(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2004-348631
(P2004-348631A)
(43)公開日　平成16年12月9日(2004.12.9)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330B	5B045
G06F 15/16	G06F	15/16	620B	5B085
H04L 9/32	H04L	9/00	675B	5J104

審査請求 未請求　請求項の数 13　ＯＬ　（全 19 頁）

(21)出願番号　特願2003-147520(P2003-147520)
(22)出願日　平成15年5月26日(2003.5.26)

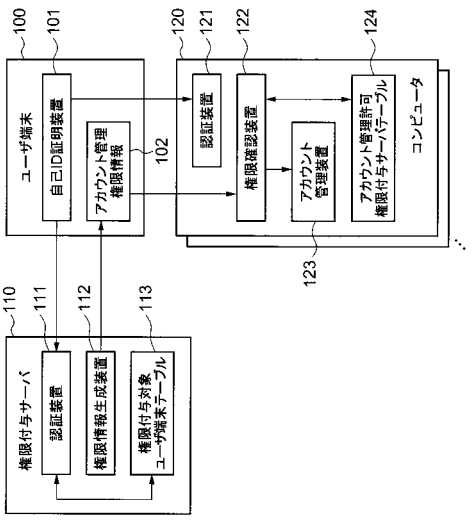
（出願人による申告）国等の委託研究の成果に係る特許出願（経済産業省からの委託研究「情報通信基盤高度化プログラム（ネットワークコンピューティング技術の開発」、産業活力再生特別措置法３０条の適用を受けるもの）

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103090
弁理士　岩壁　冬樹
(74)代理人　100114720
弁理士　須藤　浩
(72)発明者　荒木　拓也
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B045 GG01
5B085 AE09 AE23 BE04 BG01 BG02 BG07 CA02 CA04 CA06
5J104 KA01

(54)【発明の名称】アカウント管理システム、アカウント管理方法およびアカウント管理プログラム

(57)【要約】
【課題】広域分散型の処理環境において、それぞれ異なる管理者が管理する各コンピュータにおけるアカウント管理の負担およびコストを低減できるようにする。
【解決手段】権利付与サーバ１１０は、ユーザ端末ＩＤの認証確認を行うと、アカウント管理権限情報１０２を、インターネットを介してユーザ端末１００に送信する。ユーザ端末１００は、どのコンピュータ１２０に対して計算利用要求を行う場合にも、権利付与サーバ１１０から受信したアカウント管理権限情報１０２をインターネットを介して提示して計算処理要求情報を送信する。アカウント管理権限情報１０２を受信したコンピュータ１２０は、アカウント管理権限情報１０２が示すアカウント管理権限が有効な権限である場合に、ユーザのアカウントを生成し、ユーザの要求に応じて計算処理を実行する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
利用者端末からの要求に応じてコンピュータの資源を利用者に提供するコンピュータシステムにおける利用者のアカウントを管理するアカウント管理システムにおいて、
前記利用者端末は、
利用者を証明するための証明情報を送信する自己証明手段と、
アカウントの管理を要求する権利を表すアカウント管理権限を示す情報をコンピュータに提示するアカウント管理権限提示手段とを備え、
前記コンピュータは、
前記利用者端末から送信された前記証明情報にもとづいて利用者を認証する認証手段と、
前記利用者端末から前記アカウント管理権限が送信された場合に、そのアカウント管理権限が有効であるか否か判断する権限確認手段と、
前記権限確認手段がアカウント管理権限が有効であることを確認したら、アカウントの管理を実行するアカウント管理手段とを備えたことを特徴とするアカウント管理システム。
【請求項２】
権限確認手段がアカウント管理権限が有効であることを確認したら、アカウント管理手段は、アカウントが存在しない場合には自動的にアカウントを生成する請求項１記載のアカウント管理システム。
【請求項３】
利用者端末は、アカウントが生成された後に、コンピュータに対して計算機利用要求を示す情報を送信する請求項１記載のアカウント管理システム。
【請求項４】
アカウント管理権限を発行する権能を有する権限付与サーバを備え、
前記権限付与サーバは、
利用者端末から送信された前記証明情報にもとづいて利用者を認証する認証手段と、
前記証明手段が利用者を認証したら、アカウント管理権限を示す情報を生成して、前記利用者端末に対して送信する権限情報作成手段とを含む請求項１から請求項３のうちのいずれか１項に記載のアカウント管理システム。
【請求項５】
権限付与サーバにおける権限情報作成手段は、電子署名を付したアカウント管理権限を示す情報を生成する請求項４記載のアカウント管理システム。
【請求項６】
コンピュータにおける権限確認手段は、権限付与サーバを証明する証明書を、前記権限付与サーバから直接、または利用者端末を介して受信し、利用者端末から受信したアカウント管理権限を示す情報と前記証明書とにもとづいて、アカウント管理権限が有効であるか否か確認する請求項５記載のアカウント管理システム。
【請求項７】
利用者端末におけるアカウント管理権限提示手段は、
権利付与サーバを証明する第１の証明書と、権利付与サーバによってアカウント管理権限を委譲するために電子署名された第２の証明書とをコンピュータに送信する請求項４記載のアカウント管理システム。
【請求項８】
コンピュータにおける権限確認手段は、利用者端末から受信した第１の証明書および第２の証明書にもとづいて、アカウント管理権限が有効であるか否か確認する請求項７記載のアカウント管理システム。
【請求項９】
コンピュータは、計算処理を終了すると、計算機利用情報を権限付与サーバに送信する請求項４から請求項８のうちのいずれか１項に記載のアカウント管理システム。
【請求項１０】
利用者端末からの要求に応じてコンピュータの資源を利用者に提供するコンピュータシス

テムにおける利用者のアカウントを管理するアカウント管理方法において、
前記利用者端末が、利用者を証明するための証明情報を前記コンピュータに送信するステップと、
前記コンピュータが、前記利用者端末から送信された前記証明情報にもとづいて利用者を認証するステップと、
前記利用者端末が、アカウントの管理を要求する権利を表すアカウント管理権限を示す情報をコンピュータに提示するステップと、
前記コンピュータが、前記利用者端末から受信したアカウント管理権限が有効であるか否か判断するステップと、
前記コンピュータが、アカウント管理権限が有効であることを確認したら、アカウントの管理を実行するステップとを含むことを特徴とするアカウント管理方法。
【請求項１１】
利用者端末が、利用者を証明するための証明情報を、アカウント管理権限を発行する権能を有する権限付与サーバに送信するステップと、
前記権限付与サーバが、利用者端末から送信された前記証明情報にもとづいて利用者を認証するステップと、
前記権限付与サーバが、利用者を認証したら、アカウント管理権限を示す情報を生成して前記利用者端末に対して送信するステップとをさらに含む請求項１０記載のアカウント管理方法。
【請求項１２】
利用者端末からの要求に応じてコンピュータの資源を利用者に提供するコンピュータシステムにおける利用者のアカウントを管理するアカウント管理プログラムであって、
前記コンピュータに、
前記利用者端末から受信した証明情報にもとづいて利用者を認証する処理と、前記利用者端末から、アカウントの管理を要求する権利を表すアカウント管理権限を受信した場合に、そのアカウント管理権限が有効であるか否か判断する処理と、
アカウント管理権限が有効であることを確認したら、アカウントの管理を実行する処理とを実行させるためのアカウント管理プログラム。
【請求項１３】
利用者端末からの要求に応じてコンピュータの資源を利用者に提供するコンピュータシステムにおけるアカウント管理権限を発行する権能を有する権限付与サーバに搭載されるプログラムであって、
前記権限付与サーバに、
前記利用者端末から送信された証明情報にもとづいて利用者を認証する処理と、
利用者を認証したら、アカウント管理権限を示す情報を生成して前記利用者端末に対して送信する処理とを実行させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、利用者端末からの要求に応じてコンピュータの資源を利用者に提供するコンピュータシステムにおける利用者のアカウントを管理するアカウント管理システム、アカウント管理方法およびアカウント管理プログラムに関する。
【０００２】
【従来の技術】
ユーザに、それぞれ異なる管理主体によって管理される複数のコンピュータの資源を利用させる広域分散計算方式（グリッドコンピューティング（以下、単にグリッドという）の一つとして、ユーザが、高速計算処理などを、それぞれ異なるサイトに設置され異なる管理者によって管理されている複数のコンピュータに依頼する方式がある。そのような方式のコンピュータシステムでは、ユーザは、それぞれのコンピュータ毎にアカウントを取得しなければならない。なお、ユーザに利用されるコンピュータの資源は、一般にはコンピ

ュータの計算能力である。また、アカウントは、ユーザのコンピュータ資源利用権能（利用できる資格）である。

【０００３】

複数のコンピュータにおけるアカウントを管理する方式として、マイクロソフト株式会社のＡｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙ（登録商標）などがある。しかし、それらの方式は、単一の管理者が複数のコンピュータのアカウント管理を行うための方式である。すなわち、管理対象の全てのコンピュータのアカウント管理を１台のコンピュータが行う。従って、グリッドのように、複数の管理主体が存在する環境におけるアカウント管理には適用できない。その理由は、グリッドのような広域分散型の計算環境では、個々の管理主体は、サイトの外部に存在するユーザに対してコンピュータの一部の利用権限（例えば、コンピュータの計算能力を利用できる権限のみ）を与え、利用権限の全てを与えることを望まないからである。

【０００４】

非特許文献１には、グリッドによる広域分散型の計算環境におけるアカウント管理システムが記載されている。非特許文献１に記載されているアカウント管理システムでは、公開鍵暗号方式を用いた認証手段と、アクセスコントロールリストと呼ばれる手法を用いた認可手段とによってアカウント管理が行われる。なお、「認証」とは、ユーザが確かにそのユーザ本人であることを確認することをいう。また、「認可」とは、ユーザに何らかの権限を与えることをいう。

【０００５】

非特許文献１に記載されているアカウント管理システムでは、公開鍵暗号方式を用いた認証手段が用いられている。公開鍵暗号による認証方式では、公開鍵と秘密鍵のペアが作成される。秘密鍵で暗号化したデータは公開鍵のみによって復号することができ、公開鍵で暗号化したデータは秘密鍵のみによって復号することができる。ユーザ端末は、秘密鍵を秘匿し、公開鍵を通信ネットワークを介してコンピュータに渡す。従って、コンピュータが乱数などを公開鍵で暗号化したデータを通信ネットワークを介してユーザ端末に渡し、ユーザ端末が秘匿している秘密鍵で受信したデータを復号し、通信ネットワークを介してコンピュータに送り返すことによって、コンピュータがユーザ認証を行うことができる。秘密鍵を保持しているのは秘密鍵を秘匿しているユーザ端末に限られるので、コンピュータは、送り返されたデータと元データとを比較し、それらが一致すればコンピュータは認証が成功したと判断する。

【０００６】

公開鍵暗号方式を用いる場合には、公開鍵が正しいものであるかどうかが問題になる。公開鍵を郵送など別ルートを用いて配布する方法も考えられるが、配布する公開鍵の数が多い場合には負担がかかる。そのために、一般に、ＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ　：認証機関）が発行した証明書が用いられる。すなわち、公開鍵を含む証明書形式のデータが、通信ネットワークを介してコンピュータに渡される。証明書には、証明書保持者名、証明書保持者の公開鍵、およびＣＡによる電子署名などが含まれる。

【０００７】

電子署名とは、ＣＡによってなされた電子的な方法による署名である。例えば、証明書に含まれるデータについて一方向関数にもとづいてハッシュ値を算出し、算出したハッシュ値をＣＡが保持する秘密鍵で暗号化したデータが電子署名として証明書に付加される。一次方向関数として、ＭＤ（Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ　ａｌｇｏｒｉｔｈｍ）５やＳＨＡ（Ｓｅｃｕｒｅ　Ｈｕｓｈ　Ａｌｇｏｒｉｔｈｍ　）－１などと呼ばれるアルゴリズムが用いられる。

【０００８】

コンピュータは、証明書に含まれるデータから算出したハッシュ値と、証明書に含まれる電子署名をＣＡの公開鍵で復号したデータとを比較する。それらが一致すれば、コンピュータは、証明書に含まれる公開鍵がＣＡによって保証されたものであると判断し、ユーザ

端末からの公開鍵を手に入れることができる。なお、ＣＡの公開鍵の入手方法については、コンピュータは、そのＣＡよりさらに上位のＣＡによって署名された証明書を用いることによって入手することができる。コンピュータは、少なくともルートＣＡの証明書をあらかじめ保有していれば、ＣＡの公開鍵を入手することができる。

【０００９】

また、非特許文献１に記載されているアカウント管理システムでは、アクセスコントロールリストと呼ばれる手法を用いた認可手段が用いられている。そのような認可手段では、コンピュータは、あらかじめユーザごとにアカウントを作成する。また、コンピュータは、各アカウントとユーザ名との対応情報を含む対応テーブルを保持する。それぞれのコンピュータ上で計算処理を実行する際には、公開鍵方式を用いた認証確認を行ってユーザ名を確認した後に、コンピュータは、その対応テーブルにもとづいて、証明書に含まれるユーザ名に対応するアカウントが存在するか否かを確認する。そして、コンピュータは、そのユーザ名に対応するアカウントに認可されている権限に従って処理を実行する。

【００１０】

また、非特許文献２には、グリッドによる広域分散型の計算環境における他のアカウント管理システムが記載されている。非特許文献２に記載されているアカウント管理システムは、ＣＡＳ（Ｃｏｍｍｕｎｉｔｙ Ａｕｔｈｏｒｉｚａｔｉｏｎ Ｓｅｒｖｉｃｅ ）と呼ばれるアカウント共有型のシステムである。そのアカウント管理システムでは、公開鍵方式による認証システムを拡張して、ユーザ端末側に権限委譲を行うことを可能にし、権限委譲の機能を利用する。

【００１１】

権限委譲を行うために、権限が委譲される側であるユーザ端末は、新たに証明書と秘密鍵のペアを作成する。ユーザ端末は、作成した証明書に秘密鍵を用いて署名する。ユーザ端末によって署名された証明書はプロキシ証明書と呼ばれる。なお、プロキシ証明書には、有効期限が設定されている。そして、プロキシ証明書に対応する秘密鍵を保持している端末が、ユーザ端末と同じ権限をもつ端末として扱われる。従って、本方式では、ルートＣＡまでつながるＣＡのツリー構造の中に、ユーザ端末が組み込まれたものと考えることができる。

【００１２】

ＣＡＳによるシステムは、このような権限委譲の仕組みを利用したものである。ＣＡＳによるシステムでは、各コミュニティ（サイト）ごとにＣＡＳコンピュータを設置する。また、各リソース（端末）に対して、ＣＡＳコンピュータの権限でアカウントを作成する。ユーザ端末は、ＣＡＳコンピュータによって認証されて、ＣＡＳコンピュータから権限の委譲を受ける。この場合に、委譲される権限を所定の内容に制限して、ユーザ端末は権限を委譲される。例えば、ユーザ端末は、ＣＡＳコンピュータから委譲される権限の内容を示す情報を含む証明書を入手する。

【００１３】

【非特許文献１】

Ｒａｎｄｙ Ｂｕｔｌｅｒ，Ｖｏｎ Ｗｅｌｃｈ ，Ｄｏｕｇｌａｓ Ｅｎｇｅｒｔ，Ｉａｎ Ｆｏｓｔｅｒ，Ｓｔｅｖｅｎ Ｔｕｅｃｋｅ ，Ｊｏｈｎ Ｖｏｌｍｅｒ ，Ｃａｒｌ Ｋｅｓｓｅｌｍａｎ，「Ａ Ｎａｔｉｏｎａｌ－Ｓｃａｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ」，ＩＥＥＥ Ｃｏｍｐｕｔｅｒ ，２０００年，３３巻，１２号，ｐ６０－６６

【非特許文献２】

Ｌａｕｒａ Ｐｅａｒｌｍａｎ，Ｖｏｎ Ｗｅｌｃｈ ，Ｉａｎ Ｆｏｓｔｅｒ，Ｃａｒｌ Ｋｅｓｓｅｌｍａｎ，Ｓｔｅｖｅｎ Ｔｕｅｃｋｅ ，「Ａ Ｃｏｍｍｕｎｉｔｙ Ａｕｔｈｏｒｉｚａｔｉｏｎ Ｓｅｒｖｉｃｅ ｆｏｒ Ｇｒｏｕｐ Ｃｏｌｌａｂｏｒａｔｉｏｎ 」，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ ＩＥＥＥ ３ｒｄ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｗｏｒｋｓｈｏｐ ｏｎ Ｐｏｌｉｃｉｅｓ ｆｏｒ Ｄｉｓｔｒｉｂｕｔｅｄ Ｓｙｓｔｅｍｓ ａｎｄ Ｎｅｔｗｏｒｋｓ，２００２年

【００１４】
【発明が解決しようとする課題】
非特許文献１に記載されているアカウント管理システムでは、広域分散型の計算環境に参加する全てのコンピュータにおいて、ユーザのアカウントを作成しなければならない。また、全てのコンピュータにおいて、アカウントとユーザ名との対応テーブルの更新処理を行わなければならない。従って、各コンピュータの管理者の負担が大きく管理コストが大きい。
【００１５】
また、非特許文献２に記載されているアカウント管理システムでは、アカウントの追加や削除などの処理をＣＡＳコンピュータのみで行えばよい。従って、個々のコンピュータ上でアカウントを作成したり対応テーブルの更新処理を行う必要が無く、管理負担およびコストが軽減される。しかし、ＣＡＳを用いたシステムでは、ユーザ端末は、同一のアカウントを用いて複数のコンピュータに処理を依頼する。すなわち、ＣＡＳを用いたシステムは、共通のアカウントを各コンピュータで使いまわす使いまわし型のモデルと言える。そのため、ファイルの所有者が各コンピュータで同一人になってしなうなどの可能性があり、自分の作成したファイルが他人に閲覧されたり削除される可能性がある。また、ユーザがコンピュータの処理能力を利用した利用時間の統計処理がしにくいとの問題点がある。
【００１６】
そこで、本発明は、利用者端末からの要求に応じてコンピュータの資源を利用者に提供するコンピュータシステムにおける利用者のアカウントの管理に要する負担およびコストを低減できるアカウント管理システム、アカウント管理方法およびアカウント管理プログラムを提供することを目的とする。
【００１７】
【課題を解決するための手段】
本発明によるアカウント管理システムは、利用者端末が、利用者を証明するための証明情報を送信する自己証明手段と、アカウントの管理を要求する権利を表すアカウント管理権限を示す情報をコンピュータに提示するアカウント管理権限提示手段とを備え、コンピュータが、利用者端末から送信された証明情報にもとづいて利用者を認証する認証手段と、利用者端末からアカウント管理権限が送信された場合に、そのアカウント管理権限が有効であるか否か判断する権限確認手段と、権限確認手段がアカウント管理権限が有効であることを確認したら、アカウントの管理を実行するアカウント管理手段とを備えたことを特徴とする。
【００１８】
アカウント管理システムは、アカウント管理権限を発行する権能を有する権限付与サーバをさらに備え、権限付与サーバが、利用者端末から送信された証明情報にもとづいて利用者を認証する認証手段と、証明手段が利用者を認証したら、アカウント管理権限を示す情報を生成して利用者端末に対して送信する権限情報作成手段とを含むように構成されていてもよい。
【００１９】
【発明の実施の形態】
実施の形態１．
以下、本発明の第１の実施の形態を図面を参照して説明する。図１は、本発明によるアカウント管理システムを適用した広域分散型の計算環境の構成の一例を示すブロック図である。図１に示すように、広域分散型の計算環境において、ユーザ（利用者）が使用するユーザ端末（利用者端末）１００、ユーザの要求に応じて計算処理を実行するコンピュータ１２０、およびアカウント管理権限をユーザに対して発行する権限付与サーバ１１０が、インターネットを介して接続される。なお、ユーザ端末１００、コンピュータ１２０および権限付与サーバ１１０は、インターネット以外の通信ネットワークを介して接続されてもよい。また、図１では、１つの権限付与サーバ１１０のみが示されているが、複数の権限付与サーバが存在していてもよい。

【００２０】
ユーザは、ユーザ端末１００を操作して、それぞれ異なるサイトにある複数のコンピュータ１２０に対して計算機利用要求を行うことができる。複数のコンピュータ１２０に対して計算機利用要求を行うことによって、ユーザは、高速に計算処理を実行する仮想的な計算環境を得ることができる。
【００２１】
なお、「アカウント管理権限」とは、ユーザがコンピュータ１２０に対してアカウントの管理（アカウントの生成、更新および削除）を要求することができる権限である。ユーザは、権限付与サーバ１１０から１つのアカウント管理権限を受け取ると、そのアカウント管理権限を多数のコンピュータ１２０に提示することによって、各コンピュータ１２０において、アカウントの管理が実行される。
なお、各コンピュータ１２０は、あらかじめ、権限付与サーバ１１０に対して、アカウント管理権限を発行する権能を与えている。また、ユーザは、複数の権限付与サーバ１１０からアカウント管理権限を発行してもらうこともできる。その場合には、各コンピュータ１２０がそれらの権限付与サーバ１１０にアカウント管理権限を発行する権能を与えていれば、複数の権限付与サーバ１１０から発行されたいずれのアカウント管理権限でも、どのコンピュータ１２０に対してアカウント管理を行わせることができる。
【００２２】
ユーザ端末１００は、ワークステーションなどの情報処理端末である。図１に示すように、ユーザ端末１００は、ユーザであることを証明するための証明情報を保持する自己証明手段としての自己ＩＤ証明装置１０１を含む。自己ＩＤ証明装置１０１は、例えば、あらかじめユーザの識別子（以下、ユーザＩＤという。
）を含む証明情報としての公開鍵証明書を作成してもらい、それを保持する。以下、公開鍵証明書を単に証明書という。なお、証明情報として、単なるＩＤとパスワードとによる、より簡易な構造の情報を用いてもよい。また、ユーザ端末１００は、アカウント管理権限を示す情報をコンピュータ１２０に提示するアカウント管理権限提示手段（図示せず）を含む。
【００２３】
なお、自己ＩＤ証明装置１０１およびアカウント管理権限提示手段は、ユーザ端末１００の記憶装置（図示せず）が記憶するプログラムに従って処理を実行する制御部（演算処理装置：図示せず）によって実現される。
【００２４】
コンピュータ１２０は、ユーザ端末１００からの要求に応じて計算処理を実行する。本実施の形態では、ユーザ端末１００は、それぞれ異なるサイトに設置され管理者が異なる複数のコンピュータ１２０を、インターネットを介してアクセス可能である。各コンピュータ１２０は、ユーザ端末１００に対してそれぞれ別々にアカウントを生成したり、アカウントの属性変更や削除などの処理を行う。
以下、ユーザ端末１００に対してアカウントを発行したり、アカウントの属性変更や削除などの処理を行うことをアカウント管理を行うという。なお、アカウントの属性変更とは、コンピュータ１２０に登録されているアカウントについてユーザグループを変更したりすること等である。
【００２５】
図１に示すように、コンピュータ１２０は、ユーザを認証する（具体的にはユーザＩＤを認証する）認証手段としての認証装置１２１、ユーザ端末１００から受信したアカウント管理権限が有効であるか否か判断する権限確認手段としての権限確認装置１２２、およびアカウント管理を行うアカウント管理手段としてのアカウント管理装置１２３を含む。また、コンピュータ１２０の記憶装置（図示せず）は、コンピュータ１２０がアカウント管理権限を発行する権能を与えている権限付与サーバ１１０の識別子（以下、権限付与サーバＩＤという。）が記載されたアカウント管理許可権限付与サーバテーブル１２４を含む。なお、認証装置１２１、権限確認装置１２２、およびアカウント管理装置１２３は、コ

ンピュータ１２０の記憶装置に記憶されているプログラムに従って処理を実行する制御部（演算処理装置：図示せず）によって実現される。

【００２６】

権限付与サーバ１１０は、例えば、アカウント管理権限を発行する権能を与えられているアカウント管理業者によって運営される。インターネットを介してアクセスのあったユーザ端末１００に対してアカウントの作成などをしてよいか否かを判断する処理、すなわちユーザ端末１００がアカウント管理の要求を行える端末であるか否かを判断する処理は、本来コンピュータ１２０自身が行う処理である。本実施の形態では、権限付与サーバ１１０は、コンピュータ１２０に代行してユーザ端末１００がアカウント管理の要求を行える端末であるか否かを判断する権能を与えられている。

【００２７】

なお、コンピュータ１２０において、権限付与サーバ１１０の識別子がアカウント管理許可権限付与サーバテーブル１２４に記載されるということは、その権限付与サーバ１１０がアカウント管理権限をユーザに対して発行すれば、権限付与サーバ１１０が発行したアカウント管理権限を信頼して、発行を受けたユーザからのアカウント管理権限の提示に応じてアカウント管理を行うということを、コンピュータ１２０が権限付与サーバ１１０に認めたことを意味する。換言すれば、権限付与サーバ１１０に、ユーザ端末１００がアカウント管理の要求を行える端末であるか否かを判断する権能を与えたことを意味する。

【００２８】

図１に示すように、権限付与サーバ１１０は、ユーザを認証する、具体的にはユーザＩＤを認証する認証手段としての認証装置１１１、およびアカウント管理権限を示す情報であるアカウント管理権限情報１０２を発行する権限情報作成手段としての権限情報生成装置１１２を含む。また、権限付与サーバ１１０の記憶装置（図示せず）は、あらかじめ契約を締結しているユーザのユーザＩＤが記載されている権限付与対象ユーザ端末テーブル１１３を記憶している。なお、認証装置１１１および権限情報生成装置１１２は、権限付与サーバ１１０の記憶装置に記憶されているプログラムに従って処理を実行する制御部（演算処理装置：図示せず）によって実現される。

【００２９】

なお、契約締結の際に、権限付与サーバ１１０の記憶装置には、ユーザの住所や利用代金の徴収のためのクレジットカード番号などの情報が登録される。また、ＩＤなどの認証確認のために証明書を用いる場合には、あらかじめ契約によって権限付与サーバ１１０が信頼するＣＡが指定される。この場合に、権限付与サーバ１１０が信頼する複数のＣＡが指定され、ユーザは、その複数のＣＡの中から署名をうけるＣＡを選択できるようにしてもよい。

【００３０】

図２は、ユーザ端末１００における自己ＩＤ証明装置１０１および権限付与サーバ１１０における認証装置１１１が実行する処理を説明するためのブロック図である。

【００３１】

自己ＩＤ証明装置１０１は、公開鍵暗号方式のアルゴリズムに従って秘密鍵３０１および公開鍵３１２を生成する。なお、秘密鍵３０１および公開鍵３１２を、ＣＡ等の第三者に生成してもらうこともできる。自己ＩＤ証明装置１０１は、秘密鍵３０１を保持する。また、自己ＩＤ証明装置１０１は、公開鍵３１２およびＩＤ３１３（本例では、ユーザＩＤ）を含む証明情報としての証明書３１１をＣＡ３２０に発行してもらう。証明書３１１は、あらかじめアカウント管理業者とユーザとの契約時に指定されたＣＡ３２０によって署名（電子署名：ディジタル署名）されている。本実施の形態では、証明書にＣＡによって署名データが付加されていることを、単に「ＣＡによって署名されている」という。署名３１１ａは、証明書３１１に含まれるデータのハッシュ値をＣＡ３２０の秘密鍵で暗号化したデータである。

【００３２】

また、権限付与サーバ１１０の記憶装置は、あらかじめ指定されたＣＡ３２０の証明書３

１４を記憶している。証明書３１４には、ＣＡ３２０の公開鍵３１５が存在する。
【００３３】
ユーザ端末１００は、証明情報としての証明書３１１を、インターネットを介して権限付与サーバ１１０に送信する。証明書３１１を受信すると、認証装置１１１は、ＣＡの証明書３１４に含まれるＣＡの公開鍵３１５によって署名３１１ａを復号する。また、認証装置１１１は、証明書３１１に含まれるデータのハッシュ値を算出する。そして、認証装置１１１は、算出したハッシュ値と、署名３１１ａを復号して得られたハッシュ値とを比較する。それらが一致した場合には、認証装置１１１は、証明書３１１がＣＡ３２０によって署名されたものであると判断する。
【００３４】
次に、認証装置１１１は、証明書３１１に含まれる公開鍵３１２によって乱数データを暗号化したデータ（以下、乱数暗号データという）を生成する。権限付与サーバ１１０は、認証装置１１１が生成した乱数暗号データを、インターネットを介してユーザ端末１００に送信する。ユーザ端末１００が乱数暗号データを受信すると、自己ＩＤ証明装置１０１は、保持している秘密鍵３０１によって乱数暗号データを乱数データに復号する。ユーザ端末１００は、復号した乱数データを、インターネットを介して権限付与サーバ１１０に送信する。
【００３５】
権限付与サーバ１１０の認証装置１１１は、受信した乱数データと、公開鍵３１２によって暗号化される前の乱数データとを比較する。それらが一致した場合には、認証装置１１１は、証明書３１１に含まれるＩＤ３１３が、公開鍵３１２に対応する秘密鍵３０１を保有しているユーザのユーザＩＤであると判断する。
【００３６】
なお、ユーザＩＤの確認方法は、公開鍵暗号方式および証明書を用いた方法に限られない。例えば、Ｋｅｒｂｅｒｏｓなど共通鍵暗号方式を用いた方法によって、ユーザＩＤを確認してもよい。また、例えば、コンピュータ１２０は、インターネットを介してユーザ端末１００から受信したユーザＩＤおよびパスワードをにもとづいて、ユーザＩＤを確認してもよい。
【００３７】
また、上記のユーザＩＤの確認方法は、コンピュータ１２０における認証装置１２１とユーザ端末１００における自己ＩＤ証明装置１０１との間でも使用される。
【００３８】
図３は、権限付与サーバ１１０における権限情報生成装置１１２およびコンピュータ１２０における権限確認装置１２２の動作を説明するためのブロック図である。権限付与サーバ１１０は、ユーザ端末１００の要求に応じて、ユーザ端末１００にアカウント管理権限情報１０２を送信する。本例では、アカウント管理権限情報１０２は、ユーザ端末１００からコンピュータ１２０に対するアカウント管理の要求が認められるべき旨が記述されているアカウント作成許可情報４０４を含む。また、図３に示すように、アカウント管理権限情報１０２は、ユーザＩＤ４０２および権限付与サーバＩＤ４０３を含む。権限付与サーバＩＤ４０３は、アカウント管理権限を発行した権限付与サーバを特定するための情報である。さらに、アカウント管理権限情報１０２は、権限付与サーバ１１０によって署名されている。すなわち、アカウント管理権限情報１０２は、権限付与サーバ１１０による署名４０５を含む
【００３９】
コンピュータ１２０は、あらかじめ権限付与サーバ１１０の証明書４２３を権限付与サーバ１１０から受信して保持している。コンピュータ１２０は、例えば、アカウント管理業者との契約の際に郵送などによって取得した権限付与サーバの証明書４２３を、記憶装置などにあらかじめ記憶させる。また、コンピュータ１２０は、権限付与サーバの証明書４２３を、アカウント管理権限情報１０２とともにユーザ端末１００を介して受信してもよい。権限付与サーバの証明書４２３は、権限付与サーバの公開鍵４２４および権限付与サ

ーバＩＤ４２５を含む。また、権限付与サーバの証明書４２３は、あらかじめ契約の際に指定されたＣＡ３２０によって署名されている。従って、権限付与サーバの証明書４２３は、コンピュータ１２０が信頼するＣＡ３２０による署名４２６を含む。

【００４０】

また、コンピュータ１２０は、あらかじめＣＡ３２０の証明書４２１を取得し、記憶装置などに記憶させている。コンピュータ１２０は、ＣＡの証明書４２１に含まれるＣＡの公開鍵４２２を用いて、権限付与サーバの証明書４２３が、権限付与サーバ１１０が発行した証明書であることを確認する。また、コンピュータ１２０のアカウント管理許可権限付与サーバテーブル１２４には、アカウント管理権限を発行する権能が与えられている権限付与サーバ１１０のＩＤが記載されている権限付与サーバＩＤリスト４２７が含まれる。よって、権限付与サーバＩＤリスト４２７に記載されていない権限付与サーバの証明書４２３は無効である。

【００４１】

ユーザ端末１００からアカウント管理権限情報１０２を受信すると、コンピュータ１２０は、アカウント管理権限情報１０２に含まれる署名４０５を、署名４０５を行った権限付与サーバの証明書４２３の公開鍵４２４によって復号する。また、コンピュータ１２０は、アカウント管理権限情報１０２に含まれるデータのハッシュ値を算出する。そして、コンピュータ１２０は、算出したハッシュ値と復号した署名４０５の値とを比較する。それらの値が一致する場合には、コンピュータ１２０は、アカウント管理権限情報１０２が権限付与サーバ１１０によって発行されたものであると判断する。すなわち、ユーザ端末１００が提示したアカウント管理権限が有効であると判定する。

【００４２】

以上のように、コンピュータ１２０の権限確認装置１２２は、ユーザ端末１００がアカウント管理権限を提示した場合に、そのアカウント管理権限を発行した権限付与サーバが、アカウント管理権限を発行する権能を有する権限付与サーバであるか否かを確認する。そして、権能を有する権限付与サーバであることが確認されたら、ユーザ端末１００が提示したアカウント管理権限を有効であるとし、アカウント管理装置１２３に、アカウント管理を実行させる。

【００４３】

次に動作について説明する。図４は、ユーザ端末１００からの要求に応じた計算のための処理およびアカウント管理の処理を示すフローチャートである。ユーザは、ユーザ端末１００を操作して、コンピュータ１２０に処理を実行させるためのコマンドを入力する。

【００４４】

コンピュータ１２０に実行させる処理は、一般には計算処理である。しかし、既にコンピュータ１２０に登録されているアカウントの属性変更や削除などのアカウント管理の処理を要求することもある。よって、ユーザは、コンピュータ１２０に対して計算機利用要求を行いたい場合には、計算処理を実行させるためのコマンドを入力する。また、既にコンピュータ１２０に登録されているアカウントのアカウント管理の処理を行わせたい場合には、アカウント管理を行うためのコマンドを入力する。コマンドが入力されると、ユーザ端末１００、権限付与サーバ１１０およびコンピュータ１２０によって、以下に示すステップＳ１０１からステップＳ１１８までの処理が自動的に実行される。

【００４５】

ユーザ端末１００にコマンドが入力されると、ユーザ端末１００において、自己ＩＤ証明装置１０１は、インターネットを介して証明情報を権限付与サーバ１１０に送信する（ステップＳ１０１）。権限付与サーバ１１０が証明情報を受信すると、権限付与サーバ１１０の認証装置１１１は、受信した証明情報にもとづいてユーザＩＤを確認する（ステップＳ１０２）。

【００４６】

ユーザＩＤを確認すると、認証装置１１１は、アクセスしてきたユーザ端末１００が、権限付与対象ユーザ端末テーブル１１３に記載されているユーザ端末であるか否か判断する

（ステップＳ１０３）。権限付与対象ユーザ端末テーブル１１３に記載されている場合には、認証装置１１１は、ユーザ端末１００に対してアカウント管理権限を発行してよいと判断する。

【００４７】

アカウント管理権限を発行してよいと判断すると、権限付与サーバ１１０の権限情報生成装置１１２は、アカウント管理権限情報１０２を発行する（ステップＳ１０４）。そして、権限付与サーバ１１０は、アカウント管理権限情報１０２を、インターネットを介してユーザ端末１００に送信する（ステップＳ１０４）。ユーザ端末１００は、アカウント管理権限情報１０２を受信すると、アカウント管理権限情報１０２をユーザ端末１００の記憶装置などに一旦記憶させる。

【００４８】

なお、ステップＳ１０２においてユーザＩＤが確認できなかった場合には、権限情報生成装置１１２は、アカウント管理権限情報１０２を発行しない。また、ステップＳ１０３において、ユーザ端末１００が、アカウント管理権限の発行を受けるべきでないユーザ端末であることが確認された場合、すなわち権限付与対象ユーザ端末テーブル１１３に記載されていないユーザ端末であることが確認された場合には、権限情報生成装置１１２は、アカウント管理権限情報１０２を発行しない。

【００４９】

次に、ユーザ端末１００において、自己ＩＤ証明装置１０１は、証明情報を、インターネットを介してコンピュータ１２０に送信する（ステップＳ１０５）。証明情報を受信すると、コンピュータ１２０の認証装置１２１は、受信した証明情報にもとづいてユーザ端末１００のユーザＩＤを確認する（ステップＳ１０６）。なお、認証装置１２１によるユーザＩＤを確認する処理は、権限付与サーバ１０における認証装置１１１による処理と同じである。

【００５０】

また、ユーザ端末１００は、アカウント管理権限情報１０２を、インターネットを介してコンピュータ１２０に送信する（ステップＳ１０７）。そして、ユーザ端末１００は、ユーザによって入力されたコマンドがコンピュータ１２０に計算処理を要求するものであるか、アカウント管理を要求するものであるかを判断する（ステップＳ１０８）。計算処理を要求するコマンドである場合には、ユーザ端末１００は、インターネットを介して、要求する計算内容とともに計算処理を要求する旨の計算要求情報をコンピュータ１２０に送信する（ステップＳ１０９）。アカウント管理の処理を要求するコマンドである場合には、ユーザ端末１００は、インターネットを介して、アカウント管理を要求する旨のアカウント管理要求情報をコンピュータ１２０に送信する（ステップＳ１１０）。

【００５１】

コンピュータ１２０は、受信した要求情報が計算要求情報であるかアカウント管理要求情報であるかを判断する（ステップＳ１１１）。計算要求情報であると判断した場合には、コンピュータ１２０のアカウント管理装置１２３は、ステップＳ１０６で確認したユーザＩＤに対応するアカウントが存在しているか否かを判断する（ステップＳ１１２）。例えば、ユーザ端末１００が過去にコンピュータ１２０に対して計算機利用要求を行ったことがある場合には、そのユーザのアカウントは、有効期間内であれば既に登録されている。

【００５２】

ステップＳ１１２においてアカウントが存在していないと判断した場合には、コンピュータ１２０の権限確認装置１２２は、ユーザ端末１００から受信したアカウント管理権限情報１０２やアカウント管理許可権限付与サーバテーブル１２４の内容等にもとづいて、そのユーザのアカウントを作成してよいか否か確認する（ステップＳ１１３）。

【００５３】

ユーザのアカウントを作成してよいことが確認されると、アカウント管理装置１２３は、ユーザ端末１００に対するアカウントを生成する（ステップＳ１１４）。なお、本実施の形態において、コンピュータ１２０は、生成したアカウントを、ユーザ端末１００に通知

する必要はない。

【００５４】

アカウントを生成すると、コンピュータ１２０は、要求された計算処理を実行する（ステップＳ１１５）。計算処理を終了すると、コンピュータ１２０は、ユーザ端末１００がコンピュータ１２０を利用した利用時間などを示す計算機利用情報を、インターネットを介して権限付与サーバ１１０に送信する（ステップＳ１１６）。権限付与サーバ１１０は、受信した計算機利用情報にもとづいて、ユーザ端末１００に対する課金処理を行う。

【００５５】

ステップＳ１１２において、既にアカウントが存在していると判断した場合には、コンピュータ１２０は、ステップＳ１１３およびステップＳ１１４の処理を実行しない。この場合には、コンピュータ１２０は、既に登録されているアカウントにもとづいて、要求された計算処理を実行する（ステップＳ１１５）。そして、計算処理が終了すると、コンピュータ１２０は、計算機利用情報を、インターネットを介して権限付与サーバ１１０に送信する（ステップＳ１１６）。

【００５６】

ステップＳ１１１において、受信した要求がアカウント管理要求情報であると判断した場合には、権限確認装置１２２は、アカウント管理権限情報１０２等にもとづいて、ユーザ端末１００がアカウント管理権限を有するユーザの端末であるか否か確認する（ステップＳ１１７）。例えば、ユーザが既に登録されているアカウントの属性変更や削除などの処理を要求する場合に、アカウント管理要求情報がユーザ端末１００から送信される。

【００５７】

アカウント管理権限を有するユーザの端末であることが確認されると、アカウント管理装置１２３は、要求されたアカウント管理を実行する（ステップＳ１１８）。例えば、アカウントの削除を要求された場合には、アカウント管理装置１２３は、ユーザ端末１００に対応するアカウントを削除する。また、アカウントの属性変更を要求された場合には、アカウント管理装置１２３は、ユーザ端末１００に対応するアカウントのユーザグループの変更など属性変更の処理を行う。

【００５８】

なお、ユーザ端末１００は、ステップ１０７においてアカウント管理権限情報１０２をコンピュータ１２０に送信するのでなく、コンピュータ１２０から要求があった場合に送信するようにしてもよい。例えば、ステップＳ１１１において要求がアカウント管理の処理の要求であることを確認した場合や、ステップＳ１１２においてアカウントが存在していないことを確認した場合に、コンピュータ１２０は、ユーザ端末１００にアカウント管理権限情報１０２を要求する。そして、ユーザ端末１００は、コンピュータ１２０から要求に応じてアカウント管理権限情報１０２をコンピュータ１２０に送信する。

【００５９】

また、ステップＳ１１６において、コンピュータ１２０は、計算機利用情報を計算処理が完了する毎に送信するのでなく所定の期間ごとに送信してもよい。例えば、コンピュータ１２０は、あらかじめ契約で定めた所定期間ごとに、その所定期間内にユーザ端末１００がコンピュータ１２０を利用した利用時間の合計値を含む計算機利用情報を送信するようにしてもよい。

【００６０】

権限付与サーバ１１０は、あらかじめ契約で定めた所定期間ごとに、ユーザ端末１００からコンピュータ１２０の利用代金を徴収する。例えば、権限付与サーバ１１０は、あらかじめ登録しているユーザのクレジットカード情報などにもとづいて利用代金を徴収する。そして、権限付与サーバ１１０は、徴収した利用代金を、オンライン振り込みなどを利用して各コンピュータ１２０に配分する。なお、利用代金の徴収や配分の処理は、オンライン処理によらず人為的な手続きによって行ってもよい。

【００６１】

以上のように、本実施の形態によれば、ユーザは、権限付与サーバ１１０から発行された

アカウント管理権限を、計算を依頼するコンピュータ１２０に提示するだけで、コンピュータ１２０において、自動的に、そのユーザのアカウントが生成される。すなわち、権限確認装置１２２がアカウント管理権限が有効であることを確認したら、アカウント管理装置１２３は、アカウントが存在しない場合には自動的にアカウントを生成する。従って、広域分散計算環境に存在する全てのコンピュータが、上記のコンピュータ１２０の機能と同じ機能を有していれば、ユーザは、いずれのコンピュータに計算を依頼するときにも、アカウント管理権限を提示するだけで、いずれのコンピュータにおいてもアカウントが生成される。

【００６２】

すなわち、そのユーザに対して、各コンピュータにアカウント管理の要求を行ってもよいか否かを判断する権能を権限付与サーバ１１０に与えることによって、各コンピュータは、アクセスしてきたユーザ端末１００を使用しているユーザのアカウントを生成してよいか否か判断する必要はない。よって、それぞれ異なる管理者が管理する各コンピュータにおけるアカウント管理の負担およびコストを低減することができる。

【００６３】

また、ユーザは、広域分散計算環境に存在する多数のコンピュータに対して一々アカウント管理のための手続を踏むことなく、一つまたは少数の権限付与サーバにアカウント管理権限を発行してもらうだけで、各コンピュータにおいてアカウントを生成してもらうことができるようになる。さらに、ユーザは、計算処理の要求先のコンピュータ１２０が既にアカウントが登録されているコンピュータであるか否かを意識せずに、計算処理の要求を行うことができる。すなわち、ユーザは、アカウントが登録されているコンピュータであるか否かにかかわらず、同じ手順で計算処理を要求することができる。

【００６４】

さらに、本実施の形態によれば、コンピュータ１２０が権限付与サーバ１１０に計算機利用情報を送信するので、権限付与サーバ１１０が、コンピュータ１２０に代行してユーザに対する課金処理を行うことができる。従って、権限付与サーバ１１０が、コンピュータ１２０に代行して利用代金の徴収を行うことができる。

【００６５】

実施の形態２．

次に、本発明の第２の実施の形態を図面を参照して説明する。本実施の形態における広域分散型の計算環境の構成は、図１に示した構成と同様である。しかし、権限付与サーバ１１０における権限情報生成装置およびコンピュータにおける権限確認装置の動作は、第１の実施の形態の場合とは異なる。本実施の形態では、権限の委譲という概念を利用して、権限付与サーバが有するアカウント管理権限をユーザに委譲し、ユーザが、委譲されたアカウント管理権限にもとづいて、各コンピュータにアカウント管理を依頼する。

【００６６】

図５は、権限付与サーバ１１０における権限情報生成装置１１２およびコンピュータ１２０における権限確認装置１２２の動作を説明するためのブロック図である。権限付与サーバ１１０は、あらかじめ公開鍵Ａ５１２および秘密鍵Ａ５１４を生成し、公開鍵Ａ５１２を含む第１の証明書としての証明書Ａ５１１をＣＡ等に生成してもらう。証明書Ａ５１１は、権限付与サーバ１１０を証明する証明書であり、権限付与サーバＩＤ５１３を含む。証明書Ａ５１１は、あらかじめ指定されたＣＡ５３０によって署名されている。従って、証明書Ａ５１１は、ＣＡ５３０による署名５１１ａを含む。

【００６７】

ユーザ端末１００は、あらかじめ公開鍵Ｂ５０２および秘密鍵Ｂ５０４を生成している。また、ユーザ端末１００は、第２の証明書としての新たな証明書Ｂ５０１をＣＡ等に生成してもらう。証明書Ｂ５０１は、公開鍵Ｂ５０２および権限付与サーバＩＤ５０３を含む。なお、証明書Ｂ５０１は、権限付与サーバ１１０によって生成され、インターネットを介してユーザ端末１００が権限付与サーバ１１０から受信したものであってもよい。また、証明書Ｂ５０１には、アカウント管理権限の内容が明記されていてもよい。

【００６８】
本実施の形態では、権限付与サーバ１１０が、証明書Ｂ５０１に秘密鍵Ａ５１４を用いて署名５０１ａを行うことによって、ユーザ端末１００に、アカウント管理権限を委譲する。
【００６９】
ユーザ端末１００は、権限の委譲を受ける際に、証明書Ｂ５０１について署名を受けるとともに、権限付与サーバ１１０からインターネットを介して証明書Ａ５１１を受信する。そして、ユーザ端末１００は、計算処理を依頼するとき、またはアカウントの更新を依頼するときなどに、証明書Ａ５１１および証明書Ｂ５０１を、インターネットを介してコンピュータ１２０に送信する。
【００７０】
コンピュータ１２０は、あらかじめＣＡ５３０の証明書５２１を保持している。コンピュータ１２０は、証明書Ａ５１１および証明書Ｂ５０１を受信すると、ＣＡの証明書５２１に含まれるＣＡの公開鍵５２２によって、証明書Ａ５１１がＣＡ５３０によって署名された証明書であるか否か確認する。
【００７１】
コンピュータ１２０は、証明書Ａ５１１がＣＡ５３０によって署名された証明書であることを確認したら、証明書Ａ５１１に含まれる公開鍵Ａ５１２によって、証明書Ｂ５０１が権限付与サーバ１１０によって署名された証明書であるか否か確認する。
【００７２】
次に、コンピュータ１２０は、ユーザ端末１００の認証を行う。すなわち、コンピュータ１２０は、乱数データを公開鍵Ｂ５０２によって暗号化して乱数暗号データを生成し、インターネットを介してユーザ端末１００に送信する。ユーザ端末１００は、受信した乱数暗号データを秘密鍵Ｂ５０４によって乱数データに復号する。そして、ユーザ端末１００は、復号した乱数データを、インターネットを介してコンピュータ１２０に送信する。
【００７３】
コンピュータ１２０は、受信した乱数データと、公開鍵Ｂ５０２によって暗号化する前の乱数データとを比較する。これらの乱数データが一致した場合には、コンピュータ１２０は、ユーザ端末１００の認証に成功したと判断する。以上の処理によって、コンピュータ１２０は、ユーザ端末１００が権限付与サーバ１１０によってアカウント管理権限の委譲を受けた端末であると判断する。換言すれば、ユーザ端末１００が委譲されたアカウント管理権限が有効であると判定する。
【００７４】
ユーザ端末１００がアカウント管理権限の委譲を受けた端末であることが確認されると、コンピュータ１２０は、証明書Ａ５１１に含まれる権限付与サーバＩＤ５１３が権限付与サーバＩＤリスト５２４に含まれるか否かを判断する。権限付与サーバＩＤリスト５２４に含まれる場合には、コンピュータ１２０は、アカウント管理権限に従ってアカウント管理処理を実行する。
【００７５】
以上のように、権限付与サーバ１１０によるアカウント権限の発行の仕方、およびコンピュータ１２０Ａにおけるユーザ ＩＤを確認する処理や権限を確認する処理は第１の実施の形態の場合とは異なるが、その他の処理は、第１の実施の形態の場合と同じである。
【００７６】
本実施の形態によれば、ユーザが権限付与サーバ１１０からアカウント管理権限の委譲を受けたと捉え、アカウント管理権限の委譲を受けたユーザは、委譲されたアカウント管理権限にもとづいて、コンピュータ１２０に対して計算処理やアカウント管理の処理を要求することができる。
【００７７】
また、第１の実施の形態と同様に、広域分散計算環境において、それぞれ異なる管理者が管理する各コンピュータのアカウント管理の負担およびコストを低減することができる。

【００７８】
実施の形態３．
次に、本発明の第３の実施の形態を図面を参照して説明する。本実施の形態における広域分散型の計算環境の構成は、図１に示した構成と同様である。第１の実施の形態では、アカウントが登録されていないユーザ端末１００から計算処理要求がなされた場合に、コンピュータ１２０は、自動的に、アカウントを生成して、要求された計算処理を実行した。しかし、本実施の形態では、コンピュータ１２０は、ユーザ端末１００から計算処理要求がなされたときにアカウントを生成するのではなく、アカウント生成の要求に応じてアカウントを生成する。すなわち、ユーザは、アカウントの登録が完了した後に、コンピュータ１２０に計算処理を要求する。
【００７９】
図６は、ユーザ端末１００からの要求に応じて実行されるアカウント生成を含むアカウント管理の処理を示すフローチャートである。ユーザは、ユーザ端末１００を操作して、アカウント管理を要求するためのコマンドを入力する。例えば、コンピュータ１２０にアカウントが登録されていない場合には、ユーザは、まずアカウントの生成を要求するコマンドを入力する。なお、コマンドが入力されると、ユーザ端末１００、権限付与サーバ１１０およびコンピュータ１２０は、以下に示すステップＳ２０１からステップＳ２０９までの処理を自動的に実行する。
【００８０】
ユーザ端末１００は、ユーザの操作に応じて、インターネットを介して権限付与サーバ１１０に証明情報を送信する（ステップＳ２０１）。権限付与サーバ１１０が証明情報を受信すると、認証装置１１１は、受信した証明情報にもとづいてユーザＩＤを確認する（ステップＳ２０２）。
【００８１】
ユーザＩＤを確認すると、認証装置１１１は、権限付与対象ユーザ端末テーブル１１３を参照して、アクセスしてきたユーザ端末１００が、アカウント管理権限を付与してよい端末であるか否かを判断する（ステップＳ２０３）。アカウント管理権限を付与してよい端末と判断すると、権限情報生成装置１１２は、アカウント管理権限情報１０２を発行する（ステップＳ２０４）。
【００８２】
次に、ユーザ端末１００は、証明情報を、インターネットを介してコンピュータ１２０に送信する（ステップＳ２０５）。コンピュータ１２０が証明情報を受信すると、認証装置１２１は、受信した証明情報にもとづいてユーザ端末１００のユーザＩＤを確認する（ステップＳ２０６）。なお、ユーザＩＤを確認する具体的な構成は図３に示す構成と同様であり、処理手順は図２に示すステップＳ１０１およびステップＳ１０２の場合と同様である。
【００８３】
ユーザ端末１００は、アカウント管理権限情報１０２を、インターネットを介してコンピュータ１２０に送信する（ステップＳ２０７）。また、ユーザ端末１００は、アカウント管理要求情報を、インターネットを介してコンピュータ１２０に送信する（ステップＳ２０７）。以上の処理は、第１の実施の形態における処理と同じである。
【００８４】
コンピュータ１２０は、受信したアカウント管理権限情報１０２およびアカウント管理許可権限付与サーバテーブル１２４にもとづいて、ユーザ端末１００がアカウント管理権限の付与を受けることができる端末であるか否か確認する（ステップＳ２０８）。
【００８５】
ステップＳ２０８において、アカウント管理権限の付与を受けることができる端末であることが確認されると、アカウント管理装置１２３は、要求されたアカウント管理の処理を実行する（ステップＳ２０９）。例えば、アカウントの生成を要求された場合には、アカウント管理装置１２３は、ユーザ端末１００に対するアカウントを生成する。なお、既に

登録済みのアカウントの属性変更や削除が要求された場合には、アカウント管理装置１２３は、アカウントの属性変更や削除を行う。

【００８６】

次に、ユーザ端末１００からの要求に従って計算処理を実行する場合の動作について説明する。図７は、ユーザ端末１００から要求された計算処理を実行する処理を示すフローチャートである。ユーザは、アカウントが既に登録済みでありコンピュータ１２０に計算処理を依頼する場合に、ユーザ端末１００を操作して、計算処理を要求するためのコマンドを入力したりプログラムを実行する。なお、コマンドが入力されると、ユーザ端末１００およびコンピュータ１２０によって、以下に示すステップＳ３０１からステップＳ３０５までの処理が自動的に実行される。

【００８７】

ユーザ端末１００は、ユーザの操作に従って、コマンドが入力されると、証明情報を、インターネットを介して権限付与サーバ１１０に送信する（ステップＳ３０１）。コンピュータ１２０が証明情報を受信すると、認証装置１２１は、受信した証明情報にもとづいてユーザＩＤを確認する（ステップＳ３０２）。ユーザＩＤを確認し既にアカウントが登録されているユーザ端末１００であることを確認すると、コンピュータ１２０は、ユーザＩＤおよびアカウントを確認できた旨を示す確認情報を、インターネットを介してユーザ端末１００に送信する。すると、ユーザ端末１００は、要求したい計算内容を含む計算要求情報を、インターネットを介してコンピュータ１２０に送信する（ステップＳ３０３）。

【００８８】

計算要求情報を受信すると、コンピュータ１２０は、要求された計算処理を実行する（ステップＳ３０４）。計算処理が終了すると、コンピュータ１２０は、計算機利用情報を、インターネットを介して権限付与サーバ１１０に送信する（ステップＳ３０５）。そして、権限付与サーバ１１０は、受信した計算機利用情報にもとづいて、ユーザ端末１００に対する課金処理を行う。

【００８９】

以上のように、本実施の形態によれば、コンピュータ１２０に計算を実行させるための処理と、アカウント管理の処理とが独立して実行される。従って、ユーザは、アカウントが生成された後に、コンピュータ１２０に対して計算機利用要求を示す情報を送信する。第１の実施の形態の場合とは異なり、コンピュータ１２０に計算を実行させる際に権限確認処理を実行しないので、計算機利用要求の際の処理工程を軽減することができる。また、従来から存在する計算処理を要求するためのプロトコルをそのまま利用することができ、システム構築のための負担やコストを低減することができる。

【００９０】

なお、第１の実施の形態および第３の実施の形態において、ユーザ端末１００がアカウント管理権限情報１０２を権限付与サーバ１１０から受信することによって入手する場合を説明したが、ユーザは、ＣＤ－ＲＯＭ等の記録媒体に書き込まれたアカウント管理権限情報１０２を郵送等によって入手してもよい。その場合には、例えば、図４および図６に示す処理において、ステップＳ１０１～ステップＳ１０４の処理およびステップＳ２０１～Ｓ２０４を実行する必要がなくなる。

【００９１】

また、権限付与サーバ１１０を設置する必要はなく、アカウント管理業者にかかる管理負担およびコストを軽減することができる。なお、権限付与サーバ１１０からアカウント管理権限をオンラインで入手する場合に比べて、アカウント管理権限情報１０２の有効期限は十分長く設定される。また、アカウント管理業者は、ユーザ端末１００に対する課金処理のみを行うためのコンピュータを設置してもよい。

【００９２】

【発明の効果】

以上のように、本発明によれば、アカウント管理システム、アカウント管理方法およびアカウント管理プログラムは、コンピュータが、利用者端末から送信された証明情報にもと

づいて利用者を認証し、利用者端末からアカウント管理権限が有効であることを確認したらアカウントの管理を実行するように構成されているので、広域分散型の計算環境において、それぞれ異なる管理者が管理する各コンピュータのアカウント管理の負担およびコストを低減することができる。

【００９３】

また、利用者端末から送信された証明情報にもとづいて利用者を認証し、証明手段が利用者を認証したらアカウント管理権限を示す情報を生成して利用者端末に対して送信する権限付与サーバが設けられている場合には、利用者端末は、オンラインでアカウント管理権限を得ることができる。

【図面の簡単な説明】

【図１】本発明によるアカウント管理システムを適用した広域分散型の計算環境の構成の一例を示すブロック図である。

【図２】自己ＩＤ証明装置および認証装置が実行する処理を説明するためのブロック図である。

【図３】権限情報生成装置および権限確認装置の動作を説明するためのブロック図である。

【図４】計算のための処理およびアカウント管理の処理を示すフローチャートである。

【図５】権限情報生成装置および権限確認装置　の動作を説明するためのブロック図である。

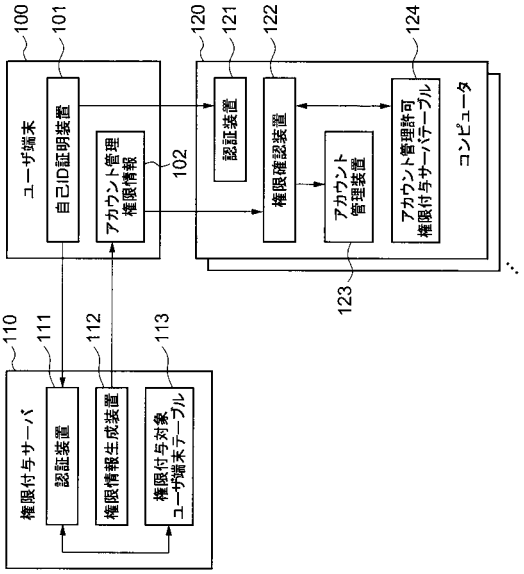
【図６】アカウント管理の処理を示すフローチャートである。

【図７】計算のための処理を示すフローチャートである。

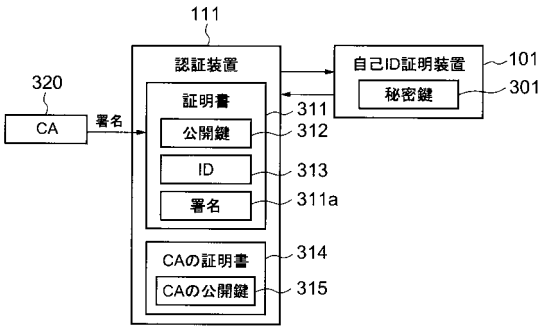
【符号の説明】

１００　ユーザ端末
１０１　自己ＩＤ証明装置
１０２　アカウント管理権限情報
１１０　権限付与サーバ
１１１　認証装置
１１２　権限情報生成装置
１１３　権限付与対象ユーザ端末テーブル
１２０　コンピュータ
１２１　認証装置
１２２　権限確認装置
１２３　アカウント管理装置
１２４　アカウント管理許可権限付与サーバテーブル

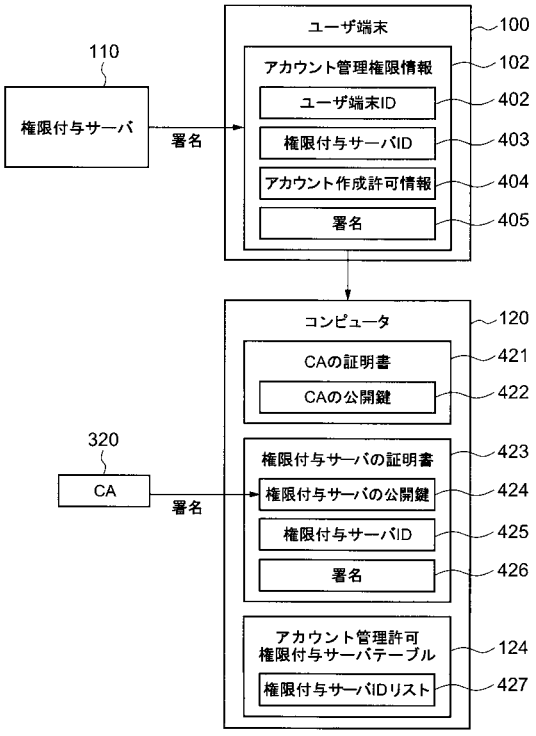
【図１】


100
101
120
121
122
124
ユーザ端末
自己ID証明装置
アカウント管理権限情報
102
認証装置
権限確認装置
アカウント管理装置
アカウント管理許可権限付与サーバテーブル
コンピュータ
123
110
111
112
113
権限付与サーバ
認証装置
権限情報生成装置
権限付与対象ユーザ端末テーブル

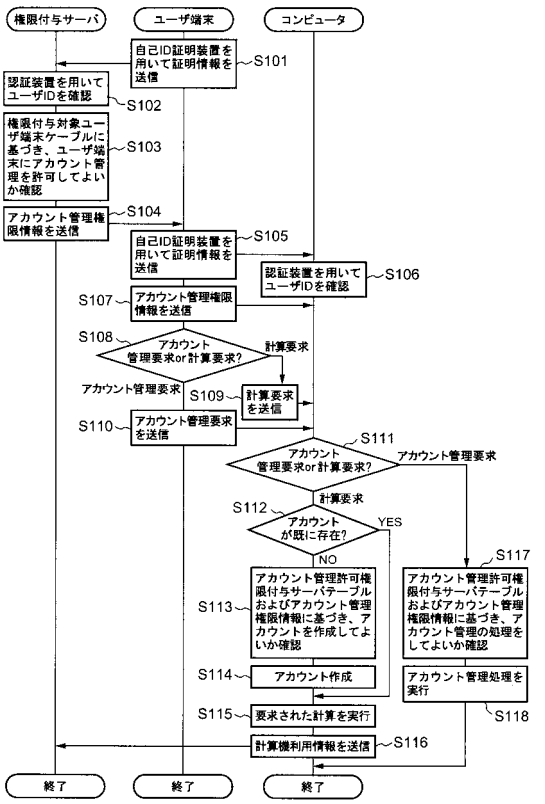
【図２】


111
認証装置
自己ID証明装置
101
秘密鍵
301
320
CA
署名
証明書
311
公開鍵
312
ID
313
署名
311a
CAの証明書
314
CAの公開鍵
315

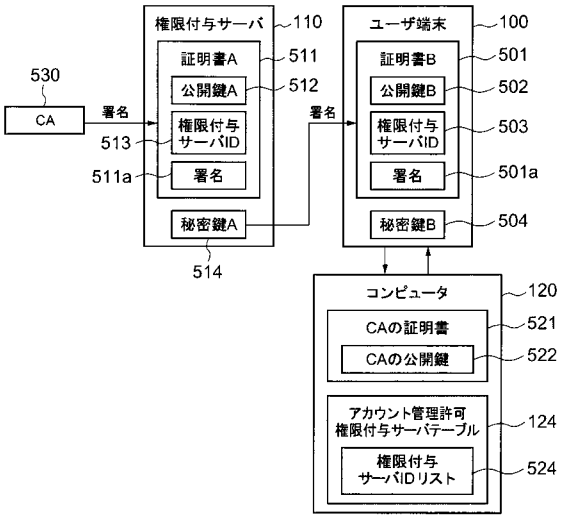
【図３】


ユーザ端末
100
110
権限付与サーバ
署名
アカウント管理権限情報
102
ユーザ端末ID
402
権限付与サーバID
403
アカウント作成許可情報
404
署名
405
コンピュータ
120
CAの証明書
421
CAの公開鍵
422
320
CA
署名
権限付与サーバの証明書
423
権限付与サーバの公開鍵
424
権限付与サーバID
425
署名
426
アカウント管理許可権限付与サーバテーブル
124
権限付与サーバIDリスト
427

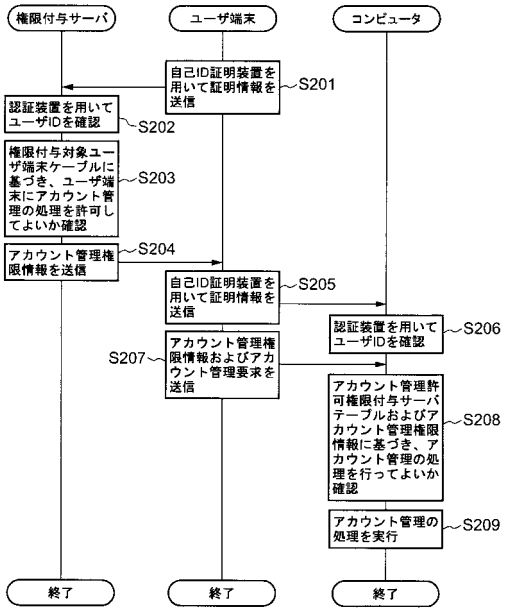
【図４】


権限付与サーバ
ユーザ端末
コンピュータ
自己ID証明装置を用いて証明情報を送信
S101
認証装置を用いてユーザIDを確認
S102
権限付与対象ユーザ端末ケーブルに基づき、ユーザ端末にアカウント管理を許可してよいか確認
S103
アカウント管理権限情報を送信
S104
自己ID証明装置を用いて証明情報を送信
S105
認証装置を用いてユーザIDを確認
S106
アカウント管理権限情報を送信
S107
アカウント管理要求or計算要求?
S108
計算要求
アカウント管理要求
S109
計算要求を送信
アカウント管理要求を送信
S110
アカウント管理要求or計算要求?
S111
アカウント管理要求
計算要求
アカウントが既に存在?
S112
YES
NO
アカウント管理許可権限付与サーバテーブルおよびアカウント管理権限情報に基づき、アカウントを作成してよいか確認
S113
アカウント作成
S114
要求された計算を実行
S115
計算機利用情報を送信
S116
アカウント管理許可権限付与サーバテーブルおよびアカウント管理権限情報に基づき、アカウント管理の処理をしてよいか確認
S117
アカウント管理処理を実行
S118
終了
終了
終了

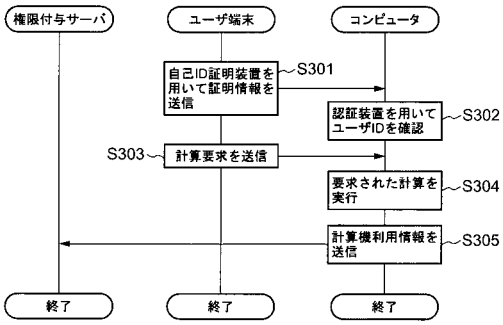
【図５】


権限付与サーバ
110
証明書A
511
公開鍵A
512
権限付与サーバID
513
署名
511a
秘密鍵A
514
530
CA
署名
署名
ユーザ端末
100
証明書B
501
公開鍵B
502
権限付与サーバID
503
署名
501a
秘密鍵B
504
コンピュータ
120
CAの証明書
521
CAの公開鍵
522
アカウント管理許可権限付与サーバテーブル
124
権限付与サーバIDリスト
524

【図６】


権限付与サーバ
ユーザ端末
コンピュータ
自己ID証明装置を用いて証明情報を送信
S201
認証装置を用いてユーザIDを確認
S202
権限付与対象ユーザ端末ケーブルに基づき、ユーザ端末にアカウント管理の処理を許可してよいか確認
S203
アカウント管理権限情報を送信
S204
自己ID証明装置を用いて証明情報を送信
S205
認証装置を用いてユーザIDを確認
S206
S207
アカウント管理権限情報およびアカウント管理要求を送信
アカウント管理許可権限付与サーバテーブルおよびアカウント管理権限情報に基づき、アカウント管理の処理を行ってよいか確認
S208
アカウント管理の処理を実行
S209
終了
終了
終了

【図７】


権限付与サーバ
ユーザ端末
コンピュータ
自己ID証明装置を用いて証明情報を送信
S301
認証装置を用いてユーザIDを確認
S302
S303
計算要求を送信
要求された計算を実行
S304
計算機利用情報を送信
S305
終了
終了
終了