(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2012-123711
(P2012-123711A)
(43)公開日　平成24年6月28日(2012.6.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B285
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104

審査請求 未請求　請求項の数 5　ＯＬ　（全 16 頁）

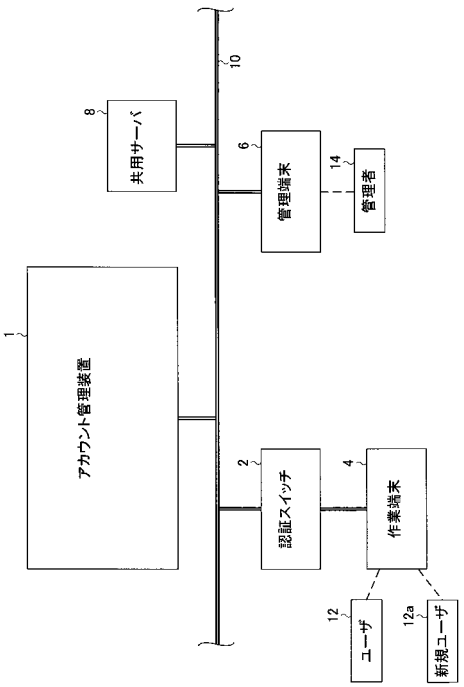
(21)出願番号　特願2010-275565 (P2010-275565)
(22)出願日　平成22年12月10日 (2010.12.10)

(71)出願人　300059979
日立電線ネットワークス株式会社
東京都千代田区外神田四丁目１４番１号
(74)代理人　100120592
弁理士　山崎　崇裕
(72)発明者　江藤　馨
東京都千代田区神田相生町１番地　日立電線ネットワークス株式会社内
(72)発明者　中和田　良平
東京都千代田区神田相生町１番地　日立電線ネットワークス株式会社内
(72)発明者　大森　晃
東京都千代田区神田相生町１番地　日立電線ネットワークス株式会社内

最終頁に続く

(54)【発明の名称】アカウント管理システム

(57)【要約】
【課題】アカウント情報を管理するネットワークを介して不正なユーザアカウントの登録を防止するとともに、正規のユーザがこのネットワークを介して新規のユーザアカウントを申請することができる。
【解決手段】アカウント管理装置１による申請アカウントの認証が成功した場合、作業端末４は、これにのみアクセス可能な限定ＶＬＡＮに設定される。新規ユーザ１２ａは、アカウント管理装置１へアクセスして新規のユーザアカウントを申請すると、これを管理者１４が審査する。管理者１４は、申請を承認すると、新規のユーザアカウントとして、アカウントデータ２８が作成される。また、アカウント管理装置１によるユーザアカウントの認証が成功した場合、作業端末４は、共用サーバ８と同じ全体ＶＬＡＮに設定される。
【選択図】図１



【特許請求の範囲】
【請求項１】
予め複数のＶＬＡＮ（Ｖｉｒｔｕａｌ　Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が設定されたネットワーク内で複数のユーザによる作業の対象として共用される共用サーバと、
前記ネットワークに接続され、所定のアカウントの認証を行う機能を有したアカウント管理装置と、
前記ネットワーク上で少なくとも前記アカウント管理装置が属する特定のＶＬＡＮ内で前記アカウント管理装置に前記アカウントの認証を要求し、受信した認証の結果を転送する認証スイッチと、
前記認証スイッチを介して前記ネットワークに接続され、前記認証スイッチから転送された認証の結果を受信する作業端末とを備え、
前記アカウント管理装置は、
前記アカウントと前記特定のＶＬＡＮに対応するＶＬＡＮ識別情報とが相互に対応付けられたアカウントデータを記憶する記憶部と、
前記認証スイッチによる認証の要求に対して前記アカウントの認証に成功した場合、認証結果とともに前記ＶＬＡＮ識別情報を応答する認証応答部とを有し、
前記認証スイッチは、
前記認証応答部から受信した前記ＶＬＡＮ識別情報に基づいて、前記作業端末を前記特定のＶＬＡＮに接続するＶＬＡＮ設定部を有する、
アカウント管理システム。
【請求項２】
請求項１に記載のアカウント管理システムにおいて、
前記アカウント管理装置の記憶部は、
前記アカウントとして、新規のユーザアカウントを申請する際に用いられる申請アカウントを予め記憶し、前記アカウントデータとして、前記ネットワーク上で前記アカウント管理装置のみにアクセスが可能な限定ＶＬＡＮに対応する限定ＶＬＡＮ識別情報を前記申請アカウントに対応付けて予め記憶していることを特徴とするアカウント管理システム。
【請求項３】
請求項１又は２に記載のアカウント管理システムにおいて、
前記アカウント管理装置の記憶部は、
前記アカウントとして、前記作業端末を操作するユーザを識別するためのユーザアカウントを予め記憶し、前記アカウントデータとして、前記ネットワーク上で前記共用サーバへのアクセスが可能な全体ＶＬＡＮに対応する全体ＶＬＡＮ識別情報を前記ユーザアカウントに対応付けて予め記憶していることを特徴とするアカウント管理システム。
【請求項４】
請求項２又は３に記載のアカウント管理システムにおいて、
前記ネットワークに接続され、申請された新規のユーザアカウントについて審査を行う管理者により操作される管理端末をさらに備え、
前記アカウント管理装置は、
前記認証応答部による前記申請アカウントの認証が成功した場合、前記ユーザに対して新規のユーザアカウントに関するユーザ情報の登録、編集、及び削除を許可する申請受付部をさらに有し、
前記アカウント管理装置の記憶部は、
前記ユーザにより登録された前記ユーザ情報を申請データとして新たに記憶し、これを審査した前記管理者が承認した場合、前記申請データに基づく前記アカウントデータとして新たに記憶することを特徴とするアカウント管理システム。
【請求項５】
請求項２から４のいずれかに記載のアカウント管理システムにおいて、
前記申請アカウントは、

ユーザＩＤとそのパスワード、生体認証、及び電子証明書のうち、少なくともいずれか一つを含んでおり、
前記アカウント管理装置の認証応答部は、
前記ユーザＩＤとそのパスワード、前記生体認証、及び前記電子証明書に基づいて前記申請アカウントの認証を行うことを特徴とするアカウント管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アカウント管理システムに関する。
【背景技術】
【０００２】
従来、ネットワーク内に配置された作業端末を利用するユーザのアカウント情報を管理する手法として、ユーザごとに割り当てた作業者ＩＤに認証情報や作業ＩＤを関連付けて管理する先行技術が知られている（例えば、特許文献１参照。）。
【０００３】
この先行技術では、ネットワーク内に作業端末、申請端末、アカウント制御情報格納装置、承認端末、及びメンテナンス対象装置が配置されており、アカウント制御情報格納装置には、予め作業者ＩＤが登録されている。ユーザがメンテナンス対象装置に対して作業を実施する場合、ユーザは、予め申請端末からアカウント制御情報格納装置に対して作業情報を申請する。申請された作業情報は、承認端末を用いて管理者に審査される。審査の結果、管理者に承認された場合、作業情報は、申請したユーザの作業者ＩＤに対応付けられてアカウント制御情報格納装置に登録される。そして登録後、ユーザが自己の作業者ＩＤを用いてメンテナンス対象装置にアクセスすると、アカウント制御情報格納装置に登録された作業情報に関する作業を行うことができる。
【０００４】
上記の先行技術によれば、メンテナンス対象装置へアクセスする作業者及び作業情報を効率的に管理することができるものと考えられる。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００９－２５８８２０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、上記の先行技術には、メンテナンス対象装置をはじめ、作業端末や申請端末、アカウント制御情報格納装置、承認端末等に対して充分なセキュリティが図られていないという問題がある。すなわち先行技術では、各種の端末及び装置が全て同一のネットワーク内に配置されており、これらの端末は常にアクセスできる状態にある。このため、管理者やユーザになりすました第三者の不正なアクセスやアカウント情報の改ざん等、セキュリティに関する脅威を排除することができない。
【０００７】
また、新規の作業者ＩＤをアカウント制御情報格納装置へ登録する場合、上記の管理者による審査や承認のステップが行われない。このため極端な場合は、ユーザになりすました第三者が申請端末を操作して不正な作業者ＩＤをアカウント制御情報格納装置へ登録することができてしまう。
【０００８】
そこで本発明は、アカウント情報を管理するネットワークを介して不正なユーザアカウントの登録を防止するとともに、正規のユーザがこのネットワークを介して新規のユーザアカウントを申請することができる技術の提供を課題とする。
【課題を解決するための手段】

【０００９】
上記の課題を解決するために本発明のアカウント管理システムは、予め複数のＶＬＡＮ（Ｖｉｒｔｕａｌ　Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が設定されたネットワーク内で複数のユーザによる作業の対象として共用される共用サーバと、ネットワークに接続され、所定のアカウントの認証を行う機能を有したアカウント管理装置と、ネットワーク上で少なくともアカウント管理装置が属する特定のＶＬＡＮ内でアカウント管理装置にアカウントの認証を要求し、受信した認証の結果を転送する認証スイッチと、認証スイッチを介してネットワークに接続され、認証スイッチから転送された認証の結果を受信する作業端末とを備え、アカウント管理装置は、アカウントと特定のＶＬＡＮに対応するＶＬＡＮ識別情報とが相互に対応付けられたアカウントデータを記憶する記憶部と、認証スイッチによる認証の要求に対してアカウントの認証に成功した場合、認証結果とともにＶＬＡＮ識別情報を応答する認証応答部とを有し、認証スイッチは、認証応答部から受信したＶＬＡＮ識別情報に基づいて、作業端末を特定のＶＬＡＮに接続するＶＬＡＮ設定部を有する。
【発明の効果】
【００１０】
本発明のアカウント管理システムによれば、作業端末を利用するユーザは、アカウント管理装置によるアカウントの認証に成功しなければ共用サーバへアクセスすることができない。このため、アカウント管理システムのネットワーク内におけるセキュリティを強化することができる。
【図面の簡単な説明】
【００１１】
【図１】本実施形態のアカウント管理システムの構成例を概略的に示す図である。
【図２】アカウント管理装置の機能的な構成を概略的に示すブロック図である。
【図３】認証スイッチの機能的な構成を概略的に示すブロック図である。
【図４】申請アカウントに基づく認証処理を示す図である。
【図５】新規ユーザアカウントの申請処理を示す図である。
【図６】新規ユーザアカウントの登録処理を示す図である。
【図７】新規ユーザアカウントの認証処理を示す図である。
【図８】新規ユーザアカウントの申請処理及び登録処理を示すフローチャートである。
【発明を実施するための形態】
【００１２】
以下、本発明の実施形態について図面を参照しながら説明する。図１は、本実施形態のアカウント管理システムの構成例を概略的に示す図である。なお、本実施形態のアカウント管理システムは、アカウント管理装置１、認証スイッチ２、作業端末４、管理端末６、及び共用サーバ８により実現される。
【００１３】
アカウント管理装置１、認証スイッチ２、作業端末４、管理端末６、及び共用サーバ８は、例えば、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｏｗｏｒｋ）に代表されるネットワーク１０に接続されている。また、ネットワーク１０には、図示しない複数のＶＬＡＮ（Ｖｅｒｔｕａｌ　ＬＡＮ：仮想ネットワーク）が規定されており、ネットワーク１０内で共通のＶＬＡＮに接続された機器同士が相互に通信を行うことができる。
【００１４】
〔アカウント管理装置〕
アカウント管理装置１は、所定のネットワーク認証方式によりユーザアカウント、申請アカウント、及び管理者アカウントを認証するためのサーバである。アカウント管理装置１は、上記のネットワーク認証方式として、例えば、ＷＥＢブラウザを介して上記のアカウントを認証する認証方式（ＷＥＢ認証）や、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｅｌｅｃｔｒｉｃａｌ　ａｎｄ　Ｅｌｅｃｔｒｏｎｉｃ　Ｅｎｇｉｎｅｅｒｓ）８０２．１Ｘ規格に基づく認証方式、ＲＡＤＩＵＳ（Ｒｅｍｏｔｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ

Ｄｉａｌ Ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ）プロトコルに基づく認証方式等を用いて、作業端末４及び管理端末６から送信されたユーザアカウント、申請アカウント、及び管理者アカウントを認証する。

【００１５】

ここで、ユーザアカウントは、作業端末４を操作するユーザ１２を識別するために用いられる認証情報である。また、申請アカウントは、ユーザアカウントが付与されていない新規ユーザ１２ａが新規のユーザアカウントを申請する際に用いられる認証情報である。管理者アカウントは、管理者特権としてアカウント管理装置１へアクセスするために用いられる認証情報である。なお、アカウント管理装置１の機能的な構成については、図２を用いてさらに詳しく後述する。

【００１６】

〔認証スイッチ〕

認証スイッチ２は、例えばＯＳＩ（Ｏｐｅｎ Ｓｙｓｔｅｍｓ Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）参照モデルのレイヤ２及びレイヤ３等のデータ転送機能を備えたスイッチングハブである。また認証スイッチ２は、申請アカウント及びユーザアカウントを認証する機能を備えている。

【００１７】

認証スイッチ２は、申請アカウント及びユーザアカウントを認証する機能として、例えば、ＷＥＢ認証機能を備えており、作業端末４がネットワーク１０に配置されたアカウント管理装置１や共用サーバ８への接続を要求した場合、作業端末４に対してアカウントを要求する。また認証スイッチ２は、作業端末４が応答したアカウントに基づいてアカウント管理装置１により実行された認証の結果を作業端末４に通知する。このとき、認証スイッチ２は、認証結果に応じて作業端末４を上記のＶＬＡＮに接続したり、ネットワーク１０への接続を遮断したりする。なお、認証スイッチ２の機能的な構成については、図３を参照してさらに詳しく後述する。

【００１８】

〔作業端末、管理端末〕

作業端末４及び管理端末６は、例えばＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）やワークステーション等、所定のユーザが操作を行いデータを送受信する装置である。本実施形態では、ユーザ１２又は新規ユーザ１２ａにより操作される端末を作業端末４として規定し、管理者１４により操作される端末を管理端末６として規定することとする。作業端末４及び管理端末６は、それぞれアカウント管理装置１によるユーザアカウント、申請アカウント、及び管理者アカウントの認証が成功した場合に、アカウント管理装置１や共用サーバ８へアクセス可能なＶＬＡＮ（限定ＶＬＡＮ）へ接続される。

【００１９】

〔共用サーバ〕

共用サーバ８は、ユーザ１２による作業の対象として、予め複数のＶＬＡＮが設定されたネットワーク１０内で複数のユーザ１２による作業の対象として共用される一般的なサーバ機器である。ユーザ１２は、作業端末４からネットワーク１０を介して共用サーバ８へアクセスして所定の作業を行うことができるが、予めアカウント管理装置１によるユーザアカウントを用いた認証が成功しなければ共用サーバ８へアクセスすることができない。

【００２０】

また本実施形態において、ユーザアカウントが与えられていない新規ユーザ１２ａが作業端末４を介して共用サーバ８へアクセスするためには、予め新規ユーザ１２ａが新たにユーザアカウントをアカウント管理装置１へ申請し、これがアカウント管理装置１に登録される必要がある。さらに、アカウント管理装置１に登録された新規のユーザアカウントが管理者１４により承認されなければ、新規ユーザ１２ａは共用サーバ８へアクセスすることができない。なお、新規のユーザアカウントをアカウント管理装置１に申請する手法、及び新規ユーザ１２ａがアカウント管理装置１や共用サーバ８へアクセスする手法につ

いては、図４～８を用いてさらに詳しく後述する。
【００２１】
図２は、アカウント管理装置１の機能的な構成を概略的に示すブロック図である。なお、図２中に示す実線の矢印は、データの転送方向を表している。
【００２２】
アカウント管理装置１は、記憶部１６、認証応答部１８、申請受付部２０、アカウント管理部２２、入出力部２４により構成されている。また、認証応答部１８、申請受付部２０、及びアカウント管理部２２は、それぞれソフトウェアにより実現されることが好ましい。
【００２３】
〔記憶部〕
記憶部１６は、新規ユーザ１２ａにより申請された新規のユーザアカウントに関するユーザ情報を申請データ２６として記憶する。また申請データ２６の他に、記憶部１６は、ユーザアカウント、申請アカウント、及び管理者アカウントにそれぞれ対応するＶＬＡＮ　ＩＤ（ＶＬＡＮ識別情報）をアカウントデータ２８として記憶している。なお、記憶部１６は、メモリや補助記憶装置等の記憶媒体により構成されていることが好ましい。
【００２４】
ユーザアカウント、申請アカウント、及び管理者アカウントに対応するＶＬＡＮ　ＩＤは、それぞれのアカウントに応じて作業端末４及び管理端末６からアクセスすることができるＶＬＡＮの範囲を示している。本実施形態において、申請アカウントに対応するＶＬＡＮ　ＩＤ（限定ＶＬＡＮ識別情報）は、作業端末４がネットワーク１０上でアカウント管理装置１のみにアクセスが可能なＶＬＡＮ（限定ＶＬＡＮ）に対応する識別情報である。また、ユーザアカウントに対応するＶＬＡＮ　ＩＤ（全体ＶＬＡＮ識別情報）は、作業端末４がアカウント管理装置１以外のネットワーク１０に接続された装置（例えば、共用サーバ８）へアクセス可能なＶＬＡＮ（全体ＶＬＡＮ）を示す。なお、管理者アカウントに対応するＶＬＡＮ　ＩＤは、上記の全体ＶＬＡＮ、もしくは、限定ＶＬＡＮのいずれに対応するものであってもよい。
【００２５】
また、アカウントデータ２８として記憶部１６に記憶された申請アカウント、ユーザアカウント、及び管理者アカウントには、例えばユーザＩＤとこれに対応するパスワードや、生体認証、電子証明書等、所定の認証方式によりユーザ１２や新規ユーザ１２ａ、管理者１４を特定するための認証情報が含まれている。
【００２６】
〔認証応答部〕
認証応答部１８では、記憶部１６に記憶されたアカウントデータ２８に基づいて、ユーザ１２、新規ユーザ１２ａ、及び管理者１４により入力されたユーザアカウント、申請アカウント、及び管理者アカウントの認証を行う。また認証応答部１８は、認証スイッチ２や、作業端末４、管理端末６等の外部装置から受けた認証結果の要求に対して、認証結果を応答する。本実施形態において、認証応答部１８は、認証が成功した場合、認証結果とともにＶＬＡＮ　ＩＤを認証スイッチ２へ向けて通知する。一方、認証に失敗した場合、認証応答部１８は、認証結果のみを認証スイッチ２へ通知する。
【００２７】
〔申請受付部〕
申請受付部２０は、新規ユーザ１２ａにより入力された新規のユーザアカウントに関するユーザ情報を申請データ２６として登録したり、記憶部１６に登録された申請データ２６の編集や削除をしたりする機能、入力されたユーザ情報が所定の様式に従って行われているか否かを判断する機能、及び、ユーザ情報を申請データ２６として登録した場合、これを外部へ通知する機能を備えている。申請データ２６の登録、編集、及び削除は、認証応答部１８にて申請アカウントに基づく認証が成功した場合に、新規ユーザ１２ａが作業端末４を操作することで実行可能となる。

【００２８】
〔アカウント管理部〕
アカウント管理部２２は、アカウントデータ２８を作成したり、アカウントデータ２８の編集や削除をしたりする機能、管理者１４により行われた申請データ２６の承認もしくは却下の決定を記憶部１６に反映する機能、及び審査結果を通知する機能を備えている。これらの機能は、認証応答部１８にて管理者アカウントに基づく認証が成功した場合に、管理者１４が管理端末６を操作することで実行可能となる。
【００２９】
入出力部２４は、図示しない複数のポートを備えており、各ポートには、図１中に示す認証スイッチ２、管理端末６、及び共用サーバ８が接続されている。入出力部２４は、例えば、認証スイッチ２や管理端末６から転送されたデータを認証応答部１８や、申請受付部２０、アカウント管理部２２に転送する。また、認証応答部１８や、申請受付部２０、アカウント管理部２２から転送されたデータを認証スイッチ２や管理端末６へ送信する。
【００３０】
図３は、認証スイッチ２の機能的な構成を概略的に示すブロック図である。なお、実線で示す矢印は、データの転送方向を表している。
【００３１】
認証スイッチ２は、一般的なフレームやパケットを転送する機能のほかに、ＷＥＢ認証部３０、アカウント認証部３２、ＶＬＡＮ設定部としてのＶＬＡＮ切替部３４、接続遮断部３６、及び入出力部３８を備えている。
【００３２】
ＷＥＢ認証部３０は、ＷＥＢブラウザを介してユーザアカウントや申請アカウントの認証を行う一般的なＷＥＢ認証の機能を備えている。ＷＥＢ認証部３０では、作業端末４からネットワーク１０への接続を要求された場合、作業端末４に対して上記のアカウントを要求する。また、作業端末４に入力されたユーザアカウントや申請アカウントをアカウント管理装置１の認証応答部１８へ転送する。
【００３３】
例えば、ＷＥＢ認証部３０は、作業端末４の図示しないディスプレイに表示されたＷＥＢブラウザに対して、ユーザアカウントや申請アカウントを入力させるための認証用ページを送信する。このとき、ユーザ１２や新規ユーザ１２ａは、作業端末４のディスプレイに表示された認証用ページにユーザアカウントや申請アカウントを入力する。作業端末４の認証用ページに入力されたユーザアカウントや申請アカウントは、認証スイッチ２のアカウント認証部３２へ送信される。
【００３４】
アカウント認証部３２は、上記の認証用ページに入力されたユーザアカウントや申請アカウントをアカウント管理装置１の認証応答部１８へ転送する。また、アカウント認証部３２は、認証応答部１８により行われた認証の結果を受信し、その認証の結果を作業端末４へ転送する。
【００３５】
〔ＶＬＡＮ設定部〕
ＶＬＡＮ切替部３４は、認証応答部１８によるユーザアカウントや申請アカウントの認証が成功した場合、これを示す認証結果を受信した時に認証応答部１８から送信されたＶＬＡＮ　ＩＤを作業端末４が接続されたポートに設定する。一方、接続遮断部３６は、認証応答部１８によるユーザアカウントや申請アカウントの認証が失敗した場合、これを示す認証結果を受信した時に作業端末４が接続されたポートを遮断（シャットダウン）する。
【００３６】
入出力部３８は、図示しない複数のポートを備えており、各ポートには、図１中に示すアカウント管理装置１、作業端末４、管理端末６、及び共用サーバ８が接続されている。入出力部３８は、例えば、ＷＥＢ認証部３０から送信された認証用ページを作業端末４へ

送信したり、作業端末４から送信されたユーザアカウントや申請アカウントをＷＥＢ認証部３０へ転送したりする。また、入出力部３８は、作業端末４から送信された認証要求をアカウント認証部３２へ転送したり、アカウント認証部３２から転送された認証結果を作業端末４へ転送したりする。入出力部３８はまた、ＶＬＡＮ切替部３４により図示しないポートにＶＬＡＮが設定されたり、接続遮断部３６によりポートが遮断（シャットダウン）されたりする。

【００３７】

〔申請アカウントに基づく認証〕

図４は、申請アカウントに基づく認証処理を示す図である。申請アカウントは、ユーザアカウントが付与されていないユーザに対して予め管理者により付与される。なお、図４中の実線で示す矢印は、申請アカウントや認証結果の転送方向を表している。また、図４中に破線で囲まれた線は、新規ユーザ１２ａが申請アカウントを用いてアクセス可能な限定ＶＬＡＮ４０を表している。

【００３８】

認証スイッチ２は、作業端末４に対してアカウントを要求する。作業端末４は、新規ユーザ１２ａが入力した申請アカウントを認証スイッチ２へ送信する。認証スイッチ２は、受信した申請アカウントをアカウント管理装置１へ転送する。

【００３９】

アカウント管理装置１の認証応答部１８は、認証スイッチ２から受信した申請アカウントの認証を行う。具体的には、新規ユーザ１２ａにより作業端末４に入力された申請アカウントと、アカウントデータ２８として記憶部１６に記憶された申請アカウントとを照合する。認証応答部１８は、照合した結果、上記の申請アカウントが一致する場合に認証成功と判断し、一致しない場合に認証失敗と判断する。認証応答部１８は、認証結果を認証スイッチ２に対して送信する。このとき、認証応答部１８は、認証成功と判断した場合、申請アカウントに対応付けられた限定ＶＬＡＮ４０を示すＶＬＡＮ　ＩＤを認証結果と合わせて認証スイッチ２に対して送信する。一方、認証失敗と判断した場合、認証応答部１８は、認証結果のみを認証スイッチ２に対して送信する。

【００４０】

認証スイッチ２は、アカウント管理装置１から受信した認証結果を作業端末４へ転送する。また、受信した認証結果が認証成功を示す場合、認証スイッチ２は、受信した限定ＶＬＡＮ４０を示すＶＬＡＮ　ＩＤを作業端末４が接続されたポートに設定する。このとき、作業端末４は、限定ＶＬＡＮ４０内において、認証スイッチ２を介してアカウント管理装置１に対してのみアクセスが可能な状態となる。

【００４１】

一方、受信した認証結果が認証失敗を示す場合、認証スイッチ２は、作業端末４が接続されたポートを遮断（シャットダウン）する。このとき、作業端末４は、ネットワーク１０から切り離され、アカウント管理装置１や共用サーバ８に対してアクセス不可能な状態となる。

【００４２】

〔新規ユーザアカウントの申請〕

図５は、新規ユーザアカウントの申請処理を示す図である。図４中のアカウント管理装置１によって申請アカウントの認証が成功すると、新規ユーザ１２ａは、アカウント管理装置１に新規のユーザアカウントを申請することができる。

【００４３】

新規ユーザ１２ａは、アカウント管理装置１の申請受付部２０へアクセスするために申請アカウントを作業端末４に入力する。入力された申請アカウントは、認証スイッチ２を介してアカウント管理装置１へ転送されて認証される。アカウント管理装置１による申請アカウントの認証が成功すると、新規ユーザ１２ａは、アカウント管理装置１の申請受付部２０にログインすることができる。

【００４４】

申請受付部２０にログインすると新規ユーザ１２ａは、ユーザアカウントの申請に関するユーザ情報を入力する。アカウント管理装置１の申請受付部２０は、入力されたユーザ情報が所定の様式に従っている場合、これを申請データ２６として記憶部１６に登録する。一方、所定の様式に従っていない場合、アカウント管理装置１の申請受付部２０は、登録を拒否する旨を作業端末４へ通知する。

【００４５】

また新規ユーザ１２ａは、作業端末４を操作して登録された申請データ２６の内容を編集したり、不要な情報を削除したりすることができる。このときアカウント管理装置１の申請受付部２０は、新規ユーザ１２ａにより行われた編集や削除を申請データ２６に反映する。

【００４６】

申請受付部２０は、新規ユーザ１２ａによる申請データ２６の登録が完了した場合、登録が完了した旨を管理者１４に対して通知する。

【００４７】

〔新規ユーザアカウントの登録〕

図６は、新規ユーザアカウントの登録処理を示す図である。管理者１４は、図５中に示すアカウント管理装置１の申請受付部２０から登録完了の通知を受信すると、申請データ２６の内容を審査する。

【００４８】

管理者１４は、管理端末６に管理者アカウントを入力してアカウント管理装置１へアクセスする。アカウント管理装置１による管理者アカウントの認証が成功すると、管理者１４は、アカウント管理装置１のアカウント管理部２２へログインすることができる。管理者１４は、アカウント管理部２２へログインすると申請データ２６の審査を行う。

【００４９】

例えば、管理者１４は、管理端末６の図示しないディスプレイに表示された申請データ２６を参照して、申請データ２６の内容に不備があるか否かを審査したり、不正なユーザ情報であるか否かを審査したりする。管理者１４は、申請データ２６を新たなユーザアカウントとして承認する場合、申請データ２６を新たなユーザアカウントとしてアカウントデータ２８の作成を行う。このとき、ユーザアカウントに対応付けて全体ＶＬＡＮを示すＶＬＡＮ　ＩＤも作成する。また、アカウント管理部２２は申請データ２６を削除する。

【００５０】

管理者１４による審査が終了すると、アカウント管理部２２は、新規ユーザ１２ａに対して審査結果を通知する。なお、アカウント管理部２２が新規ユーザ１２ａに審査結果を通知する手法としては、認証スイッチ２や、作業端末４、共用サーバ８等が接続されていない他のネットワークを介して電子メールやＦＡＸ（ファクシミリ）等により通知することが好ましい。

【００５１】

〔新規のユーザアカウントの認証〕

図７は、新規のユーザアカウントの認証処理を示す図である。図６中に示すアカウント管理装置１から申請データ２６がユーザアカウントとして承認された旨の審査結果を受領すると、新規ユーザ１２ａは、承認されたユーザアカウントを用いて共用サーバ８へアクセスすることができる。なお、図７中に示す破線は、全体ＶＬＡＮ４２を表している。

【００５２】

〔認証前〕

アカウント管理装置１によるユーザアカウントの認証が行われる前の作業端末４は、少なくともネットワーク１０に接続されているのみでＶＬＡＮが設定されていない状態か、もしくは、限定ＶＬＡＮ４０に設定されている状態である。例えば、管理者１４による申請データ２６の審査が行われている間、新規ユーザ１２ａが作業端末４の電源を落としたり、アカウント管理装置１からログアウトした場合、作業端末４が接続されていた限定ＶＬＡＮ４０は解除された状態である。一方、アカウント管理装置１へのログイン状態が維

持されている場合、作業端末４は限定ＶＬＡＮ４０に接続された状態である。
【００５３】
〔認証時〕
新規ユーザ１２ａは、共用サーバ８へアクセスするために、管理者１４により承認されたユーザアカウントを作業端末４に入力する。入力されたユーザアカウントは、認証スイッチ２を介してアカウント管理装置１へ転送され、アカウント管理装置１により認証される。アカウント管理装置１は、認証スイッチ２へ認証結果やＶＬＡＮ　ＩＤを送信する。認証スイッチ２は、受信した認証結果を作業端末４へ転送する。また、ＶＬＡＮ　ＩＤを受信した場合、認証スイッチ２は、これを作業端末４が接続されたポートに設定する。
【００５４】
具体的には、新規ユーザ１２ａは、認証スイッチ２のＷＥＢ認証部３０から送信され、作業端末４のディスプレイに表示された認証用ページにユーザアカウントを入力する。入力されたユーザアカウントは、認証スイッチ２を介してアカウント管理装置１へ転送され、アカウント管理装置１の認証応答部１８によりユーザアカウントの認証が行われる。
【００５５】
認証応答部１８は、入力されたユーザアカウント及び、アカウントデータ２８として登録されたユーザアカウントを照合する。これらのユーザアカウントが相互に一致する場合、認証応答部１８は、認証が成功したものと判断する。一方、ユーザアカウントが相互に一致しない場合、認証が失敗したものと判断する。
【００５６】
認証に成功した場合、認証応答部１８は、認証結果とともに全体ＶＬＡＮ４２を示すＶＬＡＮ　ＩＤを認証スイッチ２へ通知する。一方、認証に失敗した場合、認証応答部１８は、認証結果のみを認証スイッチ２へ通知する。
【００５７】
〔認証後〕
認証スイッチ２は、アカウント管理装置１から受信した認証結果を作業端末４へ転送する。また、ユーザアカウントの認証の成功により全体ＶＬＡＮ４２を示すＶＬＡＮ　ＩＤを受信した場合、認証スイッチ２は、作業端末４が接続されたポートにこれを設定する。これにより、作業端末４は、アカウント管理装置１以外のネットワーク１０に接続された装置（例えば、共用サーバ８）へアクセス可能な全体ＶＬＡＮ４２に接続される。
【００５８】
一方、認証に失敗した旨を示す認証結果を受信した場合、認証スイッチ２は、作業端末４が接続されているポートを遮断する。これにより、作業端末４はネットワーク１０から切り離される。
【００５９】
新規ユーザ１２ａは、作業端末４が全体ＶＬＡＮ４２に接続されると、全体ＶＬＡＮ４２内の共用サーバ８へアクセスすることができる。
【００６０】
図８は、新規ユーザアカウントの申請処理及び登録処理を示すフローチャートである。以下、手順を追って説明する。
【００６１】
〔申請アカウントの認証〕
ステップＳ１０：作業端末４は、新規ユーザ１２ａにより入力された申請アカウントを認証スイッチ２へ送信する。また、認証スイッチ２は、受信した申請アカウントをアカウント管理装置１へ転送する（ステップＳ１２）。
【００６２】
ステップＳ１４：アカウント管理装置１の認証応答部１８は、受信した申請アカウントの認証を行う。認証応答部１８は、申請アカウントの認証結果を認証スイッチ２へ送信する（ステップＳ１６）。なお、認証応答部１８は、認証に成功した場合、認証結果とともに申請アカウントに対応付けて記憶部１６に登録された限定ＶＬＡＮ４０を示すＶＬＡＮ

ＩＤを送信する。

【００６３】

ステップＳ１８：認証スイッチ２は、アカウント管理装置１から受信した認証結果を作業端末４へ転送する。また認証スイッチ２は、アカウント管理装置１による認証が成功した場合、受信した限定ＶＬＡＮ４０を示すＶＬＡＮ　ＩＤを作業端末４が接続されたポートに設定する。このとき、作業端末４は、アカウント管理装置１のみにアクセス可能な限定ＶＬＡＮ４０に接続される。一方、上記の認証が失敗した場合、認証スイッチ２は、作業端末４が接続されたポートを遮断する。これより、作業端末４はネットワーク１０から切り離される。

【００６４】

〔新規ユーザアカウントの申請〕

ステップＳ２０：申請アカウントの認証が成功した場合、新規ユーザ１２ａは、再度作業端末４に申請アカウントを入力してアカウント管理装置１の申請受付部２０へログインする。新規ユーザ１２ａは、申請受付部２０へログインすると、ユーザアカウントの申請に関するユーザ情報を入力する。

【００６５】

ステップＳ２２：アカウント管理装置１の申請受付部２０は、新規ユーザ１２ａにより入力された情報が、所定の様式に従って入力されているか否かを判断する。申請受付部２０は、ユーザ情報が所定の様式に従って入力されていると判断した場合、これを申請データ２６として登録することを許可し、記憶部１６に登録する。一方、所定の様式に従って入力されていない場合、申請受付部２０は、申請データ２６として登録することを拒否する。

【００６６】

ステップＳ２４：アカウント管理装置１の申請受付部２０は、上記の判断結果を作業端末４へ通知する。

【００６７】

〔申請データの審査〕

ステップＳ２６：アカウント管理装置１の申請受付部２０は、新規ユーザ１２ａにより入力されたユーザ情報を申請データ２６として記憶部１６に登録した場合、登録した旨を管理者１４へ通知する。

【００６８】

ステップＳ２８：管理者１４は、アカウント管理装置１の申請受付部２０から通知された判断結果を受信すると、管理端末６に管理者アカウントを入力してアカウント管理装置１のアカウント管理部２２へログインする。

【００６９】

ステップＳ３０：アカウント管理装置１のアカウント管理部２２へログインすると、管理者１４は、管理端末６を介して申請データ２６の内容を参照することができる。

ステップＳ３２：管理者１４は、申請データ２６の内容を審査する。

ステップＳ３４：管理者１４は、申請データ２６の内容に不備が無ければこれを承認する。アカウント管理装置１のアカウント管理部２２は、承認された申請データ２６をアカウントデータ２８として記憶部１６に作成する。一方、管理者１４は申請データ２６の内容に不備があればこれを却下する。

ステップＳ３６：アカウント管理装置１のアカウント管理部２２は、管理者１４による審査の結果を電子メールやＦＡＸ等、他のネットワークを介して新規ユーザ１２ａへ通知する。

【００７０】

〔申請データが却下された場合〕

ステップＳ３８：管理者１４により申請データ２６が却下された場合、新規ユーザ１２ａは、申請したユーザアカウントを用いて共用サーバ８へアクセスすることができない。このとき、新規ユーザ１２ａは、ステップＳ２０からステップＳ２４の手順に沿って、再

度、ユーザアカウントを申請することができる。そして、管理者１４によりステップＳ２８～ステップＳ３４の手順に基づいて申請データ２６の審査が行われる。

【００７１】

〔申請データが承認された場合〕

ステップＳ４０：管理者１４による審査の結果、申請データ２６が新たなユーザアカウントとして承認された場合、新規ユーザ１２ａは、共用サーバ８へアクセスすることが可能となる。このとき、新規ユーザ１２ａはまず、承認されたユーザアカウントを作業端末４に入力する。

ステップＳ４２：認証スイッチ２は、入力されたユーザアカウントをアカウント管理装置１へ転送する。

ステップＳ４４：アカウント管理装置１は、新規ユーザ１２ａにより入力されたユーザアカウントの認証を行う。

【００７２】

ステップＳ４６：アカウント管理装置１は、認証結果を認証スイッチ２へ送信する。ユーザアカウントの認証に成功した場合、アカウント管理装置１は、認証結果とともに全体ＶＬＡＮ４２を示すＶＬＡＮ　ＩＤを認証スイッチ２へ送信する。一方、ユーザアカウントの認証に失敗した場合、アカウント管理装置１は、認証結果のみを認証スイッチ２へ送信する。

ステップＳ４８：認証スイッチ２は、アカウント管理装置１から受信した認証結果を作業端末４へ転送する。認証スイッチ２は、アカウント管理装置１によるユーザアカウントの認証が成功したことにより全体ＶＬＡＮ４２を示すＶＬＡＮ　ＩＤを受信した場合、これを作業端末４が接続されているポートに設定する。一方、ユーザアカウントの認証に失敗した旨を示す認証結果を受信した場合、認証スイッチ２は、作業端末４が接続されたポートを遮断して作業端末４をネットワーク１０から切り離す。

【００７３】

ステップ５０：アカウント管理装置１によるユーザアカウントの認証に成功すると、作業端末４は、共用サーバ８と同じ全体ＶＬＡＮ４２に接続される。このとき、新規ユーザ１２ａは、作業端末４を介して共用サーバ８へアクセスすることができる。

【００７４】

このように、本発明のアカウント管理システムによれば、アカウントに応じて作業端末が接続されるＶＬＡＮの範囲を制限することができる。

【００７５】

また、記憶部１６には、申請アカウント及びユーザアカウントに対応してＶＬＡＮ　ＩＤがそれぞれ対応付けて記憶されている。このため、認証スイッチ２は、認証結果とともにアカウントに対応するＶＬＡＮ　ＩＤを受信した場合、このＶＬＡＮを作業端末４が接続されたポートに自動設定することができる。これにより、作業端末４を介して行われる不正なアクセスに対して、セキュリティの強化を図ることができる。

【００７６】

また、アカウント管理装置１による申請アカウントの認証が成功した場合、認証スイッチ２は、一時的にアカウント管理装置１にのみアクセス可能な限定ＶＬＡＮ４０に作業端末４を接続する。さらに、新規ユーザ１２ａは、申請アカウントの認証が成功した場合に限り、アカウント管理装置にログインすることができる。このとき、新規ユーザ１２ａがアカウント管理装置１に対して行える作業は、新規のユーザアカウントの申請に関する作業のみであり、すでにアカウントデータ２８として登録されたユーザアカウント、申請アカウント、及び管理者アカウントの作成、編集、削除を行うことはできない。このため、申請アカウントを知らない不正なユーザが勝手にユーザアカウントを改ざんしたり、新たにユーザアカウントを登録したりすることを防止している。

【００７７】

また、新規ユーザ１２ａによる新規のユーザアカウントの申請が行われた場合、管理者１４により申請データ２６の審査が行われ、承認された申請データ２６のみがユーザアカ

ウントとして認められる。また、作業端末４は、アカウント管理装置１によるユーザアカウントの認証が成功して初めて全体ＶＬＡＮ４２に接続される。このため、不正なネットワークへのアクセスに対するセキュリティの強化を図ることができる。

【００７８】

また、申請アカウントには、ユーザＩＤとそのパスワード、生体認証、及び電子証明書が含まれており、様々な認証手法に対応している。このため、アカウント管理装置１が実装している認証手法に応じて、申請アカウントの認証を行うことができる。

【００７９】

また本発明は、上述した第１実施形態に限定されることなく種々の変形が可能である。例えば、管理端末６の代わりにアカウント管理装置１のアカウント管理部２２を用いて、これが管理者１４により承認された申請データ２６を新規のユーザアカウントとしてアカウントデータ２８の作成を自動的に行ってもよい。

【００８０】

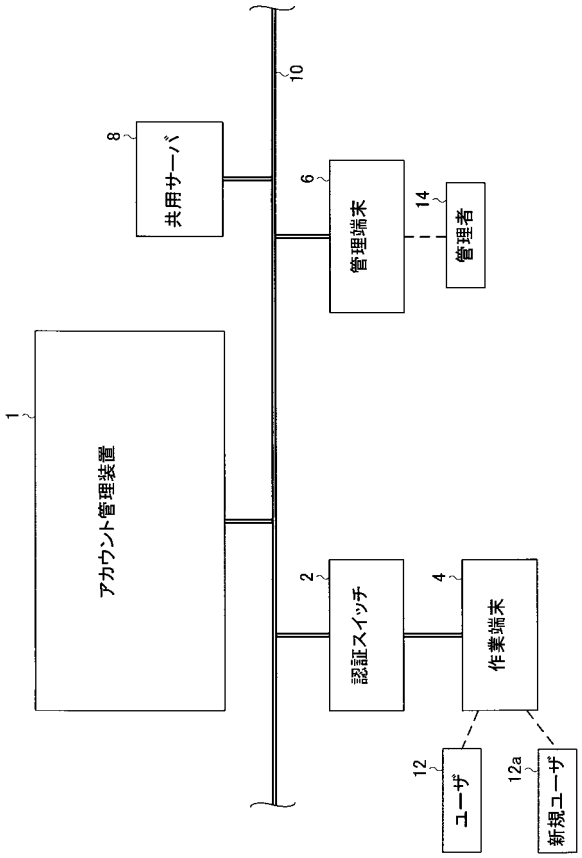
また、１台のアカウント管理装置１に備えられた申請受付部２０、アカウント管理部２２、申請データ２６、及びアカウントデータ２８を複数の装置に分けて配置し、これらの装置が相互に連動してユーザアカウント、申請アカウント、及び管理者アカウントを管理してもよい。あるいは、複数のアカウント管理装置１を用いて、上記のアカウントを管理してもよい。

【符号の説明】

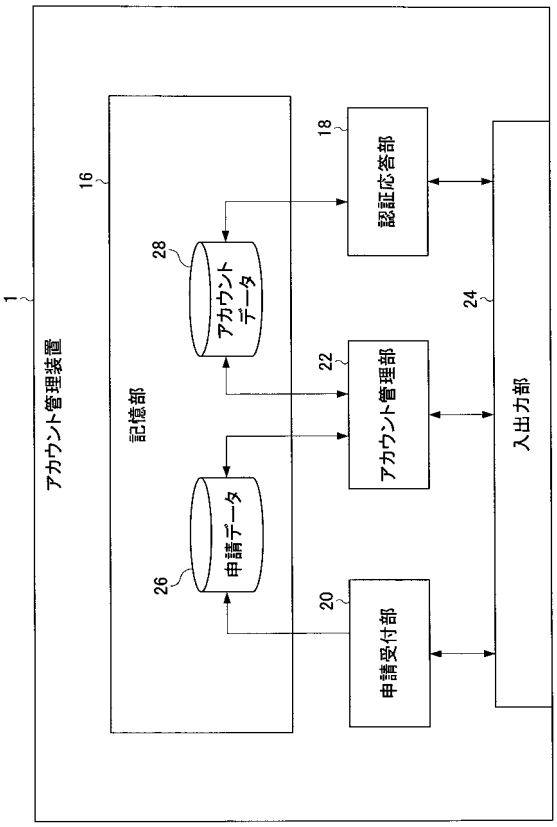
【００８１】

１　アカウント管理装置
２　認証スイッチ
４　作業端末
６　管理端末
８　共用サーバ
１０　ＬＡＮ
１２　ユーザ
１２ａ　新規ユーザ
１４　管理者
１８　認証応答部
２０　申請受付部
２２　アカウント管理部
２６　申請データ
２８　アカウントデータ
４０　限定ＶＬＡＮ
４２　全体ＶＬＡＮ

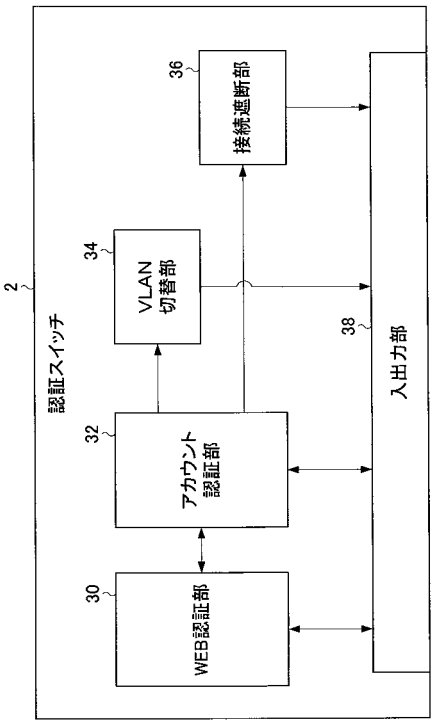
【図１】


1
アカウント管理装置
2
認証スイッチ
4
作業端末
6
管理端末
8
共用サーバ
10
12
ユーザ
12a
新規ユーザ
14
管理者

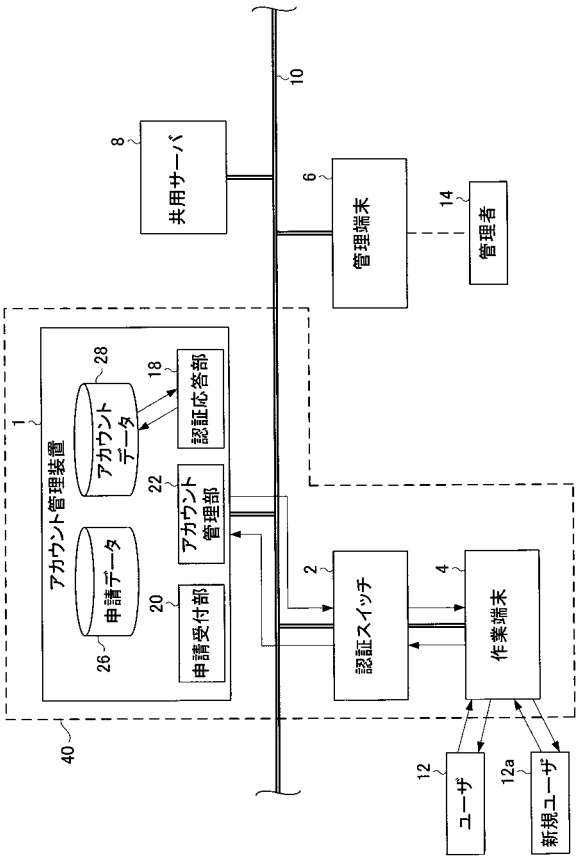
【図２】


1
アカウント管理装置
16
記憶部
18
認証応答部
20
申請受付部
22
アカウント管理部
24
入出力部
26
申請データ
28
アカウントデータ

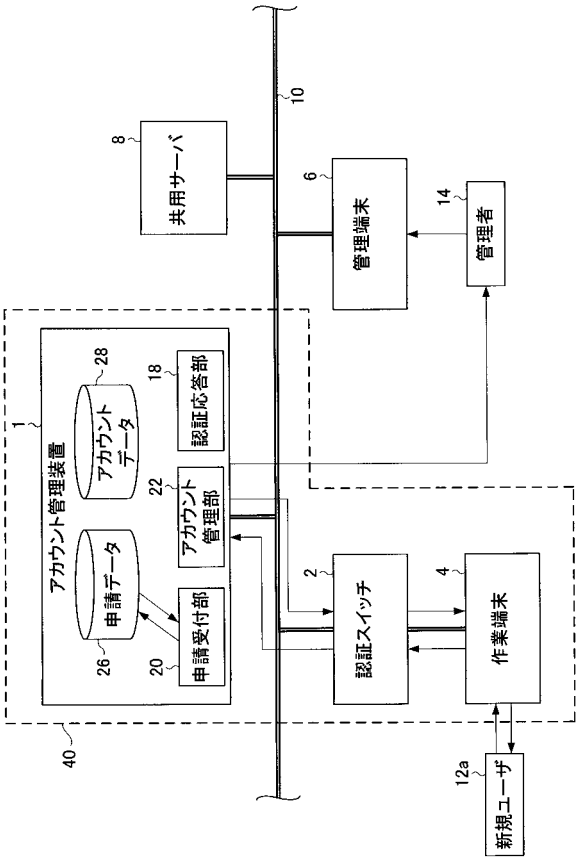
【図３】


2
認証スイッチ
30
WEB認証部
32
アカウント認証部
34
VLAN切替部
36
接続遮断部
38
入出力部

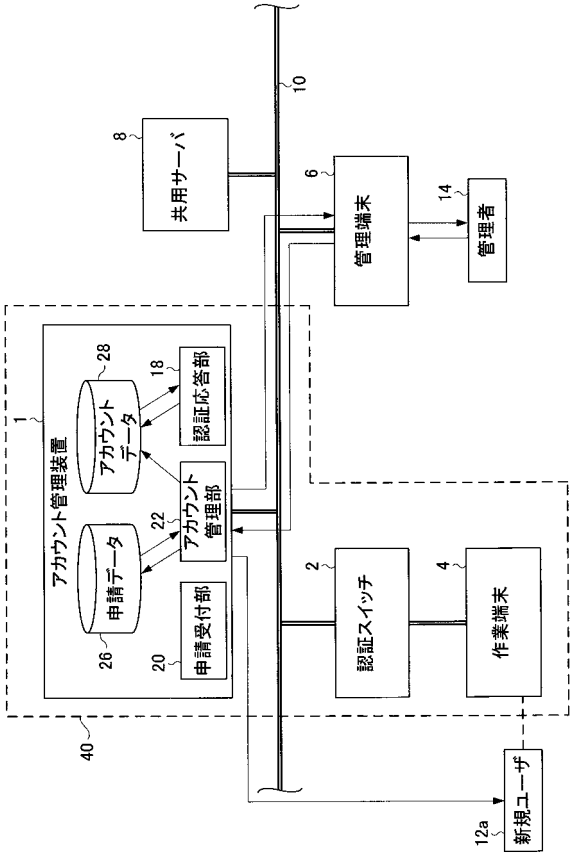
【図４】


1
アカウント管理装置
2
認証スイッチ
4
作業端末
6
管理端末
8
共用サーバ
10
12
ユーザ
12a
新規ユーザ
14
管理者
18
認証応答部
20
申請受付部
22
アカウント管理部
26
申請データ
28
アカウントデータ
40

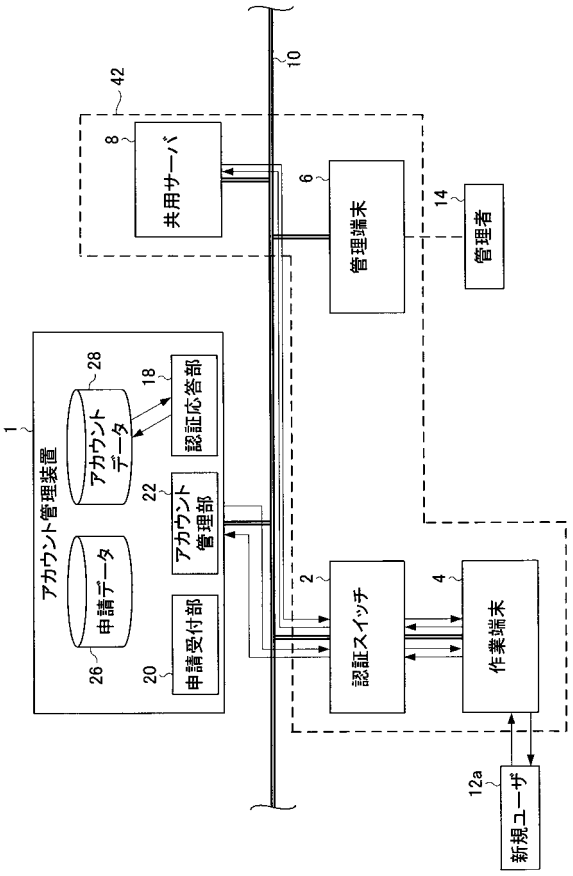
【図５】


共用サーバ
8
10
管理端末
6
管理者
14
アカウント管理装置
1
アカウントデータ
28
認証応答部
18
アカウント管理部
22
申請データ
26
申請受付部
20
認証スイッチ
2
作業端末
4
40
新規ユーザ
12a

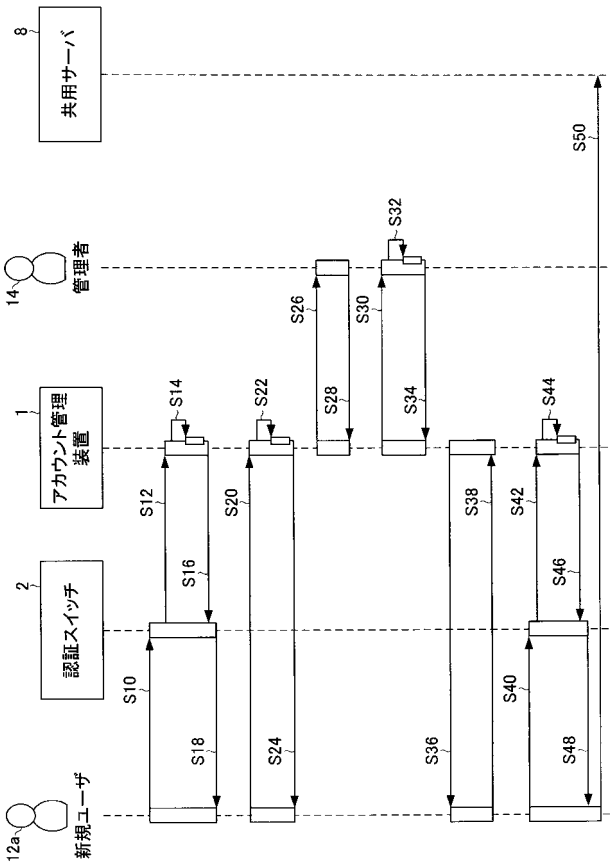
【図６】


共用サーバ
8
10
管理端末
6
管理者
14
アカウント管理装置
1
アカウントデータ
28
認証応答部
18
アカウント管理部
22
申請データ
26
申請受付部
20
認証スイッチ
2
作業端末
4
40
新規ユーザ
12a

【図７】


共用サーバ
8
42
10
管理端末
6
管理者
14
アカウント管理装置
1
アカウントデータ
28
認証応答部
18
アカウント管理部
22
申請データ
26
申請受付部
20
認証スイッチ
2
作業端末
4
新規ユーザ
12a

【図８】


共用サーバ
8
管理者
14
アカウント管理装置
1
認証スイッチ
2
新規ユーザ
12a
S10
S12
S14
S16
S18
S20
S22
S24
S26
S28
S30
S32
S34
S36
S38
S40
S42
S44
S46
S48
S50

フロントページの続き

(72)発明者　西野宮　浩志
東京都千代田区神田相生町１番地　日立電線ネットワークス株式会社内

Ｆターム(参考) 5B285 AA01 BA03 CB02 CB12 CB47 CB52 CB55 CB62 CB72
5J104 AA07 AA16 EA03 EA16 EA20 KA01 KA16 NA05 NA36 NA38