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

特許第4168052号
(P4168052)

(45)発行日　平成20年10月22日(2008.10.22)　(24)登録日　平成20年8月8日(2008.8.8)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330D
H04L 12/66 (2006.01)　　G06F 15/00 330A
　　H04L 12/66 B

請求項の数 11　(全 26 頁)

(21)出願番号　特願2005-296167(P2005-296167)
(22)出願日　平成17年10月11日(2005.10.11)
(65)公開番号　特開2006-309698(P2006-309698A)
(43)公開日　平成18年11月9日(2006.11.9)
審査請求日　平成19年4月18日(2007.4.18)
(31)優先権主張番号　特願2005-105835(P2005-105835)
(32)優先日　平成17年4月1日(2005.4.1)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　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　110000350
ポレール特許業務法人
(72)発明者　菊地　聡
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　常広　隆司
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】管理サーバ

(57)【特許請求の範囲】
【請求項１】
複数のクライアントと，該クライアントから接続される複数のコンピュータユニットの通信におけるパケットを中継する中継装置と、に接続される管理サーバであって，
順位付けされた複数の中継可否情報が設定可能であり，
受信したパケットについて，前記順位に従った複数の前記中継可否情報との照合を行い，中継可否を決定する手段と，
予め前記複数のコンピュータユニットのアドレスを含むパケットの遮断を指示する第一の中継可否情報を設定する手段と，
前記クライアントの使用者と，前記使用者が使用するコンピュータユニットを示す接続要求先識別子と，前記コンピュータユニットのアドレスと，当該コンピュータユニットの稼働状況を示す情報を含むステータスとを対応付けたエントリを管理する管理テーブルと，を備え，
いずれかの前記クライアントから接続要求を受信したら，前記接続を要求するクライアントの使用者の認証を行い，
前記認証に成功したら，前記管理テーブルを参照して，前記接続要求の送信元であるクライアントからのパケット送信を許可するいずれか一つのコンピュータユニットを，前記クライアントの前記使用者に基づいて選択し，
前記選択したコンピュータユニットが起動済みであることを確認した後に，
前記選択したコンピュータユニットを示す接続要求先識別子と，前記選択したコンピュ

ータユニットに接続するクライアントを示す接続元要求識別子と、を含む第二の中継可否情報を，前記第一の中継可否情報より高い順位で設定し，
前記第二の中継可否情報を設定した後に，前記選択したコンピュータユニットを示す接続先識別子を，前記接続を要求するクライアントに通知し，
前記コンピュータユニットに接続したクライアントと前記管理サーバ以外から，前記選択したコンピュータユニットへの接続を，前記中継装置に遮断させ，
前記選択したコンピュータユニットに接続したクライアントから，前記選択したコンピュータユニット以外への接続を，前記中継装置に遮断させることを特徴とする管理サーバ。

【請求項２】
請求項１記載の管理サーバであって，
前記接続要求先識別子はパケットの送信先識別子であり，前記接続要求元識別子はパケットの送信元識別子であり，
該送信先識別子が前記接続要求の送信元である前記クライアントを示し，該送信元識別子が前記選択したコンピュータユニットを示すパケットの中継を前記パケット中継装置に指示する第三の中継可否情報を，前記第一の中継可否情報より高い順位を与えて設定することを前記パケット中継装置に指示することを特徴とする管理サーバ。

【請求項３】
請求項1又は２記載の管理サーバであって，
前記選択したコンピュータユニットが起動済みでなかった場合には，前記選択したコンピュータユニットに起動を要求し，
前記選択したコンピュータユニットの起動完了通知を受信した場合に，前記起動済みであると判断することを特徴とする管理サーバ。

【請求項４】
請求項1乃至３のいずれか1つに記載の管理サーバであって，
前記クライアントから前記選択したコンピュータユニットへの接続の中断要求を受けた場合に，前記第二の中継可否情報の削除を前記パケット中継装置に指示し，
前記選択したコンピュータユニットは，前記起動状態を継続することを特徴とする管理サーバ。

【請求項５】
請求項1乃至３のいずれか1つに記載の管理サーバであって，
前記クライアントから前記選択したコンピュータユニットへの接続の終了要求を受けた場合に，前記コンピュータユニットがシャットダウンしたことを確認した後に，前記第二の中継可否情報の削除を前記パケット中継装置に指示することを特徴とする管理サーバ。

【請求項６】
請求項２乃至５のいずれか1つに記載の管理サーバであって，
前記第一乃至第三のいずれか1つの中継可否情報の，前記選択したコンピュータユニットの送信先識別子又は送信元識別子は，前記選択したコンピュータユニットのアドレスと通信プロトコルのポート番号の組み合わせであることを特徴とする管理サーバ。

【請求項７】
請求項２乃至５のいずれか1つに記載の管理サーバであって，
前記コンピュータユニットに係わる前記第一の中継可否情報の前記送信先識別子は，特定の通信プロトコルのポート番号を更に含み，
前記第一の中継可否情報で特定されなかったパケットの中継を前記パケット中継装置に指示する第四の中継可否情報が，前記第一の中継可否情報より低い順位が与えられて，前記パケット中継装置に予め設定されていることを特徴とする管理サーバ。

【請求項８】
請求項1乃至７のいずれか1つに記載の管理サーバであって，
前記コンピュータユニットと前記クライアントとの通信が途絶えた場合に，前記コンピュータユニットの備える前記クライアントとの通信状態の監視手段から通知を受信し，

前記第二の中継可否情報の削除を前記パケット中継装置に指示することを特徴とする管理サーバ。

【請求項９】

請求項３記載の管理サーバであって，

前記管理テーブルの初期化時に，前記ステータスとして「終了(未起動)」を設定し，

前記選択したコンピュータユニットが起動し，前記第二の中継可否情報を設定した後に，当該コンピュータユニットに係わるエントリの前記ステータスとして「接続」を設定することを特徴とする管理サーバ。

【請求項１０】

請求項４記載の管理サーバであって，

前記第二の中継可否情報の削除を前記パケット中継装置に指示した場合には，前記管理テーブルの前記コンピュータユニットに係わるエントリの前記ステータスとして「中断」を設定することを特徴とする管理サーバ。

【請求項１１】

請求項５に記載の管理サーバであって，

前記第二の中継可否情報の削除を前記パケット中継装置に指示した場合には，前記管理テーブルの前記コンピュータユニットに係わるエントリの前記ステータスとして「終了(未起動)」を設定することを特徴とする管理サーバ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ターミナルサービス等において好適なアクセス制御サービス及び制御サーバに関するものである。

【背景技術】

【０００２】

近年のインターネットの普及に伴い、外出先や自宅等あらゆる場所にて、コンピュータ（ＰＣ）を用いてメールやＷｅｂ、文書作成等、多種多様な作業（以下ＰＣ業務）を行いたいという要求がある。これを実現するため、ネットワーク経由で遠隔地のコンピュータ（リモートコンピュータ）にアクセスし、そのコンピュータのデスクトップ画面を手元の端末に表示し作業を行うシステムが実用化されており、一般にターミナルサービスと呼ばれる。このターミナルサービスにおいて、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）やＰＣ業務に使用するアプリケーション等のソフトウェア及び作成データは、全てリモートコンピュータ側のハードディスク等の二次記憶装置に格納され、各ソフトウェアはリモートコンピュータのＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）により実行される。ユーザが直接操作する手元の端末は、キーボードやマウス等のユーザＩ／Ｆデバイスから入力される制御情報をリモートコンピュータに送信し、またリモートコンピュータから送られるデスクトップ画面情報をディスプレイに表示する。

【０００３】

ターミナルサービスには２つの形態がある。第１の形態は、１台のリモートコンピュータを一人のユーザが占有するもので、Ｐ２Ｐ（Ｐｅｅｒ　ｔｏ　Ｐｅｅｒ）タイプ、リモートデスクトップ機能と呼ばれる。第２の形態は、１台のリモートコンピュータを複数のユーザが共有するもので、ＳＢＣ（Ｓｅｒｖｅｒ　Ｂａｓｅｄ　Ｃｏｍｐｕｔｉｎｇ）タイプ、ターミナルサーバと呼ばれる。

【０００４】

ユーザはＰＣ業務を始める際、手元の端末からリモートコンピュータへ接続要求を行う。このときリモートコンピュータは、他人による不正アクセスを防止するため、本人性、つまりユーザが確かにそのリモートコンピュータの利用者本人であることを検証するユーザ認証を実施する。ユーザ認証としては、ユーザＩＤとパスワードの組み合わせにより本人性を検証する手法が広く用いられる。リモートコンピュータは、接続要求を受けるとログイン画面を表示し、ユーザが入力（ログイン）したユーザＩＤとパスワードを、予め登

録されたユーザＩＤとパスワードの組み合わせと照合する。これらが一致した場合は接続要求を許可し、ユーザの端末に対してターミナルサービスを提供する。これらが一致しない場合、リモートコンピュータは接続要求を拒否する。

【０００５】

上記ユーザ認証とターミナルサービスへの接続を行う際の利便性と安全性を鑑み、ＩＣカードのような記録媒体を利用する接続方式も提案されている。例えば特許文献１に記載の技術は、ネットワークを介して端末をサーバに接続するのに必要な第１の情報とユーザを認証するための第２の情報を格納した記録媒体（ＩＣカード）を端末に装着し、ユーザが入力した情報を前記記録媒体に格納された第２の情報と照合して一致したときに前記記録媒体から読み出した第１の情報を用いてサーバに自動接続するものである。

【０００６】

また、不正ユーザによるシステムの不正利用を防止する方式も提案されている。例えば特許文献２に記載の技術は、ファイルサーバへのアクセス時にユーザ認証し、認証に成功したユーザが操作する端末からの通信パケットのみを中継し、他の端末からの通信パケットは破棄するよう、ネットワーク機器を制御するものである。

【０００７】

【特許文献１】特開２００１－２８２７４７号公報

【特許文献２】米国特許第６９０７４７０号明細書

【発明の開示】

【発明が解決しようとする課題】

【０００８】

前述したターミナルサービスへの接続方法の場合、以下のような課題がある。

【０００９】

ユーザＩＤとパスワードの組み合わせによるユーザ認証方法は、数字やアルファベットの組み合わせを総当りで試すブルートフォース攻撃や、単語、人名等の辞書による辞書攻撃等のパスワード攻撃に対し、完全には防御できない。その結果、他人にパスワードを解析され、リモートコンピュータに不正にアクセスされ、格納したデータを盗み読みされる恐れがある。特に、ターミナルサービスのようにネットワークを介したユーザ認証の場合は、ネットワークが接続されているあらゆる場所から、顔を見られることなく、また所要時間を気にすることもないので、パスワード攻撃を受けやすい。

【００１０】

上記パスワード攻撃を抑止するため、汎用のＯＳには、ログインの試みを一定回数以内に制限するアカウントロックアウト機能を備えるものが多い。すなわち、例えば３回連続してログインに失敗した場合、以降一定期間、そのコンピュータへのログインを不可能（ロックアウト状態）とするものである。アカウントロックアウト機能によれば、ログインの試みは設定時間内に一定回数しかできないので、短時間に多数回のログインを仕掛けるパスワード攻撃に対し有効な対策となる。

【００１１】

しかしながらアカウントロックアウト機能についても、これを悪用した正規のユーザに対する嫌がらせ行為の恐れもある。すなわち、正規のユーザのアカウントに対し、他人が故意にログイン失敗を続けてロックアウト状態にして、正規のユーザがコンピュータを利用できなくさせることができる。このような嫌がらせ行為も一種のパスワード攻撃と言える。

【００１２】

前記特許文献１に記載の技術を用いても、このようなパスワード攻撃に対しては、防御することは困難である。

【００１３】

前記特許文献２に記載の技術を用いることにより、認証されていない匿名ユーザによるパスワード攻撃については防御できるが、認証された正規ユーザならば他人のリモートコンピュータにアクセス可能であり、内部犯罪のパスワード攻撃を防御することは困難であ

る。
【００１４】
さらに、侵入可能な通信ポートを探るポートスキャン攻撃や、大量のデータをコンピュータに送りつけ、サービスを不能にするＤｏＳ（Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅｓ）攻撃等、コンピュータを攻撃する様々なソフトウェアが、インターネットから入手可能であり、組織内のコンピュータといえども安全ではなくなってきている。
【００１５】
本発明の目的はターミナルサービス等において、パスワード攻撃等の不正アクセスからコンピュータを防御するアクセス制御サービス及び制御サーバを提供することである。
【課題を解決するための手段】
【００１６】
上記目的を達成するため、本発明に係るアクセス制御サービスは、端末を操作するユーザを認証し、その認証結果に応じて、ユーザの操作する端末と特定のコンピュータユニットとの間の通信を可能とするネットワークリンクを設定する制御サーバを備える。そして制御サーバには、各ユーザの情報と、各ユーザが利用可能な特定のコンピュータユニットの情報とが関連付けて登録されている。
【００１７】
また本発明に係るアクセス制御サービスは、各コンピュータユニットに接続され、ユーザ毎に利用可能な記憶領域が割り当てられた共有の記憶装置と、端末を操作するユーザを認証し、その認証結果に応じて記憶装置内のそのユーザに割り当てられた記憶領域を何れかのコンピュータユニットにマウントし、ユーザの操作する端末とマウントしたコンピュータユニットとの間の通信を可能とするネットワークリンクを設定する制御サーバを備える。そして制御サーバには、各ユーザの情報と、各ユーザが利用可能な前記記憶装置内の記憶領域の情報とが関連付けて登録されている。
【００１８】
さらに本発明に係るアクセス制御サービスは、ネットワークを介して各端末に接続され、ユーザ毎に利用可能な記憶領域が割り当てられた共有の記憶装置と、端末を操作するユーザを認証し、その認証結果に応じて記憶装置内のそのユーザに割り当てられた記憶領域をユーザの操作する端末にマウントし、ユーザの操作する端末と記憶装置との間の通信を可能とするネットワークリンクを設定する制御サーバを備える。そして制御サーバには、各ユーザの情報と、各ユーザが利用可能な前記記憶装置内の記憶領域の情報とが関連付けて登録されている。
【００１９】
本発明に係る制御サーバは、端末を操作するユーザを認証する認証部と、認証結果に応じて、ユーザの操作する端末と特定の上記コンピュータユニットとの間の通信を可能とするネットワークリンクを設定するリンク設定部とを備える。
【００２０】
また本発明に係る制御サーバは、端末を操作するユーザを認証する認証部と、認証結果に応じて、各コンピュータユニットに接続された共有の記憶装置内のそのユーザに割り当てられた記憶領域を何れかのコンピュータユニットにマウントするコンピュータユニット管理部と、ユーザの操作する端末とマウントしたコンピュータユニットとの間の通信を可能とするネットワークリンクを設定するリンク設定部とを備える。
【００２１】
さらに本発明に係る制御サーバは、端末を操作するユーザを認証する認証部と、認証結果に応じて、ネットワークを介して各端末に接続された共有の記憶装置内のそのユーザに割り当てられた記憶領域をユーザの操作する端末にマウントするコンピュータユニット管理部と、ユーザの操作する端末と記憶装置との間の通信を可能とするネットワークリンクを設定するリンク設定部とを備える。
【発明の効果】
【００２２】

本発明によれば、正規ユーザ以外からの不正アクセスを防御し、ユーザデータを安全に保護するアクセス制御サービスを提供できる。

【発明を実施するための最良の形態】

【００２３】

以下、本発明によるアクセス制御サービス及び制御サーバの実施形態について、図面を用いて説明する。

【実施例１】

【００２４】

図１は、本発明によるアクセス制御サービスを実行するコンピュータシステムの第１の実施例を示す構成図である。ＬＡＮ等のネットワーク５に、１台以上（この例では３台）の端末１（１ａ，１ｂ，１ｃ）と、ハブ４を介して１台以上（この例では３台）のコンピュータユニット２（２ａ，２ｂ，２ｃ）と、アクセス制御サーバ３とが接続されている。またアクセス制御サーバ３は、ハブ４の管理用ポートに直結されている。そしてユーザは、端末１の何れかを操作して、特定のコンピュータユニット２にアクセスし、Ｐ２Ｐタイプのターミナルサービスの提供を受ける。ここに各端末１やアクセス制御サーバ３は、リピータハブやスイッチングハブ、スイッチ等のネットワーク機器を介して、ネットワーク５に接続されても良い。

【００２５】

各コンピュータユニット２は、ＯＳや業務に使用するアプリケーション等のソフトウェア、及び作成したデータ等を格納するハードディスク等の二次記憶装置と、各ソフトウェアを実行するＣＰＵ等を備えたリモートコンピュータである。

【００２６】

ハブ４は、あるコンピュータから受信した通信パケットを他のコンピュータに送信する中継機能を備え、かつその中継を指定されたコンピュータ間にのみ限定しそれ以外のコンピュータ間の中継を遮断するフィルタリング機能を備えたネットワーク機器である。ハブ４には、汎用のスイッチングハブ、スイッチ、ブリッジ等を適用できる。

【００２７】

図１３は、本実施例における端末１の内部構成の一例を示す図である。

【００２８】

端末１は、ＣＰＵ４０、メモリ４１、ディスプレイ４２、ユーザＩ／Ｆデバイス（キーボード４３やマウス４４等）、二次記憶装置４６（ハードディスクやフラッシュメモリ等）、ネットワークＩ／Ｆ６２（ネットワーク５を介して他のコンピュータとデータを授受するＬＡＮカード等）から構成されるコンピュータである。また、ユーザの本人性を検証するため、ＩＣカード等の認証デバイス４５が接続される。メモリ４１には、各種プログラムが格納される。通信制御プログラム５０は、ネットワークＩ／Ｆ６２を介して他のコンピュータと通信する。コンピュータユニット制御プログラム４７は、アクセス制御サーバ３と対話する。認証制御プログラム４８は、認証デバイス４５によりユーザの本人性を示す情報を生成する。ターミナルサービス制御プログラム４９は、ユーザＩ／Ｆデバイスから入力される制御情報をコンピュータユニット２に送信し、コンピュータユニット２から送られるデスクトップ画面情報をディスプレイ４２に表示する。これらのプログラムは、当初、二次記憶装置４６に格納され、必要に応じてメモリ４１に転送された後、ＣＰＵ４０で実行される。

【００２９】

アクセス制御サーバ３は、どの端末とどのコンピュータユニット間の中継を許可するか（すなわち「ネットワークリンク」の形成）を決定し、上記ハブ４に設定コマンドを発行する。

【００３０】

ここで、「ネットワークリンク」について説明する。各端末と各コンピュータユニットはネットワークを介して物理的に接続されている。本実施例における「ネットワークリンク」とは、ネットワーク上に形成される、特定の端末と特定のコンピュータユニット間の

論理的な通信チャネルである。双方のアプリケーションプログラムは、形成された通信チャネルを用いることにより、ネットワークを介してアプリケーションデータを送受することが可能となる。ＯＳＩ（Ｏｐｅｎ　Ｓｙｓｔｅｍｓ　Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）参照モデルを例にとると、本実施例の通信チャネルは、アプリケーション層に対して通信機能を提供する下位層（ＴＣＰ等のトランスポート層やＩＰ等のネットワーク層）に形成される。

【００３１】

これらの下位層に本実施例における通信チャネル（すなわち「ネットワークリンク」）が形成されなければ、ターミナルサービス等、アプリケーション層の通信も行えない。すなわち「ネットワークリンク」上は、ユーザ認証した端末と、アクセス制御サーバが特定したコンピュータユニット間の通信パケットが伝送され、他の通信パケットは伝送されない。

【００３２】

また、本実施例のネットワークリンクは、ユーザが利用中に限り形成される動的な通信チャネルである。よって全ユーザが利用中の場合は、ユーザ数に相当するネットワークリンクが形成される。

【００３３】

図２は、本実施例におけるアクセス制御サーバ３の論理構成の一例を示す図である。

【００３４】

通信制御部６は、ネットワーク５を介して端末１との通信処理を実行する。認証処理部７は、ユーザの本人性を検証しユーザ認証を行う。コンピュータユニット管理部８は、コンピュータユニット２の起動、シャットダウンを実行する。ＡＣＥ設定部（リンク設定部）９は、ハブ４に対し中継の許可に関するＡＣＥ（Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｅｎｔｒｙ）の追加や削除を発行し、ネットワークリンクを形成させる。管理データベース（ＤＢ）１０は、各ユーザと各コンピュータユニット２に関する管理情報を記憶し、特定のユーザと特定のコンピュータユニットとの対応付けを行うものである。

【００３５】

図１４は、本実施例におけるアクセス制御サーバ３の内部構成の一例を示す図である。

【００３６】

アクセス制御サーバ３は、ＣＰＵ５６、メモリ５７、ディスプレイ５８、ユーザＩ／Ｆデバイス（キーボード５９やマウス６０等）、二次記憶装置６１（ハードディスク等）、ネットワークＩ／Ｆ６３（ネットワークを介して他のコンピュータやハブ４とデータを授受する）から構成されるコンピュータである。メモリ５７には、各種プログラムが格納される。通信制御プログラム６４は、ネットワークＩ／Ｆ６３を介して他のコンピュータやハブ４と通信する。認証処理プログラム６５は図２の認証処理部７に相当し、コンピュータユニット管理プログラム６６はコンピュータユニット管理部８に相当し、ＡＣＥ設定プログラム６７はＡＣＥ設定部９に相当する。これらのプログラムは、当初、二次記憶装置６１に格納され、必要に応じてメモリ５７に転送された後、ＣＰＵ５６で実行される。また、二次記憶装置６１には管理ＤＢ１０も格納される。

【００３７】

図３は、管理ＤＢ１０の記憶する情報の内容の一例を示す図である。ユーザ管理テーブル１１にはユーザに関する管理情報を記憶し、コンピュータユニット管理テーブル１２にはコンピュータユニット２に関する管理情報を記憶する。

【００３８】

ユーザ管理テーブル１１は、コンピュータユニット２を利用するユーザ数に相当する配列（ユーザエントリ）を有する。各ユーザエントリに記憶する情報は、そのユーザを一意に識別するユーザＩＤ１３、そのユーザが使用する特定のコンピュータユニット２のＩＤ１４、そのＩＰアドレス１５、およびそのステータス（稼動状況、接続／中断／終了）１６などである。ステータス１６は「終了」に初期化されるが、それ以外の各管理情報は、システム管理者の権限でその値を設定する。

【００３９】
コンピュータユニット管理テーブル１２は、利用するコンピュータユニット２の設置数に相当する配列（コンピュータユニットエントリ）を有する。各コンピュータユニットエントリに記憶する情報は、そのコンピュータユニットを一意に識別するコンピュータユニットＩＤ１７、そのコンピュータユニットを起動させる際に用いるＭＡＣアドレス１８などである。各管理情報は、システム管理者の権限で値を設定する。なお、各情報の配置は必ずしもこれに限らない。例えば、ＩＰアドレス１５はＯＳに登録される情報であるため、ユーザ管理テーブル１１に含めたが、コンピュータユニット２に関連した情報と捉えて、コンピュータユニット管理テーブル１２に含めても良い。

【００４０】
特定のユーザと特定のコンピュータユニットとの対応付け、すなわち、個々のユーザエントリと個々のコンピュータユニットエントリの対応は、それぞれが記憶するコンピュータユニットＩＤ１４とコンピュータユニットＩＤ１７の情報を共有することで関連付けられる。

【００４１】
図４は、アクセス制御サーバ３がハブ４に対して設定する中継可否情報（ＡＣＥ）の一例を示すものである。ＡＣＥは、３つのパートから成り、「，」により区切られる。第１のパートは中継の可否を表し、「ｐｅｒｍｉｔ」は中継可を、「ｄｅｎｙ」は中継不可を示す。第２及び第３のパートは、アクセス制御対象の通信パケットを指定するものであり、第２のパートはソースアドレス（発信側コンピュータのＩＰアドレス）、第３のパートはデスティネーションアドレス（着信側コンピュータのＩＰアドレス）である。図４に示したＡＣＥ１９は、ＩＰアドレス「１９２．１６８．４．７１」からＩＰアドレス「１９２．１６８．０．２」宛の通信パケットの中継を許可するものである。

【００４２】
ハブ４には複数のＡＣＥを設定できる。これらＡＣＥのリストはＡＣＬ（Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ Ｌｉｓｔ）と呼ばれる。一般のハブ４においては、ＡＣＬにＡＣＥを追加する際、検索順位を指定可能である。検索順位の指定方法としては、例えば、先頭からｍ番目のＡＣＥとして挿入する、もしくは後端からｎ番目のＡＣＥとして挿入する方法や、追加するＡＣＥに検索順位番号を付与する方法等が挙げられる。ハブ４は、通信パケットを受信した際、検索順位に従って、ＡＣＬ内のＡＣＥを順に読み込み、通信パケットに記述されるソースアドレス及びデスティネーションアドレスと照合する。そして、これらのアドレスと一致するＡＣＥを発見した場合は、そのＡＣＥの第１パートを参照し、その指示（ｐｅｒｍｉｔ／ｄｅｎｙ）に従ってその通信パケットを中継あるいは遮断する。アドレスが一致するＡＣＥをＡＣＬ内に発見できなかったときは、その通信パケットに対して、デフォルトのＡＣＥが適用される。デフォルトのＡＣＥは、第１パート（ｐｅｒｍｉｔ／ｄｅｎｙ）のみを記述したものである。本実施例においては、システム管理者がシステム稼動前に、デフォルトＡＣＥの第１パートに「ｄｅｎｙ」を設定しておくことで、設定外のアドレス間での通信を遮断することができる。

【００４３】
尚、本実施例のアクセス制御サーバ３は、後述するように、コンピュータユニットに対して、起動を要求する「マジックパケット」と呼ばれる通信パケットを送信する。このパケットをハブ４経由で送信する場合は、第１パートが「ｐｅｒｍｉｔ」、第２パートがアクセス制御サーバ３のＩＰアドレス、そして第３パートが「空き」のＡＣＥを、ハブ４に予め設定しておけば良い。ＡＣＥの第２もしくは第３パートが「空き」の場合、ハブ４は無指定と解釈する。前記ＡＣＥの場合、アクセス制御サーバ３が送信した通信パケットは、宛先のコンピュータユニットに関わらず、全て中継される。また、コンピュータユニット２がアクセス制御サーバ３に対して送信する通信パケットが存在する場合は、第１パートが「ｐｅｒｍｉｔ」、第２パートが「空き」、そして第３パートがアクセス制御サーバ３のＩＰアドレスであるＡＣＥを、ハブ４に予め追加しておいても良い。

【００４４】

次に、本実施例のアクセス制御サービスの処理フローについて説明する。

【００４５】

図５は、各機器間での一連の通信シーケンスを示す図、図６、図７、図８は、各々接続処理、中断処理、終了処理のフローチャートを示す図である。なおここで言う「接続／中断」とは、端末とコンピュータユニットの間で通信可能／不可能な状態を意味する。

【００４６】

最初に、図５と図６を用いて、ユーザが端末１を操作してコンピュータユニット２へ接続する際の処理を説明する。

【００４７】

ユーザは端末１のコンピュータユニット制御プログラム４７を操作し、アクセス制御サーバ３に対して接続要求（Ｆ５０１）を送信する。アクセス制御サーバ３の通信制御部６は、接続要求（Ｆ５０１）を受信し、認証処理部７に対してユーザ認証を依頼する。

【００４８】

本実施例においては、ユーザ認証方式として、インターネットにおける標準化機関であるＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ）が規格化しているＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）プロトコルを利用する。ＴＬＳはＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）として広く知られた技術であり、公開鍵と秘密鍵の鍵ペアによりデータを暗復号する公開鍵暗号技術と、公開鍵の正当性を保証する公開鍵証明書を用いて、通信者の本人性を検証するとともに、通信データの暗号化を行うプロトコルである。認証する対象として、サーバの本人性を検証するサーバ認証と、クライアントの本人性を検証するクライアント認証が規定されている。クライアント認証を用いる場合は、各ユーザが自分の公開鍵と秘密鍵、そして公開鍵証明書を持つ。これらは、端末１の二次記憶装置４６に格納しても良いし、ＩＣカード等、鍵を安全に保管可能な認証デバイス４５に格納しても良い。

【００４９】

認証処理部７は、上記ＴＬＳクライアント認証を用いて、端末１を操作するユーザの本人性を検証する（Ｓ６０１）。その検証結果と、正規のユーザであることが検証できた場合にはユーザの公開鍵証明書に含まれる主体者名（ｓｕｂｊｅｃｔ）を通信制御部６へ返す。通信制御部６は、コンピュータユニット管理部８に対して、主体者名を渡し、コンピュータユニット２の起動を依頼する（Ｓ６０２）。

【００５０】

依頼を受けたコンピュータユニット管理部８は、管理ＤＢ１０内のユーザ管理テーブル１１を検索し、渡された主体者名と同一の値がユーザＩＤ１３として登録されたユーザエントリを探す。エントリを発見すると、そのユーザが利用する特定のコンピュータユニット２のコンピュータユニットＩＤ１４とそのステータス１６を参照し、そのコンピュータユニット２が起動されているか否かを確認する（Ｓ６０３）。ステータス１６の値が「終了（未起動）」である場合は、そのコンピュータユニット２を起動する。

【００５１】

本実施例においては、コンピュータユニットを起動するために、マジックパケットと呼ばれる技術を用いる。マジックパケットは、ネットワークを介して接続されたコンピュータをリモート起動するための通信パケットであり、ＬＡＮカード固有のＭＡＣアドレスにより、起動するコンピュータを指定する。

【００５２】

コンピュータユニット管理部８は、コンピュータユニットＩＤ１４の値を取り出し、コンピュータユニット管理テーブル１２から同一の値がコンピュータユニットＩＤ１７に登録されたコンピュータユニットエントリを探す。そして、発見したエントリのＭＡＣアドレス１８に登録された値を取り出し、それを含むマジックパケット（Ｆ５０２）を組み立て、ネットワーク５を介してコンピュータユニット２へ送信する（Ｓ６０４）。コンピュータユニット２は起動完了すると、起動完了通知（Ｆ５０３）を返す。コンピュータユニット管理部８は起動完了を確認すると、ユーザエントリ内のＩＰアドレス１５に登録され

た値を取り出して、通信制御部６へ通知する。

【００５３】

次に通信制御部６は、受信した接続要求（Ｆ５０１）の通信パケットからソースアドレスを抽出し、コンピュータユニット管理部８から通知されたコンピュータユニット２のＩＰアドレス１５と共にＡＣＥ設定部９に渡し、ＡＣＥの追加設定を依頼する。

【００５４】

通信制御部６から依頼を受けたＡＣＥ設定部９は、図４に示したＡＣＥを生成する（Ｓ６０５）。ＡＣＥの構成は、具体的には、第１パートが「ｐｅｒｍｉｔ」、第２パートが渡されたソースアドレス、第３パートが渡されたＩＰアドレスである。次にＡＣＥ設定部９は、生成したＡＣＥを追加設定する要求（Ｆ５０４）を、管理用ポートを介してハブ４に依頼する（Ｓ６０６）。これにより、接続を要求した端末１とそのユーザが利用する特定のコンピュータユニット２間にネットワークリンクが形成される。その後、ＡＣＥ設定部９は通信制御部６へ制御を返す。

【００５５】

通信制御部６は、コンピュータユニット管理部８に対して、ユーザエントリ内のステータス１６の値を「接続」に変更するよう依頼する（Ｓ６０７）。その後、接続要求（Ｆ５０１）に対する応答として、コンピュータユニット管理部８から通知されたコンピュータユニット２のＩＰアドレス１５と共に、接続の準備が整ったことを表す接続可通知（Ｆ５０５）を、端末１へ返す（Ｓ６０８）。

【００５６】

接続可通知（Ｆ５０５）を受信すると、端末１のコンピュータユニット制御プログラム４７は、通知されたＩＰアドレスをターミナルサービス制御プログラム４９に伝達する。ターミナルサービス制御プログラム４９はそのＩＰアドレスを用いて、コンピュータユニット２にターミナルサービス接続要求（Ｆ５０６）を送る。そしてユーザは、ログイン画面にユーザＩＤとパスワードを入力後、ターミナルサービスの提供を受けて、ＰＣ業務を行う。

【００５７】

上記認証工程（Ｓ６０２）において、認証処理部７が端末１を操作するユーザの本人性を検証できなかった場合には、通信制御部６は、端末１に対して利用不可通知を返し（Ｓ６０９）、何れのコンピュータユニット２に対しても起動やネットワークリンクの設定を行わない。

【００５８】

次に、図５と図７を用いて、離席時等、ユーザが一時的に端末１から離れる際の中断処理を行う場合を説明する。これは、ユーザが離席している間に、他のユーザがその端末を操作し不正なアクセスを行うことを防止するために有効となる。

【００５９】

ユーザは端末１から離れる際、端末１のコンピュータユニット制御プログラム４７を操作し、アクセス制御サーバ３に対して中断要求（Ｆ５０７）を送信する。アクセス制御サーバ３の通信制御部６は、中断要求（Ｆ５０７）を受信し、ＡＣＥ設定部９に対してＡＣＥの削除を依頼する。

【００６０】

通信制御部６から依頼を受けたＡＣＥ設定部９は、前記接続工程（図６のＳ６０６）において追加設定したＡＣＥを削除する要求（Ｆ５０８）を、管理用ポートを介してハブ４に依頼する（Ｓ７０１）。これにより、接続中の端末１とそのユーザが利用する特定のコンピュータユニット２間に設定されていたネットワークリンクが解除され、両者の通信は遮断される。ただし、コンピュータユニット２はそのまま起動状態を継続する。その後、ＡＣＥ設定部９は通信制御部６へ制御を返す。

【００６１】

次に通信制御部６は、コンピュータユニット管理部８に対して、ユーザエントリ内のステータス１６の値を「中断」に変更するよう依頼（Ｓ７０２）する。そして、中断要求（

Ｆ５０７）に対する応答として、中断処理が正常に完了したことを表す中断完通知（Ｆ５０９）を、端末１へ返す（Ｓ７０３）。

【００６２】

その後、ユーザは端末１の前に戻り、ＰＣ業務を再開する。再開時の処理は、先に図６にて説明した接続要求時と同様であり、端末１のコンピュータユニット制御プログラム４７を操作し、アクセス制御サーバ３に対して接続要求（Ｆ５１０）を送信し、再度ユーザ認証とＡＣＥの設定を行う。ただし接続対象のコンピュータユニット２はすでに起動状態「中断」にあるので、コンピュータユニット２を起動する工程（Ｓ６０４）をスキップする。生成したＡＣＥの追加要求（Ｆ５１１）をハブ４へ送信する（Ｓ６０６）と、中断していた端末１と特定のコンピュータユニット２の間に再びネットワークリンクが形成される。

【００６３】

接続可通知（Ｆ５１２）を受信した端末１のコンピュータユニット制御プログラム４７はターミナルサービス制御プログラム４９を起動し、コンピュータユニット２にターミナルサービス接続要求（Ｆ５１３）を送り、ユーザがログイン操作（ユーザＩＤとパスワードを入力）を行って、ＰＣ業務を再開する。

【００６４】

次に、図５と図８を用いて、帰宅時等、ユーザがＰＣ業務を終了する際の終了処理を説明する。

【００６５】

ユーザは、ＰＣ業務を終了する際、端末１のコンピュータユニット制御プログラム４７を操作し、アクセス制御サーバ３に対して終了要求（Ｆ５１４）を送信する。アクセス制御サーバ３の通信制御部６は、終了要求（Ｆ５１４）を受信し、コンピュータユニット管理部８に対してコンピュータユニット２のシャットダウンを依頼する。

【００６６】

依頼を受けたコンピュータユニット管理部８は、ネットワーク５を介して、コンピュータユニット２へシャットダウン要求（Ｆ５１５）を送信し（Ｓ８０１）、シャットダウン完了通知（Ｆ５１６）を待つ。シャットダウン完了を確認したコンピュータユニット管理部８は、通信制御部６へ制御を返す。

【００６７】

通信制御部６は、ＡＣＥ設定部９に対してＡＣＥの削除を依頼する。通信制御部６から依頼を受けたＡＣＥ設定部９は、設定中のＡＣＥを削除する要求（Ｆ５１７）を、管理用ポートを介してハブ４に発行する（Ｓ８０２）。これにより、接続中の端末１と特定のコンピュータユニット２間に設定されていたネットワークリンクが解除され、両者の通信は遮断される。その後、ＡＣＥ設定部９は通信制御部６へ制御を返す。

【００６８】

また通信制御部６は、コンピュータユニット管理部８に対して、ユーザエントリ内のステータス１６の値を「終了」に変更するよう依頼（Ｓ８０３）する。そして、終了要求（Ｆ５１４）に対する応答として、シャットダウン処理が正常に完了したことを表す終了完通知（Ｆ５１８）を、端末１へ返す（Ｓ８０４）。

【００６９】

次に、図９を用いて、本実施例によるアクセス制御動作とその作用効果、すなわち不正アクセス防止機能について説明する。

【００７０】

ネットワーク５に、３台の端末１ａ，１ｂ，１ｃと３台のコンピュータユニット２ａ，２ｂ，２ｃが接続されている。各端末のＩＰアドレスを、各々「１９２．１６８．４．７１」、「１９２．１６８．５．４８」、「１９２．１６８．６．１０」とする。一方、各コンピュータユニットのＩＰアドレスを、各々「１９２．１６８．０．２」、「１９２．１６８．０．３」、「１９２．１６８．０．４」とする。２人のユーザａ，ｂはそれぞれ端末１ａ，１ｂを操作し、各々特定のコンピュータユニット２ａ，２ｂを利用できるもの

とする。

【００７１】

端末１ａを操作するユーザａが、アクセス制御サーバ３に対して接続要求を送信すると、アクセス制御サーバ３はユーザａの本人性を確認後、ＡＣＬ２０にＡＣＥ２１を追加するよう、ハブ４に依頼する。これにより、端末１ａとコンピュータユニット２ａの間にネットワークリンクが形成され、通信パケットが送受可能となる。この結果、端末１ａを操作するユーザａは、コンピュータユニット２ａが提供するターミナルサービスを受けられるようになる。

【００７２】

端末１ｂの場合も同様に、アクセス制御サーバ３が、ハブ４に対してＡＣＥ２２を追加するよう依頼し、端末１ｂとコンピュータユニット２ｂの間にネットワークリンクが形成され、端末１ｂを操作するユーザｂは、コンピュータユニット２ｂが提供するターミナルサービスを受けられるようになる。

【００７３】

ここで、アクセス制御サーバ３からユーザ認証を受けていない端末１ｃは、ＡＣＬ２０内の何れのＡＣＥとも合致しない。つまり端末１ｃとコンピュータユニット間には、ネットワークリンクが形成されていないため、他のユーザｃが端末１ｃを操作しても何れのコンピュータユニットにもアクセスできない。また、アクセス制御サーバ３のユーザ認証を受けた端末でも、特定以外のコンピュータユニットにはアクセスできない。例えば端末１ｂとコンピュータユニット２ｃの間にはネットワークリンクが形成されていないため、端末１ｂからコンピュータユニット２ｃにアクセスできない。さらにコンピュータユニットから他のコンピュータユニットへもアクセスできない。例えば、ユーザｂが端末１ｂからコンピュータユニット２ｂへターミナルサービス接続した後、コンピュータユニット２ｂからコンピュータユニット２ｃへのターミナルサービス接続を試みても、アクセスできない。

【００７４】

以上のように本実施例のアクセス制御サービスおよびアクセス制御サーバでは、ユーザ認証した端末と、そのユーザが利用する特定のコンピュータユニットの間にのみ、通信可能なネットワークリンクを設定する。どのユーザがどのコンピュータを利用可能であるかは、予めシステム管理者等が定め、アクセス制御サーバ内に登録しておく。このため、ユーザ認証されていない端末はもちろん、他のユーザにより認証された端末からも、正規ユーザのコンピュータユニットにアクセスできない。つまり、コンピュータユニットに対してターミナルサービス接続を試みても、ハブによりネットワークが遮断されているため、ログイン画面すら表示されず、ログインを試みることはできない。これにより、ブルートフォース攻撃や辞書攻撃、そしてアカウントロックアウト機能を悪用した嫌がらせ行為等のパスワード攻撃を排除でき、さらに、ポートスキャン攻撃やＤｏＳ攻撃等の不正アクセスからコンピュータユニットを防御する、安全なアクセス制御サービスを提供可能である。

【００７５】

なお、本実施例のアクセス制御サーバは、ユーザ認証された端末をそのユーザが操作中（ＰＣ業務中）の場合に限り、ネットワークリンクを設定する。操作中断時や操作終了時の場合はネットワークリンクを解除するため、離席時や帰宅時等にも、自分のコンピュータユニットが、他人からパスワード攻撃を受けることはない。また本実施例のアクセス制御サーバは、まず接続要求を送信したユーザを認証し、認証に成功した場合、そのユーザが、現在操作中の端末を認識してその端末を対象としたネットワークリンクを設定する。このため、操作する端末自体もしくは端末が接続されるネットワーク環境は固定されず、例えば、ユーザが外出先や自宅のＰＣもしくはネットワーク環境を利用する場合等、端末や環境の制限なくターミナルサービスを受けることができる。

【００７６】

周知技術によれば、システム管理者は、端末を接続するネットワークのＩＰアドレスを

全てハブのＡＣＬに手作業で設定する必要があり、大規模なネットワーク環境においては作業負荷が膨大である。また、端末のＩＰアドレスがハブのＡＣＬに登録されたものであっても、その端末を操作しているのが正当なユーザとは限らない。さらに、正当なユーザがコンピュータユニットを利用していない間、端末のＩＰアドレス詐称等により、他のユーザがそのコンピュータを不正アクセスできてしまう。本実施例によれば、アクセス制御サーバが端末のＩＰアドレスを検出し、ハブのＡＣＬに自動的に追加するため、システムの保守作業が容易である。また、本実施例のネットワークリンクは、本人性が検証されたユーザに対してのみ提供され、さらに、コンピュータユニットを利用している間のみ提供されるものであり、他のユーザによる不正アクセスからコンピュータユニットを防御可能である。

【００７７】

上記述べた本実施例は一例であり、以下に述べる各種変形例が可能である。

【００７８】

本実施例のアクセス制御サービスでは、アクセス制御サーバ３とハブ４とを分離して構成している。このため、汎用のハブを採用することができる。これに対し、図１０に示すように、アクセス制御サーバをハブと一体化して、アクセス制御サーバ２３として構成したアクセス制御サービスも可能である。

【００７９】

本実施例のアクセス制御サーバは、ハブの管理用ポートを介してＡＣＥの追加や削除を依頼しているが、管理用ポートを備えていない等、ハブの装置仕様によっては、ネットワーク５を介してＡＣＥの追加や削除を依頼しても良い。

【００８０】

本実施例のアクセス制御サーバは、通信パケットのソース及びデスティネーションアドレスを用いて端末とコンピュータユニットを特定しているが、他の識別情報を用いてこれらの装置を特定しても良い。

【００８１】

本実施例においては、ネットワークリンクの設定を、ハブの中継可否の制御機能により実現した場合を例示しているが、他の手段を用いても実現可能である。例えば、ＶＬＡＮ（Ｖｉｒｔｕａｌ　ＬＡＮ）等の特定のコンピュータ間にのみ通信を限定できるような機能がハブに搭載されていれば、それを利用して実現しても良い。また、コンピュータユニットにファイアウォール機能が搭載されているならば、ハブを利用しなくても、相応の効果が得られる。コンピュータユニットのファイアウォール機能を利用する場合、アクセス制御サーバが、ハブに対して実施しているＡＣＥの追加、削除処理を、コンピュータユニットのファイアウォール機能に対して行うように置き換え、指定したソースアドレスからの通信パケットを受け入れるよう、ファイアウォールに依頼すれば良い。

【００８２】

尚、本実施例においては、端末のアドレスをソースアドレス、コンピュータユニットのアドレスをデスティネーションアドレスとするＡＣＥにより形成するネットワークリンクを説明した。これにより、ユーザ認証された端末から特定のコンピュータユニットへの通信パケットのみがハブ４により中継される。しかし実際は、逆方向、つまり特定のコンピュータユニットからユーザ認証された端末へ通信パケットが送信される場合がある。これに対しては、図６のＳ６０５，Ｓ６０６において、図４に示すＡＣＥを生成、追加するのと同時に、逆方向のＡＣＥも生成、追加すれば良い。具体的には、第１パートが「ｐｅｒｍｉｔ」、第２パートのソースアドレスがコンピュータユニットのアドレス、第３パートのデスティネーションアドレスが端末のアドレスであるＡＣＥである。両ＡＣＥの追加により、ユーザ認証された端末と特定のコンピュータユニットが双方向で通信可能なネットワークリンクを提供可能である。

【００８３】

本実施例においては、通信パケットのソースアドレスを用いて端末を特定し、ネットワークリンクを提供しているが、端末とハブの間にプロキシーやゲートウェイが介在する場

合等、ハブが受信した通信パケットのソースアドレスが、端末によらず全て同じになってしまうケースも考えられる。このようなケースでは、他の手段により端末を特定すれば良い。例えば、ソースアドレスと通信ポート番号の組み合わせにより、端末を特定することもできる。一般のハブ４においては、ＡＣＥの第２もしくは第３パートとして、アドレスだけでなく、通信ポート番号も組み合わせた指定が可能である。この場合には、図４に示したＡＣＥの第２パートに、ソースアドレスと通信ポート番号を記述すれば良い。

【００８４】

本実施例のアクセス制御サーバは、図４に示したような通信パケットのソースアドレスとデスティネーションアドレスにより、特定の端末と特定のコンピュータユニット間にネットワークリンクを提供しており、特定の端末と特定のコンピュータユニット間ではあらゆる通信パケットを送受可能である。しかし、セキュリティ等を考慮し、端末とコンピュータユニット間の通信パケットを特定のプロトコルのみに限定させたいというニーズも考えられる。このようなニーズを満足するには、図４に示したＡＣＥの第３パートに、デスティネーションアドレスと利用を許可する通信プロトコルのポート番号を組み合わせた値を設定すれば良い。例えばターミナルサービスのみに限定する場合は、ターミナルサービスプロトコルのポート番号（例えば３３８９）を設定する。この場合のネットワークリンクは、ターミナルサービス専用のネットワークリンクと言える。さらに、双方向のネットワークリンクを提供する場合は、逆方向のＡＣＥも生成して追加すれば良い。具体的には、第１パートが「ｐｅｒｍｉｔ」、第２パートがコンピュータユニットのアドレスとターミナルサービスプロトコルのポート番号を組み合わせた値、第３パートが端末のアドレスであるＡＣＥである。もしくは、第１パートが「ｐｅｒｍｉｔ」、第２パートがコンピュータユニットのアドレス、第３パートが端末のアドレスとターミナルサービス制御プログラムのポート番号を組み合わせた値であるＡＣＥでも良い。その場合には、アクセス制御サーバは、端末のターミナルサービス制御プログラムのポート番号を検出するものとする。

【００８５】

本実施例のアクセス制御サーバは、特定の端末と特定のコンピュータユニット間にネットワークリンクを提供しており、特定の端末以外は特定のコンピュータユニットにネットワーク経由でアクセスできない。しかし、コンピュータユニットで、Ｗｅｂサーバ等、他の通信プロトコルを受け入れたいケースも考えられる。

【００８６】

また、今日のＰＣ業務には、Ｗｅｂやメール等、他のコンピュータと通信するアプリケーションプログラムが欠かせない。本実施例においてはターミナルサービスへの適用を例示したが、この場合、各コンピュータユニットが他のコンピュータと通信する必要がある。これらの他のコンピュータがネットワーク５上に接続されている場合には、ネットワークリンクがアプリケーションプログラムの通信を妨害することのないようにしなければならない。

【００８７】

上記二つのケースに対応するには、アクセス制御サーバが追加するＡＣＥより後の検索順位として、第１パートが「ｄｅｎｙ」、第２パートが「空き」、第３パートが各コンピュータユニットのアドレス（もしくは「空き」）とターミナルサービスを提供する通信ポート番号を組み合わせたＡＣＥを追加する。それと共に、第１パートが「ｐｅｒｍｉｔ」のＡＣＥをデフォルトＡＣＥとして登録すれば良い。これらのＡＣＥは、システム管理者等が、ハブ４に対して予め設定する。これにより、特定の端末以外はターミナルサービスに接続できず、つまりログインを試みることはできないという不正アクセス防御の機能を確保しつつ、コンピュータユニットと他のコンピュータとのターミナルサービス以外の通信を受け入れることができる。

【００８８】

しかしながら上記のように設定した場合、コンピュータユニットを起動するマジックパケットも通過させることになり、コンピュータユニットのＭＡＣアドレスさえ判明すれば

、何れの端末からもコンピュータユニットを不正に起動できる恐れがあり、さらなる対応が必要となる。

【００８９】

図１５は、上記ケースに対応するために、前記図５の通信シーケンスを変形した例である。ここでは、ＡＣＥによるパケットのフィルタリングだけでなく、コンピュータユニットが接続されたハブのポートを開閉制御するようにしている。

【００９０】

端末１からの接続要求（Ｆ７０１）を受信したアクセス制御サーバ３は、ユーザの本人性を確認し、コンピュータユニット２を起動した後（Ｆ７０２）、ＡＣＥを追加するとともに（Ｆ７０４）、そのコンピュータユニット２が接続されたポートを開くよう（Ｆ７０５）、ハブ４に依頼する。また、端末１から終了要求（Ｆ７１５）を受信した場合、コンピュータユニット２をシャットダウンした後（Ｆ７１６）、追加したＡＣＥを削除するとともに（Ｆ７１８）、Ｆ７０５において開いたポートを閉じるよう（Ｆ７１９）、ハブ４に依頼する。ハブ４へのポート開閉は、例えばポートの番号で指示する。このため、各コンピュータユニット管理テーブルには、コンピュータユニットが接続されたポートの番号を記憶する領域を設ける。これにより、コンピュータユニット２の不正起動を防止することが可能である。

【００９１】

また、ユーザがＰＣ業務を中断している間、コンピュータユニット２が他の機器と通信する必要がなければ、ポートを閉じるように制御を変更しても良い。例えば、端末１からの中断要求（Ｆ７０８）を受信したアクセス制御サーバ３は、Ｆ７０４において追加したＡＣＥを削除した後（Ｆ７０９）、Ｆ７０５において開いたポートを閉じるようにハブ４に依頼する。端末１から再び接続要求（Ｆ７１１）を受信した場合、ＡＣＥを追加した後（Ｆ７１２）、閉じたポートを開くようにハブ４に依頼する。また、Ｆ７０９の「ＡＣＥ削除」を「ポート閉」、Ｆ７１２の「ＡＣＥ追加」を「ポート開」に置き換えても同様の効果が得られる。

【００９２】

本実施例においては、Ｐ２Ｐタイプのターミナルサービスを例に説明しているが、本実施例はＳＢＣタイプのターミナルサービスにも適応可能である。認証されていないユーザは、ＳＢＣタイプのターミナルサービスに接続を試みることすらできない。また、ＳＢＣタイプのターミナルサービスは、複数のユーザが１台のコンピュータユニットを共有するものである。１台のコンピュータユニットを共有可能なユーザとして、数十名程度のグループを割り当てるのが適当である。これにより、あるグループに属さないユーザは、特定のコンピュータユニットにはアクセスできない。また、通信データをユーザ毎に識別することで、ユーザ間のプライバシーを保護することができる。本実施例は、さらに、複数のユーザと特定の複数台のコンピュータユニットとの間でのサービス形態に発展させることも可能である。その際、アクセス先のコンピュータユニットを指定するための情報を追加すれば良い。

【００９３】

尚、既知のターミナルサービスは、端末とリモートコンピュータがネットワークを介してデータを授受するため、ネットワーク障害等によりデータを授受できない状態に陥ると、ターミナルサービスの通信セッションは切断される。ユーザは、ネットワークが復旧した後、利用していたリモートコンピュータに対して、再度ターミナルサービス接続することにより、ＰＣ業務を再開可能である。しかし、ネットワーク障害によりターミナルサービスが利用できない状況になった際、ユーザが本実施例の中断操作を行うことなく離席すると、ネットワークの復旧後、そのユーザが使用していた端末を用いて、他のユーザによりコンピュータユニットへのパスワード攻撃を受ける恐れがある。

【００９４】

図１６は、上記ケースに対応するために、前記図５の通信シーケンスを変形した例である。ここでは、端末とコンピュータユニット間の通信が不可能となった時点で、形成して

いたネットワークリンクを解除するものである。

【００９５】

各コンピュータユニット２上では、端末１との通信状態を監視するエージェントを稼働させる。エージェントは、端末１との通信が途絶えたことを検出した場合、その旨をアクセス制御サーバ３へ通知する（Ｆ６０７）。切断通知を受信したアクセス制御サーバ３は、図７に示した手順と同様、Ｆ６０４において追加設定したＡＣＥを削除する要求（Ｆ６０８）をハブ４に依頼し、端末１とコンピュータユニット２間に設定されていたネットワークリンクを解除する。これにより、ネットワーク復旧後のコンピュータユニットへの不正アクセスを防止可能である。

【００９６】

また、一般のターミナルサービスクライアント（図１３のターミナルサービス制御プログラム４９）において、ユーザは、リモートＰＣとのターミナルサービス通信セッションを切断することが可能である。本実施例においては、ユーザが端末１から離れる際、端末１のコンピュータユニット制御プログラム４７を操作し、アクセス制御サーバ３に対して中断要求を送信するものとしている。しかし、中断要求の前に、ユーザがターミナルサービス通信セッションを切断した場合、ネットワークリンクは形成されたままとなる。他の端末がコンピュータユニットにアクセスできるわけではないが、潜在的な不正アクセスに備え、ターミナルサービスを利用していない間はネットワークリンクを解除した方が安全である。これに対応するには、端末１のコンピュータユニット制御プログラム４７がリモートＰＣとのターミナルサービス通信セッションを監視し、切断を検知した場合、アクセス制御サーバ３に対して中断要求を自動送信する処理を追加すれば良い。

【００９７】

本実施例においては、コンピュータユニットに対する不正アクセスをハブで遮断している。ハブで遮断した不正アクセスに関する情報（端末のＩＰアドレス、通信パケット、プロトコル等）をシステム管理者に通知するようにしておけば、システム管理者は不正アクセスに対する対策を即座に実施でき、さらに安全なシステムを構築可能である。システム管理者への不正アクセス通知は、ハブの機能を利用しても良いし、ハブが備えていなければ、アクセス制御サーバがハブのログ等から情報を抽出し、それをシステム管理者に通知する手段を追加しても良い。

【００９８】

本実施例のアクセス制御サーバは、ユーザ認証手段としてＴＬＳを利用しているが、本人性を検証可能であれば、他の手段を用いても良い。例えば、指紋や虹彩、指静脈等、人間固有の特徴を利用する生体認証なども有効である。

【００９９】

本実施例におけるコンピュータユニットは、ＣＰＵ、ハードディスク、ＬＡＮカード等が筐体内に搭載された、汎用のＰＣ等である。しかし、本実施例におけるコンピュータユニットの役割はターミナルサービスの提供であり、筐体は必ずしも必要ではなく、ＣＰＵ、ハードディスク、ＬＡＮカード等が実装された基板だけでも良い。このような基板は、一般にブレードコンピュータと称される。ブレードコンピュータは様々なシステムに導入され始めており、本実施例のコンピュータユニットとして適用することも可能である。

【０１００】

本実施例においては、コンピュータユニットの起動をマジックパケットにより実現する場合を例示しているが、他の手段を用いても実現可能である。例えば、コンピュータユニットがＩＰＭＩ（Ｉｎｔｅｌｌｉｇｅｎｔ Ｐｌａｔｆｏｒｍ Ｍａｎａｇｅｍｅｎｔ Ｉｎｔｅｒｆａｃｅ）をサポートしていれば、それを利用しても実現できる。

【０１０１】

尚、本実施例のアクセス制御サーバは、端末からの接続要求を受けてコンピュータユニットの稼働状況を確認し、未起動の場合は起動し、起動が完了した後端末へターミナルサービスへの接続準備完了を通知する。これを受けて端末は、コンピュータユニットへのターミナルサービス接続を開始する。しかし、通常のコンピュータユニットの起動には数十

秒から数分かかるため、コンピュータユニットが起動中であることを、ユーザに知らせるほうが好ましい。これに対応するには、コンピュータユニットの起動（図６のＳ６０４）の前に、コンピュータユニットが起動中であることを端末１に対して通知する処理を追加すれば良い。端末１は、その通知を受けた際、「ただいまＰＣを起動中です。しばらくお待ち下さい。」等のメッセージをディスプレイ４２に表示する。

【０１０２】

本実施例において、各コンピュータユニットのＩＰアドレスは、管理者が予め管理ＤＢに登録するものとしており、これは、各コンピュータユニットに対して固定のＩＰアドレスを割り当てる運用形態を想定している。一方、各コンピュータユニットに対してＩＰアドレスを動的に割り当てる運用形態も考えられる。この形態では、一般にＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）サーバが利用される。本実施例を動的なＩＰアドレスに対応させるには、ＩＰアドレスを通知するプログラムを各コンピュータユニットに搭載すれば良い。そのプログラムは、コンピュータユニットの起動毎に実行され、ＤＨＣＰサーバにより割り当てられたＩＰアドレスを検出して、アクセス制御サーバに通知する。通知を受けたアクセス制御サーバは、管理ＤＢのＩＰアドレス領域に値を格納し、以降の処理において参照する。

【０１０３】

なお、本実施例においては、アクセス制御サーバが１台の構成を説明したが、無停止運転等の高信頼なシステムを構築するには、アクセス制御サーバを２台以上に冗長化すれば良い。そして、稼働中のサーバが装置の障害等により不能となった場合、他のサーバに切り換え、サービスを継続できるようにすれば良い。また、ユーザ数が多い大規模システム等、１台のアクセス制御サーバでは処理能力が不足する場合は、複数台のアクセス制御サーバを稼働させ、並列運用すれば良い。この場合、各端末は負荷の最も少ないアクセス制御サーバに対して要求を送信するか、もしくはアクセス制御サーバとネットワークの間に負荷分散装置を設置することにより、アクセス制御サーバの負荷を平準化することが可能である。

【実施例２】

【０１０４】

図１１は、本発明によるアクセス制御サービスを実行するコンピュータシステムの第２の実施例を示す構成図である。本実施例は、各コンピュータユニットが大容量のハードディスクを共有する構成である。第１の実施例との異なる点は、各ユーザは特定のコンピュータユニットを専有するのではなく、ハードディスクに、専有の領域を設けたものである。本実施例のシステムでは、ユーザの使用するコンピュータユニットを共有しているので、少ない台数のコンピュータユニットで効率的な運用を可能とするものである。

【０１０５】

１台以上（ここでは２台）のコンピュータユニット２（２ａ、２ｂ）を大容量のハードディスク２４に接続する。ハードディスク２４は、登録したユーザ（ここでは３人、ａ、ｂ、ｃ）毎に領域を分割し、各領域（２４ａ、２４ｂ、２４ｃ）には、各ユーザが利用するＯＳや業務に使用するアプリケーション等のソフトウェア及びデータを格納する。ユーザ（例えばユーザａ）が利用を始める際は、ハードディスク２４上のユーザ領域（２４ａ）をマウントし、そのユーザ領域に格納されたＯＳによりコンピュータユニット２を起動する。その際に使用するコンピュータユニット２は、空き状態の何れかのコンピュータユニット２を動的に割り当てる。本実施例の場合は、コンピュータユニット２とハードディスク２４を分離しているため、利用するユーザに対して、コンピュータユニット２を静的に割り当てる必要がない。

【０１０６】

図１２は、本実施例におけるアクセス制御サーバ３が有する管理データベース３０の情報の一例を示す図である。ユーザ管理テーブル３１のユーザエントリに、ハードディスク２４上のユーザ領域を示すマウント情報３７と、コンピュータユニット管理テーブル３２のコンピュータユニットエントリに、コンピュータユニット２のステータス情報（稼動／

空き）４０を加える。ユーザエントリのマウント情報３７は、ユーザ登録時等に、システム管理者が情報を登録する。コンピュータユニットエントリのステータス情報４０は、システム導入時等に「空き」に初期化される。一方、ユーザエントリ内のコンピュータユニットＩＤ３４は、アクセス制御サーバ３が値を設定するため、システム管理者が事前登録する必要はない。本実施例では、使用するコンピュータユニットの台数を、ユーザ数以下の台数としてサービスを行うことができる。あるいは、使用するコンピュータユニットの台数は、ネットワークに接続される端末１の台数以下となる。

【０１０７】

本実施例のアクセス制御サービスの接続処理フローについて説明する。なお、前記第１の実施例と共通の部分については、前記図面（図５、図６）も参照して説明する。アクセス制御サーバ３はユーザ認証（Ｓ６０１）の結果、正規のユーザであることを検証すると、コンピュータユニット管理部８は、ハードディスク２４のマウントとコンピュータユニット２の起動（Ｓ６０４）を行う。

【０１０８】

まず、コンピュータユニット管理テーブル３２を検索し、ステータス情報４０として「空き」が登録されたコンピュータユニットエントリを探し、そのエントリのステータス情報４０を「稼動」に変更して、今回使用するコンピュータユニットとして決定する。次に、ユーザ管理テーブル３１を検索し、認証したユーザが登録されているユーザエントリを探し、そこに登録されたマウント情報３７の値を取り出す。そして、上記使用するコンピュータユニット２に対して、上記マウント情報３７に基づきハードディスク２４をマウントするよう指示する。そして、ＭＡＣアドレス３９に登録された値を取り出しマジックパケット（Ｆ５０２）を組み立て、上記コンピュータユニット２へ送信して起動させる。

【０１０９】

コンピュータユニット管理部８は起動完了通知（Ｆ５０３）を受けると、コンピュータユニットエントリ内のコンピュータユニットＩＤ３８に登録された値を、ユーザエントリ内のコンピュータユニットＩＤ３４に登録した後、ＩＰアドレス３５に登録された値を取り出して、通信制御部６へ渡す。

【０１１０】

通信制御部６は、受信した通信パケットから接続を要求した端末１のソースアドレスを抽出し、コンピュータユニット管理部８から通知された使用するコンピュータユニット２のＩＰアドレス３５と共にＡＣＥ設定部（リンク設定部）９に渡す。ＡＣＥ設定部９はＡＣＥを生成し（Ｓ６０５）、ＡＣＥを追加設定する要求（Ｆ５０４）をハブ４に依頼する（Ｓ６０６）。ＡＣＥの構成は、前記実施例１と同様である。これにより、接続を要求した端末１とコンピュータユニット２間にネットワークリンクが形成される。その結果、ユーザは、ログイン実行後、ハードディスクの特定のユーザ領域をマウントしたコンピュータユニット２からターミナルサービスの提供を受けて、ＰＣ業務を行うことができる。ＰＣ業務の中断、終了の処理も、実施例１と同様に行う。

【０１１１】

以上のように本実施例においては、ユーザ認証した端末と、そのユーザが利用する特定のコンピュータユニットの間にのみ、通信可能なネットワークリンクを設定する。これにより、パスワード攻撃を排除でき、安全なアクセス制御サービスを提供可能である。

【０１１２】

さらに本実施例では、各コンピュータユニットは大容量のハードディスクを共有するため、必ずしも個々のコンピュータユニットがハードディスクを備える必要はない。また、利用するユーザに対して、空き状態のコンピュータユニットを動的に割り当てるため、コンピュータリソースを有効活用可能である。すなわち、コンピュータユニットの台数は、同時に利用するユーザ数だけあれば良い。また一部のコンピュータユニットに障害が発生しても、すぐに代用のコンピュータユニットを割り当てることができるので、システム規模の縮小と信頼性の向上を図ることができる。

【０１１３】

本発明の他の実施例として、上記第１、第２の実施例を組み合わせた形態も可能である。すなわち、各コンピュータユニットは大容量のハードディスクを共有し、各ユーザは、特定のコンピュータユニットと、ハードディスク内の特定の領域を専有するものである。

【０１１４】

また本実施例においては、接続を要求したユーザに対して空き状態の何れかのコンピュータユニットを動的に割り当てている。しかし、例えば故障したコンピュータユニットやネットワークの障害により通信不可能なコンピュータユニットは、空き状態であっても、割り当てる対象から除外すべきである。ネットワーク障害の要因としては、ハブ自体もしくはハブ内の一つのポートの故障や、ハブとコンピュータユニットを接続するケーブルの断線や外れ等が挙げられる。さらに、システム管理者の判断により、あるコンピュータユニットを割り当て対象から除外できるようにしても良い。このようにコンピュータユニットを割り当てることにより、ユーザに対して快適に利用可能なコンピュータユニットを提供できる。

【実施例３】

【０１１５】

図１７は、本発明によるアクセス制御サービスを実行するコンピュータシステムの第３の実施例を示す構成図である。本実施例は、各端末がネットワークを介して大容量のハードディスク（記憶装置）を共有する構成である。第２の実施例（図１１）と同様、ハードディスクは、登録したユーザ毎に領域を分割し、各領域には、各ユーザが利用するＯＳや業務に使用するアプリケーション等のソフトウェア及びデータを格納している。第２の実施例においては、各コンピュータユニットがハードディスクを共有し、端末はターミナルサービスを用いてコンピュータユニットに接続する構成であったのに対し、本実施例では、コンピュータユニットを廃止し、各端末がハードディスクを共有する構成である。つまり、本実施例においては、ＯＳやアプリケーション等のソフトウェア及びデータはリモートのハードディスクに格納されるが、ソフトウェアを実行するのは端末のＣＰＵであって、ターミナルサービスを利用しないシステムである。本実施例の構成では、第１もしくは第２の実施例のコンピュータユニットが不要となり、システムの導入コストを低減可能である。反面、ハードディスクに対するデータの読み込みや書き込みが全てネットワーク５を介して行われるため、各端末からハードディスクへのアクセス頻度が多量の場合は、高速なネットワークが必要となる。

【０１１６】

図１８は、本実施例におけるアクセス制御サーバ３が有する管理データベース５１の情報の一例を示す図である。ユーザ管理テーブル５２の各ユーザエントリに記憶する情報は、そのユーザを一意に識別するユーザＩＤ５３、ハードディスク２４上のユーザ領域のステータス（稼動状況、接続／中断／終了）５４、ハードディスク２４上のユーザ領域を示すマウント情報５５などである。

【０１１７】

図１９は、本実施例における各機器間での一連の通信シーケンスを示す図である。

【０１１８】

ユーザは端末１を操作し、アクセス制御サーバ３に対して接続要求（Ｆ８０１）を送信する。接続要求を受信したアクセス制御サーバ３はユーザ認証を実施し、ユーザの本人性を検証できた場合には、ハブ４に対してＡＣＥの追加を依頼する（Ｆ８０２）。ＡＣＥの構成は、具体的には、第１パートが「ｐｅｒｍｉｔ」、第２パートが端末のＩＰアドレス、第３パートがハードディスクのＩＰアドレスである。尚、ハブ４に接続される機器が単一のハードディスク２４である場合、第３パートは「空き」でも良い。次にアクセス制御サーバ３は、接続要求を発行したユーザのユーザエントリを探し、ステータス５４を変更するとともに、マウント情報５５の値を取り出し、端末１へ通知する（Ｆ８０３）。端末１は、アクセス制御サーバ３から通知されたユーザ領域を示すマウント情報を用いて、ハードディスク２４に対してマウントを要求する（Ｆ８０４）。マウントの完了後、端末１は、ハードディスクに格納されたＯＳを読み込んで起動する。以後ユーザは、リモートの

ハードディスク２４のユーザ専有領域に対してアクセスして、アプリケーションの実行、データの読み出し／書き込み等の処理を実行する。

【０１１９】

ユーザは、ＰＣ業務を終了する際、端末１を操作し、まずハードディスク２４に対してマウントの解除を要求し（Ｆ８０５）、次にアクセス制御サーバ３に対して終了要求（Ｆ８０６）を送信する。終了要求を受信したアクセス制御サーバ３は、ハブ４に対してＡＣＥの削除を依頼し（Ｆ８０７）、完了した後、端末１へ終了完了を通知する（Ｆ８０８）。

【０１２０】

以上のように本実施例のアクセス制御サービスおよびアクセス制御サーバによれば、ユーザ認証した端末にのみ、共有するハードディスク上のユーザ専有領域と通信可能なネットワークリンクを設定する。ユーザ認証されていない端末は、ハードディスクへのアクセスを、ネットワークレベルで遮断されているため、各ユーザのデータを安全に保護することができる。

【０１２１】

本実施例においては、各端末が単一のハードディスクを共有するケースを例示した。しかし、ユーザ数やユーザ毎に割り当てるディスク領域等によっては、複数のハードディスクを設置することも可能である。例えばユーザ数が５００名で、各ユーザに２０ギガバイトの領域を割り当てる場合、１テラバイトの領域を備えるハードディスクを１０台設置し、ユーザにより使い分ける必要がある。これに対応するには、マウント情報５５に、そのユーザが使用するハードディスクのＩＰアドレスとユーザ領域を示す情報を登録し、ユーザ認証した端末とそのユーザが使用するハードディスクとの間にネットワークリンクを形成すれば良い。

【図面の簡単な説明】

【０１２２】

【図１】本発明によるアクセス制御サービスを実行するコンピュータシステムの第１の実施例を示す構成図。

【図２】図１におけるアクセス制御サーバ３の論理構成の一例を示す図。

【図３】図２における管理ＤＢ１０の記憶する情報の内容の一例を示す図。

【図４】図２のアクセス制御サーバ３が設定する中継可否情報（ＡＣＥ）の一例を示す図。

【図５】図１における機器間の通信シーケンスの一例を示す図。

【図６】接続処理のフローチャートの一例を示す図。

【図７】中断処理のフローチャートの一例を示す図。

【図８】終了処理のフローチャートの一例を示す図。

【図９】図１におけるアクセス制御機能を説明する図。

【図１０】図１の実施例の一変形例を示す構成図。

【図１１】本発明によるアクセス制御サービスを実行するコンピュータシステムの第２の実施例を示す構成図。

【図１２】図１１において管理ＤＢ３０の記憶する情報の内容の一例を示す図。

【図１３】図１における端末１の内部構成の一例を示す図。

【図１４】図１におけるアクセス制御サーバ３の内部構成の一例を示す図。

【図１５】図５の通信シーケンスの一変形例を示す図。

【図１６】図５の通信シーケンスの一変形例を示す図。

【図１７】本発明によるアクセス制御サービスを実行するコンピュータシステムの第３の実施例を示す構成図。

【図１８】図１７において管理ＤＢ５１の記憶する情報の内容の一例を示す図。

【図１９】図１７における機器間の通信シーケンスの一例を示す図。

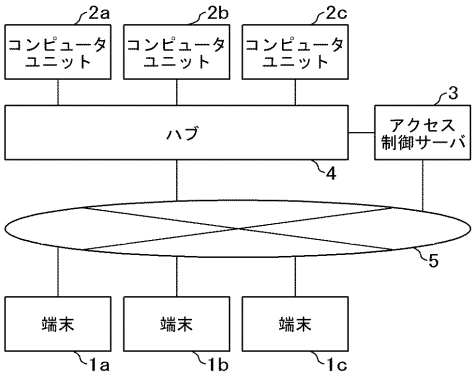
【符号の説明】

【０１２３】

１…端末、２…コンピュータユニット、３…アクセス制御サーバ、４…ハブ、５…ネットワーク、６…通信制御部、７…認証処理部、８…コンピュータユニット管理部、９…ＡＣＥ設定部、１０，３０，５１…管理ＤＢ、１１，３１，５２…ユーザ管理テーブル、１２，３２…コンピュータユニット管理テーブル、１９，２１，２２…ＡＣＥ、２４…ハードディスク、４０，５６…ＣＰＵ、４１，５７…メモリ、４２，５８…ディスプレイ、４３，５９…キーボード、４５…認証デバイス、４６，６１…二次記憶装置、４７…コンピュータユニット制御プログラム、４８…認証制御プログラム、４９…ターミナルサービス制御プログラム、５０，６４…通信制御プログラム、６２，６３…ネットワークＩ／Ｆ、６５…認証処理プログラム、６６…コンピュータユニット管理プログラム、６７…ＡＣＥ設定プログラム。

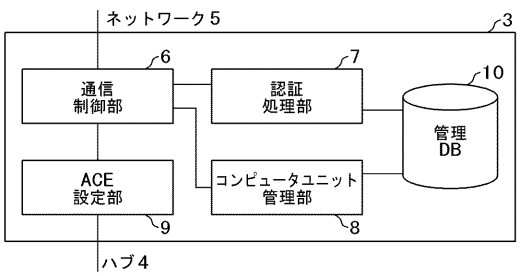
【図１】

図１



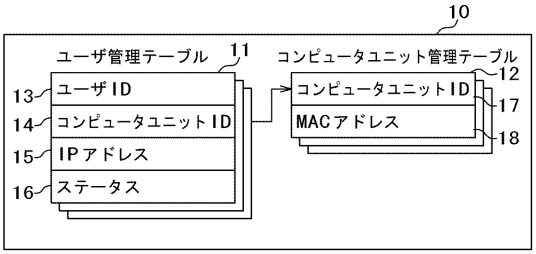
【図２】

図２



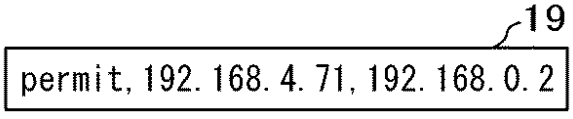
【図３】

図３



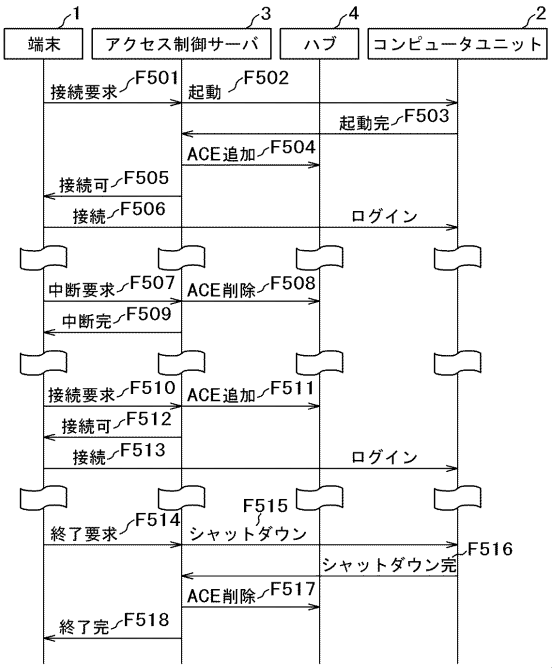
【図４】

図４



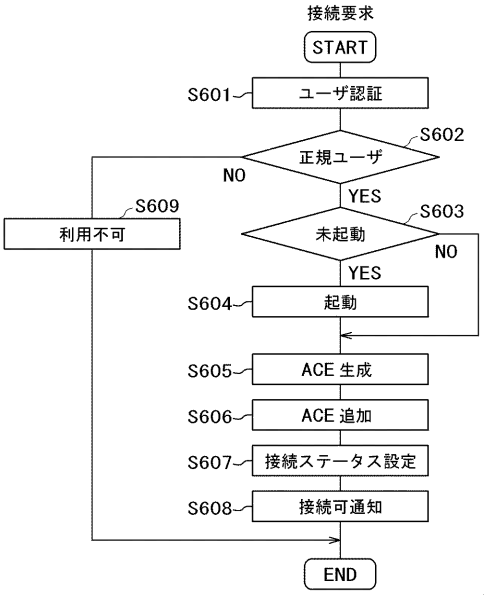
【図５】

図５



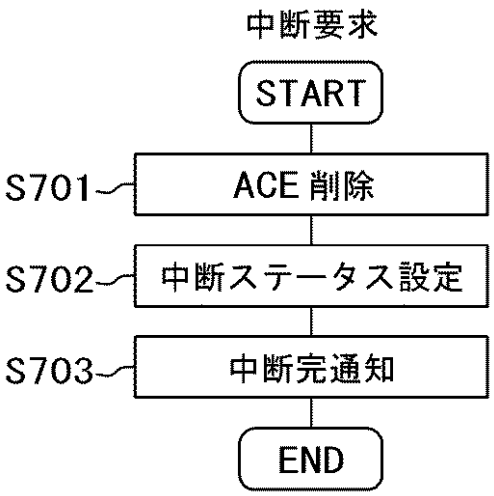
【図６】

図６



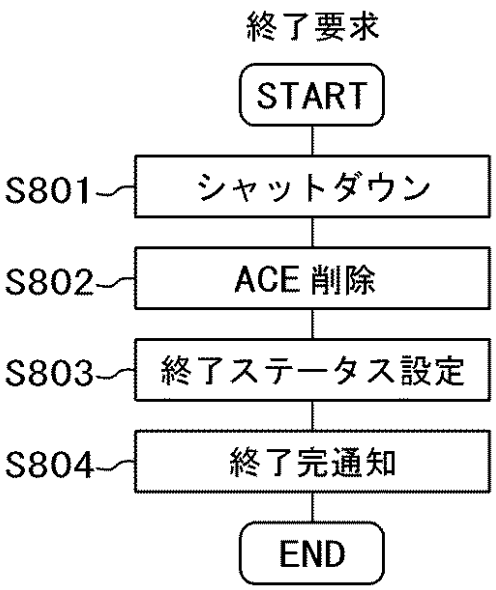
【図７】

図７



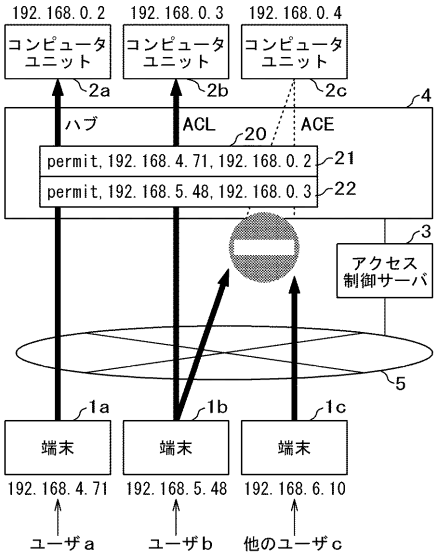
【図８】

図８



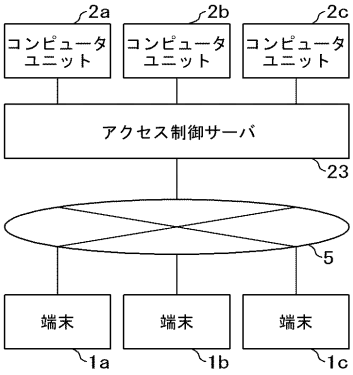
【図９】

図９



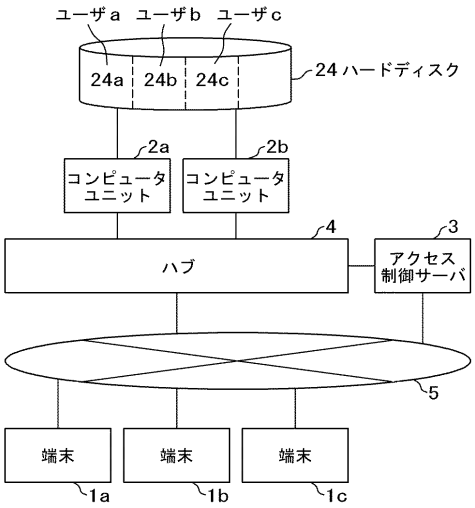
【図１０】

図１０



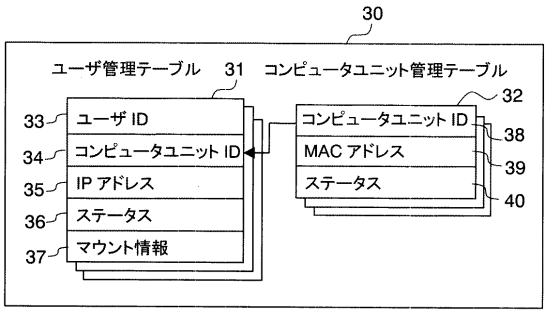
【図１１】

図１１



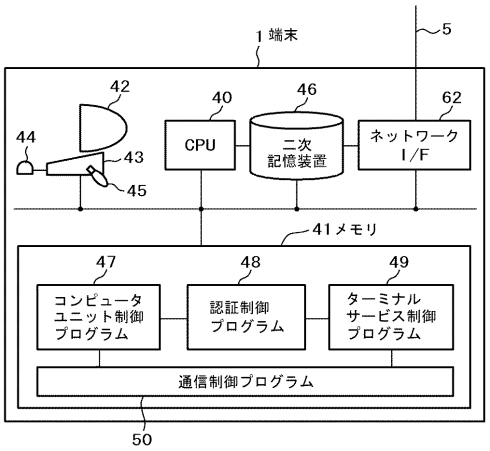
【図１２】

図１２



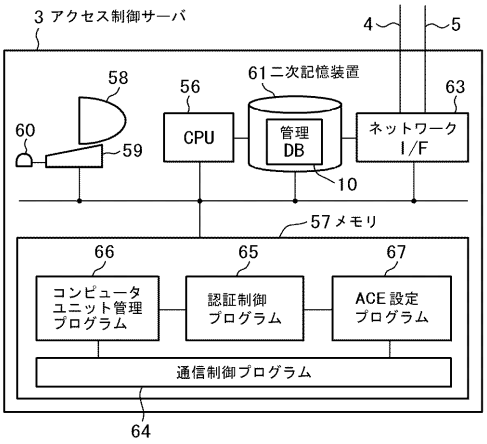
【図１３】

図１３



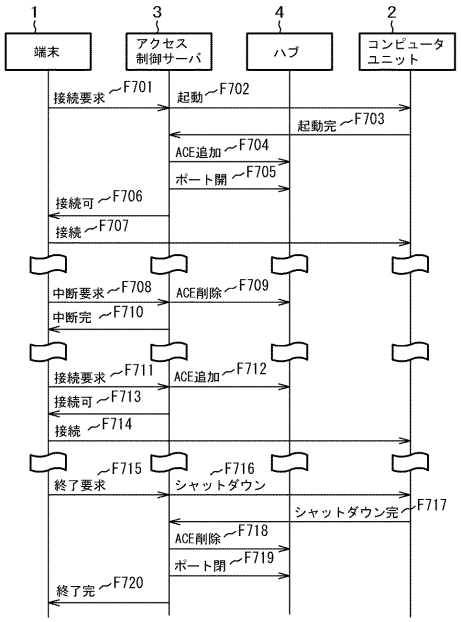
【図１４】

図１４



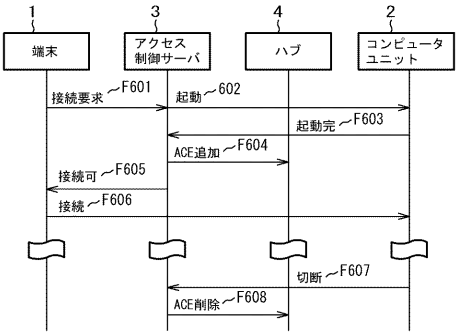
【図１５】

図１５



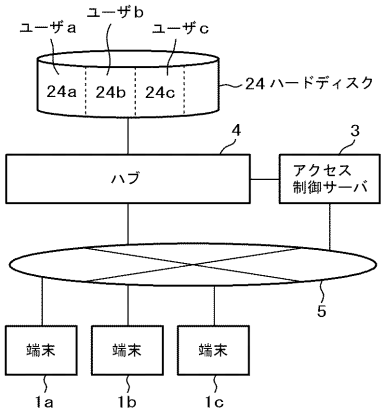
【図１６】

図１６



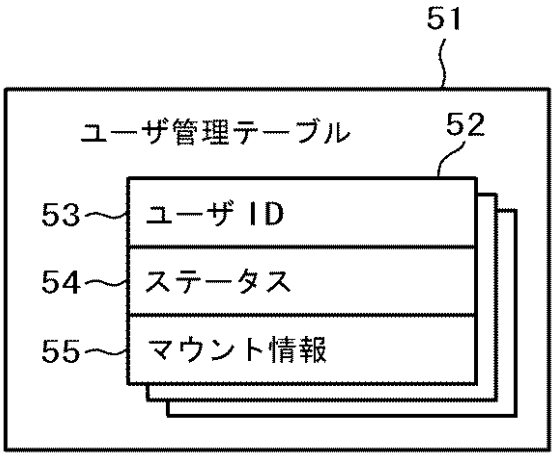
【図１７】

図１７



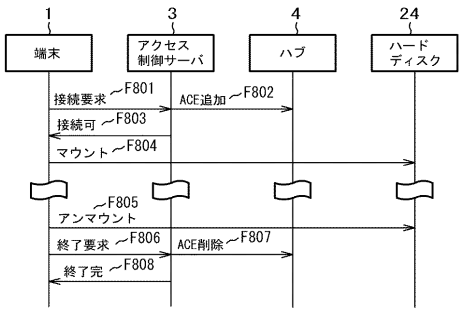
【図１８】

図１８



【図１９】

図１９



フロントページの続き

(72)発明者　小林　恵美子
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　宮脇　当為
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

審査官　小林　秀和

(56)参考文献　特開２００３－２４２１０９（ＪＰ，Ａ）
特開２００４－２５４０１０（ＪＰ，Ａ）
特開２００３－３１９０８３（ＪＰ，Ａ）
特開平１０－２２９４１８（ＪＰ，Ａ）
国際公開第２００５／０１５４１８（WO，Ａ１）
特開２００４－２４９９２５（ＪＰ，Ａ）
特開２００４－３５００９０（ＪＰ，Ａ）
特開２００２－０８４３０６（ＪＰ，Ａ）
特開２００３－０８５０５９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　１２／６６