(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6570480号
(P6570480)

(45)発行日　令和1年9月4日(2019.9.4)　(24)登録日　令和1年8月16日(2019.8.16)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
G09C	1/00	(2006.01)	G09C	1/00	640E
G06F	21/31	(2013.01)	H04L	9/00	673D
G06F	21/34	(2013.01)	G06F	21/31	
			G06F	21/34	

請求項の数 12　(全 29 頁)

(21)出願番号　特願2016-113928(P2016-113928)
(22)出願日　平成28年6月7日(2016.6.7)
(62)分割の表示　特願2015-175486(P2015-175486)の分割
原出願日　平成27年9月7日(2015.9.7)
(65)公開番号　特開2017-55384(P2017-55384A)
(43)公開日　平成29年3月16日(2017.3.16)
審査請求日　平成30年8月15日(2018.8.15)

(73)特許権者　500257300
ヤフー株式会社
東京都千代田区紀尾井町１番３号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　五味　秀仁
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　上野　博司
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　山口　修司
東京都港区赤坂九丁目７番１号　ヤフー株式会社内

最終頁に続く

(54)【発明の名称】生成装置、端末装置、生成方法、生成プログラム及び認証処理システム

(57)【特許請求の範囲】
【請求項１】
端末装置と協働して、当該端末装置を利用するユーザの本人性を認証サーバに認証させるための処理を行う生成装置であって、
予め登録された登録データと所定の入力データとの照合結果に基づき前記ユーザの認証を行う、前記端末装置に備えられた、または当該端末装置に接続された認証器であって、当該ユーザの認証に用いられる認証手段が互いに異なる複数の認証器に関する情報を記憶する記憶部と、
前記記憶部に記憶された複数の認証器の各々における認証の信頼性の度合いに関する情報を前記認証サーバと同期させることで、当該認証サーバ側と共通した当該信頼性の度合いに関する情報を管理する管理部と、
前記ユーザの本人性を前記認証サーバが認証するための情報であり、前記複数の認証器のいずれかから取得された照合結果から生成される情報であって、前記端末装置と前記認証サーバとの間で用いられる特定のプロトコルで処理される情報である認証結果情報の生成を制御するとともに、前記端末装置を介して当該認証結果情報を当該認証サーバに送信させるよう制御する生成部と、
を備えることを特徴とする生成装置。
【請求項２】
前記生成部は、
前記認証器から取得された照合結果に対して、前記生成装置内に保持されている鍵を用

いて署名することにより、前記認証結果情報を生成する、
ことを特徴とする請求項１に記載の生成装置。
【請求項３】
前記生成部は、
前記記憶部に記憶された複数の認証器から取得される各々の照合結果に対して、共通する前記鍵を用いて前記認証結果情報を生成する、
ことを特徴とする請求項２に記載の生成装置。
【請求項４】
前記生成部は、
前記記憶部に記憶された複数の認証器から取得される各々の照合結果に対して、対応する認証器ごとに発行された個別の鍵を用いて前記認証結果情報を生成する、
ことを特徴とする請求項２に記載の生成装置。
【請求項５】
前記生成部は、
前記特定のプロトコルで処理される情報を生成可能な外部装置に対して、前記認証器から取得された照合結果に基づいて前記認証結果情報を生成させる、
ことを特徴とする請求項１に記載の生成装置。
【請求項６】
前記生成部は、
前記認証サーバと、前記生成装置及び前記外部装置との信頼性に基づいて、前記生成部が前記認証結果情報を生成するか、あるいは、前記外部装置によって前記認証結果情報を生成させるか、を選択する、
ことを特徴とする請求項５に記載の生成装置。
【請求項７】
前記管理部は、
前記認証サーバが指定する前記認証器の信頼性に基づいて、前記認証器の信頼性に関する情報を更新し、
前記生成部は、
前記認証サーバが指定する前記認証器の信頼性に基づいて、前記認証結果情報を生成する元となる前記認証器を選択する、
ことを特徴とする請求項１～６のいずれか一つに記載の生成装置。
【請求項８】
前記生成部は、
前記認証器から取得された照合結果から生成される前記認証結果情報に、当該認証器の信頼性に関する情報を含ませる、
ことを特徴とする請求項７に記載の生成装置。
【請求項９】
請求項１～８のいずれか一つに記載された前記生成装置と通信する通信部と、
前記複数の認証器のいずれかによる前記照合結果を前記生成装置に送信する認証部と、
前記認証部によって送信された前記照合結果を取得した前記生成装置から、前記認証結果情報を取得する取得部と、
前記取得部によって取得された前記認証結果情報を前記認証サーバに送信する送信部と、
を備えたことを特徴とする端末装置。
【請求項１０】
端末装置と協働して、当該端末装置を利用するユーザの本人性を認証サーバに認証させるための処理を行う生成装置が実行する生成方法であって、
前記生成装置が、予め登録された登録データと所定の入力データとの照合結果に基づき前記ユーザの認証を行う、前記端末装置に備えられた、または当該端末装置に接続された認証器であって、当該ユーザの認証に用いられる認証手段が互いに異なる複数の認証器に

関する情報を所定の記憶部に記憶する記憶工程と、
前記生成装置が、前記記憶部に記憶された複数の認証器の各々における認証の信頼性の度合いに関する情報を前記認証サーバと同期させることで、当該認証サーバ側と共通した当該信頼性の度合いに関する情報を管理する管理工程と、
前記生成装置が、前記ユーザの本人性を前記認証サーバが認証するための情報であり、前記複数の認証器のいずれかから取得された照合結果から生成される情報であって、前記端末装置と前記認証サーバとの間で用いられる特定のプロトコルで処理される情報である認証結果情報の生成を制御するとともに、前記端末装置を介して当該認証結果情報を当該認証サーバに送信させるよう制御する生成工程と、
を含んだことを特徴とする生成方法。
【請求項１１】
端末装置と協働して、当該端末装置を利用するユーザの本人性を認証サーバに認証させるための処理を行う生成装置に実行させる生成プログラムであって、
予め登録された登録データと所定の入力データとの照合結果に基づき前記ユーザの認証を行う、前記端末装置に備えられた、または当該端末装置に接続された認証器であって、当該ユーザの認証に用いられる認証手段が互いに異なる複数の認証器に関する情報を所定の記憶部に記憶する記憶手順と、
前記記憶部に記憶された複数の認証器の各々における認証の信頼性の度合いに関する情報を前記認証サーバと同期させることで、当該認証サーバ側と共通した当該信頼性の度合いに関する情報を管理する管理手順と、
前記ユーザの本人性を前記認証サーバが認証するための情報であり、前記複数の認証器のいずれかから取得された照合結果から生成される情報であって、前記端末装置と前記認証サーバとの間で用いられる特定のプロトコルで処理される情報である認証結果情報の生成を制御するとともに、前記端末装置を介して当該認証結果情報を当該認証サーバに送信させるよう制御する生成手順と、
を含んだことを特徴とする生成プログラム。
【請求項１２】
端末装置と協働して、当該端末装置を利用するユーザの本人性を認証サーバに認証させるための処理を行う生成装置と、認証サーバとを含む認証処理システムであって、
前記生成装置は、
予め登録された登録データと所定の入力データとの照合結果に基づき前記ユーザの認証を行う、前記端末装置に備えられた、または当該端末装置に接続された認証器であって、当該ユーザの認証に用いられる認証手段が互いに異なる複数の認証器に関する情報を記憶する記憶部と、
前記記憶部に記憶された複数の認証器の各々における認証の信頼性の度合いに関する情報を前記認証サーバと同期させることで、当該認証サーバ側と共通した当該信頼性の度合いに関する情報を管理する管理部と、
前記ユーザの本人性を前記認証サーバが認証するための情報であり、前記複数の認証器のいずれかから取得された照合結果から生成される情報であって、前記端末装置と前記認証サーバとの間で用いられる特定のプロトコルで処理される情報である認証結果情報であり、かつ、前記生成装置内に保持される鍵を用いて署名される情報である認証結果情報の生成を制御するとともに、前記端末装置を介して当該認証結果情報を当該認証サーバに送信させるよう制御する生成部と、を備え、
前記認証サーバは、
前記鍵を有する生成装置と、当該鍵に対応する公開鍵とを対応付けて管理する管理部、
を備えることを特徴とする認証処理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、生成装置、端末装置、生成方法、生成プログラム及び認証処理システムに関

する。
【背景技術】
【０００２】
近年、通信ネットワークの普及が進み、ネットワークを介したサービスが盛んに提供されている。ユーザは、通信端末装置を用いて、ネットワークを介して提供されるサービスにログインし、サービスを利用する。ネットワークを介したサービスの利用では、サービスを利用するユーザの本人認証を確実に行うことが望まれる。
【０００３】
例えば、本人認証の技術として、ユーザ認証用のパケットに機器情報を含ませてパケットを送信する端末と、パケットを受信して、ユーザ認証プロトコルを用いてパケットについて認証する認証側システム（サーバ）とを有することにより、端末を扱うユーザの認証を行う技術が知られている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００４－３６２０６１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記の従来技術では、認証要求に柔軟に対応することは難しい。例えば、端末側から要求される認証手段がパスワードやユーザＩＤに限られず、指紋認証、虹彩認証など、種々な認証手段を含む場合には、認証サーバ側は、各々の認証手段に対応する認証プロトコルを実装したり、予め認証手段を登録したりしておくことが要求される。このため、認証サーバ側は、未知の認証手段に対応して、柔軟にユーザからの要求に応じることが難しい。
【０００６】
本願は、上記に鑑みてなされたものであって、認証要求に柔軟に対応することができる生成装置、端末装置、生成方法、生成プログラム及び認証処理システム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】
【０００７】
本願に係る生成装置は、予め登録された登録データと所定の入力データとの照合結果に基づき認証を行う認証器に関する情報を記憶する記憶部と、前記認証器から取得された照合結果から生成される情報であって、前記認証器を利用するユーザの本人認証を行う認証サーバとの間で用いられる特定の認証手順で処理される情報である認証結果情報の生成を制御する生成部と、を備えたことを特徴とする。
【発明の効果】
【０００８】
実施形態の一態様によれば、認証要求に柔軟に対応することができるという効果を奏する。
【図面の簡単な説明】
【０００９】
【図１】図１は、実施形態に係る認証処理の一例を示す図である。
【図２】図２は、実施形態に係る認証方式を説明するシーケンス図（１）である。
【図３】図３は、実施形態に係る認証方式を説明するシーケンス図（２）である。
【図４】図４は、実施形態に係る認証処理システムの構成例を示す図である。
【図５】図５は、実施形態に係るユーザ端末の構成例を示す図である。
【図６】図６は、実施形態に係る認証器情報記憶部の一例を示す図である。
【図７】図７は、実施形態に係る認証サーバの構成例を示す図である。
【図８】図８は、実施形態に係るメタ認証器情報記憶部の一例を示す図である。

【図９】図９は、実施形態に係るメタ認証器による認証処理手順を示すフローチャートである。
【図１０】図１０は、変形例に係るメタ認証器情報記憶部の一例を示す図である。
【図１１】図１１は、変形例に係る認証処理システムの構成例を示す図（１）である。
【図１２】図１２は、変形例に係る認証処理システムの構成例を示す図（２）である。
【図１３】図１３は、生成装置の機能を実現するコンピュータの一例を示すハードウェア構成図である。
【発明を実施するための形態】
【００１０】
以下に、本願に係る生成装置、端末装置、生成方法、生成プログラム及び認証処理システムを実施するための形態（以下、「実施形態」と呼ぶ）について図面を参照しつつ詳細に説明する。なお、この実施形態により本願に係る生成装置、端末装置、生成方法、生成プログラム及び認証処理システムが限定されるものではない。また、各実施形態は、処理内容を矛盾させない範囲で適宜組み合わせることが可能である。また、以下の各実施形態において同一の部位には同一の符号を付し、重複する説明は省略される。
【００１１】
〔１．認証処理の一例〕
まず、図１を用いて、実施形態に係る認証処理の一例について説明する。図１は、実施形態に係る認証処理の一例を示す図である。図１では、本願に係る生成装置に対応するメタ認証器５０と、認証サーバ１００とによって、ユーザ端末１０を利用するユーザの認証処理が行われる例を示す。
【００１２】
図１の例において、ユーザ端末１０は、ユーザＵ１によって利用される情報処理端末である。ユーザＵ１は、ユーザ端末１０を用いて、ネットワークを介して提供されるサービス、例えば、ウェブサーバから提供されるサービスを利用する。以下における説明では、ユーザ端末１０をユーザＵ１と表記する場合がある。すなわち、以下では、ユーザＵ１をユーザ端末１０と読み替えることもできる。
【００１３】
認証サーバ１００は、ユーザ端末１０から送信される情報を取得し、取得した情報に基づいてユーザＵ１の本人認証を行うサーバ装置である。認証サーバ１００が取得する情報とは、例えば、生体認証器等を用いて、ユーザ端末１０を利用しているユーザがユーザＵ１本人であることをユーザ端末１０側が証明したことを示す情報である。認証サーバ１００は、取得した情報に基づいてＵ１本人であることを認証し、認証済みであることを示す情報（署名）を付す。ユーザ端末１０は、認証サーバ１００から署名された情報が各種サービス側（ウェブサーバ等）に送信されることにより、各種サービスへのログインや、サービス毎に発行されるサービスＩＤの利用や、ネットワークを介した決済など、本人認証を要するサービスを利用することが可能となる。
【００１４】
（認証サーバ１００の認証方式）
ここで、認証サーバ１００が所定の情報処理端末（以下、「クライアント２０」と表記する）を利用するユーザの本人認証を行う方式について説明する。
【００１５】
認証サーバ１００は、クライアント２０の認証において、予め発行される公開鍵と秘密鍵との照合によって情報の確実性を担保する、いわゆる公開鍵暗号方式を基礎とした認証方式を採用するものとする。認証サーバ１００は、クライアント２０が有する各認証器に対して発行される公開鍵と秘密鍵のペアに基づいて認証を行う。認証器とは、クライアント２０がローカルにおいて本人認証を行うことができる機能を有する装置をいう。ローカルにおける認証とは、インターネット等の広域なネットワークの接続を要しない状況で行われる認証をいい、例えば、クライアント２０内部に備えられた機能を用いて行われる認証をいう。認証器は、例えば生体情報など、ユーザ本人を認証することが可能な情報につ

いて、予め登録を受け付ける。そして、認証器は、認証の際には、ユーザから生体情報等の入力を受け付ける。そして、認証器は、登録データと入力データとの照合結果に基づいて本人認証を行う。具体的には、認証器には、指紋認証器や、虹彩認証器や、声紋認証器等が含まれる。なお、認証器は、クライアント２０内部にインストールされたソフトウェアにより実現されてもよいし、クライアント２０とローカルで接続可能なハードウェアにより実現されてもよい。すなわち、認証器には、インターネット等の外部ネットワークを介さない、例えば、クライアント２０に備えられたインターフェイスに直接接続されることによりクライアント２０と協働するようなハードウェア等も含まれる。

【００１６】

以下、図２及び図３を用いて、認証サーバ１００がクライアント２０の認証を行う方式について説明する。図２は、実施形態に係る認証方式を説明するシーケンス図（１）である。図２では、認証処理に先立ち、認証サーバ１００が認証を行うクライアント２０に関する登録を行う処理の流れを示している。

【００１７】

クライアント２０は、認証サーバ１００にアクセスし、認証器の登録を要求する（ステップＳ１１）。認証サーバ１００は、クライアント２０から送信された要求に応答して、認証器による認証を要求する（ステップＳ１２）。

【００１８】

クライアント２０を利用するユーザは、認証サーバ１００への登録を要求した認証器を動作させ、ローカルにおいて本人認証を実行する（ステップＳ１３）。例えば、認証に利用する認証器として指紋認証器をユーザが選択した場合には、ユーザは、認証が行われる箇所に指をかざすことにより、認証処理を行う。クライアント２０側の認証器がユーザを正規のユーザと確認できた場合、認証器（又は、クライアント２０）は、その認証処理に対応する公開鍵と秘密鍵とを発行する（ステップＳ１４）。そして、クライアント２０は、発行された秘密鍵をクライアント２０内部に記憶するとともに、秘密鍵とペアになる公開鍵を認証サーバ１００に送信する（ステップＳ１５）。認証サーバ１００は、クライアント２０から公開鍵を受けとり、認証器と対応付けて、公開鍵を記憶する（ステップＳ１６）。これにより、クライアント２０が備える認証器について、認証サーバ１００への登録が完了する。

【００１９】

続いて、図３について説明する。図３は、実施形態に係る認証方式を説明するシーケンス図（２）である。図３では、クライアント２０がサービスを利用する際など、本人認証を認証サーバ１００に要求する場面における処理の流れを示している。

【００２０】

ユーザは、認証サーバ１００に、所定のアクセス制限付きサービスへのアクセスを要求する（ステップＳ２１）。なお、かかる要求は、例えば、ネットワークを介してサービスを行うウェブサーバ等を経由して送信される場合がある。すなわち、ユーザは、サービスを利用する過程において、接続先のウェブサーバから本人認証を求められる場合がある。この場合、ユーザが本人認証を行う旨を表明すると、かかる情報は、クライアント２０又は接続先のウェブサーバから認証サーバ１００に送信される。

【００２１】

要求を受け付けた認証サーバ１００は、クライアント２０に対して、予め登録された認証器による認証を要求する（ステップＳ２２）。要求を受け付けたクライアント２０のユーザは、予め登録された認証器によるローカルな認証を実行する（ステップＳ２３）。

【００２２】

認証器による認証が成功した場合（ローカルにおいて本人認証が確認された場合）、ユーザは、クライアント２０内部に記憶されている秘密鍵へのアクセスが可能となる。そして、クライアント２０は、認証器によって正規のユーザと認められたユーザしかアクセスすることのできない秘密鍵を用いて、認証の結果に関する情報に対する署名（ハッシュ値）を生成する。言い換えれば、クライアント２０は、予め発行されていた秘密鍵による署

名付き情報を生成する（ステップＳ２４）。このようにして生成される情報を、「認証結果情報」と表記する。

【００２３】

続いて、クライアント２０は、認証サーバ１００との間で規定された特定の認証手順（プロトコル）に従って、生成した認証結果情報を送信し（ステップＳ２５）、認証結果情報を処理させる。認証サーバ１００は、秘密鍵とペアとなる公開鍵を用いて、送信された認証結果情報を検証する（ステップＳ２６）。すなわち、認証サーバ１００は、認証結果情報に改竄がないこと、言い換えれば、適切な秘密鍵によって認証結果情報が生成されているか否かを検証する。このように、認証サーバ１００は、認証対象である認証器が適切な秘密鍵を保有していることを確認する。この確認ができた場合、認証サーバ１００は、認証結果情報に基づいてクライアント２０を利用するユーザが正規のユーザであることを認証する。そして、認証サーバ１００は、自身が認証したことを示し、ステップＳ２１においてアクセス要求したサービスの情報が含まれる、認証がなされた旨の情報をクライアント２０に送信する（ステップＳ２７）。認証がなされた旨の情報とは、例えば、認証クッキーである。

【００２４】

このように、上記認証方式によれば、クライアント２０は、一般的な認証で用いられることの多いパスワードやサービスＩＤなど、認証に用いる情報そのものをネットワークに送信することがない。すなわち、第三者がクライアント２０から送信された情報を傍受したとしても、第三者は公開鍵を有しないことから、傍受した情報を利用できないため、安全性の高い方式であるといえる。

【００２５】

さらに、上記のように、認証サーバ１００は、クライアント２０から送信される認証結果情報の処理において、クライアント２０との間で規定される特定の認証手順（プロトコル）に従う。例えば、認証サーバ１００は、ＵＡＦ（Universal Authentication Framework）や、Ｕ２Ｆ（Universal Second Factor)といったプロトコルに従う。これにより、認証サーバ１００とクライアント２０との通信は、より高い安全性が確保される。

【００２６】

説明してきたように、認証サーバ１００とクライアント２０の認証器との間に公開鍵暗号方式を基礎とした認証方式を採用する場合、クライアント２０は、パスワード等の認証情報そのものをネットワーク上に送信することなく、本人認証を認証サーバ１００に対して行うことができる。しかしながら、上述した方式においては、ユーザは、認証サーバ１００に登録されていない認証器については利用することができず、また、認証器ごとに新たな登録を要するため、手間がかかる。さらに、クライアント２０側が認証サーバ１００の規定するプロトコルに対応していない場合、ユーザは、認証サーバ１００による認証を受けることができず、認証を要する各種サービスを利用することができないといった課題がある。

【００２７】

そこで、本願に係る生成装置に対応するメタ認証器５０は、単独では認証サーバ１００による認証処理を受けることが困難な情報処理端末（図１の例では、ユーザ端末１０が該当する）と協働することにより、認証サーバ１００による認証処理を受けることを可能にする。以下、図１の説明に戻り、メタ認証器５０を含む認証処理の一例を流れに沿って説明する。なお、図１に示す例では、ユーザ端末１０が指紋認証器１４ａを有するものの、指紋認証器１４ａは、ユーザＵ１を認証する認証器として認証サーバ１００に登録されていないものとする。また、ユーザ端末１０は、認証サーバ１００との間の通信に用いられる特定の認証手順（プロトコル）に対応する情報を、ユーザ端末１０単独では生成することができないものとする。

【００２８】

図１に示す例では、ユーザＵ１は、ユーザ端末１０内に含まれる認証部１４に対して認証を試みるものとする。認証部１４は、指紋認証器１４ａを有し、指紋認証器１４ａには

、ユーザＵ１の認証に用いる指紋データＦ０１が予め登録されているものとする。すなわち、ユーザＵ１は、ユーザ端末１０において入力を受け付ける箇所（例えば、ユーザ端末１０が備えるタッチパネルディスプレイ）に対して、指紋データＦ０１に対応する指を触れることにより、指紋認証器１４ａへ指紋データを入力する。指紋認証器１４ａは、登録データである指紋データＦ０１と、入力された指紋データとを照合することにより、ユーザＵ１を認証する（ステップＳ０１）。すなわち、指紋認証器１４ａは、照合結果に基づいて、ユーザＵ１を本人であると認証する。

【００２９】

そして、認証部１４は、指紋認証器１４ａによる認証結果をメタ認証器５０に送る。メタ認証器５０は、認証器情報記憶部５１と、認証器管理部５２と、生成部５３とを有する。ここで、メタ認証器５０は、認証サーバ１００に登録された認証器として扱われているものとする。かかる登録は、例えば、認証サーバ１００の管理者等により予め行われる。この場合、メタ認証器５０は、認証サーバ１００の認証に関する秘密鍵Ｋ０１を保持している。また、認証サーバ１００は、秘密鍵Ｋ０１とペアとなる公開鍵Ｋ０２をメタ認証器５０から受け取り、保持している。

【００３０】

メタ認証器５０に係る認証器管理部５２は、ユーザ端末１０に係る認証部１４に含まれる認証器を管理する処理部である。例えば、認証器管理部５２は、認証部１４に含まれる各認証器の信頼性を判定し、認証に関して一定の信頼性を有する認証器を認証器情報記憶部５１に記憶する。認証器管理部５２は、認証器情報記憶部５１に記憶された認証器によって認証された結果情報を受け付けた場合、かかる認証結果が信頼できるものと判定する。図１の例では、認証器管理部５２は、認証部１４から受け付けた、指紋認証器１４ａによる認証結果を信頼できる情報と判定する。そして、認証器管理部５２は、判定した結果を生成部５３に送る。

【００３１】

メタ認証器５０に係る生成部５３は、認証サーバ１００との通信に用いられる特定のプロトコルに対応する情報の生成を制御する処理部である。生成部５３は、認証器管理部５２が信頼した認証結果を受け付ける。そして、生成部５３は、受け付けた情報について、秘密鍵Ｋ０１を用いて署名された情報である認証結果情報を生成する（ステップＳ０２）。生成部５３は、生成した認証結果情報をユーザ端末１０に係る送信部１７へ送る。

【００３２】

送信部１７は、メタ認証器５０によって生成された情報であって、特定の認証手順によって認証サーバ１００に処理される情報である認証結果情報を認証サーバ１００に送信する（ステップＳ０３）。

【００３３】

認証サーバ１００に係る受信部１３１は、ユーザ端末１０から送信された認証結果情報を受信する（ステップＳ０４）。受信部１３１は、受信した認証結果情報を解析部１３２に送る。

【００３４】

解析部１３２は、認証結果情報を解析する（ステップＳ０５）。このとき、解析部１３２は、認証結果情報に基づき、情報の送信元であるメタ認証器５０を特定する。そして、解析部１３２は、メタ認証器に関する情報を管理するメタ認証器管理部１３３に、メタ認証器の信頼性を問い合わせる。例えば、メタ認証器管理部１３３は、登録部１３４によってメタ認証器情報記憶部１２１に記憶された情報に、メタ認証器５０が含まれるか否かを判定する。また、メタ認証器管理部１３３は、トラスト情報管理部１３５によって設定されたメタ認証器ごとの信頼性を判定する。その結果、メタ認証器管理部１３３は、解析対象である認証結果情報の生成元であるメタ認証器５０は、信頼に足るメタ認証器であると判定する。メタ認証器管理部１３３は、判定の結果を解析部１３２に送る。

【００３５】

解析部１３２は、認証結果情報の生成元であるメタ認証器５０が信頼に足るメタ認証器

であると判定した場合、メタ認証器５０との間で予め発行されていた公開鍵Ｋ０２を用いて、認証結果情報の署名を検証する。そして、解析部１３２は、受け付けた認証結果情報が適切な秘密鍵Ｋ０１によって署名されていたことを確認する。これにより、解析部１３２は、認証結果情報に対応するユーザであるユーザＵ１を認証する（ステップＳ０６）。

【００３６】

このように、メタ認証器５０は、予め登録された登録データと所定の入力との照合結果に基づき認証を行う認証器に関する情報を記憶する認証器情報記憶部５１を有する。さらに、メタ認証器５０は、認証器から取得された照合結果から生成される情報であって、認証器を利用するユーザＵ１の本人認証を行う認証サーバ１００との間で規定された特定のプロトコルで処理される情報である認証結果情報の生成を制御する生成部５３を有し、上記の処理を実行する。

【００３７】

すなわち、メタ認証器５０によれば、メタ認証器５０がユーザ端末１０内にある認証器の信頼性を判定し、認証器を管理することができる。これにより、ユーザＵ１は、ユーザ端末１０で利用したい認証器が複数ある場合であっても、認証サーバ１００への登録をその都度行うことを要さない。そして、図１の例のように、ユーザ端末１０自体では、特定のプロトコルに対応した情報が生成できない場合であっても、ユーザ端末１０は、メタ認証器５０と協働することにより、秘密鍵Ｋ０１を用いて、認証サーバ１００が認証に用いる情報を生成することができる。また、認証サーバ１００側にとっては、メタ認証器５０の信頼性を担保することにより、ユーザ端末１０側で使用される様々な認証器については、メタ認証器５０が代理して認証器の信頼性を判定させることができる。そして、認証サーバ１００は、認証に関しては、メタ認証器５０との間で発行された公開鍵と秘密鍵を用いることで、安全な認証を行うことができる。このように、メタ認証器５０によれば、認証の安全性を損なわず、かつ、認証要求に柔軟に対応することができる。

【００３８】

〔２．認証処理システムの構成〕

次に、図４を用いて、実施形態に係るメタ認証器５０が含まれる認証処理システム１の構成について説明する。図４は、実施形態に係る認証処理システム１の構成例を示す図である。図４に例示するように、実施形態に係る認証処理システム１には、ユーザ端末１０と、ユーザ端末１０内部に含まれるメタ認証器５０と、認証サーバ１００と、ウェブサーバ２００とが含まれる。これらの各種装置は、ネットワークＮを介して、有線又は無線により通信可能に接続される。

【００３９】

ユーザ端末１０は、デスクトップ型ＰＣ（Personal Computer）や、ノート型ＰＣや、タブレット端末や、スマートフォンを含む携帯電話機、ＰＤＡ（Personal Digital Assistant）等の情報処理端末である。また、ユーザ端末１０には、眼鏡型や時計型の情報処理端末であるウェアラブルデバイス（wearable device）も含まれる。さらに、ユーザ端末１０には、情報処理機能を有する種々のスマート機器が含まれてもよい。例えば、ユーザ端末１０には、ＴＶ（Television）や冷蔵庫、掃除機などのスマート家電や、自動車などのスマートビークル（Smart vehicle）や、ドローン（drone）、家庭用ロボットなどが含まれてもよい。

【００４０】

ユーザ端末１０は、各種認証器を備える。例えば、ユーザ端末１０は、ユーザの生体情報を利用する生体認証器を備える。これにより、ユーザ端末１０は、ローカルにおいて、ユーザ端末１０を利用するユーザの本人認証を行う。上述のように、認証器は、ユーザ端末１０内に含まれるソフトウェアであってもよいし、ユーザ端末１０に接続されるハードウェアであってもよい。

【００４１】

メタ認証器５０は、ユーザ端末１０及びユーザ端末１０が備える認証器と協働し、認証サーバ１００に対して、ローカルで行われたユーザの認証結果情報の生成を制御する生成

装置である。メタ認証器５０は、認証サーバ１００に予め登録され、認証サーバ１００が有する公開鍵とペアとなる秘密鍵を管理する。また、メタ認証器５０は、ユーザ端末１０が備える認証器を管理し、管理した認証器における認証の信頼性を担保する。メタ認証器５０は、信頼に足る認証器による認証が行われた場合に、かかる認証器の照合結果に基づいて、認証サーバ１００に送信するための認証結果情報を生成する。

【００４２】

認証サーバ１００は、上述のように、ユーザ端末１０を利用するユーザの本人認証を行うサーバ装置である。認証サーバ１００は、ユーザ端末１０から送信された認証結果情報を受信し、対応する公開鍵によって認証結果情報の署名を検証する。ユーザ端末１０は、署名がなされた情報を用いることにより、ウェブサーバ２００等が提供するサービスにおいて、認証処理を行うことができる。

【００４３】

ウェブサーバ２００は、ユーザ端末１０からアクセスされた場合に、各種ウェブページを提供するサーバ装置である。ウェブサーバ２００は、例えば、ニュースサイト、天気予報サイト、ショッピングサイト、ファイナンス（株価）サイト、路線検索サイト、地図提供サイト、旅行サイト、飲食店紹介サイト、ウェブブログなどに関する各種ウェブページを提供する。

【００４４】

ウェブサーバ２００は、サービスの提供にあたり、ユーザの本人認証を要求する場合がある。例えば、ウェブサーバ２００が決済サービスを提供する際に、ユーザ端末１０を利用しているユーザが間違いなくユーザＵ１であると認証できないときには、ウェブサーバ２００は、ユーザ端末１０による決済サービスの実行を制限することができる。一方、ウェブサーバ２００は、認証サーバ１００がユーザＵ１を認証したことを示す情報をユーザ端末１０、又は認証サーバ１００から受信した場合には、ユーザ端末１０を利用しているユーザがユーザＵ１であると信頼する。この場合、ウェブサーバ２００は、ユーザ端末１０による決済など、本人認証を要する行動を受け付ける。

【００４５】

〔３．ユーザ端末の構成〕

次に、図５を用いて、実施形態に係るユーザ端末１０の構成について説明する。図５は、実施形態に係るユーザ端末１０の構成例を示す図である。図５に示すように、ユーザ端末１０は、通信部１１と、入力部１２と、表示部１３と、認証部１４と、制御部１５とを有する。また、図５に示す例では、ユーザ端末１０は、メタ認証器５０を内蔵するものとする。なお、ユーザ端末１０が有する各処理部の接続関係は、図５に示した接続関係に限られず、他の接続関係であってもよい。

【００４６】

通信部１１は、ネットワークＮと有線又は無線で接続され、認証サーバ１００やウェブサーバ２００等との間で情報の送受信を行う。例えば、通信部１１は、ＮＩＣ（Network Interface Card）等によって実現される。

【００４７】

入力部１２は、ユーザから各種操作を受け付ける入力装置である。例えば、入力部１２は、ユーザ端末１０に備えられた操作キー等によって実現される。また、入力部１２には、画像を撮影するための撮像装置（カメラ等）や、音声を集音する集音機器（マイク等）が含まれてもよい。表示部１３は、各種情報を表示するための表示装置である。例えば、表示部１３は、液晶ディスプレイ等によって実現される。なお、ユーザ端末１０にタッチパネルが採用される場合には、入力部１２の一部と表示部１３とは一体化される。

【００４８】

認証部１４は、ユーザ端末１０を利用するユーザの認証を行う。具体的には、認証部１４は、各種認証器を用いて、ユーザから入力される情報を受け付ける。そして、認証部１４は、各種認証器に予め登録されているデータと入力データとを照合させる。そして、認証部１４は、照合結果を制御部１５やメタ認証器５０に送る。

【００４９】
認証部１４は、認証器として、例えば、指紋認証器１４ａや、虹彩認証器１４ｂや、声紋認証器１４ｃを備える。指紋認証器１４ａは、ユーザから予め指紋データの登録を受け付ける。そして、指紋認証器１４ａは、認証の際には、ユーザ端末１０を利用するユーザから指紋の入力を受け付け、登録されていた指紋データとの照合により、本人認証を行う。虹彩認証器１４ｂは、ユーザから予め虹彩データの登録を受け付ける。そして、虹彩認証器１４ｂは、認証の際には、ユーザ端末１０を利用するユーザから虹彩の入力を受け付け、登録されていた虹彩データとの照合により、本人認証を行う。この場合、虹彩認証器１４ｂは、ユーザ端末１０が備えるカメラの機能を適宜利用する。声紋認証器１４ｃは、ユーザから予め声紋データの登録を受け付ける。そして、声紋認証器１４ｃは、認証の際には、ユーザ端末１０を利用するユーザから音声の入力を受け付け、登録されていた声紋データとの照合により、本人認証を行う。この場合、声紋認証器１４ｃは、ユーザ端末１０が備えるマイクの機能を適宜利用する。

【００５０】
なお、ユーザ端末１０は、認証器として、上記の例以外にも、種々の情報を用いる認証器を備えていてもよい。例えば、ユーザ端末１０は、ユーザの顔の画像データを用いて認証を行う顔認証器を備えていてもよい。また、ユーザ端末１０がウェアラブルデバイスである場合、ユーザ端末１０は、備えられた各種センサを認証器として用いてもよい。すなわち、ユーザ端末１０は、ユーザから取得されるセンサデータを予め保持しておき、ユーザに利用される際に、予め保持していたセンサデータとの照合を行うことで、ユーザの本人性を認証する。なお、認証器は、生体情報を用いた認証を行う認証器に限られない。例えば、認証器は、ユーザＵ１が所有する所定の物理キーをユーザ端末１０に接続することによって認証を行うハードウェア認証器であってもよいし、ユーザ端末１０に内蔵されるＳＩＭカード（Subscriber Identity Module Card）の内容を判定することで認証を行うＳＩＭカード認証器であってもよい。また、ユーザ端末１０は、ユーザ端末１０が接続した機器に割り当てられた識別情報に基づいてユーザを認証するような認証器を備えていてもよい。この場合、認証器は、例えば、ユーザ端末１０と無線で接続されるルータ等に固有に割り当てられる識別情報（ＭＡＣ（Media Access Control）アドレス等）を判定する。そして、認証器は、判定した識別情報が、認証対象となるユーザが通常利用している機器の識別情報と齟齬がない場合、ユーザ端末１０を利用するユーザを本人であると認証する。

【００５１】
制御部１５は、例えば、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）等によって、ユーザ端末１０内部の記憶装置に記憶されている各種プログラムがＲＡＭ（Random Access Memory)を作業領域として実行されることにより実現される。また、制御部１５は、例えば、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）等の集積回路により実現される。

【００５２】
制御部１５は、ユーザ端末１０において行われる認証処理や、メタ認証器５０と協働する処理や、認証サーバ１００やウェブサーバ２００と送受信する情報の管理等の処理を制御する。図５に示すように、制御部１５は、取得部１６と、送信部１７とを有し、以下に説明する情報処理の機能や作用を実現または実行する。例えば、制御部１５は、ＲＡＭを作業領域として上述したアプリを実行することにより、取得部１６及び送信部１７を実現する。なお、制御部１５の内部構成は、図５に示した構成に限られず、後述する情報処理を行う構成であれば他の構成であってもよい。

【００５３】
取得部１６は、各種情報を取得する。例えば、取得部１６は、認証サーバ１００やウェブサーバ２００から送信される情報を受信する。また、取得部１６は、認証サーバ１００やウェブサーバ２００から送信される、ユーザ端末１０を利用するユーザの本人認証を求

める通信パケットを受信する。また、取得部１６は、認証部１４から要求される各種情報を取得する。例えば、取得部１６は、入力部１２を介して、ユーザ端末１０を利用するユーザの指紋データを取得する。また、取得部１６は、メタ認証器５０によって生成された認証結果情報を取得する。

【００５４】

送信部１７は、各種情報を送信する。例えば、送信部１７は、メタ認証器５０に係る生成部５３によって生成された認証結果情報を認証サーバ１００に送信する。また、送信部１７は、認証サーバ１００から送信された、認証済みの署名がなされた情報をウェブサーバ２００等に送信する。

【００５５】

(メタ認証器５０について)

メタ認証器５０は、認証器情報記憶部５１と、認証器管理部５２と、生成部５３とを有し、ユーザ端末１０と協働して、各種処理を行う。

【００５６】

認証器情報記憶部５１は、ユーザ端末１０が有する認証器に関する情報を記憶する。認証器情報記憶部５１は、例えば、ＲＡＭ、フラッシュメモリ（Flash Memory）等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される。ここで、図６に、実施形態に係る認証器情報記憶部５１の一例を示す。図６は、実施形態に係る認証器情報記憶部５１の一例を示す図である。図６に示した例では、認証器情報記憶部５１は、「認証器ＩＤ」、「タイプ」、「登録データ」、「認証ユーザ」、「信頼性」といった項目を有する。

【００５７】

「認証器ＩＤ」は、認証器を識別する識別情報を示す。なお、実施形態において、認証器ＩＤは、認証器の参照符号と一致するものとする。例えば、指紋認証器１４ａの認証器ＩＤは、「１４ａ」と示される。

【００５８】

「タイプ」は、認証器のタイプを示す。実施形態において、認証器のタイプは、認証器が照合することのできる情報によって示される。例えば、認証器のタイプが「指紋」である場合、かかる認証器は、指紋データによって本人認証を行うことを示す。

【００５９】

「登録データ」は、本人認証のため、予め認証器に登録されるデータを識別する情報を示す。図６では、「登録データ」は、「Ａ０１」など概念的に示しているが、実際には、登録データの項目には、ユーザの指紋データであったり、虹彩データであったり、声紋データ等が記憶される。なお、図６に示すように、一つの認証器に複数の登録データが登録されてもよい。例えば、図６では、指紋認証器１４ａに「Ａ０１」と「Ａ０２」の２つのデータが登録されている。これは、一人のユーザＵ１が、例えば、親指と人差し指という２種類の指紋データを登録していることを示している。

【００６０】

「認証ユーザ」は、認証器が認証するユーザを示す。なお、認証ユーザは、一つの認証器に対して複数登録されていてもよい。この場合、認証器は、登録データと認証ユーザを１つのペアとし、認証ユーザの数と同じ数の登録データを少なくとも有する。

【００６１】

「信頼性」は、メタ認証器５０によって管理される認証器の信頼性を示す。図６の例では、信頼性は、１から５までの５段階の数値で示すものとし、数字が大きいほど信頼性が高いものとする。信頼性の項目は、例えば、認証器の信頼性を示すリストを参照し、メタ認証器５０に係る認証器管理部５２により自動的に設定されてもよいし、メタ認証器５０の管理者により設定されてもよい。また、信頼性の項目は、認証サーバ１００からの指定により設定されてもよい。また、信頼性の項目は、認証器ごとではなく、登録データごとに設定されてもよい。

【００６２】

すなわち、図６では、認証器ＩＤ「１４ａ」で識別される認証器は、タイプが「指紋」認証型であり、登録データとして「Ａ０１」や「Ａ０２」が登録されており、登録データ「Ａ０１」や「Ａ０２」に対応する認証ユーザは「Ｕ１」であり、信頼性は「４」である例を示している。

【００６３】

認証器管理部５２は、ユーザ端末１０が備える認証器を管理する。例えば、認証器管理部５２は、ユーザ端末１０を利用するユーザが認証を行うための認証器の登録を受け付ける。また、認証器管理部５２は、登録された認証器に関する情報の更新を行う。例えば、ユーザ端末１０を利用するユーザが新たな認証器の使用を所望する場合には、認証器管理部５２は、新たな認証器を認証器情報記憶部５１に登録する。なお、認証器管理部５２は、新たな認証器を登録する際に、かかる認証器の信頼性を判定し、一定の信頼性のある認証器のみを登録するようにしてもよい。この場合、認証器管理部５２は、例えば、予め認証サーバ１００の管理者等により作成された認証器の信頼性を示すリスト等を参照し、認証器の信頼性を判定するようにしてもよい。

【００６４】

なお、認証器管理部５２は、認証サーバ１００から送信される情報に基づいて、認証器に関する情報の更新を行ってもよい。例えば、認証器管理部５２は、認証サーバ１００が指定する信頼性の値に基づいて、認証器に設定される信頼性の値を更新する。また、認証器管理部５２は、認証サーバ１００が信頼できないと判定した認証器に関して、認証器情報記憶部５１から削除するようにしてもよい。このように、認証器管理部５２は、ユーザ端末１０に備えられた認証器を管理し、認証器の信頼性を担保することにより、ローカルで行われるユーザ端末１０の認証の適切性を担保する。

【００６５】

生成部５３は、認証結果情報の生成を制御する処理部である。まず、生成部５３は、認証器情報記憶部５１に記憶された認証器による照合結果を取得する。そして、生成部５３は、照合結果から生成される情報であって、認証器を利用するユーザの本人認証を行う認証サーバ１００との間で用いられる特定のプロトコルで処理される情報である認証結果情報を生成する。この際、生成部５３は、認証器から取得された照合結果に対して、認証サーバ１００が有する公開鍵と対になる秘密鍵を用いて署名することにより、認証結果情報を生成する。具体的には、生成部５３は、認証器から取得された照合結果において、照合結果がユーザの本人性を認めるものである場合にアクセス可能となる秘密鍵にアクセスする。そして、生成部５３は、認証器の照合結果に基づきアクセス可能となる秘密鍵で署名を行った認証結果情報を生成する。言い換えれば、生成部５３は、ユーザ端末１０においてローカルで行われた本人認証が成功したことを示す情報を生成する。生成部５３は、生成した認証結果情報をユーザ端末１０に係る送信部１７に戻し、認証結果情報を認証サーバ１００に送信させる。なお、生成部５３は、メタ認証器５０内で認証結果情報を生成するのではなく、所定の外部装置を用いて、認証結果情報を生成させてもよい。この点について、詳細は後述する。

【００６６】

なお、生成部５３は、所定の条件に基づいて、ユーザ端末１０のユーザの認証を行う認証器を選択してもよい。例えば、生成部５３は、ユーザ端末１０が認証サーバ１００から認証要求を受け付けた際に、要求される認証の信頼性を参照する。例えば、認証サーバ１００は、ユーザ端末１０が利用しようとするサービスが、本人認証に高い信頼性を要求している場合、ユーザ端末１０で行われる認証が信頼性の高い認証器で行われることを求めることができる。具体的には、決済サービス等を提供するウェブサーバ２００は、ユーザ端末１０を利用するユーザに対して、信頼性の高い認証が行われることを所望する。

【００６７】

この場合、生成部５３は、認証器の信頼性に関する情報に基づいて、認証結果情報を生成する元となる認証器を選択する。例えば、生成部５３は、信頼性が「４」以上の認証器によってユーザの認証が行われることが望ましい旨をユーザ端末１０に通知する。ユーザ

端末１０は、例えば、表示部１３にその旨を表示し、ユーザにその旨を通知する。一例として、ユーザ端末１０は、表示部１３に対応するディスプレイに「指紋または虹彩による認証を行ってください」といった旨を表示することで、選択された認証器をユーザに通知する。なお、生成部５３は、上述のように、認証サーバ１００から各認証器の信頼性の指定を受けた場合には、認証サーバ１００から指定された信頼性に基づいて、認証結果情報を生成する元となる認証器を選択する。なお、生成部５３は、認証器情報記憶部５１に記憶された認証器が複数ある場合、複数の認証器から取得される各々の照合結果に対して、共通する秘密鍵を用いて認証結果情報を生成するようにしてもよい。すなわち、メタ認証器５０と認証サーバ１００との間で信頼性が確立されている場合、メタ認証器５０は、認証器の種類によらず、自らの秘密鍵によって、認証サーバ１００に対する認証処理を行うことができる。

【００６８】

〔４．認証サーバの構成〕

次に、図７を用いて、実施形態に係る認証サーバ１００の構成について説明する。図７は、実施形態に係る認証サーバ１００の構成例を示す図である。図７に示すように、認証サーバ１００は、通信部１１０と、記憶部１２０と、制御部１３０とを有する。なお、認証サーバ１００は、認証サーバ１００を利用する管理者等から各種操作を受け付ける入力部（例えば、キーボードやマウス等）や、各種情報を表示するための表示部（例えば、液晶ディスプレイ等）を有してもよい。

【００６９】

（通信部１１０について）

通信部１１０は、例えば、ＮＩＣ等によって実現される。通信部１１０は、ネットワークＮと有線又は無線で接続され、ネットワークＮを介して、ユーザ端末１０やウェブサーバ２００との間で情報の送受信を行う。なお、通信部１１０は、ユーザ端末１０から送信される認証結果情報を処理する場合には、安全性の高い特定のプロトコルに従う。

【００７０】

（記憶部１２０について）

記憶部１２０は、例えば、ＲＡＭ、フラッシュメモリ等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される。記憶部１２０は、メタ認証器情報記憶部１２１を有する。

【００７１】

（メタ認証器情報記憶部１２１について）

メタ認証器情報記憶部１２１は、メタ認証器に関する情報を記憶する。ここで、図８に、実施形態に係るメタ認証器情報記憶部１２１の一例を示す。図８は、実施形態に係るメタ認証器情報記憶部１２１の一例を示す図である。図８に示した例では、メタ認証器情報記憶部１２１は、「メタ認証器ＩＤ」、「認証ユーザ」、「信頼性」、「公開鍵」といった項目を有する。

【００７２】

「メタ認証器ＩＤ」は、メタ認証器を識別する識別情報を示す。なお、実施形態において、メタ認証器ＩＤは、メタ認証器の参照符号と一致するものとする。例えば、メタ認証器５０の認証器ＩＤは、「５０」と示される。

【００７３】

「認証ユーザ」は、メタ認証器が認証するユーザを示す。なお、認証ユーザは、一つのメタ認証器に対して複数登録されていてもよい。

【００７４】

「信頼性」は、認証サーバ１００に対するメタ認証器の信頼性を示す。図８の例では、信頼性は、１から５までの５段階の数値で示すものとし、数字が大きいほど信頼性が高いものとする。信頼性の項目は、例えば、メタ認証器の信頼性を示すリストを参照し、認証サーバ１００の管理者等により手動で設定される。

【００７５】

「公開鍵」は、メタ認証器から送信される認証結果情報に対応する公開鍵を示す。公開鍵は、メタ認証器が認証サーバ１００に登録される際に発行される。なお、公開鍵と対になる秘密鍵は、各メタ認証器内部に保持される。

【００７６】

すなわち、図８では、メタ認証器ＩＤ「５０」で識別されるメタ認証器は、認証ユーザが「Ｕ１」であり、信頼性は「５」であり、公開鍵が「Ｋ０２」である例を示している。

【００７７】

（制御部１３０について）

制御部１３０は、例えば、ＣＰＵやＭＰＵ等によって、認証サーバ１００内部の記憶装置に記憶されている各種プログラム（生成プログラムの一例に相当）がＲＡＭを作業領域として実行されることにより実現される。また、制御部１３０は、例えば、ＡＳＩＣやＦＰＧＡ等の集積回路により実現される。

【００７８】

図７に示すように、制御部１３０は、受信部１３１と、解析部１３２と、メタ認証器管理部１３３と、送信部１３６とを有し、以下に説明する情報処理の機能や作用を実現または実行する。なお、制御部１３０の内部構成は、図７に示した構成に限られず、後述する情報処理を行う構成であれば他の構成であってもよい。また、制御部１３０が有する各処理部の接続関係は、図７に示した接続関係に限られず、他の接続関係であってもよい。

【００７９】

（受信部１３１について）

受信部１３１は、各種情報を受信する。例えば、受信部１３１は、ユーザ端末１０から送信される認証結果情報を受信する。また、受信部１３１は、ユーザ端末１０がウェブサーバ２００にアクセスし、アクセス先のウェブサーバ２００が提供するサービスがユーザ端末１０に認証を要求する場合に、かかる認証要求をウェブサーバ２００から受信する。この場合、受信部１３１が受け付けた認証要求に対応して、後述する送信部１３６は、ユーザ端末１０に認証を行わせる旨の通知を送信する。

【００８０】

（解析部１３２について）

解析部１３２は、認証結果情報を解析する。具体的には、解析部１３２は、ユーザ端末１０から送信された認証結果情報を解析し、認証結果情報の生成元であるメタ認証器５０を特定する。この際、解析部１３２は、メタ認証器管理部１３３を介して、認証結果情報の生成元であるメタ認証器５０に対応する公開鍵を用いて、認証結果情報の署名を検証する。

【００８１】

そして、解析部１３２は、認証結果情報の生成元となったメタ認証器５０が信頼に足るメタ認証器である場合に、ユーザ端末１０から送信された認証結果情報を正規な認証情報として認める。そして、解析部１３２は、認証結果情報を認証したことを示す情報を送信部１３６に送り、ユーザ端末１０に送信させる。

【００８２】

なお、解析部１３２は、認証結果情報を生成した所定のメタ認証器が、所定の基準よりも信頼性に劣る装置である場合、その認証結果情報で示されたユーザの本人性を認めないものとしてもよい。例えば、解析部１３２は、認証結果情報を生成した所定のメタ認証器が、メタ認証器管理部１３３が管理するメタ認証器情報記憶部１２１に記憶されていない場合や、生成元のメタ認証器の信頼性の値が特に低い場合には、その認証結果情報で示されたユーザの本人性を認めないようにしてもよい。

【００８３】

（メタ認証器管理部１３３について）

メタ認証器管理部１３３は、メタ認証器５０に関する情報を管理する。例えば、メタ認証器管理部１３３は、秘密鍵を有するメタ認証器５０と、その秘密鍵に対応する公開鍵とを対応付けて管理する。メタ認証器管理部１３３は、登録部１３４と、トラスト情報管理

部１３５とを有する。
【００８４】
（登録部１３４について）
登録部１３４は、所定のメタ認証器を登録する。例えば、登録部１３４は、認証サーバ１００の管理者による入力を受け付け、メタ認証器５０をメタ認証器情報記憶部１２１に登録する。また、登録部１３４は、メタ認証器５０が認証するユーザＵ１や、メタ認証器５０の信頼性についても併せてメタ認証器情報記憶部１２１に登録する。
【００８５】
また、登録部１３４は、認証サーバ１００とメタ認証器５０との間で対になる公開鍵と秘密鍵のうち、公開鍵をメタ認証器５０と対応付けて登録する。解析部１３２が認証結果情報を解析する際には、メタ認証器管理部１３３は、登録部１３４によって登録された公開鍵を解析部１３２に渡し、認証結果情報を解析させる。
【００８６】
（トラスト情報管理部１３５について）
トラスト情報管理部１３５は、メタ認証器の信頼性について管理する。例えば、トラスト情報管理部１３５は、メタ認証器が認証に用いる認証器を参照し、各メタ認証器が行う認証の信頼性を判定することにより、メタ認証器情報記憶部１２１に記憶されているメタ認証器の信頼性の値を更新する。トラスト情報管理部１３５は、認証サーバ１００の管理者による入力により、メタ認証器の信頼性を更新してもよい。
【００８７】
（送信部１３６について）
送信部１３６は、各種情報を送信する。例えば、送信部１３６は、サービスの利用に際してユーザ端末１０を利用するユーザの本人性の認証を行うことが求められた場合に、ユーザ端末１０に、認証を要求する旨の情報を送信する。また、送信部１３６は、認証結果情報を解析した解析部１３２により公開鍵を用いて検証された情報であって、ユーザの本人認証が済んだことを示す情報をユーザ端末１０に送信する。なお、送信部１３６は、サービスを提供するウェブサーバ２００側に認証済みを示す情報を送信してもよい。すなわち、受信部１３１がウェブサーバ２００側を介して、ユーザ端末１０に関する認証要求を受信した場合、認証サーバ１００は、ユーザ端末１０に認証を要求する。そして、認証サーバ１００は、ユーザ端末１０のユーザを認証する。この場合、送信部１３６は、ユーザ端末１０に関する認証要求を送信したウェブサーバ２００に対して、認証済みを示す情報を返信する。そして、ウェブサーバ２００は、返信された認証済みを示す情報に基づいて、ユーザ端末１０のユーザにサービスを提供する。
【００８８】
〔５．処理手順〕
次に、図９を用いて、実施形態に係るメタ認証器５０による処理の手順について説明する。図９は、実施形態に係るメタ認証器５０による認証処理手順を示すフローチャートである。
【００８９】
図９に示すように、生成部５３は、任意の認証器から照合結果を受け付けたか否かを判定する（ステップＳ１０１）。生成部５３は、照合結果を受け付けていない場合（ステップＳ１０１；Ｎｏ）、受け付けるまで待機する。
【００９０】
一方、生成部５３が照合結果を受け付けた場合（ステップＳ１０１；Ｙｅｓ）、認証器管理部５２は、当該照合結果を送信した認証器に関する情報を取得する（ステップＳ１０２）。
【００９１】
そして、生成部５３は、認証器管理部５２によって取得された認証器に関する情報を参照し、当該認証器から受け付けた照合結果に基づいて、認証結果情報を生成する（ステップＳ１０３）。そして、生成部５３は、生成した認証結果情報をユーザ端末１０に送信す

る（ステップＳ１０４）。
【００９２】
〔６．変形例〕
上述したメタ認証器５０による認証処理は、上記実施形態以外にも種々の異なる形態にて実施されてよい。そこで、以下では、メタ認証器５０の他の実施形態について説明する。
【００９３】
〔６－１．認証器ごとの管理〕
上記実施形態では、メタ認証器５０は、予め登録された認証サーバ１００との間で発行される秘密鍵と公開鍵を用いた認証を行う例を示した。このとき、認証サーバ１００は、メタ認証器５０を登録することにより、メタ認証器５０から送信された認証結果情報を信頼することで認証を行う例を示した。ここで、メタ認証器５０は、自身が管理する認証器に関する情報を認証サーバ１００に送信し、認証器ごとに異なる認証処理を受けるようにしてもよい。この点について、図１０を用いて説明する。
【００９４】
図１０は、変形例に係るメタ認証器情報記憶部１２１の一例を示す図である。図１０に示した例では、メタ認証器情報記憶部１２１は、「メタ認証器ＩＤ」、「端末ＩＤ」、「認証ユーザ」、「認証器ＩＤ」、「信頼性」、「公開鍵」といった項目を有する。なお、既に説明した項目については、説明を省略する。
【００９５】
「端末ＩＤ」は、メタ認証器と協働する情報処理端末を識別する情報である。なお、端末ＩＤは、ユーザ端末の参照符号と一致するものとする。例えば、ユーザ端末１０の端末ＩＤは、「１０」と示される。
【００９６】
すなわち、図１０では、メタ認証器ＩＤ「５０」で識別されるメタ認証器は、端末ＩＤ「１０」で識別されるユーザ端末１０に備えられた認証器を管理しており、ユーザ端末１０に備えられた認証器はそれぞれ「１４ａ」、「１４ｂ」、「１４ｃ」で識別され、それぞれの認証器が認証するユーザは「Ｕ１」であり、それぞれの信頼性は「４」、「５」、「３」であり、メタ認証器５０に対応する公開鍵は「Ｋ０２」であることを示している。なお、認証器ごとの信頼性は、上述のように、メタ認証器５０によって設定されてもよいし、認証サーバ１００側で設定されてもよい。また、認証器の信頼性について、いずれか一方の指定により、メタ認証器５０側と認証サーバ１００側とで同期をとるようにしてもよい。このように、メタ認証器５０及び認証サーバ１００は、認証器の信頼性を相互に確認することで、ローカルで行われる認証に関する信頼性を担保することができる。
【００９７】
すなわち、変形例に係るメタ認証器管理部１３３は、メタ認証器５０自体を管理するとともに、メタ認証器５０によって管理されている認証器を管理する。この場合、メタ認証器５０は、認証結果情報の中に、どの認証器による照合結果に基づいて生成された認証結果情報であるかを含ませる。そして、送信された認証結果情報を受け付けた解析部１３２は、認証結果情報を解析する。
【００９８】
このとき、解析部１３２は、メタ認証器管理部１３３から情報を取得することにより、メタ認証器５０のうち、どの認証器の照合結果に基づく認証結果情報が信頼に足るものなのかを、メタ認証器情報記憶部１２１に記憶された信頼性の項目の値により判定する。例えば、解析部１３２は、送信された認証結果情報が認証器ＩＤ「１４ｂ」で示される認証器の照合結果に基づく認証結果情報である場合、かかる認証結果情報について、最も信頼性が高いと判定する。
【００９９】
そして、解析部１３２は、メタ認証器５０に対応する公開鍵Ｋ０２で署名を行う際に、認証器に対応する信頼性の情報を含ませる。すなわち、解析部１３２は、ユーザ端末１０

で行われた認証が、どのくらい信頼性が高い認証器を用いられて行われたものであるかを示す情報を含ませることができる。そして、認証サーバ１００は、かかる情報が含まれた情報をユーザ端末１０に戻す。このように、メタ認証器５０及び認証サーバ１００によれば、メタ認証器そのものの信頼性のみならず、メタ認証器５０が管理する各認証器の信頼性に関する情報が含まれた本人認証情報をユーザ端末１０に渡すことができる。これにより、例えば、ウェブサーバ２００等のサービス提供者は、ユーザ端末１０が有する本人認証情報の信頼性に適合するレベルのサービスを提供するといった、アクセスコントロールを容易に行うことができる。

【０１００】

なお、上記の処理は、メタ認証器５０に係る生成部５３が行ってもよい。すなわち、生成部５３は、認証器から取得された照合結果から認証結果情報を生成する際に、当該認証器の信頼性に関する情報を認証結果情報に含ませてもよい。これにより、生成部５３は、認証器ごとの信頼性が含まれた認証結果情報を生成することができるので、例えば、より安全性の高い認証器に基づいて生成された認証結果情報であることを認証サーバ１００に伝えることができる。

【０１０１】

なお、上記説明してきた処理は、認証器ごとに発行された個別の秘密鍵で認証結果情報が生成されることにより実現されてもよい。すなわち、生成部５３は、認証器情報記憶部５１に記憶された認証器が複数ある場合、複数の認証器から取得される各々の照合結果に対して、対応する認証器ごとに発行された個別の秘密鍵を用いて認証結果情報を生成する。これにより、生成部５３は、個々の認証器の信頼性等が含まれた認証結果情報を生成することができる。そして、メタ認証器５０は、個別の秘密鍵を用いた認証結果情報を認証サーバ１００に送信することで、個々の認証器の信頼性に基づく認証処理を受けることができる。

【０１０２】

〔６－２．認証処理システムの構成（１）〕

上記実施形態では、メタ認証器５０は、ユーザ端末１０が備える認証器から取得した照合結果に基づいて、認証結果情報を生成する例を示した。ここで、メタ認証器５０は、自らが認証結果情報を生成するのではなく、所定の外部装置に認証結果情報を生成させてもよい。この点について、図１１を用いて説明する。

【０１０３】

図１１は、変形例に係る認証処理システム１の構成例を示す図（１）である。図１１に示すように、変形例に係る認証処理システム１は、ユーザ端末１０、メタ認証器５０、認証サーバ１００、ウェブサーバ２００に加え、代理端末３０を含む。また、代理端末３０は、生成部３１を有する。

【０１０４】

代理端末３０は、ユーザ端末１０やメタ認証器５０等と通信可能な情報処理端末である。また、代理端末３０に係る生成部３１は、実施形態に係るメタ認証器５０が有する生成部５３と同様、認証器による照合結果に基づいて、認証サーバ１００との間で規定された特定のプロトコルで処理される情報である認証結果情報を生成することのできる処理部である。

【０１０５】

図１１で示す例において、メタ認証器５０は、代理端末３０を信頼に足る端末であるとして予め登録し、管理しているものとする。また、代理端末３０は、予め認証サーバ１００との間で発行された公開鍵と秘密鍵を有するものとし、また、代理端末３０とメタ認証器５０（あるいは、ユーザ端末１０）は、相互に関連付けられて認証サーバ１００に登録されているものとする。

【０１０６】

メタ認証器５０は、ユーザが認証器を用いて認証を試みた場合、認証結果情報を生成する前の段階において、認証器による照合結果を代理端末３０に送信する。そして、代理端

末３０は、認証サーバ１００との間で予め発行されている秘密鍵を用いて、メタ認証器５０から送信された照合結果から、認証結果情報を生成する。そして、代理端末３０は、生成した認証結果情報を認証サーバ１００に送信する。

【０１０７】

認証サーバ１００は、代理端末３０との間で予め発行されていた公開鍵を用いて、代理端末３０から送信された認証結果情報の署名を検証する。そして、認証サーバ１００は、認証サーバ１００が管理する情報において、メタ認証器５０（あるいは、ユーザ端末１０）と代理端末３０とが対応付けられて登録されている情報を参照する。そして、認証サーバ１００は、代理端末３０から送信された認証結果情報に基づいて、ユーザ端末１０を利用するユーザの本人認証を行う。認証サーバ１００は、代理端末３０から送信された認証結果情報に対して、本人認証済みの情報を付し、ユーザ端末１０に送信する。

【０１０８】

このように、メタ認証器５０は、認証結果情報の生成に際して、特定のプロトコルで処理される情報を生成可能な代理端末３０に対して、認証器から取得された照合結果に基づいて認証結果情報を生成させてもよい。

【０１０９】

すなわち、メタ認証器５０は、認証結果情報を生成する処理を管理するものの、生成処理自体は、処理を代理する代理端末３０に委ねることができる。このため、メタ認証器５０は、例えば、認証サーバ１００が利用するプロトコルの規定が変わるなどの状況の変化によって、自身が認証結果情報を生成できない場合であっても、認証結果情報を生成することのできる代理端末３０を新たに登録することにより、ユーザ端末１０の認証を行わせることができる。このように、メタ認証器５０は、様々な状況に対応した柔軟な認証処理を行うことができる。

【０１１０】

また、メタ認証器５０は、認証結果情報の生成に際して、認証サーバ１００と、メタ認証器５０及び代理端末３０との信頼性に基づいて、メタ認証器５０が認証結果情報を生成するか、あるいは、代理端末３０によって認証結果情報を生成させるか、を選択してもよい。

【０１１１】

すなわち、メタ認証器５０は、認証サーバ１００で管理される情報を参照し、メタ認証器５０と代理端末３０のいずれが認証サーバ１００に対して高い信頼性を有しているかを判定する。そして、メタ認証器５０は、例えば、信頼性の高い方に認証結果情報を生成させる。認証サーバ１００との信頼性が高いということは、言い換えれば、認証強度が高いことを意味する。そこで、メタ認証器５０は、より確実性の高い本人認証を行うことができると想定される装置を選択して処理を行う。これにより、メタ認証器５０は、本人認証の安全性、確実性を担保することができる。なお、この場合、認証サーバ１００は、メタ認証器５０や、代理端末３０の信頼性に関する情報について、メタ認証器情報記憶部１２１に適宜記憶するようにしてもよい。

【０１１２】

〔６－３．認証処理システムの構成（２）〕

上記実施形態では、メタ認証器５０は、ユーザ端末１０の内部に備えられ、ユーザ端末１０と協働して処理を行う例を示した。ここで、メタ認証器５０は、ユーザ端末１０の内部に備えられず、ユーザ端末１０と接続可能な外部装置として構成されてもよい。この点について、図１２を用いて説明する。

【０１１３】

図１２は、変形例に係る認証処理システム１の構成例を示す図（２）である。図１２に示すように、変形例に係る認証処理システム１は、ユーザ端末１０、メタ認証器５０、認証サーバ１００、ウェブサーバ２００を含み、ユーザ端末１０とメタ認証器５０とは別々の装置として構成される。図１２の例において、メタ認証器５０は、例えば、独立した生成装置として認識されるサーバ装置である。

【０１１４】
この場合、ユーザ端末１０は、認証部１４が備える所定の認証器により登録データと入力データとの照合が行われた場合、照合結果をメタ認証器５０に送信する。そして、メタ認証器５０は、上記実施形態で説明したように、認証結果情報を生成し、認証サーバ１００にかかる情報を送信する。認証サーバ１００は、メタ認証器５０が管理する（信頼する）端末としてユーザ端末１０が予め登録されている情報を参照し、メタ認証器５０から送信された認証結果情報に基づいて、ユーザ端末１０を利用するユーザの本人認証を行う。
【０１１５】
このように、メタ認証器５０は、ユーザ端末１０内部に備えられるのではなく、独立した生成装置として扱われてもよい。この場合、メタ認証器５０は、ユーザ端末１０と有線接続されてもよいし、例えば、クラウド上に設置され、ユーザ端末１０からの要求があった場合にのみ稼働するようにしてもよい。また、メタ認証器５０は、一台のユーザ端末１０に利用されることに限られず、複数台の情報処理端末を管理し、複数台の情報処理端末から利用されてもよい。この場合、認証サーバ１００は、メタ認証器５０が管理する複数台の情報処理端末について、メタ認証器５０と関連付けてメタ認証器情報記憶部１２１に記憶してもよい。このように、メタ認証器５０は、様々な状況に対応した柔軟な認証処理を行うことができる。
【０１１６】
〔６－４．形態〕
上記実施形態及び変形例で述べたように、メタ認証器５０は、様々な形態で実現されてよい。例えば、メタ認証器５０は、ユーザ端末１０に埋め込まれたＩＣチップとして実現されてもよいし、独立した生成装置として実現されてもよい。また、メタ認証器５０は、認証器管理部５２や生成部５３の機能が一体化されたプログラム（アプリケーション）として実現されてもよい。メタ認証器５０がアプリケーションである場合、当該アプリケーションは、ユーザの操作に従ってユーザ端末１０にインストールされることにより実行される。また、この場合、認証器情報記憶部５１は、ユーザ端末１０が有する所定の記憶領域を利用すること等により実現される。
【０１１７】
〔６－５．各装置の構成〕
上記実施形態では、ユーザ端末１０やメタ認証器５０の構成例について図５を用いて説明した。また、認証サーバ１００の構成例について図７を用いて説明した。しかし、認証処理システム１に含まれる各装置は、必ずしも例示した構成によって実現されなくともよい。例えば、ユーザ端末１０は、図５で例示した全ての処理部を備えることを必ずしも要しない。すなわち、ユーザ端末１０は、表示部１３や認証部１４を必ずしも内部に備えていなくてもよい。また、ユーザ端末１０は、２以上の機器に分離されて図５に示す構成が実現されてもよい。例えば、ユーザ端末１０は、少なくとも認証部１４と取得部１６とを有する認証機器と、少なくとも通信部１１を有する通信機器とが分離された構成を有する、２台以上の機器により実現されてもよい。
【０１１８】
〔６－６．認証器〕
上記実施形態では、認証器が行うローカルな認証として、インターネット等の広域なネットワークの接続を要しない状況で行われる認証、例えば、ユーザ端末１０内部に備えられた指紋認証器１４ａ等を用いた認証を例に示した。しかし、ローカルな認証は上記例に限られず、例えば、メタ認証器５０は、通信回線を提供する通信事業者から提供される認証器による認証をローカルな認証と認めてもよい。例えば、通信事業者は、営業する店舗に据置き型の認証器を設置する。ユーザは、メタ認証器５０を備えたユーザ端末１０を店舗に持参し、据置き型の認証器によって本人認証を行う。メタ認証器５０は、店舗に設置された回線を利用して据置き型の認証器による照合結果を取得する。そして、メタ認証器５０は、据置き型の認証器による照合結果に基づいて、認証結果情報を生成し、認証サーバ１００に送信する。この場合、例えば、通信事業者は、通信事業者が提供する通信回線

の契約利用者のみが据置き型の認証器を利用することができるといった利用制限を設けてもよい。これにより、メタ認証器５０は、認証器を備えないユーザ端末１０であっても、認証サーバ１００による認証処理を受けさせることができる。また、信頼される所定のアクセスコントロールがなされていれば、認証器は、クラウド上に存在していてもよい。この場合、ユーザは、クラウド上の認証器にアクセスする所定の条件（例えば、事前の本人登録等）を満たすことにより、クラウド上の認証器による認証を行うことができる。そして、メタ認証器５０は、クラウド上の認証器から取得された照合結果に基づいて、認証結果情報を生成する。このように、メタ認証器５０は、状況に応じて、種々の認証器から取得される照合結果に基づいて認証結果情報を生成してもよい。これにより、メタ認証器５０は、柔軟な認証処理に対応することができる。

【０１１９】

〔７．ハードウェア構成〕

上述してきた実施形態に係るユーザ端末１０や、メタ認証器５０に対応する生成装置や、認証サーバ１００は、例えば図１３に示すような構成のコンピュータ１０００によって実現される。以下、メタ認証器５０を例に挙げて説明する。図１３は、メタ認証器５０の機能を実現するコンピュータ１０００の一例を示すハードウェア構成図である。コンピュータ１０００は、ＣＰＵ１１００、ＲＡＭ１２００、ＲＯＭ１３００、ＨＤＤ１４００、通信インターフェイス（Ｉ／Ｆ）１５００、入出力インターフェイス（Ｉ／Ｆ）１６００、及びメディアインターフェイス（Ｉ／Ｆ）１７００を有する。

【０１２０】

ＣＰＵ１１００は、ＲＯＭ１３００又はＨＤＤ１４００に記憶されたプログラムに基づいて動作し、各部の制御を行う。ＲＯＭ１３００は、コンピュータ１０００の起動時にＣＰＵ１１００によって実行されるブートプログラムや、コンピュータ１０００のハードウェアに依存するプログラム等を記憶する。

【０１２１】

ＨＤＤ１４００は、ＣＰＵ１１００によって実行されるプログラム、及び、かかるプログラムによって使用されるデータ等を記憶する。通信インターフェイス１５００は、通信網５００（図２に示したネットワークＮに対応）を介して他の機器からデータを受信してＣＰＵ１１００へ送り、ＣＰＵ１１００が生成したデータを、通信網５００を介して他の機器へ送信する。

【０１２２】

ＣＰＵ１１００は、入出力インターフェイス１６００を介して、ディスプレイやプリンタ等の出力装置、及び、キーボードやマウス等の入力装置を制御する。ＣＰＵ１１００は、入出力インターフェイス１６００を介して、入力装置からデータを取得する。また、ＣＰＵ１１００は、入出力インターフェイス１６００を介して生成したデータを出力装置へ出力する。

【０１２３】

メディアインターフェイス１７００は、記録媒体１８００に記憶されたプログラム又はデータを読み取り、ＲＡＭ１２００を介してＣＰＵ１１００に提供する。ＣＰＵ１１００は、かかるプログラムを、メディアインターフェイス１７００を介して記録媒体１８００からＲＡＭ１２００上にロードし、ロードしたプログラムを実行する。記録媒体１８００は、例えばＤＶＤ（Digital Versatile Disc）、ＰＤ（Phase change rewritable Disk）等の光学記録媒体、ＭＯ（Magneto-Optical disk）等の光磁気記録媒体、テープ媒体、磁気記録媒体、または半導体メモリ等である。

【０１２４】

例えば、コンピュータ１０００が実施形態に係るメタ認証器５０として機能する場合、コンピュータ１０００のＣＰＵ１１００は、ＲＡＭ１２００上にロードされたプログラムを実行することにより、認証器管理部５２や、生成部５３の機能を実現する。また、ＨＤＤ１４００には、認証器情報記憶部５１内のデータが記憶される。コンピュータ１０００のＣＰＵ１１００は、これらのプログラムを記録媒体１８００から読み取って実行するが

、他の例として、他の装置から通信網５００を介してこれらのプログラムを取得してもよい。

【０１２５】

〔８．その他〕

また、上記実施形態において説明した各処理のうち、自動的に行われるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行われるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。例えば、各図に示した各種情報は、図示した情報に限られない。

【０１２６】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。例えば、図５に示した認証器管理部５２と、生成部５３とは統合されてもよい。また、例えば、認証器情報記憶部５１に記憶される情報は、ネットワークＮを介して、外部に備えられた記憶装置に記憶されてもよい。

【０１２７】

また、上述してきた実施形態及び変形例は、処理内容を矛盾させない範囲で適宜組み合わせることが可能である。

【０１２８】

〔９．効果〕

上述してきたように、実施形態に係るメタ認証器５０（生成装置の一例）は、認証器情報記憶部５１と、生成部５３とを有する。認証器情報記憶部５１は、予め登録された登録データと所定の入力データとの照合結果に基づき認証を行う認証器に関する情報を記憶する。生成部５３は、認証器から取得された照合結果から生成される情報であって、認証器を利用するユーザの本人認証を行う認証サーバ１００との間で用いられる特定の認証手順で処理される情報である認証結果情報の生成を制御する。

【０１２９】

このように、実施形態に係るメタ認証器５０は、ローカルにおいてユーザが本人認証で用いる認証器に関する情報を記憶する。そして、メタ認証器５０は、認証器で行われた照合結果に基づく情報であり、特定のプロトコルで処理される認証結果情報の生成を制御する。これにより、メタ認証器５０は、認証サーバ１００が管理する認証器に限らず、自身が管理する認証器を用いた認証をローカルで行い、その結果情報のみを用いて認証サーバ１００に送信するための情報を生成することができる。すなわち、メタ認証器５０は、認証サーバ１００側が管理する認証器等によらずに認証処理を行うことができるため、認証要求に柔軟に対応することができる。

【０１３０】

また、生成部５３は、認証器から取得された照合結果を、認証サーバ１００が有する公開鍵と対になる秘密鍵であって、メタ認証器５０内に保持されている秘密鍵を用いて署名を生成することにより、認証結果情報を生成する。

【０１３１】

このように、実施形態に係るメタ認証器５０は、公開鍵暗号方式に対応する認証結果情報を生成することにより、安全性の高い認証結果情報を生成することができる。また、メタ認証器５０は、認証器ごとではなく、認証サーバ１００とメタ認証器５０との間で発行された秘密鍵を用いて、認証結果情報を生成する。すなわち、メタ認証器５０によれば、認証器ごとに公開鍵と秘密鍵を発行することを要しないので、柔軟な認証処理を実現することができる。

【０１３２】

また、生成部５３は、認証器情報記憶部５１に記憶された認証器が複数ある場合、複数の認証器から取得される各々の照合結果に対して、共通する秘密鍵を用いて認証結果情報を生成する。

【０１３３】

このように、実施形態に係るメタ認証器５０は、例えばユーザ端末１０で利用される認証器が複数ある場合であっても、共通する秘密鍵によって認証処理を行わせることができる。すなわち、メタ認証器５０によれば、複数の認証器が一元的に管理されるため、個々の認証器を認証サーバ１００に登録する（認証器ごとの鍵を発行する）といった手順を要さずとも、個々の認証器を用いて認証を行うことができる。このように、メタ認証器５０によれば、ユーザ端末１０を利用するユーザは、認証サーバ１００へ各認証器を登録する手間を省くことができるため、認証処理を簡略化することができる。

【０１３４】

また、生成部５３は、認証器情報記憶部５１に記憶された認証器が複数ある場合、複数の認証器から取得される各々の照合結果に対して、対応する認証器ごとに発行された個別の鍵を用いて認証結果情報を生成するようにしてもよい。

【０１３５】

このように、メタ認証器５０は、認証器ごとに異なる鍵を用いて認証結果情報を生成することができる。このため、メタ認証器５０は、例えば、認証サーバ１００やウェブサーバ２００が指定する所定の認証器による認証を求められた場合に、適切な認証器によって生成された認証結果情報を認証サーバ１００に送信することができる。すなわち、メタ認証器５０は、例えば、ローカルでの認証で使用された認証器によって提供されるサービスのレベルが異なるようなサービスに対して、サービスに応じた認証結果情報を適切に生成することができる。

【０１３６】

また、生成部５３は、特定の認証手順で処理される情報を生成可能な代理端末３０（外部装置の一例）に対して、認証器から取得された照合結果に基づいて認証結果情報を生成させてもよい。

【０１３７】

このように、実施形態に係るメタ認証器５０は、必ずしも自らが認証結果情報を生成することを要せず、外部装置を管理することにより、認証結果情報を生成させてもよい。これにより、メタ認証器５０は、認証サーバ１００との通信のプロトコルの変更や、認証器に関する情報の更新など、想定される種々の状況の変化に対応して、柔軟に認証処理を行うことができる。

【０１３８】

また、生成部５３は、認証サーバ１００と、メタ認証器５０及び代理端末３０との信頼性に基づいて、生成部５３が認証結果情報を生成するか、あるいは、代理端末３０によって認証結果情報を生成させるか、を選択する。

【０１３９】

このように、実施形態に係るメタ認証器５０は、認証サーバ１００との関係において、より信頼性が高いと設定されている装置を選択して、認証結果情報を生成させることができる。認証サーバ１００との信頼性が高いということは、すなわち、認証強度が高いことを意味するため、メタ認証器５０は、より確実に本人認証を行うことができると想定される装置を選択して処理を行うことができる。これにより、メタ認証器５０は、本人認証の安全性、確実性を担保することができる。

【０１４０】

また、実施形態に係るメタ認証器５０は、認証器の信頼性に関する情報を管理する認証器管理部５２をさらに有する。生成部５３は、認証器の信頼性に関する情報に基づいて、認証結果情報を生成する元となる認証器を選択する。

【０１４１】

このように、実施形態に係るメタ認証器５０は、認証器ごとの信頼性を管理する。そし

て、メタ認証器５０は、より信頼性の高い認証器を選択し、認証結果情報を生成することができる。例えば、メタ認証器５０は、なりすましなど第三者に悪用される可能性の低い情報を認証で用いる認証器を信頼性が高いものとして管理する。これにより、メタ認証器５０は、より安全性の高い認証器を用いて認証結果情報を生成することになるので、安全な認証処理を行うことができる。

【０１４２】

また、認証器管理部５２は、認証サーバ１００が指定する認証器の信頼性に基づいて、認証器の信頼性に関する情報を更新する。生成部５３は、認証サーバ１００が指定する認証器の信頼性に基づいて、認証結果情報を生成する元となる認証器を選択する。

【０１４３】

このように、実施形態に係るメタ認証器５０は、認証サーバ１００側から受け付ける認証器ごとの信頼性に基づいて処理を行ってもよい。すなわち、メタ認証器５０は、認証サーバ１００と相互に認証器の信頼性を確認しながら認証処理を行うため、認証器の信頼性が担保された、安全な認証を行うことができる。

【０１４４】

また、生成部５３は、認証器から取得された照合結果から生成される認証結果情報に、当該認証器の信頼性に関する情報を含ませてもよい。

【０１４５】

このように、実施形態に係るメタ認証器５０は、生成される認証結果情報に、認証で用いた認証器の信頼性に関する情報を含ませることができる。すなわち、メタ認証器５０は、本人認証情報に関して、より確実性のある認証がなされた情報か否かといったことを示すことができる。これにより、例えばウェブサーバ２００を管理するサービス提供者等は、メタ認証器５０の処理に基づく認証を受けたユーザに対して、サービスにおいて許可する範囲を設定したり、認めるサービスを適宜調整したりといった、アクセスコントロールを容易に行うことができる。

【０１４６】

また、本願に係るユーザ端末１０は、メタ認証器５０と通信する通信部１１と、メタ認証器５０から取得した認証結果情報を認証サーバ１００に送信する送信部１７とを有する。

【０１４７】

このように、ユーザ端末１０は、メタ認証器５０と通信することにより、例えば、自らが認証サーバ１００との通信で用いられる特定のプロトコルに対応する機能を有していない場合や、認証サーバ１００に対応する秘密鍵を有していない場合であっても、認証サーバ１００による本人認証を受けることができる。このように、メタ認証器５０は、ユーザ端末１０のユーザが利用することのできる認証処理の幅を広げ、柔軟な認証処理を実現させることができる。

【０１４８】

以上、本願の実施形態のいくつかを図面に基づいて詳細に説明したが、これらは例示であり、発明の開示の欄に記載の態様を始めとして、当業者の知識に基づいて種々の変形、改良を施した他の形態で本発明を実施することが可能である。

【０１４９】

また、上述してきた「部（section、module、unit）」は、「手段」や「回路」などに読み替えることができる。例えば、生成部は、生成手段や生成回路に読み替えることができる。

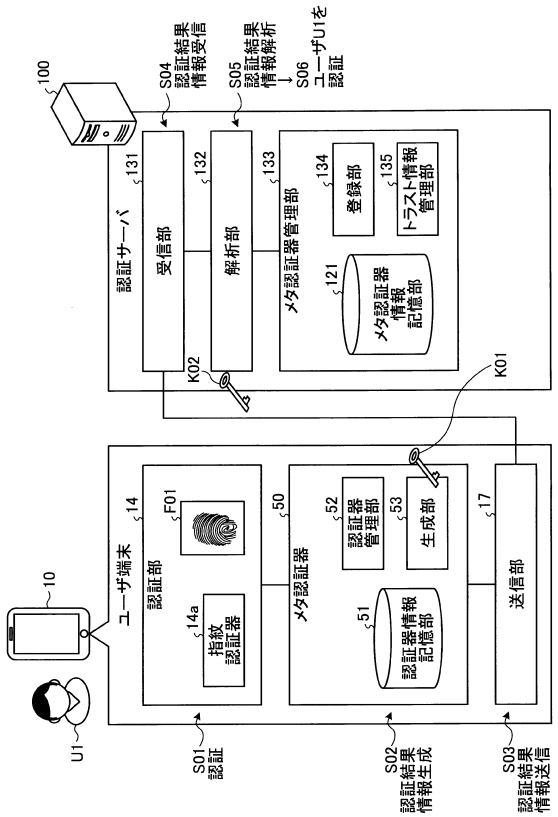
【符号の説明】

【０１５０】

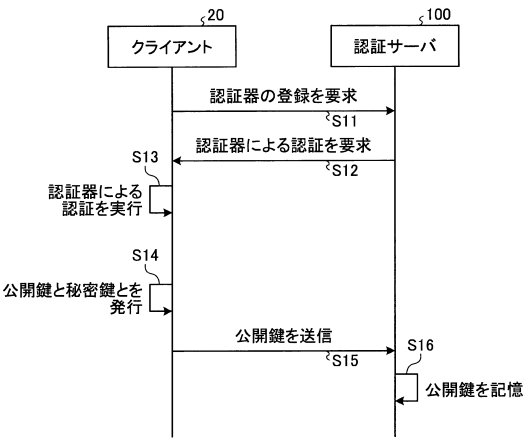
１　認証処理システム
１０　ユーザ端末
２０　クライアント
３０　代理端末

５０　メタ認証器
５１　認証器情報記憶部
５２　認証器管理部
５３　生成部
１００　認証サーバ
２００　ウェブサーバ

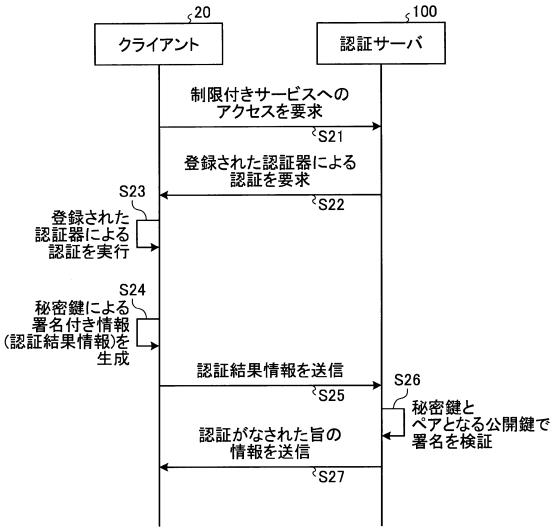
【図１】



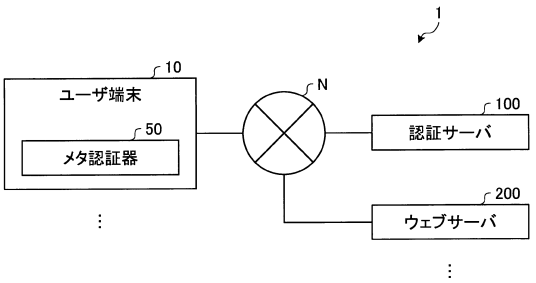
【図２】



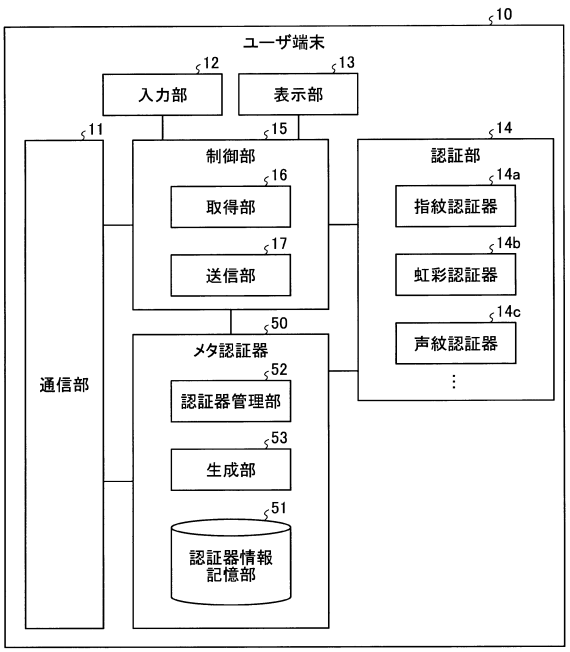
【図３】



【図４】



【図５】

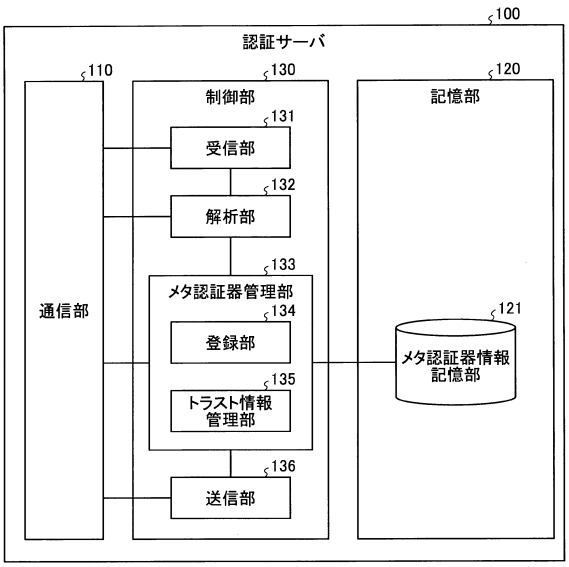


【図６】

51

認証器ID	タイプ	登録データ	認証ユーザ	信頼性	…
…	…	…	…	…	…
14a	指紋	A01	U1	4	…
		A02	U1	4	…
		…	…	…	…
14b	虹彩	B01	U1	5	…
		–	–	–	…
		…	…	…	…
14c	声紋	C01	U1	3	…
		–	–	–	…
		…	…	…	…
…	…	…	…	…	…

【図７】

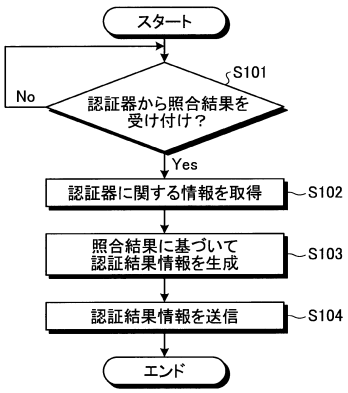


【図８】

121

メタ認証器ID	認証ユーザ	信頼性	公開鍵	…
…	…	…	…	…
50	U1	5	K02	…
	–			…
	–			…
	…			…
60	U11	4	K12	…
	U12			…
	U13			…
	…			…
…	…	…	…	…

【図９】

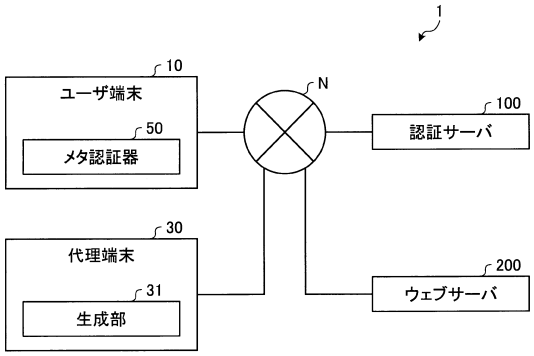


【図１０】

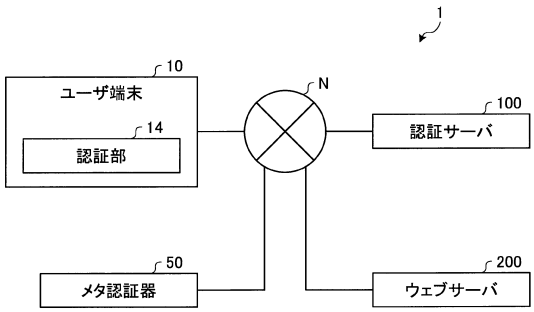
121

メタ認証器ID	端末ID	認証器ID	認証ユーザ	信頼性	公開鍵	…
…	…	…	…	…	…	…
50	10	14a	U1	4	K02	…
		14b	U1	5		…
		14c	U1	3		…
		…	…	…		…
…	…	…	…	…	…	…

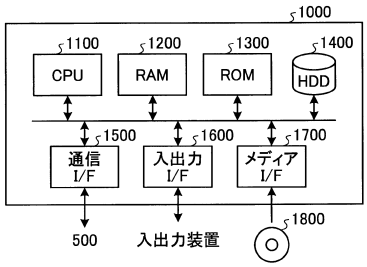
【図１１】


1
10
ユーザ端末
50
メタ認証器
N
100
認証サーバ
30
代理端末
31
生成部
200
ウェブサーバ

【図１２】


1
10
ユーザ端末
14
認証部
N
100
認証サーバ
50
メタ認証器
200
ウェブサーバ

【図１３】


1000
1100
CPU
1200
RAM
1300
ROM
1400
HDD
1500
通信
I/F
1600
入出力
I/F
1700
メディア
I/F
1800
500
入出力装置

フロントページの続き

(72)発明者　久住　貴史
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　河崎　真人
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　大神　渉
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　近藤　裕介
東京都港区赤坂九丁目７番１号　ヤフー株式会社内

審査官　岸野　徹

(56)参考文献　国際公開第２０１４／１７６５３９（WO，Ａ１）
特開２００４－１７８４０８（ＪＰ，Ａ）
米国特許出願公開第２００４／０１０４２６５（ＵＳ，Ａ１）
米国特許出願公開第２０１４／０１８９７９１（ＵＳ，Ａ１）
特表２０１６－５０２３７３（ＪＰ，Ａ）
特開２００７－２５７４２８（ＪＰ，Ａ）
欧州特許出願公開第０２０００９４１（ＥＰ，Ａ１）
特表２０１６－５２５８０７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／３４
Ｇ０９Ｃ　　１／００