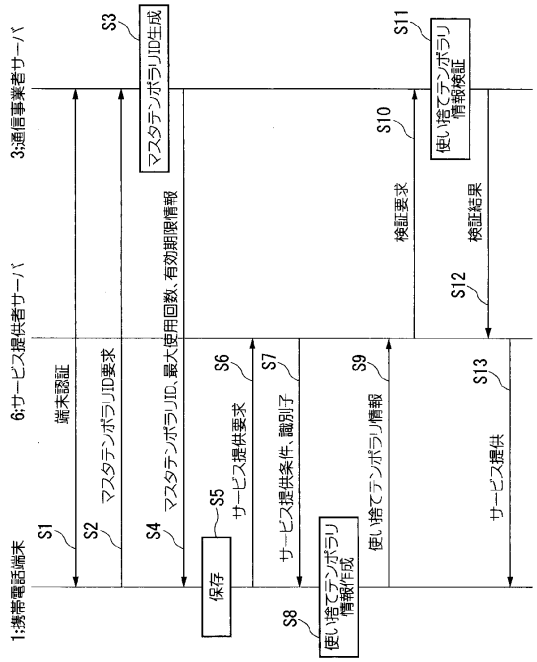
【００４０】

１…携帯電話端末、２…携帯電話通信網、３…通信事業者サーバ、４…ＩＤ管理データベース、５…インターネット、６…サービス提供者サーバ。

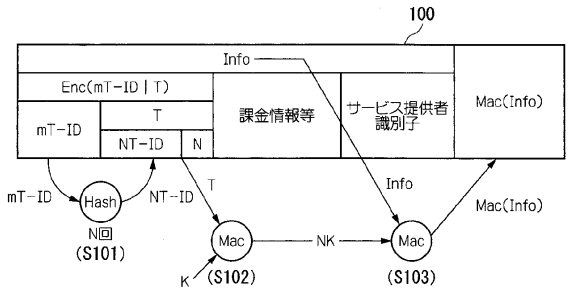
【図１】


ID管理
データベース
4
2
3;通信事業者サーバ
携帯電話通信網
5
無線通信
インターネット
1;携帯電話端末
6;サービス提供者サーバ

【図２】


3;通信事業者サーバ
6;サービス提供者サーバ
1;携帯電話端末
S1
端末認証
S2
マスタテンポラリID要求
S3
マスタテンポラリID生成
S4
マスタテンポラリID、最大使用回数、有効期限情報
S5
サービス提供要求
保存
S6
S7
サービス提供条件、識別子
S8
使い捨てテンポラリ情報作成
S9
使い捨てテンポラリ情報
S10
検証要求
S11
使い捨てテンポラリ情報検証
S12
検証結果
S13
サービス提供

【図３】


100
Info
Enc(mT-ID | T)
mT-ID
T
NT-ID
N
課金情報等
サービス提供者識別子
Mac(Info)
mT-ID
Hash
NT-ID
N回
(S101)
T
Info
Mac(Info)
Mac
NK
Mac
K
(S102)
(S103)

フロントページの続き

審査官　和田　財太

(56)参考文献　特許第３３７９５１７（ＪＰ，Ｂ２）
国際公開第２００４／０３２４１５（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　９／３２