(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2009-123154
(P2009-123154A)
(43)公開日　平成21年6月4日(2009.6.4)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B017
G06F 21/24	(2006.01)	G06F	12/14	520A	5B285
G09C 1/00	(2006.01)	G06F	12/14	530D	5J104
		G09C	1/00	640E	

審査請求 未請求　請求項の数 17　ＯＬ　（全 35 頁）

(21)出願番号　特願2007-299234 (P2007-299234)
(22)出願日　平成19年11月19日 (2007.11.19)

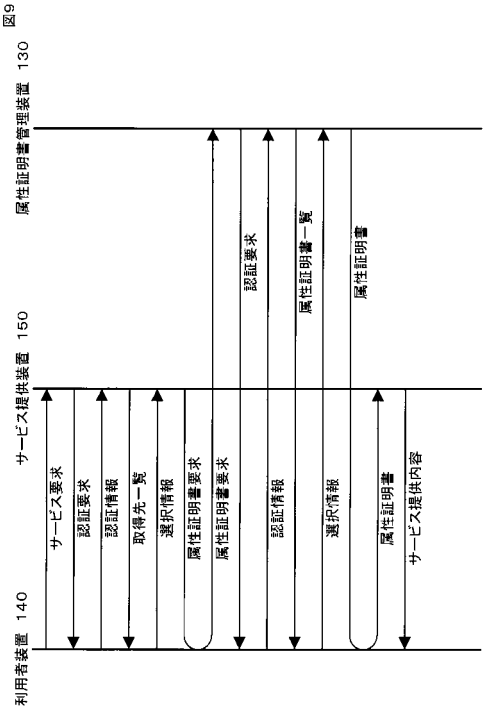
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000062
特許業務法人第一国際特許事務所
(72)発明者　笈川　光浩
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　馬場　健治
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】属性証明書管理方法及び装置

(57)【要約】
【課題】利用者装置に属性証明書を取り扱うための特別なソフトウェアを組み込むことなく、意図しない相手に属性証明書を提示しないよう、属性証明書の管理を適切に実現する。
【解決手段】属性証明書の管理方法及び装置において、利用者の属性証明書を属性証明書管理装置内で保管しておき、利用者がもつ標準的なパーソナルコンピュータの環境で使用可能な機能のみを用いて、サービス提供装置の要求に応じて利用者装置は属性証明書管理装置にアクセスし、開示する属性証明書もしくは属性証明書のポインタを属性証明書管理装置から利用者装置を介してサービス提供者に提示することで、サービス利用者側に特別なプログラムを導入させることなく、意図しない相手に属性証明書を提示しないようにすることを実現する。
【選択図】図９

図9



【特許請求の範囲】
【請求項１】
属性証明書管理装置とサービス提供装置と利用者装置がネットワークにより接続された属性証明書管理システムにおいて、ネットワーク上でサービスを提供するサービス提供装置が、前記サービスを利用しようとする利用者の属性情報を確認する際の属性証明書管理方法であって、
前記属性証明書管理装置は、利用者の属性証明書の管理を行う属性証明書開示部を備え、かつ、当該属性証明書管理装置内には利用者の属性証明書が予め保管されている状況において、
前記サービス提供装置は、前記利用者が利用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信する認証要求ステップを実行し、
前記利用者装置は、前記認証要求を受信し、認証情報の生成及び送信を行う認証情報送信ステップを実行し、
前記サービス提供装置は、前記認証情報を受信し、利用者の認証を行うといったサービス提供装置側利用者認証ステップを実行し、
前記サービス提供装置は、属性証明書の取得先情報を取得する属性証明書取得先取得ステップを実行し、
前記サービス提供装置は、前記利用者経由で、取得した属性証明書の取得先である前記属性証明書管理装置に、属性証明書を要求するためのメッセージを送信する属性証明書要求ステップを実行し、
前記利用者装置は、属性証明書を要求するためのメッセージを受信し、属性証明書管理装置に転送する属性証明書要求転送ステップを実行し、
前記属性証明書管理装置は、属性証明書を要求するためのメッセージを受信する属性証明書要求受信ステップを実行し、
前記属性証明書管理装置は、属性証明書を要求するためのメッセージを送信してきた利用者装置の認証を行う属性証明書管理装置側利用者認証ステップを実行し、
前記属性証明書管理装置は、サービス提供者に提示してもよい属性証明書を選択するという属性証明書選択ステップを実行し、
前記属性証明書管理装置は、選択した属性証明書を、前記利用者経由で、前記サービス提供装置に送信する属性証明書送信ステップを実行し、
前記利用者装置は、属性証明書を受信し、サービス提供装置に転送する属性証明書転送ステップを実行し、
前記サービス提供装置は、属性証明書を受信し、当該属性証明書を検証し、属性証明書内の属性情報をもとにサービスの認可を行い、認可結果に応じたサービスを実行する、認可ステップを実行する
ことを特徴とする属性証明書管理方法。
【請求項２】
属性証明書管理装置とサービス提供装置と利用者装置がネットワークにより接続された属性証明書管理システムにおいて、
ネットワーク上でサービスを提供する複数のサービス提供装置に対して、属性証明書管理装置で属性証明書の開示権限を設定するために、
前記属性証明書管理装置は、前記利用者が使用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信する認証要求ステップを実行し、
前記利用者装置は、前記認証要求を受信し、認証情報の生成及び送信を行う認証情報送信ステップを実行し、
前記属性証明書管理装置は、前記認証情報を受信し、利用者の認証を行う利用者認証ステップを実行し、
前記属性証明書管理装置は、前記利用者の属性証明書の開示権限の登録、変更あるいは削除を行うための要求を利用者装置から受信した場合に、当該要求に応じた設定情報を入力する画面の情報を利用者装置に送信する設定画面送信ステップを実行し、

前記利用者装置は、設定情報を入力するための画面の情報を受信、表示し、属性証明書の開示の登録、変更あるいは削除に必要な設定情報を利用者に入力させ、入力された情報を属性証明書管理装置に送信する設定情報入力ステップを実行し、
前記属性証明書管理装置は、前記設定情報を受信し、属性証明書管理装置内の設定情報に反映する開示権限設定ステップを実行し、
さらに、ネットワーク上でサービスを提供するサービス提供装置が、前記サービスを利用しようとする利用者の属性情報を確認するために、
前記属性証明書管理装置は、利用者の属性証明書の管理を行う属性証明書開示部を備え、かつ、当該属性証明書管理装置内には利用者の属性証明書が予め保管されている状況において、
前記サービス提供装置は、前記利用者が利用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信する認証要求ステップを実行し、
前記利用者装置は、前記認証要求を受信し、認証情報の生成及び送信を行う利用者認証情報送信ステップを実行し、
前記サービス提供装置は、前記認証情報を受信し、利用者の認証を行う利用者認証ステップを実行し、
前記サービス提供装置は、属性証明書管理装置に、属性証明書を要求するためのメッセージを送信する属性証明書要求ステップを実行し、
前記属性証明書管理装置は、属性証明書を要求するためのメッセージを受信する属性証明書要求受信ステップを実行し、
前記属性証明書管理装置は、前記サービス提供装置からのアクセスに応じ、サービス提供装置に対して認証要求を送信するサービス提供装置認証要求ステップを実行し、
前記サービス提供装置は、前記認証要求を受信し、認証情報の生成及び送信を行うサービス提供装置認証情報送信ステップを実行し、
前記属性証明書管理装置は、前記認証情報を受信し、サービス提供装置の認証を行うサービス提供装置認証ステップを実行し、
前記属性証明書管理装置は、当該サービス提供者に開示権限を与えられている属性証明書を取得する属性証明書取得ステップを実行し、
前記属性証明書管理装置は、選択した属性証明書及びその関連情報を、前記サービス提供装置に送信する属性証明書情報送信ステップを実行し、
前記サービス提供装置は、属性証明書情報を受信し、当該属性証明書を検証し、属性証明書内の属性情報をもとにサービスの認可を行い、認可結果に応じたサービスを実行する、認可ステップを実行する
ことを特徴とする属性証明書管理方法。
【請求項３】
属性証明書管理装置とサービス提供装置と利用者装置がネットワークより接続された属性証明書管理システムにおいて、ネットワーク上でサービスを提供するサービス提供装置が、前記サービスを利用しようとする利用者の属性情報を確認する際の属性証明書管理方法であって、
属性証明書管理装置は、利用者の属性証明書の管理を行う属性証明書開示部を備え、かつ、当該属性証明書管理装置内には利用者の属性証明書が予め保管されている状況において、
前記サービス提供装置は、前記利用者が利用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信する認証要求ステップを実行し、
前記利用者装置は、前記認証要求を受信し、認証情報の生成及び送信を行う認証情報送信ステップを実行し、
前記サービス提供装置は、前記認証情報を受信し、利用者の認証を行うサービス提供装置側利用者認証ステップを実行し、
前記サービス提供装置は、属性証明書の取得先情報を取得する属性証明書取得先取得ステップを実行し、

前記サービス提供装置は、前記利用者経由で、取得した属性証明書の取得先である前記属性証明書管理装置に、属性証明書を要求するためのメッセージを送信する属性証明書要求ステップを実行し、
前記利用者装置は、属性証明書を要求するためのメッセージを受信し、属性証明書管理装置に転送する属性証明書要求転送ステップを実行し、
前記属性証明書管理装置は、属性証明書を要求するためのメッセージを受信する属性証明書要求受信ステップを実行し、
前記属性証明書管理装置は、属性証明書を要求するためのメッセージを送信してきた利用者装置の認証を行う属性証明書管理装置側利用者認証ステップを実行し、
前記属性証明書管理装置は、サービス提供者に提示してもよい属性証明書を選択する属性証明書選択ステップを実行し、
前記属性証明書管理装置は、選択した属性証明書に関連するポインタ情報を、前記利用者経由で、前記サービス提供装置に送信する属性証明書ポインタ情報送信ステップを実行し、
前記利用者装置は、属性証明書ポインタ情報を受信し、サービス提供装置に転送する属性証明書ポインタ情報転送ステップを実行し、
前記サービス提供装置は、属性情報ポインタ情報を受信し、当該ポインタ情報にも基づいて属性証明書を要求するためのメッセージを属性証明書管理装置に送信する属性証明書要求ステップを実行し、
前記属性証明書管理装置は、前記サービス提供装置からのアクセスに応じ、サービス提供装置に対して認証要求を送信するサービス提供装置認証要求ステップを実行し、
前記サービス提供装置は、前記認証要求を受信し、認証情報の生成及び送信を行うサービス提供装置認証情報送信ステップを実行し、
前記属性証明書管理装置は、前記認証情報を受信し、サービス提供装置の認証を行うサービス提供装置認証ステップを実行し、
前記属性証明書管理装置は、属性証明書を要求するためのメッセージを受信する属性証明書要求受信ステップを実行し、
前記属性証明書管理装置は、当該サービス提供者に開示権限を与えられている属性証明書を取得するという属性証明書取得ステップを実行し、
前記属性証明書管理装置は、選択した属性証明書及びその関連情報を、前記サービス提供装置に送信する属性証明書情報送信ステップを実行し、
前記サービス提供装置は、属性証明書情報を受信し、当該属性証明書を検証し、属性証明書内の属性情報をもとにサービスの認可を行い、認可結果に応じたサービスを実行する、認可ステップを実行する
ことを特徴とする属性証明書管理方法。
【請求項４】
請求項１あるいは請求項３に記載の属性証明書管理方法において、
前記属性証明書取得先取得ステップは、
前記サービス提供装置が、属性証明書取得先の一覧を利用者装置に送信し、
前記利用者装置が、属性証明書取得先の一覧を受信、表示し、当該一覧の中から、属性証明書の取得先を利用者に選択させ、選択した属性証明書の取得先に関する情報を前記サービス提供装置に送信することで具現化される
ことを特徴とする属性証明書管理方法。
【請求項５】
請求項１あるいは請求項３に記載の属性証明書管理方法において、
前記認可ステップは、
前記サービス提供装置が、サービスの認可に成功した場合の属性証明書の取得先情報を予め記録しておくことを含むことで具現化され、
前記属性証明書取得先取得ステップは、
前記サービス提供装置が、過去に実施された認可ステップによって記録された前記取得

先情報を読み出すことで具現化される
ことを特徴とする属性証明書管理方法。
【請求項６】
請求項１あるいは請求項３に記載の属性証明書管理方法において、
前記属性証明書管理装置側利用者認証ステップは、
前記サービス提供装置が、前記利用者が利用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信し、
前記利用者装置が、前記認証要求を受信し、認証情報の生成及び送信を行い、
前記サービス提供装置は、前記認証情報を受信し、利用者の認証を行うことで具現化される
ことを特徴とする属性証明書管理方法。
【請求項７】
請求項１あるいは請求項３に記載の属性証明書管理方法において、
前記属性証明書要求ステップは、
前記サービス提供装置が、属性証明書要求に認証済みであることを示す認証済み情報を含めることで具現化され
前記属性証明書管理装置側利用者認証ステップは、
前記属性証明書管理装置が、利用者認証として当該認証済み情報の検証を行うことで具現化される
ことを特徴とする属性証明書管理方法。
【請求項８】
請求項１あるいは請求項３に記載の属性証明書管理方法において、
前記属性証明書選択ステップは、
前記属性証明書管理装置が、認証された利用者の属性証明書の一覧を利用者装置に送信するという属性証明書一覧送信ステップを実行し、
前記利用者装置が、属性証明書の一覧を受信、表示し、当該一覧の中から、サービス提供装置に提示してもよい属性証明書を利用者に選択させ、選択した属性証明書に関する情報を前記属性証明書管理装置に送信するという属性証明書利用者選択ステップを実行し、
前記属性証明書管理装置が、選択された属性証明書に関する情報を受信するという属性証明書選択情報受信ステップを実行することで具現化される
ことを特徴とする属性証明書管理方法。
【請求項９】
請求項８に記載の属性証明書管理方法において、
前記属性証明書一覧送信ステップは、
前記属性証明書管理装置に保管されている前記利用者の属性証明書の中でも、有効かつ属性条件の適したもののみを利用者の属性証明書の一覧として、属性証明書の一覧を利用者装置に送信することで具現化される
ことを特徴とする属性証明書管理方法。
【請求項１０】
請求項８に記載の属性証明書管理方法において、
前記属性証明書一覧送信ステップは、
前記属性証明書管理装置に予め記録してあるサービス提供装置のホワイトリストもしくはブラックリストと比較して、提示するにふさわしいもののみを利用者の属性証明書の一覧として、属性証明書の一覧を利用者装置に送信することで具現化される
ことを特徴とする属性証明書管理方法。
【請求項１１】
請求項２あるいは請求項３に記載の属性証明書管理方法において、
前記属性証明書送信ステップにおける属性証明書情報は、利用者の属性証明書と、当該属性証明書が暗号化されていた場合に、当該属性証明書の属性情報の暗号化に使用した１つ以上の暗号鍵を含むことで具現化され、

認可ステップは、
属性証明書内の属性情報をもとにサービスの認可を行う際に、前記暗号鍵を用いて属性情報の復号を行い、サービスの認可を行うことで具現化される
ことを特徴とする属性証明書管理方法。
【請求項１２】
ネットワーク上でサービスを提供するサービス提供装置が、前記サービスを利用しようとする利用者の属性情報を確認する際に用いるサービス提供装置であって、
前記利用者が使用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信する認証要求送信機能と、
前記利用者装置から受信した前記認証情報を用いて、利用者の認証を行う利用者認証機能と、
属性証明書の取得先情報を取得する属性証明書取得先取得機能と、
前記利用者経由で、取得した属性証明書の取得先に、属性証明書を要求するためのメッセージを送信する属性証明書要求送信機能と、
前記利用者経由で、利用者の属性証明書を受信し、当該属性証明書を検証し、属性証明書内の属性情報をもとにサービスの認可を行う認可機能と、を有する
ことを特徴とするサービス提供装置。
【請求項１３】
ネットワーク上でサービスを提供するサービス提供装置が、前記サービスを利用しようとする利用者の属性情報を確認する際に用いる属性証明書管理装置であって、
前記利用者の属性証明書を登録し、保管しておく属性証明書登録機能と、
利用者装置から属性証明書を要求するためのメッセージを受信する属性証明書要求受信機能と、
属性証明書を要求するためのメッセージを送信してきた利用者装置の認証を行う利用者認証機能と、
サービス提供者に提示してもよい属性証明書を選択するという属性証明書選択機能と、
選択した属性証明書もしくはそのポインタ情報を、前記利用者経由で、戻り先であるサービス提供装置に送信する属性証明書情報送信機能と、を有する
ことを特徴とする属性証明書管理装置。
【請求項１４】
ネットワーク上でサービスを提供するサービス提供装置が、前記サービスを利用しようとする利用者の属性情報を確認する際に用いる属性証明書管理装置であって、
前記利用者が使用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信する認証要求送信機能と、
前記利用者装置から前記認証情報を受信し、利用者の認証を行う利用者認証機能と、
前記利用者の属性証明書の開示権限の登録、変更あるいは削除を行うための要求を利用者装置から受信した場合に、当該要求に応じた設定情報を入力する画面の情報を利用者装置に送信する設定画面送信機能と、
前記利用者装置から設定情報を受信し、属性証明書管理装置内の設定情報に反映する開示権限設定機能と、を有する
ことを特徴とする属性証明書管理装置。
【請求項１５】
ネットワーク上でサービスを提供するサービス提供装置が、前記サービスを利用しようとする利用者の属性情報を確認する際に用いるサービス提供装置であって、
前記利用者が利用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信する認証要求送信機能と、
前記利用者装置から認証情報を受信し、利用者の認証を行う利用者認証機能と、
属性証明書管理装置に、属性証明書を要求するためのメッセージを送信する属性証明書要求送信機能と、
前記属性証明書管理装置から認証要求を受信し、認証情報の生成及び送信を行うサービ

ス提供装置認証情報送信機能と、
前記属性証明書管理装置から属性証明書情報を受信し、当該属性証明書を検証し、属性証明書内の属性情報をもとにサービスの認可を行う認可機能と、を有する
ことを特徴とするサービス提供装置。
【請求項１６】
請求項１４に記載された属性証明書管理装置であって、
更に、
サービス提供装置から属性証明書を要求するためのメッセージを受信する属性証明書要求受信機能と、
前記サービス提供装置からのアクセスに応じ、サービス提供装置に対して認証要求を送信するサービス提供装置認証要求機能と、
前記サービス提供装置から認証情報を受信し、サービス提供装置の認証を行うサービス提供装置認証機能と、
前記サービス提供者に開示権限を与えられている属性証明書を取得する属性証明書取得機能と、
選択した属性証明書及びその関連情報を、前記サービス提供装置に送信する属性証明書情報送信機能と、を有することを
ことを特徴とする属性証明書管理装置。
【請求項１７】
ネットワーク上でサービスを提供するサービス提供装置が、前記サービスを利用しようとする利用者の属性情報を確認する際に用いるサービス提供装置であって、
前記利用者が使用する利用者装置からのアクセスに応じ、利用者装置に対して認証要求を送信する認証要求送信機能と、
前記利用者装置から受信した前記認証情報を用いて、利用者の認証を行う利用者認証機能と、
属性証明書の取得先情報を取得する属性証明書取得先取得機能と、
前記利用者経由で、取得した属性証明書の取得先に、属性証明書を要求するためのメッセージを送信する属性証明書要求送信機能と、
前記利用者経由で、利用者の属性証明書にポインタ情報を受信する属性証明書ポインタ情報受信機能と、
属性証明書管理装置に、取得した属性証明書のポインタ情報を基に、属性証明書を要求するためのメッセージを送信する属性証明書要求送信機能と、
前記属性証明書管理装置から認証要求を受信し、認証情報の生成及び送信を行うサービス提供装置認証情報送信機能と、
前記属性証明書管理装置から利用者の属性証明書情報を受信し、当該属性証明書を検証し、属性証明書内の属性情報をもとにサービスの認可を行う認可機能と、を有する
ことを特徴とするサービス提供装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、属性証明書を用いたサービスを利用する者の利便性を向上させる場合に好適な属性証明書管理技術に関する。
【背景技術】
【０００２】
近年のＩＴの普及により、様々な情報が電子化され、ネットワークを介してやり取りされるようになってきている。このようなネットワークを介した情報のやり取りは、遠く離れた人とでも簡単かつ高速に行うことができる反面、通信相手が他人になりすますといった脅威も存在する。通信相手のなりすましを防ぐ方法の１つとして、公開鍵証明書を用いた認証方法が存在する。加えて、通信相手の本人性の確認だけでなく、資格や権限を確認する方法として、属性証明書を利用する方法も存在する（例えば、非特許文献１参照）。

【０００３】
ここで、公開鍵証明書とは、ある公開鍵の値と、当該公開鍵に対応した秘密鍵の所有者とを結びつけたデータのことである。このデータに認証局が電子署名を付与することによって、その内容が保証される仕組みとなっている。
【０００４】
一方、属性証明書とは、公開鍵証明書を特定するためのポインタ（例えば、公開鍵証明書の発行者名とシリアル番号など）と、公開鍵証明書の所有者が保持する属性情報（例えば、生年月日、性別、住所、役職、所属など）を結びつけたデータである。このデータに属性認証局が電子署名を付与することによって、その内容が保証される仕組みとなっている。
【０００５】
サービスで利用される属性情報は様々なので、属性証明書を利用するサービスが増えれば増えるほど、属性証明書の種類も多数存在する可能性がある。その場合、サービスの利用者は、複数の属性証明書を管理することになる。しかし、属性証明書内に含まれる属性情報には、特定の相手以外には開示したくないような個人情報などが含まれる事も多い。そのため、利用するサービスの提供者に応じて、提示すべき属性証明書を制御できるようにする事が望まれる。サービス利用者が必要以上の個人情報を開示することがなく、サービス提供者に適切な属性証明書を送付する方法として、特許文献１や特許文献２が存在している。
【特許文献１】特開２００３－３４５９３０号公報
【特許文献２】特開２００６－２６８７９０号公報
【非特許文献１】International Telecommunication Union著「Informationtechnology - Open systems interconnection - The Directory: Public-key andattribute certificate frameworks (ITU-T Recommendation X.509)」、（スイス）、InternationalTelecommunication Union、２０００年３月３１日、ｐ．１－１２９
【発明の開示】
【発明が解決しようとする課題】
【０００６】
意図しない相手に属性証明書を提示しないように管理する方法には、上述のとおり、特許文献１や特許文献２の方法が存在する。しかし、これらの方法はいずれもサービス利用者側に特別なプログラムを必要とするものである。サービス利用者の中には、情報リテラシの高くない者もいると考えられ、そのような場合において特別なプログラムを導入するという仕組みは望ましい形態ではない。また、特別なプログラムを入手するためには、当該プログラムの費用を利用者が負担しなければいけないということも考えられる。従って、サービス利用者側に特別なプログラムを必要とする仕組みは、属性証明書を利用するサービスの普及における阻害要因となっているため、サービス利用者の利便性をより向上させることが必要である。本発明は、上記の課題を解決するものである。
【課題を解決するための手段】
【０００７】
本発明は、属性証明書を用いてサービスの利用可否を判定するようなＷｅｂサービスシステムにおいて、当該サービスを利用するために必要となる属性証明書を属性証明書管理システム内で保管しておくことで、サービスの利用時には、サービス利用者がパーソナルコンピュータを購入した時点から一般的に使用可能なＷｅｂブラウザを介して、サービス提供者に提示できるようにする。また、上記属性証明書管理システムに、サービス提供者毎の属性証明書のアクセス権を設定しておくことで、サービス提供装置が直接属性証明書管理システムにサービスの属性証明書を要求してきた場合でも、適切な属性証明書のみを開示できるようにする。上述の装置及び方法によって、サービス利用者側に特別なプログラムを導入させることなく、意図しない相手に属性証明書を提示しないような属性証明書の管理を実現する。
【発明の効果】

【０００８】
本発明によれば、サービス利用者側に特別なプログラムを導入する必要がないので、サービス利用者にかかる負担を低減できる。結果として、属性証明書を利用するサービスシステムの導入を容易にする効果をもたらす。
【発明を実施するための最良の形態】
【０００９】
以下、本発明による好適な実施形態を、図面を用いて説明する。なお、以下で説明する図面において、同一の番号は同様の部品・要素を表すものとする。また、これにより本発明が限定されるものではない。
【実施例１】
【００１０】
図１は、本実施例を適用するためのシステム構成を示す図である。あるエンティティ（本実施例の例では利用者装置１４０を使用する利用者）に対して公開鍵証明書を発行する認証局装置１１０と、認証局装置１１０によって発行された公開鍵証明書に前記エンティティの属性情報を割り付けた属性証明書を発行する属性認証局装置１２０と、属性認証局装置１２０によって発行された前記エンティティの属性証明書を管理する属性証明書管理装置１３０と、サービスの利用者が使用する装置である利用者装置１４０と、資格の認証を伴うサービスを提供する装置であるサービス提供装置１５０と、がネットワーク１６０で接続されている。
【００１１】
図２は、各装置のハードウェア構成を示す図である。認証局装置１１０、属性認証局装置１２０、属性証明書管理装置１３０、利用者装置１４０、サービス提供装置１５０は、入力装置２１０と、表示装置２２０と、ＣＰＵ２３０と、メモリ２４０と、記憶装置２５０と、通信装置２６０と、これらを接続するバス２７０とから構成されている。
【００１２】
入力装置２１０は、装置を利用する人が、データや命令等を入力するために操作されるものであり、キーボード、マウス、生体情報の入力装置、その他認証に必要な装置等で構成される。
【００１３】
表示装置２２０は、装置を利用する人に対してメッセージ等を表示するために用いられるものであり、ＣＲＴや液晶ディスプレイ等で構成される。
【００１４】
ＣＰＵ２３０は、メモリ２４０や記憶装置２５０に格納されたプログラムを実行することで、装置の各構成要素を制御したり、様々な演算処理を行ったりして、以下に説明する様々な処理を実現する。
【００１５】
メモリ２４０は、図３から図７に示すようなプログラムや、処理に必要なデータが一時的に格納されるものであり、ＲＡＭ等の揮発性記憶媒体で構成することが多い。
【００１６】
記憶装置２５０は、装置内で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスク等の不揮発性記憶媒体で構成される。
【００１７】
通信装置２６０は、ネットワーク１６０を介して他の装置とデータの送受信を行うために必要な物理的インタフェースであり、ＬＡＮボードや無線ＬＡＮカード等で構成される。
【００１８】
図３は、認証局装置１１０の構成を示す図である。認証局装置１１０のメモリ２４０には、オペレーティングシステム３１０と、公開鍵証明書発行プログラム３２０と、失効情報発行プログラム３３０がロードされている領域である。これらのプログラムは、必要に応じて、ＣＰＵ２３０により実行され、後に説明する機能を実現する。

【００１９】
また、認証局装置１１０の記憶装置２５０には、認証局の所有する秘密鍵３５０と、当該秘密鍵に対応した認証局の公開鍵証明書３６０と、当該認証局が発行した公開鍵証明書に関する失効情報３７０と、当該認証局が各利用者に対して発行した公開鍵証明書３８０等のデータが格納されている。
【００２０】
次に、各プログラムの機能を説明する。各プログラムは、それぞれが格納されている装置内で読み出されＣＰＵ２３０によって実行されることにより、その機能が実現されるものであるが、説明の便宜上、各プログラムを実行主体として説明する。
【００２１】
図３において、オペレーティングシステム３１０は、装置全体の制御を行うために、ファイル管理、プロセス管理、デバイス管理といった機能を実現するためのプログラムである。
【００２２】
公開鍵証明書発行プログラム３２０は、ある利用者に関して、当該利用者の識別名とユーザの所有する公開鍵とを結びつけ、この結びつけた情報に対し認証局の秘密鍵３５０を用いて電子署名を施した公開鍵証明書を発行するプログラムである。本実施例においては、当該プログラムによって、ルート証明書となる認証局の公開鍵証明書３６０と、属性認証局装置１２０を運用する属性認証局の公開鍵証明書４６０と、利用者装置１４０を使用する利用者の公開鍵証明書３８０を発行する。
【００２３】
失効情報発行プログラム３３０は、当該認証局が発行した公開鍵証明書に関して、失効されている公開鍵証明書の情報の一覧に、当該認証局の秘密鍵３５０を用いて電子署名を施した失効情報３７０を生成するプログラムである。当該プログラムによって生成された失効情報３７０は記憶装置２５０内で保管される。
【００２４】
認証局の秘密鍵３５０は、公開鍵証明書を発行する際に認証局の電子署名を付与する際に用いる暗号鍵である。当該秘密鍵３５０は、認証局が所有する秘密鍵情報であり、当該認証局内で安全に管理されるものとする。本実施例においては、認証局装置の記憶装置２５０の内部で管理するものとしているが、ハードウェアセキュリティモジュール等を用いて管理してもよい。
【００２５】
認証局の公開鍵証明書３６０は、認証局が自身に対して発行した自己署名の公開鍵証明書である。当該公開鍵証明書に記載された公開鍵と、前記秘密鍵３５０は一対の鍵ペアをなすものである。
【００２６】
失効情報３７０は、公開鍵証明書が失効しているかどうかを確認するために用いられる情報である。例えば、証明書失効リスト（ＣＲＬ）等が該当する。
【００２７】
利用者の公開鍵証明書３８０は、公開鍵証明書発行プログラム３２０によって発行された利用者用の公開鍵証明書である。
【００２８】
図４は、本実施例に関連する属性認証局装置１２０の構成を示す図である。
【００２９】
属性認証局装置１２０のメモリ２４０には、オペレーティングシステム４１０と、属性証明書発行プログラム４２０と、属性証明書失効情報発行プログラム４３０がロードされている。これらのプログラムは、必要に応じて、ＣＰＵ２３０により実行され、後に説明する機能を実現する。
【００３０】
また、属性認証局装置１２０の記憶装置２５０には、属性認証局の所有する秘密鍵４５

０と、当該秘密鍵に対応した属性認証局の公開鍵証明書４６０と、当該属性認証局が発行した属性証明書に関する失効情報４７０と、当該属性認証局が各利用者に対して発行した属性証明書４８０等のデータが格納されている。

【００３１】

次に、各プログラムの機能を説明する。各プログラムは、それぞれが格納されている装置内で読み出されＣＰＵ２３０によって実行されることにより、その機能が実現されるものであるが、説明の便宜上、各プログラムを実行主体として説明する。

【００３２】

図４において、オペレーティングシステム４１０は、装置全体の制御を行うために、ファイル管理、プロセス管理、デバイス管理といった機能を実現するためのプログラムである。

【００３３】

公開鍵証明書発行プログラム３２０は、ある利用者に関して、当該利用者の識別名とユーザの所有する公開鍵とを結びつけ、この結びつけた情報に対し認証局の秘密鍵３５０を用いて電子署名を施した公開鍵証明書を発行する。

【００３４】

属性証明書発行プログラム４２０は、公開鍵証明書を所有している或る利用者に関して、当該利用者の公開鍵証明書情報と当該利用者の属性情報とを結びつけ、この結びつけた情報に対し属性認証局の秘密鍵４５０を用いて電子署名を施した属性証明書を発行するプログラムである。本実施例においては、当該プログラムによって、利用者装置１４０を使用する利用者の属性証明書４８０を発行する。

【００３５】

属性証明書失効情報発行プログラム４３０は、属性認証局が発行した属性証明書に関して、失効されている属性証明書の情報の一覧に、当該属性認証局の秘密鍵４５０を用いて電子署名を施した失効情報４７０を生成するプログラムである。当該プログラムによって生成された失効情報は記憶装置２５０内で保管される。

【００３６】

属性認証局の秘密鍵４５０は、属性証明書を発行する際に属性認証局の電子署名を付与する際に用いる暗号鍵である。当該秘密鍵４５０は、属性認証局が所有する秘密鍵情報であり、当該属性認証局内で安全に管理されるものとする。本実施例においては、属性認証局装置の記憶装置２５０の内部で管理するものとしているが、ハードウェアセキュリティモジュール等を用いて管理してもよい。

【００３７】

属性認証局の公開鍵証明書４６０は、認証局装置１１０によって発行された当該属性認証局用の公開鍵証明書である。当該公開鍵証明書に記載された公開鍵と、前記秘密鍵４５０は一対の鍵ペアをなすものである。

【００３８】

属性証明書失効情報４７０は、属性証明書が失効しているかどうかを確認するために用いられる情報である。例えば、属性証明書失効リスト（ＡＣＲＬ）等が該当する。

【００３９】

利用者の属性証明書４８０は、利用者の公開鍵証明書３８０に結びつく属性情報を含む属性証明書として、属性証明書発行プログラム４２０を用いて発行された利用者用の属性証明書である。

【００４０】

図５は、本実施例に関連する属性証明書管理装置１３０のソフトウェア構成を示す図である。

【００４１】

属性証明書管理装置１３０のメモリ２４０には、オペレーティングシステム５１０と、属性証明書登録プログラム５２０と、属性証明書開示プログラム５３０がロードされている領域である。これらのプログラムは、必要に応じて、ＣＰＵ２３０により実行され、後

に説明する機能を実現する。

【００４２】

また、属性証明書管理装置１３０の記憶装置２５０には、利用者の属性証明書４８０と、アクセス制御情報５５０等のデータが格納されている。実施形態に応じて、さらに、属性開示に関する設定情報５６０や暗号化鍵５７０が格納される。

【００４３】

次に、各プログラムの機能を説明する。各プログラムは、それぞれが格納されている装置内で読み出されＣＰＵ２３０によって実行されることにより、その機能が実現されるものであるが、説明の便宜上、各プログラムを実行主体として説明する。

【００４４】

図５において、オペレーティングシステム５１０は、装置全体の制御を行うために、ファイル管理、プロセス管理、デバイス管理といった機能を実現するためのプログラムである。

【００４５】

属性証明書登録プログラム５２０は、ある利用者の属性証明書を、属性証明書管理装置１３０内に登録するためのプログラムである。当該プログラムは、属性認証局装置１２０から直接属性証明書の登録を受け付ける、あるいは、利用者の要求に応じて属性証明書の登録を受け付ける。

【００４６】

属性証明書開示プログラム５３０は、属性証明書登録プログラム５２０によって登録された利用者の属性証明書を開示するプログラムである。当該プログラムでは、利用者自身が開示を要求する場合と属性証明書の内容を確認しようとする者（本実施例の例ではサービス提供者）が開示を要求する場合がある。利用者自身が属性証明書の開示を要求してきた場合には、要求した者が正当な属性証明書の所有者であることをアクセス制御情報５５０に基づいて認証した上で、属性証明書の開示を行う。

【００４７】

また、サービス提供者等が属性証明書の開示を要求してきた場合には、要求した者が誰であるかをアクセス制御情報５５０に基づいて認証し、さらに当該者が属性証明書の開示権限を有しているかを属性開示に関する設定情報５６０に基づいて判定した上で、属性証明書の開示を行う。当該開示プログラムは、属性開示に関する設定情報５６０の登録、変更、削除に関する設定機能も有している。

【００４８】

格納されている利用者の属性証明書は、場合によっては、属性情報単位に異なる暗号化鍵を用いて暗号化されているものも存在する。このような暗号化属性証明書を取り扱う場合には、開示してもよい属性情報を暗号化した暗号化鍵５７０と暗号化属性証明書と併せて当該者に送付する。

【００４９】

アクセス制御情報５５０は、属性証明書管理装置１３０にアクセスを要求してきた者の認証や、当該装置内の各プログラムを利用する権限があるかを確認する際に用いられるポリシー情報である。ＰＫＩでの認証におけるトラストアンカー情報、属性証明書管理装置の運用者が定めた要求者のホワイトリストやブラックリストも当該アクセス制御情報に含まれるものとする。

【００５０】

属性開示に関する設定情報５６０は、利用者の属性証明書を、利用者以外の者に開示する際に必要な条件を定めた情報である。例えば、属性証明書単位もしくはその中に含まれる属性情報単位に、開示可能な者が割り当てられているデータである。暗号化属性証明書が使われる場合には、暗号化鍵との対応関係も当該設定情報内に割り当てられる。暗号化鍵５７０は、暗号化属性証明書における属性情報の暗号化に用いた暗号鍵のことである。

【００５１】

図６は、利用者装置１４０の構成を示す図である。

【００５２】

利用者装置１４０のメモリ２４０には、オペレーティングシステム６１０と、Ｗｅｂブラウザプログラム６２０とがロードされている。これらのプログラムは、必要に応じて、ＣＰＵ２３０により実行され、後に説明する機能を実現する。

【００５３】

また、メモリ領域２５０には、利用者の秘密鍵６５０と、利用者の公開鍵証明書３８０が格納されている。

【００５４】

次に、各プログラムの機能を説明する。各プログラムは、それぞれが格納されている装置内で読み出されＣＰＵ２３０によって実行されることにより、その機能が実現されるものであるが、説明の便宜上、各プログラムを実行主体として説明する。

【００５５】

図６において、オペレーティングシステム６１０は、装置全体の制御を行うために、ファイル管理、プロセス管理、デバイス管理といった機能を実現するためのプログラムである。

【００５６】

Ｗｅｂブラウザプログラム６２０は、ネットワーク上のＷｅｂサーバに公開されたＨＴＭＬファイル、画像ファイル、音楽ファイル等をダウンロードし、レイアウトを解析して表示あるいは再生するプログラムであり、フォームを使用してユーザがデータをＷｅｂサーバに送信することや、Ｊａｖａ（登録商標）等で記述されたプログラムを動作することも可能なプログラムである。また、ＳＳＬもしくはＴＬＳ通信を行うために必要な暗号処理を行う機能と鍵及び証明書を管理する機能も当該プログラムに含むものとする。

【００５７】

利用者の秘密鍵６５０は、利用者装置１４０のＷｅｂブラウザプログラム６２０によって生成された秘密鍵もしくは認証局装置１３０によって生成された利用者用の秘密鍵をインポートしたものである。

【００５８】

利用者の公開鍵証明書３８０は、認証局装置１１０によって生成された利用者用の公開鍵証明書を、Ｗｅｂブラウザプログラム６２０によってインポートしたものである。

【００５９】

図７は、サービス提供装置１５０の構成を示す図である。サービス提供装置１５０のメモリ２４０には、オペレーティングシステム７１０と、サービス提供プログラム７２０と、認証・認可プログラム７３０とがロードされている。これらのプログラムは、必要に応じて、ＣＰＵ２３０により実行され、後に説明する機能を実現する。

【００６０】

また、メモリ領域２５０には、サービス提供用データ７５０と、アクセス制御情報７６０と、属性の条件に関する情報７７０が格納されている。また、実施形態に応じて、属性証明書取得先情報７８０、サービス提供装置の秘密鍵７９０、サービス提供装置７９１が格納されている。

【００６１】

次に、各プログラムの機能を説明する。各プログラムは、それぞれが格納されている装置内で読み出されＣＰＵ２３０によって実行されることにより、その機能が実現されるものであるが、説明の便宜上、各プログラムを実行主体として説明する。

【００６２】

図７において、オペレーティングシステム７１０は、装置全体の制御を行うために、ファイル管理、プロセス管理、デバイス管理といった機能を実現するためのプログラムである。

【００６３】

サービス提供プログラム７２０は、サービス提供者によって提供されるネットワークサ

ービスの受付や応答を行うプログラムである。Ｗｅｂサーバの機能とその上位で動作するアプリケーションプログラム等が当該プログラムに該当する。

【００６４】

認証・認可プログラム７３０は、他の装置からネットワークを介してアクセス要求があった場合などに、アクセス要求してきた利用者が誰であるかを認証し、アクセス要求されたサービスに対して権限のある者だけに利用を認可するプログラムである。認証の機能については、例えば、ＳＳＬもしくはＴＬＳによるクライアント認証機能を有したサーバによって実現される。認可の機能については、利用者の属性証明書を用いて判定を行うので、属性証明書の取得から判定を行うまでの一連の処理を当該プログラムが実施することになる。

【００６５】

サービス提供用データ７５０は、サービス提供者がサービスを提供する際に用いるデータであり、サービス提供プログラム７２０によって使用されるものである。

【００６６】

アクセス制御情報７６０は、サービス提供装置１５０にアクセスを要求してきた者の認証や、当該装置が提供するサービスを利用する権限があるかを確認する際に用いられるポリシー情報である。ＰＫＩでの認証におけるトラストアンカー情報、利用者の属性情報に応じたサービスの提供範囲を定めた情報がアクセス制御情報に含まれる。

【００６７】

属性の条件に関する情報７７０は、利用者に提示してもらいたい属性情報の種類を定めた情報である。属性証明書取得先情報７８０は、利用者の属性証明書の取得先を記録した情報である。例えば、利用者ごとに取得先のＵＲＬもしくは取得先を識別可能な情報が割り当てられたデータである。

【００６８】

サービス提供装置の秘密鍵７９０は、サービス提供装置１５０が属性証明書管理装置１３０にアクセスする際の認証に用いるための暗号鍵である。サービス提供装置が所有する秘密鍵情報であり、当該サービス提供装置局内で安全に管理されるものとする。本実施例においては、サービス提供装置１５０内の記憶装置２５０の内部で管理するものとしているが、ハードウェアセキュリティモジュール等を用いて管理してもよい。

【００６９】

サービス提供装置の公開鍵証明書７９１は、認証局装置１１０によって発行された当該サービス提供装置用の公開鍵証明書である。当該公開鍵証明書に記載された公開鍵と、前記秘密鍵７９０は一対の鍵ペアをなすものである。

【００７０】

図８は、本実施例で用いる、利用者の公開鍵証明書３８０、及び、属性証明書４８０のデータ仕様を示す図である。利用者の公開鍵証明書３８０は、従来技術であるＸ．５０９の仕様に基づくものとする。具体的には、公開鍵証明書シリアル番号、公開鍵証明書の発行者名、公開鍵証明書のサブジェクト名、公開鍵証明書の有効期間、公開鍵情報等の要素を署名対象に含むデータであり、認証局の秘密鍵３５０によって電子署名が付与される。公開鍵証明書シリアル番号と公開鍵証明書の発行者の組み合わせは、一般的に公開鍵証明書を一意に特定するものであり、その組み合わせを公開鍵証明書のポインタとする。

【００７１】

利用者の属性証明書４８０も、従来技術であるＸ．５０９の仕様に基づくものとする。具体的には、利用者の公開鍵証明書の発行者名、利用者の公開鍵証明書シリアル番号、属性証明書の発行者名、属性証明書の有効期間、属性情報等の要素を署名対象に含むデータであり、属性認証局の秘密鍵４５０によって電子署名が付与される。利用者の公開鍵証明書の発行者名と利用者の公開鍵証明書シリアル番号に記載する値は、利用者の公開鍵証明書３８０のシリアル番号と発行者名に一致させることで、公開鍵証明書と属性証明書を対応づける。

【００７２】

図９は、本発明の実施形態に係る属性証明書管理装置を用いた資格認証の処理フロー概要を示す図である。利用者装置１４０と、サービス提供装置１５０と、属性証明書管理装置１３０との間において、サービス提供装置１５０が属性証明書を用いて利用者の資格や属性を確認するための手順について記述する。

【００７３】

図９において、利用者装置１４０は、サービス提供装置１５０にサービス要求を送信する。当該サービス提供装置は、当該利用者装置に対して認証要求を送信する。当該利用者装置は、認証要求を受け、認証情報を生成し、当該サービス提供装置に送信する。当該サービス提供装置は、認証情報からアクセスしてきた相手の認証を行った上で、属性証明書の取得先一覧を当該利用者装置に送信する。当該利用者装置は、属性証明書の取得先一覧を表示し、それを利用者に選択させ、選択された情報を当該サービス提供装置に送信する。

【００７４】

当該サービス提供装置は、受信した取得先の情報に基づき、属性証明書を取得するための要求を利用者装置経由で属性証明書管理装置に送信する。当該属性証明書管理装置は、当該利用者装置に対して認証要求を送信する。当該利用者装置は、認証要求を受け、認証情報を生成し、当該属性証明書管理装置に送信する。当該属性証明書管理装置は、認証情報からアクセスしてきた相手の認証を行った上で、属性証明書の一覧を当該利用者装置に送信する。当該利用者装置は、属性証明書の一覧を表示し、それを利用者に選択させ、選択された情報を当該属性証明書管理装置に送信する。

【００７５】

当該属性証明書管理装置は、属性証明書を、当該利用者装置経由で、属性証明書の要求元である当該サービス提供装置に送信する。当該サービス提供装置は、受信した属性証明書の検証を行った結果に応じて、当該利用者装置に、サービス提供内容を送信する。以上が本発明における属性証明書の管理方法の実施形態の１つとなる。

【００７６】

図１０、図１１及び図１２は、図９の内容の詳細な処理フロー示す図である。

【００７７】

図１０において、利用者装置１４０では、Ｗｅｂブラウザプログラム６２０を起動し、サービス提供装置１５０が提供するサービスにアクセスするためのＵＲＬを入力し、サービス提供装置１５０に対してサービス要求を送信する（ステップ２００１）。

【００７８】

サービス提供装置１５０では、利用者装置１４０が送信したサービス要求をサービス提供プログラム７２０にて受信する（ステップ２００２）。

上記ステップにてサービス要求を受信したら、サービス提供プログラム７２０は、利用者の認証を行うために必要な認証情報の要求、すなわち、認証要求を、利用者装置１４０に送信する。例えば、ＳＳＬ（Secure Socket Layer）あるいはＴＬＳ（Transport Layer Security）によるクライアント認証の要求が本ステップに相当する（ステップ２００３）。

【００７９】

利用者装置１４０では、上記ステップ２００３にて送信された認証要求を、Ｗｅｂブラウザプログラム６２０にて受信する（ステップ２００４）。

【００８０】

続いて、利用者装置１４０では、Ｗｅｂブラウザプログラム６２０を用いて、認証要求に応じた認証情報を生成する。例えば、ＳＳＬあるいはＴＬＳにおける認証であれば、利用者の秘密鍵６５０を用いた電子署名データを生成することに相当する（ステップ２００５）。

【００８１】

さらに、利用者装置１４０は、上記ステップ２００５にて生成した認証情報及び当該認証情報を検証するために必要なその他の情報を、サービス提供装置１５０に送信する。例

えば、ＳＳＬあるいはＴＬＳによる認証の場合、利用者装置１４０からサービス提供装置１５０に送信される情報として、電子署名データの他に、利用者の公開鍵証明書３８０も送信される（ステップ２００６）。

【００８２】

サービス提供装置１５０では、利用者装置１４０が送信した認証情報をサービス提供プログラム７２０にて受信する（ステップ２００７）。

【００８３】

続いて、サービス提供装置１５０では、認証・認可プログラム７３０によって、利用者装置１４０が送信した認証情報を検証し、ユーザの認証を行う。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、利用者装置から送信された電子署名データを、利用者の公開鍵証明書３８０を用いて検証を行うとともに、利用者の公開鍵証明書３８０の認証パスを検証し、当該サービス提供装置が予め設定しているトラストアンカーの証明書まで辿れることを確認することに相当する。

【００８４】

なお、トラストアンカーとなる証明書は、アクセス制御情報７６０に含むものとする。また、必要に応じて、認証局装置１１０にアクセスして失効情報３７０を取得し、当該失効情報に基づいた利用者の公開鍵証明書３８０の有効性確認も行う（ステップ２００８）。

【００８５】

上記ステップ２００８にて、ユーザの認証が完了したら、サービス提供装置１５０の認証・認可プログラム７３０は、当該利用者の属性証明書の取得先を検索する（ステップ２００９）。

【００８６】

上記ステップ２００９の検索の結果、例えば、ステップ２０３９において属性証明書取得先情報７８０が生成されている状況など、属性証明書の取得先情報を取得できた場合には、ステップ２０１７まで、処理を省略してよい。逆に、属性証明書の取得先情報を取得できなかった場合には、次ステップ２０１１に処理が移行する（ステップ２０１０）。

【００８７】

上記ステップ２０１０にて、属性証明書の取得先を取得できなかった場合には、利用者にその取得先を指定させるため、サービス提供装置１５０の認証・認可プログラム７３０は、利用者装置１４０に属性証明書の取得先一覧を送信する。属性証明書の取得先一覧は、サービス提供装置側で予め登録されているものとする（ステップ２０１１）。

【００８８】

利用者装置１４０では、上記ステップ２０１１にて送信されてきた属性証明書の取得先一覧を、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ２０１２）。

【００８９】

続いて、利用者装置１４０のＷｅｂブラウザプログラム６２０は、受信した属性証明書の取得先一覧を表示する（ステップ２０１３）。

【００９０】

さらに、利用者装置１４０のＷｅｂブラウザプログラム６２０は、表示した属性証明書の取得先一覧の中から、適切な属性証明書の取得先を利用者に選択させる（ステップ２０１４）。

【００９１】

利用者装置１４０のＷｅｂブラウザプログラム６２０は、上記ステップ２０１４にて利用者が選択した属性証明書の取得先に関する情報を、サービス提供装置１５０に送信する（ステップ２０１５）。

【００９２】

サービス提供装置１５０では、利用者装置１４０が送信した属性証明書の取得先に関する情報をサービス提供プログラム７２０にて受信する（ステップ２０１６）。

【００９３】

次に、図１０におけるステップ２０１６以降の手順について、図１１を用いて説明する。

上記ステップ２００９もしくは２０１６にて、属性証明書の取得先に関する情報を取得したら、サービス提供装置１５０は、利用者の属性証明書を属性証明書管理装置１３０に要求する旨のメッセージを、利用者装置１４０に送信する。属性証明書を要求する際のメッセージとしては、サービス提供者が必要とする属性情報の種類を示す情報（例えば、属性の型を表すオブジェクト識別子等）、セッション情報（例えば、Ｃｏｏｋｉｅにセッション情報を組み込む方法や、ＵＲＬのクエリーに組み込む方法などがよく知られている）、属性証明書管理装置１３０にアクセスした後に当該サービス提供装置１５０に通信を戻すために必要な戻り先ＵＲＬ情報などが含まれる。

【００９４】

属性情報の種類を示す情報は、属性の条件に関する情報７７０にて予め設定されているものとする。また、当該メッセージは、利用者端末１４０のＷｅｂブラウザプログラムが、上記ステップ２００９もしくは２０１６にて取得した属性証明書の取得先にリダイレクトできるようにするための情報も含まれるものとする。さらに、必要に応じて、本メッセージには、サービス提供装置１５０にて認証済みである旨のチケットを添付してもよい。この認証済みであるチケットは、例えば、ＳＡＭＬ（Security Assertion Markup Language）における認証アサーションもしくはアーティファクトに相当する（ステップ２０１７）。

【００９５】

利用者装置１４０では、上記ステップ２０１７にて送信されてきた属性証明書要求を、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ２０１８）。

【００９６】

上記ステップ２０１８にて受信した属性証明書要求は、属性証明書管理装置１３０へのリダイレクトを行う旨のメッセージとなっているため、利用者装置１４０のＷｅｂブラウザプログラム６２０は、上記ステップ２０１８にて受信したメッセージの内容をそのまま属性証明書管理装置１３０に送信する（ステップ２０１９）。

【００９７】

属性証明書管理装置１３０では、利用者装置１４０が送信した属性証明書要求を属性証明書開示プログラム５３０にて受信する（ステップ２０２０）。

【００９８】

上記ステップ２０２０にて受信した属性証明書要求の中に、認証済みのチケットが含まれているような場合など、利用者装置１４０に認証を要求する必要のない場合は、ステップ２０２８まで処理を省略してもよい。但し、認証済みのチケットを受け取っている場合には、そのチケットの検証は本ステップにて実施する。一方、属性証明書要求の中に、認証済みのチケット等が含まれておらず、利用者装置１４０に認証を要求する必要がある場合には、次ステップ２０２２に処理を移行する（ステップ２０２１）。

【００９９】

上記ステップ２０２１にて利用者側の認証が必要であると判断した場合には、属性証明書開示プログラム５３０は、利用者の認証を行うために必要な認証情報の要求、すなわち、認証要求を、利用者装置１４０に送信する。例えば、ＳＳＬあるいはＴＬＳによるクライアント認証の要求が本ステップに相当する（ステップ２０２２）。

【０１００】

利用者装置１４０では、上記ステップ２０２２にて送信された認証要求を、Ｗｅｂブラウザプログラムにて受信する（ステップ２０２３）。

【０１０１】

続いて、利用者装置１４０では、Ｗｅｂブラウザプログラム６２０を用いて、認証要求に応じた認証情報を生成する。例えば、ＳＳＬあるいはＴＬＳにおける認証であれば、利用者の秘密鍵６５０を用いた電子署名データを生成することに相当する（ステップ２０２４）。

【０１０２】
さらに、利用者装置１４０は、上記ステップ２０２４にて生成した認証情報及び当該認証情報を検証するために必要なその他の情報を、属性証明書管理装置１３０に送信する。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、利用者装置１４０から属性証明書管理装置１３０に送信される情報として、電子署名データの他に、利用者の公開鍵証明書３８０も送信される（ステップ２０２５）。
【０１０３】
属性証明書管理装置１３０では、利用者装置１４０が送信した認証情報を属性証明書開示プログラム５３０にて受信する（ステップ２０２６）。
【０１０４】
続いて、属性証明書管理装置１３０では、属性証明書開示プログラム５３０によって、利用者装置１４０が送信した認証情報を検証し、ユーザの認証を行う。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、利用者装置から送信された電子署名データを、利用者の公開鍵証明書３８０を用いて検証を行うとともに、利用者の公開鍵証明書３８０の認証パスを検証し、当該サービス提供装置が予め設定しているトラストアンカーの証明書まで辿れることを確認することに相当する。
【０１０５】
なお、トラストアンカーとなる証明書は、アクセス制御情報５５０に含むものとする。また、必要に応じて、認証局装置１１０にアクセスして失効情報３７０を取得し、当該失効情報に基づいた利用者の公開鍵証明書３８０の有効性確認も行う（ステップ２０２７）。
【０１０６】
上記ステップ２０２７にて、ユーザの認証が完了したら、サービス提供装置１５０に提示する属性証明書を利用者に指定させるため、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、利用者装置１４０に属性証明書の一覧を送信する。利用者の属性証明書４８０は、利用者の要求もしくは属性認証局１２０が利用者の属性証明書を発行したタイミング等であらかじめ登録されているものとする。１人の利用者に対して、属性証明書は複数登録されていてもよい。また、この際に送信する一覧は、ステップ２０２０において受信した認証済みチケット、あるいは、ステップ２０２６にて受信した利用者の公開鍵証明書３８０に関連する利用者の属性証明書のみが含まれ、他のユーザの属性証明書は含まないように制御する。
【０１０７】
なお、属性証明書の一覧を提示するにあたっては、属性証明書の検証の観点において有効であるもののみを一覧に加えることで、利用者の不要な選択をさけることが可能となる。
【０１０８】
また、上記ステップ２０２０にて受信した属性証明書要求のメッセージの中に、サービス提供装置１５０が要求する属性情報の条件が含まれていることから、この条件に適合するもののみを一覧に加えることで、利用者の不要な選択をさけることが可能となる。さらに、属性証明書を提示してもよいサイトの一覧、あるいは、属性証明書の提示をしてはいけないサイトの一覧を属性証明書管理装置１３０側で予め登録しておき、それらの情報と、上記ステップ２０２０にて受信した属性証明書要求のメッセージの中に含まれる戻り先ＵＲＬとを比較し、属性証明書を提示してもよいと判断したもののみを、選択させる一覧に加えることで、利用者の不要な選択をさけることが可能となる（ステップ２０２８）。
【０１０９】
利用者装置１４０では、上記ステップ２０２８にて送信されてきた属性証明書の一覧を、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ２０２９）。
【０１１０】
続いて、利用者装置１４０のＷｅｂブラウザプログラム６２０は、受信した属性証明書の一覧を表示する（ステップ２０３０）。

【０１１１】
さらに、利用者装置１４０のＷｅｂブラウザプログラム６２０は、表示した属性証明書の一覧の中から、サービス提供装置１５０に開示する属性証明書を利用者に選択させる（ステップ２０３１）。
【０１１２】
利用者装置１４０のＷｅｂブラウザプログラム６２０は、上記ステップ２０３１にて利用者が選択した属性証明書に関する情報を、属性証明書管理装置１３０に送信する（ステップ２０３２）。
【０１１３】
属性証明書管理装置１３０では、利用者装置１４０が送信した属性証明書に関する情報を属性証明書開示プログラム５３０にて受信する（ステップ２０３３）。
【０１１４】
続いて、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、上記ステップ２０３３にて指定された利用者の属性証明書４８０を戻り先ＵＲＬであるサービス提供装置１５０に送信する旨のメッセージを利用者装置１４０に送信する。送信する明書を要求する際のメッセージとしては、上記ステップ２０３３にて指定された利用者の属性証明書４８０の他、利用者端末１４０のＷｅｂブラウザプログラムが、戻り先ＵＲＬに利用者の属性証明書４８０を転送できるようにするための情報あるいはスクリプトも含まれるものとする。また、上記ステップ２０２０にて、セッション情報も受信していた場合には、本メッセージに、当該セッション情報を含めてもよい（ステップ２０３４）。
【０１１５】
利用者装置１４０では、上記ステップ２０３４にて送信されてきた属性証明書を含むメッセージ、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ２０３５）。
【０１１６】
上記ステップ２０３５にて受信したメッセージは、当該メッセージ内に含まれる利用者の属性証明書４８０をサービス提供装置１５０に転送する旨のメッセージとなっている、もしくは、スクリプトが記述されているため、利用者装置１４０のＷｅｂブラウザプログラム６２０は、上記ステップ２０３５にて受信した利用者の属性証明書４８０をサービス提供装置１５０に送信する。また、上記ステップ２０１８にて、Ｗｅｂブラウザプログラム６２０に記録する形式のセッション情報を受信していた場合には、当該セッション情報を本メッセージに加えて送信してもよい（ステップ２０３６）。
【０１１７】
サービス提供装置１５０では、利用者装置１４０が送信した属性証明書をサービス提供プログラム７２０にて受信する（ステップ２０３７）。
【０１１８】
次に、図１１におけるステップ２０３７以降の手順について、図１２を用いて説明する。
上記ステップ２０３７にて、利用者の属性証明書４８０を受信したら、サービス提供装置１５０の認証・認可プログラム７３０は、当該属性証明書の認証パス検証を行い、当該サービス提供装置が予め設定しているトラストアンカーの証明書まで辿れることを確認することに相当する。なお、トラストアンカーとなる証明書は、アクセス制御情報７６０に含むものとする。さらに、当該属性証明書が指し示す公開鍵証明書のポインタと、上記ステップ２００７で受信した利用者の公開鍵証明書３８０との対応関係がとれることを確認する。また、必要に応じて、属性認証局装置１２０にアクセスして属性証明書失効情報４７０を取得し、当該失効情報に基づいた利用者の属性証明書４８０の有効性確認も行う（ステップ２０３８）。
【０１１９】
続いて、上記ステップ２０３８において利用者の属性証明書の検証に成功した場合、サービス提供装置１５０の認証・認可プログラム７３０は、当該属性証明書内に記載されている属性情報が、予め設定されているアクセス制御情報７６０の条件を満たすことを確認

する。属性証明書を取得した際に、属性証明書の属性情報の暗号化に用いた暗号化鍵５７０を併せて取得している場合には、当該暗号化鍵を用いて、属性証明書の属性情報の復号処理を行った上で、属性情報を取り出す。

【０１２０】

また、当該ステップで使用した利用者の属性証明書４８０が、当該サービス提供装置の提供するサービスに適合するものであった場合には、上記ステップ２０１６にて取得した当該属性証明書の取得先を、属性証明書取得先情報７８０として、当該属性証明書の利用者に結び付くようにして記録しておく（ステップ２０３９）。

【０１２１】

上記ステップ２０３９において、アクセス制御情報の条件を満たすことが確認された場合、サービス提供装置１５０のサービス提供プログラム７２０は、認証・認可された利用者の情報に基づいて、要求されたサービスを実行する。必要に応じて、サービス提供用データ７５０も使用する（ステップ２０４０）。

【０１２２】

さらに、サービス提供装置１５０のサービス提供プログラム７２０は、上記ステップ２０４０において実行された結果をサービス提供内容として利用者装置１４０に送信する（ステップ２０４１）。

【０１２３】

利用者装置１４０では、上記ステップ２０４０にて送信されてきたサービス提供内容に関する情報を、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ２０４２）。

【０１２４】

続いて、利用者装置１４０のＷｅｂブラウザプログラム６２０は、受信したサービス提供内容に関する情報を表示する（ステップ２０４３）。

【０１２５】

以上の手順を実施することにより、利用者装置側に特別なプログラムを導入することなく、サービス提供者に対して適切な属性証明書を開示することが可能となる。

【実施例２】

【０１２６】

図１３は、本発明の実施例２に係る属性証明書管理装置を用いたアクセス権設定の処理フロー概要を示す図である。本処理フローは、本発明の実施例２の図１６の処理を行うにあたって予め実施しておく手順となる。本処理フローでは、利用者装置１４０と、属性証明書管理装置１３０との間において、サービス提供装置１５０等に属性証明書を開示するためのアクセス権を設定するための手順について記述する。

【０１２７】

図１３において、利用者装置１４０は、属性証明書管理装置１３０にアクセス要求を送信する。当該属性証明書管理装置は、当該利用者装置に対して認証要求を送信する。当該利用者装置は、認証要求を受け、認証情報を生成し、当該属性証明書管理装置に送信する。

【０１２８】

当該属性証明書管理装置は、認証情報からアクセスしてきた相手の認証を行った上で、属性証明書を管理するためのメニュー画面を当該利用者装置に送信する。当該利用者装置は、メニュー画面を表示し、それを利用者に選択させ、選択された情報を当該属性証明書管理装置に送信する。ここでの説明は、メニューとしてアクセス権の登録を選択した例を記述する。アクセス権の変更、あるいは削除を選択した場合でも処理の流れは同様である。当該属性証明書管理装置は、受信したメニューの選択内容に基づき、属性証明書を開示する際のアクセス権を登録するための画面を利用者装置に送信する。

【０１２９】

当該利用者装置は、アクセス権の登録画面を表示し、アクセス権の登録に必要な情報を利用者に入力させ、入力された情報を当該属性証明書管理装置に送信する。当該属性証明

書管理装置は、入力された登録情報に基づいた確認画面を利用者装置に送信する。当該利用者装置は、アクセス権の登録確認画面を表示し、画面の内容で登録を実施してよいか否かを確認させ、確認結果を当該属性証明書管理装置に送信する。当該属性証明書管理装置は、確認の結果、登録が決定された場合にはアクセス権を設定し、登録が完了した旨の画面を利用者装置に送信する。利用者装置は登録完了画面を受信し、その内容を表示する。

以上が、本発明における属性証明書管理装置におけるアクセス権の設定方法の実施形態の１つとなる。

【０１３０】

図１４及び図１５は、図１３の内容の詳細な処理フロー示す図である。図１４において、利用者装置１４０では、Ｗｅｂブラウザプログラム６２０を起動し、属性証明書管理装置１３０にアクセスするためのＵＲＬを入力し、属性証明書管理装置１３０に対してアクセス要求を送信する（ステップ３００１）。

【０１３１】

属性証明書管理装置１３０では、利用者装置１４０が送信した属性証明書開示プログラム５３０にて受信する（ステップ３００２）。

【０１３２】

上記ステップにてサービス要求を受信したら、属性証明書開示プログラム５３０は、利用者の認証を行うために必要な認証情報の要求、すなわち、認証要求を、利用者装置１４０に送信する。例えば、ＳＳＬ（Secure Socket Layer）あるいはＴＬＳ（Transport Layer Security）によるクライアント認証の要求が本ステップに相当する（ステップ３００３）。

【０１３３】

利用者装置１４０では、上記ステップ３００３にて送信された認証要求を、Ｗｅｂブラウザプログラムにて受信する（ステップ３００４）。

【０１３４】

続いて、利用者装置１４０では、Ｗｅｂブラウザプログラム６２０を用いて、認証要求に応じた認証情報を生成する。例えば、ＳＳＬあるいはＴＬＳにおける認証であれば、利用者の秘密鍵６５０を用いた電子署名データを生成することに相当する（ステップ３００５）。

【０１３５】

さらに、利用者装置１４０は、上記ステップ３００５にて生成した認証情報及び当該認証情報を検証するために必要なその他の情報を、属性証明書管理装置１３０に送信する。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、利用者装置１４０から属性証明書管理装置１３０に送信される情報として、電子署名データの他に、利用者の公開鍵証明書３８０も送信される（ステップ３００６）。

【０１３６】

属性証明書管理装置１３０では、利用者装置１４０が送信した認証情報を属性証明書開示プログラム５３０にて受信する（ステップ３００７）。

【０１３７】

続いて、属性証明書管理装置１３０では、属性証明書開示プログラム５３０によって、利用者装置１４０が送信した認証情報を検証し、ユーザの認証を行う。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、利用者装置から送信された電子署名データを、利用者の公開鍵証明書３８０を用いて検証を行うとともに、利用者の公開鍵証明書３８０の認証パスを検証し、当該属性証明書管理装置が予め設定しているトラストアンカーの証明書まで辿れることを確認することに相当する。

【０１３８】

なお、トラストアンカーとなる証明書は、アクセス制御情報７６０に含むものとする。また、必要に応じて、認証局装置１１０にアクセスして失効情報３７０を取得し、当該失効情報に基づいた利用者の公開鍵証明書３８０の有効性確認も行う（ステップ３００８）。

【０１３９】
上記ステップ３００８にて、ユーザの認証が完了したら、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、利用者装置１４０に、メニュー画面を送信する。本実施例においては、当該メニュー画面には、アクセス権の登録、変更、削除というメニューが含まれているものとする（ステップ３００９）。
【０１４０】
利用者装置１４０では、上記ステップ３００９にて送信されてきたメニュー画面を、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ３０１０）。
【０１４１】
続いて、利用者装置１４０のＷｅｂブラウザプログラム６２０は、受信したメニュー画面を表示する（ステップ３０１１）。
【０１４２】
さらに、利用者装置１４０のＷｅｂブラウザプログラム６２０は、表示したメニュー画面の中から、利用者が実行したいメニューを利用者に選択させる。本実施例においては、アクセス権の登録等を選択した場合の例を記述するが、変更、削除を選択した場合であっても本ステップ以降の処理は同様で、登録を変更もしくは削除に置き換えればよい（ステップ３０１２）。
【０１４３】
利用者装置１４０のＷｅｂブラウザプログラム６２０は、上記ステップ３０１３にて利用者が選択したメニューの情報を、属性証明書管理装置１３０に送信する（ステップ３０１３）。
【０１４４】
属性証明書管理装置１３０では、利用者装置１４０が送信したメニューの情報を属性証明書開示プログラム５３０にて受信する（ステップ３０１４）。
【０１４５】
次に、図１４におけるステップ３０１４以降の手順について、図１５を用いて説明する。
【０１４６】
属性証明書管理装置１３０では、上記ステップ３０１４において受信したメニューの情報に基づき、アクセス権を登録等するための画面を利用者装置１４０に送信する（ステップ３０１５）。
【０１４７】
利用者装置１４０では、上記ステップ３０１５にて送信されてきたアクセス権登録等画面を、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ３０１６）。
【０１４８】
続いて、利用者装置１４０のＷｅｂブラウザプログラム６２０は、アクセス権登録等画面を表示する（ステップ３０１７）。
【０１４９】
さらに、利用者装置１４０のＷｅｂブラウザプログラム６２０は、アクセス権登録等画面によって、アクセス権の登録等に必要な情報を利用者に入力させる。例えば、利用者の所有する属性証明書の一覧が表示され、属性証明書毎あるいは各属性証明書内の属性情報毎に対して、開示してもよいサービス提供者の情報を割り当てるものを想定する（ステップ３０１８）。
【０１５０】
利用者装置１４０のＷｅｂブラウザプログラム６２０は、上記ステップ３０１９にて利用者が入力した登録等情報を、属性証明書管理装置１３０に送信する（ステップ３０１９）。
【０１５１】
属性証明書管理装置１３０では、利用者装置１４０が送信した登録等情報を属性証明書開示プログラム５３０にて受信する（ステップ３０２０）。

【０１５２】
続いて、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、上記ステップ３０２１において受信した登録等情報に基づき、アクセス権の登録等を確認するための画面を利用者装置１４０に送信する（ステップ３０２１）。
【０１５３】
利用者装置１４０では、上記ステップ３０２１にて送信されてきたアクセス権登録等確認画面を、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ３０２２）。
続いて、利用者装置１４０のＷｅｂブラウザプログラム６２０は、アクセス権登録等確認画面を表示する（ステップ３０２３）。
【０１５４】
さらに、利用者装置１４０のＷｅｂブラウザプログラム６２０は、アクセス権登録等確認画面として、上記ステップ３０１８で入力された情報を表示し、例えば、その内容について決定、修正もしくはキャンセルといった中から、確認結果として次に実行すべき内容を利用者に選択させる（ステップ３０２４）。
【０１５５】
利用者装置１４０のＷｅｂブラウザプログラム６２０は、上記ステップ３０２４にて利用者が選択した確認結果を、属性証明書管理装置１３０に送信する（ステップ３０２５）。
【０１５６】
属性証明書管理装置１３０では、利用者装置１４０が送信した確認結果を属性証明書開示プログラム５３０にて受信する（ステップ３０２６）。
【０１５７】
続いて、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、上記ステップ３０２６において受信した確認結果が、登録を決定する旨の内容であった場合には、次ステップ３０２８に処理を移行する。確認結果が、登録を修正する旨の内容であった場合には、ステップ３０１５に戻る。確認結果が、登録をキャンセルする旨の内容であった場合には、例えば、ステップ３００９に戻るものとする（ステップ３０２７）。
【０１５８】
上記ステップ３０２７において、登録が決定された場合には、ステップ３０２０にて受信した登録情報の内容を反映するべく、属性開示に関する設定情報５６０として記録する（ステップ３０２８）。
【０１５９】
さらに、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、上記ステップ３０２８において実施したアクセス権の反映が完了した旨のメッセージを利用者装置１４０に送信する（ステップ３０２９）。
【０１６０】
利用者装置１４０では、上記ステップ３０２９にて送信されてきた完了結果の画面を、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ３０３０）。
続いて、利用者装置１４０のＷｅｂブラウザプログラム６２０は、完了結果の画面を表示する（ステップ３０３１）。
【０１６１】
図１６は、本発明の実施例２の属性証明書管理装置を用いた資格認証の処理フロー概要を示す図である。本処理フローは、図１３におけるアクセス権の登録等処理が行われた後に実施される、サービス提供者１５０に属性証明書の開示を行うための手順である。本処理フローでは、利用者装置１４０と、サービス提供装置１５０と、属性証明書管理装置１３０との間において、サービス提供装置１５０が属性証明書を用いて利用者の資格や属性を確認するための手順について記述する。
【０１６２】
図１６において、利用者装置１４０は、サービス提供装置１５０にサービス要求を送信する。当該サービス提供装置は、当該利用者装置に対して認証要求を送信する。当該利用

者装置は、認証要求を受け、認証情報を生成し、当該サービス提供装置に送信する。当該サービス提供装置は、認証情報からアクセスしてきた相手の認証を行った上で、当該利用者の属性証明書の取得要求を、属性証明書管理装置に送信する。

【０１６３】

当該属性証明書管理装置は、当該サービス提供装置に対して認証要求を送信する。当該サービス提供装置は、認証要求を受け、認証情報を生成し、当該属性証明書管理装置に送信する。当該属性証明書管理装置は、予め設定された属性証明書のアクセス権に基づき、当該サービス提供装置に対して利用者の属性証明書を送信する。属性証明書が暗号化されている場合には、それを復号するための暗号化鍵もあわせて送信する。当該サービス提供装置は、受信した属性証明書の検証を行った結果に応じて、当該利用者装置に、サービス提供内容を送信する。以上が本発明における属性証明書の管理方法の実施形態の１つとなる。

【０１６４】

図１７は、図１６の内容の詳細な処理フロー示す図である。図１７において、利用者装置１４０では、Ｗｅｂブラウザプログラム６２０を起動し、サービス提供装置１５０が提供するサービスにアクセスするためのＵＲＬを入力し、サービス提供装置１５０に対してサービス要求を送信する（ステップ４００１）。

【０１６５】

サービス提供装置１５０では、利用者装置１４０が送信したサービス要求をサービス提供プログラム７２０にて受信する（ステップ４００２）。

上記ステップにてサービス要求を受信したら、サービス提供プログラム７２０は、利用者の認証を行うために必要な認証情報の要求、すなわち、認証要求を、利用者装置１４０に送信する。例えば、ＳＳＬ（Secure Socket Layer）あるいはＴＬＳ（Transport Layer Security）によるクライアント認証の要求が本ステップに相当する（ステップ４００３）。

【０１６６】

利用者装置１４０では、上記ステップ２００３にて送信された認証要求を、Ｗｅｂブラウザプログラムにて受信する（ステップ４００４）。

続いて、利用者装置１４０では、Ｗｅｂブラウザプログラム６２０を用いて、認証要求に応じた認証情報を生成する。例えば、ＳＳＬあるいはＴＬＳにおける認証であれば、利用者の秘密鍵６５０を用いた電子署名データを生成することに相当する（ステップ４００５）。

【０１６７】

さらに、利用者装置１４０は、上記ステップ２００５にて生成した認証情報及び当該認証情報を検証するために必要なその他の情報を、サービス提供装置１５０に送信する。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、利用者装置１４０からサービス提供装置１５０に送信される情報として、電子署名データの他に、利用者の公開鍵証明書３８０も送信される（ステップ４００６）。

【０１６８】

サービス提供装置１５０では、利用者装置１４０が送信した認証情報をサービス提供プログラム７２０にて受信する（ステップ４００７）。

【０１６９】

続いて、サービス提供装置１５０では、認証・認可プログラム７３０によって、利用者装置１４０が送信した認証情報を検証し、ユーザの認証を行う。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、利用者装置から送信された電子署名データを、利用者の公開鍵証明書３８０を用いて検証を行うとともに、利用者の公開鍵証明書３８０の認証パスを検証し、当該サービス提供装置が予め設定しているトラストアンカーの証明書まで辿れることを確認することに相当する。なお、トラストアンカーとなる証明書は、アクセス制御情報７６０に含むものとする。また、必要に応じて、認証局装置１１０にアクセスして失効情報３７０を取得し、当該失効情報に基づいた利用者の公開鍵証明書３８０の有効性確認

も行う（ステップ４００８）。

【０１７０】

上記ステップ４００８にて、利用者の認証が完了したら、サービス提供装置１５０の認証・認可プログラム７３０は、属性証明書管理装置１３０に、当該利用者の属性証明書を要求する旨のメッセージを送信する。当該要求には、要求する属性証明書の所有者（すなわち、本実施例における利用者）の情報や、要求する属性情報の種類などが含まれる（ステップ４００９）。

【０１７１】

属性証明書管理装置１３０では、サービス提供装置１５０が送信した属性証明書要求を属性証明書開示プログラム５３０にて受信する（ステップ４０１０）。

【０１７２】

上記ステップにて属性証明書要求を受信したら、属性証明書開示プログラム５３０は、属性証明書の要求者の認証を行うために必要な認証情報の要求、すなわち、認証要求を、サービス提供装置１５０に送信する。例えば、ＳＳＬ（Secure Socket Layer）あるいはＴＬＳ（Transport Layer Security）によるクライアント認証の要求が本ステップに相当する（ステップ４０１１）。

【０１７３】

サービス提供装置１５０では、上記ステップ４０１１にて送信された認証要求を、認証・認可プログラム７３０にて受信する（ステップ４０１２）。

【０１７４】

続いて、サービス提供装置１５０では、認証・認可プログラム７３０を用いて、認証要求に応じた認証情報を生成する。例えば、ＳＳＬあるいはＴＬＳにおける認証であれば、サービス提供装置の秘密鍵７９０を用いた電子署名データを生成することに相当する（ステップ４０１３）。

【０１７５】

さらに、サービス提供装置１５０は、上記ステップ４０１３にて生成した認証情報及び当該認証情報を検証するために必要なその他の情報を、属性証明書管理装置１３０に送信する。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、サービス提供装置１５０から属性証明書管理装置１３０に送信される情報として、電子署名データの他に、サービス提供装置の公開鍵証明書７９１も送信される（ステップ４０１４）。

【０１７６】

属性証明書管理装置１３０では、サービス提供装置１５０が送信した属性証明書開示プログラム５３０にて受信する（ステップ４０１５）。

【０１７７】

続いて、属性証明書管理装置１３０では、属性証明書開示プログラム５３０によって、サービス提供装置１５０が送信した認証情報を検証し、属性証明書の要求者の認証を行う。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、サービス提供装置から送信された電子署名データを、サービス提供装置の公開鍵証明書７９１を用いて検証を行うとともに、サービス提供装置の公開鍵証明書７９１の認証パスを検証し、当該サービス提供装置が予め設定しているトラストアンカーの証明書まで辿れることを確認することに相当する。なお、トラストアンカーとなる証明書は、アクセス制御情報５５０に含むものとする。また、必要に応じて、認証局装置１１０にアクセスして失効情報３７０を取得し、当該失効情報に基づいたサービス提供装置の公開鍵証明書７９１の有効性確認も行う（ステップ４０１６）。

【０１７８】

上記ステップ４０１６にて認証に成功した場合、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、属性開示に関する設定情報５６０に設定されている属性証明書のアクセス権に基づいて、要求された利用者の属性証明書に、認証されたサービス提供装置がアクセスしてよいかどうかを判定し、アクセスが許可されれば、属性証明書を、サービス提供装置１５０に送信する。

【０１７９】
また、暗号化された属性証明書を使用している場合には、当該属性証明書の属性情報を暗号化する際に用いた暗号化鍵も送信する。上記ステップ４０１６にて認証に失敗した場合や、本ステップにてアクセスを拒否された場合には、属性証明書へのアクセスを拒否する旨のメッセージを返信する（ステップ４０１７）。
【０１８０】
サービス提供装置１５０では、上記ステップ４０１７にて送信された属性証明書を、認証・認可プログラム７３０にて受信する。また、暗号化された属性証明書を使用している場合には、当該属性証明書の属性情報を暗号化する際に用いた暗号化鍵も受信する。アクセス拒否のメッセージを受信した場合には、認証・認可に失敗したこととして以降の処理を進める（ステップ４０１８）。
【０１８１】
以降の処理は、図１２で示したステップ２０３８からステップ２０４３と同様である。
【０１８２】
以上の手順を実施することにより、利用者装置側に特別なプログラムを導入することなく、サービス提供者に対して適切な属性証明書を開示することが可能となる。また、利用者装置に搭載されているＷｅｂブラウザプログラムが、リダイレクト等の機能をもたないような場合であっても、属性証明書の取扱いが可能となる。
【実施例３】
【０１８３】
図１８は、本発明の実施例３の属性証明書管理装置を用いた資格認証の処理フロー概要を示す図である。本処理フローでは、利用者装置１４０と、サービス提供装置１５０と、属性証明書管理装置１３０との間において、サービス提供装置１５０が属性証明書を用いて利用者の資格や属性を確認するための手順について記述する。
【０１８４】
図１８において、利用者装置１４０は、サービス提供装置１５０にサービス要求を送信する。当該サービス提供装置は、当該利用者装置に対して認証要求を送信する。当該利用者装置は、認証要求を受け、認証情報を生成し、当該サービス提供装置に送信する。当該サービス提供装置は、認証情報からアクセスしてきた相手の認証を行った上で、属性証明書の取得先一覧を当該利用者装置に送信する。当該利用者装置は、属性証明書の取得先一覧を表示し、それを利用者に選択させ、選択された情報を当該サービス提供装置に送信する。
【０１８５】
当該サービス提供装置は、受信した取得先の情報に基づき、属性証明書を取得するために必要な情報の要求を利用者装置経由で属性証明書管理装置に送信する。当該属性証明書管理装置は、当該利用者装置に対して認証要求を送信する。当該利用者装置は、認証要求を受け、認証情報を生成し、当該属性証明書管理装置に送信する。当該属性証明書管理装置は、認証情報からアクセスしてきた相手の認証を行った上で、属性証明書の一覧を当該利用者装置に送信する。当該利用者装置は、属性証明書の一覧を表示し、それを利用者に選択させ、選択された情報を当該属性証明書管理装置に送信する。
【０１８６】
当該属性証明書管理装置は、属性証明書に関するポインタの情報を、当該利用者装置経由で、属性証明書の要求元である当該サービス提供装置に送信する。当該サービス提供装置は、受信した属性証明書のポインタ情報を基に、当該利用者の属性証明書の取得要求を、属性証明書管理装置に送信する。当該属性証明書管理装置は、当該サービス提供装置に対して認証要求を送信する。当該サービス提供装置は、認証要求を受け、認証情報を生成し、当該属性証明書管理装置に送信する。
【０１８７】
当該属性証明書管理装置は、予め設定された属性証明書のアクセス権に基づき、当該サービス提供装置に対して利用者の属性証明書を送信する。属性証明書が暗号化されている

場合には、それを復号するための暗号化鍵もあわせて送信する。当該サービス提供装置は、受信した属性証明書の検証を行った結果に応じて、当該利用者装置に、サービス提供内容を送信する。以上が本発明における属性証明書の管理方法の実施形態の１つとなる。

【０１８８】

図１９は、図１８の内容の詳細な処理フロー示す図である。利用者装置１４０が、サービス提供装置１５０にサービス要求を送信するところから、属性証明書管理装置１３０が、利用者に属性証明書の一覧を表示し、それを利用者に選択させ、選択された情報を当該属性証明書管理装置に送信するところまでの手順は、図１０のステップ２００１から図１１のステップ２０３３までの説明で示した内容と同様である。

【０１８９】

上記ステップ２０３３に続いて、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、上記ステップ２０３３にて指定された利用者の属性証明書４８０に関するポインタ（例えば、当該属性証明書の発行者名とシリアル番号など）を戻り先ＵＲＬであるサービス提供装置１５０に送信する旨のメッセージを利用者装置１４０に送信する。送信する明書を要求する際のメッセージとしては、上記ステップ２０３３にて指定された利用者の属性証明書のポインタ情報の他、利用者端末１４０のＷｅｂブラウザプログラムが、戻り先ＵＲＬに利用者の属性証明書のポインタ情報を転送できるようにするための情報あるいはスクリプトも含まれるものとする。また、上記ステップ２０２０にて、セッション情報も受信していた場合には、本メッセージに、当該セッション情報を含めてもよい（ステップ５００１）。

【０１９０】

利用者装置１４０では、上記ステップ５００１にて送信されてきた属性証明書を含むメッセージ、Ｗｅｂブラウザプログラム６２０によって受信する（ステップ５００２）。

【０１９１】

上記ステップ５００２にて受信したメッセージは、当該メッセージ内に含まれる利用者の属性証明書のポインタ情報をサービス提供装置１５０に転送する旨のメッセージとなっている、もしくは、スクリプトが記述されているため、利用者装置１４０のＷｅｂブラウザプログラム６２０は、上記ステップ５００２にて受信した利用者の属性証明書のポインタ情報をサービス提供装置１５０に送信する。また、上記ステップ２０１８にて、Ｗｅｂブラウザプログラム６２０に記録する形式のセッション情報を受信していた場合には、当該セッション情報を本メッセージに加えて送信してもよい（ステップ５００３）。

【０１９２】

サービス提供装置１５０では、利用者装置１４０が送信した属性証明書のポインタ情報をサービス提供プログラム７２０にて受信する（ステップ５００４）。

【０１９３】

上記ステップ５００４にて受信した属性証明書のポインタ情報を基に、サービス提供装置１５０の認証・認可プログラム７３０は、属性証明書管理装置１３０に、当該利用者の属性証明書を要求する旨のメッセージを送信する。当該要求には、要求する属性証明書のポインタ情報や、要求する属性情報の種類などが含まれる（ステップ５００５）。

【０１９４】

属性証明書管理装置１３０では、サービス提供装置１５０が送信した属性証明書要求を属性証明書開示プログラム５３０にて受信する（ステップ５００６）。

【０１９５】

上記ステップ５００６にて属性証明書要求を受信したら、属性証明書開示プログラム５３０は、属性証明書の要求者の認証を行うために必要な認証情報の要求、すなわち、認証要求を、サービス提供装置１５０に送信する。例えば、ＳＳＬ（Secure Socket Layer）あるいはＴＬＳ（Transport Layer Security）によるクライアント認証の要求が本ステップに相当する（ステップ５００７）。

【０１９６】

サービス提供装置１５０では、上記ステップ５００７にて送信された認証要求を、認証

・認可プログラム７３０にて受信する（ステップ５００８）。
続いて、サービス提供装置１５０では、認証・認可プログラム７３０を用いて、認証要求に応じた認証情報を生成する。例えば、ＳＳＬあるいはＴＬＳにおける認証であれば、サービス提供装置の秘密鍵７９０を用いた電子署名データを生成することに相当する（ステップ５００９）。
【０１９７】
さらに、サービス提供装置１５０は、上記ステップ５００９にて生成した認証情報及び当該認証情報を検証するために必要なその他の情報を、属性証明書管理装置１３０に送信する。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、サービス提供装置１５０から属性証明書管理装置１３０に送信される情報として、電子署名データの他に、サービス提供装置の公開鍵証明書７９１も送信される（ステップ５０１０）。
【０１９８】
属性証明書管理装置１３０では、サービス提供装置１５０が送信した属性証明書開示プログラム５３０にて受信する（ステップ５０１１）。
【０１９９】
続いて、属性証明書管理装置１３０では、属性証明書開示プログラム５３０によって、サービス提供装置１５０が送信した認証情報を検証し、属性証明書の要求者の認証を行う。例えば、ＳＳＬあるいはＴＬＳによる認証の場合、サービス提供装置から送信された電子署名データを、サービス提供装置の公開鍵証明書７９１を用いて検証を行うとともに、サービス提供装置の公開鍵証明書７９１の認証パスを検証し、当該サービス提供装置が予め設定しているトラストアンカーの証明書まで辿れることを確認することに相当する。
【０２００】
なお、トラストアンカーとなる証明書は、アクセス制御情報５５０に含むものとする。また、必要に応じて、認証局装置１１０にアクセスして失効情報３７０を取得し、当該失効情報に基づいたサービス提供装置の公開鍵証明書７９１の有効性確認も行う（ステップ５０１２）。
【０２０１】
上記ステップ５０１２にて認証に成功した場合、属性証明書管理装置１３０の属性証明書開示プログラム５３０は、属性開示に関する設定情報５６０に設定されている属性証明書のアクセス権に基づいて、要求された利用者の属性証明書に、認証されたサービス提供装置がアクセスしてよいかどうかを判定し、アクセスが許可されれば、属性証明書を、サービス提供装置１５０に送信する。また、暗号化された属性証明書を使用している場合には、当該属性証明書の属性情報を暗号化する際に用いた暗号化鍵も送信する。上記ステップ５０１２にて認証に失敗した場合や、本ステップにてアクセスを拒否された場合には、属性証明書へのアクセスを拒否する旨のメッセージを返信する（ステップ５０１３）。
【０２０２】
サービス提供装置１５０では、上記ステップ５０１３にて送信された属性証明書を、認証・認可プログラム７３０にて受信する。また、暗号化された属性証明書を使用している場合には、当該属性証明書の属性情報を暗号化する際に用いた暗号化鍵も受信する。アクセス拒否のメッセージを受信した場合には、認証・認可に失敗したこととして以降の処理を進める（ステップ５０１４）。以降の処理は、図１２で示したステップ２０３８からステップ２０４３と同様である。
【０２０３】
以上の手順を実施することにより、利用者装置側に特別なプログラムを導入することなく、サービス提供者に対して適切な属性証明書を開示することが可能となる。
【図面の簡単な説明】
【０２０４】
【図１】図１は本発明の実施例１のシステム構成を例示する図である。
【図２】図２は認証局装置、属性認証局装置、属性証明書管理装置、利用者装置及びサービス提供装置のハードウェア構成を例示する図である。

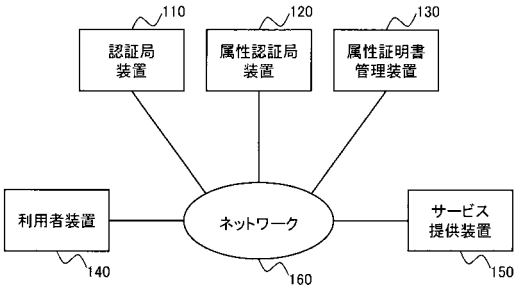
【図３】図３は認証局装置の構成を例示する図である。
【図４】図４は属性認証局装置の構成を例示する図である。
【図５】図５は属性証明書管理装置の構成を例示する図である。
【図６】図６は利用者装置の構成を例示する図である。
【図７】図７はサービス提供装置の構成を例示する図である。
【図８】図８は利用者の公開鍵証明書及び属性証明書のデータ仕様を例示する図である。
【図９】図９は本発明の実施例１に係る属性証明書管理装置を用いた資格認証の処理フロー概要を示す図である。
【図１０】図１０は本発明の実施例１に係る属性証明書管理装置を用いた資格認証の処理フロー詳細（前段）を示す図である。
【図１１】図１１は本発明の実施例１に係る属性証明書管理装置を用いた資格認証の処理フロー詳細（中段）を示す図である。
【図１２】図１２は本発明の実施例１に係る属性証明書管理装置を用いた資格認証の処理フロー詳細（後段）を示す図である。
【図１３】図１３は本発明の実施例２に係る属性証明書管理装置を用いたアクセス権設定の処理フロー概要を示す図である。
【図１４】図１４は本発明の実施例２に係る属性証明書管理装置を用いたアクセス権設定の処理フロー詳細（前段）を示す図である。
【図１５】図１５は本発明の実施例２に係る属性証明書管理装置を用いたアクセス権設定の処理フロー詳細（後段）を示す図である。
【図１６】図１６は本発明の実施例２に係る属性証明書管理装置を用いた資格認証の他の態様の処理フロー概要を示す図である。
【図１７】図１７は本発明の実施例２に係る属性証明書管理装置を用いた資格認証の他の態様の処理フロー詳細を示す図である。
【図１８】図１８は本発明の実施例３に係る属性証明書管理装置を用いた資格認証の別の態様の処理フロー概要を示す図である。
【図１９】図１９は本発明の実施例３に係る属性証明書管理装置を用いた資格認証の別の態様の処理フロー詳細を示す図である。
【符号の説明】
【０２０５】

１１０	認証局装置
１２０	属性認証局装置
１３０	属性証明書管理装置
１４０	利用者装置
１５０	サービス提供装置
１６０	ネットワーク
２１０	入力装置
２２０	表示装置
２３０	ＣＰＵ
２４０	メモリ
２５０	記憶装置
２６０	通信装置
２７０	バス
３１０	オペレーティングシステム
３２０	公開鍵証明書発行プログラム
３３０	失効情報発行プログラム
３５０	認証局の秘密鍵
３６０	認証局の公開鍵証明書
３７０	失効情報
３８０	利用者の公開鍵証明書

４１０　オペレーティングシステム
４２０　属性証明書発行プログラム
４３０　属性証明書失効情報発行プログラム
４５０　属性認証局の秘密鍵
４６０　属性認証局の公開鍵証明書
４７０　属性証明書失効情報
４８０　利用者の属性証明書
５１０　オペレーティングシステム
５２０　属性証明書登録プログラム
５３０　属性証明書開示プログラム
５５０　アクセス制御情報
５６０　属性開示に関する設定情報
５７０　暗号化鍵
６１０　オペレーティングシステム
６２０　Ｗｅｂブラウザプログラム
６５０　利用者の秘密鍵
７１０　オペレーティングシステム
７２０　サービス提供プログラム
７３０　認証・認可プログラム
７５０　サービス提供用データ
７６０　アクセス制御情報
７７０　属性の条件に関する情報
７８０　属性証明書取得先情報
７９０　サービス提供装置の秘密鍵
７９１　サービス提供装置の公開鍵証明書

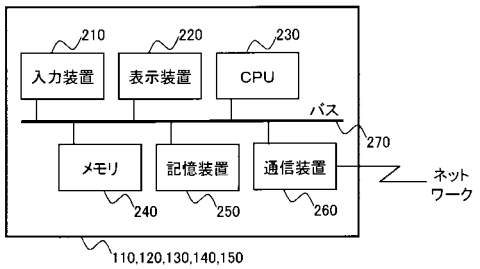
【図１】

図1



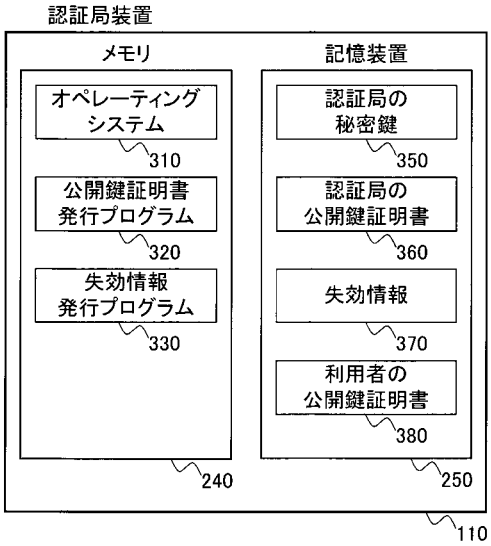
【図２】

図2



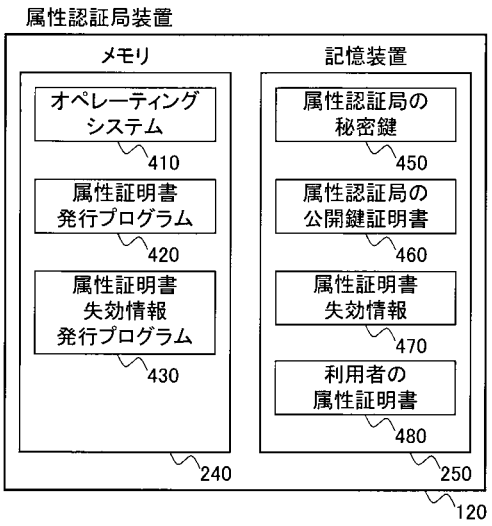
【図３】

図3



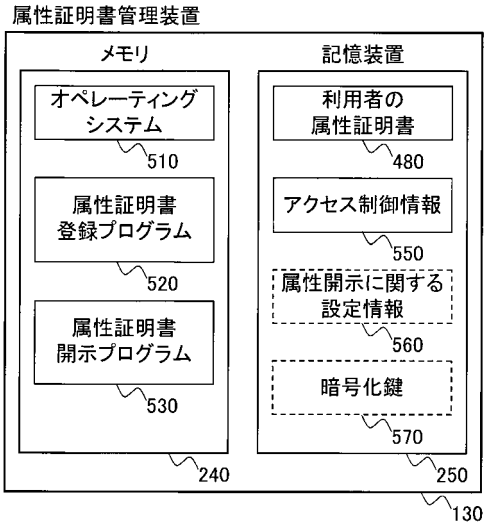
【図４】

図4



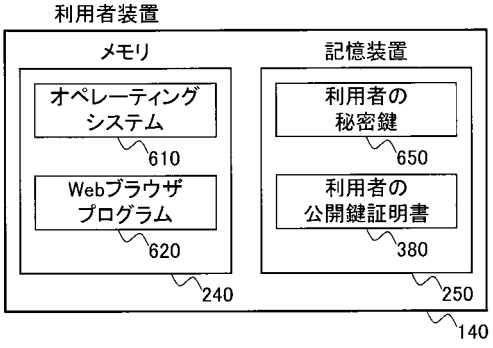
【図５】

図5



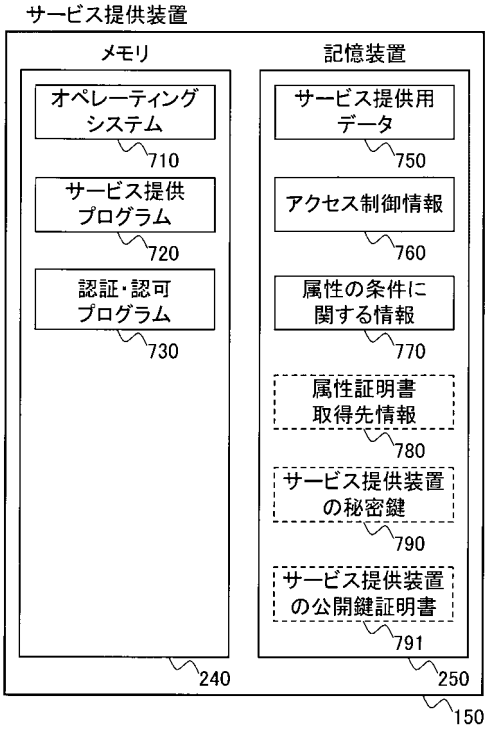
【図６】

図6



【図７】

図7



【図８】

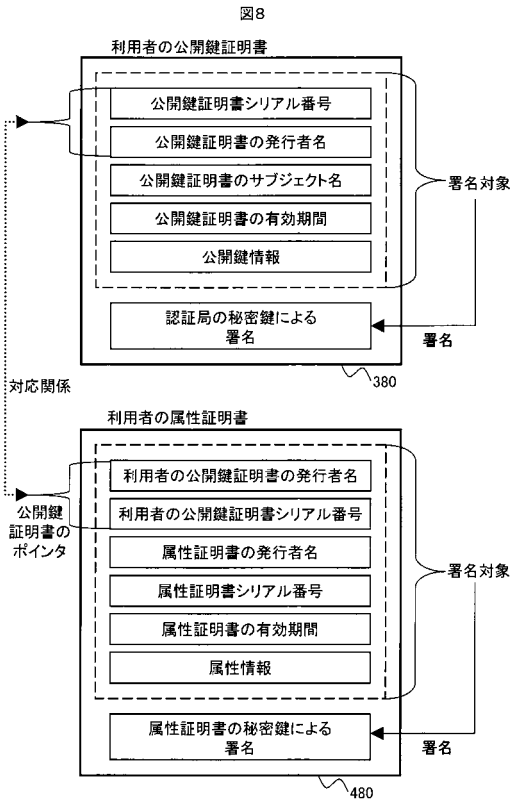


図8
利用者の公開鍵証明書
公開鍵証明書シリアル番号
公開鍵証明書の発行者名
公開鍵証明書のサブジェクト名
公開鍵証明書の有効期間
公開鍵情報
署名対象
認証局の秘密鍵による署名
署名
380
対応関係
利用者の属性証明書
利用者の公開鍵証明書の発行者名
利用者の公開鍵証明書シリアル番号
属性証明書の発行者名
属性証明書シリアル番号
属性証明書の有効期間
属性情報
署名対象
公開鍵証明書のポインタ
属性証明書の秘密鍵による署名
署名
480

【図９】

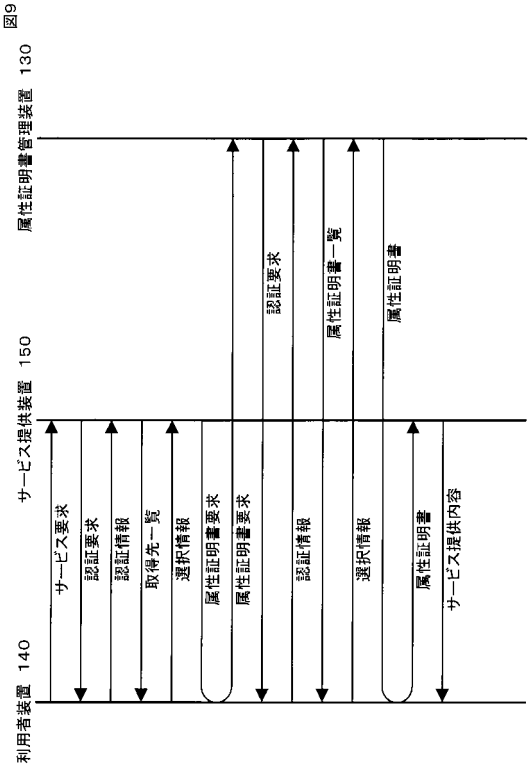


図9
属性証明書管理装置 130
サービス提供装置 150
利用者装置 140
サービス要求
認証要求
認証情報
取得先一覧
選択情報
属性証明書要求
認証情報
選択情報
属性証明書
サービス提供内容
認証要求
属性証明書一覧
属性証明書

【図１０】

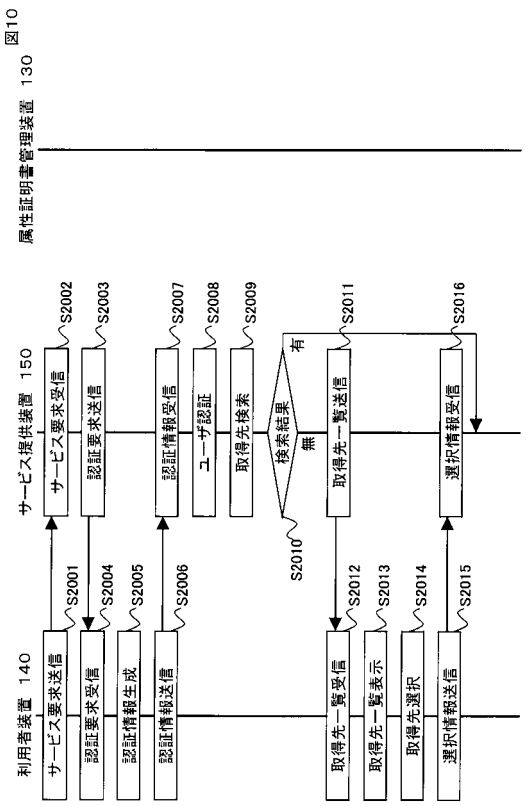


図10
属性証明書管理装置 130
サービス提供装置 150
利用者装置 140
サービス要求送信
サービス要求受信
認証要求送信
認証要求受信
認証情報生成
認証情報送信
認証情報受信
ユーザ認証
取得先検索
検索結果
有
無
取得先一覧送信
取得先一覧受信
取得先一覧表示
取得先選択
選択情報送信
選択情報受信
S2001
S2002
S2003
S2004
S2005
S2006
S2007
S2008
S2009
S2010
S2011
S2012
S2013
S2014
S2015
S2016

【図１１】

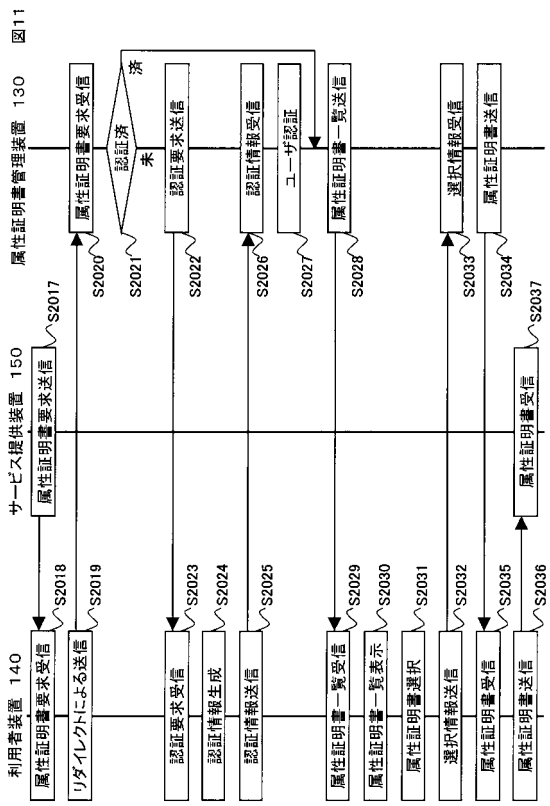
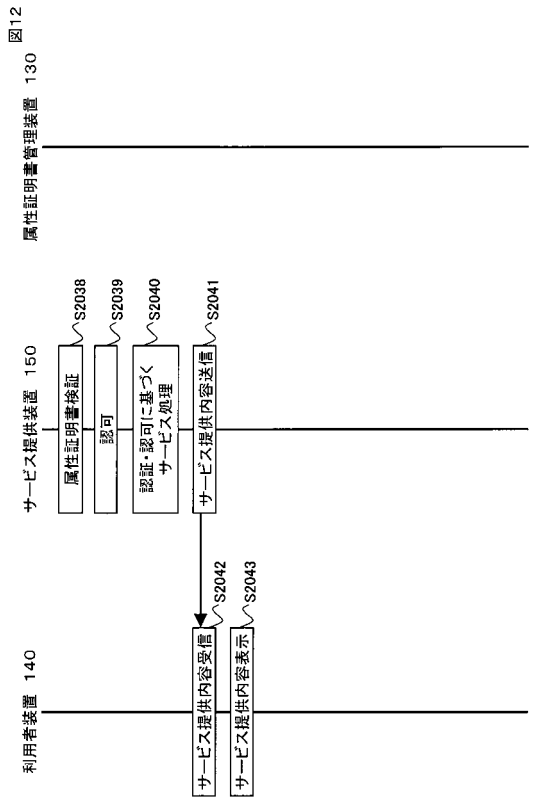
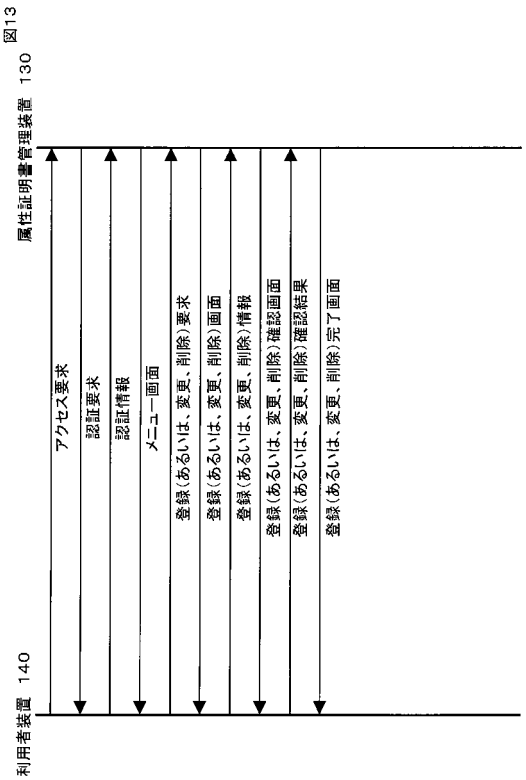


図11
属性証明書管理装置 130
サービス提供装置 150
利用者装置 140
属性証明書要求受信
認証済
未
認証要求送信
認証情報受信
ユーザ認証
属性証明書一覧送信
選択情報受信
属性証明書送信
属性証明書要求送信
リダイレクトによる送信
認証要求受信
認証情報生成
認証情報送信
属性証明書一覧受信
属性証明書一覧表示
属性証明書選択
選択情報送信
属性証明書受信
属性証明書送信
S2017
S2018
S2019
S2020
S2021
S2022
S2023
S2024
S2025
S2026
S2027
S2028
S2029
S2030
S2031
S2032
S2033
S2034
S2035
S2036
S2037

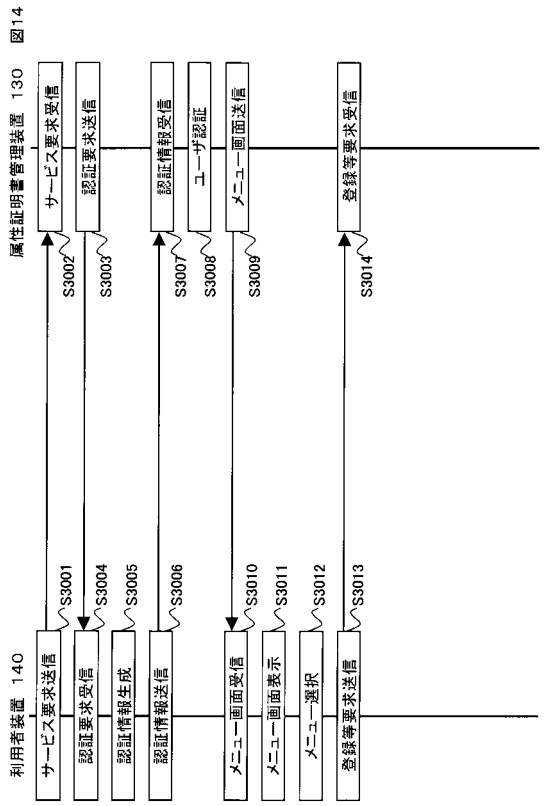
【図１２】



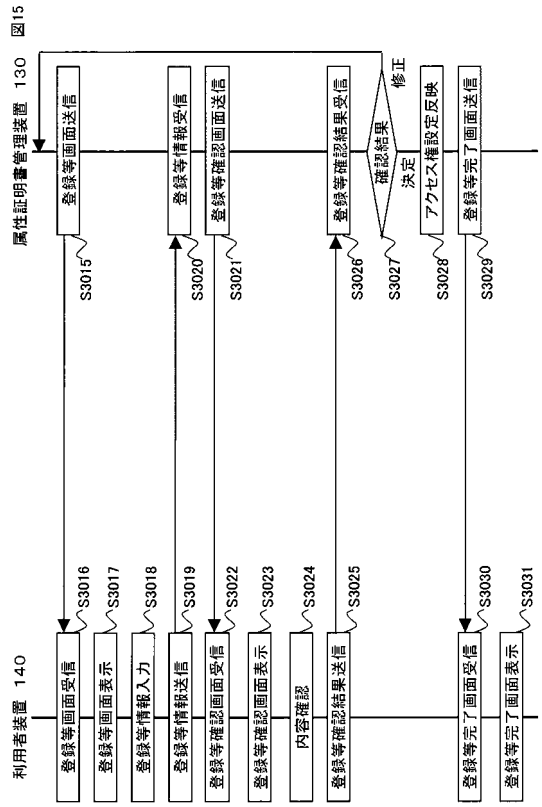
【図１３】



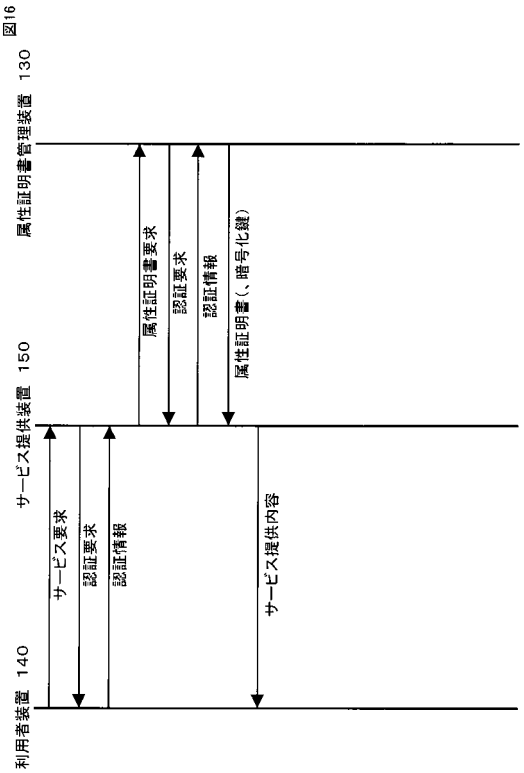
【図１４】



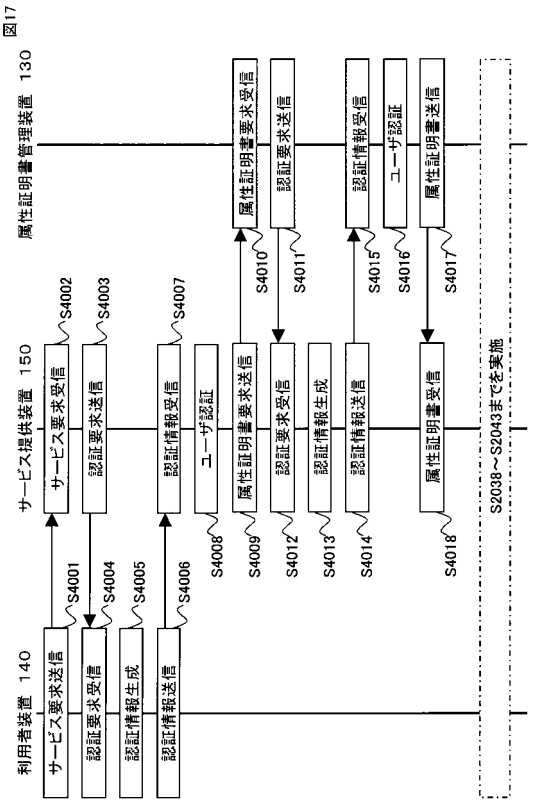
【図１５】



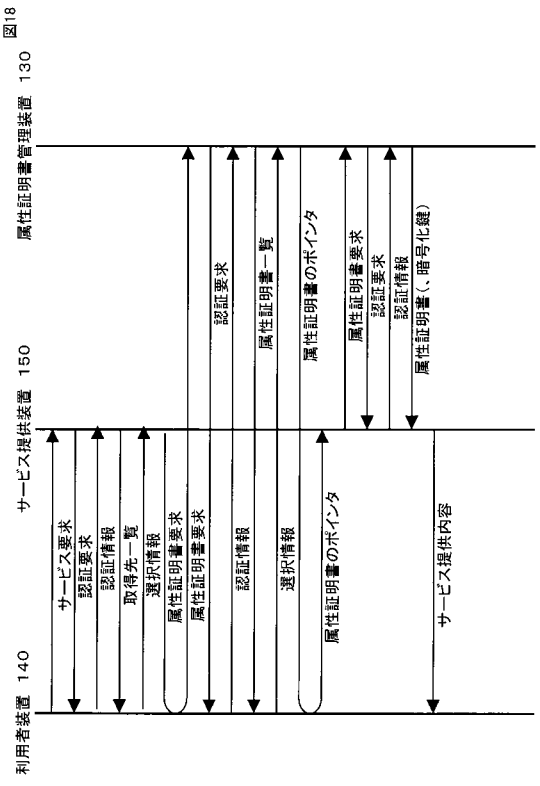
【図１６】



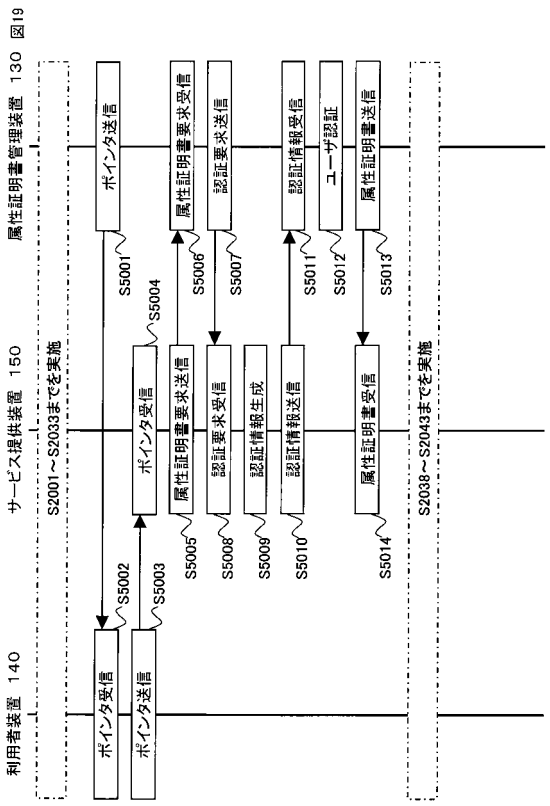
【図１７】



【図１８】



【図１９】



フロントページの続き

(72)発明者　竹内　国人
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所金融システム事業部内

Ｆターム(参考) 5B017 AA03 AA04 BA05 BA06 CA16
5B285 AA01 BA01 CA02 CA43 CA44 CA45 CB47 CB52 CB62 CB73
CB85 CB92 DA05
5J104 AA07 KA01 PA07 PA10