(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2008-134902
(P2008-134902A)
(43)公開日　平成20年6月12日(2008.6.12)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330C	5B176
G09C 1/00	(2006.01)	G09C	1/00	640E	5B276
G06F 21/22	(2006.01)	G06F	9/06	660F	5B285
G06F 9/445	(2006.01)	G06F	9/06	640A	5J104

審査請求 有　請求項の数 9　ＯＬ　（全 13 頁）

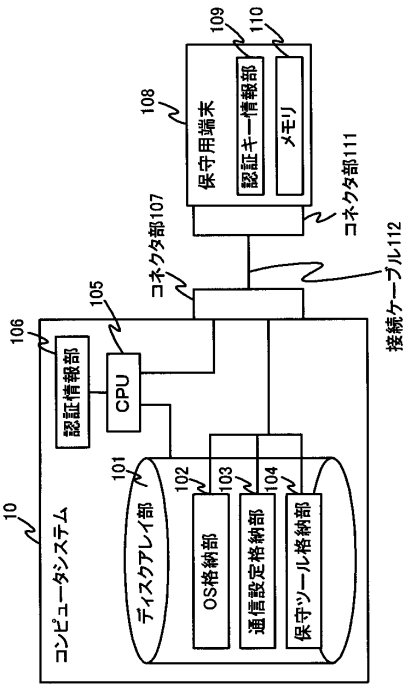
(21)出願番号　特願2006-321684 (P2006-321684)
(22)出願日　平成18年11月29日 (2006.11.29)

(71)出願人　000232140
ＮＥＣフィールディング株式会社
東京都港区三田１丁目４番２８号
(74)代理人　100087790
弁理士　尾関　伸介
(72)発明者　足立　英治
東京都港区三田一丁目４番２８号
ＮＥＣフィールディング株式会社内

Ｆターム(参考)　5B176 AA13 BB06
5B276 FB01
5B285 AA01 BA03 CA00 CB42 CB62 CB63 CB72 CB81
5J104 AA07 KA02 PA07

(54)【発明の名称】コンピュータシステム

(57)【要約】
【課題】不正な端末が保守用端末として接続された際に不正な接続が継続されることを防止可能なコンピュータシステムを提供する。
【解決手段】コンピュータシステム１０の保守専用の接続ポートであるコネクタ部１０７に保守用端末１０８が接続されたことを検知した際に、ＣＰＵ１０５は、保守用端末１０８の認証キー情報部１０９の認証キーを自動的に読み取り、認証情報部１０６に格納されている認証情報と照合して、正しい保守用端末１０８として認証可能か否かを判別し、認証に失敗した場合、コネクタ部１０７の接続ポートをロックし、たとえ、異なる端末が新たにコネクタ部１０７に接続されても、以降のアクセスを一切禁止する。コネクタ部１０７のロックの解除は、コンピュータシステム１０の管理者から解除指示が入力されるか、または、コンピュータシステム１０にあらかじめ設定されている解除条件が成立した場合に実施する。
【選択図】図１



【特許請求の範囲】
【請求項１】
保守用端末として、ハードディスクを備えていないシンクライアント型の端末を接続ポートに接続して保守されるコンピュータシステムにおいて、前記保守用端末を前記接続ポートに接続した際に実施される認証に失敗したことを検知した場合、前記接続ポートをロックし、以降のアクセスを一切禁止することを特徴とするコンピュータシステム。
【請求項２】
請求項１に記載のコンピュータシステムにおいて、前記接続ポートのロックは、当該コンピュータシステムが認証失敗を検知した際に、人手を介することなく自動的に実施されることを特徴とするコンピュータシステム。
【請求項３】
請求項１または２に記載のコンピュータシステムにおいて、前記接続ポートをロックするまでの間に、当該コンピュータシステムからは、前記接続ポートに接続した端末に対して、情報転送を一切実施しないことを特徴とするコンピュータシステム。
【請求項４】
請求項１ないし３のいずれかに記載のコンピュータシステムにおいて、前記接続ポートのロックは、当該コンピュータシステムの管理者からの解除指示、あるいは、当該コンピュータシステムにおいてあらかじめ設定された解除条件が成立した場合に限って、解除されることを特徴とするコンピュータシステム。
【請求項５】
請求項１ないし４のいずれかに記載のコンピュータシステムにおいて、前記保守用端末用のＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）、当該コンピュータシステムとの通信を行うために前記保守用端末に設定する通信設定情報、当該コンピュータシステムの保守を行うための保守ツールを、当該コンピュータシステム側にあらかじめ記憶し、前記保守用端末を前記接続ポートに接続した際に実施される認証が成功したことを検知した場合に、あらかじめ記憶されている前記ＯＳを、前記保守用端末側に自動的にダウンロードし、前記保守用端末が受信したＯＳの起動が終了したことを検知した時点で、前記通信設定情報を前記保守用端末側に自動的にダウンロードすることにより、前記保守用端末との間の通信動作を確立した後、前記保守用端末に対して前記保守ツールを転送することを特徴とするコンピュータシステム。
【請求項６】
請求項１ないし５のいずれかに記載のコンピュータシステムにおいて、前記保守用端末を前記接続ポートに接続した際に実施される認証動作が、前記保守用端末が前記接続ポートに接続されたことを検知した際に、前記保守用端末にあらかじめ格納されている認証キーを自動的に読み取って、当該コンピュータシステムにあらかじめ設定している認証情報と照合することによって実施されることを特徴とするコンピュータシステム。
【請求項７】
請求項１ないし６のいずれかに記載のコンピュータシステムにおいて、前記保守用端末を接続する前記接続ポートは、当該コンピュータシステムの保守専用の保守ポートであり、当該保守ポート以外からの保守指令は一切無視し、前記保守用端末から当該保守ポートを介して入力される保守指令のみを有効とすることを特徴とするコンピュータシステム。
【請求項８】
請求項１ないし７のいずれかに記載のコンピュータシステムにおいて、前記保守用端末を接続する前記接続ポートが、コンピュータシステムに対して外部機器を接続する際に用いられる任意の形式の入出力端子からなっていることを特徴とするコンピュータシステム。
【請求項９】
請求項８に記載のコンピュータシステムにおいて、前記保守用端末を接続する前記接続ポートが、ＬＡＮポートまたはＲＳ－２３２Ｃポートのいずれかからなっていることを特徴とするコンピュータシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータシステムに関し、特に、保守用端末接続時の認証処理を行うコンピュータシステムに関する。
【背景技術】
【０００２】
コンピュータシステムを保守するための保守用端末としては、一般に、各種の機能を有するＰＣを接続して使用している場合が多いが、ＰＣよりもより安価な端末を利用する例として、例えば、特許文献１の特開２００２－３７４３６１号公報「リモートコンソールシステム」のように、携帯電話などのリモート機器とハードディスクを備えていない簡易なシンクライアント端末とを用いている場合もある。該特許文献１においては、携帯電話と簡単な送受信部およびインタフェース変換機能のみを有するコンソールボックスとの組み合わせによって、安価に、遠隔地からコンピュータシステムをリモート保守することを可能にしようとしている。
【特許文献１】特開２００２－３７４３６１号公報（第２－３頁）
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、前記特許文献１の技術では、リモート保守する携帯電話やコンソールボックスの認証機能を備えたものではなく、コンピュータシステム内の情報が漏洩してしまうおそれが高く、さらに、保守用端末にはコンピュータシステムの保守機能が利用可能になる高い権限が付与されるために、コンピュータシステム（特に、各種のサービス機能を集中させているサーバ）の保守用としては、そのまま利用することができない。
【０００４】
また、従来のコンピュータシステムの保守用端末として、前述のように、開発コストを削減するために、各種機能を有し、ＯＳが内蔵された一般的なパーソナルコンピュータを使用する場合は、通常、認証上の配慮がなされていて、接続に当たって、パスワードなどを用いて、正しく認証された場合に、保守動作を可能としている。しかし、かかるＰＣを保守用端末として利用している場合には、該保守用端末を保守対象のコンピュータシステムの接続ポートに接続して、当該コンピュータシステムにログインするための認証処理を行った際に、認証処理に複数回失敗したとしても、通信を行う接続ポートは接続可能のままのオープンな状態が維持されているため、何度でも、認証用のパスワードを変更して認証処理を繰り返すことが可能になっており、当該コンピュータシステムに不正にアクセスしようとしている不正アクセス者に対する対策が不十分になってしまうという問題点があった。
【０００５】
さらに、正常な保守用端末として認証された場合であっても、コンピュータシステムを保守するために、使用者が、その都度、保守対象の当該コンピュータシステムと通信するために保守用端末の通信設定を変更したり、さらには、当該コンピュータシステムの保守を実行する保守ツールを保守用端末にインストールしたりすることが必要になるという問題点もあった。
【０００６】
本発明は、かかる事情に鑑みてなされたものであり、保守用端末側に認証キー情報を設け、保守対象のコンピュータシステムの接続ポートに接続した際に、自動的に認証キーを読み取り、認証に失敗した場合には、コンピュータシステムが当該接続ポートを自らロックすることにより、不正な接続が継続されることを防止するコンピュータシステムを提供することにある。
【０００７】
さらに、接続した端末が保守用端末としての認証に成功した場合に、はじめて、シンク

ライアント型の端末からなる保守用端末に対して、コンピュータシステムに内蔵されたディスクアレイ部から、保守用端末のＯＳ、保守用端末が当該コンピュータシステムと通信するための通信設定情報、さらには、当該コンピュータシステムを保守するための保守ツールを自動的にダウンロードすることにより、保守用端末の汎用性を維持しつつ、従来、保守用端末に対して人手で行っていた通信の設定や、保守ツールをインストールする不便さを解消するコンピュータシステムを提供することにある。

【課題を解決するための手段】

【０００８】

前述の課題を解決するため、本発明によるコンピュータシステムは、次のような特徴的な構成を採用している。

【０００９】

（１）保守用端末として、ハードディスクを備えていないシンクライアント型の端末を接続ポートに接続して保守されるコンピュータシステムにおいて、前記保守用端末を前記接続ポートに接続した際に実施される認証に失敗したことを検知した場合、前記接続ポートをロックし、以降のアクセスを一切禁止するコンピュータシステム。

（２）上記（１）のコンピュータシステムにおいて、前記接続ポートのロックは、当該コンピュータシステムが認証失敗を検知した際に、人手を介することなく自動的に実施されるコンピュータシステム。

（３）上記（１）または（２）のコンピュータシステムにおいて、前記接続ポートをロックするまでの間に、当該コンピュータシステムからは、前記接続ポートに接続した端末に対して、情報転送を一切実施しないコンピュータシステム。

（４）上記（１）ないし（３）のいずれかのコンピュータシステムにおいて、前記接続ポートのロックは、当該コンピュータシステムの管理者からの解除指示、あるいは、当該コンピュータシステムにおいてあらかじめ設定された解除条件が成立した場合に限って、解除されるコンピュータシステム。

（５）上記（１）ないし（４）のいずれかのコンピュータシステムにおいて、前記保守用端末用のＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）、当該コンピュータシステムとの通信を行うために前記保守用端末に設定する通信設定情報、当該コンピュータシステムの保守を行うための保守ツールを、当該コンピュータシステム側にあらかじめ記憶し、前記保守用端末を前記接続ポートに接続した際に実施される認証が成功したことを検知した場合に、あらかじめ記憶されている前記ＯＳを、前記保守用端末側に自動的にダウンロードし、前記保守用端末が受信したＯＳの起動が終了したことを検知した時点で、前記通信設定情報を前記保守用端末側に自動的にダウンロードすることにより、前記保守用端末との間の通信動作を確立した後、前記保守用端末に対して前記保守ツールを転送するコンピュータシステム。

（６）上記（１）ないし（５）のいずれかのコンピュータシステムにおいて、前記保守用端末を前記接続ポートに接続した際に実施される認証動作が、前記保守用端末が前記接続ポートに接続されたことを検知した際に、前記保守用端末にあらかじめ格納されている認証キーを自動的に読み取って、当該コンピュータシステムにあらかじめ設定している認証情報と照合することによって実施されるコンピュータシステム。

（７）上記（１）ないし（６）のいずれかのコンピュータシステムにおいて、前記保守用端末を接続する前記接続ポートは、当該コンピュータシステムの保守専用の保守ポートであり、当該保守ポート以外からの保守指令は一切無視し、前記保守用端末から当該保守ポートを介して入力される保守指令のみを有効とするコンピュータシステム。

（８）上記（１）ないし（７）のいずれかのコンピュータシステムにおいて、前記保守用端末を接続する前記接続ポートが、コンピュータシステムに対して外部機器を接続する際に用いられる任意の形式の入出力端子からなっているコンピュータシステム。

（９）上記（８）のコンピュータシステムにおいて、前記保守用端末を接続する前記接続ポートが、ＬＡＮポートまたはＲＳ－２３２Ｃポートのいずれかからなっているコンピュータシステム。

【発明の効果】
【００１０】
本発明のコンピュータシステムによれば、次のような効果を奏することができる。
【００１１】
（１）まず、コンピュータシステムを保守するための保守用端末としてシンクライアント型の端末を使用し、保守対象のコンピュータシステムに、保守用端末のＯＳ、保守用端末が当該コンピュータシステムと通信するための通信設定情報、さらには、当該コンピュータシステムを保守するための保守ツールをあらかじめ格納しておいて、コンピュータシステムに接続した際に保守用端末へ自動的に読み出す仕組みを有して構成し、さらに、保守対象のコンピュータシステムにログイン用の認証情報を設けるとともに、保守用端末側にコンピュータシステムにログインするための認証キーを設けることにより、認証に失敗する端末が接続された場合に、当該コンピュータシステム自体の動作によって、接続ポート（保守専用ポート）に接続されている端末との間の接続を切断するとともに、当該接続ポート（保守専用ポート）をロックすることにしているので、当該コンピュータシステムへの以降のアクセスを確実に抑止し、不正な接続が継続されることを確実に防止することができる。
【００１２】
（２）さらに、当該コンピュータシステムに接続した端末の認証に失敗した場合は、当該コンピュータシステムからＯＳを端末側にダウンロードする動作を含め、一切の情報を転送することなく、端末との接続を切断するので、端末側に情報が漏洩することを防止することができる。
【００１３】
（３）また、コンピュータシステムに接続した端末の認証に成功した場合に、はじめて、当該端末を当該コンピュータシステムの保守を行うための保守用端末として認識して、保守対象の当該コンピュータシステムから、保守用端末のＯＳ、保守用端末が当該コンピュータシステムと通信するための通信設定情報、さらには、当該コンピュータシステムを保守するための保守ツールを保守用端末側へ自動的に転送することを可能とすることにより、保守用端末の汎用性を維持しつつ、従来の保守用端末に対して人手で行っていた通信の設定や、保守ツールのインストール操作などの不便さを解消することができる。
【００１４】
（４）さらに、当該コンピュータシステムに接続するコネクタ部は、ＬＡＮポートに限ることなく、任意の外部インタフェースを用いることが可能であり、ＲＳ－２３２ＣやＷＡＮを介した通信インタフェースなど各種の外部インタフェースを適用することができ、拡張性を確保することができる。
【発明を実施するための最良の形態】
【００１５】
以下、本発明によるコンピュータシステムの好適実施形態例について添付図を参照して説明する。
【００１６】
（本発明の特徴）
まず、本発明の特徴について、その概要を説明する。本発明においては、ハードディスクを備えていないシンクライアント端末を保守用端末として使用し、コンピュータシステムを保守するための該保守用端末上で動作するＯＳ、コンピュータシステムとの間の通信のための通信設定情報、保守ツールを、当該コンピュータシステム側に格納し、保守用端末の接続時の認証が得られた時点で、当該コンピュータシステムから保守用端末側にダウンロードして、当該コンピュータシステムに対する保守動作を可能とする一方、保守用端末の接続時の認証に失敗した場合は、コンピュータシステム側から接続ポート（保守専用ポート）のロックを行い、以降、如何なる端末を接続しようとしても、コンピュータシステム側から、当該接続ポートのロック解除の指示を実施しない限り、当該コンピュータシステムへのアクセスを一切無効にすることを、その主要な特徴としている。

【００１７】
したがって、保守対象のコンピュータシステムに対する通信用の設定や保守ツールなどの保守用の特殊なソフトの設定は、当該コンピュータシステム側で管理し、保守用端末接続時の認証成功時に、自動的に保守用端末側に設定するので、保守用端末の設定処理を容易に行うことができる。一方、接続時の認証失敗時には、コンピュータシステム側から接続ポートをロックするため、不正な接続が繰り返し試みられるような事態を確実に防止することができる。
【００１８】
コンピュータシステムを保守する保守用端末は、当該コンピュータシステムに対する保守動作を実施することを可能とするために、通常、高い権限を有して動作することになるので、その取り扱いには、十分な注意が必要であり、特に、不正アクセス対策を十分に考慮しておくことが必要であるが、本発明においては、前述のように、保守用端末に専用の接続ポート（保守ポート）を用意しており、保守用端末からの保守機能は、当該接続ポートから入力された場合にのみ有効とするようにするとともに、保守専用の当該接続ポート（保守ポート）に対する接続に不正を検知した場合には、コンピュータシステム側で保守専用の当該接続ポート（保守ポート）をロックし、以降の一切のアクセスを無効としている。この結果、以降は、コンピュータシステム側から、保守専用の当該接続ポート（保守ポート）のロックを解除しない限り、たとえ、接続する端末を変えても、当該接続ポート（保守ポート）からは、コンピュータシステムの保守機能へのアクセスは一切不可能になる。
【００１９】
（実施例の構成）
次に、本発明の実施例の構成について、図面を参照して詳細に説明する。図１は、本発明に係るコンピュータシステムの接続構成の一例を説明するためのシステム構成図である。
【００２０】
図１を参照すると、本実施例であるコンピュータシステム１０は、ディスクアレイ部１０１とＣＰＵ１０５と認証情報部１０６とコネクタ部１０７とを少なくとも備えて構成されている。また、ディスクアレイ部１０１には、ＯＳ格納部１０２と通信設定格納部１０３と保守ツール格納部１０４とが少なくとも備えられている。ディスクアレイ部１０１は、一般に、複数の磁気ディスク装置を使用し、かつ、冗長性を持たせたＲＡＩＤシステムで構成される。なお、コネクタ部１０７は、保守用端末１０８を接続するための保守専用の接続ポート（すなわち保守ポート）であり、当該接続ポートから入力された保守指令についてのみ、コンピュータシステムの保守機能に受け入れられて動作可能としているものであり、当該接続ポート以外のコネクタ部から当該コンピュータシステム１０に対する保守用の保守指令が入力されてきても、一切受け付けることはない。
【００２１】
一方、ハードディスクを備えていないシンクライアント端末構造である保守用端末１０８は、認証キー情報部１０９とメモリ１１０とコネクタ部１１１とを少なくとも備えて構成され、コネクタ部１１１に接続した接続ケーブル１１２によって、コンピュータシステム１０のコネクタ部１０７に接続される。
【００２２】
ここに、コンピュータシステム１０のＯＳ格納部１０２は、ディスクアレイ部１０１に設定されたデータ記録領域であり、保守用端末１０８が動作するためのＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）に関する情報が格納されている。つまり、ＯＳ格納部１０２に格納されているＯＳは、保守用端末１０８を動作させるための基本ソフトウェアであり、保守用端末１０８のメモリ１１０上で動作して保守用端末１０８の動作を制御するものである。
【００２３】
また、通信設定格納部１０３は、ディスクアレイ部１０１に設定されたデータ記録領域であり、保守用端末１０８がコンピュータシステム１０と通信するために使用される通信

設定に関する情報が格納されている。つまり、通信設定格納部１０３に格納されている通信設定情報は、保守用端末１０８上で動作するＯＳに設定すべき情報のうち、特に、コンピュータシステム１０との通信の設定に関するパラメータ情報のことであり、従来、保守用端末１０８において人手で実施していた通信の設定を、保守用端末１０８上のＯＳが自動的に設定するために使用される。

【００２４】

保守ツール格納部１０４は、ディスクアレイ部１０１に設定されたデータ記録領域であり、コンピュータシステム１０を保守するためのツールが格納されている。つまり、保守ツール格納部１０４に格納されている保守ツールは、保守用端末１０８のＯＳ上で動作するアプリケーションであり、コンピュータシステム１０のステータス確認やログ確認や構成設定等、コンピュータシステム１０を保守する際に使用される。

【００２５】

また、コンピュータシステム１０のＣＰＵ１０５は、マイクロプロセッサ等で構成されている中央処理装置であり、保守専用の接続ポートを形成するコネクタ部１０７に保守用端末１０８が接続された際に、接続された保守用端末１０８の認証キー情報部１０９から自動的に当該保守用端末１０８に設定されている認証キー情報を読み取る。しかる後、ＣＰＵ１０５は、認証情報部１０６にあらかじめ設定されている認証情報と保守用端末１０８の認証キー情報部１０９から読み取った認証キー情報とを照合して、保守用端末１０８の認証処理を行う。

【００２６】

ここで、ＣＰＵ１０５は、保守用端末１０８の認証キー情報部１０９から認証キー情報を正しく読み取れなかった場合、あるいは、認証情報部１０６にあらかじめ設定されている認証情報との照合結果として、保守用端末１０８の認証処理に失敗した場合には、コネクタ部１０７に接続された保守用端末１０８との接続を切断し、以降のアクセスを一切遮断するために接続ポートのロックを行う。

【００２７】

以降は、コンピュータシステム１０のＣＰＵ１０５側から接続ポートのロックを解除しない限り、コネクタ部１０７に接続する端末を他の端末（たとえ、正しい保守用端末１０８）に変えても、認証動作を実施することはなく、コンピュータシステム１０へのアクセスは不可能である。コンピュータシステム１０を管理する管理者が、接続ポートのロックを解除する指示をＣＰＵ１０５に対して行うか、あるいは、独自に設定したロック解除条件（例えば、あらかじめ設定した任意の時間経過した時点など）が成立した場合において、はじめて、接続ポートのロックを解除した状態に復帰させる。

【００２８】

一方、ＣＰＵ１０５は、保守用端末１０８の認証処理に成功した場合は、ディスクアレイ部１０１に対して、ＯＳ格納部１０２に格納されているＯＳ情報を保守用端末１０８側へ送信する指示を行う。さらに、ＣＰＵ１０５は、ディスクアレイ部１０１へのＯＳ送信指示の後、保守用端末１０８のＯＳ起動状態を定期的に確認し、保守用端末１０８のＯＳ起動を確認することができた場合に、ディスクアレイ部１０１に対して、通信設定格納部１０３に格納されている通信設定に関する情報を保守用端末１０８側へ送信する指示を行う。ＣＰＵ１０５は、ディスクアレイ部１０１への通信設定情報の送信指示の後、保守用端末１０８がコンピュータシステム１０との間の通信を可能とする通信設定を終了して、保守用端末１０８から保守ツールの送信要求が送信されてきた際に、ディスクアレイ部１０１に対して、保守ツール格納部１０４に格納されている保守ツールに関する情報を保守用端末１０８側へ送信する指示を行う。

【００２９】

なお、コンピュータシステム１０のディスクアレイ部１０１は、ＣＰＵ１０５からの指示に応じて、ＯＳ格納部１０２に格納されているＯＳ情報を、コネクタ部１０７、接続ケーブル１１２を介して、保守用端末１０８へ送信する動作を行う。また、コンピュータシステム１０のディスクアレイ部１０１は、ＣＰＵ１０５からの指示に応じて、通信設定格

納部１０３に格納されている通信設定に関する情報を、コネクタ部１０７、接続ケーブル１１２を介して、保守用端末１０８へ送信する動作を行う。さらに、コンピュータシステム１０のディスクアレイ部１０１は、ＣＰＵ１０５からの指示に応じて、保守ツール格納部１０４に格納されている保守ツールに関する情報を、コネクタ部１０７、接続ケーブル１１２を介して、保守用端末１０８へ送信する動作を行う。

【００３０】

また、コンピュータシステム１０の認証情報部１０６は、コンピュータシステム１０に内蔵される不揮発性の半導体記録装置であり、認証情報部１０６にあらかじめ記録された認証情報は、当該コンピュータシステム１０に固有のＩＤ情報であり、保守用端末１０８をコンピュータシステム１０に接続した際の認証処理に使用される。

【００３１】

つまり、認証情報部１０６にあらかじめ記録された認証情報は、コンピュータシステム１０の製品モデルごとに定められた一意のＩＤ情報であり、変更することはできない。図４は、本発明に係るコンピュータシステム１０の認証情報部１０６に記録された認証情報の一例を示すテーブルであり、認証用ＩＤ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ＩＤ）として、例えば、「１２３４５６７８９０」が設定されている例を示している。

【００３２】

また、コネクタ部１０７は、保守用の外部機器である保守用端末１０８を接続するための保守専用の接続ポートとして、コンピュータシステム１０に設けられた外部入出力端子であり、例えば、標準的なＬＡＮコネクタ規格であるＲＪ-４５を用いた外部入出力端子を適用して、接続ケーブル１１２を接続する。あるいは、コネクタ部１０７には、外部機器の接続ポートとしてＲＳ－２３２ＣやＷＡＮを介した通信インタフェースなど、任意の形式の入出力端子を適用しても良い。図３には、コネクタ部１０７としてＬＡＮポートを用いている場合の通信設定格納部１０３の通信設定情報の一例を示している。

【００３３】

すなわち、図３は、本発明に係るコンピュータシステム１０の通信設定格納部１０３に記録された通信設定情報の一例を示すテーブルであり、保守用端末１０８に設定すべき通信設定情報の一例を示しており、ＬＡＮポートのポート番号１（ＬＡＮ　Ｐｏｒｔ１）として、ＩＰアドレスが「１０．０．０．１」、サブネットマスクが「２５５．２５５．２５５．１９２」、デフォルト・ゲートウェイ・アドレスが「１０．０．０．２５４」の場合を例示している。

【００３４】

保守用端末１０８は、前述のように、ハードディスクを内蔵していないシンクライアント型のパーソナルコンピュータあるいは簡易型の携帯端末であり、コンピュータシステム１０を保守するための外部操作端末として使用される。したがって、保守用端末１０８は、コンピュータシステム１０の保守を行うために、コンピュータシステム１０に接続した際に、当該保守用端末１０８の動作を制御するためのＯＳ、コンピュータシステム１０との間の通信を行うために必要な通信設定情報、コンピュータシステム１０を保守するための保守ツールを、コンピュータシステム１０からダウンロードすることによって、はじめて保守動作を実行することが可能になる。

【００３５】

保守用端末１０８の認証キー情報部１０９は、保守用端末１０８に内蔵される不揮発性半導体記録装置である。認証キー情報部１０９に記録された認証キーは、コンピュータシステム１０を識別するためのＩＤ情報であり、コンピュータシステム１０と接続した際に、コンピュータシステム１０側に転送されて、接続した端末が、当該コンピュータシステム１０を保守するための保守用端末であることを認証するために使用される。

【００３６】

つまり、認証キー情報部１０９に記録された認証キーは、コンピュータシステム１０の認証情報部１０６に記録された認証情報と整合性を有する情報であり、保守対象であるコンピュータシステム１０の製品モデルが複数存在している場合には、それぞれのコンピュ

ータシステム１０に対応した複数の認証情報を格納することができる。図５は、本発明に係るコンピュータシステム１０に接続する保守用端末１０８の認証キー情報部１０９に記録された認証キーの一例を示すテーブルであり、ＫＥＹ　ＩＤ　Ａとして、当該コンピュータシステム１０の認証情報「１２３４５６７８９０」と一致する認証キーを有し、さらに、その他のコンピュータシステムの保守も可能とするために、複数個の認証キーを設定している場合を例示している。

【００３７】

保守用端末１０８のメモリ１１０は、保守用端末１０８に内蔵される揮発性半導体記憶装置であり、コンピュータシステム１０のＯＳ格納部１０２から読み出されたＯＳと通信設定格納部１０３から読み出された通信設定のパラメータ情報と保守ツール格納部１０４から読み出された保守ツールを一時的に記憶し、記憶された各種の情報は、保守用端末１０８で動作、実行させるために使用される。

【００３８】

保守用端末１０８のコネクタ部１１１は、コンピュータシステム１０と接続するための接続ポートとして、コンピュータシステム１０のコネクタ部１０７と対応するコネクタであって、保守用端末１０８に設けられた外部入出力端子であり、例えば、標準的なＬＡＮコネクタ規格であるＲＪ-４５を用いた外部入出力端子を適用して、接続ケーブル１１２を接続する。あるいは、コンピュータシステム１０のコネクタ部１０７に対応して、コネクタ部１１１には、ＲＳ－２３２ＣやＷＡＮを介した通信インタフェースなど、任意の形式の入出力端子を適用しても良い。なお、接続ケーブル１１２は、例えば、標準的なＬＡＮ規格である１０００ＢＡＳＥ－ＴＸに準拠したケーブルであり、保守用端末１０８をコンピュータシステム１０と接続する際に使用される。あるいは、コネクタ部１０７，１１１にＲＳ－２３２Ｃ用の外部入出力端子を使用している場合には、シリアル通信用のＲＳ－２３２Ｃケーブルが使用される。

【００３９】

（実施例の動作の説明）

次に、図２を用いて、図１に示すコンピュータシステム１０と保守用端末１０８との接続時における認証動作について詳細に説明する。図２は、図１に示すコンピュータシステム１０と保守用端末１０８との接続時における認証動作の一例を説明するためのフローチャートである。

【００４０】

図２において、まず、コンピュータシステム１０のコネクタ部１０７と保守用端末１０８のコネクタ部１１１とを、接続ケーブル１１２を用いて接続する（ステップＡ１）。しかる後、保守用端末１０８の電源を投入すると（ステップＡ２）、コンピュータシステム１０のＣＰＵ１０５は、保守用端末１０８の認証キー情報部１０９に記録されている認証キー情報を自動的に読み出す。（ステップＡ３）

【００４１】

ＣＰＵ１０５は、保守用端末１０８の認証キー情報部１０９から認証キー情報を正しく読み出せなかった場合には（ステップＡ４のＮｏ）、接続された端末が保守用端末１０８ではないものと判断し、接続された端末との通信を直ちに切断して（ステップＡ５）、以降のコネクタ部１０７からのアクセスを禁止するように、接続ポートをロックする（ステップＡ６）。

【００４２】

一方、ＣＰＵ１０５は、保守用端末１０８の認証キー情報部１０９から認証キー情報を正しく読み出すことができた場合には（ステップＡ４のＹｅｓ）、認証情報部１０６に記録されている認証情報と照合することによって、認証キー情報の認証処理を行う（ステップＡ７）。ＣＰＵ１０５は、認証処理の結果、認証情報部１０６に記録されている認証情報との照合が得られず、接続された端末が保守用端末１０８ではないものと判断した場合には（ステップＡ８のＮｏ）、ステップＡ５の処理に移行して、接続された端末との通信を直ちに切断し、以降のコネクタ部１０７からのアクセスを禁止するように、接続ポート

をロックする。すなわち、認証処理に失敗した場合は、ＯＳなどの情報を保守用端末１０８側にローディングする動作を行うことなく、直ちに切断し、かつ、以降のアクセスを抑止するために、接続ポートをロックする。

【００４３】

一方、ＣＰＵ１０５は、認証処理の結果、認証情報部１０６に記録されている認証情報との照合が得られ、コネクタ部１０７に接続された端末が保守用端末１０８であると判断した場合には（ステップＡ８のＹｅｓ）、ディスクアレイ部１０１に対して、ＯＳ格納部１０２に格納されているＯＳを、保守用端末１０８に送信するように指示する（ステップＡ９）。ディスクアレイ部１０１は、ＣＰＵ１０５の指示に従い、ＯＳ格納部１０２に格納されているＯＳを、保守用端末１０８に送信する（ステップＡ１０）。

【００４４】

保守用端末１０８は、コンピュータシステム１０から受信したＯＳをメモリ１１０に一時的に記憶する（ステップＡ１１）。しかる後、保守用端末１０８は、メモリ１１０に記憶したＯＳを自動的に起動する（ステップＡ１２）。

【００４５】

コンピュータシステム１０のＣＰＵ１０５は、ＯＳを保守用端末１０８に送信した後、保守用端末１０８のＯＳが起動されたか否かをあらかじめ定めた周期で定期的な確認を行っており、保守用端末１０８でＯＳが起動されたことを確認すると（ステップＡ１３）、ディスクアレイ部１０１に対して、通信設定格納部１０３に格納されている通信設定情報を、保守用端末１０８に送信するよう指示する（ステップＡ１４）。ディスクアレイ部１０１は、ＣＰＵ１０５の指示に従い、通信設定格納部１０３に格納されている通信設定情報を、保守用端末１０８に送信する（ステップＡ１５）。

【００４６】

保守用端末１０８は、コンピュータシステム１０から受信した通信設定情報をメモリ１１０に一時的に記憶する（ステップＡ１６）。しかる後、保守用端末１０８は、メモリ１１０に記憶した通信設定情報に基づき、コンピュータシステム１０との通信に必要な通信設定を自動的に行う（ステップＡ１７）。

【００４７】

保守用端末１０８は、通信設定が終了すると、直ちに、コンピュータシステム１０との通信を開始し（ステップＡ１８）、コンピュータシステム１０のＣＰＵ１０５に対して保守ツールを送信するように要求する（ステップＡ１９）。コンピュータシステム１０のＣＰＵ１０５は、保守用端末１０８からの要求を受け取って、ディスクアレイ部１０１に対して、保守ツール格納部１０４に格納されている保守ツールを、保守用端末１０８に送信するよう指示する。ディスクアレイ部１０１は、ＣＰＵ１０５の指示に従い、保守ツール格納部１０４に格納されている保守ツールを、保守用端末１０８に送信する（ステップＡ２０）。

【００４８】

保守用端末１０８は、コンピュータシステム１０から受信した保守ツールをメモリ１１０に一時的に記憶して（ステップＡ２１）、ＯＳの制御の下、メモリ１１０に記憶した保守ツールを起動し、コンピュータシステム１０の保守を実行することが可能な状態に設定する（ステップＡ２２）。以降、保守用端末１０８の保守ツールの動作に応じて、コンピュータシステム１０の保守が実施される。

【００４９】

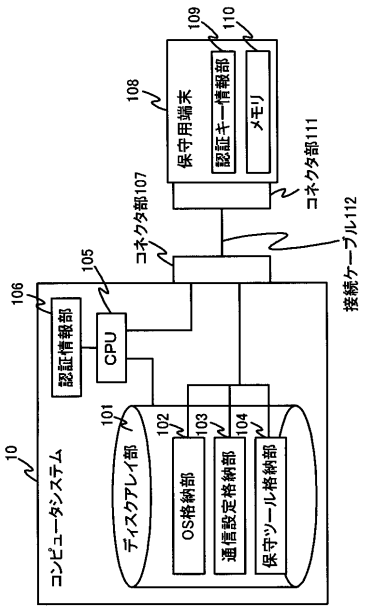
（本実施例の効果の説明）

従来のコンピュータシステムの保守用端末には、認証処理を実施可能とする場合、通常、ＯＳが内蔵された一般的なパーソナルコンピュータが使用されており、コンピュータシステムを保守するためには、使用者が、その都度、保守対象の当該コンピュータシステムと通信する際の保守用端末の通信設定を変更したり、さらには、当該コンピュータシステムの保守を実行する保守ツールを保守用端末にインストールしたりすることが必要になるという問題点があった。

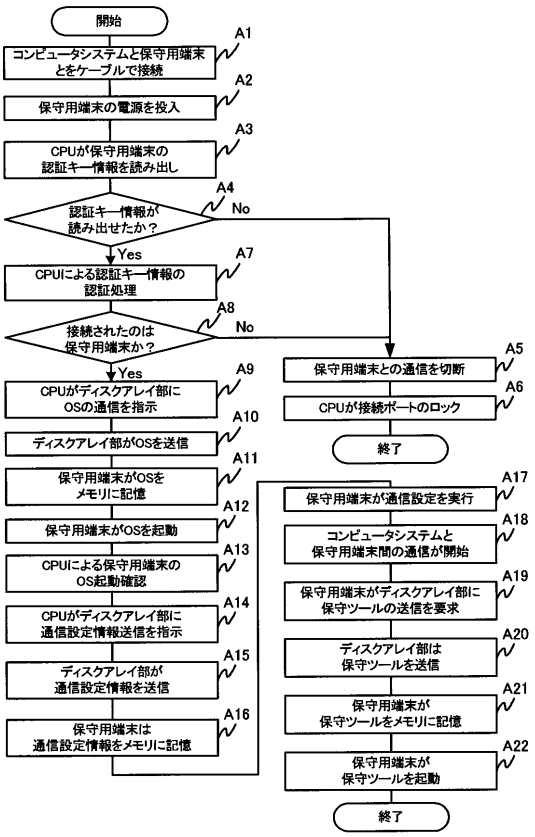
【００５０】
さらに、保守用端末を保守対象のコンピュータシステムの接続ポートに接続して、当該コンピュータシステムにログインするための認証処理を行った際に、認証処理に複数回失敗したとしても、通信を行う接続ポートは接続可能のままのオープンな状態が維持されているため、当該コンピュータシステムに不正にアクセスしようとしている不正アクセス者の場合、何度でも、認証を試みることができるという問題点もあった。
【００５１】
しかし、本発明に係る前述の実施例においては、以下のように、かかる問題点を確実に解決することができる。
【００５２】
（１）まず、コンピュータシステム１０を保守するための保守用端末１０８としてシンクライアント型の端末を使用し、保守対象のコンピュータシステム１０に内蔵されるディスクアレイ部１０１に、保守用端末１０８のＯＳ、保守用端末１０８が当該コンピュータシステム１０と通信するための通信設定情報、さらには、当該コンピュータシステム１０を保守するための保守ツールをあらかじめ格納しておいて、コンピュータシステム１０に接続した際に保守用端末１０８へ自動的に読み出す仕組みを有して構成し、さらに、保守対象のコンピュータシステム１０にログイン用の認証情報を設けるとともに、保守用端末１０８側にコンピュータシステム１０にログインするための認証キーを設けることにより、認証に失敗する端末が接続された場合に、当該コンピュータシステム１０のＣＰＵ１０５自体の動作によって、接続ポート（保守専用ポート）に接続されている端末との間の接続を切断するとともに、当該接続ポート（保守専用ポート）をロックすることにしているので、当該コンピュータシステム１０への以降のアクセスを確実に抑止し、不正な接続が継続されることを確実に防止することができる。
【００５３】
（２）さらに、当該コンピュータシステム１０に接続した端末の認証に失敗した場合は、当該コンピュータシステム１０からＯＳを端末側にダウンロードする動作を含め、一切の情報を転送することなく、端末との接続を切断するので、端末側に情報が漏洩することを防止することができる。
【００５４】
（３）また、コンピュータシステム１０に接続した端末の認証に成功した場合に、はじめて、当該端末を当該コンピュータシステム１０の保守を行うための保守用端末１０８として認識して、保守対象の当該コンピュータシステム１０のディスクアレイ部１０１から、保守用端末１０８のＯＳ、保守用端末１０８が当該コンピュータシステム１０と通信するための通信設定情報、さらには、当該コンピュータシステム１０を保守するための保守ツールを保守用端末１０８側へ自動的に転送することを可能とすることにより、保守用端末１０８の汎用性を維持しつつ、従来の保守用端末に対して人手で行っていた通信の設定や、保守ツールのインストール操作などの不便さを解消することができる。
【００５５】
（４）さらに、当該コンピュータシステム１０に接続するコネクタ部１０７は、ＬＡＮポートに限ることなく、任意の外部インタフェースを用いることが可能であり、ＲＳ－２３２Ｃなど各種の外部インタフェースを適用することができ、拡張性を確保することができる。
【００５６】
以上、本発明の好適実施例の構成を説明した。しかし、斯かる実施例は、本発明の単なる例示に過ぎず、何ら本発明を限定するものではないことに留意されたい。本発明の要旨を逸脱することなく、特定用途に応じて種々の変形変更が可能であることは、当業者には容易に理解できよう。
【図面の簡単な説明】
【００５７】
【図１】本発明に係るコンピュータシステムの接続構成の一例を説明するためのシステム

構成図である。
【図２】図１に示すコンピュータシステムと保守用端末との接続時における認証動作の一例を説明するためのフローチャートである。
【図３】本発明に係るコンピュータシステムの通信設定格納部に記録された通信設定情報の一例を示すテーブルである。
【図４】本発明に係るコンピュータシステムの認証情報部に記録された認証情報の一例を示すテーブルである。
【図５】本発明に係るコンピュータシステムに接続する保守用端末の認証キー情報部に記録された認証キーの一例を示すテーブルである。
【符号の説明】
【００５８】
１０　　コンピュータシステム
１０１　　ディスクアレイ部
１０２　　ＯＳ格納部
１０３　　通信設定格納部
１０４　　保守ツール格納部
１０５　　ＣＰＵ
１０６　　認証情報部
１０７　　コネクタ部
１０８　　保守用端末
１０９　　認証キー情報部
１１０　　メモリ
１１１　　コネクタ部
１１２　　接続ケーブル

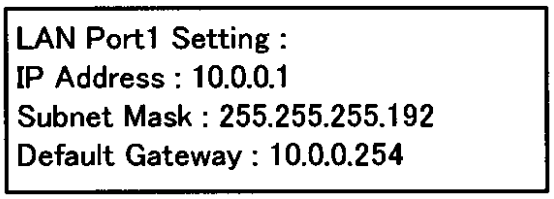
【図１】



【図２】



【図３】



【図４】

Authentication ID	1234567890

【図５】

KEY ID A	1234567890
KEY ID B	0987654321
KEY ID C	