(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6065623号
(P6065623)
(45)発行日　平成29年1月25日(2017.1.25)　(24)登録日　平成29年1月6日(2017.1.6)

(51)Int.Cl.　　F I
G06F 21/44 (2013.01)　　G06F 21/44
G06F 21/88 (2013.01)　　G06F 21/88

請求項の数 11　(全 20 頁)

(21)出願番号　特願2013-20245(P2013-20245)
(22)出願日　平成25年2月5日(2013.2.5)
(65)公開番号　特開2014-153741(P2014-153741A)
(43)公開日　平成26年8月25日(2014.8.25)
審査請求日　平成27年11月11日(2015.11.11)

(73)特許権者　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(74)代理人　100096699
弁理士　鹿嶋　英實
(72)発明者　鈴木　秀夫
東京都羽村市栄町３丁目２番１号
カシオ計算機株式会社
羽村技術センター内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】情報管理装置、携帯端末装置及びプログラム

(57)【特許請求の範囲】
【請求項１】
通信ネットワークを介して接続可能な携帯端末装置からの要求に応答してその要求に応じた情報を送信する情報管理装置であって、
前記携帯端末装置によりアクセスが可能な電子機器を識別する機器識別情報と当該機器識別情報毎にその機器自体の認証に用いる機器用認証情報を記憶する機器情報記憶手段と、
前記携帯端末装置の使用を許可するか否かを示す使用可否情報を記憶する端末情報記憶手段と、
前記携帯端末装置から当該情報管理装置を経由する電子機器への間接アクセスの要求を受信した場合に、前記機器情報記憶手段を参照することによってその電子機器へのアクセスが可能な携帯端末装置からの要求であるか否かを判別すると共に、前記端末情報記憶手段を参照することによってその端末使用が許可されている携帯端末装置からの要求であるか否かを判別する判別手段と、
前記判別手段により電子機器へのアクセスが可能な携帯端末装置からの要求であり、かつ端末使用が許可されている携帯端末装置からの要求であると判別された場合に、前記アクセス要求された電子機器の前記機器用認証情報をその要求元の携帯端末装置に対して送信する送信手段と、
を備えたことを特徴とする情報管理装置。
【請求項２】

前記判別手段は、前記携帯端末装置からアクセス要求を受信した場合に、更に、アクセス権限を持っている正規なユーザからのアクセス要求であるか否かを判別し、
前記送信手段は、前記判別手段により電子機器へのアクセスが可能な携帯端末装置からの要求であり、かつ端末使用が許可されている携帯端末装置からの要求であり、更に、前記判別手段により正規なユーザからの要求であると判別された場合に、前記アクセス要求された電子機器の前記機器用認証情報をその要求元の携帯端末装置に対して送信する、
ようにしたことを特徴とする請求項１に記載の情報管理装置。
【請求項３】
アクセス権限を持っている正規なユーザの認証情報を認証処理の基準情報として記憶する基準情報記憶手段と、
前記携帯端末装置からアクセス要求を受信した場合にそのアクセス要求に含まれている認証情報と前記基準情報とを照合することによって認証処理を実行する認証手段と、
を更に備え、
前記判別手段は、前記認証手段による処理結果に基づいて正規なユーザであるか否かを判別する、
ようにしたことを特徴とする請求項２に記載の情報管理装置。
【請求項４】
前記携帯端末装置から当該情報管理装置を経由する間接アクセスが要求された電子機器は、その携帯端末装置が近距離通信によって探索した電子機器であり、
前記携帯端末装置から当該情報管理装置を経由する電子機器への間接アクセスの要求は、当該携帯端末装置が近距離通信によって探索した電子機器から受信取得したその機器識別情報を含むアクセス要求である、
ことを特徴とする請求項１に情報管理装置。
【請求項５】
前記判別手段は、前記携帯端末装置から当該情報管理装置を経由する電子機器への間接アクセスの要求に応じて当該電子機器へのアクセスが可能な携帯端末装置からの要求であるか否かを判別する場合に、前記機器情報記憶手段を参照し、その携帯端末装置に対応して当該電子機器の機器識別情報と機器用認証情報が記憶されていれば、当該電子機器へのアクセスが可能な携帯端末装置からの要求であると判別する、
ようにしたことを特徴とする請求項１に記載の情報管理装置。
【請求項６】
近距離無線通信により周辺の外部機器をアクセスする携帯端末装置であって、
アクセス対象となる外部機器を識別する機器識別情報を取得する取得手段と、
携帯端末装置毎にアクセスが可能な外部機器の機器識別情報及びその機器自体の認証に用いる機器用認証情報を記憶管理する情報管理装置に対して、前記取得手段により取得した機器識別情報と共に自己の端末識別情報を送信することにより当該外部機器をアクセスするに必要な情報の要求を行う情報要求手段と、
前記情報管理装置側において前記情報の要求に応答して前記機器識別情報が示す外部機器を前記端末識別情報が示す携帯端末装置によってアクセスすることが可能であると判別された場合に、それを条件に送信される当該外部機器の機器用認証情報を受信する受信手段と、
前記受信手段により受信した機器用認証情報を前記アクセス対象の外部機器に対して近距離無線通信により送信する送信手段と、
を備えたことを特徴とする携帯端末装置。
【請求項７】
当該携帯端末装置自体の認証に用いる端末用認証情報を認証基準情報として記憶する基準情報記憶手段と、
入力された端末用認証情報と前記認証基準情報とを照合することによって認証処理を実行することにより正規なユーザであるかを認証する認証手段と、
を更に備え、

前記情報要求手段は、前記認証手段により正規なユーザであることが認証された場合に、前記機器識別情報と共に自己の端末識別情報を送信して情報の要求を行う、
ようにしたことを特徴とする請求項６に記載の携帯端末装置。
【請求項８】
前記受信手段は、前記情報管理装置側において前記情報要求に応答して前記機器識別情報が示す外部機器を前記端末識別情報が示す携帯端末装置によってアクセスすることが可能であると判別され、かつ、携帯端末装置の使用を許可するか否かを示す使用可否情報を参照することによってその端末使用が許可されている携帯端末装置からの要求であると判別された場合にそれを条件に送信される機器用認証情報を受信する、
ようにしたことを特徴とする請求項６に記載の携帯端末装置。
【請求項９】
アクセスが可能な複数の電子機器毎にその個々を識別する機器識別情報と当該機器識別情報毎にその機器用認証情報を記憶する機器情報記憶手段と、
前記取得手段により取得した機器識別情報に基づいて前記機器情報記憶手段を参照することによりその機器識別情報に該当する機器用認証情報が記憶されているか否かを判別する判別手段と、
を更に備え、
前記情報要求手段は、前記判別手段によって該当する機器用認証情報が記憶されていないと判別された場合に、前記情報管理装置に対して情報要求を行う、
ようにしたことを特徴とする請求項６に記載の携帯端末装置。
【請求項１０】
コンピュータに対して、
携帯端末装置に対応してその携帯端末装置によりアクセスが可能な電子機器を識別する機器識別情報と当該機器識別情報毎にその機器自体の認証に用いる機器用認証情報を機器情報として記憶管理する機能と、
前記携帯端末装置に対応して任意に設定された情報であってその端末装置の使用を許可するか否かを示す使用可否情報を端末情報として記憶管理する機能と、
前記携帯端末装置から通信ネットワークを介して電子機器への間接アクセスの要求を受信した場合に、前記機器情報を参照することによってその電子機器へのアクセスが可能な携帯端末装置からの要求であるか否かを判別すると共に、前記端末情報を参照することによってその端末使用が許可されている携帯端末装置からの要求であるか否かを判別する機能と、
前記電子機器へのアクセスが可能な携帯端末装置からの要求であり、かつ端末使用が許可されている携帯端末装置からの要求であると判別された場合に、前記アクセス要求された電子機器の前記機器用認証情報をその要求元の携帯端末装置に対して送信する機能と、
を実現させるためのプログラム。
【請求項１１】
コンピュータに対して、
アクセス対象の外部機器を識別する機器識別情報を取得する機能と、
携帯端末装置毎にアクセスが可能な外部機器の機器識別情報及び機器用認証情報を記憶管理する情報管理装置に対して、通信ネットワークを介して前記取得の機器識別情報と共に自己の端末識別情報を送信することにより当該外部機器をアクセスするに必要な情報の要求を行う機能と、
前記情報の要求時に受信した機器識別情報及び端末識別情報に基づいて、前記情報管理装置側で当該機器識別情報が示す外部機器を当該端末識別情報が示す携帯端末装置でアクセス可能であると判断されたことを条件に、その情報管理装置から送信される機器用認証情報を受信する機能と、
前記受信した機器用認証情報を前記アクセス対象の外部機器に対して近距離無線通信により送信する機能と、
を実現させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、携帯端末装置からの要求に応答してその要求に応じた情報を送信する情報管理装置、携帯端末装置及びプログラムに関する。
【背景技術】
【０００２】
近年、多数の電子機器の中からユーザが所望する電子機器を任意にアクセスすることが可能な携帯端末装置として、例えば、複数台の電子機器の個々に要求されるユーザ認証を一台の携帯端末装置を使用することによって実現可能な技術が存在している（特許文献１参照）。この携帯端末装置は、電子機器（例えば、家の玄関や自動車などの電子キー、家のパーソナルコンピュータなど）毎に、その機器識別情報（機器ＩＤ）及び機器用認証情報（機器用パスワード）を記憶管理しており、アクセスしたい任意の電子機器が指定されると、その機器識別情報（機器ＩＤ）に対応する機器用パスワードを読み出して当該電子機器に対して発信することによりその電子機器側でユーザ認証を行わせるようにしている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０００－２９８４０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
上述の特許文献１の技術にあっては、携帯端末装置に対するユーザ認証のみで各電子機器に対するユーザ認証が可能となるために、電子機器毎に煩雑なユーザ認証用の入力操作が不要となり、利便性の高いものとなるが、このような技術の更なる発展として、携帯端末装置を紛失したとき、盗難されたときの安全性が要望されている。例えば、携帯端末装置の紛失時や盗難時には、その携帯端末装置を取得した第三者が、その端末装置のパスワードさえ分かれば、そのまま複数の電子機器へのアクセスが可能となる状況となり、玄関や自動車などの電子キーが開錠されるなどの危険性があった。また、その携帯端末装置に用いられるパスワードが分からないとしても、携帯端末装置内には各種の電子機器の機器用パスワードが記憶されているため、その端末装置内の記憶データを解読されることで全てのパスワードが盗まれてしまうという危険性もあった。
【０００５】
本発明の課題は、電子機器を任意にアクセス可能な携帯端末装置を紛失したり、盗難されたりした場合でもその携帯端末装置による電子機器への不正なアクセスを防止できるようにすることである。
【課題を解決するための手段】
【０００６】
上述した課題を解決するために本発明の情報管理装置は、
通信ネットワークを介して接続可能な携帯端末装置からの要求に応答してその要求に応じた情報を送信する情報管理装置であって、
前記携帯端末装置によりアクセスが可能な電子機器を識別する機器識別情報と当該機器識別情報毎にその機器自体の認証に用いる機器用認証情報を記憶する機器情報記憶手段と、
前記携帯端末装置の使用を許可するか否かを示す使用可否情報を記憶する端末情報記憶手段と、
前記携帯端末装置から当該情報管理装置を経由する電子機器への間接アクセスの要求を受信した場合に、前記機器情報記憶手段を参照することによってその電子機器へのアクセスが可能な携帯端末装置からの要求であるか否かを判別すると共に、前記端末情報記憶手

段を参照することによってその端末使用が許可されている携帯端末装置からの要求であるか否かを判別する判別手段と、
前記判別手段により電子機器へのアクセスが可能な携帯端末装置からの要求であり、かつ端末使用が許可されている携帯端末装置からの要求であると判別された場合に、前記アクセス要求された電子機器の前記機器用認証情報をその要求元の携帯端末装置に対して送信する送信手段と、
を備えたことを特徴とする情報管理装置である。
【０００７】
上述した課題を解決するために本発明の携帯端末装置は、
近距離無線通信により周辺の外部機器をアクセスする携帯端末装置であって、
アクセス対象となる外部機器を識別する機器識別情報を取得する取得手段と、
携帯端末装置毎にアクセスが可能な外部機器の機器識別情報及びその機器自体の認証に用いる機器用認証情報を記憶管理する情報管理装置に対して、前記取得手段により取得した機器識別情報と共に自己の端末識別情報を送信することにより当該外部機器をアクセスするに必要な情報の要求を行う情報要求手段と、
前記情報管理装置側において前記情報の要求に応答して前記機器識別情報が示す外部機器を前記端末識別情報が示す携帯端末装置によってアクセスすることが可能であると判別された場合に、それを条件に送信される当該外部機器の機器用認証情報を受信する受信手段と、
前記受信手段により受信した機器用認証情報を前記アクセス対象の外部機器に対して近距離無線通信により送信する送信手段と、
を備えたことを特徴とする携帯端末装置である。
【発明の効果】
【０００８】
本発明によれば、電子機器を任意にアクセス可能な携帯端末装置を紛失したり、盗難されたりした場合でもその携帯端末装置による電子機器への不正なアクセスを防止することができ、セキュリティを高めることが可能となる。
【図面の簡単な説明】
【０００９】
【図１】情報管理サーバ装置を中核とする通信ネットワークシステム（機器認証管理システム）を示したブロック図。
【図２】情報管理サーバ装置１の基本的な構成要素を説明するためのブロック図。
【図３】携帯端末装置２の基本的な構成要素を説明するためのブロック図。
【図４】（１）、（２）は、機器情報テーブルＥＴ及び端末情報テーブルＴＴを説明するための図。
【図５】情報管理サーバ装置１の全体動作のうち、本実施形態の特徴部分の動作概要を示したフローチャート。
【図６】図５の動作に続くフローチャート。
【図７】携帯端末装置２の全体動作のうち、本実施形態の特徴部分の動作概要を示したフローチャート。
【図８】図７の動作に続くフローチャート。
【発明を実施するための形態】
【００１０】
以下、図１～図８を参照して本発明の実施形態を説明する。
図１は、情報管理サーバ装置を中核とする通信ネットワークシステム（機器認証管理システム）を示したブロック図である。
通信ネットワークシステムは、情報管理サーバ装置（情報管理装置）１、携帯端末装置２、各種の電子機器３を有する通信システムで、各種の電子機器３へのアクセス時に個別に要求されるユーザ認証を、一台の携帯端末装置２を使用することによって実行可能な機器認証管理システムである。

【００１１】
機器認証管理システムでは、家庭又は会社の出入口、自動車などに設置されている複数の電子機器（例えば、電子キーなど）３のうち、携帯端末装置２の近辺に存在している電子機器３をアクセスするために、その携帯端末装置２から当該電子機器３に対してその機器自体の認証に用いる機器用認証情報（例えば、電子機器３をアクセスする際に用いられる機器用パスワードなど）を送信するようにしている。その際、携帯端末装置２は、アクセス対象の電子機器３の機器用認証情報を情報管理サーバ装置１から公衆通信網（広域通信網）４を介して取得した後、近距離無線通信により当該電子機器３に送信するようにしている。
【００１２】
すなわち、情報管理サーバ装置１は、携帯端末装置２毎にアクセスが可能な複数の電子機器３の個々に対応してその機器用認証情報を記憶管理しており、携帯端末装置２は電子機器３をアクセスする毎にその機器用認証情報を情報管理サーバ装置１から受信取得するようにしているが、以下、携帯端末装置２が情報管理サーバ装置１を経由して電子機器３をアクセスすることを、電子機器３への間接アクセスと呼称するものとする。電子機器３側では、携帯端末装置２から近距離無線通信により受信した機器用認証情報に基づいてユーザ認証を行い、当該電子機器３のアクセス権限を持った正規なユーザであると認証したことを条件に、その機器特有の処理（例えば、開錠処理、アクセス制限解除処理など）を行うようにしている。
【００１３】
情報管理サーバ装置１は、この機器認証管理システムの中核を成すサーバ装置であり、携帯端末装置２毎に、どの携帯端末装置２でどの電子機器３をアクセス可能であるかの対応関係を示す情報やアクセス可能な電子機器３毎にその機器用認証情報などを一括して記憶管理するもので、後述する機器情報テーブルＥＴ、端末情報テーブルＴＴなどを有している。そして、情報管理サーバ装置１は、インターネットや移動体通信網などの公衆通信網（広域通信網）４を介して各携帯端末装置２、他の装置（例えば、タブレット端末、パーソナルコンピュータなどの情報処理装置）５に接続されている。なお、他の装置５は、電子機器３のいずれかであってもよい。
【００１４】
携帯端末装置２は、例えば、多機能型携帯電話機（スマートフォン）であり、通話機能、電子メール機能、インターネット接続機能（Ｗｅｂアクセス機能）のほか、携帯端末装置２に対して外部機器となる電子機器３との間で近距離通信を行う近距離無線通信機能などを備えている。そして、携帯端末装置２は、自己の端末装置（自端末）によってアクセス可能な各種の電子機器（例えば、家の玄関や自動車などの電子キー、家のパーソナルコンピュータなど）３のうち、アクセス対象の電子機器（近辺に存在している電子機器）３の機器用認証情報を、上述した電子機器３への間接アクセスによって情報管理サーバ装置１から取り寄せた後、その機器用認証情報を当該電子機器３に送信するようにしている。
【００１５】
図２は、情報管理サーバ装置１の基本的な構成要素を説明するためのブロック図である。
情報管理サーバ装置１の中核を成すＣＰＵ１１は、電源部１２からの電力供給によって動作し、記憶部１３内の各種のプログラムに応じてこの情報管理サーバ装置１の全体動作を制御する中央演算処理装置である。記憶部１３は、図示省略したが、後述する図５及び図６のフローチャートに示すプログラムなどを記憶するプログラム領域と、この情報管理サーバ装置１で必要とされる各種のデータを記憶するデータ領域と、フラグなど一時記憶用のワーク領域を有し、このデータ領域には、携帯端末装置２自体の認証に用いる端末用認証情報が記憶されている。
【００１６】
端末用認証情報は、携帯端末装置２をアクセスする権限を持った正規なユーザからのアクセスであるか否かを認証するための基準となる認証基準情報であり、例えば、数値列デ

ータ、文字列データからなるユーザパスワード、キーワードである。なお、記憶部１３は、ＳＤカードなどの記録メディアを含む構成であってもよく、他のサーバ装置（図示省略）側の記憶領域を含むものであってもよい。広域通信部１４は、多数同時アクセスが可能なもので、ブロードバンドのインターネットに接続（例えば、光通信接続）されている。操作部１５は、フルキーボードなどを有し、ＣＰＵ１１は、操作部１５からの入力信号に応じた処理を実行する。表示部１６は、例えば、オペレータ用の確認画面や作業画面などを表示する。

【００１７】

図３は、携帯端末装置２の基本的な構成要素を説明するためのブロック図である。

携帯端末装置２の中核を成すＣＰＵ２１は、二次電池を備えた電源部２２からの電力供給によって動作し、記憶部２３内の各種のプログラムに応じてこの携帯端末装置２の全体動作を制御する。記憶部２３は、図示省略したが、後述する図７及び図８のフローチャートに示すプログラムなどを記憶するプログラム領域と、この携帯端末装置２で必要とされる各種のデータを記憶するデータ領域と、一時記憶用のワーク領域を有している。広域通信部２４は、通話機能、電子メール機能、インターネット接続機能などの動作時に、音声やデータを変調して送信したり、無線電波を受信して音声やデータに復調して受信したりすることで通話やデータ通信を行う。

【００１８】

近距離通信部２５は、近辺に存在している電子機器３との間でデータの送受信を行うもので、非接触タイプのBluetooth（登録商標）による近距離無線通信を、その通信可能エリア内（例えば、半径３ｍ以内）で交信を行うようにしている。この場合、携帯端末装置２と近辺の電子機器３との間での交信時には、互いの自己の識別情報（端末ＩＤ、機器ＩＤ）を送受信して通信相手を連携対象として特定するようにしている。なお、近距離通信部２５は、Bluetooth（登録商標）通信に限らず、赤外線通信などを行う構成であってもよい。操作部２６は、電源ボタンなどの押しボタン式の各種のキーを有し、認証時には認証情報（例えば、パスワードなど）が入力される。タッチ表示部２７は、表示パネル２７ａにタッチパネル２７ｂを積層配設した構成で、ソフトウェアキー（ソフトキー）としての機能名を表示したり、各種のアイコンなどを表示したりする。

【００１９】

なお、各種の電子機器３の構成については、それぞれ図示省略したが、各電子機器３には、ＡＣ電源や二次電池などの電源部、全体動作を制御する中央演算処理装置（ＣＰＵ）、プログラムや機器識別情報（機器ＩＤ）などのデータを記憶する記憶部の基本デバイスを有するほか、携帯端末装置２との間でデータの送受信を行う近距離通信部などが備えられている。そして、電子機器３は、携帯端末装置２から送信される機器用認証情報を受信すると、この機器用認証情報に基づいて認証処理を実行し、正規なユーザであれば、開錠やアクセス制限解除などの所定の処理を実行する。

【００２０】

図４は、機器情報テーブルＥＴ及び端末情報テーブルＴＴを説明するための図である。

図４（１）は、機器情報テーブルＥＴを説明するための図である。この機器情報テーブルＥＴは、電子機器３に関する情報として、携帯端末装置２の「端末識別情報」毎に複数の「機器識別情報」、「機器用認証情報」を記憶可能な構成で、その内容は、携帯端末装置２などのユーザ側での入力操作によって入力された情報が情報管理サーバ装置１に送信されることによって任意に登録された情報である。「端末識別情報」は、携帯端末装置２を識別する端末識別情報である。「機器識別情報」は、対応する携帯端末装置２によってアクセス可能な電子機器３を識別するための機器識別情報であり、「端末識別情報」と「機器識別情報」は、どの携帯端末装置２でどの電子機器３をアクセス可能であるかの対応関係を示す情報である。「機器用認証情報」は、対応する電子機器３のアクセス時に実行される認証処理時に用いられるユーザパスワードなどで、数値列データや文字列データである。また、「機器用認証情報」の項目にはデータ形式などの情報も記憶するようにしてもよい。

【００２１】
図４（２）は、端末情報テーブルＴＴを説明するための図である。この端末情報テーブルＴＴは、携帯端末装置２に関する情報として、携帯端末装置２の「端末識別情報」毎に「端末使用可否情報」、「認証情報」を記憶可能な構成で、その内容は、携帯端末装置２などのユーザ側での入力操作によって入力された情報が情報管理サーバ装置１に送信されることによって任意に登録された情報である。「端末使用可否情報」は、対応する携帯端末装置２の使用を許可するか否かを示す情報（携帯端末装置２の有効／無効を示す情報）で、“無効”は、その携帯端末装置２の盗難、紛失などによって第三者による不正使用を制限（使用不能）とするために設定される情報であり、“有効”は正規なユーザによる正常な使用を許可するために設定される情報である。

【００２２】
ここで、携帯端末装置２を盗難、紛失したユーザは、他の装置（例えば、タブレット端末、自宅のパーソナルコンピュータなど）５を使用して情報管理サーバ装置１をアクセスし、その認証処理によって正規なユーザであると認証された際に、盗難、紛失の携帯端末装置２に対応する「端末使用可否情報」の内容を“無効”に設定する操作を行う。また、盗難、紛失の携帯端末装置２がそのユーザに戻った場合には、その「端末使用可否情報」の内容を“有効”に設定する操作を行う。この場合、「端末使用可否情報」の内容を“無効”から“有効”への変更は、当該携帯端末装置２、他の装置５のいずれを使用しても実行可能としてもよいが、当該携帯端末装置２による変更を禁止するようにしてもよい。また、正規なユーザであっても、例えば、当該携帯端末装置２を長期間使用しないような場合には、その携帯端末装置２を使用して情報管理サーバ装置１をアクセスし、「端末使用可否情報」の内容を“無効”に設定するようにしてもよい。

【００２３】
携帯端末装置２は、このようなユーザ操作によって入力された端末使用の無効／有効を示す情報を情報管理サーバ装置１に送信すると、情報管理サーバ装置１は、端末情報テーブルＴＴを検索し、その「端末使用可否情報」に無効／有効を設定する処理を行う。「認証情報」は、情報管理サーバ装置１をアクセスする権限を持った正規なユーザからのアクセスであるか否かを認証するための基準となる認証基準情報であり、情報管理サーバ装置１自体の認証に用いるサーバアクセス用の認証情報で、例えば、数値列データ、文字列データからなるユーザパスワード、キーワードである。

【００２４】
次に、本実施形態における機器認証管理システムを構成する情報管理サーバ装置１及び携帯端末装置２の動作概念を図５～図８に示すフローチャートを参照して説明する。ここで、これらのフローチャートに記述されている各機能は、読み取り可能なプログラムコードの形態で格納されており、このプログラムコードにしたがった動作が逐次実行される。また、ネットワークなどの伝送媒体を介して伝送されてきた上述のプログラムコードに従った動作を逐次実行することもできる。すなわち、記録媒体のほかに、伝送媒体を介して外部供給されたプログラム／データを利用して本実施形態特有の動作を実行することもできる。

【００２５】
図５及び図６は、情報管理サーバ装置１の全体動作のうち、本実施形態の特徴部分の動作概要を示したフローチャートである。
先ず、情報管理サーバ装置１のＣＰＵ１１は、携帯端末装置２からのアクセス要求待ちの状態において（図５のステップＡ１）、いずれからの携帯端末装置２からアクセス要求を受信すると（ステップＡ１でＹＥＳ）、携帯端末装置２側で実行された認証処理の結果を受信したかを調べる（ステップＡ２）。本実施形態においては、情報管理サーバ装置１を使用するアクセス権限を持ったユーザからの要求であるかをチェックする認証処理を情報管理サーバ装置１側で行うか、携帯端末装置２側で行うかを任意に選択して設定可能となっており、情報管理サーバ装置１は、携帯端末装置２側で実行された認証処理の処理結果を受信したときには（ステップＡ２でＹＥＳ）、その処理結果に基づいてアクセス権限

を持った正規なユーザからの要求であるかを調べる（ステップＡ４）。

【００２６】

また、情報管理サーバ装置１は、携帯端末装置２側でユーザ操作によって入力されたサーバアクセス用の認証情報（例えば、パスワード及びキーワード）を受信したときには（ステップＡ２でＮＯ）、その認証情報と端末情報テーブルＴＴ内の「認証情報」とを照合する認証処理を実行し（ステップＡ３）、その処理結果に基づいてアクセス権限を持った正規なユーザからの要求であるかを調べる（ステップＡ４）。ここで、正規なユーザからの要求でなければ（ステップＡ４でＮＯ）、その要求を受け付けないなめに最初のステップＡ１に戻るが、正規なユーザからの要求であれば（ステップＡ４でＹＥＳ）、機器情報テーブルＥＴ又は端末情報テーブルＴＴへの設定を要求するアクセスであるかを調べる（ステップＡ５）。

【００２７】

いま、テーブルへの設定要求を受けた場合において（ステップＡ５でＹＥＳ）、その設定要求が機器情報テーブルＥＴへの要求であれば（ステップＡ６でＹＥＳ）、携帯端末装置２から送信された情報を機器情報テーブルＥＴの「端末識別情報」、「機器識別情報」、「機器用認証情報」に設定する処理を行い（ステップＡ７）、端末情報テーブルＴＴへの要求であれば（ステップＡ６でＮＯ）、携帯端末装置２から送信された情報を端末情報テーブルＴＴの「端末識別情報」、「端末使用可否情報」、「認証情報」に設定する処理を行う（ステップＡ８）。その後、最初のステップＡ１に戻る。なお、「端末使用可否情報」は、盗難、紛失した携帯端末装置２に代わってそのユーザの他の装置（タブレット端末など）５から情報管理サーバ装置１をアクセスすることにより「端末使用可否情報」の内容を“有効”から“無効”に変更することができる。

【００２８】

一方、機器情報テーブルＥＴ又は端末情報テーブルＴＴへの設定要求でなければ（ステップＡ５でＮＯ）、図６のフローに移り、アクセス対象の電子機器３を情報管理サーバ装置１を経由する間接アクセスの要求かを調べ（ステップＡ９）、この間接アクセスの要求でなければ（ステップＡ９でＮＯ）、その他の要求に応じた処理（ステップＡ１０）を行った後、図５の最初のステップＡ１に戻る。また、間接アクセスの要求であれば（ステップＡ９でＹＥＳ）、その携帯端末装置２から送信されるアクセス対象の機器識別情報と自端末の端末識別情報とを受信取得し（ステップＡ１１）、この機器識別情報及び端末識別情報に基づいて機器情報テーブルＥＴを参照し（ステップＡ１２）、この端末識別情報にその機器識別情報が対応付けて記憶されているか、つまり、機器識別情報の電子機器３をアクセスすることが可能な携帯端末装置２からの要求であるかを調べる（ステップＡ１３）。

【００２９】

ここで、端末識別情報と機器識別情報とが対応していなければ、つまり、機器識別情報の電子機器３をアクセスが可能な携帯端末装置２からの要求でなければ（ステップＡ１３でＮＯ）、エラーメッセージを要求元の携帯端末装置２に送信（ステップＡ１９）した後、図５の最初のステップＡ１に戻る。また、端末識別情報と機器識別情報とが対応付けて記憶されていれば、つまり、アクセスが可能な端末であれば（ステップＡ１３でＹＥＳ）、この端末識別情報に基づいて端末情報テーブルＴＴを参照し（ステップＡ１４）、その「端末使用可否情報」は、“有効”か、つまり、使用が許可されている携帯端末装置２からの要求であるかを調べる（ステップＡ１５）。いま、「端末使用可否情報」が“無効”の場合、例えば、携帯端末装置２の盗難、紛失などによって端末使用が許可されていない状態でのアクセス要求であれば（ステップＡ１５でＮＯ）、エラーメッセージをその要求元の携帯端末装置２に送信（ステップＡ１９）した後、図５の最初のステップＡ１に戻る。

【００３０】

また、「端末使用可否情報」が“有効”の場合、つまり、端末使用が許可されている状態でのアクセス要求であれば（ステップＡ１５でＹＥＳ）、アクセス対象の電子機器３に

対応して端末情報テーブルＴＴに「機器用認証情報」が記憶されているかを調べ（ステップＡ１６）、「機器用認証情報」が記憶されていなければ（ステップＡ１６でＮＯ）、エラーメッセージをその要求元の携帯端末装置２に送信（ステップＡ１９）した後、図５の最初のステップＡ１に戻る。ここで、対象機器をアクセスすることが可能な携帯端末装置２からの要求であり（ステップＡ１３でＹＥＳ）、かつ、使用が許可されている携帯端末装置２からの要求である場合には（ステップＡ１５でＹＥＳ）、更に、端末情報テーブルＴＴに「機器用認証情報」が記憶されていることを条件に（ステップＡ１６でＹＥＳ）、その「機器用認証情報」を読み出して（ステップＡ１７）、要求元の携帯端末装置２に機器用認証情報を送信する（ステップＡ１８）。その後、図５の最初のステップＡ１に戻る。

【００３１】

図７及び図８は、携帯端末装置２の全体動作のうち、本実施形態の特徴部分の動作概要を示したフローチャートであり、電源投入に応じて実行開始される。

先ず、携帯端末装置２のＣＰＵ２１は、電源投入に応じて認証入力画面を表示した状態において（図７のステップＢ１）、この入力画面内に操作部２６から認証情報が入力されると（ステップＢ２）、この認証情報に基づいて認証処理を行う（ステップＢ３）。この場合、認証情報は、携帯端末装置２自体の認証に用いる端末用認証情報（例えば、携帯端末装置２をアクセスする際に用いられる端末用パスワード、キーワード）であり、携帯端末装置２は、予め記憶されている認証基準情報（図示省略）と入力された端末用認証情報とを照合することにより認証処理を行う。その結果、携帯端末装置２をアクセスする権限を持った正規なユーザからのアクセスであるか否かを判別し（ステップＢ４）、正規なユーザからのアクセスでなければ（ステップＢ４でＮＯ）、そのアクセスを無効とするために最初のステップＢ１に戻る。

【００３２】

いま、正規なユーザからのアクセスであれば（ステップＢ４でＹＥＳ）、ユーザ操作によって情報管理サーバ装置１へのアクセス要求が指示されたかを調べる（ステップＢ５）。その結果、情報管理サーバ装置１へのアクセスが指示されなければ（ステップＢ５でＮＯ）、ステップＢ６に移り、着信処理、発信処理などの処理が実行可能となるが、情報管理サーバ装置１へのアクセスが指示されたときには（ステップＢ５でＹＥＳ）、情報管理サーバ装置１を使用するアクセス権限を持った正規なユーザからの要求であるかをチェックする認証処理を情報管理サーバ装置１側で行う設定となっているかを調べる（ステップＢ７）。

【００３３】

いま、情報管理サーバ装置１側で認証処理を行うべきことが予め設定されている場合には（ステップＢ７でＹＥＳ）、認証入力画面を表示する（ステップＢ８）。そして、この入力画面内に認証情報が入力されると（ステップＢ９）、この認証情報を情報管理サーバ装置１に送信する（ステップＢ１０）。この場合、認証情報は、情報管理サーバ装置１自体の認証に用いるサーバアクセス用の認証情報（例えば、情報管理サーバ装置１をアクセスする際に用いられるサーバ用パスワード、キーワード）である。また、情報管理サーバ装置１側での認証処理が省略されている場合には（ステップＢ７でＮＯ）、上述のステップＢ３での処理結果（正規なユーザからの要求であることを示す情報）を情報管理サーバ装置１に送信する（ステップＢ１１）。

【００３４】

そして、図８のフローに移り、情報管理サーバ装置１へのアクセス指示はテーブル設定を指示するものであるか（ステップＢ１２）、携帯端末装置２から情報管理サーバ装置１を経由して電子機器３をアクセスする間接アクセスが指示されたかを調べる（ステップＢ１６）。いま、テーブル設定の指示であれば（ステップＢ１２でＹＥＳ）、更に機器情報テーブルＥＴへの設定指示であるかを調べ（ステップＢ１３）、機器情報テーブルＥＴへの設定指示であれば（ステップＢ１３でＹＥＳ）、ユーザ操作により入力された情報を機器情報テーブルＥＴへの設定情報として情報管理サーバ装置１に送信する処理を行う（ス

テップＢ１４）。また、端末情報テーブルＴＴへの設定指示であれば（ステップＢ１３でＮＯ）、ユーザ操作により入力された情報を端末情報テーブルＴＴへの設定情報として情報管理サーバ装置１に送信する処理を行う（ステップＢ１５）。

【００３５】

また、携帯端末装置２から情報管理サーバ装置１を経由して電子機器３をアクセスする間接アクセスが指示された場合には（ステップＢ１６でＹＥＳ）、近距離通信部２５を起動して近辺に存在している電子機器３との間でデータの送受信を行うことにより互いの自己の識別情報（端末ＩＤ、機器ＩＤ）を送受信して通信相手（近辺機器）を検索する（ステップＢ１７）。その結果、通信が確立した電子機器（検索機器）３からその機器識別情報を受信取得し（ステップＢ１８）、この機器識別情報と自端末の端末識別情報とを情報管理サーバ装置１に送信することによって間接アクセスの要求を行う（ステップＢ１９）。

【００３６】

この間接アクセスに応答して情報管理サーバ装置１から機器用認証情報を受信したかを調べ（ステップＢ１７）、機器用認証情報を受信しなければ（ステップＢ２０でＮＯ）、エラーメッセージを表示するが（ステップＢ２２）、機器用認証情報を受信したときには（ステップＢ２０でＹＥＳ）、近距離通信部２５に介してその機器認証情報を含むアクセス要求を近辺の電子機器（検索機器）３に送信する（ステップＢ２１）。その後、図７のステップＢ１に戻る。なお、電子機器３側では携帯端末装置２から機器認証情報を受信すると、認証処理を実行し、正規なユーザからのアクセス要求であれば、開錠やアクセス制限解除などの処理を行う。

【００３７】

以上のように、本実施形態において情報管理サーバ装置１は、携帯端末装置２から当該情報管理サーバ装置１を経由する電子機器３への間接アクセスの要求を受信した場合に、機器情報テーブルＥＴを参照してその電子機器３へのアクセスが可能な携帯端末装置２からの要求であるか否かを判別すると共に、端末情報テーブルＴＴを参照してその端末使用が許可されている携帯端末装置２からの要求であるか否かを判別した結果、当該電子機器３へのアクセスが可能な携帯端末装置２からの要求であり、かつ端末使用が許可されている携帯端末装置２からの要求であると判別された場合に、当該電子機器３の機器用認証情報をその要求元の携帯端末装置２に対して送信するようにしたので、携帯端末装置２を紛失したり、盗難されたりした場合でもその携帯端末装置２による電子機器３への不正なアクセスを防止することができ、セキュリティを高めることが可能となる。

【００３８】

すなわち、携帯端末装置２は、アクセス可能な各電子機器３に対応付けてその機器用認証情報を自端末側で記憶管理しておかなくても、情報管理サーバ装置１から取り寄せた機器用認証情報を電子機器３に送信することによって当該電子機器３をアクセスすることができ、また、携帯端末装置２を紛失したり、盗難されたりした場合にそのユーザは他の装置５を使用して情報管理サーバ装置１をアクセスして、その携帯端末装置２の使用を無効に設定しておくことができるので、紛失、盗難の携帯端末装置２を使用した電子機器３への不正アクセスを防止することができ、セキュリティを高めることが可能となる。

【００３９】

情報管理サーバ装置１は、携帯端末装置２からのアクセス要求を受信した場合に、その携帯端末装置２の正規なユーザからの要求であるか否かを判別するようにしたので、電子機器３をアクセスが可能な携帯端末装置２からの要求であること、端末使用が許可されている携帯端末装置２からの要求であること、更にアクセス権限を持った正規なユーザからの要求であることを条件として、その電子機器の機器用認証情報を送信することができ、更にセキュリティを高めることが可能となる。

【００４０】

情報管理サーバ装置１は、携帯端末装置２からアクセス要求を受信した場合に、その携帯端末装置２側で実行された認証処理の結果を受信し、その処理結果に基づいて正規なユ

ーザであるか否かを判別するようにしたので、当該情報管理サーバ装置１へのアクセス時に携帯端末装置２側で実行された認証処理の結果を受信するだけで正規なユーザからのアクセスであるか否かを判別することができる。この場合、携帯端末装置２側で正規なユーザであると認証されていれば、情報管理サーバ装置１へのアクセス時にサーバ用認証情報を入力する操作を省略することが可能となる。

【００４１】

情報管理サーバ装置１は、携帯端末装置２からアクセス要求を受信した場合に、そのアクセス要求に含まれている認証情報と端末情報テーブルＴＴ内の「認証情報」とを照合することによって認証処理を行い、その処理結果に基づいてアクセス権限を持った正規なユーザからの要求であるかを判別するようにしたので、更にセキュリティを高めることができる。

【００４２】

情報管理サーバ装置１において機器情報テーブルＥＴは、複数の携帯端末装置２の個々に対応して、その携帯端末装置２によりアクセスが可能な複数の電子機器３を識別する機器識別情報を記憶すると共に、当該機器識別情報毎にその自体の認証に用いる機器用認証情報を記憶し、端末情報テーブルＴＴは、複数の携帯端末装置２の個々に対応して使用可否情報を記憶するようにしたので、情報管理サーバ装置１は、複数の携帯端末装置２に関する情報を一括管理することにより個々の携帯端末装置２からのアクセス要求に応じた機器用認証情報をその要求元の携帯端末装置２に送信することが可能となる。

【００４３】

携帯端末装置２から情報管理サーバ装置１を経由する電子機器３への間接アクセスの要求は、携帯端末装置２が近距離通信によって探索した電子機器３から受信取得したその機器識別情報を含むアクセス要求であるので、携帯端末装置２側で電子機器３を指定するユーザ操作が行われなくても、情報管理サーバ装置１側ではアクセス対象の電子機器３を特定することが可能となる。

【００４４】

情報管理サーバ装置１は、携帯端末装置２からの間接アクセスの要求に応じて電子機器３へのアクセスが可能な携帯端末装置２からの要求であるか否かを判別する場合に、機器情報テーブルＥＴを参照し、その携帯端末装置２に対応して当該電子機器３の機器識別情報と機器用認証情報が記憶されていれば、当該電子機器３へのアクセスが可能な携帯端末装置２からの要求であると判別するようにしたので、情報の設定を忘れた場合などにも対応することができ、より確実な判別が可能となる。

【００４５】

携帯端末装置２は、アクセス対象の電子機器３の機器識別情報を取得して電子機器３をアクセスする場合に、その機器識別情報と共に自己の端末識別情報を情報管理サーバ装置１に送信して情報の要求を行った後、その電子機器３が当該携帯端末装置２によってアクセス可能であることを条件に情報管理サーバ装置１から送信されてくる機器用認証情報を受信し、その機器用認証情報をアクセス対象の電子機器３に近距離無線通信により送信するようにしたので、各電子機器３の機器用認証情報を自端末側で記憶管理しておかなくても、情報管理サーバ装置１から取り寄せた機器用認証情報を電子機器３に送信することによって当該電子機器３をアクセスすることができ、携帯端末装置２を紛失したり、盗難されたりしても機器用認証情報が解読されることもない。

【００４６】

携帯端末装置２は、端末認証情報に基づいて携帯端末装置２の正規なユーザであることが認証された場合に、情報管理サーバ装置１に対して間接アクセスの要求を行うようにしたので、携帯端末装置２側で正規なユーザであると認証されていれば、情報管理サーバ装置１へのアクセス時にサーバ用認証情報を入力する操作を省略することが可能となる。

【００４７】

携帯端末装置２は、携帯端末装置２をアクセスする権限を持った正規なユーザであることを認証した結果を情報管理サーバ装置１に送信するようにしたので、情報管理サーバ装

置１側でその確認が可能となる。
【００４８】
携帯端末装置２は、情報管理サーバ装置１自体の認証に用いる認証情報が入力された場合に、その認証情報も合わせて情報管理サーバ装置１に送信するようにしたので、情報管理サーバ装置１をアクセスする権限を持った正規なユーザであるかを情報管理サーバ装置１側で認証する処理を行うことができる。
【００４９】
携帯端末装置２は、情報管理サーバ装置１側において電子機器３をアクセスすることが可能な携帯端末装置２からの要求であり、かつ、端末使用が許可されている携帯端末装置２からの要求であることを条件に送信される機器用認証情報を受信して電子機器３に送信するようにしたので、携帯端末装置２を紛失したり、盗難されたりした場合にそのユーザは他の装置５を使用して情報管理サーバ装置１をアクセスして、その携帯端末装置２の使用の有効／無効を設定しておけば、紛失、盗難の携帯端末装置２を使用した電子機器３への不正アクセスを防止することができる。
【００５０】
携帯端末装置２は、近距離通信によって探索した近辺の電子機器３からその機器識別情報を受信取得するようにしたので、ユーザ操作で機器識別情報を入力する手間を省くことができる。
【００５１】
なお、上述した実施形態において情報管理サーバ装置１は、携帯端末装置２毎にアクセスが可能な各電子機器３の機器用認証情報を全て記憶管理する場合を例示したが、アクセスが可能な電子機器３のうち、その一部の電子機器３の機器用認証を携帯端末装置２側で記憶するようにしてもよい。例えば、厳重なセキュリティ維持を必要とする電子機器３については、その機器用認証情報を情報管理サーバ装置１側で記憶するが、その他の電子機器３については、その機器用認証情報を情報管理サーバ装置１側で記憶するようにしてもよい。
【００５２】
このように携帯端末装置２側に一部の電子機器３の機器用認証を記憶する場合には、その機器識別情報に対応付けてその機器用認証情報を記憶するテーブルを携帯端末装置２に設けておけばよい。そして、携帯端末装置２は、近辺の電子機器３から機器識別情報を受信取得した際に上述のテーブルを参照し、機器識別情報に対応して機器用認証情報が記憶されているかをチェックし、記憶されていれば、そのテーブルから直接読み出した機器用認証情報を近距離通信によって送信するが、テーブルに記憶されていなければ、情報管理サーバ装置１に対して間接アクセスの要求を行い、それに応答して受信した機器用認証情報を近距離通信によって送信すればよい。このように電子機器３の種類（セキュリティ）に応じて電子機器３へのアクセスの仕方を使い分けることができる。
【００５３】
上述した実施形態においては、認証情報としてパスワード、キーワードを例示したが、ユーザの音声を録音した音声、顔画像、指紋などの生体情報であってもよい。
【００５４】
また、上述した実施形態においては、情報管理サーバ装置１としては、会社内、家庭内のサーバ装置であってもよく、全国規模のサービスを展開する事業者側のサーバ装置であってもよい。また、携帯端末装置２として多機能型携帯電話機（スマートフォン）に適用した場合を例示したが、電子腕時計、鍵型端末、タブレット端末などのＰＤＡ（個人向け携帯型情報通信機器）、デジタルカメラ、音楽プレイヤーなどであってもよい。
【００５５】
また、上述した各実施形態において示した“装置”や“部”とは、機能別に複数の筐体に分離されていてもよく、単一の筐体に限らない。また、上述したフローチャートに記述した各ステップは、時系列的な処理に限らず、複数のステップを並列的に処理したり、別個独立して処理したりするようにしてもよい。

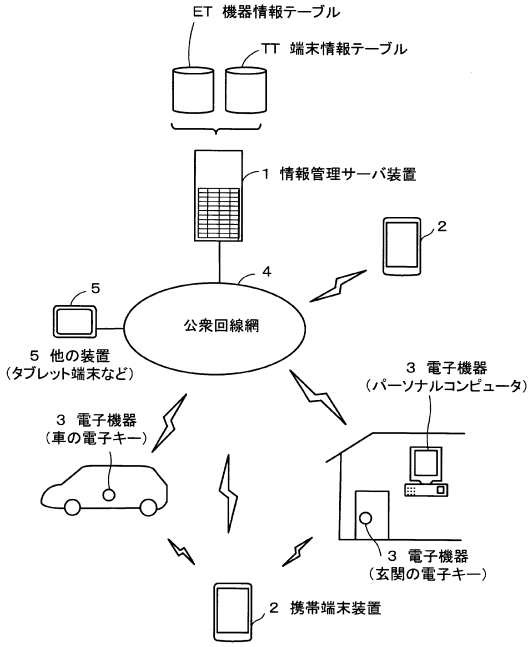
【００５６】
以上、この発明の実施形態について説明したが、この発明は、これに限定されるものではなく、特許請求の範囲に記載された発明とその均等の範囲を含むものである。
以下、本願出願の特許請求の範囲に記載された発明を付記する。
（付記）
（請求項１）
請求項１に記載の発明は、
通信ネットワークを介して接続可能な携帯端末装置からの要求に応答してその要求に応じた情報を送信する情報管理装置であって、
前記携帯端末装置によりアクセスが可能な電子機器を識別する機器識別情報と当該機器識別情報毎にその機器自体の認証に用いる機器用認証情報を記憶する機器情報記憶手段と、
前記携帯端末装置の使用を許可するか否かを示す使用可否情報を記憶する端末情報記憶手段と、
前記携帯端末装置から当該情報管理装置を経由する電子機器への間接アクセスの要求を受信した場合に、前記機器情報記憶手段を参照することによってその電子機器へのアクセスが可能な携帯端末装置からの要求であるか否かを判別すると共に、前記端末情報記憶手段を参照することによってその端末使用が許可されている携帯端末装置からの要求であるか否かを判別する判別手段と、
前記判別手段により電子機器へのアクセスが可能な携帯端末装置からの要求であり、かつ端末使用が許可されている携帯端末装置からの要求であると判別された場合に、前記アクセス要求された電子機器の前記機器用認証情報をその要求元の携帯端末装置に対して送信する送信手段と、
を備えたことを特徴とする情報管理装置である。
（請求項２）
請求項２に記載の発明は、請求項１に記載の情報管理装置において、
前記判別手段は、前記携帯端末装置からアクセス要求を受信した場合に、更に、アクセス権限を持っている正規なユーザからのアクセス要求であるか否かを判別し、
前記送信手段は、前記判別手段により電子機器へのアクセスが可能な携帯端末装置からの要求であり、かつ端末使用が許可されている携帯端末装置からの要求であり、更に、前記判別手段により正規なユーザからの要求であると判別された場合に、前記アクセス要求された電子機器の前記機器用認証情報をその要求元の携帯端末装置に対して送信する、
ようにしたことを特徴とする情報管理装置である。
（請求項３）
請求項３に記載の発明は、請求項２に記載の情報管理装置において、
前記判別手段は、前記携帯端末装置からアクセス要求を受信した場合に、当該携帯端末装置側で実行された認証処理の処理結果を受信し、その処理結果に基づいて正規なユーザであるか否かを判別する、
ようにしたことを特徴とする情報管理装置である。
（請求項４）
請求項４に記載の発明は、請求項２に記載の情報管理装置において、
アクセス権限を持っている正規なユーザの認証情報を認証処理の基準情報として記憶する基準情報記憶手段と、
前記携帯端末装置からアクセス要求を受信した場合にそのアクセス要求に含まれている認証情報と前記基準情報とを照合することによって認証処理を実行する認証手段と、
を更に備え、
前記判別手段は、前記認証手段による処理結果に基づいて正規なユーザであるか否かを判別する、
ようにしたことを特徴とする情報管理装置である。
（請求項５）

請求項５に記載の発明は、請求項１に記載の情報管理装置において、
前記機器情報記憶手段は、複数の携帯端末装置の個々に対応して、その携帯端末装置によりアクセスが可能な複数の電子機器を識別する機器識別情報を記憶すると共に、当該機器識別情報毎にその機器自体の認証に用いる機器用認証情報を記憶し、
前記端末情報記憶手段は、複数の携帯端末装置の個々に対応して前記使用可否情報を記憶する、
ようにしたことを特徴とする情報管理装置である。
（請求項６）
請求項６に記載の発明は、請求項１に情報管理装置において、
前記携帯端末装置から当該情報管理装置を経由する間接アクセスが要求された電子機器は、その携帯端末装置が近距離通信によって探索した電子機器であり、
前記携帯端末装置から当該情報管理装置を経由する電子機器への間接アクセスの要求は、当該携帯端末装置が近距離通信によって探索した電子機器から受信取得したその機器識別情報を含むアクセス要求である、
ことを特徴とする情報管理装置である。
（請求項７）
請求項７に記載の発明は、請求項１に記載の情報管理装置において、
前記判別手段は、前記携帯端末装置から当該情報管理装置を経由する電子機器への間接アクセスの要求に応じて当該電子機器へのアクセスが可能な携帯端末装置からの要求であるか否かを判別する場合に、前記機器情報記憶手段を参照し、その携帯端末装置に対応して当該電子機器の機器識別情報と機器用認証情報が記憶されていれば、当該電子機器へのアクセスが可能な携帯端末装置からの要求であると判別する、
ようにしたことを特徴とする情報管理装置である。
（請求項８）
請求項８に記載の発明は、
近距離無線通信により周辺の外部機器をアクセスする携帯端末装置であって、
前記アクセスの対象となる外部機器を識別する機器識別情報を取得する取得手段と、
携帯端末装置毎にアクセスが可能な外部機器の機器識別情報及びその機器自体の認証に用いる機器用認証情報を記憶管理する情報管理装置に対して、前記取得手段により取得した機器識別情報と共に自己の端末識別情報を送信することにより当該外部機器をアクセスするに必要な情報の要求を行う情報要求手段と、
前記情報管理装置側において前記情報要求に応答して前記機器識別情報が示す外部機器を前記端末識別情報が示す携帯端末装置によってアクセスすることが可能であると判別された場合に、それを条件に送信される当該外部機器の機器用認証情報を受信する受信手段と、
前記受信手段により受信した機器用認証情報を前記アクセス対象の外部機器に対して近距離無線通信により送信する送信手段と、
を備えたことを特徴とする携帯端末装置である。
（請求項９）
請求項９に記載の発明は、請求項８に記載の携帯端末装置において、
当該携帯端末装置自体の認証に用いる端末用認証情報を認証基準情報として記憶する基準情報記憶手段と、
入力された端末用認証情報と前記認証基準情報とを照合することによって認証処理を実行することにより正規なユーザであるかを認証する認証手段と、
を更に備え、
前記情報要求手段は、前記認証手段により正規なユーザであることが認証された場合に、前記機器識別情報と共に自己の端末識別情報を送信して情報の要求を行う、
ようにしたことを特徴とする携帯端末装置である。
（請求項１０）
請求項１０に記載の発明は、請求項９に記載の携帯端末装置において、

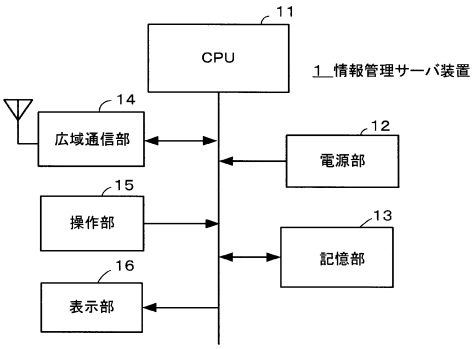
前記情報要求手段は、更に、前記認証処理手段による認証結果も送信する、
ようにしたことを特徴とする携帯端末装置である。
（請求項１１）
請求項１１に記載の発明は、請求項８に記載の携帯端末装置において、
前記情報管理装置自体の認証に用いる認証情報を入力する入力手段を更に備え、
前記情報要求手段は、前記情報管理装置に対して前記入力手段により入力された認証情報も合わせて送信することにより情報の要求を行う、
ようにしたことを特徴とする携帯端末装置である。
（請求項１２）
請求項１２に記載の発明は、請求項８に記載の携帯端末装置において、
前記受信手段は、前記情報管理装置側において前記情報要求に応答して前記機器識別情報が示す外部機器を前記端末識別情報が示す携帯端末装置によってアクセスすることが可能であると判別され、かつ、携帯端末装置の使用を許可するか否かを示す使用可否情報を参照することによってその端末使用が許可されている携帯端末装置からの要求であると判別された場合にそれを条件に送信される機器用認証情報を受信する、
ようにしたことを特徴とする携帯端末装置である。
（請求項１３）
請求項１３に記載の発明は、請求項８に記載の携帯端末装置において、
前記取得手段は、近距離通信によって探索した電子機器からその機器識別情報を受信取得する、
ようにしたことを特徴とする携帯端末装置である。
（請求項１４）
請求項１４に記載の発明は、請求項８に記載の携帯端末装置において、
アクセスが可能な複数の電子機器毎にその個々を識別する機器識別情報と当該機器識別情報毎にその機器用認証情報を記憶する機器情報記憶手段と、
前記取得手段により取得した機器識別情報に基づいて前記機器情報記憶手段を参照することによりその機器識別情報に該当する機器用認証情報が記憶されているか否かを判別する判別手段と、
を更に備え、
前記情報要求手段は、前記判別手段によって該当する機器用認証情報が記憶されていないと判別された場合に、前記情報管理装置に対して情報要求を行う、
ようにしたことを特徴とする携帯端末装置である。
（請求項１５）
請求項１５に記載の発明は、
コンピュータに対して、
携帯端末装置に対応してその携帯端末装置によりアクセスが可能な電子機器を識別する機器識別情報と当該機器識別情報毎にその機器自体の認証に用いる機器用認証情報を機器情報として記憶管理する機能と、
前記携帯端末装置に対応して任意に設定された情報であってその端末装置の使用を許可するか否かを示す使用可否情報を端末情報として記憶管理する機能と、
前記携帯端末装置から通信ネットワークを介して当該情報管理装置を経由する電子機器への間接アクセスの要求を受信した場合に、前記機器情報を参照することによってその電子機器へのアクセスが可能な携帯端末装置からの要求であるか否かを判別すると共に、前記端末情報を参照することによってその端末使用が許可されている携帯端末装置からの要求であるか否かを判別する機能と、
前記電子機器へのアクセスが可能な携帯端末装置からの要求であり、かつ端末使用が許可されている携帯端末装置からの要求であると判別された場合に、前記アクセス要求された電子機器の前記機器用認証情報をその要求元の携帯端末装置に対して送信する機能と、
を実現させるためのプログラムである。
（請求項１６）

請求項１６に記載の発明は、
コンピュータに対して、
アクセスする対象の外部機器を識別する機器識別情報を取得する機能と、
携帯端末装置毎にアクセスが可能な外部機器の機器識別情報及び機器用認証情報を記憶管理する情報管理装置に対して、通信ネットワークを介して前記取得の機器識別情報と共に自己の端末識別情報を送信することにより当該外部機器をアクセスするに必要な情報の要求を行う機能と、
前記情報要求時に受信した機器識別情報及び端末識別情報に基づいて、前記情報管理装置側で当該機器識別情報が示す外部機器を当該端末識別情報が示す携帯端末装置でアクセス可能であると判断されたことを条件に、その情報管理装置から送信される機器用認証情報を受信する機能と、
前記受信した機器用認証情報を前記アクセス対象の外部機器に対して近距離無線通信により送信する機能と、
を実現させるためのプログラムである。
【符号の説明】
【００５７】
１　情報管理サーバ装置
２　携帯端末装置
３　電子機器（外部装置）
４　公衆通信網（広域通信網）
１１、２１　ＣＰＵ
１３、２３　記憶部
１４、２４　広域通信部
２５　近距離通信部
ＥＴ　機器情報テーブル
ＴＴ　端末情報テーブル

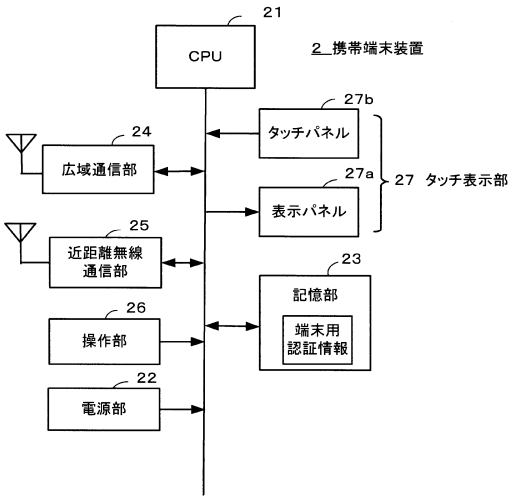
【図１】



【図２】



【図３】



【図４】

ET 機器情報テーブル

端末識別情報	機器識別情報	機器用認証情報
＊＊＊＊	＊＊＊＊	＊＊＊＊
	⋮	⋮
	＊＊＊＊	＊＊＊＊
⋮	⋮	⋮

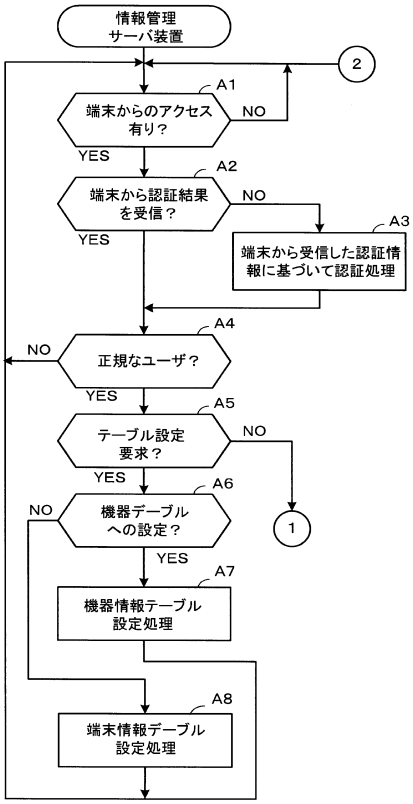
(1)

TT 端末情報テーブル

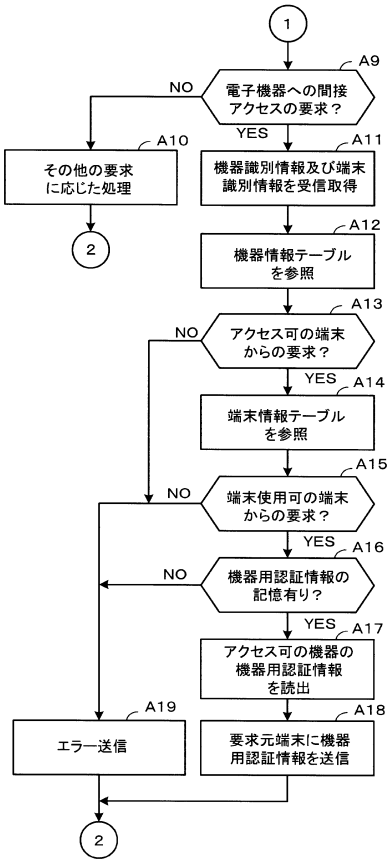
端末識別情報	端末使用 可否情報	認証情報
＊＊＊＊	有効	＊＊＊＊
＊＊＊＊	有効	＊＊＊＊
＊＊＊＊	無効	＊＊＊＊
⋮	⋮	⋮

(2)

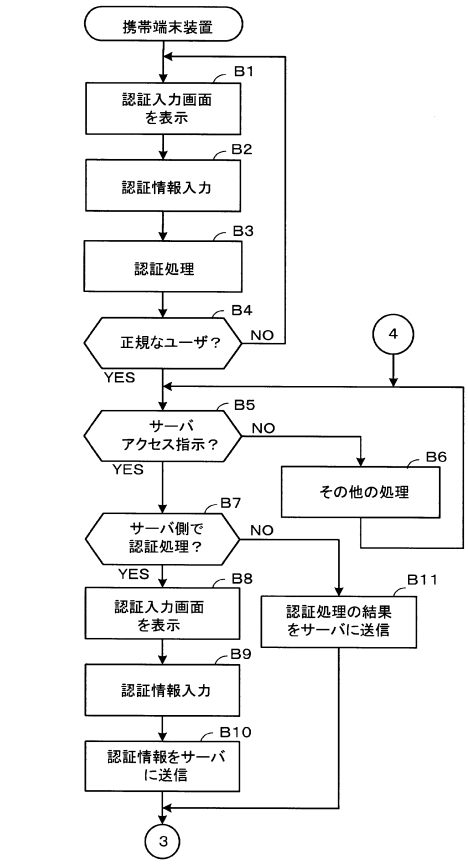
【図５】


情報管理
サーバ装置
2
A1
端末からのアクセス
有り？
NO
YES
A2
端末から認証結果
を受信？
NO
YES
A3
端末から受信した認証情
報に基づいて認証処理
A4
NO
正規なユーザ？
YES
A5
テーブル設定
要求？
NO
YES
A6
NO
機器テーブル
への設定？
1
YES
A7
機器情報テーブル
設定処理
A8
端末情報テーブル
設定処理

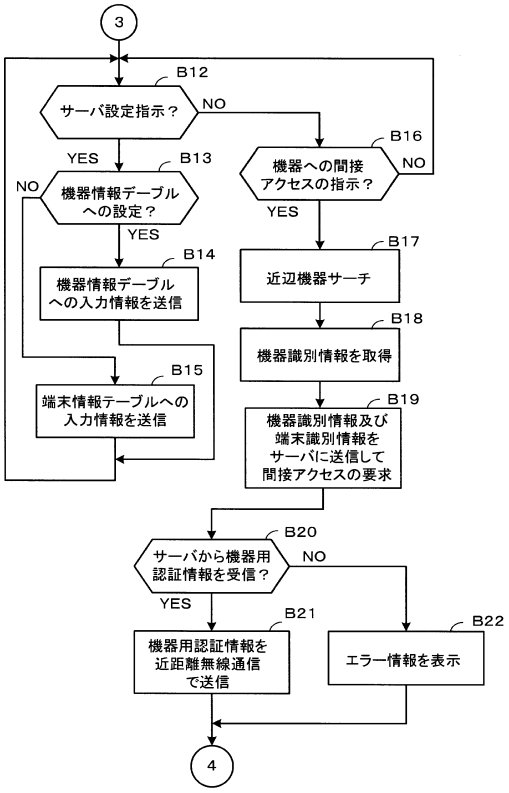
【図６】


1
A9
NO
電子機器への間接
アクセスの要求？
YES
A10
その他の要求
に応じた処理
A11
機器識別情報及び端末
識別情報を受信取得
2
A12
機器情報テーブル
を参照
A13
NO
アクセス可の端末
からの要求？
YES
A14
端末情報テーブル
を参照
A15
NO
端末使用可の端末
からの要求？
YES
A16
NO
機器用認証情報の
記憶有り？
YES
A17
アクセス可の機器の
機器用認証情報
を読出
A19
エラー送信
A18
要求元端末に機器
用認証情報を送信
2

【図７】


携帯端末装置
B1
認証入力画面
を表示
B2
認証情報入力
B3
認証処理
B4
正規なユーザ？
NO
YES
4
B5
サーバ
アクセス指示？
NO
YES
B6
その他の処理
B7
サーバ側で
認証処理？
NO
YES
B8
認証入力画面
を表示
B11
認証処理の結果
をサーバに送信
B9
認証情報入力
B10
認証情報をサーバ
に送信
3

【図８】


3
B12
サーバ設定指示？
NO
YES
B16
機器への間接
アクセスの指示？
NO
YES
B13
NO
機器情報テーブル
への設定？
YES
B17
近辺機器サーチ
B14
機器情報テーブル
への入力情報を送信
B18
機器識別情報を取得
B15
端末情報テーブルへの
入力情報を送信
B19
機器識別情報及び
端末識別情報を
サーバに送信して
間接アクセスの要求
B20
サーバから機器用
認証情報を受信？
NO
YES
B21
機器用認証情報を
近距離無線通信
で送信
B22
エラー情報を表示
4

フロントページの続き

(56)参考文献 特開２００５－３２３０７０（ＪＰ，Ａ）
特開２００６－０９９４１５（ＪＰ，Ａ）
特開２００７－１０２４４０（ＪＰ，Ａ）
特開２０００－０２９８４０（ＪＰ，Ａ）
特開２００２－３５４５５７（ＪＰ，Ａ）
米国特許出願公開第２０１２／０１６７２３２（ＵＳ，Ａ１）
特開２００６－３５２２８６（ＪＰ，Ａ）
国際公開第２０１１／０４１４１９（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４
Ｇ０６Ｆ　２１／８８