(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2010-55393
(P2010-55393A)
(43)公開日　平成22年3月11日(2010.3.11)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330G	5B058
G06K 17/00	(2006.01)	G06F	15/00	330B	5B285
H04L 9/32	(2006.01)	G06F	15/00	330C	5J104
		G06K	17/00	S	
		H04L	9/00	675A	

審査請求 有　請求項の数 18　ＯＬ　（全 26 頁）

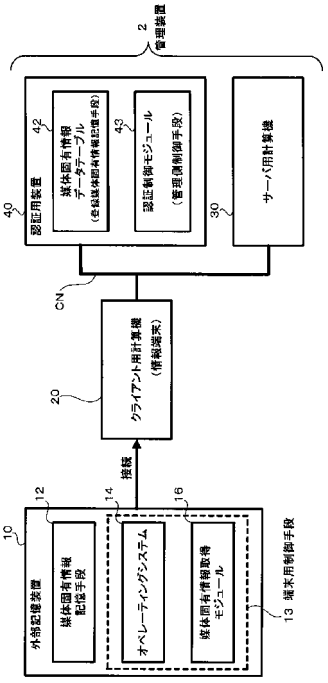
(21)出願番号　特願2008-219973 (P2008-219973)
(22)出願日　平成20年8月28日 (2008.8.28)

(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　100079164
弁理士　高橋　勇
(72)発明者　竹下　智彦
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)　5B058 CA01 KA32
5B285 AA01 BA03 CA43 CB06 CB07 CB12 CB14 CB15 CB16 CB17 CB18 CB23 CB24 CB25 CB26 CB42 CB44 CB52 CB55 CB62 CB63 CB64 CB73 CB84 CB92
5J104 AA07 KA02 PA07

(54)【発明の名称】認証システム、認証制御方法、及び認証制御プログラム

(57)【要約】
【課題】本発明は、導入コストが高価になり認証データの改ざんの機会を防止可能な認証システムを提供する。
【解決手段】情報端末２０、情報端末と接続され情報端末を外部から制御可能な外部記憶装置１０、情報端末からのアクセス許可を認証可能な管理装置３０・４０を含む。外部記憶装置は、媒体固有情報を記憶し自身が情報端末に装着した状態で情報端末を起動すると媒体固有情報を取得して情報端末を介して管理装置に向けて送信制御する。管理装置は、予め登録された登録媒体固有情報を記憶し送信された媒体固有情報を受信し媒体固有情報と登録媒体固有情報に基づいてアクセス許可に関する第１の認証をする。
【選択図】図１



【特許請求の範囲】
【請求項１】
情報端末と、この情報端末に接続され当該情報端末を外部から制御可能な外部記憶装置と、前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置と、を含み、
前記外部記憶装置は、
当該自己の識別情報である媒体固有情報を記憶した媒体固有情報記憶手段と、
この記憶された媒体固有情報を認証データとして前記情報端末を介して前記管理装置に向けて送信制御する端末用制御手段と、
を含み、
前記管理装置は、
前記外部記憶装置の識別用として予め登録された既登録媒体固有情報を記憶した登録媒体固有情報記憶手段と、
この既登録媒体固有情報と前記情報端末を介して送られてくる媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行する管理側制御手段と、
を含み、
前記管理側制御手段は、前記認証動作によって前記外部記憶装置を認証した場合に前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アクセス許容機能を備えていることを特徴とする認証システム。
【請求項２】
請求項１に記載の認証システムにおいて、
前記情報端末は、当該自己の識別情報である端末固有情報を記憶した端末固有情報記憶手段を含み、
前記管理装置は、前記情報端末の識別用として予め登録された既登録端末固有情報を記憶した登録端末固有情報記憶手段をさらに含み、
前記外部記憶装置の端末用制御手段は、
前記媒体固有情報とともに前記情報端末用の端末固有情報を認証データとして前記情報端末を介して前記管理装置に向けて送信する第１送信制御機能を有し、
前記管理装置の管理側制御手段は、
前記第１の認証動作により前記外部記憶装置が認証された場合に稼動し、前記既登録端末固有情報と前記情報端末から送信された前記端末固有情報とに基づいて前記情報端末にかかる第２の認証動作を実行する第２の認証動作実行機能と、
この第２の認証動作実行機能による第２の認証動作によって前記情報端末を認証した場合に前記管理装置に対する前記情報端末からのアクセス要求を許容するｂ級アクセス許容機能と、
を備えていることを特徴とする認証システム。
【請求項３】
請求項２に記載の認証システムにおいて、
前記管理装置は、
前記情報端末のユーザに関するユーザ情報を予め登録し既登録ユーザ情報として記憶した登録ユーザ情報記憶手段をさらに含み、
前記外部記憶装置の端末用制御手段は、
前記情報端末に外部入力されるユーザ情報を前記媒体固有情報及び前記端末固有情報とともに認証データとして前記管理装置に向けて送信制御する第２送信制御機能を有し、
前記管理側制御手段は、
前記第２の認証動作により前記情報端末が認証された場合に稼動し、前記既登録ユーザ情報と前記情報端末から送信されたユーザ情報とに基づいて前記情報端末のユーザにかかる第３の認証動作を実行する第３の認証動作実行機能と、
この第３の認証動作実行機能による第３の認証動作によって前記情報端末のユーザを認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するｃ級ア

クセス許容機能を備えていることを特徴とする認証システム。
【請求項４】
請求項３に記載の認証システムにおいて、
前記管理側制御手段は、
前記第３の認証動作を、ユーザ名及びパスワードによるユーザ認証、公開鍵認証、およびバイオメトリクス認証を組み合わせて行なうことを特徴とする認証システム。
【請求項５】
情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続し、この外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置であって、
前記外部記憶装置を識別するために予め登録された登録媒体固有情報を記憶した登録媒体固有情報記憶手段と、
予め前記外部記憶装置に記憶された媒体固有情報を取得した前記外部記憶装置付きの情報端末にから送信された前記媒体固有情報を受信し、この媒体固有情報と前記登録媒体固有情報とに基づいて第１の認証をし、この第１の認証が成功した場合に前記外部記憶装置付きの情報端末からの前記管理装置に対するアクセス要求を許可する管理側制御手段と、
を含むことを特徴とする管理装置。
【請求項６】
管理装置と通信網を介して通信可能な情報端末と接続され前記情報端末を外部から制御可能な外部記憶装置であって、
自身を識別する媒体固有情報を記憶した媒体固有情報記憶手段と、
前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス要求に関する第１の認証を前記管理装置にて行なうために、自身を前記情報端末に接続された状態で前記情報端末を起動し前記媒体固有情報を取得して前記情報端末を介して前記管理装置に向けて送信制御する端末用制御手段と、
を含むことを特徴とする外部記憶装置。
【請求項７】
情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続し、この外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置を用いた認証制御方法であって、
予め前記外部記憶装置に記憶された媒体固有情報を認証データとして前記情報端末より受信し、
前記外部記憶装置の識別用として予め登録された既登録媒体固有情報と、前記媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行し、
前記第１の認証動作によって前記外部記憶装置を認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アクセス許容を行う、
ことを特徴とする認証制御方法。
【請求項８】
請求項７に記載の認証制御方法において、
前記認証データは、予め前記情報端末に記憶された端末固有情報を含み、
前記第１の認証動作により前記外部記憶装置が認証された場合に稼動し、前記情報端末の識別用として予め登録された既登録端末固有情報と、前記端末固有情報とに基づいて前記情報端末にかかる第２の認証動作を実行し、
この第２の認証動作によって前記情報端末を認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するｂ級アクセス許容を行う、
ことを特徴とする認証制御方法。
【請求項９】
請求項８に記載の認証制御方法において、

前記認証データは、前記情報端末から入力されるユーザ情報を含み、
前記第２の認証動作により前記情報端末が認証された場合に稼動し、前記ユーザ情報を予め登録した既登録ユーザ情報と、前記ユーザ情報とに基づいて前記情報端末のユーザにかかる第３の認証動作を実行し、
この第３の認証動作によって前記情報端末のユーザを認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するｃ級アクセス許容を行う、
ことを特徴とする認証制御方法。
【請求項１０】
請求項９に記載の認証制御方法において、
前記第３の認証動作をするに際しては、ユーザ名及びパスワードによるユーザ認証、公開鍵認証、およびバイオメトリクス認証を組み合わせた認証をする、
ことを特徴とする認証制御方法。
【請求項１１】
管理装置と通信可能な情報端末と接続され前記情報端末を外部から制御可能な外部記憶装置を用いて、この外部記憶装置付きの前記情報端末からの前記管理装置に対するアクセス要求を前記管理装置にて認証する認証制御方法であって、
前記外部記憶装置が前記情報端末に接続した状態で前記外部記憶装置から前記情報端末を起動し、
予め前記外部記憶装置に記憶された媒体固有情報を取得し、
前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス要求に関する第１の認証を前記管理装置にて行なうために、前記媒体固有情報を前記情報端末を介して前記管理装置に向けて送信制御し前記第１の認証を実行させる、
ことを特徴とする認証制御方法。
【請求項１２】
請求項１１に記載の認証制御方法において、
前記媒体固有情報を取得する際には、予め前記情報端末の特定の記憶領域に記憶された端末固有情報とともに取得し、
前記媒体固有情報を送信制御する際には、前記端末固有情報を利用した第２の認証を前記管理装置にて行なうために前記端末固有情報とともに送信制御し前記第１の認証とともに前記第２の認証を実行させる、
ことを特徴とする認証制御方法。
【請求項１３】
請求項１２に記載の認証制御方法において、
前記媒体固有情報及び前記端末固有情報を取得する際には、前記情報端末より入力されたユーザ情報とともに取得し、
前記媒体固有情報及び前記端末固有情報を送信制御する際には、前記ユーザ情報を利用した第３の認証を前記管理装置にて行なうために前記ユーザ情報とともに送信制御し前記第１の認証及び第２の認証とともに前記第３の認証を実行させる、
ことを特徴とする認証制御方法。
【請求項１４】
情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続し、この外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置が備えたコンピュータに諸機能を実現させることが可能な管理装置用認証制御プログラムであって、
予め前記外部記憶装置に記憶された媒体固有情報を認証データとして前記情報端末より受信制御する受信制御機能と、
前記外部記憶装置の識別用として予め登録された既登録媒体固有情報と、前記媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行する第１の認証動作実行機能と、

前記第１の認証動作によって前記外部記憶装置を認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アクセス許容機能と、
を前記コンピュータに実現させることを特徴とする管理装置用認証制御プログラム。
【請求項１５】
請求項１４に記載の管理装置用認証制御プログラムにおいて、
前記受信制御機能では、
予め前記情報端末に記憶された端末固有情報を取得した前記外部記憶装置付きの情報端末から送信された前記端末固有情報とともに前記媒体固有情報を受信制御する機能を前記コンピュータに実現させ、
前記第１の認証動作により前記外部記憶装置が認証された場合に稼動し、前記情報端末の識別用として予め登録された既登録端末固有情報と、前記端末固有情報とに基づいて前記情報端末にかかる第２の認証動作を実行する第２の認証動作実行機能と、
この第２の認証動作実行機能による第２の認証動作によって前記情報端末を認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するｂ級アクセス許容機能と、
をさらに前記コンピュータに実現させることを特徴とする管理装置用認証制御プログラム。
【請求項１６】
請求項１５に記載の管理装置用認証制御プログラムにおいて、
前記受信制御機能では、
前記情報端末から入力されるユーザ情報を取得した前記外部記憶装置付きの情報端末から送信された前記ユーザ情報とともに前記端末固有情報及び前記媒体固有情報を受信制御する機能を前記コンピュータに実現させ、
前記第２の認証動作により前記情報端末が認証された場合に稼動し、前記ユーザ情報を予め登録した既登録ユーザ情報と、前記ユーザ情報とに基づいて前記情報端末のユーザにかかる第３の認証動作を実行する第３の認証動作実行機能と、
この第３の認証動作実行機能による第３の認証動作によって前記情報端末のユーザを認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するｃ級アクセス許容機能と、
をさらに前記コンピュータに実現させることを特徴とする管理装置用認証制御プログラム。
【請求項１７】
請求項１６に記載の管理装置用認証制御プログラムにおいて、
前記第３の認証動作実行機能では、
ユーザ名及びパスワードによるユーザ認証、公開鍵認証、およびバイオメトリクス認証を組み合わせた認証を行う機能をその内容とし、これを前記コンピュータに実現させることを特徴とする管理装置用認証制御プログラム。
【請求項１８】
管理装置と通信可能な情報端末と接続され前記情報端末を外部から制御可能な外部記憶装置を用いて、この外部記憶装置付きの前記情報端末からの前記管理装置に対するアクセス要求を前記管理装置にて認証するため、外部記憶装置付きの前記情報端末が備えたコンピュータに諸機能を実現させることが可能な外部記憶装置用認証制御プログラムであって、
前記外部記憶装置が前記情報端末に接続した状態で前記外部記憶装置から前記情報端末を起動すると、予め前記外部記憶装置に記憶された媒体固有情報を取得する情報取得機能と、
前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス許可に関する第１の認証を前記管理装置にて行なうために、前記媒体固有情報を前記情報端末を介して前記管理装置に向けて送信制御し前記第１の認証を実行させる端末用制御機能と、
を含む機能を前記コンピュータに実現させることを特徴とする外部記憶装置用認証制御

プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証システム、管理装置、外部記憶装置、認証制御方法、管理装置用認証制御プログラム、及び外部記憶装置用認証制御プログラムに関する。
【背景技術】
【０００２】
クライアント・サーバシステムでは、クライアント（情報端末）からサーバ（管理装置）にアクセスするには、多くの場合、クライアント用の情報端末に予め専用ソフトウェアをインストールする必要がある。
【０００３】
このため、外出先の環境などに用意された情報端末を利用する場合、クライアント用の専用ソフトウェアをインストールすることができないため、外出先からサーバにアクセスすることができない。
この際、サーバにアクセスするためには、外出先に前記専用ソフトウェアをインストールした情報端末（例えばノートPCなど）を用意したり、持ち運んだりする必要があった。
【０００４】
このような情報端末自体を持ち運ぶことなくサーバにアクセスする手法として、外部記憶媒体を用いる手法が挙げられる。
具体的には、ＵＳＢメモリやフラッシュディスク、ＣＤ－ＲＯＭなどの外部記憶媒体から直接オペレーティングシステムを起動することのできる計算機を利用して、サーバにアクセスする。
これにより、オペレーティングシステムを持ち運び可能な外部記憶媒体に記憶させておき、会社、自宅、訪問先、インターネットカフェなど環境において計算機を利用して、場所を選ばずにオペレーティングシステムを起動し、クライアント・サーバシステムのクライアントとして利用できる。
【０００５】
しかし、外部記憶媒体から起動する手法でサーバアクセスをする場合、ユーザ名とパスワード等をベースとした一般的な認証では、ユーザ名とパスワードが漏洩した場合、誰でもサーバへアクセスできる危険があり、認証の仕組みを強化する必要がある。
この認証の仕組みを強化する手法としては、ハードウェアによる認証が考えられ、ＵＳＢトークンを用いた認証方法やＴＰＭチップを用いた認証などやその他の様々な認証が挙げられる。
【０００６】
また、このような認証の仕組みに関連する技術として、例えば以下に示す特許文献１などが挙げられる。
【０００７】
特許文献１では、携帯端末装置がＤＢカードをアクセスする際、このカード内の「ハード識別番号」と自己の「ハード識別番号」とを照合し、その照合結果に基づいて当該ＤＢカードに対するアクセス可否を決定する。
ここで、「ハード識別番号」は、携帯端末装置とＤＢカードとを対応付けておくために予め携帯端末装置やＤＢカードに書き込まれたものである。すなわち、サーバ装置が携帯端末装置やＤＢカードへ書き込むための内容を予めテーブル設定しておく際に、「ハード識別番号」は、同一グループに属する携帯端末装置のうち、いずれか一台の端末から読み

込んだ固有の端末識別情報（製造番号）に応じて生成されたもので、サーバ装置はグループ対応の各携帯端末装置およびそれらの端末で利用される各ＤＢカード内に、ハード識別番号をそれぞれ書き込む。

したがって、同一グループに属する各携帯端末装置および各ＤＢカード内には、それぞれ同一のハード識別番号が共通のアクセス制限情報としてそれぞれ書き込まれる。

【０００８】

特許文献１では、セキュリティ管理システムは、例えば、会社組織において会社側に設置させているサーバ装置と、各営業担当者が持参するモバイル型のクライアント端末（携帯端末装置）と、この携帯端末装置にセットされて利用される可搬型記憶媒体とを有している。

そして、サーバ装置側で記憶管理されているアプリケーションソフト／データベース等を持ち運び自在な可搬型記憶媒体を介して携帯端末装置側に外部提供するようにしており、この記憶媒体にデータベース等を書き込んで端末装置へ配布する際に、サーバ装置は当該端末と記憶媒体とを対応付けるための情報を設定したり、各種のセキュリティ対策を講じることによって、記憶媒体内のアプリケーションソフト／データベース等が第三者によって不正コピーされたり、情報が漏洩されることを確実に防止するようにしたものである。

【０００９】

特許文献１では、各営業担当者は、外出先で可搬型記憶媒体３内のアプリケーションソフト／データベースをアクセスしながら営業活動を行い、そして、1日の営業終了時に端末本体から可搬型記憶媒体を抜き取り、それをサーバ装置側のカードリーダ／ライタにセットすると、サーバ装置はカードリーダ／ライタを介して記憶媒体内の営業記録を収集処理するようにしている。そして、サーバ装置と複数台の携帯端末装置とはシリアルケーブルを介して着脱自在に接続可能となっている。

【特許文献１】特開２００１－１９５３１１号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

ところで、このような関連技術のＵＳＢトークンを用いた認証方法やＴＰＭチップを用いたハードウェアによる認証手法では、導入コストが高価であるなどの課題があった。

【００１１】

また、ＰＣに内蔵されたＴＰＭ（トラスティッドプラットフォームモジュール）チップを用いて、固有の情報端末を識別する場合、利用するすべての情報端末がＴＰＭチップを実装しているわけではなく、すべての機器の入れ替えを必要とする環境への適用は非常に難しい上、ＴＰＭチップを搭載した比較的重量の重い専用の情報端末を持ち運ぶ必要があった。

【００１２】

加えて、特許文献１では、各携帯端末装置および各ＤＢカード内にそれぞれ同一の端末識別情報（製造番号）を書き込むためＤＢカードと端末とを個別に識別することはできず、さらには、利用者が自由に触れることができる情報端末側に認証データを保持することで、認証データの改ざんの機会が増加するなどセキュリティ上認証強度が弱くなり、サーバへの不正アクセスが生じる可能性が高まる、という課題があった。

【００１３】

本発明の目的は、上述の関連技術の課題を解決することにあり、ＴＰＭチップなどを搭載した専用の情報端末を持ち運ぶ必要がなく、サーバへの不正アクセスを防止可能とした比較的安価な認証システム、管理装置、外部記憶装置、認証制御方法、管理装置用認証制御プログラム、及び外部記憶装置用認証制御プログラムを提供することにある。

【課題を解決するための手段】

【００１４】

上記目的を達成するため、本発明にかかる認証システムは、情報端末と、この情報端末

に接続され当該情報端末を外部から制御可能な外部記憶装置と、前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置と、を含み、前記外部記憶装置は、当該自己の識別情報である媒体固有情報を記憶した媒体固有情報記憶手段と、この記憶された媒体固有情報を認証データとして前記情報端末を介して前記管理装置に向けて送信制御する端末用制御手段と、を含み、前記管理装置は、前記外部記憶装置の識別用として予め登録された既登録媒体固有情報を記憶した登録媒体固有情報記憶手段と、この既登録媒体固有情報と前記情報端末を介して送られてくる媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行する管理側制御手段と、を含み、前記管理側制御手段は、前記認証動作によって前記外部記憶装置を認証した場合に前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アクセス許容機能を備えていることを特徴としている。

【００１５】

本発明の（認証システムにおける）管理装置は、情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続し、この外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置であって、前記外部記憶装置を識別するために予め登録された登録媒体固有情報を記憶した登録媒体固有情報記憶手段と、予め前記外部記憶装置に記憶された媒体固有情報を取得した前記外部記憶装置付きの情報端末にから送信された前記媒体固有情報を受信し、この媒体固有情報と前記登録媒体固有情報とに基づいて第１の認証をし、この第１の認証が成功した場合に前記外部記憶装置付きの情報端末からの前記管理装置に対するアクセス要求を許可する管理側制御手段と、を含むことを特徴としている。

【００１６】

本発明の（認証システムにおける）外部記憶装置は、管理装置と通信網を介して通信可能な情報端末と接続され前記情報端末を外部から制御可能な外部記憶装置であって、自身を識別する媒体固有情報を記憶した媒体固有情報記憶手段と、前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス要求に関する第１の認証を前記管理装置にて行なうために、自身を前記情報端末に接続された状態で前記情報端末を起動し前記媒体固有情報を取得して前記情報端末を介して前記管理装置に向けて送信制御する端末用制御手段と、を含むことを特徴としている。

【００１７】

本発明の（管理装置側における）認証制御方法は、情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続し、この外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置を用いた認証制御方法であって、予め前記外部記憶装置に記憶された媒体固有情報を認証データとして前記情報端末より受信し、前記外部記憶装置の識別用として予め登録された既登録媒体固有情報と、前記媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行し、前記第１の認証動作によって前記外部記憶装置を認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アクセス許容を行う、ことを特徴としている。

【００１８】

本発明の（情報端末側における）認証制御方法は、管理装置と通信可能な情報端末と接続され前記情報端末を外部から制御可能な外部記憶装置を用いて、この外部記憶装置付きの前記情報端末からの前記管理装置に対するアクセス要求を前記管理装置にて認証する認証制御方法であって、前記外部記憶装置が前記情報端末に接続した状態で前記外部記憶装置から前記情報端末を起動し、予め前記外部記憶装置に記憶された媒体固有情報を取得し、前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス要求に関する第１の認証を前記管理装置にて行なうために、前記媒体固有情報を前記情報端末を介して前記管理装置に向けて送信制御し前記第１の認証を実行させる、ことを特徴としている。

【００１９】

本発明の管理装置用認証制御プログラムは、情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続し、この外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置が備えたコンピュータに諸機能を実現させることが可能な管理装置用認証制御プログラムであって、予め前記外部記憶装置に記憶された媒体固有情報を認証データとして前記情報端末より受信制御する受信制御機能と、前記外部記憶装置の識別用として予め登録された既登録媒体固有情報と、前記媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行する第１の認証動作実行機能と、前記第１の認証動作によって前記外部記憶装置を認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アクセス許容機能と、を前記コンピュータに実現させることを特徴としている。

【００２０】

本発明の外部記憶装置用認証制御プログラムは、管理装置と通信可能な情報端末と接続され前記情報端末を外部から制御可能な外部記憶装置を用いて、この外部記憶装置付きの前記情報端末からの前記管理装置に対するアクセス要求を前記管理装置にて認証するため、外部記憶装置付きの前記情報端末が備えたコンピュータに諸機能を実現させることが可能な外部記憶装置用認証制御プログラムであって、前記外部記憶装置が前記情報端末に接続した状態で前記外部記憶装置から前記情報端末を起動すると、予め前記外部記憶装置に記憶された媒体固有情報を取得する情報取得機能と、前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス許可に関する第１の認証を前記管理装置にて行なうために、前記媒体固有情報を前記情報端末を介して前記管理装置に向けて送信制御し前記第１の認証を実行させる端末用制御機能と、を含む機能を前記コンピュータに実現させることを特徴としている。

【発明の効果】

【００２１】

本発明によれば、外部記憶装置を用いることで、ＵＳＢトークンやＴＰＭチップ内蔵の情報端末などと比べ安価に手に入る機材を使って認証を実現でき、他の外部記憶装置に不正に複製されたオペレーティングシステムからサーバへのアクセスなどの不正アクセスを防止できるという、関連技術にない優れた認証システム、管理装置、外部記憶装置、認証制御方法、管理装置用認証制御プログラム、及び外部記憶装置用認証制御プログラムを提供することができる。

【発明を実施するための最良の形態】

【００２２】

〔第１の実施の形態〕

（認証システムの基本的構成）

先ず、認証システムの基本的構成について説明する。図１に示すように、本発明の認証システム１は、情報端末としてのクライアント用計算機２０と、前記情報端末と接続（又は着脱自在に装着）され前記情報端末を外部から制御可能な外部記憶装置１０と、前記外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に関する認証を可能とする管理装置２を構成するサーバ用計算機３０及び認証用装置４０と、を含む構成としている。

ここで、管理装置２は、前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器（情報端末及び／又は外部記憶装置）に対する認証を前提として許容する認証機能を備える。

【００２３】

外部記憶装置１０は、自身を識別する（自己の識別情報である）媒体固有情報を記憶した媒体固有情報記憶手段１２と、自身が前記情報端末に接続した状態で前記情報端末を起動すると前記媒体固有情報を取得して前記情報端末を介して前記管理装置に向けて送信制御する端末用制御手段としてのオペレーティングシステム１４及び媒体固有情報取得モジュール１６と、を含む構成としている。

端末用制御手段は、この記憶された媒体固有情報を認証データとして前記情報端末を介して前記管理装置に向けて送信制御する送信制御機能（第０送信制御機能）を備える。

【００２４】

管理装置２を構成する認証用装置４０は、前記外部記憶装置を識別する識別用として予め登録された登録媒体固有情報（既登録媒体固有情報）を記憶した登録媒体固有情報記憶手段（既登録媒体固有情報記憶手段）としての媒体固有情報データテーブル４２と、送信された前記媒体固有情報を受信し、この媒体固有情報と前記登録媒体固有情報とに基づいて前記情報端末からのアクセス要求に関する第１の認証をし、この第１の認証が成功した場合に前記外部記憶装置付きの情報端末からの前記管理装置に対するアクセス要求を許可する管理側制御手段としての認証制御モジュール４３と、を含む構成としている。

管理側制御手段は、この既登録媒体固有情報と前記情報端末を介して送られてくる媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行する機能を備える。

また、前記管理側制御手段は、前記認証動作によって前記外部記憶装置を認証した場合に前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アクセス許容機能を備える。

【００２５】

このような認証システムでは、オペレーティングシステム、およびクライアント機能を持ったソフトウェアを含む外部記憶媒体を持ち運ぶことで、端末自体を持ち運ぶ必要なく、外出先などの計算機に外部記憶装置を接続するオペレーティングシステムを起動し、認証を行いサーバにアクセスすることが可能になる。

【００２６】

ここで、ハードディスクやＵＳＢメモリ、ＣＦカード、ＳＤカード、ＣＤ－ＲＯＭなどの外部記憶装置はプログラム上から取り出せる領域に、シリアル番号やベンダＩＤなどの各媒体で固有の情報を持つものがある。

【００２７】

そして、上述の認証システムでは、持ち運びに便利な外部記憶媒体にサーバクライアントシステムのクライアント機能のあるソフトウェアをオペレーティングシステムとともにインストールし、サーバへのアクセスの際には、外部記憶装置のシリアル番号等ソフトウェア的に、ほかの媒体に複製できない外部記憶媒体固有の一意に定まる情報を基にした情報を要求する。

これにより、ほかの外部記憶媒体に不正に複製されたオペレーティングシステムからサーバへのアクセスなどの不正アクセスを防ぐことができる。

【００２８】

また、上述の認証システムでは、ＵＳＢメモリやＳＤカードなどの外部記憶装置を用いることで、ＵＳＢトークンやＴＰＭチップ内蔵のＰＣなどと比べ安価に手に入る機材を使っても外部記憶装置による認証を実現することができる。

【００２９】

このように、脱着可能な外部記憶媒体から起動したオペレーティングシステムを用いてサーバにアクセスする際に、起動する媒体の固有情報を用いて認証を行う媒体認証により、外部記憶媒体のオペレーティングシステムを含むソフトウェアを複製しても、複製したソフトウェアがサーバへのアクセスが認められず、不正利用を防止できる。

【００３０】

以下、このような本発明の「認証システム」のさらに詳細な実施の形態の一例について、図面を参照して具体的に説明する。

【００３１】

（認証システムの全体構成）

先ず、本実施の形態の認証システムの具体的構成について、全体構成から説明し、続いて各部の詳細構成について説明することとする。図１は、本発明における第１実施の形態の認証システムの全体の概略構成の一例を示すブロック図である。

【００３２】
図１に示すように、本実施の形態の認証システム１は、情報端末としてのクライアント用計算機２０と、クライアント用計算機２０と接続（又は着脱自在に装着）されクライアント用計算機２０を外部から制御可能な外部記憶装置１０と、前記外部記憶装置付きのクライアント用計算機２０と通信網ＣＮを介して通信可能に形成されクライアント用計算機２０からのアクセス許可（アクセス要求）を認証可能な管理装置２を構成するサーバ用計算機３０及び認証用装置４０と、を含む構成としている。
クライアント用計算機２０と認証用装置４０、およびサーバ用計算機３０は、有線・無線等の通信網ＣＮであるネットワーク経路を介して互いに通信接続される。
ここで、管理装置２は、前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備える。
【００３３】
外部記憶装置１０は、自身を識別する（自己の識別情報である）媒体固有情報を記憶した媒体固有情報記憶手段１２と、自身が前記クライアント用計算機２０に接続した状態で前記クライアント用計算機２０を起動すると前記媒体固有情報を取得してクライアント用計算機２０を介して前記管理装置に向けて送信制御する端末用制御手段１３としてのオペレーティングシステム１４及び媒体固有情報取得モジュール１６と、を含む構成としている。
【００３４】
外部記憶装置１０は、クライアント用計算機２０におけるＵＳＢポートやＣＦカードスロット、ＰＣカードインターフェース、ＣＤ－ＲＯＭドライブなどのリムーバブルメディア用インターフェース、各種スマートメディア用インターフェースなど、クライアント用計算機２０が、オペレーティングシステム１４を起動できる方式で接続される。
【００３５】
媒体固有情報記憶手段１２は、ハードウェア固有のベンダＩＤやシリアル番号などのような、媒体を一意に認識できる媒体固有情報を有する。
また、ベンダＩＤとデバイスＩＤとを組み合わせることもできる。あるいは、必要に応じてサブシステムベンダＩＤなどを組み合わせることもできる。
例えばスマートメディアの場合、ＩＤＩ（ＩＤ　ｉｎｆｏｍａｔｉｏｎ　ｆｉｅｌｄｓ）領域のコードを用いることもできる。
【００３６】
オペレーティングシステム１４は、クライアント用計算機２０を外部記憶装置１０から直接起動が可能なように構成される。
オペレーティングシステム１４は、種々のＯＳを採用でき、ネットワークＯＳなどが好ましい。また、セキュアＯＳのように標準的ＯＳがカスタマイズされたものであってもよい。
媒体固有情報取得モジュール１６は、オペレーティングシステム１４上で媒体固有情報を取得する処理を行う。
【００３７】
これにより、端末用制御手段１３は、前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス許可に関する第１の認証を前記管理装置にて行なうために、自身を前記情報端末に接続された状態で前記情報端末を起動し前記媒体固有情報を取得して前記情報端末を介して前記管理装置に向けて送信制御する機能を備えてよい。
端末用制御手段１３は、この記憶された媒体固有情報を認証データとして前記情報端末を介して前記管理装置に向けて送信制御する送信制御機能（第０送信制御機能）を備えてよい。
【００３８】
管理装置を構成する認証用装置４０は、前記外部記憶装置を識別する識別用として予め登録された登録媒体固有情報（既登録媒体固有情報）を記憶した登録媒体固有情報記憶手段（既登録媒体固有情報記憶手段）としての媒体固有情報データテーブル４２と、送信さ

れた前記媒体固有情報を受信し、この媒体固有情報と前記登録媒体固有情報とに基づいて前記情報端末からのアクセス要求に関する第１の認証をし、この第１の認証が成功した場合に前記外部記憶装置付きの情報端末からの前記管理装置に対するアクセス要求を許可する管理側制御手段としての認証制御モジュール４３と、を含む構成としている。

【００３９】

媒体固有情報データテーブル４２は、アクセスを許可する外部記憶装置１０の媒体固有情報を登録してリスト化した登録媒体固有情報を有する。

認証制御モジュール４３は、この既登録媒体固有情報と前記情報端末を介して送られてくる媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行する機能を備える。

また、認証制御モジュール４３は、前記認証動作によって前記外部記憶装置を認証した場合に前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アクセス許容機能を備える。

【００４０】

ここで、認証用装置４０は、サーバ用計算機３０にソフトウェアとして実装してもよく、その場合はまとめて一つの管理装置を構成できる。

【００４１】

クライアント用計算機２０、サーバ用計算機２０、認証用装置４０は、プログラム制御により動作するものであり、ネットワーク関連の通信機能を有していれば、デスクトップ、ラップトップコンピュータ、その他無線・有線通信機能を有する情報機器、情報家電機器、またはこれに類するコンピュータなどいかなるコンピュータでもよく、移動式・固定式を問わない。

【００４２】

クライアント用計算機２０、サーバ用計算機２０、認証用装置４０のハードウエア構成は、それぞれ、種々の情報等を表示するための表示部（スクリーン）、この表示部の表示画面上（の各種入力欄等）にデータを操作入力するための操作入力部（例えばキーボード・マウス・各種ボタン・表示操作部＜画面上のボタン＞・タッチパネル等）、各種信号・データを送受信するための送受信部ないしは通信部（モデムなど）、各種プログラム・各種データを記憶しておく記憶部（例えばメモリ、ハードディスク等）、これらの制御を司る制御部（例えばＣＰＵ、ＭＰＵ、ＤＳＰ等）などを有することができる。

ただし、クライアント用計算機２０は、シンクライアント（ネットワークコンピュータ）であることが好ましい。この場合、記憶部のハードディスクなどは不要となる。

【００４３】

（動作について）

（全体の概略動作）

次に、上述のような構成を有する認証システムの全体の概略動作について説明する。

【００４４】

本実施の形態に係る認証システムにおける動作を示す認証制御手順は、情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続（又は着脱自在に装着）し、この外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置を用いたものを対象とする。

【００４５】

この認証制御手順は、管理装置側における基本的手順として、予め前記外部記憶装置に記憶された媒体固有情報を認証データとして前記情報端末より受信し（例えば図２に示すステップA１５：受信制御ステップないしは受信制御機能）、前記外部記憶装置の識別用として予め登録された既登録媒体固有情報と、前記媒体固有情報とに基づいて前記外部記憶装置にかかる第１の認証動作を実行し（例えば図２に示すステップA１６：第１の認証動作実行ステップないしは機能）、前記第１の認証動作によって前記外部記憶装置を認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するa級アク

セス許容を実行する（例えば図２に示すステップA１７：ａ級アクセス許容ステップないしは機能）手順を行う。

すなわち、予め前記外部記憶装置に記憶された媒体固有情報を取得した前記外部記憶装置付きの情報端末から送信された前記媒体固有情報を受信し、この媒体固有情報と予め登録された登録媒体固有情報とに基づいて第１の認証をし、この第１の認証が成功した場合に前記外部記憶装置付きの情報端末からの前記管理装置に対するアクセス要求を許可する。

【００４６】

また、この認証制御手順は、管理装置と通信可能な情報端末と接続（又は着脱自在に装着）され前記情報端末を外部から制御可能な外部記憶装置を用いて、この外部記憶装置付きの前記情報端末からの前記管理装置に対するアクセス要求を前記管理装置にて認証するものを対象とする。

【００４７】

この認証制御手順は、情報端末側における基本的手順として、前記外部記憶装置が前記情報端末に接続した状態で前記外部記憶装置から前記情報端末を起動し（例えば図２に示すステップA１２）、予め前記外部記憶装置に記憶された媒体固有情報を取得し（例えば図２に示すステップA１３）、前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス要求に関する第１の認証を前記管理装置にて行なうために、前記媒体固有情報を前記情報端末を介して前記管理装置に向けて送信制御し（例えば図２に示すステップA１４）前記第１の認証を実行させる手順を行う。

【００４８】

（詳細動作）

以下、これらの各種の動作処理手順の詳細について、図２を参照しつつ説明する。図２は、図１の認証システムにおける処理手順の一例を示すフローチャートである。

【００４９】

先ず、サーバ用計算機３０又は認証用装置４０が保有する操作入力部を用いることによって、認証用装置４０は、サーバ用計算機３０へのアクセス（アクセス要求）を許可するアクセス許可条件（例えば外部記憶装置１０の媒体固有情報、又は媒体固有情報をもとにした情報など）を媒体固有情報データテーブル４２に登録する（図２に示すステップＡ１１：媒体固有情報登録ステップないしは媒体固有情報登録機能）。

これにより、媒体固有情報データベース４２は、登録媒体固有情報が格納される。

【００５０】

次に、外部記憶装置１０をクライアント用計算機２０に接続（装着）すると（又は装着した状態でクライアント用計算機２０の電源を投入すると）、クライアント用計算機２０は、外部記憶装置１０に搭載されたオペレーティングシステム１４を起動制御し、ネットワークコンピュータとしての諸機能を実現可能な状態となる（図２に示すステップＡ１２：起動制御ステップないしは起動制御機能）。

【００５１】

続いて、オペレーティングシステム１４が起動することで媒体固有情報取得モジュールが動作する。

外部記憶装置１０の媒体固有情報取得モジュール１６は、媒体固有情報記憶手段１２から媒体固有情報を取得する（図２に示すステップＡ１３：媒体固有情報取得ステップないしは媒体固有情報取得機能）。

【００５２】

その後、クライアント用計算機２０は、サーバ用計算機３０に対しアクセス要求を送信し、サーバ用計算機３０へのアクセスを試みる（図２ステップＡ１４：アクセス要求（媒体固有情報）送信ステップないしはアクセス要求送信機能）。

このアクセス要求には、外部記憶装置１０の媒体固有情報が含まれる。

【００５３】

一方、サーバ用計算機３０は、クライアント用計算機２０からの（媒体固有情報を含む

）アクセス要求を受信する。
そして、サーバ用計算機３０は、認証用装置４０の媒体固有情報データテーブル４２に、一致する情報（登録媒体固有情報）があるかを問い合わせる処理を行うことができる（図２に示すステップＡ１５：媒体固有情報受信制御ステップないしは媒体固有情報受信制御機能）。
【００５４】
認証用装置４０の認証制御モジュール４３は、クライアント用計算機２０で起動に使われた外部記憶装置１０がステップＡ１１で定めたアクセス許可条件に適合しているか否かの判定を行う（図２に示すステップＡ１６：アクセス許可条件判定ステップないしはアクセス許可条件判定機能）。
ここで、本実施の形態では、アクセス許可条件の判定として第１の認証を行う。この第１の認証では、認証用装置４０の認証制御モジュール４３が、クライアント用計算機２０から送信されてきた外部記憶装置１０の媒体固有情報と、認証用装置４０に予め登録された登録媒体固有情報とを照合する。
【００５５】
認証用装置４０の認証制御モジュール４３は、ステップＡ１６において媒体固有情報データテーブル４２に一致する情報があると判定した場合には、クライアント用計算機２０からサーバ用計算機３０へのアクセスを許可する処理を行う（図２に示すステップＡ１７：アクセス許可制御ステップないしはアクセス許可制御機能）。
【００５６】
一方、認証用装置４０の認証制御モジュール４３は、ステップＡ１６において一致する情報が存在しないと判定した場合には、サーバ用計算機３０への接続を不許可とする処理を行う（図２ステップＡ１７：アクセス不許可制御ステップないしはアクセス不許可制御機能）。
例えば、ユーザなどに不許可である旨のメッセージを通知し、クライアント計算機２０の電源をシャットダウンさせることもできる。
【００５７】
ここで、以上のステップＡ１６、ステップＡ１７、ステップＡ１８からなるステップは、認証制御ステップないしは認証制御機能の一例ということもできる。
この認証制御機能では、媒体固有情報と予め登録された登録媒体固有情報とに基づいて第１の認証をし、この第１の認証が成功した場合に前記外部記憶装置付きの情報端末からの前記管理装置に対するアクセスを許可する認証制御を行うことができる。
また、以上のステップＡ１５は、受信制御ステップないしは受信制御機能ということもできる。この受信制御機能では、予め前記外部記憶装置に記憶された媒体固有情報を取得した前記外部記憶装置付きの情報端末から送信された前記媒体固有情報を受信制御することができる。
【００５８】
さらに、以上のステップＡ１２、ステップＡ１３からなるステップは、情報取得ステップないしは情報取得機能の一例ということもできる。
この情報取得機能では、前記外部記憶装置が前記情報端末に接続した状態で前記外部記憶装置から前記情報端末を起動すると、予め前記外部記憶装置に記憶された媒体固有情報を取得することができる。
【００５９】
さらにまた、以上のステップＡ１４は、端末用制御ステップないしは端末用制御機能の一例ということもできる。
この端末用制御機能では、前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス許可に関する第１の認証を前記管理装置にて行なうために、前記媒体固有情報を前記情報端末を介して前記管理装置に向けて送信制御し前記第１の認証を実行させることができる。
【００６０】

以上のように本実施の形態によれば、以下の効果を奏することができる。
すなわち、第一の効果は、サーバへのアクセスの際に、オペレーティングシステム起動媒体自体の媒体固有情報をもとにデバイス認証を行うことである。
【００６１】
第二の効果は、複製品によるサーバへの不正アクセスを防ぐことができる点である。
オペレーティングシステムや媒体固有情報取得モジュールを外部記憶装置不正に複製しても、その外部記憶装置からサーバへのアクセスが、認証用装置での認証の段階で許可されず、不正な利用を防ぐことができるためである。
【００６２】
第三の効果は、オペレーティングシステムを含んだ外部記憶媒体を用い、その媒体自体固有の情報を使い認証ができるので、起動用媒体以外にＩＣカードやＵＳＢドングルなど別途認証専用デバイスを必要としない点である。
【００６３】
第四の効果は、特別に専用のデバイスを必要とせず、ベンダＩＤやシリアル番号などの媒体固有情報の取得でき、オペレーティングシステムを格納することのできる媒体であれば、媒体の種別を選ばない点である。
【００６４】
第五の効果は、端末側ではなく接続先の認証を用いて行うので、接続の管理を認証用装置で行うことができる点である。
【００６５】
第六の効果は、外出先のＰＣから利用しても、認証用装置に登録された外部記憶装置から起動したオペレーティングシステムで、接続することがサーバへのアクセス条件となるので、例え内蔵ディスクがウイルス感染したＰＣからサーバにアクセスしたとしても、外部記憶装置から起動したオペレーティングシステムを利用し、内蔵ディスク自体を使わないので、安全にサーバへアクセスできる点である。
【００６６】
さらに、特許文献１では、サーバ側で認証情報を管理する場合と比較し、端末利用者が自由に触れることができる端末側に認証データを保持することで、認証データの改ざんの機会が増加するなどセキュリティ上認証強度が弱くなるが、本実施の形態では端末利用者に触れられないサーバ側で認証情報の管理を行うという点でセキュリティ強度が増す。
また、クライアントサーバシステムで、データ自体は、端末側に一切置かないこともできる。
【００６７】
ここで、図１に示すブロック図における一部の各ブロックは、コンピュータにより実行可能なプログラムにより機能化された状態を示すソフトウエアモジュール構成であってもよい。
【００６８】
すなわち、物理的構成は例えば一又は複数のＣＰＵ（或いは一又は複数のＣＰＵと一又は複数のメモリ）等ではあるが、各部（回路・手段）によるソフトウエア構成は、プログラムの制御によってＣＰＵが発揮する複数の機能を、それぞれ複数の部（手段）による構成要素として表現したものである。
【００６９】
ＣＰＵがプログラムによって実行されている動的状態（プログラムを構成する各手順を実行している状態）を機能表現した場合、ＣＰＵ内に各部（手段）が構成されることになる。プログラムが実行されていない静的状態にあっては、各手段の構成を実現するプログラム全体（或いは各手段の構成に含まれるプログラム各部）は、メモリなどの記憶領域に記憶されている。
【００７０】
以上に示した各部、モジュール（手段）は、プログラムにより機能化されたコンピュータをプログラムの機能と共に実現し得るように構成しても、また、固有のハードウエアに

より恒久的に機能化された複数の電子回路ブロックからなる装置で構成してもよい。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現でき、いずれかに限定されるものではない。

【００７１】

［第２の実施の形態］

次に、本発明にかかる第２の実施の形態について、図３に基づいて説明する。以下には、前記第１の実施の形態の実質的に同様の構成に関しては説明を省略し、異なる部分についてのみ述べる。図３は、本発明の認証システムの第２の実施の形態の一例を示すブロック図である。

【００７２】

上述の第１の実施の形態では、アクセス許可条件として第１の認証のみによる認証制御を行う構成としたが、本実施の形態では、アクセス許可条件として第１の認証に加えて第２の認証および第３の認証による認証制御を行う構成としている。

【００７３】

具体的には、本実施の形態の認証システム１００は、図３に示すように、端末固有情報取得モジュール１１８、登録ユーザ情報記憶手段としてのユーザ情報データテーブル１４４、登録端末固有情報記憶手段としての端末固有情報データテーブル１４６、端末固有情報記憶手段１２２を有する点で前記第１の実施の形態と異なる。

【００７４】

端末固有情報記憶手段１２２は、情報端末であるクライアント計算機１２０自身を識別する（自己の識別情報である）端末固有情報を記憶している。

【００７５】

端末固有情報データテーブル１４６（登録端末固有情報記憶手段又は既登録端末固有情報記憶手段）は、クライアント計算機１２０（情報端末）を識別する識別用として予め登録された登録端末固有情報（既登録端末固有情報）を有する。

【００７６】

ユーザ情報データテーブル１４４（登録ユーザ情報記憶手段又は既登録ユーザ情報記憶手段）は、クライアント計算機１２０（情報端末）のユーザに関するユーザ情報を予め登録し登録ユーザ情報（既登録ユーザ情報）として記憶している。

【００７７】

端末固有情報取得モジュール１１８は、外部記憶装置１１０がクライアント計算機１２０に接続され、オペレーティングシステム１１４が起動し、媒体固有情報取得モジュール１１６が動作を開始すると動作し、クライアント用計算機１２０が有する端末固有情報記憶手段１２２の端末固有情報を取得する。

【００７８】

ここで、端末固有情報は、例えばＣＰＵのＩＤ、ＭＡＣアドレス、ハードディスクＩＤなどクライアント用計算機１２０を一意に特定できる情報、またはその組み合わせである。

【００７９】

認証用装置１４０は、前記第１の実施の形態の構成に加え、ユーザ情報データテーブル１４４と端末固有情報データテーブル１４６を有する。

認証用装置１４０は、外部記憶装置１１０から起動したクライアント用計算機１２０がサーバ用計算機１３０にアクセスする際に、媒体固有情報による第１の認証、端末固有情報による第２の認証、およびユーザ情報による第３の認証の組み合わせでアクセスの許可を判断する。

【００８０】

例えば、「特定の外部記憶装置は特定のクライアント用計算機でのみがサーバへのアクセス可能」とか「特定の外部記憶装置から起動したクライアント用計算機は特定のユーザのみがサーバへのアクセス可能」等のように設定することができる。

【００８１】

ここで、オペレーティングシステム１１４と媒体固有情報取得モジュール１１６と端末固有情報取得モジュール１１８とによる構成は、端末用制御手段１１３の一例ということもできる。

端末用制御手段１１３の構成例としては、オペレーティングシステム１１４に、各モジュール１１６、１１８の機能を組み込んでおいてもよい。

端末用制御手段１１３の一態様では、外部記憶装置１１０に記憶された一又は二以上のプログラムが、クライアント用計算機１２０のＣＰＵによって実行される際に発揮する制御機能ということができる。

【００８２】

端末用制御手段１１３は、前記媒体固有情報とともに前記端末固有情報を取得して前記管理装置に向けて送信制御する機能を備えることができる。すなわち、端末用制御手段１１３は、前記媒体固有情報とともに前記情報端末用の端末固有情報を認証データとして前記情報端末を介して前記管理装置に向けて送信する第１送信制御機能を有する。

また、端末用制御手段１１３は、情報端末から入力されるユーザ情報を前記媒体固有情報及び前記端末固有情報とともに前記管理装置に向けて送信制御する機能を備えることができる。すなわち、端末用制御手段１１３は、前記情報端末に外部入力されるユーザ情報を前記媒体固有情報及び前記端末固有情報とともに認証データとして前記管理装置に向けて送信制御する第２送信制御機能を有する。

【００８３】

管理側制御手段としての認証制御モジュール１４３は、前記媒体固有情報と前記端末固有情報を受信し、前記第１の認証が成功した場合に前記端末固有情報と前記登録端末固有情報とに基づいて第２の認証をし、前記第２の認証が成功した場合に前記アクセス要求を許可する機能を備えることができる。

すなわち、前記管理側制御手段としての認証制御モジュール１４３は、前記第１の認証動作により前記外部記憶装置が認証された場合に稼動し、前記既登録端末固有情報と前記情報端末から送信された前記端末固有情報とに基づいて前記情報端末にかかる第２の認証動作を実行する第２の認証動作実行機能を備えてよい。

また、認証制御モジュール１４３は、この第２の認証動作実行機能による第２の認証動作によって前記情報端末を認証した場合に前記管理装置に対する前記情報端末からのアクセス要求を許容するｂ級アクセス許容機能を備えてよい。

【００８４】

また、認証制御モジュール１４３は、前記媒体固有情報と前記端末固有情報と前記ユーザ情報を受信し、前記第２の認証が成功した場合に前記ユーザ情報と前記登録ユーザ情報とに基づいて第３の認証をし、前記第３の認証が成功した場合に前記アクセス要求を許可する機能を備えることができる。

すなわち、前記管理側制御手段としての認証制御モジュール１４３は、前記第２の認証動作により前記情報端末が認証された場合に稼動し、前記既登録ユーザ情報と前記情報端末から送信されたユーザ情報とに基づいて前記情報端末のユーザにかかる第３の認証動作を実行する第３の認証動作実行機能を備えてよい。

また、認証制御モジュール１４３は、この第３の認証動作実行機能による第３の認証動作によって前記情報端末のユーザを認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するｃ級アクセス許容機能を備えてよい。

さらに、認証制御モジュール１４３は、前記第３の認証動作をユーザ名及びパスワードによるユーザ認証、公開鍵認証、およびバイオメトリクス認証を組み合わせて行なう機能を備えてよい。

【００８５】

（動作について）

次に、図４のフローチャートを用いて、動作の詳細について説明する。

図４は、図２と比較し、ステップＡ１１のサーバへのアクセス許可条件が複雑化したもので、ステップＡ１１のフローがステップＢ１１、ステップＢ１２で置換されている。ま

た、ステップＡ１３の後に、クライアント用計算機１２０の固有情報を取得するステップＢ１３が追加されている。

また、ステップＳ１６では、図５に示すステップＡ１６１、Ａ１６２、Ａ１６３を実行する必要がある。

【００８６】

本実施の形態における動作における認証制御手順は、管理装置側では、先ず、前記媒体固有情報を認証データとして受信する際には、予め前記情報端末に記憶された端末固有情報を取得した前記外部記憶装置付きの情報端末から送信された前記端末固有情報とともに受信する（図４に示すステップＡ１５：受信制御ステップないしは受信制御機能）。すなわち、前記認証データは、予め前記情報端末に記憶された端末固有情報を含む。

次に、前記第１の認証動作により前記外部記憶装置が認証された場合に稼動し、前記情報端末の識別用として予め登録された既登録端末固有情報と、前記端末固有情報とに基づいて前記情報端末にかかる第２の認証動作を実行する（図５に示すステップＡ１６２：第２の認証動作実行ステップないしは機能）。

さらに、この第２の認証動作によって前記情報端末を認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するｂ級アクセス許容を行う（図４に示すステップＡ１７：ｂ級アクセス許容ステップないしは機能）。

すなわち、前記第１の認証が成功した場合に、さらに、前記端末固有情報と予め登録された登録端末固有情報とに基づいて第２の認証をし、この第２の認証が成功した場合に前記アクセス要求を許可する手順を行うことができる。

【００８７】

また、この認証制御手順では、前記媒体固有情報と前記端末固有情報とを認証データとして受信する際には、前記情報端末から入力されるユーザ情報を取得した前記外部記憶装置付きの情報端末から送信された前記ユーザ情報とともに受信する（ステップＡ１５：受信制御ステップないしは受信制御機能）。すなわち、前記認証データは、前記情報端末から入力されるユーザ情報を含む。

さらに、前記第２の認証動作により前記情報端末が認証された場合に稼動し、前記ユーザ情報を予め登録した既登録ユーザ情報と、前記ユーザ情報とに基づいて前記情報端末のユーザにかかる第３の認証動作を実行する（図５に示すステップＡ１６３：第３の認証動作実行ステップないしは機能）。

次に、この第３の認証動作によって前記情報端末のユーザを認証した場合に、前記管理装置に対する前記情報端末からのアクセス要求を許容するｃ級アクセス許容を行う（図４に示すステップＡ１７：ｃ級アクセス許容ステップないしは機能）。

すなわち、前記第２の認証が成功した場合に、さらに、前記ユーザ情報と予め登録された登録ユーザ情報とに基づいて第３の認証をし、この第３の認証が成功した場合に前記アクセス要求を許可する手順を行うことができる。

【００８８】

さらに、この認証制御手順では、前記第３の認証動作をするに際し、ユーザ名及びパスワードによるユーザ認証、公開鍵認証、およびバイオメトリクス認証を組み合わせて行い、これらの各認証が成功した場合に前記アクセスを許可することもできる。

以下、これを詳述する。

【００８９】

まず、ステップＢ１１では、上述の第１の実施の形態で示した外部記憶装置の媒体固有情報（又は媒体固有情報をもとにした情報）に加え、認証用装置１４０は、ユーザ名、パスワードなどを含んだユーザ情報、およびクライアント用計算機１２０の端末固有情報（又は端末固有情報をもとにした情報）を、各々媒体固有情報データテーブル１４２、ユーザ情報データテーブル１４４、端末固有情報データテーブル１４６に登録する（図４に示すステップＢ１１：媒体固有情報登録ステップないしは媒体固有情報登録機能、端末固有情報登録ステップないしは端末固有情報登録機能、ユーザ情報登録ステップないしはユーザ情報登録機能）。

これにより、媒体固有情報データテーブル１４２には、登録媒体固有情報が格納される。また、端末固有情報データテーブル１４６には、登録端末固有情報が格納される。さらに、ユーザ情報データテーブル１４４には、登録ユーザ情報が格納される。

【００９０】

そして、これらの各情報の組み合わせをアクセス許可条件として関連付けを行う（図４に示すステップＢ１２：アクセス許可条件生成ステップないしはアクセス許可条件生成機能）。

すなわち、登録媒体固有情報、登録端末固有情報、登録ユーザ情報の全条件を満たすことがアクセス許可条件となる。

【００９１】

次に、外部記憶装置１１０をクライアント用計算機１２０に接続（装着）すると（又は接続した状態でクライアント計算機の電源を投入すると）、クライアント用計算機１２０は、外部記憶装置１１０に搭載されたオペレーティングシステム１１４を起動制御し、ネットワークコンピュータとしての諸機能を実現可能な状態となる（図４に示すステップＡ１２：起動制御ステップないしは起動制御機能）。

【００９２】

続いて、オペレーティングシステム１１４が起動することで媒体固有情報取得モジュール１１６が動作する。

外部記憶装置１１０の媒体固有情報取得モジュール１１６は、媒体固有情報記憶手段１１２から媒体固有情報を取得する（図４に示すステップＡ１３：媒体固有情報取得ステップないしは媒体固有情報取得機能）。

【００９３】

さらに、オペレーティングシステム１１４が起動することで、又は媒体固有情報取得モジュールが動作することで、端末固有情報取得モジュール１１８が動作する。

外部記憶装置１１０の端末固有情報取得モジュール１１８は、端末固有情報記憶手段１２２から端末固有情報を取得する（図４に示すステップＢ１３：端末固有情報取得ステップないしは端末固有情報取得機能）。

【００９４】

さらにまた、オペレーティングシステム１１４起動後のいずれかのステップ間において、オペレーティングシステム１１４自身が保有するユーザ認証制御機能又は他のユーザ認証制御機能によってユーザに対しユーザ情報の入力を促す。

これにより、クライアント用計算機１２０からのユーザの操作入力に基づいて、オペレーティングシステム１１４は、ユーザ情報を取得する（ユーザ情報取得ステップないしはユーザ情報取得機能）。

【００９５】

その後、クライアント用計算機１２０は、サーバ用計算機１３０に対しアクセス要求を送信し、サーバ用計算機１３０へのアクセスを試みる（図４に示すステップＡ１４：アクセス要求送信ステップないしはアクセス要求送信機能）。

このアクセス要求には、外部記憶装置１１０の媒体固有情報、クライアント用計算機１２０の端末固有情報、外部記憶装置１１０付きのクライアント用計算機１２０から入力されたユーザ情報が含まれる。

【００９６】

一方、サーバ用計算機１３０は、クライアント用計算機１２０からの（媒体固有情報、端末固有情報、ユーザ情報を含む）アクセス要求を受信する。

そして、サーバ用計算機１３０は、認証用装置１４０の媒体固有情報データテーブル１４２、端末固有情報データテーブル１４６、ユーザ情報データテーブル１４４に対し、アクセス許可条件に一致する情報（登録媒体固有情報、登録端末固有情報、登録ユーザ情報）があるかを問い合わせる処理を行うことができる（図４に示すステップＡ１５：媒体固有情報受信制御ステップないしは媒体固有情報受信制御機能、端末固有情報受信制御ステップないしは端末固有情報受信制御機能、ユーザ情報受信制御ステップないしはユーザ情

報受信制御機能）。
【００９７】
認証用装置１４０は、クライアント用計算機１２０で起動に使われた外部記憶装置がステップＡ１１で定めたアクセス許可条件に適合しているか否かの判定を行う（図４に示すステップＡ１６：アクセス許可条件判定ステップないしはアクセス許可条件判定機能）。
【００９８】
（認証制御の詳細）
ここで、本実施の形態では、アクセス許可条件の判定として第１の認証、第２の認証、および第３の認証を行う。
すなわち、図５に示すように、認証用装置１４０の認証制御モジュール１４３は、第１の認証として媒体固有情報が一致するか否かの判定を行う（図５ステップＡ１６１：第１の認証ステップないしは第１の認証機能又は第１の認証動作実行機能）。
この第１の認証では、クライアント用計算機１２０から送信されてきた外部記憶装置１１０の媒体固有情報と、認証用装置１４０に予め登録された登録媒体固有情報（既登録媒体固有情報）とを照合する。
【００９９】
前記ステップＡ１６１において、認証用装置１４０の認証制御モジュール１４３は、媒体固有情報が一致しないと判定した場合にはステップＡ１８に進む。
一方、前記ステップＡ１６１において、媒体固有情報が一致すると判定した場合（前記認証動作によって前記外部記憶装置を認証した場合）には、前記管理装置に対する前記情報端末からのアクセス要求を許容する第１段階をクリアしたことになる（a級アクセス許容機能）。
そして、前記ステップＡ１６１において、媒体固有情報が一致すると判定した場合、認証用装置１４０の認証制御モジュール１４３は、第２の認証として端末固有情報が一致するか否かの判定を行う（図５ステップＡ１６２：第２の認証ステップないしは第２の認証機能又は第２の認証動作実行機能）。
この第２の認証では、クライアント用計算機１２０から送信されてきた端末固有情報と、認証用装置１４０に予め登録された登録端末固有情報（既登録端末固有情報）とを照合する。
【０１００】
前記ステップＡ１６２において、認証用装置１４０の認証制御モジュール１４３は、端末固有情報が一致しないと判定した場合にはステップＡ１８に進む。
一方、前記ステップＡ１６２において、端末固有情報が一致すると判定した場合（第２の認証動作実行機能による第２の認証動作によって前記情報端末を認証した場合）には、前記管理装置に対する前記情報端末からのアクセス要求を許容する第２段階をクリアしたことになる（ｂ級アクセス許容機能）。
そして、前記ステップＡ１６２において、端末固有情報が一致すると判定した場合には、認証用装置１４０の認証制御モジュール１４３は、第３の認証としてユーザ情報が一致するか否かの判定を行う（図５ステップＡ１６３：第３の認証ステップないしは第３の認証機能又は第３の認証動作実行機能）。
この第３の認証では、クライアント用計算機１２０から送信されてきたユーザ情報と、認証用装置１４０に予め登録された登録ユーザ情報（既登録ユーザ情報）とを照合する。
【０１０１】
前記ステップＡ１６３において、認証用装置１４０の認証制御モジュール１４３は、ユーザ情報が一致しないと判定した場合にはステップＡ１８に進む。
一方、前記ステップＡ１６３において、ユーザ情報が一致すると判定した場合（第３の認証動作実行機能による第３の認証動作によって前記情報端末のユーザを認証した場合）には、前記管理装置に対する前記情報端末からのアクセス要求を許容する第３段階をクリアしたことになる（ｃ級アクセス許容機能）。
そして、前記ステップＡ１６３において、ユーザ情報が一致すると判定した場合、認証

用装置１４０の認証制御モジュール１４３は、ステップＡ１７に進む。

【０１０２】

次に、認証用装置４０は、ステップＡ１６（ステップＡ１６１、Ａ１６２、Ａ１６３）において媒体固有情報データテーブル１４２、端末固有情報データテーブル１４６、ユーザ情報データテーブル１４４に一致する情報があると判定した場合には、クライアント用計算機２０からサーバ用計算機３０へのアクセス（アクセス要求）を許可する処理を行う（図４に示すステップＡ１７：アクセス許可制御ステップないしはアクセス許可制御機能）。

【０１０３】

一方、認証用装置４０は、ステップＡ１６（ステップＡ１６１、Ａ１６２、Ａ１６３）においてステップＡ１６において一つの条件でも一致する情報が存在しないと判定した場合には、サーバ用計算機３０への接続を不許可とする処理を行う（図４ステップＡ１７：アクセス不許可制御ステップないしはアクセス不許可制御機能）。

【０１０４】

ここで、以上のステップＡ１６ないしステップＡ１８からなるステップは、認証制御ステップないしは認証制御機能の一例である。

また、以上のステップＡ１５は、受信制御ステップないしは受信制御機能をその内容とする。

前記認証制御機能では、前記第１の認証が成功した場合に前記端末固有情報と予め登録された登録端末固有情報とに基づいて第２の認証をし、この第２の認証が成功した場合に前記アクセス要求を許可する機能を備えてよい。

【０１０５】

また、前記受信制御機能では、前記情報端末から入力されるユーザ情報を取得した前記外部記憶装置付きの情報端末から送信された前記ユーザ情報とともに前記端末固有情報及び前記媒体固有情報を受信制御する機能を備えてよい。

この場合、前記認証制御機能では、前記第２の認証が成功した場合に前記ユーザ情報と予め登録された登録ユーザ情報とに基づいて第３の認証をし、この第３の認証が成功した場合に前記アクセス要求を許可する機能を備えてよい。

【０１０６】

さらに、前記認証制御機能では、前記第３の認証をユーザ名及びパスワードによるユーザ認証、公開鍵認証、およびバイオメトリクス認証を組み合わせて行い、これらの各認証が成功した場合に前記アクセスを許可する機能を備えてよい。

【０１０７】

さらに、以上のステップＡ１２、ステップＡ１３からなるステップは、情報取得ステップないしは情報取得機能の一例ということもできる。さらにまた、以上のステップＡ１４は、端末用制御ステップないしは端末用制御機能の一例である。

また、前記第１の認証、第２の認証、第３の認証は、必ずしも３つ行う必要はなく、前記第１の実施形態のように第１の認証のみ、第１の認証と第２の認証のみであってもよい。この場合、前記ステップA１４のアクセス要求送信機能（端末用制御機能）においては、記憶された媒体固有情報を認証データとして前記情報端末を介して前記管理装置に向けて送信制御する第０送信制御機能、前記媒体固有情報とともに前記情報端末用の端末固有情報を認証データとして前記情報端末を介して前記管理装置に向けて送信する第１送信制御機能、前記情報端末に外部入力されるユーザ情報を前記媒体固有情報及び前記端末固有情報とともに認証データとして前記管理装置に向けて送信制御する第２送信制御機能のそれぞれの場合を備えてよい。

【０１０８】

ここで、本実施の形態では、ユーザ名パスワードのユーザ認証を扱ったが、公開鍵認証やバイオメトリクス認証など既存の認証方法と組み合わせることも可能である。

バイオメトリクス認証としては、例えば指紋認証、掌形（手のひらの幅や指の長さ）認証、網膜（目の網膜の毛細血管のパターンの認識）認証、虹彩認証、顔認証、血管（静脈

パターン）認証、音声（声紋）認証、耳形認証、ＤＮＡ認証、筆跡認証、キーストローク（打鍵の速度やタイミングの癖）認証、リップムーブメント認証、まばたき（黒目領域の変化量）認証などが挙げられる。

【０１０９】

その他の構成およびその他のステップないしは機能並びにその作用効果については、前述した実施の形態の場合と同一となっている。また、上記の説明において、上述した各ステップの動作内容及び各部の構成要素並びにそれらによる各機能をプログラム化（ソフトウエアプログラム）し、コンピュータに実行させてもよい。

【０１１０】

この場合、情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続（又は着脱自在に装着）し、この外部記憶装置付きの情報端末と通信可能に形成され前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置が備えたコンピュータに諸機能を実現させることが可能な管理装置用認証制御プログラムとすることができる。

また、管理装置と通信可能な情報端末と接続（又は着脱自在に装着）され前記情報端末を外部から制御可能な外部記憶装置を用いて、この外部記憶装置付きの前記情報端末からの前記管理装置に対するアクセス要求を前記管理装置にて認証するため、外部記憶装置付きの前記情報端末が備えたコンピュータに諸機能を実現させることが可能な外部記憶装置用認証制御プログラムとすることができる。

【０１１１】

さらに、以上説明した方法は、コンピュータがプログラムを記録媒体から読み込んで実行することによっても実現することが出来る。すなわち、上述のプログラムを、情報記録媒体に記録した構成であってもよい。

【０１１２】

[その他の各種変形例]

また、本発明にかかる装置及び方法は、そのいくつかの特定の実施の形態に従って説明してきたが、本発明の主旨および範囲から逸脱することなく本発明の本文に記述した実施の形態に対して種々の変形が可能である。

【０１１３】

例えば、上記構成部材の数、位置、形状等は上記実施の形態に限定されず、本発明を実施する上で好適な数、位置、形状等にすることができる。すなわち、上記実施の形態では、情報端末に接続される外部記憶装置が１個の場合を示したが、本発明は、これらの個数を制限するものではなく、ＵＳＢメモリ、ＣＦカード、ＣＤ－ＲＯＭ、ＤＶＤ、外付けＨＤＤなど複数の外部記憶装置（各々に同一種類又は異なる種類のＯＳなどを有する）が情報端末に接続される場合であってもよい。

【０１１４】

外部記憶装置としては、例えばＲＯＭ、ＲＡＭ、フラッシュメモリやＳＲＡＭ等の半導体メモリ並びに集積回路、あるいはそれらを含むＵＳＢメモリやメモリカードなどのリムーバブルメディアや、光ディスク、光磁気ディスク、磁気記録媒体等を用いてよく、さらに、フレキシブルディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＦＤ、ＤＶＤＲＯＭ、ＨＤＤＶＤ（ＨＤＤＶＤ－Ｒ－ＳＬ＜1層＞、ＨＤＤＶＤ－Ｒ－ＤＬ＜２層＞、ＨＤＤＶＤ－ＲＷ－ＳＬ、ＨＤＤＶＤ－ＲＷ－ＤＬ、ＨＤＤＶＤ－ＲＡＭ－ＳＬ）、ＤＶＤ±Ｒ－ＳＬ、ＤＶＤ±Ｒ－ＤＬ、ＤＶＤ±ＲＷ－ＳＬ、ＤＶＤ±ＲＷ－ＤＬ、ＤＶＤ－ＲＡＭ、Ｂｌｕ－Ｒａｙ　Ｄｉｓｋ＜登録商標＞（ＢＤ－ＲＳＬ、ＢＤ－Ｒ－ＤＬ、ＢＤ－ＲＥ－ＳＬ、ＢＤ－ＲＥ－ＤＬ）、ＭＯ、ＺＩＰ、磁気カード、磁気テープ、ＳＤカード、メモリスティック、不揮発性メモリカード、ＩＣカード、等の可搬媒体、外付けハードディスク等の記憶装置、その他これに類するもの等にて構成して用いてよい。

【０１１５】

また、本発明の一実施形態にかかる管理装置は、情報端末を外部から制御可能な外部記憶装置を前記情報端末に接続し、この外部記憶装置付きの情報端末と通信可能に形成され

前記情報端末からのアクセス要求に対しては当該アクセス要求にかかる機器に対する認証を前提として許容する認証機能を備えた管理装置であって、前記外部記憶装置を識別するために予め登録された登録媒体固有情報を記憶した登録媒体固有情報記憶手段と、予め前記外部記憶装置に記憶された媒体固有情報を取得した前記外部記憶装置付きの情報端末にから送信された前記媒体固有情報を受信し、この媒体固有情報と前記登録媒体固有情報とに基づいて第１の認証をし、この第１の認証が成功した場合に前記外部記憶装置付きの情報端末からの前記管理装置に対するアクセス要求を許可する管理側制御手段とを含む。

【０１１６】

さらに、本発明の一実施形態にかかる外部記憶装置は、管理装置と通信網を介して通信可能な情報端末と接続され前記情報端末を外部から制御可能な外部記憶装置であって、自身を識別する媒体固有情報を記憶した媒体固有情報記憶手段と、前記媒体固有情報を利用した前記情報端末から前記管理装置へのアクセス要求に関する第１の認証を前記管理装置にて行なうために、自身を前記情報端末に接続された状態で前記情報端末を起動し前記媒体固有情報を取得して前記情報端末を介して前記管理装置に向けて送信制御する端末用制御手段と、を含む。

【０１１７】

また、上記実施の形態における認証システムにおいて、情報端末と管理装置との間の通信構造は、クライアントサーバーシステムに限らず、サーバを介さずに端末同士がネットワークを組み、相互にデータを送受信するピアツーピア（Ｐｅｅｒ　Ｔｏ　Ｐｅｅｒ）通信によるシステムであってもよい。その際、管理装置は、ピア・ツゥ・ピア方式におけるマスタ端末であってもよい。

【０１１８】

また、前記実施の形態における「システム」とは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない。

【０１１９】

さらに、本明細書において、フローチャートに示されるステップは、記載された手順に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理を含むものである。また、プログラム手順（ステップ）が実行される順序を変更することもできる。

例えば、第１の認証、第２の認証、第３の認証、その他の認証は必ずしもこの順である必要はない。

【０１２０】

さらに、「通信」では、無線通信および有線通信は勿論、無線通信と有線通信とが混在した通信、即ち、ある区間では無線通信が行われ、他の区間では有線通信が行われるようなものであってもよい。さらに、ある装置から他の装置への通信が有線通信で行われ、他の装置からある装置への通信が無線通信で行われるようなものであってもよい。

【０１２１】

また、外部記憶装置と情報端末との間の通信構造において形成されるインタフェースの種類は、例えばパラレルインタフェース、ＵＳＢインタフェース、ＩＥＥＥ１３９４、ＬＡＮやＷＡＮ等のネットワークやその他これに類するもの、もしくは今後開発される如何なるインタフェースであっても構わない。

【０１２２】

さらに、このような各外部記憶装置、認証用装置は、単独で存在する場合もあるし、ある機器（例えば電子機器など）に組み込まれた状態で利用されることもあるなど、発明の思想としてはこれに限らず、各種の態様を含むものである。

さらにまた、一部がソフトウェアであって、一部がハードウェアで実現されている場合であってもよく、一部を記憶媒体上に記憶しておいて必要に応じて適宜読み込まれるような形態のものとしてあってもよい。

【０１２３】

また、発明の範囲は、図示例に限定されないものとする。さらに、上記各実施の形態に

は種々の段階が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。つまり、上述の各実施の形態同士、あるいはそれらのいずれかと各変形例のいずれかとの組み合わせによる例をも含む。

【産業上の利用可能性】

【０１２４】

本発明は、コンピュータシステム全般にて利用可能であり、より詳細には、シンクライアントシステムなどのセキュリティ的にユーザや接続する端末を限定する必要があるクライアント・サーバシステムで、クライアントを持ち運び可能な外部記憶装置に格納したオペレーティングシステムから起動する場合に利用できる。

また、不正アクセスや不正複製ソフトウェアによるサーバ資産の利用を防ぐことが必要な分野に利用できる。

【図面の簡単な説明】

【０１２５】

【図１】本発明の第１の実施の形態による認証システムの全体構成の一例を示すブロック図である。

【図２】本発明の第１の実施の形態による認証システムにおける処理手順の一例を示すフローチャートである。

【図３】本発明の第２の実施の形態による認証システムの全体構成の一例を示すブロック図である。

【図４】本発明の第２の実施の形態による認証システムにおける処理手順の一例を示すフローチャートである。

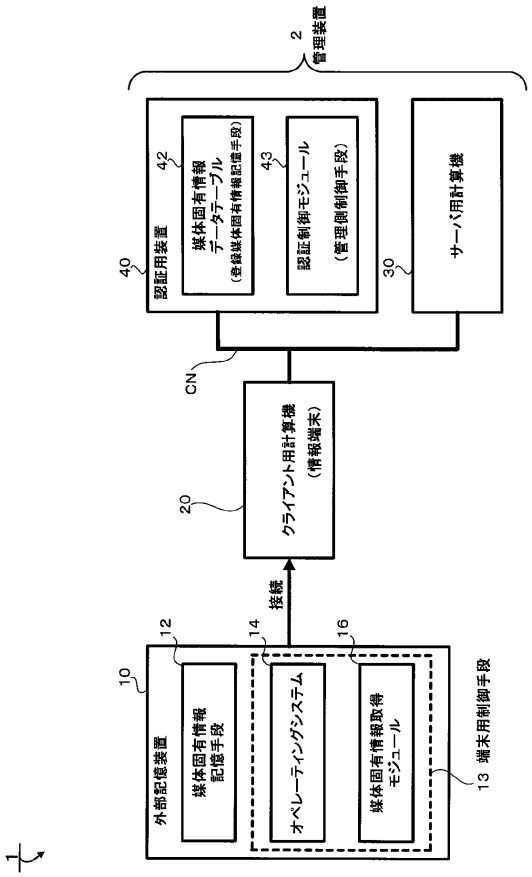
【図５】図４の処理手順の詳細処理手順の一例を示すフローチャートである。

【符号の説明】

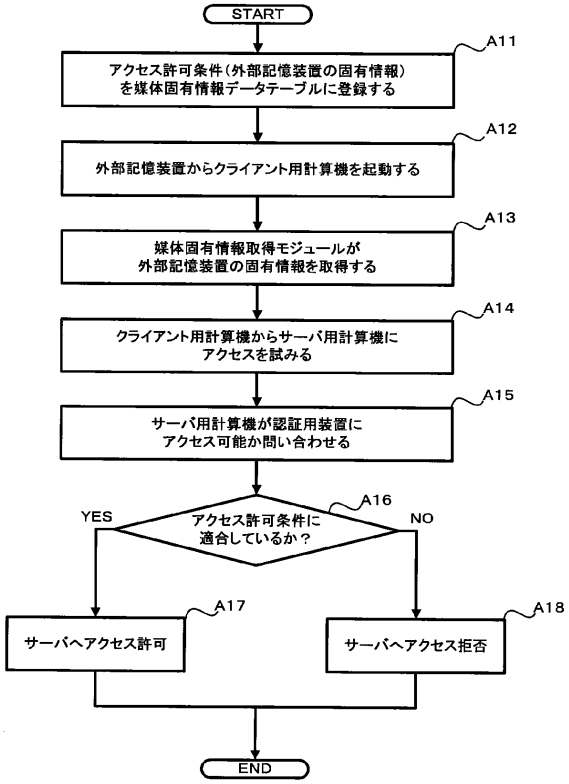
【０１２６】

１、１００　認証システム
２、１０２　管理装置
１０、１１０　外部記憶装置
１２、１１２　媒体固有情報記憶手段
１３、１１３　端末用制御手段
１４、１１４　オペレーティングシステム
１６、１１６　媒体固有情報取得モジュール
２０、１２０　クライアント用計算機（情報端末）
３０、１３０　サーバ用計算機（管理装置）
４０、１４０　認証用装置（管理装置）
４２、１４２　媒体固有情報データテーブル（登録媒体固有情報記憶手段）
４３、１４３　認証制御モジュール（管理側制御手段）
１１８　端末固有情報取得モジュール
１２２　端末固有情報記憶手段
１４４　ユーザ情報データテーブル（ユーザ情報記憶手段）
１４６　端末固有情報データテーブル（登録端末固有情報記憶手段）

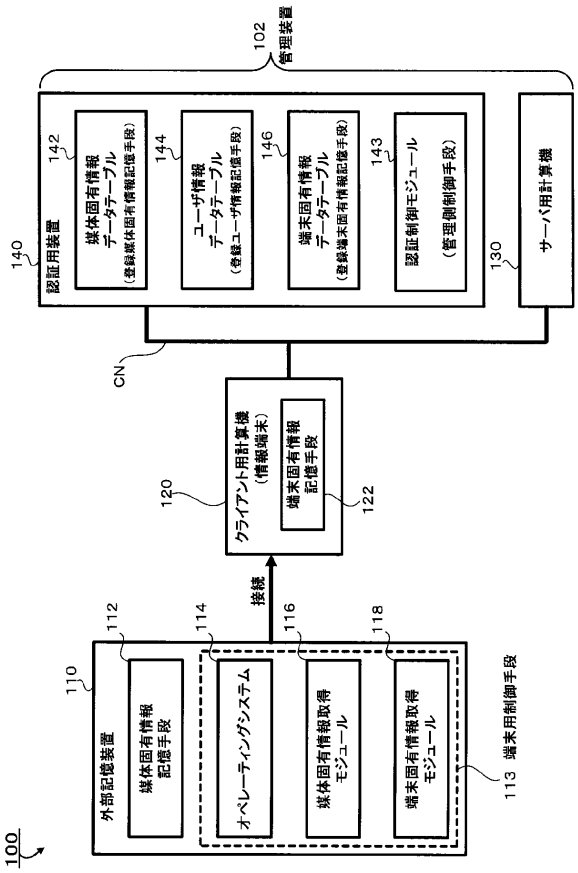
【図１】


2
管理装置
認証用装置
42
媒体固有情報
データテーブル
（登録媒体固有情報記憶手段）
43
認証制御モジュール
（管理側制御手段）
40
30
サーバ用計算機
CN
20
クライアント用計算機
（情報端末）
接続
12
14
16
10
外部記憶装置
媒体固有情報
記憶手段
オペレーティングシステム
媒体固有情報取得
モジュール
13 端末用制御手段
1

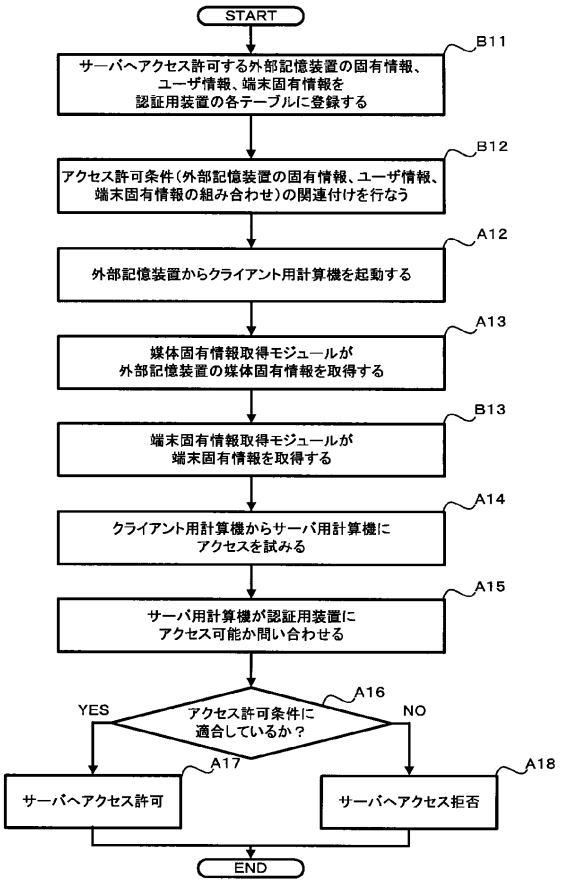
【図２】


START
A11
アクセス許可条件（外部記憶装置の固有情報）
を媒体固有情報データテーブルに登録する
A12
外部記憶装置からクライアント用計算機を起動する
A13
媒体固有情報取得モジュールが
外部記憶装置の固有情報を取得する
A14
クライアント用計算機からサーバ用計算機に
アクセスを試みる
A15
サーバ用計算機が認証用装置に
アクセス可能か問い合わせる
A16
YES
アクセス許可条件に
適合しているか？
NO
A17
サーバへアクセス許可
A18
サーバへアクセス拒否
END

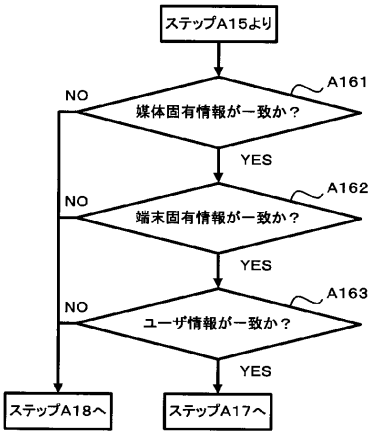
【図３】


102
管理装置
認証用装置
142
媒体固有情報
データテーブル
（登録媒体固有情報記憶手段）
144
ユーザ情報
データテーブル
（登録ユーザ情報記憶手段）
146
端末固有情報
データテーブル
（登録端末固有情報記憶手段）
143
認証制御モジュール
（管理側制御手段）
140
130
サーバ用計算機
CN
120
クライアント用計算機
（情報端末）
端末固有情報
記憶手段
122
接続
112
114
116
118
110
外部記憶装置
媒体固有情報
記憶手段
オペレーティングシステム
媒体固有情報取得
モジュール
端末固有情報取得
モジュール
113 端末用制御手段
100

【図４】


START
B11
サーバへアクセス許可する外部記憶装置の固有情報、
ユーザ情報、端末固有情報を
認証用装置の各テーブルに登録する
B12
アクセス許可条件（外部記憶装置の固有情報、ユーザ情報、
端末固有情報の組み合わせ）の関連付けを行なう
A12
外部記憶装置からクライアント用計算機を起動する
A13
媒体固有情報取得モジュールが
外部記憶装置の媒体固有情報を取得する
B13
端末固有情報取得モジュールが
端末固有情報を取得する
A14
クライアント用計算機からサーバ用計算機に
アクセスを試みる
A15
サーバ用計算機が認証用装置に
アクセス可能か問い合わせる
A16
YES
アクセス許可条件に
適合しているか？
NO
A17
サーバへアクセス許可
A18
サーバへアクセス拒否
END

【図５】


ステップA15より
A161
NO
媒体固有情報が一致か？
YES
A162
NO
端末固有情報が一致か？
YES
A163
NO
ユーザ情報が一致か？
YES
ステップA18へ
ステップA17へ