(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2008-97205
(P2008-97205A)
(43)公開日　平成20年4月24日(2008.4.24)

(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)	G06K	17/00	T	5B285
H04L 9/32	(2006.01)	H04L	9/00	673E	5J104
		G06K	17/00	V	

審査請求 未請求　請求項の数 8　ＯＬ　（全 29 頁）

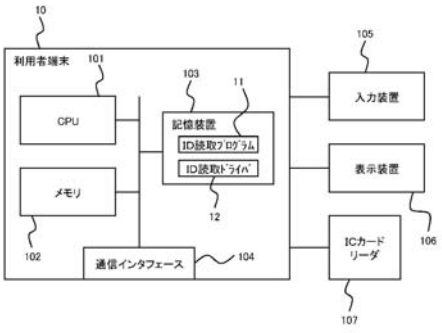
(21)出願番号　特願2006-276665 (P2006-276665)
(22)出願日　平成18年10月10日 (2006.10.10)

(71)出願人　000211307
中国電力株式会社
広島県広島市中区小町４番３３号
(74)代理人　110000176
一色国際特許業務法人
(72)発明者　浜田　浩和
広島県広島市中区小町４番３３号　中国電力株式会社内

Ｆターム(参考)　5B058 CA01 KA02 KA31 KA37
5B285 AA04 CB07 CB64
5J104 AA07 AA16 EA03 EA22 KA01 KA02 KA04 NA05 NA27 NA35 NA36 NA38

(54)【発明の名称】認証システムおよび認証方法

(57)【要約】　（修正有）
【課題】サーバ側からクライアント側のＩＣカードに記録されているデータを取得して認証を行うことができるようにする。
【解決手段】利用者端末１０は、ＩＣカードから利用者ＩＤを読み取るＩＣカードリーダ１０７と、ＩＣカードリーダ１０７を制御してＩＣカードから利用者ＩＤを読み取るためのＩＤ読取プログラム１１を記憶する記憶装置１０３とを備える。サービスを提供するポータルサーバは、ＩＤ読取プログラム１１を起動させるコマンドを含む認証画面データを利用者端末１０に送信し、利用者端末１０は、認証画面データに含まれるコマンドに応じて、ＩＤ読取プログラム１１を起動してＩＣカードリーダ１０７から利用者ＩＤを取得し、取得した利用者ＩＤをポータルサーバに送信する。ポータルサーバは、利用者端末１０から送信される利用者ＩＤに基づいて利用者の認証を行う。
【選択図】図６



【特許請求の範囲】
【請求項１】
利用者の認証システムであって、
利用者が操作するクライアント装置と、
利用者の認証を行うサーバ装置とを含んで構成され、
前記クライアント装置は、
利用者を特定する利用者ＩＤを記憶するＩＣカードから前記利用者ＩＤを読み取るＩＣカードリーダと、
前記ＩＣカードリーダを制御して前記ＩＣカードから前記利用者ＩＤを読み取るためのＩＤ読取プログラムを記憶する記憶装置と、
を備え、
前記サーバ装置は、前記ＩＤ読取プログラムを起動させる命令を含む画面データである認証画面データを前記クライアント装置に送信する認証画面データ送信部を備え、
前記クライアント装置は、
前記認証画面データを受信する認証画面データ受信部と、
前記認証画面データに含まれている前記命令に応じて、前記ＩＤ読取プログラムを起動し、前記ＩＤ読取プログラムにより前記ＩＣカードリーダから読み取られた前記利用者ＩＤを取得し、取得した前記利用者ＩＤを前記サーバ装置に送信する利用者ＩＤ送信部と、を備え、
前記サーバ装置は、
前記クライアント装置から前記利用者ＩＤを受信する利用者ＩＤ受信部と、
受信した前記利用者ＩＤに基づいて利用者の認証を行う利用者認証部と、
を備え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であって、
前記クライアント装置が備える前記記憶装置は、前記利用者ＩＤ送信部を実現するプラグインプログラムを記憶しており、
前記認証画面データに含まれている前記命令には、前記プラグインプログラムを特定する情報が含まれており、
前記クライアント装置は、前記認証画面データに応じた画面を表示するとともに、前記命令によって特定される前記プラグインプログラムを起動する画面表示部を備えること、
を特徴とする認証システム。
【請求項３】
請求項１に記載の認証システムであって、
前記サーバ装置は、
前記利用者ＩＤを表示するとともに利用者の認証情報を入力する認証画面を表示するための認証画面データを前記クライアント装置に送信する認証画面データ送信部を備え、
前記クライアント装置は、
前記認証画面データに基づいて前記認証画面を表示する認証画面表示部と、
前記認証画面を介して前記認証情報の入力を受け付ける認証情報入力部と、
前記認証情報を前記サーバ装置に送信する認証情報送信部と、
を備え、
前記利用者認証部は、前記利用者ＩＤと、前記クライアント装置から受信した前記認証情報とに基づいて利用者の認証を行うこと、
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であって、
前記サーバ装置は、他の利用者の前記利用者ＩＤに基づく認証を行う権限を有する利用者を特定する前記利用者ＩＤを記憶する特殊権限者記憶部を備え、
前記利用者ＩＤ受信部が受信した前記利用者ＩＤが前記特殊権限者記憶部に登録されて

いる場合、
前記認証画面データ送信部は、前記利用者ＩＤおよび前記認証情報の両方を入力する前記認証画面を表示するための前記認証画面データを前記クライアント装置に送信し、
前記利用者認証部は、前記クライアント装置から受信した、前記認証画面に入力された前記利用者ＩＤおよび前記認証情報に基づいて利用者の認証を行うこと、
を特徴とする認証システム。
【請求項５】
請求項１に記載の認証システムであって、
前記サーバ装置は、
利用者に一時的に貸与された前記ＩＣカードに記憶されている第１の前記利用者ＩＤと、利用者が所有する前記ＩＣカードに記憶されている第２の前記利用者ＩＤとを対応付けて記憶する貸与情報データベースと、
前記利用者ＩＤ受信部が受信した前記利用者ＩＤが所定の条件を満たすかどうかにより、前記ＩＣカードが利用者に一時的に貸与されたものであるかどうかを判定する貸与判定部と、
前記ＩＣカードが利用者に一時的に貸与されたものであると判定した場合には、前記クライアント装置から受信した前記利用者ＩＤに対応する前記第２の利用者ＩＤを前記貸与情報データベースから読み出し、読み出した前記第２の利用者ＩＤを前記利用者ＩＤとする利用者ＩＤ取得部と、
を備えることを特徴とする認証システム。
【請求項６】
請求項１に記載の認証システムであって、
前記利用者ＩＤ送信部は所定の前記サーバ装置にのみ前記利用者ＩＤを送信すること、
を特徴とする認証システム。
【請求項７】
請求項１に記載の認証システムであって、
前記クライアント装置は、利用者の認証を行うように指示する認証要求を前記サーバ装置に送信する認証要求送信部を備え、
前記サーバ装置は、
前記クライアント装置に付与されているアドレスに対応付けて、前記利用者ＩＤを記憶するアドレス管理テーブルと、
前記認証要求の送信元となる前記クライアント装置の前記アドレスを取得するアドレス取得部と、
を備え、
前記利用者認証部は、取得した前記アドレスに対応する前記利用者ＩＤが前記アドレス管理テーブルに登録されている場合には、前記アドレスに対応する前記利用者ＩＤに基づいて利用者の認証を行うこと、
を特徴とする認証システム。
【請求項８】
利用者が操作するクライアント装置と、利用者の認証を行うサーバ装置とを含んで構成される認証システムにおける利用者の認証方法であって、
前記クライアント装置は、
利用者を特定する利用者ＩＤを記憶するＩＣカードから前記利用者ＩＤを読み取るＩＣカードリーダと、
前記ＩＣカードリーダを制御して前記ＩＣカードから前記利用者ＩＤを読み取るためのＩＤ読取プログラムを記憶する記憶装置と、
を備えており、
前記サーバ装置が、前記ＩＤ読取プログラムを起動させる命令を含む画面データである認証画面データを前記クライアント装置に送信し、
前記クライアント装置が、前記認証画面データを受信し、

前記クライアント装置が、前記認証画面データに含まれている前記命令に応じて、前記ＩＤ読取プログラムを起動し、前記ＩＤ読取プログラムにより前記ＩＣカードリーダから読み取られた前記利用者ＩＤを取得し、取得した前記利用者ＩＤを前記サーバ装置に送信し、

前記サーバ装置が、前記クライアント装置から前記利用者ＩＤを受信し、

前記サーバ装置が、受信した前記利用者ＩＤに基づいて利用者の認証を行うこと、

を特徴とする認証方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、認証システムおよび認証方法に関する。

【背景技術】

【０００２】

近年、コンピュータシステムにおけるセキュリティを向上すべく、耐タンパ性のあるＩＣ（Integrated Circuit）カードが利用者の認証に用いられている。例えば、特許文献１には、ＩＣカードにホストコンピュータへのアクセスコードを格納することで、ホストコンピュータへの不正アクセスを防止するとともに、使用者のキー入力を低減する仕組みが提案されている。

【特許文献１】特開平７－２００４８１号公報

【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、特許文献１に記載のシステムでは、サーバ側のホストコンピュータからクライアント側のＩＣカードにアクセスすることは考慮されておらず、サーバ側においてＩＣカードに記録されているデータを取得して利用者の認証を行うことはできない。

【０００４】

本発明は、このような背景を鑑みてなされたものであり、サーバ側からクライアント側のＩＣカードに記録されているデータを取得して認証を行うことのできる認証システムおよび認証方法を提供することを目的とする。

【課題を解決するための手段】

【０００５】

上記課題を解決するための本発明のうち請求項１に記載の発明は、利用者の認証システムであって、利用者が操作するクライアント装置と、利用者の認証を行うサーバ装置とを含んで構成され、前記クライアント装置は、利用者を特定する利用者ＩＤを記憶するＩＣカードから前記利用者ＩＤを読み取るＩＣカードリーダと、前記ＩＣカードリーダを制御して前記ＩＣカードから前記利用者ＩＤを読み取るためのＩＤ読取プログラムを記憶する記憶装置と、を備え、前記サーバ装置は、前記ＩＤ読取プログラムを起動させる命令を含む画面データである認証画面データを前記クライアント装置に送信する認証画面データ送信部を備え、前記クライアント装置は、前記認証画面データを受信する認証画面データ受信部と、前記認証画面データに含まれている前記命令に応じて、前記ＩＤ読取プログラムを起動し、前記ＩＤ読取プログラムにより前記ＩＣカードリーダから読み取られた前記利用者ＩＤを取得し、取得した前記利用者ＩＤを前記サーバ装置に送信する利用者ＩＤ送信部と、を備え、前記サーバ装置は、前記クライアント装置から前記利用者ＩＤを受信する利用者ＩＤ受信部と、受信した前記利用者ＩＤに基づいて利用者の認証を行う利用者認証部と、を備えることとする。

【０００６】

本発明の認証システムによれば、サーバ装置から送信される認証画面データに基づいてクライアント装置においてＩＤ読取プログラムが起動されるので、サーバ装置からクライアント装置におけるＩＣカードへのアクセスを制御することができる。すなわち、サーバ装置は、クライアント装置１０が備えるＩＣカードリーダを利用して、ＩＣカードに記録

されている利用者ＩＤを取得し、取得した利用者ＩＤに基づいて利用者の認証を行うことができる。

【０００７】

また、本発明のうち請求項２に記載の発明は、請求項１に記載の認証システムであって、前記クライアント装置が備える前記記憶装置は、前記利用者ＩＤ送信部を実現するプラグインプログラムを記憶しており、前記認証画面データに含まれている前記命令には、前記プラグインプログラムを特定する情報が含まれており、前記クライアント装置は、前記認証画面データに応じた画面を表示するとともに、前記命令によって特定される前記プラグインプログラムを起動する画面表示部を備えることとする。

【０００８】

また、本発明のうち請求項３に記載の発明は、請求項１に記載の認証システムであって、前記サーバ装置は、前記利用者ＩＤを表示するとともに利用者の認証情報を入力する認証画面を表示するための認証画面データを前記クライアント装置に送信する認証画面データ送信部を備え、前記クライアント装置は、前記認証画面データに基づいて前記認証画面を表示する認証画面表示部と、前記認証画面を介して前記認証情報の入力を受け付ける認証情報入力部と、前記認証情報を前記サーバ装置に送信する認証情報送信部と、を備え、前記利用者認証部は、前記利用者ＩＤと、前記クライアント装置から受信した前記認証情報とに基づいて利用者の認証を行うこととする。

この場合、ＩＣカードに記録されている利用者ＩＤと、利用者本人のみが知るパスワードとの両方に基づいて利用者の認証を行うことができる。したがって、例えば他人のＩＣカードを利用して利用者になりすまして認証を受けようとしても、パスワードを知らなければ認証を受けることができないので、他人のＩＣカードを悪用した、いわゆる「なりすまし」を防ぐことができる。

【０００９】

また、本発明のうち請求項４に記載の発明は、請求項３に記載の認証システムであって、前記サーバ装置は、他の利用者の前記利用者ＩＤに基づく認証を行う権限を有する利用者を特定する前記利用者ＩＤを記憶する特殊権限者記憶部を備え、前記利用者ＩＤ受信部が受信した前記利用者ＩＤが前記特殊権限者記憶部に登録されている場合、前記認証画面データ送信部は、前記利用者ＩＤおよび前記認証情報の両方を入力する前記認証画面を表示するための前記認証画面データを前記クライアント装置に送信し、前記利用者認証部は、前記クライアント装置から受信した、前記認証画面に入力された前記利用者ＩＤおよび前記認証情報に基づいて利用者の認証を行うこととする。

【００１０】

また、本発明のうち請求項５に記載の発明は、請求項１に記載の認証システムであって、前記サーバ装置は、利用者に一時的に貸与された前記ＩＣカードに記憶されている第１の前記利用者ＩＤと、利用者が所有する前記ＩＣカードに記憶されている第２の前記利用者ＩＤとを対応付けて記憶する貸与情報データベースと、前記利用者ＩＤ受信部が受信した前記利用者ＩＤが所定の条件を満たすかどうかにより、前記ＩＣカードが利用者に一時的に貸与されたものであるかどうかを判定する貸与判定部と、前記ＩＣカードが利用者に一時的に貸与されたものであると判定した場合には、前記クライアント装置から受信した前記利用者ＩＤに対応する前記第２の利用者ＩＤを前記貸与情報データベースから読み出し、読み出した前記第２の利用者ＩＤを前記利用者ＩＤとする利用者ＩＤ取得部と、を備えることとする。

この場合、利用者がＩＣカードを忘れた場合でも、一時的に貸与したＩＣカードを利用して、その利用者の認証を行うことができる。

【００１１】

また、本発明のうち請求項６に記載の発明は、請求項１に記載の認証システムであって、前記利用者ＩＤ送信部は所定の前記サーバ装置にのみ前記利用者ＩＤを送信することとする。

この場合、クライアント装置において、認証画面データに基づかずに、ＩＤ読取プログ

ラムが不正に実行されたとしても、ＩＣカードから読み取られた利用者ＩＤは、所定のサーバ装置にのみ送信される。したがって、例えば、汎用的なプログラムが不正に利用されることにより、ＩＣカードに記録されているデータが他のコンピュータに送信されるようなことがないので、利用者ＩＤの漏洩リスクを低減することができる。

【００１２】

また、本発明のうち請求項７に記載の発明は、請求項１に記載の認証システムであって、前記クライアント装置は、利用者の認証を行うように指示する認証要求を前記サーバ装置に送信する認証要求送信部を備え、前記サーバ装置は、前記クライアント装置に付与されているアドレスに対応付けて、前記利用者ＩＤを記憶するアドレス管理テーブルと、前記認証要求の送信元となる前記クライアント装置の前記アドレスを取得するアドレス取得部と、を備え、前記利用者認証部は、取得した前記アドレスに対応する前記利用者ＩＤが前記アドレス管理テーブルに登録されている場合には、前記アドレスに対応する前記利用者ＩＤに基づいて利用者の認証を行うこととする。

この場合、サーバ装置では、クライアント装置のアドレスに応じて利用者の認証を行うことができるので、ＩＣカードから利用者ＩＤを読み出す処理に係る負荷を低減することができる。

【００１３】

その他本願が開示する課題やその解決方法については、発明の実施形態の欄及び図面により明らかにされる。

【発明の効果】

【００１４】

本発明によれば、サーバ側からクライアント側のＩＣカードに記録されているデータを取得して認証を行うことができる。

【発明を実施するための最良の形態】

【００１５】

以下、本発明の一実施形態である認証システムについて説明する。本実施形態の認証システムでは、Ｗｅｂによる情報処理サービスの提供に先だって、ＩＣカードを用いて利用者の認証を行うことを想定している。

【００１６】

ＩＣカードには、ＩＣカードの識別情報（以下、カードＩＤという。）が記憶されており、通常はＩＣカードに記憶されているカードＩＤを、そのＩＣカードを携帯する利用者を特定する識別情報（以下、利用者ＩＤという。）として用いるものとする。また、本実施形態では、貸出用のＩＣカード（以下、貸与カードという。）が準備されているものとし、利用者がＩＣカードを携帯し忘れた場合には、利用者に対して貸与カードが一時的に貸し出され、貸与カードを利用して利用者の認証が行われる。

【００１７】

利用者ＩＤは０～８の何れかから始まる英数字の文字列とする。一方、利用者がＩＣカードを携帯し忘れた場合にその利用者に一時的に貸与されるＩＣカードには、０～８以外の英数字で始まるカードＩＤが記録される。したがって、ＩＣカードに記録されているカードＩＤの頭１桁が０～８であるかどうかにより、ＩＣカードが一時的に貸与されたものかどうかが判断可能となっている。

【００１８】

＝＝システム構成＝＝

図１は、本実施形態に係る認証システムの全体構成を示す図である。本実施形態の認証システムは、利用者端末１０、ポータルサーバ２０、ＬＤＡＰサーバ３０、および管理者端末４０を含んで構成されている。利用者端末１０、ポータルサーバ２０、ＬＤＡＰサーバ３０、および管理者端末４０はそれぞれ通信ネットワーク５０に接続されており、互いに通信が可能となっている。通信ネットワーク５０は、例えば、イーサネット（登録商標）やＡＴＭ（Asynchronous Transfer Mode）ネットワーク、ＬＡＮ（Local Area Network）などである。

【００１９】
ポータルサーバ２０（本発明のサーバ装置に該当する。）は、利用者に対して情報処理サービスを提供する、例えば、パーソナルコンピュータやワークステーションなどのコンピュータである。ポータルサーバ２０は、ＨＴＴＰ（HyperText Transfer Protocol）リクエストに応答する、いわゆるＷｅｂアプリケーションの形態により情報処理サービスを提供する。本実施形態では、ポータルサーバ２０が提供する情報処理サービスは、各種の情報をまとめて表示するための画面データを生成するポータルサイトを提供することを想定している。ポータルサーバ２０は、情報処理サービスの提供前に利用者の認証を行う。ポータルサーバ２０が行う認証は、例えば、ユーザ名（利用者ＩＤ）とパスワードを用いる一般的なものである。

【００２０】
利用者端末１０（本発明のクライアント装置に該当する。）は、利用者が操作する例えばパーソナルコンピュータやワークステーション、携帯電話、ＰＤＡ（Personal Digital Assistant）などのコンピュータである。利用者端末１０は、ＨＴＴＰプロトコルによりポータルサーバ２０にアクセスするＷｅｂブラウザの機能を有しており、利用者は利用者端末１０のＷｅｂブラウザを操作してポータルサーバ２０が提供する情報処理サービスにアクセスする。

【００２１】
ＬＤＡＰサーバ３０は、利用者に関するディレクトリ情報を管理する、例えば、パーソナルコンピュータやワークステーションなどのコンピュータである。ＬＤＡＰサーバ３０は、ＬＤＡＰ（Lightweight Directory Access Protocol）に従って、ディレクトリ情報を提供する。ＬＤＡＰサーバ３０が管理するディレクトリ情報の一例を図２に示す。同図に示すように、ＬＤＡＰサーバ３０が管理するディレクトリ情報には、カードＩＤをキーとして、利用者のパスワード、利用者の姓名およびその読み仮名（カナ１、カナ２）、利用者が所属する部署等を示す所属コードおよび所属名、利用者の役職を示す役職コードおよび役職名、一時利用区分、ポータルＩＤ、オンラインＩＤ等が含まれている。一時利用区分は、利用者の区分を示す項目であり、「社員」「出向」および「一時利用」の何れかが設定される。利用者がＩＣカードを忘れて、貸与カードを一時的に貸与された場合などには、一時利用区分に「一時利用」が設定される。ポータルＩＤは、ＩＣカードを携帯している利用者を特定する利用者ＩＤである。通常カードＩＤとポータルＩＤとは一致するが、貸与カードでは、カードＩＤとポータルＩＤとは異なる。オンラインＩＤは、ポータルサーバ２０が提供する情報処理サービスのひとつとして、他のホストコンピュータにアクセスする場合に用いられるＩＤである。

【００２２】
管理者端末４０は、ＬＤＡＰサーバ３０に管理されるディレクトリ情報を管理する管理者が操作する、例えば、パーソナルコンピュータやワークステーション、携帯電話、ＰＤＡなどである。

【００２３】
本実施形態では、管理者には、ＬＤＡＰサーバ３０に管理されるディレクトリ情報の管理を行うＬＤＡＰ設定変更管理者と、ＩＣカードの管理を行うカード保管管理者とがいるものとする。利用者は、ＩＣカードを携帯し忘れた場合、カード保管管理者に届け出て、カード保管管理者から貸与カードの貸与を受ける。ＬＤＡＰ設定変更管理者は、貸与カードを貸し出した利用者を、後述するように、ＬＤＡＰサーバ３０に登録する。

【００２４】
＝＝管理者端末４０＝＝
図３は管理者端末４０のハードウェア構成を示す図である。同図に示すように管理者端末４０は、ＣＰＵ４０１、メモリ４０２、記憶装置４０３、通信インタフェース４０４、入力装置４０５、表示装置４０６、ＩＣカードリーダ４０７を備えている。
記憶装置４０３は、プログラムやデータを記憶する、例えば、ハードディスクドライブやＣＤ－ＲＯＭドライブ、フラッシュメモリなどである。ＣＰＵ４０１は、記憶装置４０

３に記憶されているプログラムをメモリ４０２に読み出して実行することにより、各種の機能を実現する。通信インタフェース４０４は、通信ネットワーク５０に接続するためのインタフェースである。通信インタフェース４０４は、例えば、イーサネット（登録商標）に接続するためのアダプタや、電話回線網に接続するためのモデムなどである。入力装置４０５は、ＬＤＡＰ設定変更管理者からデータの入力を受け付ける、例えば、キーボードやマウスなどである。表示装置４０６は、ＬＤＡＰ設定変更管理者に対して情報を表示する、例えば、ディスプレイである。ＩＣカードリーダ４０７は、接触型または非接触型のＩＣカードに記録されているデータを読み出す装置である。

【００２５】

図４は、管理者端末４０のソフトウェア構成を示す図である。同図に示すように、管理者端末４０は、貸与利用者入力部４１１、カードＩＤ取得部４１２、エントリ更新部４１３を備えている。

貸与利用者入力部４１１は、ＬＤＡＰ設定変更管理者から、入力装置４０５を介して、貸与カードを貸し出した利用者（以下、貸与利用者という。）の利用者ＩＤの入力を受け付ける。

カードＩＤ取得部４１２は、ＩＣカードリーダ４０７を介して、ＩＣカードに記憶されているカードＩＤを取得する。

エントリ更新部４１３は、カードＩＤ取得部４１２が取得したカードＩＤに対応するディレクトリ情報のポータルＩＤを、貸与利用者入力部４１１が受け付けた利用者ＩＤに更新する。エントリ更新部４１３は、ＬＤＡＰに規定される更新コマンド（changetype:modify replace:ポータルＩＤ）をＬＤＡＰサーバ３０に送信することにより、ＬＤＡＰサーバ３０で管理されているディレクトリ情報を更新する。

なお、貸与利用者入力部４１１、カードＩＤ取得部４１２、およびエントリ更新部４１３は、管理者端末４０が備えるＣＰＵ４０１が記憶装置４０３に記憶されているプログラムを実行することにより実現される。

【００２６】

本実施形態では、上述したように、利用者がＩＣカードを携帯し忘れた場合、カード保管管理者は利用者からの届出に応じて、貸与カードをその利用者に貸与する。ＬＤＡＰ設定変更管理者は、カード保管管理者が利用者に貸与カードを貸し出す前に、貸与カードに記録されているカードＩＤに対応するディレクトリ情報のポータルＩＤを、貸与先となる利用者の利用者ＩＤに更新する。図５は、貸与カードに対応するディレクトリ情報を更新する処理の流れを示す図である。

【００２７】

カードＩＤ取得部４１２は、ＩＣカードリーダ４０７を介してＩＣカードにアクセスできない場合には（Ｓ４４１：ＮＯ）、その旨のエラーを表示して（Ｓ４４７）、処理を終了する。

カードＩＤ取得部４１２は、ＩＣカードにアクセスできる場合（Ｓ４４１：ＹＥＳ）、ＩＣカードからカードＩＤを取得し（Ｓ４４２）、カードＩＤの先頭１桁が０～８であれば（Ｓ４４３：ＮＯ）、エラーを表示して（Ｓ４４７）、処理を終了する。

【００２８】

ＩＣカードのカードＩＤが０～８以外の英数字で始まっている場合（Ｓ４４３：ＹＥＳ）、貸与利用者入力部４１１は、キーボードやマウス等の入力装置１０５から、貸与カードの貸出先となる利用者を特定する利用者ＩＤの入力を受け付ける（Ｓ４４４）。

【００２９】

エントリ更新部４１３は、カードＩＤ取得部４１２が取得したカードＩＤをキーにして、ディレクトリ情報のポータルＩＤを、貸与利用者入力部４１１が受け付けた利用者ＩＤに更新するように指示する更新コマンドをＬＤＡＰサーバ３０に送信して、ディレクトリ情報を更新する（Ｓ４４５）。

【００３０】

以上のようにして、利用者に貸与カードが一時的に貸し出された場合には、貸与カード

のカードＩＤに対応するポータルＩＤには、その利用者の利用者ＩＤが設定されることになる。後述するように、貸与カードのカードＩＤに対応するポータルＩＤが利用者の認証に用いられるため、利用者がＩＣカードを携帯し忘れた場合でも、その利用者自身の利用者ＩＤを用いて認証を行うことができる。ポータルサイトでは、利用者ＩＤに応じて表示する情報を変化させる、いわゆるパーソナライゼーションが行われるが、利用者は常に自分自身の利用者ＩＤを利用してポータルサーバ２０のサービスを受けることができるので、ポータルサーバ２０によるパーソナライゼーションも適切に行われるようにすることができる。

【００３１】

＝＝利用者端末１０＝＝

図６は、利用者端末１０のハードウェア構成を示す図である。同図に示すように、利用者端末１０は、ＣＰＵ１０１、メモリ１０２、記憶装置１０３、通信インタフェース１０４、入力装置１０５、表示装置１０６、ＩＣカードリーダ１０７を備えている。

【００３２】

ＩＣカードリーダ１０７は、接触型または非接触型のＩＣカードに記憶されているデータを読み出す装置である。記憶装置１０３は、ＩＤ読取プログラム１１やＩＤ読取ドライバ１２などのプログラムや、プログラムの実行時に用いられる各種のデータを記憶する。記憶装置１０３には、例えば、ハードディスクドライブやＣＤ－ＲＯＭドライブ、フラッシュメモリなどを用いることができる。

【００３３】

ＩＤ読取ドライバ１２は、利用者端末１０で実行される各種のプログラムからＩＣカードリーダ１０７を介してデータを読み出すためのデバイスドライバプログラムである。ＩＤ読取プログラム１１は、ＩＤ読取ドライバ１２を用いてＩＣカードに記憶されているカードＩＤを読み出すためのプログラムである。ＩＤ読取プログラム１１は、例えば、ＡｃｔｉｖｅＸ（登録商標）コントロールや、Ｊａｖａ（登録商標）アプレットといった、利用者端末１０で動作するＷｅｂブラウザから呼び出されるプラグインプログラムである。

【００３４】

ＣＰＵ１０１は記憶装置１０３に記憶されているプログラムをメモリ１０２に読み出して実行することにより各種の機能を提供する。通信インタフェース１０４は、通信ネットワーク５０に接続するためのインタフェースであり、例えば、イーサネット（登録商標）に接続するためのアダプタや、公衆電話回線網に接続するためのモデムなどである。入力装置１０５、利用者からの操作を受け付ける、例えば、キーボードやマウスなどである。表示装置１０６は、利用者に対して情報を表示するディスプレイなどである。

【００３５】

図７は、利用者端末１０のソフトウェア構成を示す図である。同図に示すように、利用者端末１０は、認証要求送信部１１１、カードＩＤ取得画面受信部１１２、カードＩＤ取得部１１３、カードＩＤ送信部１１４、認証画面データ受信部１１５、認証情報入力部１１６、認証情報送信部１１７を備えている。

【００３６】

認証要求送信部１１１は、利用者の認証を行うように指示するコマンド（以下、認証要求という。）をポータルサーバ２０に送信する。本実施形態では、認証要求送信部１１１は、利用者の操作に応じて、ポータルサーバ２０上の所定のＵＲＬ（Uniform Resource Locator）に対するＨＴＴＰリクエストを認証要求としてポータルサーバ２０に送信するものとする。

【００３７】

カードＩＤ取得画面受信部１１２は、認証要求に応じてポータルサーバ２０から送信される、ＩＤ読取プログラム１１を起動するコマンドを含む画面データ（以下、カードＩＤ取得画面データという。）を受信する。なお、本実施形態では、カードＩＤ取得画面データはＨＴＭＬ（HyperText Markup Language）で記述されているものとし、カードＩＤ取得画面データに含まれるコマンドは、例えば、ＡｃｔｉｖｅＸ（登録商標）コントロール

やＪａｖａ（登録商標）アプレットなどのプラグインプログラムを起動するための、＜ＯＢＪＥＣＴ＞タグや＜ＥＭＢＥＤ＞タグなどである。利用者端末１０は、カードＩＤ取得画面データに基づく画面をＷｅｂブラウザに表示する際に、ＩＤ読取プログラム１１を起動することになる。

【００３８】

カードＩＤ取得部１１３は、ＩＣカードリーダ１０７を介してＩＣカードからカードＩＤを取得する。カードＩＤ送信部１１４（本発明の利用者ＩＤ送信部に該当する。）は、カードＩＤ取得部１１３が取得したカードＩＤを、例えば、ＨＴＴＰに規定されるＧＥＴ要求やＰＯＳＴ要求により、ポータルサーバ２０に送信する。なお、カードＩＤ取得部１１３およびカードＩＤ送信部１１４は、ＩＤ読取プログラム１１が実行されることにより実現される。

【００３９】

認証画面データ受信部１１５は、利用者を認証するための情報（以下、認証情報という。）の入力を受け付ける画面（以下、認証画面という。）を表示するための画面データ（以下、認証画面データという。）をポータルサーバ２０から受信する。なお、本実施形態では、認証情報はパスワードである。また、本実施形態では、後述するように、認証画面には、ＩＣカードから特定される利用者の利用者ＩＤの入力欄と、パスワードの入力欄とが含まれるが、管理者以外の利用者の認証時には、利用者ＩＤの入力欄は編集不能となる。

【００４０】

認証情報入力部１１６は、利用者からパスワードの入力を受け付ける。また、認証情報入力部１１６は、認証画面において利用者ＩＤの入力欄が編集可能になっている場合には、利用者ＩＤとパスワードとの両方の入力を受け付ける。

認証情報送信部１１７は利用者ＩＤとパスワードとをポータルサーバ２０に送信する。

【００４１】

なお、上述した認証要求送信部１１１、カードＩＤ取得画面受信部１１２、認証画面データ受信部１１５、認証情報入力部１１６、認証情報送信部１１７は、利用者端末１０が備えるＣＰＵ１０１が記憶装置１０３に記憶されているプログラム（不図示）を実行することにより実現される。

【００４２】

＝＝ポータルサーバ２０＝＝

図８は、ポータルサーバ２０のハードウェア構成を示す図である。同図に示すように、ポータルサーバ２０は、ＣＰＵ２０１、メモリ２０２、記憶装置２０３、通信インタフェース２０４、入力装置２０５、表示装置２０６を備えている。

【００４３】

記憶装置２０３は、データやプログラムを記憶する、例えば、ハードディスクドライブやＣＤ－ＲＯＭドライブ、フラッシュメモリなどである。ＣＰＵ２０１は、記憶装置２０３に記憶されているプログラムをメモリ２０２に読み出して実行することにより各種の機能を実現する。通信インタフェース２０４は、通信ネットワーク５０に接続するためのインタフェースであり、例えば、イーサネット（登録商標）に接続するためのアダプタや、公衆電話回線網に接続するためのモデムなどである。入力装置２０５、利用者からの操作を受け付ける、例えば、キーボードやマウスなどである。表示装置２０６は、利用者に対して情報を表示するディスプレイなどである。

【００４４】

図９は、ポータルサーバ２０のソフトウェア構成を示す図である。同図に示すように、ポータルサーバ２０は、認証要求受信部２１１、ＩＰアドレス認証部２１２、カードＩＤ取得画面送信部２１３、カードＩＤ受信部２１４、ディレクトリ情報取得部２１５、認証画面作成部２１６、認証画面データ送信部２１７、認証情報受信部２１８、認証処理部２１９、画面データ送信部２２０、アドレス管理テーブル２５１、管理者管理テーブル２５２を備えている。

【００４５】
アドレス管理テーブル２５１は、通信ネットワーク５０上における利用者端末１０のネットワーク上で端末を特定するためのアドレスと、その利用者端末１０を使用している利用者の利用者ＩＤとを含む情報（以下、アドレス管理情報という。）を記憶する。なお、本実施携帯において、利用者端末１０のアドレスは、ＩＰアドレスであるものとする。
【００４６】
図１０は、アドレス管理テーブル２５１に記憶されるアドレス管理情報の構成例を示す図である。同図に示すように、アドレス管理情報には、利用者端末１０のＩＰアドレスをキーとして、利用者ＩＤと、管理者フラグとが含まれている。管理者フラグは、利用者端末１０を使用する利用者が管理者であるかどうかを示す情報である。後述するように、利用者が管理者である場合には、他の利用者の利用者ＩＤを入力して、他の利用者としてポータルサーバ２０にアクセスすることができる。これにより、例えば、管理者が、通常業務においてポータルサーバ２０にアクセスする場合の利用者ＩＤと、管理業務においてポータルサーバ２０にアクセスする場合の利用者ＩＤとを変えているような場合に対応できるようにしている。
なお、アドレス管理テーブル２５１には、全ての利用者端末１０についてのアドレス管理情報が登録されていなくてもよい。
【００４７】
管理者管理テーブル２５２は、管理者を特定する利用者ＩＤを記憶する。本実施形態において、管理者は、他の利用者の利用者ＩＤに基づく認証を行う権限を有するものとする。図１１に管理者管理テーブル２５２の構成例を示す。同図に示すように、管理者管理テーブル２５２には利用者ＩＤが登録される。利用者ＩＤが管理者管理テーブル２５２に登録されているかどうかにより、利用者が管理者であるかどうかを判別することができる。
【００４８】
認証要求受信部２１１は、利用者端末１０から送信される認証要求を受信する。
ＩＰアドレス認証部２１２は、認証要求の送信元となる利用者端末１０のＩＰアドレスに対応するアドレス管理情報がアドレス管理テーブル２５１に登録されているかどうかを判定する。利用者端末１０のＩＰアドレスに対応するアドレス管理情報が登録されている場合には、後述するように、そのアドレス管理情報に含まれる利用者ＩＤを利用して利用者の認証が行われる。
【００４９】
カードＩＤ取得画面送信部２１３は、認証要求に応じてカードＩＤ取得画面データを作成し、作成したカードＩＤ取得画面データを利用者端末１０に送信する。
カードＩＤ受信部２１４（本発明の利用者ＩＤ受信部に該当する。）は、カードＩＤ取得画面データに応じて利用者端末１０からカードＩＤを受信する。利用者端末１０では、上述したように、ＩＣカード取得画面データに含まれるコマンドに応じてＩＤ読取プログラム１１が起動されて、ＩＣカードリーダ１０７を介してＩＣカードからカードＩＤが読み取られる。
【００５０】
ディレクトリ情報取得部２１５は、利用者端末１０から受信したカードＩＤに対応するディレクトリ情報をＬＤＡＰサーバ３０から取得する。また、ディレクトリ情報取得部２１５は、カードＩＤが貸与カードである場合（本実施形態では、カードＩＤの先頭１桁が０～８以外の英数字である場合）には、取得したディレクトリ情報に含まれるポータルＩＤに対応するディレクトリ情報を取得する。
【００５１】
認証画面作成部２１６は、利用者ＩＤの入力欄と、パスワードの入力欄とを備える認証画面を表示するための認証画面データを作成する。認証画面作成部２１６は、認証画面の利用者ＩＤの入力欄に、予めディレクトリ情報取得部２１５が取得したディレクトリ情報のカードＩＤを設定する。認証画面作成部２１６は、利用者が管理者である場合、すなわち利用者ＩＤが管理者管理テーブル２５２に登録されている場合には、利用者ＩＤの入力

欄が編集可能になるようにし、それ以外の利用者については利用者ＩＤの入力欄は編集不能になるように認証画面データを作成する。

認証画面データ送信部２１７は、認証画面作成部２１６が作成した認証画面データを利用者端末１０に送信する。

【００５２】

認証情報受信部２１８は、利用者端末１０から送信される認証情報を受信する。本実施形態では、認証情報受信部２１８は、利用者端末１０から利用者ＩＤとパスワードとを受信する。

【００５３】

認証処理部２１９は、認証情報受信部２１８が受信した認証情報を用いて利用者の認証を行う。本実施形態では、認証処理部２１９は、認証情報受信部２１８が受信した利用者ＩＤとパスワードとを用いて認証を行う。具体的には、認証処理部２１９は、利用者ＩＤに対応するディレクトリ情報のパスワードエントリをＬＤＡＰサーバ３０から取得し、取得したパスワードエントリの内容と、利用者端末１０から受信したパスワードとが一致するかどうかにより利用者の認証を行うことができる。

【００５４】

画面データ送信部２２０は、認証に成功した場合に、利用者に応じたポータルサイトを実現する画面データを利用者端末１０に送信する。また、認証に失敗した場合には、画面データ送信部２２０は、その旨を示すエラーメッセージを表示するための画面データを利用者端末１０に送信する。

【００５５】

＝＝処理＝＝

次に、本実施形態に係る認証システムにおいて、利用者の認証を行う仕組みについて説明する。図１２は、利用者を認証する処理の流れを示す図である。本実施形態の認証システムでは、まずＩＣカードからカードＩＤを取得し（Ｓ５０１）、取得したカードＩＤに基づいて利用者に対応するディレクトリ情報をＬＤＡＰサーバ３０から取得し（Ｓ５０２）、取得したディレクトリ情報に基づいて利用者の認証処理を行う（Ｓ５０３）。以下、詳細について説明する。

【００５６】

図１３は、ＩＣカードからカードＩＤを取得する処理の流れを示す図である。

利用者が利用者端末１０で動作するＷｅｂブラウザを操作してポータルサーバ２０にアクセスすると、利用者端末１０からは、所定のＵＲＬへのＨＴＴＰリクエストとして、認証要求がポータルサーバ２０に送信される（Ｓ５２１）。

【００５７】

ポータルサーバ２０は、利用者端末１０から認証要求を受信すると、認証要求の送信元となる利用者端末１０のＩＰアドレスを取得する。ＩＰアドレス認証部２１２は、取得したＩＰアドレスに対応するアドレス管理情報をアドレス管理テーブル２５１から検索する（Ｓ５２２）。認証要求の送信元のＩＰアドレスに対応するアドレス管理情報がアドレス管理テーブル２５１に登録されていれば（Ｓ５２３：ＹＥＳ）、アドレス管理情報の利用者ＩＤをカードＩＤとして（Ｓ５２４）、処理を終了する。

【００５８】

一方、認証要求の送信元のＩＰアドレスに対応するアドレス管理情報が登録されていない場合には（Ｓ５２３：ＮＯ）、カードＩＤ取得画面送信部２１３は、ＩＣカードからカードＩＤを読み出すためのカードＩＤ取得画面データを作成する（Ｓ５２５）。カードＩＤ取得画面データ１６の一例を図１４に示す。同図の例では、カードＩＤ取得画面データ１６には、ＩＣカードリーダ１０７からＩＣカードにアクセス可能になるように指示するメッセージ１６１と、利用者端末１０においてＩＤ読取プログラム１１を起動するように示すコマンド１６２が含まれている。図１４の例では、コマンド１６２は、ＷｅｂブラウザからＡｃｔｉｖｅＸ（登録商標）コントロールを起動するためのＯＢＪＥＣＴタグとなっている。カードＩＤ取得画面送信部２１３は、作成したカードＩＤ取得画面データを利

用者端末１０に送信する（Ｓ５２６）。

【００５９】

利用者端末１０において、カードＩＤ取得画面受信部１１２は、カードＩＤ取得画面データを受信し、受信したカードＩＤ取得画面データに基づいてカードＩＤ取得画面１６２を表示する（Ｓ５２７）。カードＩＤ取得画面受信部１１２が表示するカードＩＤ取得画面１７の一例を図１５に示す。同図の例では、カードＩＤ取得画面１７の表示欄１７１には、上述の図１４に示すカードＩＤ取得画面データ１６に含まれていたメッセージ１６１が表示されている。また、カードＩＤ取得画面受信部１１２は、上記のカードＩＤ取得画面１７を表示するとともに、カードＩＤ取得画面データに含まれているコマンド１６２に応じてＩＤ読取プログラム１１を起動する（Ｓ５２８）。ＩＤ読取プログラム１１が実行されることにより実現されるカードＩＤ取得部１１３は、ＩＣカードリーダ１０７を介してＩＣカードからカードＩＤを読み取り（Ｓ５２９）、カードＩＤ送信部１１４は、読み取ったカードＩＤをポータルサーバ２０に送信する（Ｓ５３０）。

ポータルサーバ２０では、カードＩＤ受信部２１４が、利用者端末１０から送信されるカードＩＤを受信する（Ｓ５３１）。

【００６０】

このように、本実施形態の認証システムでは、ＡｃｔｉｖｅＸ（登録商標）コントロールなどのプラグインプログラムを起動することにより、ポータルサーバ２０からＩＣカードリーダ１０７を制御してＩＣカードからカードＩＤを取得することを可能としている。一般に、ポータルサーバ２０側から、クライアントである利用者端末１０に接続されているデバイスを制御することは困難であるが、本実施形態の認証システムによれば、プラグインプログラムを起動するためのタグを含むカードＩＤ取得画面データを用いて、ＩＣカードを利用した利用者の認証を、Ｗｅｂアプリケーションの形態であっても、容易に実現することができる。

【００６１】

次に、カードＩＤに基づいてディレクトリ情報を取得する処理の流れを図１６に示す。

ディレクトリ情報取得部２１５は、上述の図１５の処理により取得されるカードＩＤに対応するディレクトリ情報を、ＬＤＡＰサーバ３０から取得する（Ｓ５４１）。

ディレクトリ情報取得部２１５は、カードＩＤの先頭１桁が０～８であるかどうかにより、ＩＣカードが貸与カードであるかどうかを判定する（Ｓ５４２）。カードＩＤの先頭１桁が０～８である場合、すなわち貸与カードでない場合には（Ｓ５４２：ＹＥＳ）、ディレクトリ情報取得部２１５は、カードＩＤを利用者ＩＤとして（Ｓ５４３）、処理を終了する。

【００６２】

一方、カードＩＤの先頭１桁が０～８以外の英数字である場合、すなわち貸与カードである場合には（Ｓ５４２：ＮＯ）、ディレクトリ情報取得部２１５は、上記のディレクトリ情報に含まれているポータルＩＤを利用者ＩＤとして（Ｓ５４４）、ポータルＩＤにカードＩＤが一致するディレクトリ情報をＬＤＡＰサーバ３０から取得する（Ｓ５４５）。

【００６３】

上述したように、貸与カードが利用者に貸し出される場合には、貸与カードのカードＩＤに対応するディレクトリ情報のポータルＩＤには、貸出先となった利用者の利用者ＩＤが設定される。したがって、貸与カードの場合には、ポータルＩＤに対応するディレクトリ情報が取得され、通常のＩＣカードの場合には、ＩＣカードに記録されているカードＩＤに対応するディレクトリ情報が取得される。このように、本実施形態の認証システムでは、利用者がＩＣカードを携帯し忘れた場合であっても、ポータルサーバ２０は、適切なディレクトリ情報を取得することができるようになっている。

【００６４】

また、本実施形態の認証システムでは、利用者がＩＣカードを携帯し忘れた場合であっても、貸与カードのカードＩＤに対応するポータルＩＤが利用者ＩＤとして決定される。

したがって、認証に用いられる利用者ＩＤが適切に利用者を識別することが可能となる。

【００６５】

以上のようにして、利用者ＩＤが決定されて、ディレクトリ情報が取得されると、次に利用者の認証処理が行われる。図１７は、利用者の認証処理の流れを示す図である。

ポータルサーバ２０において、認証画面作成部２１６は、利用者ＩＤの入力欄のためのＩＮＰＵＴタグと、パスワードの入力欄のためのＩＮＰＵＴタグとを含む認証画面データ１８を作成する（Ｓ５６１）。認証画面作成部２１６は、利用者ＩＤが管理者管理テーブル２５２に登録されているかどうかを判定し（Ｓ５６２）、利用者ＩＤが管理者管理テーブル２５２に登録されていない場合には（Ｓ５６２：ＮＯ）、認証画面データ１８に含まれる利用者ＩＤの入力欄を編集不能にすべく、利用者ＩＤの入力欄のためのＩＮＰＵＴタグにＤＩＳＡＢＬＥＤ属性を設定する（Ｓ５６３）。上記のようにして作成された認証画面データ１８の一例を図１８に示す。同図の例において、認証画面データ１８には、利用者ＩＤの入力欄のためのタグ１８１と、パスワードの入力欄のためのタグ１８２とが含まれており、タグ１８１には「ＤＩＳＡＢＬＥＤ」属性が設定されている。上記のようにして認証画面データ１８が作成されると、認証画面データ送信部２１７は、認証画面データ１８を利用者端末１０に送信する（Ｓ５６４）。

【００６６】

利用者端末１０では、認証画面データ受信部１１５がポータルサーバ２０から認証画面データ１８を受信し、受信した認証画面データ１８に基づく認証画面１９を表示装置１０６に表示する（Ｓ５６５）。上述した図１８の例の認証画面データ１８に基づく認証画面１９の一例を図１９に示す。同図に示すように、認証画面１９は、利用者ＩＤの入力欄１９１と、パスワードの入力欄１９２とを備えている。しかし、図１８の例の認証画面データ１８に基づく認証画面１９では、タグ１８１に「ＤＩＳＡＢＬＥＤ」属性が設定されているため、入力欄１９１は編集不能の状態となる。認証情報入力部１１６は、入力欄１９１に入力されたパスワードを受け付ける（Ｓ５６６）。なお、利用者が管理者である場合には、上述したように、入力欄１９１は編集可能となる。この場合、認証情報入力部１１６は、入力欄１９１に入力された利用者ＩＤと、入力欄１９２に入力されたパスワードとの両方を受け付ける。

【００６７】

認証画面１９において、ログインボタン１９３が押下されると、認証情報送信部１１７は、入力欄１９１に設定されている利用者ＩＤと、入力欄１９２に入力されたパスワードとをポータルサーバ２０に送信する（Ｓ５６７）。

【００６８】

ポータルサーバ２０では、認証情報受信部２１８が、利用者端末１０から送信される利用者ＩＤとパスワードとを受信し、受信した利用者ＩＤと、上記図１６に示す処理により決定された利用者ＩＤとが異なる場合には（Ｓ５６８：ＮＯ）、ディレクトリ情報取得部２１５は、受信した利用者ＩＤに対応するディレクトリ情報をＬＤＡＰサーバ３０から取得する（Ｓ５６９）。

【００６９】

認証処理部２１９は、利用者端末１０から受信したパスワードが、利用者ＩＤに対応するディレクトリ情報のパスワードと一致するかどうかを判断する（Ｓ５７０）。画面データ送信部２２０は、受信したパスワードとディレクトリ情報のパスワードとが一致すれば（Ｓ５７０：ＹＥＳ）、ポータルサイトに係る画面データを利用者端末１０に送信し（Ｓ５７１）、一致しなければ（Ｓ５７０：ＮＯ）、その旨を示すエラーメッセージを表示するための画面データを利用者端末１０に送信する（Ｓ５７２）。

【００７０】

上記のようにして、管理者以外の利用者に対しては、利用者ＩＤの入力欄が編集不能となった認証画面が利用者端末１０に表示され、利用者からのパスワードが利用者端末１０からポータルサーバ２０に応答される。これにより、ポータルサーバ２０においては、ＩＣカードに記録されていた利用者ＩＤと、認証画面において入力されたパスワードとを用

いて利用者の認証を行うことができる。本実施形態の認証システムでは、ＩＣカードに記録されている利用者ＩＤに加えて、認証画面においてパスワードの入力も受け付けるようにしている。したがって、他人のＩＣカードを使用したとしても、その他人のパスワードを知らなければ、他人としてポータルサーバ２０において認証を受けることはできない。よって、他人のＩＣカードを利用して他人になりすますような不正な認証を防ぐことができる。

【００７１】

その一方で、管理者に対しては、利用者ＩＤの入力欄が編集可能となった認証画面が利用者端末１０に表示される。したがって、例えば、ポータルサイトにおいて異なる利用権限が付与された利用者ＩＤを複数用意しておき、管理者がそれらの利用者ＩＤを使い分けることが可能となる。これにより、管理者は、例えば、ポータルサイトにおいて、利用権限に応じた使い勝手を調査することができる。

【００７２】

なお、本実施形態では、利用者ＩＤとパスワードによる認証に先だって、ＩＰアドレスによる認証を行うものとしたが、ＩＰアドレスを利用した認証を省略してもよい。

【００７３】

また、本実施形態では、管理者管理テーブル２５２に利用者ＩＤが登録されているかどうかにより、利用者が管理者であるかどうかを判断するものとしたが、これに限らず、例えば、利用者ＩＤの先頭１桁が０である場合など、利用者ＩＤに対する所定の条件を満たすかどうかにより管理者であるかどうかを判断するようにしてもよい。

【００７４】

また、本実施形態では、ＬＤＡＰにより利用者のディレクトリ情報を管理するものとしたが、これに限らず、ポータルサーバ２０が備えるＲＤＢＭＳにおいてディレクトリ情報を管理するようにしてもよい。

【００７５】

また、本実施形態では、ポータルサーバ２０が提供する情報処理サービスは、Ｗｅｂアプリケーションの形態であるものとしたが、これに限らず、各種のクライアント・サーバ形態に適用することができる。

【００７６】

また、本実施形態では、管理者以外の利用者については、認証画面において、ＩＮＰＵＴタグに「ＤＩＳＡＢＬＥＤ」属性を設定することにより、利用者ＩＤの入力欄を編集不能にするものとしたが、入力欄を表示することなく、利用者ＩＤを表示するテキスト情報を認証画面に表示するようにしてもよい。

【００７７】

以上、本実施形態について説明したが、上記実施形態は本発明の理解を容易にするためのものであり、本発明を限定して解釈するためのものではない。本発明は、その趣旨を逸脱することなく、変更、改良され得ると共に、本発明にはその等価物も含まれる。

【図面の簡単な説明】

【００７８】

【図１】本実施形態に係る認証システムの全体構成を示す図である。

【図２】ＬＤＡＰサーバ３０が管理するディレクトリ情報の一例を示す図である。

【図３】管理者端末４０のハードウェア構成を示す図である。

【図４】管理者端末４０のソフトウェア構成を示す図である。

【図５】貸与カードに対応するディレクトリ情報を更新する処理の流れを示す図である。

【図６】利用者端末１０のハードウェア構成を示す図である。

【図７】利用者端末１０のソフトウェア構成を示す図である。

【図８】ポータルサーバ２０のハードウェア構成を示す図である。

【図９】ポータルサーバ２０のソフトウェア構成を示す図である。

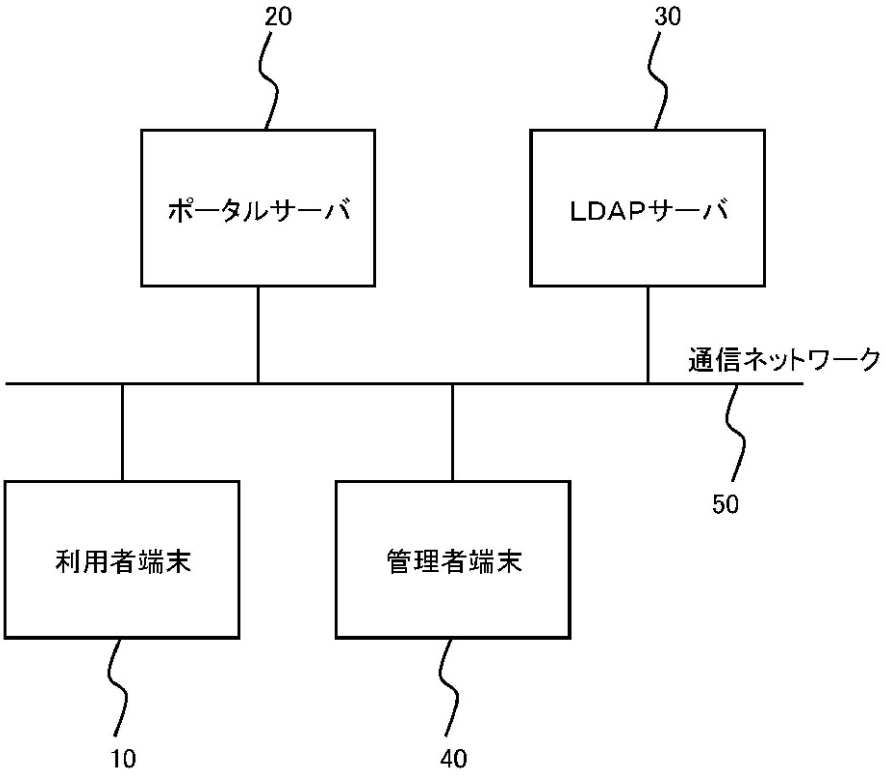
【図１０】アドレス管理テーブル２５１に記憶されるアドレス管理情報の構成例を示す図である。

【図１１】管理者管理テーブル２５２の構成例を示す図である。
【図１２】利用者を認証する処理の流れを示す図である。
【図１３】ＩＣカードからカードＩＤを取得する処理の流れを示す図である。
【図１４】カードＩＤ取得画面データ１６の一例を示す図である。
【図１５】カードＩＤ取得画面１７の一例を示す図である。
【図１６】カードＩＤに基づいてディレクトリ情報を取得する処理の流れを示す図である。
【図１７】利用者の認証処理の流れを示す図である。
【図１８】認証画面データ１８の一例を示す図である。
【図１９】認証画面データ１８に基づく認証画面１９の一例を示す図である。

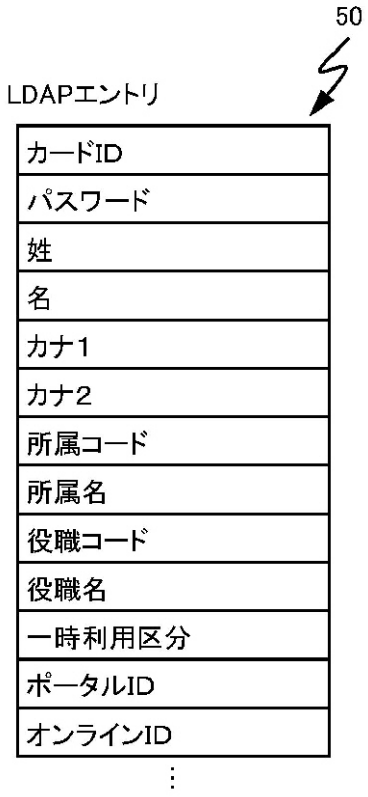
【符号の説明】
【００７９】

１０　利用者端末
１１　ＩＤ読取プログラム
１２　ＩＤ読取ドライバ
１０１　ＣＰＵ
１０２　メモリ
１０３　記憶装置
１０４　通信インタフェース
１０５　入力装置
１０６　表示装置
１０７　ＩＣカードリーダ
１１１　認証要求送信部
１１２　カードＩＤ取得画面受信部
１１３　カードＩＤ取得部
１１４　カードＩＤ送信部
１１５　認証画面データ受信部
１１６　認証情報入力部
１１７　認証情報送信部
１６１　メッセージ
１６２　コマンド
１７　カードＩＤ読取画面
１８　認証画面データ
１８１　タグ
１８２　タグ
１９　認証画面
１９１　入力欄
１９２　入力欄
１９３　ログインボタン
２０　ポータルサーバ
２０１　ＣＰＵ
２０２　メモリ
２０３　記憶装置
２０４　通信インタフェース
２０５　入力装置
２０６　表示装置
２１１　認証要求受信部
２１２　ＩＰアドレス認証部
２１３　カードＩＤ取得画面送信部
２１４　カードＩＤ受信部
２１５　ディレクトリ情報取得部
２１６　認証画面作成部
２１７　認証画面データ送信部
２１８　認証情報受信部
２１９　認証処理部
２２０　画面データ送信部
２５１　アドレス管理テーブル
２５２　管理者管理テーブル
３０　ＬＤＡＰサーバ
４０　管理者端末
４０１　ＣＰＵ
４０２　メモリ
４０３　記憶装置
４０４　通信インタフェース
４０５　入力装置
４０６　表示装置
４０７　ＩＣカードリーダ
４１１　貸与利用者入力部
４１２　カードＩＤ取得部
４１３　エントリ更新部
５０　通信ネットワーク

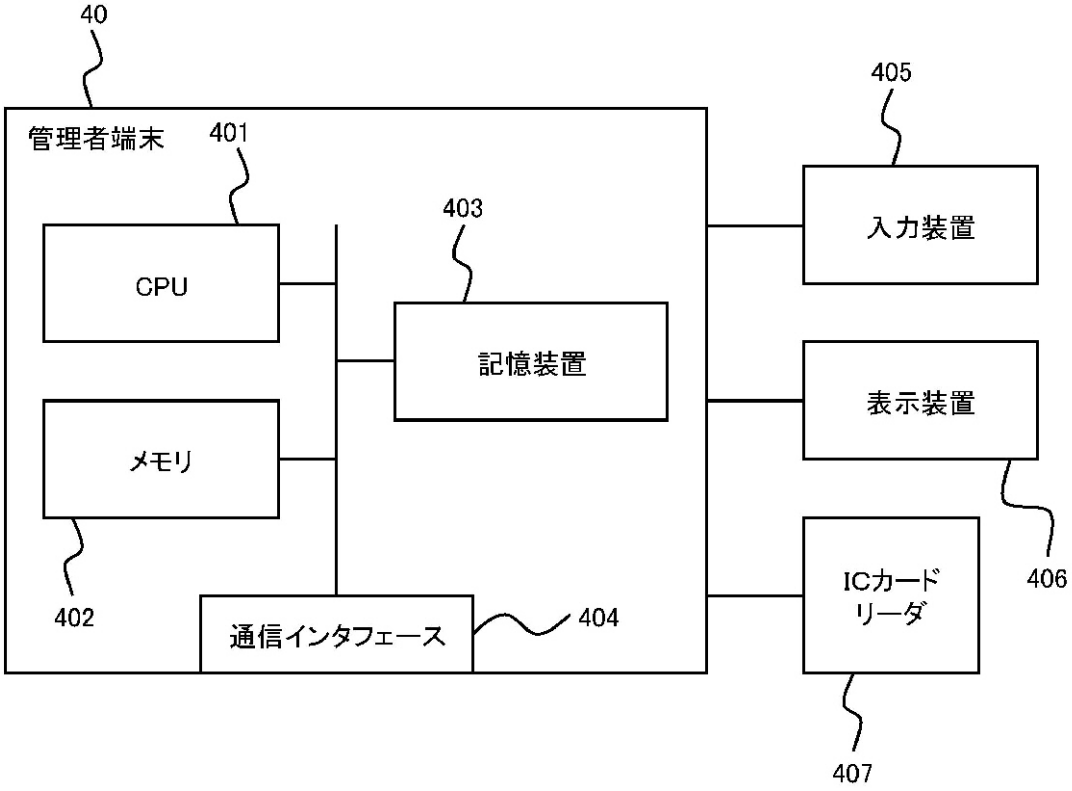
【図１】


20
30
ポータルサーバ
LDAPサーバ
通信ネットワーク
50
利用者端末
管理者端末
10
40

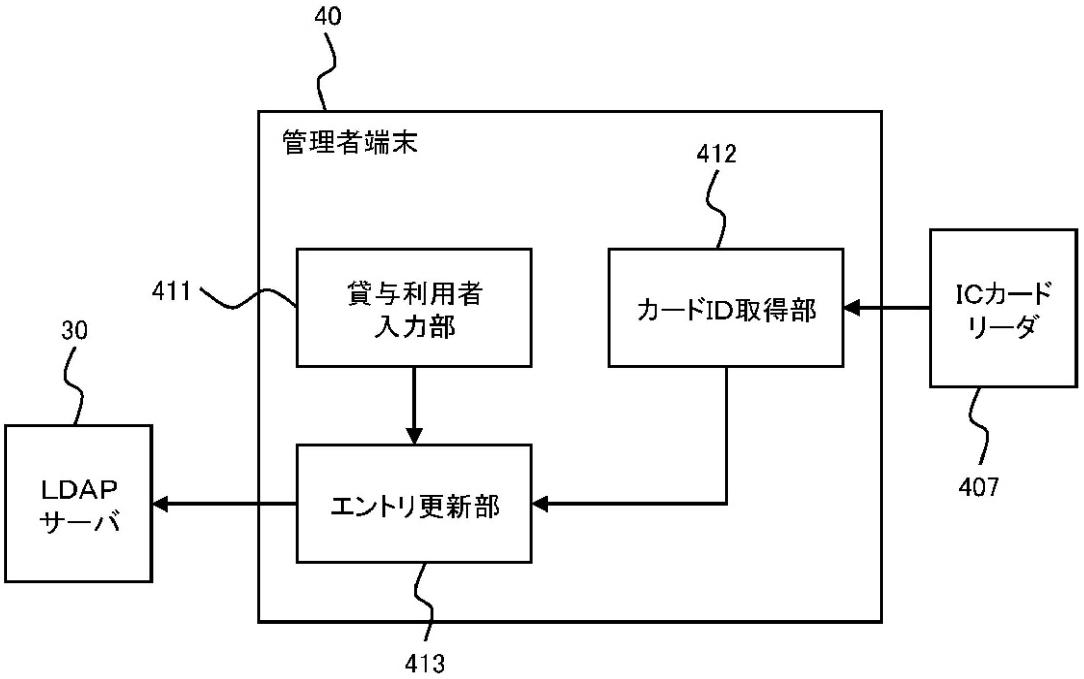
【図２】


50
LDAPエントリ
カードID
パスワード
姓
名
カナ1
カナ2
所属コード
所属名
役職コード
役職名
一時利用区分
ポータルID
オンラインID

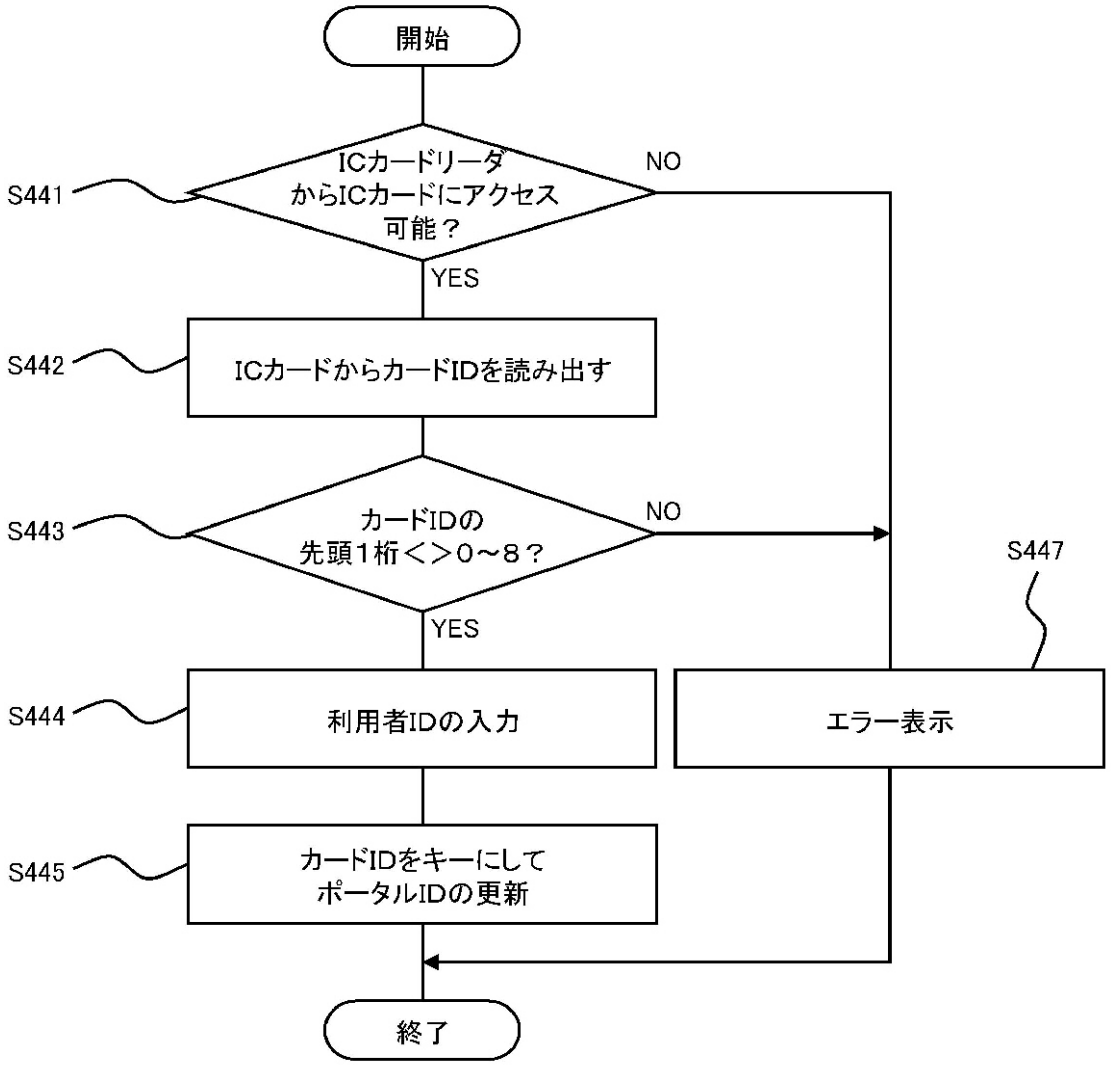
【図３】


40
管理者端末
401
CPU
403
記憶装置
メモリ
402
通信インタフェース
404
405
入力装置
表示装置
406
ICカード
リーダ
407

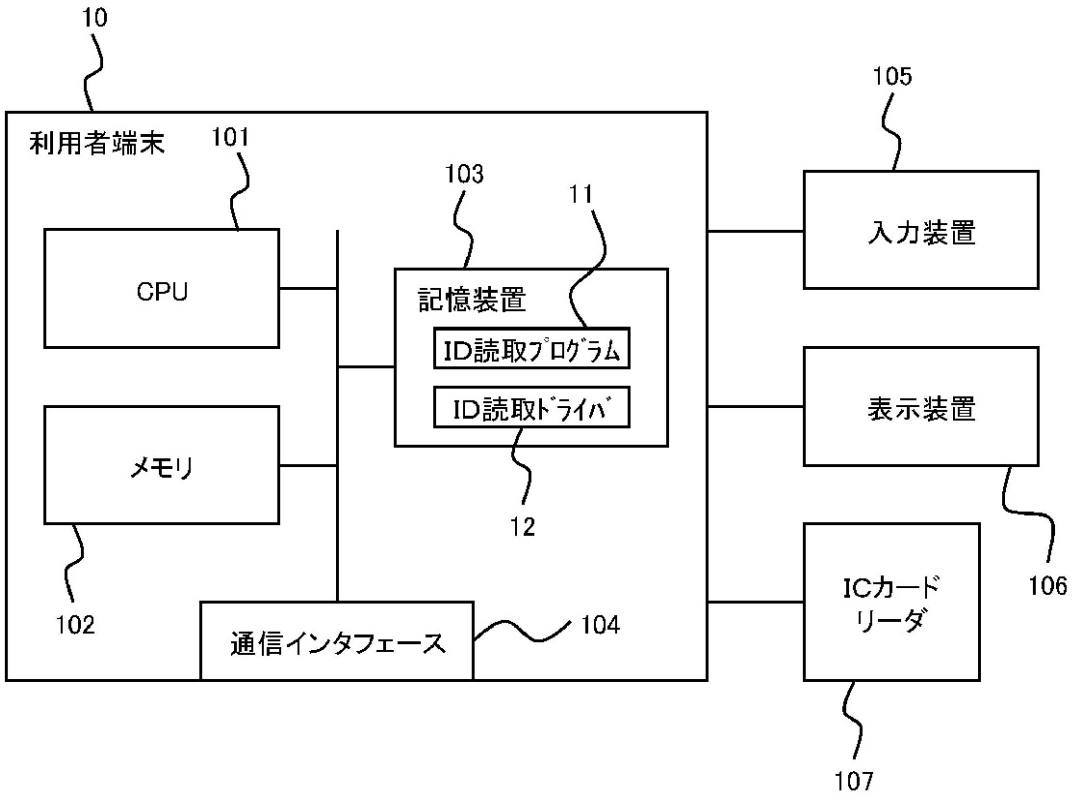
【図４】


40
管理者端末
412
411
貸与利用者
入力部
カードID取得部
ICカード
リーダ
30
LDAP
サーバ
エントリ更新部
407
413

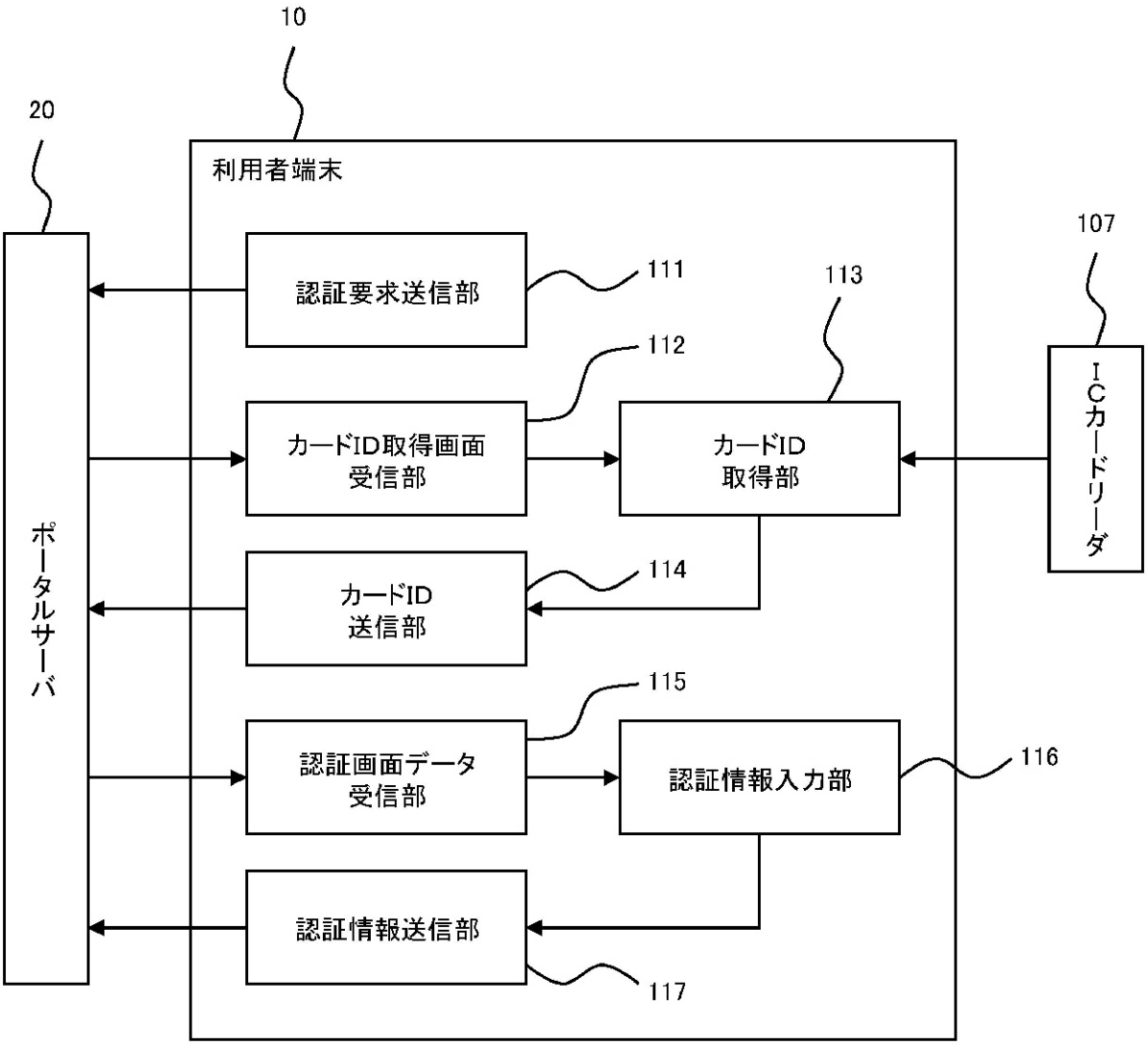
【図５】


開始
S441
ICカードリーダからICカードにアクセス可能？
NO
YES
S442
ICカードからカードIDを読み出す
S443
カードIDの先頭1桁＜＞0～8？
NO
YES
S447
S444
利用者IDの入力
エラー表示
S445
カードIDをキーにしてポータルIDの更新
終了

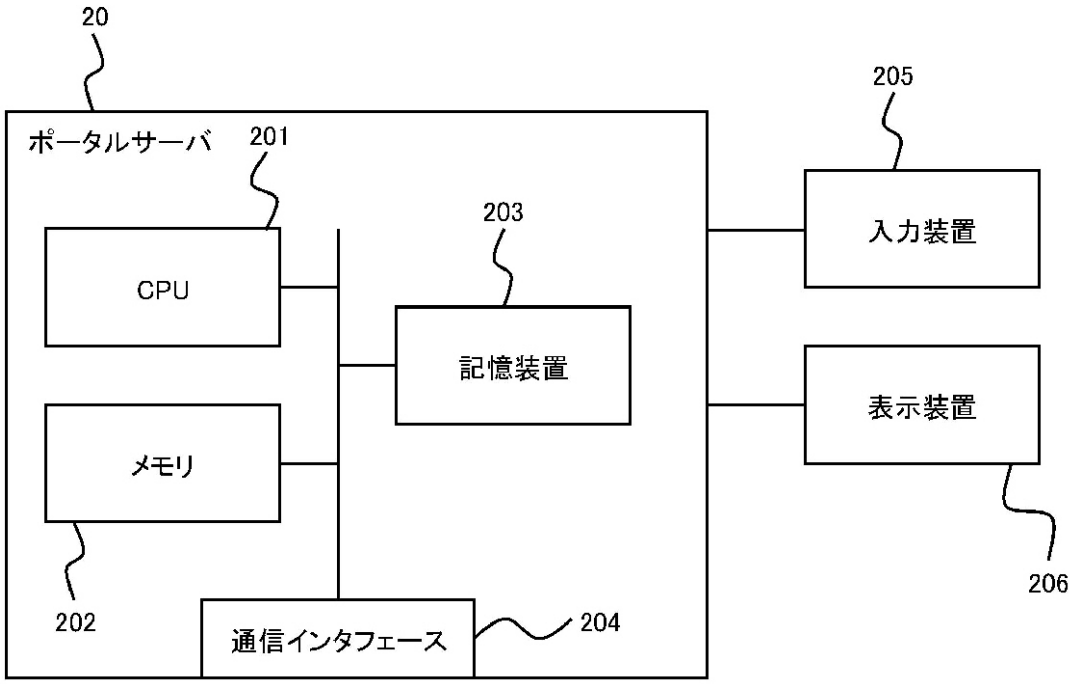
【図６】


10
利用者端末
101
CPU
メモリ
102
103
11
記憶装置
ID読取ﾌﾟﾛｸﾞﾗﾑ
ID読取ﾄﾞﾗｲﾊﾞ
12
通信インタフェース
104
105
入力装置
表示装置
106
ICカード
リーダ
107

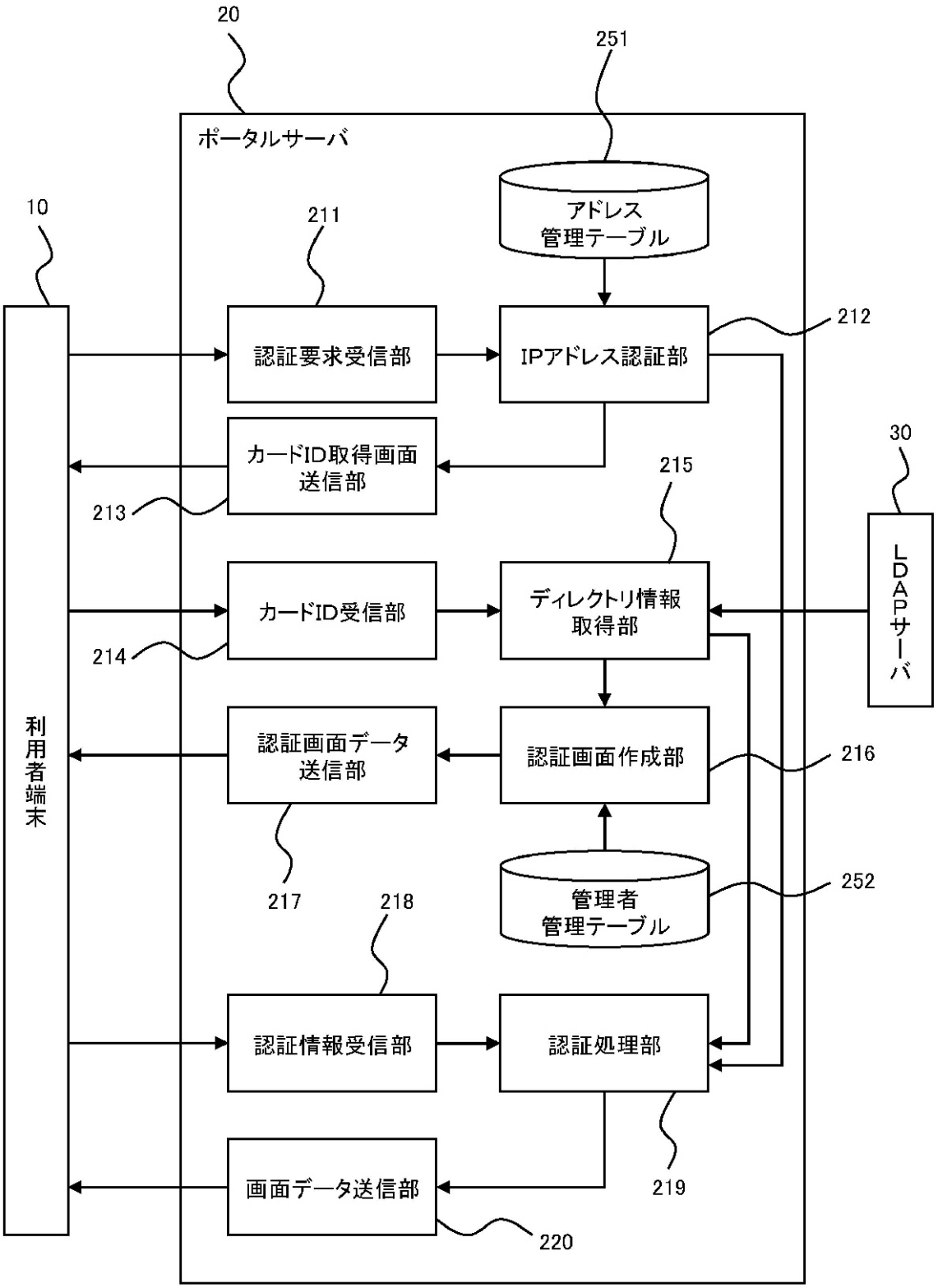
【図７】


10
20
利用者端末
ポータルサーバ
認証要求送信部
111
113
107
112
カードID取得画面
受信部
カードID
取得部
ICカードリーダ
カードID
送信部
114
115
認証画面データ
受信部
認証情報入力部
116
認証情報送信部
117

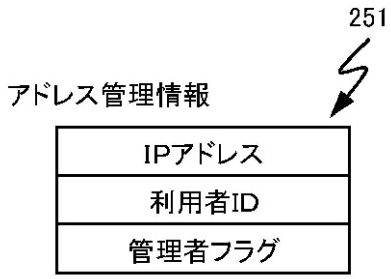
【図８】


20
ポータルサーバ
201
CPU
203
記憶装置
メモリ
202
通信インタフェース
204
205
入力装置
表示装置
206

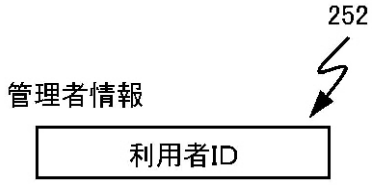
【図９】


20
251
ポータルサーバ
アドレス
管理テーブル
10
211
認証要求受信部
IPアドレス認証部
212
カードID取得画面
送信部
213
30
215
カードID受信部
ディレクトリ情報
取得部
LDAPサーバ
214
利用者端末
認証画面データ
送信部
認証画面作成部
216
217
218
管理者
管理テーブル
252
認証情報受信部
認証処理部
219
画面データ送信部
220

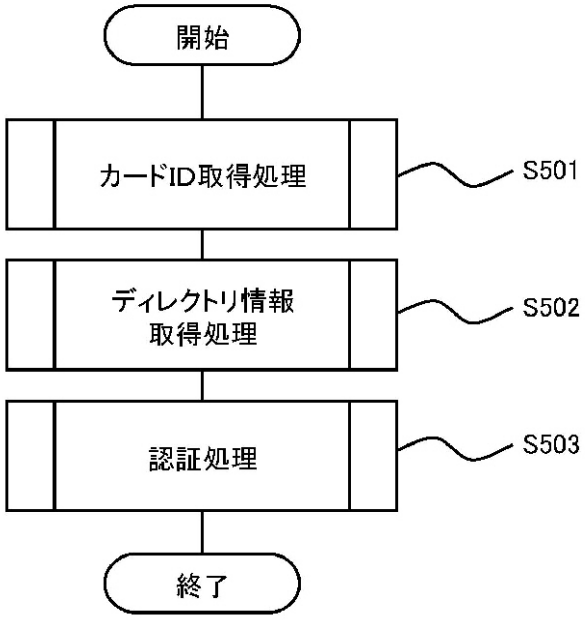
【図１０】


251
アドレス管理情報
IPアドレス
利用者ID
管理者フラグ

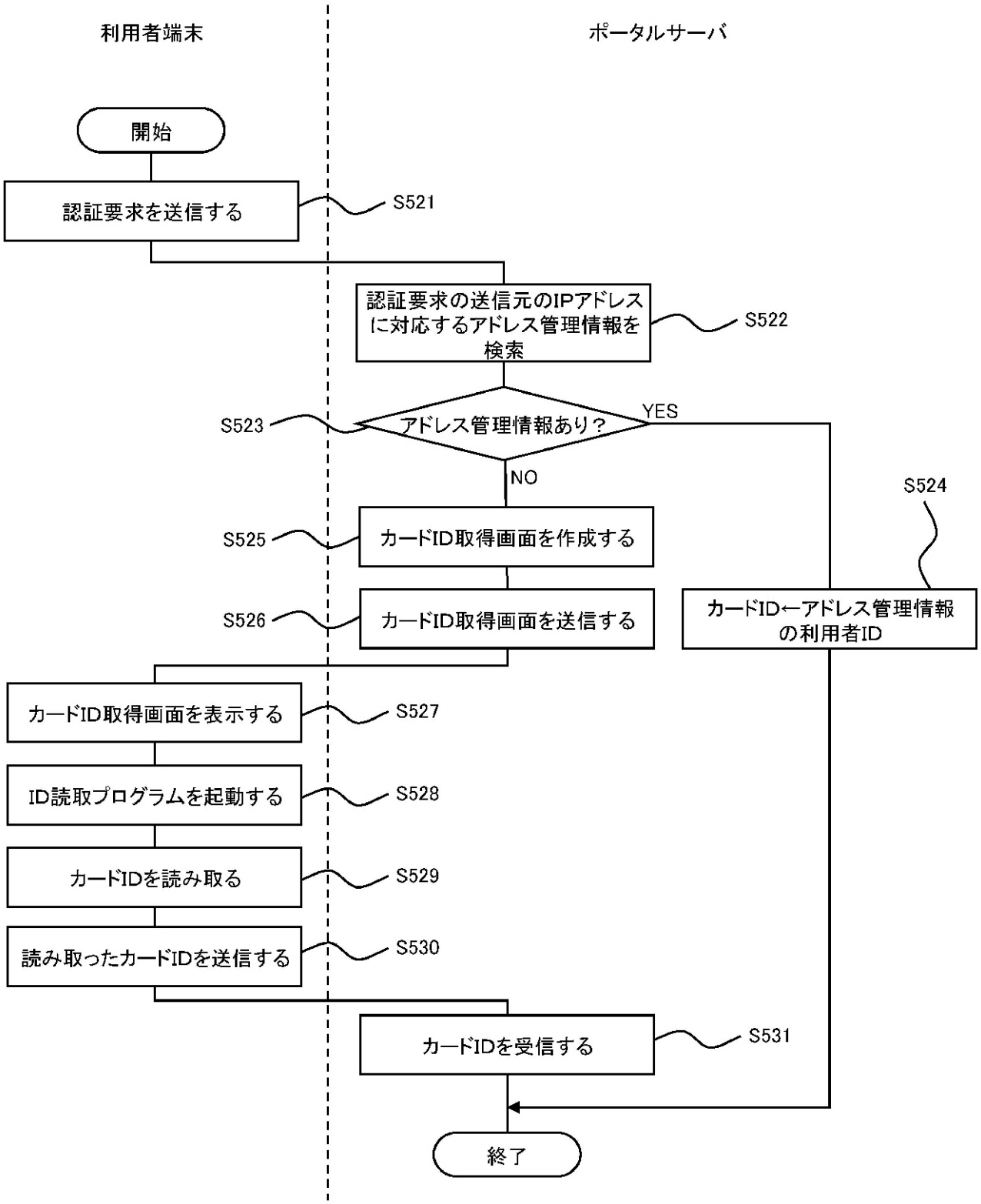
【図１１】


252
管理者情報
利用者ID

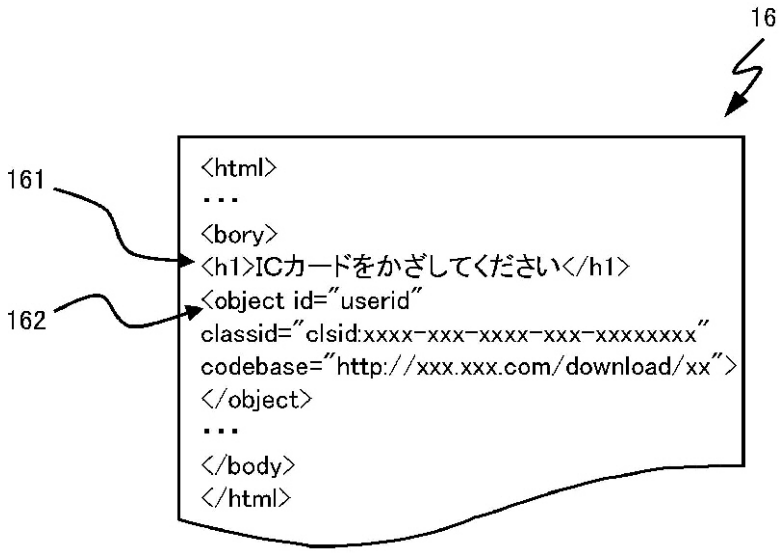
【図１２】


開始
カードID取得処理
S501
ディレクトリ情報
取得処理
S502
認証処理
S503
終了

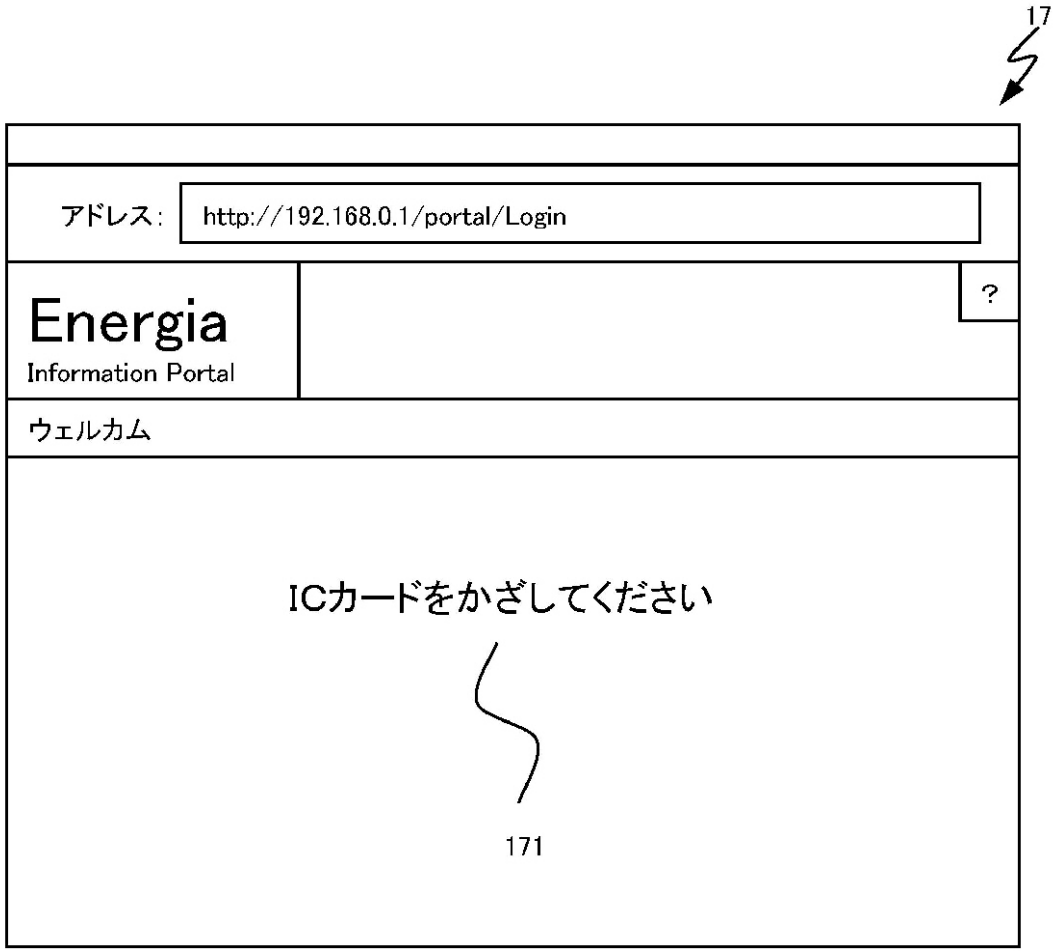
【図１３】


利用者端末
ポータルサーバ
開始
認証要求を送信する
S521
認証要求の送信元のIPアドレスに対応するアドレス管理情報を検索
S522
S523
アドレス管理情報あり？
YES
NO
S524
S525
カードID取得画面を作成する
S526
カードID取得画面を送信する
カードID←アドレス管理情報の利用者ID
カードID取得画面を表示する
S527
ID読取プログラムを起動する
S528
カードIDを読み取る
S529
読み取ったカードIDを送信する
S530
カードIDを受信する
S531
終了

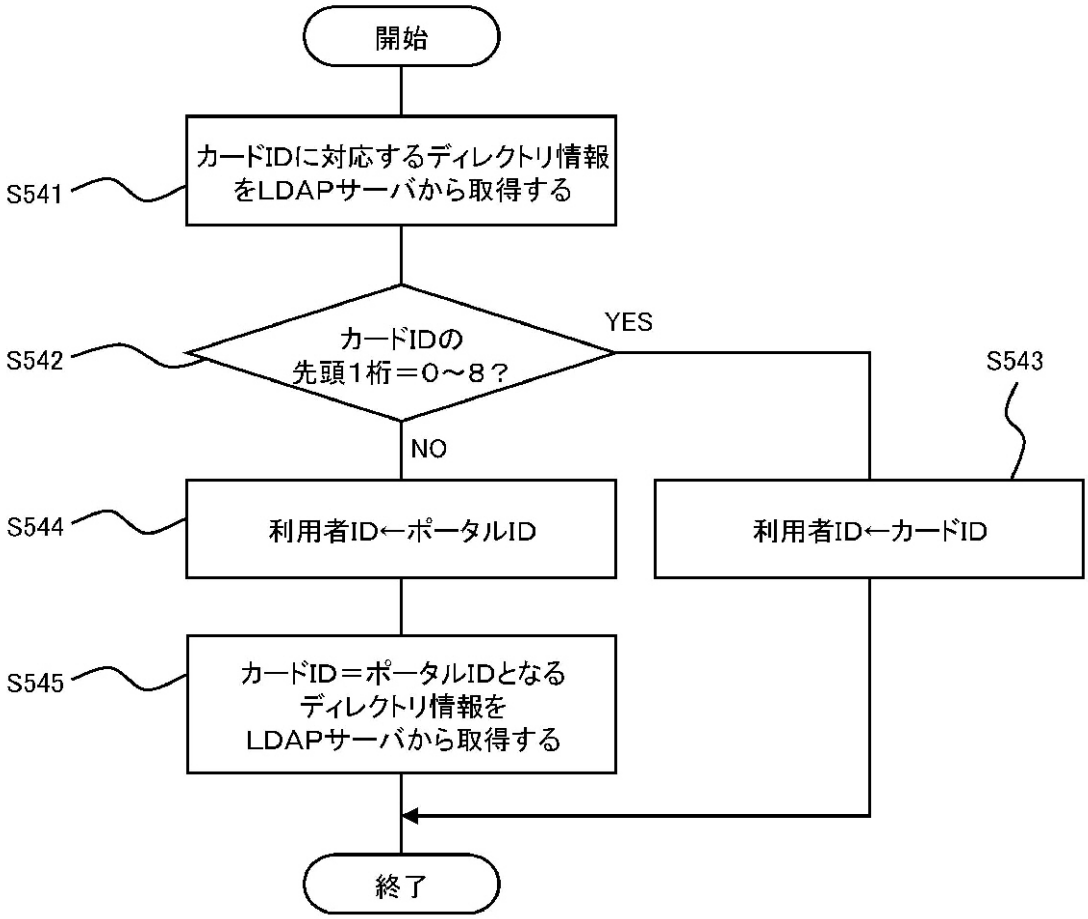
【図１４】


16
161
162
<html>
・・・
<bory>
<h1>ICカードをかざしてください</h1>
<object id="userid"
classid="clsid:xxxx-xxx-xxxx-xxx-xxxxxxxx"
codebase="http://xxx.xxx.com/download/xx">
</object>
・・・
</body>
</html>

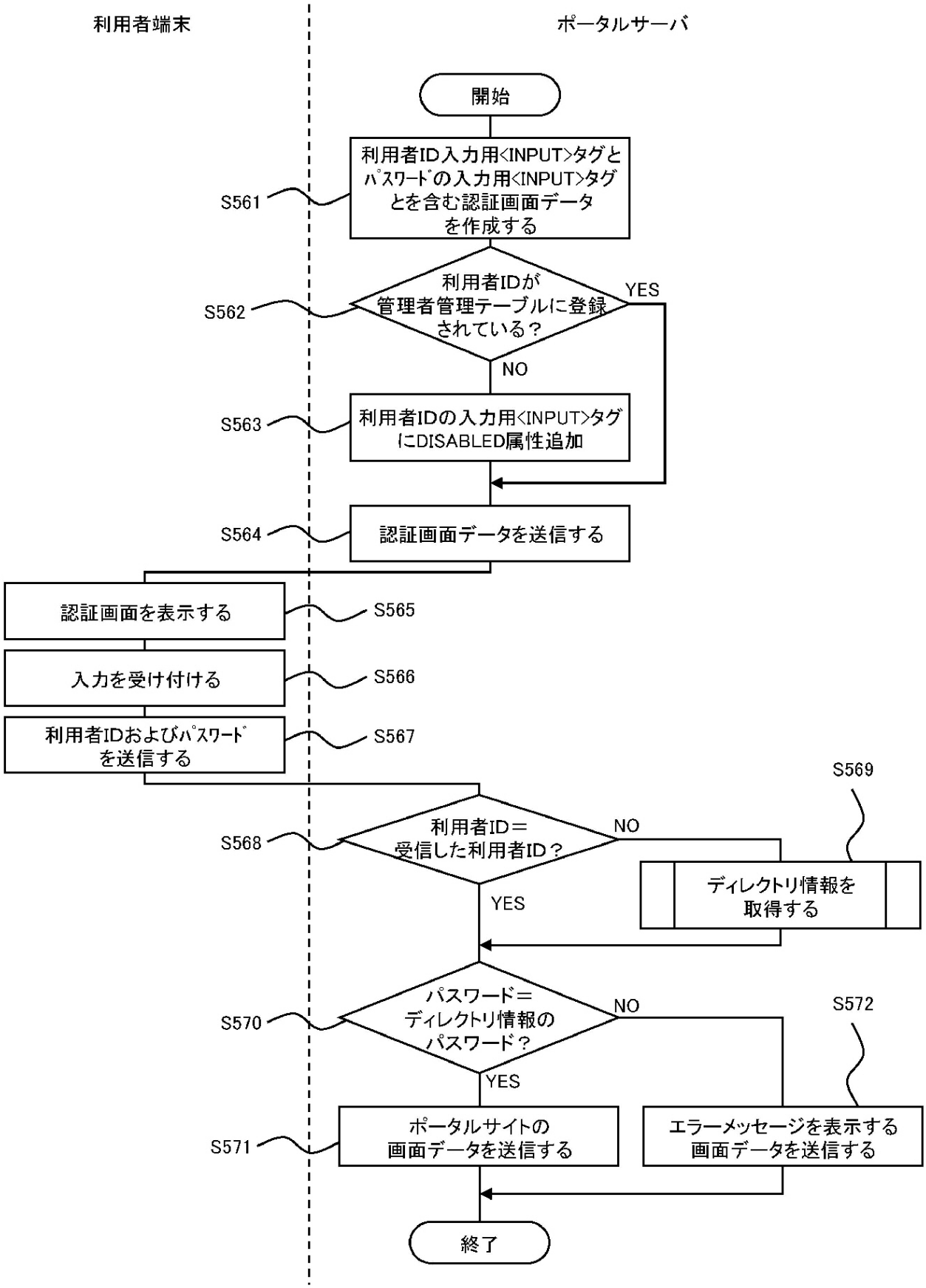
【図１５】


17
アドレス:
http://192.168.0.1/portal/Login
?
Energia
Information Portal
ウェルカム
ICカードをかざしてください
171

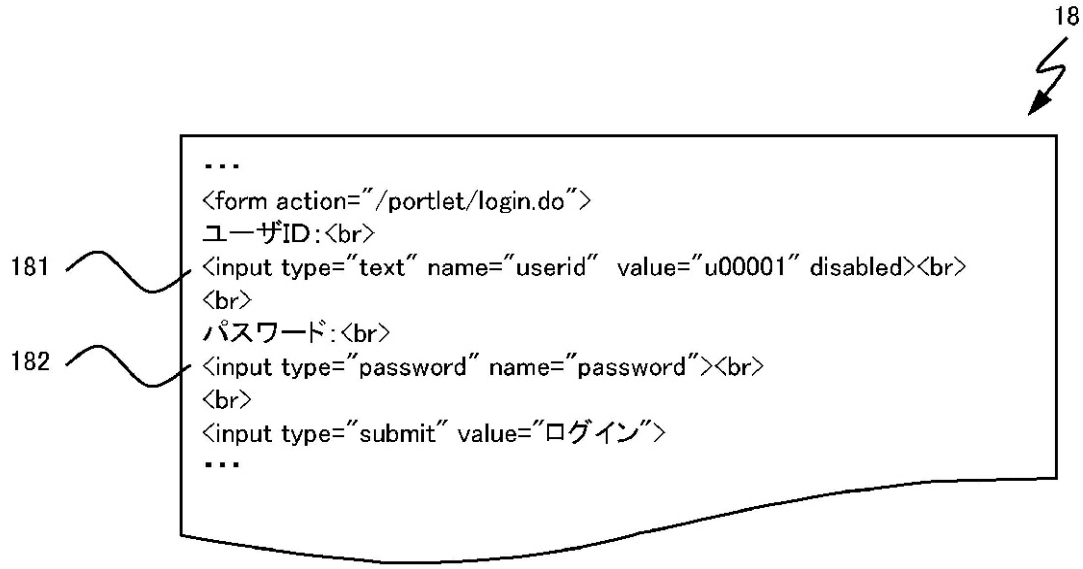
【図１６】


開始
カードIDに対応するディレクトリ情報をLDAPサーバから取得する
S541
カードIDの先頭1桁＝0～8？
S542
YES
NO
S543
利用者ID←ポータルID
S544
利用者ID←カードID
カードID＝ポータルIDとなるディレクトリ情報をLDAPサーバから取得する
S545
終了

【図１７】


利用者端末
ポータルサーバ
開始
利用者ID入力用<INPUT>タグとパスワードの入力用<INPUT>タグとを含む認証画面データを作成する
S561
利用者IDが管理者管理テーブルに登録されている？
S562
YES
NO
利用者IDの入力用<INPUT>タグにDISABLED属性追加
S563
認証画面データを送信する
S564
認証画面を表示する
S565
入力を受け付ける
S566
利用者IDおよびパスワードを送信する
S567
利用者ID＝受信した利用者ID？
S568
NO
S569
ディレクトリ情報を取得する
YES
パスワード＝ディレクトリ情報のパスワード？
S570
NO
S572
YES
ポータルサイトの画面データを送信する
S571
エラーメッセージを表示する画面データを送信する
終了

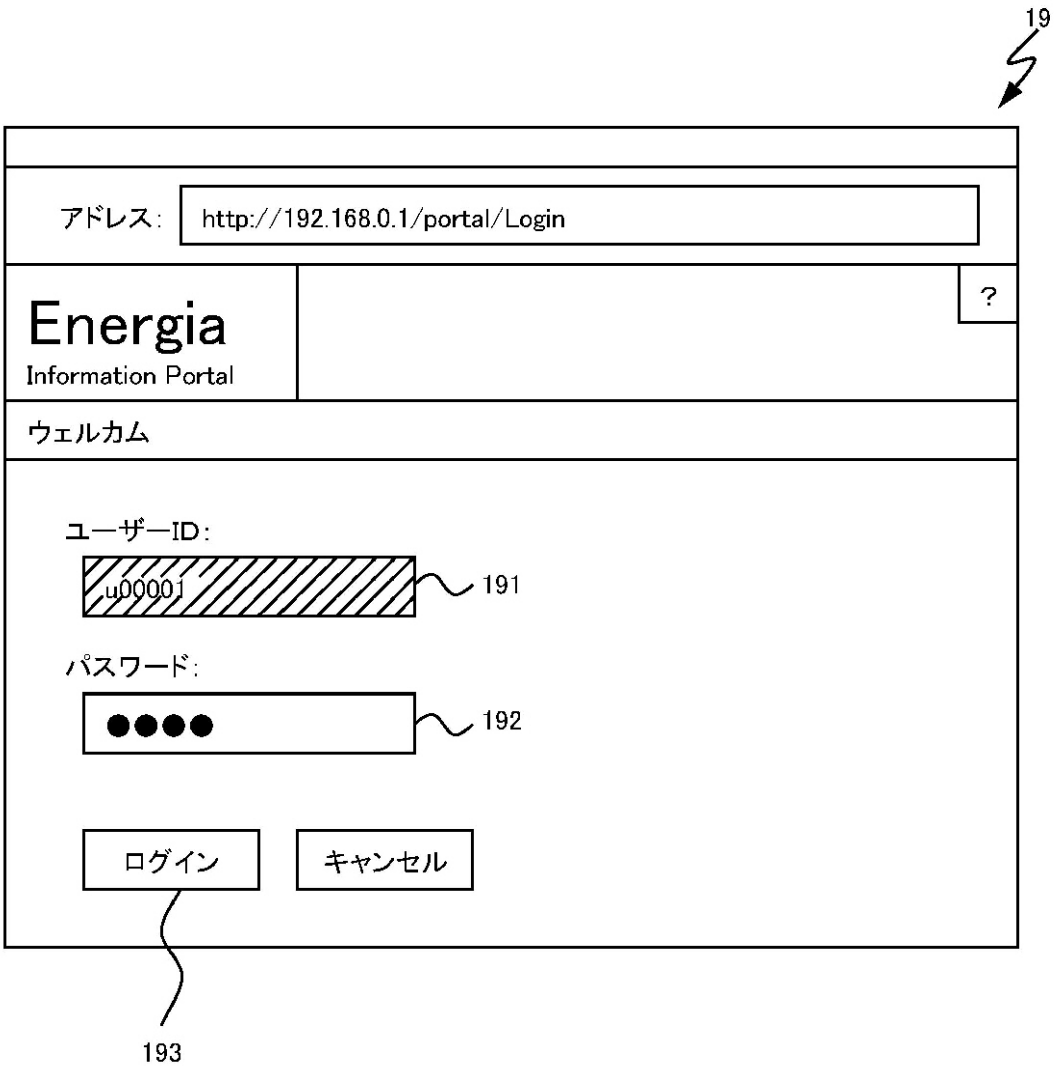
【図１８】


18
・・・
<form action="/portlet/login.do">
ユーザID:
181
<input type="text" name="userid" value="u00001" disabled>

パスワード:
182
<input type="password" name="password">

<input type="submit" value="ログイン">
・・・

【図１９】


19
アドレス:
http://192.168.0.1/portal/Login
?
Energia
Information Portal
ウェルカム
ユーザーID:
u00001
191
パスワード:
192
ログイン
キャンセル
193