

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4844980号
(P4844980)

(45) 発行日 平成23年12月28日 (2011.12.28)

(24) 登録日 平成23年10月21日 (2011.10.21)

(51) Int.Cl.		F I			
G06Q	50/00	(2006.01)	G06F	17/60	1 3 2
G06Q	10/00	(2006.01)	G06F	17/60	5 0 6
G06F	21/20	(2006.01)	G06F	17/60	5 1 2
			G06F	15/00	3 3 0 B

請求項の数 10 (全 21 頁)

(21) 出願番号	特願2007-290689 (P2007-290689)	(73) 特許権者	000232140
(22) 出願日	平成19年11月8日 (2007.11.8)		NECフィールディング株式会社
(65) 公開番号	特開2009-116726 (P2009-116726A)		東京都港区三田1丁目4番28号
(43) 公開日	平成21年5月28日 (2009.5.28)	(74) 代理人	100123788
審査請求日	平成20年11月13日 (2008.11.13)		弁理士 宮崎 昭夫
		(74) 代理人	100106138
			弁理士 石橋 政幸
		(74) 代理人	100127454
			弁理士 緒方 雅昭
		(72) 発明者	玉岡 英樹
			東京都港区三田一丁目4番28号 NEC
			フィールディング株式会社内
		審査官	大野 朋也

最終頁に続く

(54) 【発明の名称】 情報管理システム、携帯端末、サーバ装置、情報処理方法およびプログラム

(57) 【特許請求の範囲】

【請求項1】

ネットワークを介して接続される携帯端末およびサーバ装置を含む情報管理システムであって、

前記携帯端末の利用者が操作する端末であって、前記ネットワークに接続され、前記サーバ装置から受信する情報を表示する情報端末を有し、

前記携帯端末は、

秘匿情報が保存される端末記憶部と、該秘匿情報が入力されると、該秘匿情報を前記端末記憶部に保存し、前記サーバ装置と前記ネットワークを介して通信可能か否かを判定し、通信可能であれば、前記秘匿情報を前記サーバ装置に送信する端末制御部とを有し、

前記サーバ装置は、

前記秘匿情報が保存される記憶部と、前記携帯端末から前記秘匿情報を受信すると、該秘匿情報を前記記憶部に保存する制御部とを有し、

前記携帯端末の端末制御部は、

前記秘匿情報の参照要求が入力されると、該秘匿情報を前記端末記憶部から読み出して表示し、該秘匿情報の参照が実行されたことを示す参照実行情報を前記サーバ装置に送信し、

前記サーバ装置の制御部は、

前記参照実行情報を前記携帯端末から受信すると、該参照実行情報を前記記憶部に保存するとともに、該参照実行情報を前記情報端末に送信する、情報管理システム。

10

20

【請求項 2】

前記サーバ装置の制御部は、

前記携帯端末における前記秘匿情報の消去または前記携帯端末の動作停止を要求する旨の端末使用停止要求信号を前記情報端末から受信すると、前記秘匿情報の消去または前記携帯端末の動作停止を要求する旨の使用停止信号を前記携帯端末に送信し、

前記携帯端末の端末制御部は、

前記使用停止信号を前記サーバ装置から受信すると、前記端末記憶部に保存された前記秘匿情報を消去するか、自端末の操作を無効にする、請求項 1 記載の情報管理システム。

【請求項 3】

サーバ装置とネットワークを介して接続される携帯端末であって、

秘匿情報が保存される端末記憶部と、

前記秘匿情報が入力されると、該秘匿情報を前記端末記憶部に保存し、前記サーバ装置と前記ネットワークを介して通信可能か否かを判定し、通信可能であれば、前記秘匿情報を保存することを要求する旨の情報を前記サーバ装置に送信する端末制御部と、
を有し、

前記端末制御部は、

前記秘匿情報の参照要求が入力されると、該秘匿情報を前記端末記憶部から読み出して表示し、該秘匿情報の参照が実行されたことを示す参照実行情報を、前記携帯端末の利用者が操作する端末であって、該携帯端末とは異なる情報端末へ前記ネットワークを介して前記サーバ装置に通知させるために、前記参照実行情報を該サーバ装置に送信する、携帯
端末。

【請求項 4】

前記端末制御部は、

前記秘匿情報の消去または動作停止を要求する旨の情報を前記サーバ装置から受信すると、前記端末記憶部に保存された前記秘匿情報を消去するか、自端末の操作を無効にする、請求項 3 記載の携帯端末。

【請求項 5】

秘匿情報を格納した携帯端末とネットワークを介して接続されるサーバ装置であって、
秘匿情報が保存される記憶部と、

前記秘匿情報を保存することを要求する旨の情報を前記携帯端末から受信すると、該秘匿情報を前記記憶部に保存し、該秘匿情報の参照が前記携帯端末で実行されたことを示す参照実行情報を該携帯端末から受信すると、該参照実行情報を前記記憶部に保存する制御部と、
を有し、

前記制御部は、

前記参照実行情報を前記携帯端末から受信すると、前記携帯端末の利用者が操作する端末であって、該携帯端末とは異なる情報端末へ前記ネットワークを介して前記参照実行情報を送信する、サーバ装置。

【請求項 6】

前記制御部は、

前記携帯端末における前記秘匿情報の消去または前記携帯端末の動作停止を要求する旨の端末使用停止要求信号を前記情報端末から受信すると、前記秘匿情報の消去または前記携帯端末の動作停止を要求する旨の情報を前記携帯端末に送信する、請求項 5 記載のサーバ装置。

【請求項 7】

サーバ装置とネットワークを介して接続される携帯端末による情報処理方法であって、
秘匿情報が入力されると、該秘匿情報を端末記憶部に保存し、

前記サーバ装置と前記ネットワークを介して通信可能か否かを判定し、通信可能であれば、前記秘匿情報を保存することを要求する旨の情報を前記サーバ装置に送信し、

前記秘匿情報の参照要求が入力されると、該秘匿情報を前記端末記憶部から読み出して

10

20

30

40

50

表示し、

前記秘匿情報の参照が実行されたことを示す参照実行情報を、前記携帯端末の利用者が操作する端末であって、該携帯端末とは異なる情報端末へ前記ネットワークを介して前記サーバ装置に通知させるために、前記参照実行情報を該サーバ装置に送信する、情報処理方法。

【請求項 8】

秘匿情報を格納した携帯端末とネットワークを介して接続されるサーバ装置による情報処理方法であって、

前記秘匿情報を保存することを要求する旨の情報を前記携帯端末から受信すると、該秘匿情報を記憶部に保存し、

前記秘匿情報の参照が前記携帯端末で実行されたことを示す参照実行情報を該携帯端末から受信すると、該参照実行情報を前記記憶部に保存するとともに、前記携帯端末の利用者が操作する端末であって、該携帯端末とは異なる情報端末へ前記ネットワークを介して前記参照実行情報を送信する、情報処理方法。

【請求項 9】

サーバ装置とネットワークを介して接続されるコンピュータに実行させるためのプログラムであって、

秘匿情報が入力されると、該秘匿情報を記憶部に保存し、

前記サーバ装置と前記ネットワークを介して通信可能か否かを判定し、通信可能であれば、前記秘匿情報を保存することを要求する旨の情報を前記サーバ装置に送信し、

前記秘匿情報の参照要求が入力されると、該秘匿情報を前記記憶部から読み出して表示し、

前記秘匿情報の参照が実行されたことを示す参照実行情報を、前記コンピュータの利用者が操作する端末であって、該コンピュータとは異なる情報端末へ前記ネットワークを介して前記サーバ装置に通知させるために、前記参照実行情報を該サーバ装置に送信する処理を前記コンピュータに実行させるためのプログラム。

【請求項 10】

秘匿情報を格納した携帯端末とネットワークを介して接続されるコンピュータに実行させるためのプログラムであって、

前記秘匿情報を保存することを要求する旨の情報を前記携帯端末から受信すると、該秘匿情報を記憶部に保存し、

前記秘匿情報の参照が前記携帯端末で実行されたことを示す参照実行情報を該携帯端末から受信すると、該参照実行情報を前記記憶部に保存するとともに、前記携帯端末の利用者が操作する端末であって、該携帯端末とは異なる情報端末へ前記ネットワークを介して前記参照実行情報を送信する処理を前記コンピュータに実行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、秘匿情報の管理のための情報管理システム、携帯端末、サーバ装置、情報処理装置、情報処理方法、およびその方法をコンピュータに実行させるためのプログラムに関する。

【背景技術】

【0002】

現代生活において、個人が管理するパスワードの数は非常に多くなっている。これらのパスワードは単一のサイト内にとどまっておらず、仕事上あるいは個人生活上で、様々なシステムを利用していく上で、我々は多数のパスワードを持ち、それぞれ違ったルールでつけられたパスワードを管理していく必要がある。

【0003】

これら複数のパスワードを管理する際に、あまりに多くのパスワードがあるためすべてを記憶できない場合は、パスワード管理ソフトを用いて管理する手段、または、個人の手

10

20

30

40

50

帳などにメモをしておくなどの手段がとられている（特許文献1参照）。

【特許文献1】特開2004-295711号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかし、パスワード管理ソフトを使った管理方法の場合、パスワード参照のためには、ソフトウェアがインストールされたパーソナルコンピュータ（PC）などの機器が必要となり、外出時に利用する場合などは、著しく利便性に欠けてしまう。また、故障、紛失時は復元のために別途バックアップを取得しておく必要がある。また、パスワード管理ソフトの「パスワード」を忘れた場合、復旧方法が無いなどの問題もある。

10

【0005】

手帳などの紙媒体で管理する場合、媒体紛失時にパスワード情報が漏洩してしまうおそれがある。また、情報の復旧についても、別途コピーを取るなどのバックアップを取得しておかないと、復旧が困難になる。

【0006】

本発明は上述したような技術が有する問題点を解決するためになされたものであり、パスワードなどの秘匿情報を外出先でも参照することが可能で、かつ、万が一、その秘匿情報を紛失しても復旧することが可能な情報管理システム、携帯端末、サーバ装置、情報処理装置、情報処理方法およびプログラム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】

20

【0007】

上記目的を達成するための本発明の情報管理システムは、ネットワークを介して接続される携帯端末およびサーバ装置を含む情報管理システムであって、

前記携帯端末の利用者が操作する端末であって、前記ネットワークに接続され、前記サーバ装置から受信する情報を表示する情報端末を有し、

前記携帯端末は、

秘匿情報が保存される端末記憶部と、該秘匿情報が入力されると、該秘匿情報を前記端末記憶部に保存し、前記サーバ装置と前記ネットワークを介して通信可能か否かを判定し、通信可能であれば、前記秘匿情報を前記サーバ装置に送信する端末制御部とを有し、

前記サーバ装置は、

30

前記秘匿情報が保存される記憶部と、前記携帯端末から前記秘匿情報を受信すると、該秘匿情報を前記記憶部に保存する制御部とを有し、

前記携帯端末の端末制御部は、

前記秘匿情報の参照要求が入力されると、該秘匿情報を前記端末記憶部から読み出して表示し、該秘匿情報の参照が実行されたことを示す参照実行情報を前記サーバ装置に送信し、

前記サーバ装置の制御部は、

前記参照実行情報を前記携帯端末から受信すると、該参照実行情報を前記記憶部に保存するとともに、該参照実行情報を前記情報端末に送信する構成である。

【0008】

40

また、上記目的を達成するための本発明の携帯端末は、サーバ装置とネットワークを介して接続される携帯端末であって、

秘匿情報が保存される端末記憶部と、

前記秘匿情報が入力されると、該秘匿情報を前記端末記憶部に保存し、前記サーバ装置と前記ネットワークを介して通信可能か否かを判定し、通信可能であれば、前記秘匿情報を保存することを要求する旨の情報を前記サーバ装置に送信する端末制御部と、

を有し、

前記端末制御部は、

前記秘匿情報の参照要求が入力されると、該秘匿情報を前記端末記憶部から読み出して表示し、該秘匿情報の参照が実行されたことを示す参照実行情報を、前記携帯端末の利用

50

者が操作する端末であって、該携帯端末とは異なる情報端末へ前記ネットワークを介して前記サーバ装置に通知させるために、前記参照実行情報を該サーバ装置に送信する構成である。

【0009】

また、上記目的を達成するための本発明のサーバ装置は、秘匿情報を格納した携帯端末とネットワークを介して接続されるサーバ装置であって、

秘匿情報が保存される記憶部と、

前記秘匿情報を保存することを要求する旨の情報を前記携帯端末から受信すると、該秘匿情報を前記記憶部に保存し、該秘匿情報の参照が前記携帯端末で実行されたことを示す参照実行情報を該携帯端末から受信すると、該参照実行情報を前記記憶部に保存する制御部と、

を有し、

前記制御部は、

前記参照実行情報を前記携帯端末から受信すると、前記携帯端末の利用者が操作する端末であって、該携帯端末とは異なる情報端末へ前記ネットワークを介して前記参照実行情報を送信する構成である。

【0011】

また、上記目的を達成するための本発明の情報処理方法は、サーバ装置とネットワークを介して接続される携帯端末による情報処理方法であって、

秘匿情報が入力されると、該秘匿情報を端末記憶部に保存し、

前記サーバ装置と前記ネットワークを介して通信可能か否かを判定し、通信可能であれば、前記秘匿情報を保存することを要求する旨の情報を前記サーバ装置に送信し、

前記秘匿情報の参照要求が入力されると、該秘匿情報を前記端末記憶部から読み出して表示し、

前記秘匿情報の参照が実行されたことを示す参照実行情報を、前記携帯端末の利用者が操作する端末であって、該携帯端末とは異なる情報端末へ前記ネットワークを介して前記サーバ装置に通知させるために、前記参照実行情報を該サーバ装置に送信するものである。

【0012】

さらに、上記目的を達成するための本発明のプログラムは、サーバ装置とネットワークを介して接続されるコンピュータに実行させるためのプログラムであって、

秘匿情報が入力されると、該秘匿情報を記憶部に保存し、

前記サーバ装置と前記ネットワークを介して通信可能か否かを判定し、通信可能であれば、前記秘匿情報を保存することを要求する旨の情報を前記サーバ装置に送信し、

前記秘匿情報の参照要求が入力されると、該秘匿情報を前記記憶部から読み出して表示し、

前記秘匿情報の参照が実行されたことを示す参照実行情報を、前記コンピュータの利用者が操作する端末であって、該コンピュータとは異なる情報端末へ前記ネットワークを介して前記サーバ装置に通知させるために、前記参照実行情報を該サーバ装置に送信する処理を前記コンピュータに実行させるものである。

【発明の効果】

【0013】

本発明では、秘匿情報が携帯端末に保存されているため、外出先であっても秘匿情報を確認できる。また、他の装置に秘匿情報のバックアップを取っているため、携帯端末を紛失したり、秘匿情報を誤って消去したりしても、その装置から秘匿情報を読み出すことができる。

【発明を実施するための最良の形態】

【0014】

(第1の実施形態)

本実施形態の情報管理システムの構成を説明する。

【0015】

図1は本実施形態の情報管理システムの一構成例を示すブロック図である。

【0016】

図1に示すように、利用者がパスワードの管理に用いるための携帯端末10および情報端末40がインターネットなどのネットワーク90を介して管理センタ20のLAN (Local Area Network) 60と接続されている。管理センタ20内には、パスワード管理サーバ30、端末管理サーバ50およびユーザ情報データベース80がLAN60に接続されている。なお、ネットワーク90とLAN60の間には、図に示さないファイアウォールが設けられている。以下に、各構成について詳細に説明する。

【0017】

10

図2は携帯端末の一構成例を示すブロック図である。

【0018】

携帯端末10は、音声および文字の情報の無線通信機能を備えたPDA (Personal Digital Assistant) である。携帯端末10は利用者が所有しているものであってもよく、管理センタ20から支給されるものであってもよい。以下では、管理センタ20が利用者に支給する場合とする。

【0019】

図2に示すように、携帯端末10は、ネットワーク90を介してデータを送受信する端末通信部11と、パスワードを記憶する端末記憶部13と、利用者に情報を表示するための表示部15と、各部を制御する端末制御部17と、利用者が指示を入力するための操作部19とを有する。

20

【0020】

端末制御部17は、プログラムにしたがって処理を実行するCPU (Central Processing Unit) (不図示) と、プログラムを格納するためのメモリ (不図示) とを備えている。また、このメモリには、携帯端末10毎に異なる識別子である端末識別子 (端末ID) の情報が予め登録されている。

【0021】

プログラムには、無線通信機能のためのパケット通信処理およびPDAとしての演算処理に関する内容が記述されている。また、本実施形態では、端末記憶部13に情報を保存する際に情報を暗号化するための処理と、端末記憶部13に格納された情報を読み出す際に情報を復号化するための処理の内容が記述されている。なお、パケット通信処理および演算処理については、通常の携帯電話機およびPDAと同様であるため、その詳細な説明を省略する。

30

【0022】

さらに、端末制御部17に格納されたプログラムには、利用者を認証するための認証方法が記述されている。認証方法は生体認証またはパスワード認証などいずれを用いてもよく、その方法は限定されない。生体認証の場合、認証手段が光彩認証であれば光彩を読み取るためのセンサが携帯端末10に設けられ、認証手段が指紋認証であれば指紋を読み取るためのセンサが携帯端末10に設けられ、センサが端末制御部17と接続される。以下では、認証方法がパスワード認証の場合で説明する。

40

【0023】

操作部19は、ダイヤルキーまたはキーボードなど、文字入力のためのキーが設けられている。

【0024】

端末制御部17は、受信する情報および入力される情報を暗号化して端末記憶部13に保存する。また、端末記憶部13に保存した情報を読み出す旨の指示の受信または入力があると、対象の情報を端末記憶部13から読み出して復号化した後、その情報を表示部15に出力、または端末通信部11を介して外部に送信する。

【0025】

図3は情報端末の一構成例を示すブロック図である。情報端末40は、デスクトップ型

50

やノート型のPCなどの情報処理装置である。図3に示すように、情報端末40は、通信部41、記憶部43、表示部45、制御部47および操作部49を有している。本実施形態における情報端末40の特徴は、動作手順で説明する。

【0026】

管理センタ20のLAN60は、インターネットデータセンタレベルのセキュリティを保つための設備が設けられている。上記ファイアウォール（不図示）もその設備に含まれる。パスワード管理サーバ30は利用者が登録するパスワードを管理し、端末管理サーバ50は利用者の携帯端末10の識別番号などを管理する。ユーザ情報データベース80には、利用者の登録したパスワードおよび携帯端末10の識別番号などの情報が格納される。

10

【0027】

図4はユーザ情報データベースに格納される情報の一例を示す図である。図4(a)は利用者IDテーブルであり、図4(b)はID/パスワードテーブルであり、図4(c)は利用履歴テーブルである。

【0028】

図4(a)に示すように、利用者IDテーブルは、端末ID、利用者ID、初期パスワード、利用開始フラグ、利用停止フラグ、通知機能および通知先アドレスの情報が組になって記述されている。通知機能は、登録された秘匿情報が参照された場合に携帯端末10以外の通知先に通知するか否かを示すものである。参照が実行された場合にその旨の通知先が、「通知先アドレス」である。

20

【0029】

図4(b)に示すように、ID/パスワードテーブルは、端末ID、登録ID、登録パスワードおよび利用サービスの情報が組になって記述されている。

【0030】

図4(c)に示すように、利用履歴テーブルは、シーケンス識別子（シーケンスID）、端末ID、利用サービス、利用年月日および利用時刻の情報が組になって記述されている。

【0031】

図5はパスワード管理サーバの一構成例を示すブロック図である。

【0032】

図5に示すように、パスワード管理サーバ30は、LAN60を介して通信する通信部31と、制御部37とを有する。制御部37は、プログラムにしたがって処理を実行するCPU（不図示）と、プログラムを格納するためのメモリ（不図示）とを備えている。

30

【0033】

制御部37は、LAN60およびネットワーク90を介して携帯端末10または情報端末40と情報を送受信し、プログラムにしたがって処理を実行する。処理の内容についての詳細は後述する。

【0034】

図6は端末管理サーバの一構成例を示すブロック図である。

【0035】

図6に示すように、端末管理サーバ50は、LAN60を介して通信する通信部51と、制御部57とを有する。制御部57は、プログラムにしたがって処理を実行するCPU（不図示）と、プログラムを格納するためのメモリ（不図示）とを備えている。

40

【0036】

制御部57は、LAN60およびネットワーク90を介して携帯端末10または情報端末40と情報を送受信し、プログラムにしたがって処理を実行する。処理の内容についての詳細は後述する。

【0037】

なお、ネットワーク90を介して情報の送受信には、SSL（Secure Sockets Layer）などの暗号化技術を用いるものとする。携帯端末10、情報端末40および管理センタ2

50

0内の各サーバにはその暗号化技術で情報をやり取りするためのプログラムが予め格納されている。

【0038】

上述の構成のシステムにおいて、利用者が携帯端末10を登録する手順について説明する。

【0039】

図7は携帯端末の新規登録の手順を説明するための図である。図8および図9はその手順を示すフローチャートである。

【0040】

パスワード管理のサービスの利用を開始する際、利用者は、情報端末40を操作してサービス利用を要求する旨を入力すると、情報端末40は、サービス利用を要求する旨の情報を含む新規端末登録要求信号をネットワーク90を介して端末管理サーバ50に送信する(ステップ101)。

【0041】

端末管理サーバ50は、新規端末登録要求信号を情報端末40から受信すると、図4(a)に示した利用者IDテーブルに、支給予定の携帯端末10の端末IDを新規に書き込む。そして、未使用の利用者IDおよびパスワードを生成し、これらの情報を新規の端末IDの欄に書き込む(ステップ102)。続いて、利用者IDおよびパスワードの情報をネットワーク90を介して情報端末40に送信するとともに(ステップ103)、利用者IDテーブルを更新する(ステップ104)。情報端末40は、端末管理サーバ50から受信した利用者IDおよびパスワードを表示部45に表示して利用者に通知する(ステップ105)。

【0042】

管理センタ20は、新規に登録した端末IDの携帯端末10を利用者に配送する。または、利用者が管理センタ20の受付窓口に行って携帯端末10を受け取ってもよい。その後の手順を、図9を用いて説明する。

【0043】

利用者は、携帯端末10の操作部19を操作して、利用者IDとパスワードを入力し(ステップ111)、サービス利用の開始を通知する旨を入力すると、携帯端末10は、端末ID、利用者IDおよびパスワードとサービス利用の開始を通知する旨の情報を含むサービス利用開始通知信号をネットワーク90を介して端末管理サーバ50に送信する(ステップ112)。

【0044】

図10は端末登録のための入力画面の一例を示す図である。図10に示す画面が表示部15に表示される。図10では、利用者IDの欄に入力された数字が表示され、パスワードの欄に入力された文字が表示されている。また、画面には、「送信」および「キャンセル」のボタンが表示されている。利用者が操作部19を操作して「送信」を選択すれば、携帯端末10は、入力された利用者IDとパスワードの情報を含むサービス利用開始通知信号を端末管理サーバ50に送信する。「キャンセル」を選択すれば、前の画面に戻ることが可能となる。

【0045】

端末管理サーバ50は、携帯端末10からサービス利用開始通知信号を受信すると、その信号に含まれる端末IDを利用者IDテーブルで検索する。検索の結果、端末IDが一致する組を見つけると、サービス利用開始通知信号に含まれる利用者IDおよびパスワードを読み出す。そして、これらの情報がその組に記述された情報と一致するか否かを調べる。それらの情報が一致することを確認すると(ステップ113)、利用開始フラグをオンにする。図4(a)に示す例では、利用開始フラグの欄に○印を記述している。

【0046】

そして、端末管理サーバ50は、サービス利用の開始を了承する旨のサービス利用開始了承信号をネットワーク90を介して携帯端末10に送信する(ステップ114)。携帯

10

20

30

40

50

端末10は、端末管理サーバ50からサービス利用開始了承信号を受信することで（ステップ115）、サービスを利用することが可能になる。

【0047】

次に、本サービスを利用して、秘匿対象とする利用者IDとパスワードの情報を登録する手順を説明する。以下では、秘匿すべき情報としてIDとパスワードの両方の場合で説明するが、いずれか一方であってもよく、これらの情報を登録対象情報と称する。

【0048】

図11は秘匿対象の利用者IDおよびパスワードの登録および参照の手順を説明するための図である。図12はその手順を示すフローチャートである。

【0049】

利用者が操作部19を操作して、利用者IDおよびパスワードを登録する旨を入力すると（ステップ121）、携帯端末10は、利用者IDとパスワードの入力を要求する旨の情報を表示部15に表示する。利用者は、表示部15の表示を見て、登録対象となる利用者IDおよびパスワードを入力すると（ステップ122）、携帯端末10は、入力された利用者IDおよびパスワードを暗号化して端末記憶部13に保存する（ステップ123）。

【0050】

携帯端末10は、ネットワーク90の通信圏内にあるか否かを調べる（ステップ124）。ネットワーク90の通信圏内にある場合、入力された利用者IDおよびパスワードならびに端末IDを含む登録対象情報をネットワーク90を介してパスワード管理サーバ30に送信する。パスワード管理サーバ30は、携帯端末10から登録対象情報を受信すると（ステップ125）、登録対象情報をユーザ情報データベース80のID／パスワードテーブルに書き込む（ステップ126）。

【0051】

一方、ステップ124で、ネットワーク90の通信圏外である場合、携帯端末10は、登録対象情報を送信しない。一定時間経過後、ステップ124に戻り（ステップ127）、ネットワーク90の通信圏内に入ると、登録対象情報をネットワーク90を介してパスワード管理サーバ30に送信する。

【0052】

図13は利用者IDおよびパスワードを登録するための入力画面の一例を示す図である。図13に示す画面が表示部15に表示される。図13は、〇〇銀行に設けた口座をネット上で利用する際に必要な利用者IDとパスワードを登録するためのものである。画面には、利用者IDおよびパスワードが必要となる利用システムと、利用者IDと、パスワードとがそれぞれ表示されている。利用システムが図4（b）に示すテーブルの利用サービスに相当する。

【0053】

また、画面には、「OK」および「キャンセル」のボタンが表示されている。利用者が操作部19を操作して「OK」を選択すれば、携帯端末10は、入力された利用者IDとパスワードの情報を含む登録依頼情報をパスワード管理サーバ30に送信する。「キャンセル」を選択すれば、前の画面に戻ることが可能となる。

【0054】

次に、利用者が携帯端末10を操作して登録した利用者IDおよびパスワードを参照する手順を説明する。図14はその手順を示すフローチャートである。

【0055】

利用者は携帯端末10の操作部19を操作して、利用者認証のためのパスワードを入力する。携帯端末10は、入力されたパスワードが利用者自身のものであることを確認すると、操作可能な状態にする。利用者が操作部19を操作して、登録対象情報の参照を要求する旨を入力すると（ステップ131）、携帯端末10は、端末記憶部13に登録されたIDおよびパスワードの情報を表示部15に表示する（ステップ132）。続いて、ネットワーク90の通信圏内にあるか否かを調べる（ステップ133）。

【0056】

ステップ133で、ネットワーク90の通信圏内である場合、携帯端末10は、登録情報の参照が行われたことを通知する旨の参照実行情報をネットワーク90を介してパスワード管理サーバ30に送信する。パスワード管理サーバ30は、携帯端末10から参照実行情報を受信すると（ステップ134）、参照実行情報を履歴として図4（c）に示した利用履歴テーブルに登録する（ステップ135）。そして、図4（a）に示した利用者IDテーブルを参照して、通知機能がオンしているか否かを調べる（ステップ136）。

【0057】

ステップ136でオンしている場合、パスワード管理サーバ30は、通知先アドレスに参照実行情報を転送する。ここでは、通知先アドレスが情報端末40で登録されたメールアドレスになっているため、情報端末40を宛先として参照実行情報を転送する（ステップ137）。

10

【0058】

一方、ステップ133で、携帯端末10がネットワーク90の通信圏外である場合、携帯端末10は、参照実行情報を送信しない。一定時間経過後、ステップ133に戻り（ステップ138）、携帯端末10は、ネットワーク90の通信圏内に入ると、参照実行情報をネットワーク90を介してパスワード管理サーバ30に送信する。

【0059】

このように、予め通知機能をオンに設定しておくことで、利用者ID／パスワードの登録対象情報が携帯端末10において参照されたという情報が、携帯端末10からパスワード管理サーバ30に参照実行情報が送られたタイミングで、予め指定された通知先にパスワード管理サーバ30から送信される。この参照実行情報の通知は、インターネットメールやSMS（Short Message Service）送信などによるメールで行われる。通知先は、情報端末40に限らず、その他のPDAや携帯端末であってもよい。

20

【0060】

図15は登録対象情報を参照したときの表示画面の一例を示す図である。図15に示す画面が表示部15に表示される。画面には、利用者IDおよびパスワードが必要となる利用システムと、利用者IDと、パスワードとがそれぞれ表示されている。利用システムの欄の「▼」を選択すると、その他の利用システムが表示されるようになっている。別の利用システムの利用者IDとパスワードが知りたければ、対象となる利用システムを選択した後、「OK」を選択すればよい。「キャンセル」を選択すれば、前の画面に戻ることが可能となる。

30

【0061】

次に、利用者が携帯端末10を紛失した際、他人が不正に利用者IDおよびパスワードを見たか否かを確認する場合を説明する。

【0062】

図16は携帯端末を紛失したときの対処法を説明するための図である。図17は参照履歴を確認するための手順を示すフローチャートである。

【0063】

利用者が情報端末40を操作して、参照履歴を要求する旨を入力すると（ステップ141）、情報端末40は、参照履歴を要求する旨と携帯端末10の端末IDの情報を含む参照履歴要求信号をネットワーク90を介してパスワード管理サーバ30に送信する（ステップ142）。パスワード管理サーバ30は、情報端末40から参照履歴要求信号を受信すると、その信号に含まれる端末IDについての参照履歴を示す情報である参照履歴情報をユーザ情報データベース80内の利用履歴テーブルから読み出し（ステップ143）、要求元の情報端末40宛にネットワーク90を介して参照履歴情報を送信する（ステップ144）。

40

【0064】

情報端末40は、パスワード管理サーバ30から参照履歴情報を受信すると、参照履歴情報を表示する（ステップ145）。図18は参照履歴情報の表示画面の一例を示す図で

50

ある。画面には、参照された年月日および時刻、参照された利用システムの名称、ならびに参照された秘匿情報が組になって、古い日時の参照から新しい日時の参照の順に示されている。参照された情報がパスワードのみであると、「パスワードのみ」と表示されている。

【0065】

利用者は、上述のようにして表示された参照履歴情報を見て、身に覚えのない参照履歴があるか否かを調べ、利用者IDおよびパスワードの秘匿情報の漏洩があったかどうかをチェックすることが可能となる。このようにして、利用者は、携帯端末10を紛失したとき、情報端末40を利用し、管理センタ20に登録された参照履歴情報を確認することで、他人が利用者IDまたはパスワードを参照したかどうかを確認することができる。

10

【0066】

また、図14で説明したように、通知機能をオンにしておけば、利用者IDまたはパスワードが参照された時点で、そのことをメールなどの手段を用いて携帯端末10以外の端末に受信することが可能となる。これにより、自分の利用者IDまたはパスワードを他人が参照したことをリアルタイムに知ることができる。

【0067】

自分の秘匿情報を他人が参照したか否かの情報を元に、利用者は、情報漏洩したおそれのある利用者IDおよびパスワードの使用を停止したり、それらの情報を変更したりすることなどの対処ができる。

【0068】

20

次に、自分の利用者IDおよびパスワードの他人による参照の形跡を参照履歴情報で確認し、それらの情報が漏洩したおそれがあると判断した場合、登録した利用者IDおよびパスワードの使用を停止する手順を説明する。

【0069】

図19は登録した利用者IDおよびパスワードを消去するための手順を示すフローチャートである。

【0070】

利用者は、情報端末40の操作部49を操作して、登録対象情報の消去を要求する旨を入力すると、情報端末40は、携帯端末10の端末ID、登録対象情報の消去を要求する旨、および携帯端末10の動作停止を要求する旨の端末使用停止要求信号をネットワーク90を介して端末管理サーバ50に送信する（ステップ151）。

30

【0071】

端末管理サーバ50は、情報端末40から端末使用停止要求信号を受信すると（ステップ152）、その信号から端末IDを読み出し、使用停止対象とする携帯端末10を特定する（ステップ153）。続いて、特定した携帯端末10がネットワーク90の通信圏内にあるか否かを調べる（ステップ154）。

【0072】

ステップ154で携帯端末10がネットワーク90の通信圏内にある場合、端末管理サーバ50は、登録対象情報の消去と動作停止を指示する旨の使用停止信号をネットワーク90を介して携帯端末10に送信する。携帯端末10は、端末管理サーバ50から使用停止信号を受信すると（ステップ155）、端末記憶部13に保存した登録対象情報を消去するとともに、操作部19の操作が無効になるようにロックする（ステップ156）。

40

【0073】

一方、ステップ154で、携帯端末10がネットワーク90の通信圏外である場合、端末管理サーバ50は、使用停止信号を送信しない。一定時間経過後、ステップ154に戻り（ステップ157）、携帯端末10がネットワーク90の通信圏内に入ると、端末管理サーバ50は、使用停止信号をネットワーク90を介して携帯端末10に送信する。

【0074】

このようにして、携帯端末10の紛失時に、秘匿すべき登録対象情報を消去し、携帯端末10の操作をロックさせることで、登録対象情報の流出被害の拡大を防ぐことができる

50

。なお、ここでは、登録対象情報の消去と操作ロックの両方を実施したが、いずれか一方だけであってもよい。

【0075】

次に、新たな携帯端末70を利用者に配付するための手順を説明する。図20は携帯端末を再配付する手順を説明するための図であり、図21はその手順を示すフローチャートである。なお、新たに配付される携帯端末70の構成は図2で説明した携帯端末10と同様な構成であるため、その詳細な説明を省略する。

【0076】

利用者は、図17で説明したようにして参照履歴情報を見て、他人が自分の登録対象情報を参照したと判断すると、参照履歴情報を元に、利用者IDおよびパスワードの使用先となる利用システムを特定する。そして、それらの利用システムについて漏洩した可能性のある利用者IDおよびパスワードの情報を、情報端末40を操作して変更する（ステップ161）。ここでいう利用システムとは、自分の勤める会社の社員用サーバ、Webメール、および銀行キャッシュディスペンサーなどである。

10

【0077】

利用者は情報端末40を操作して、新たな端末を要求する旨を入力すると、情報端末40は、本サービスを利用するために発行された利用者ID、変更した登録対象情報、および携帯端末の再配付を要求する旨の情報を含む端末再配付要求信号をネットワーク90を介して端末管理サーバ50に送信する（ステップ162）。

20

【0078】

端末管理サーバ50は、情報端末40から端末再配付要求信号を受信すると、信号に含まれる利用者IDに一致するIDを利用者IDテーブルで特定し、その組の端末IDに新規の端末IDと、新たに生成したパスワードを書き込む。また、その端末IDに関するデータを入力するための欄をID／パスワードテーブルに新たに設け、端末再配付要求信号に含まれる登録対象情報を書き込む（ステップ163）。

【0079】

続いて、端末管理サーバ50は、予め通信可能に接続された、上記端末IDの携帯端末70に上記登録対象情報をLAN60を介して送信する（ステップ164）。携帯端末70は、端末管理サーバ50から受信した登録対象情報を端末記憶部13に保存する（ステップ165）。その後、図7で説明したのと同様にして、端末管理サーバ50は、ネットワーク90を介して情報端末40宛に、利用者IDおよびパスワードの情報を情報端末40に送信する。

30

【0080】

管理センタ20は、新規に登録した端末IDの携帯端末70を利用者に配送する。または、利用者が管理センタ20の受付窓口に行って携帯端末70を受け取ってもよい。配付方法は、本人認証やセキュリティが担保される方法であれば、特に方法は問わない（キャッシュカード、クレジットカードの送付程度のセキュリティが確保されればかまわない）。

【0081】

利用者が携帯端末70の操作部19を操作して、サービス利用の開始を通知する旨を入力すると、携帯端末70は、サービス利用開始通知信号をネットワーク90を介して端末管理サーバ50に送信する。端末管理サーバ50は、携帯端末70からサービス利用開始通知信号を受信すると、図9で説明した処理を行って、サービス利用開始了承信号をネットワーク90を介して携帯端末70に送信する。携帯端末70は、端末管理サーバ50からサービス利用開始了承信号を受信することで、サービスを利用することが可能になる。

40

【0082】

なお、ここでは、パスワード管理サーバ30は、既に発行された利用者IDを用いて携帯端末70を再配付したが、新規に利用者IDを取得してもよい。

【0083】

本実施形態では、秘匿情報が携帯端末に保存されているため、外出先であっても携帯端

50

末を操作して秘匿情報を確認することが可能となる。また、管理センタのユーザ情報データベースのように、携帯端末とは別の装置に通信可能な状態のときに、秘匿情報のバックアップを取っているため、携帯端末を紛失したり、秘匿情報を誤って消去したりしても、その装置から秘匿情報を読み出すことができる。

【0084】

また、携帯端末に秘匿情報を保存するときに暗号化したり、携帯端末を操作する際に認証を必要としたりすることで、情報漏洩のリスクが低減する。

【0085】

本実施形態によれば、携帯端末に保存した秘匿情報を参照する際に利用者の認証が行われるため、一度の認証で複数の秘匿情報を管理でき、利用者は複数のパスワードを覚える必要がない。

10

【0086】

また、秘匿情報が携帯端末そのものに登録しているため、ネットワークを介してサーバ装置から秘匿情報を読み出す必要がなく、ネットワークの通信圏外でも秘匿情報を利用できる。

【0087】

また、携帯端末による秘匿情報に対する参照履歴が管理センタ側に記録されているため、携帯端末の紛失時に、利用者はそれを参照することにより、自身の覚えのない参照履歴があるか否かを確認でき、情報漏洩の可能性を判断できる。

【0088】

20

また、参照が実行されたときに他の情報端末に通知するようにしておくことで、携帯端末で他人により秘匿情報の参照が行われると、参照が実行されたことが正規の利用者に通知される。

【0089】

また、携帯端末紛失時に、他の端末を介して携帯端末に秘匿情報の消去または操作を無効化するので、秘匿情報の流出被害の拡大を防ぐことができる。

【0090】

さらに、サーバ装置に秘匿情報のバックアップを取っているため、携帯端末を紛失しても秘匿情報の復旧が容易である。

【0091】

30

(第2の実施形態)

第1の実施形態では、携帯端末10を直接操作して秘匿情報を携帯端末10に保存していたが、本実施形態では、他の端末として情報端末40を操作してそれらの情報を携帯端末10に登録するものである。

【0092】

本実施形態の情報管理システムでは、情報端末40は、秘匿情報の登録を要求する旨が入力されると、その入力を要求する旨を表示部45に表示する。そして、秘匿情報とその登録先となる携帯端末10の端末IDが入力されると、秘匿情報、秘匿情報のサーバへの登録、端末ID、および該端末IDで特定される端末への秘匿情報の登録を要求する旨の情報を含む登録要求情報をパスワード管理サーバ30に送信する。なお、端末IDは予め記憶部43に格納されていてもよい。

40

【0093】

パスワード管理サーバ30は、記憶部(不図示)を備え、情報端末40から登録要求情報を受信すると、そのうちの秘匿情報を携帯端末10に送信するまで記憶部に保存する。

【0094】

また、携帯端末10は、秘匿情報をネットワーク90を介してパスワード管理サーバ30から受信すると、秘匿情報を暗号化して端末記憶部13に保存する。それ以外の構成については、第1の実施形態と同様であるため、その詳細な説明を省略する。以下では、第1の実施形態と異なる点を詳しく説明する。

【0095】

50

本実施形態における、秘匿情報の携帯端末１０への登録方法を説明する。

【００９６】

図２２は秘匿情報の携帯端末への登録のための手順を示すフローチャートである。

【００９７】

利用者が情報端末４０の操作部４９を操作して、利用者ＩＤおよびパスワードを登録する旨を入力すると、情報端末４０は、利用者ＩＤとパスワードの入力を要求する旨の情報を表示部４５に表示する。利用者は、表示部４５の表示を見て、秘匿情報となる利用者ＩＤおよびパスワードを入力すると、情報端末４０は、携帯端末１０の端末ＩＤ、秘匿情報、および秘匿情報の登録を要求する旨の情報を含む登録要求情報をネットワーク９０を介してパスワード管理サーバ３０に送信する（ステップ２０１）。 10

【００９８】

パスワード管理サーバ３０は、情報端末４０から登録要求情報を受信すると（ステップ１２５）、登録要求情報を記憶部（不図示）に保存する（ステップ２０２）。続いて、その情報に含まれる端末ＩＤの携帯端末１０がネットワーク９０の通信圏内にあるか否かを調べる（ステップ２０３）。 20

【００９９】

ステップ２０３で携帯端末１０がネットワーク９０の通信圏内にある場合、パスワード管理サーバ３０は、秘匿情報をネットワーク９０を介して携帯端末１０に送信する。携帯端末１０は、パスワード管理サーバ３０から秘匿情報を受信すると（ステップ２０４）、秘匿情報を暗号化して端末記憶部１３に保存する（ステップ１５６）。パスワード管理サーバ３０は、秘匿情報をユーザ情報データベース８０に保存し、記憶部内の登録要求情報を消去する。 30

【０１００】

一方、ステップ２０３で、携帯端末１０がネットワーク９０の通信圏外である場合、パスワード管理サーバ３０は、秘匿情報を送信しない。一定時間経過後、ステップ２０３に戻り（ステップ２０６）、携帯端末１０がネットワーク９０の通信圏内に入ると、秘匿情報をネットワーク９０を介して携帯端末１０に送信する。その後、上述したように、パスワード管理サーバ３０は、記憶部に保存した秘匿情報をユーザ情報データベース８０に移す。 40

【０１０１】

本実施形態では、秘匿情報の携帯端末１０への登録が情報端末４０でなければならないようにすることで、携帯端末１０での処理が図１２で説明した場合よりも簡略化することができ、携帯端末１０の製作コストの削減が可能になる。 50

【０１０２】

なお、上記実施形態では、管理センタ２０内のサーバをパスワード管理サーバ３０と端末管理サーバ５０とに別々に設けたが、パスワード管理サーバ３０が端末管理サーバ５０の機能を備えるようにしてもよい。また、ユーザ情報データベース８０を記憶部として、サーバに設けられていてもよい。

【０１０３】

また、携帯端末を管理センタ２０が配付する場合で説明したが、利用者が所有する携帯端末で行うようにしてもよい。また、図２に示す構成のうち、操作部１９、表示部１５および端末通信部１１は、通常用いられる携帯端末と同様な構成であっても、本発明を実施することが可能である。図３に示す構成のうち、操作部４９、表示部４５および通信部４１は、通常用いられるＰＣ等の情報処理装置と同様な構成であっても、本発明を実施することが可能である。 60

【０１０４】

本発明は、個人でいくつもの利用者ＩＤおよびパスワードを管理および記憶することが困難な場合に有効である。

【０１０５】

また、企業での利用も考えられる。特に、中小規模の企業で自社内ですべての業務用シ 70

システムを構築できず、複数のASPサービスを利用している場合、シングルサインオンなどの仕組みが構築できないケースにおいて、統合的に利用者IDおよびパスワードを管理する用途に、本発明を利用できる。

【図面の簡単な説明】

【0106】

【図1】第1の実施形態のパスワード管理システムの一構成例を示すブロック図である。

【図2】携帯端末の一構成例を示すブロック図である。

【図3】情報端末の一構成例を示すブロック図である。

【図4】ユーザ情報データベースに格納される情報の一例を示す図である。

【図5】パスワード管理サーバの一構成例を示すブロック図である。

10

【図6】端末管理サーバの一構成例を示すブロック図である。

【図7】携帯端末の新規登録の手順を説明するための図である。

【図8】携帯端末の新規登録の手順を示すフローチャートである。

【図9】携帯端末の新規登録の手順を示すフローチャートである。

【図10】端末登録のための入力画面の一例を示す図である。

【図11】秘匿対象の利用者IDおよびパスワードの登録および参照の手順を説明するための図である。

【図12】秘匿対象の利用者IDおよびパスワードの登録の手順を示すフローチャートである。

【図13】利用者IDおよびパスワードを登録するための入力画面の一例を示す図である。

20

【図14】利用者IDおよびパスワードを参照する手順を示すフローチャートである。

【図15】登録対象情報を参照したときの表示画面の一例を示す図である。

【図16】携帯端末を紛失したときの対処法を説明するための図である。

【図17】参照履歴を確認するための手順を示すフローチャートである。

【図18】参照履歴情報の表示画面の一例を示す図である。

【図19】登録した利用者IDおよびパスワードを消去するための手順を示すフローチャートである。

【図20】携帯端末を再配付する手順を説明するための図である。

【図21】携帯端末を再配付する手順を示すフローチャートである。

30

【図22】第2の実施形態における、秘匿情報の携帯端末への登録のための手順を示すフローチャートである。

【符号の説明】

【0107】

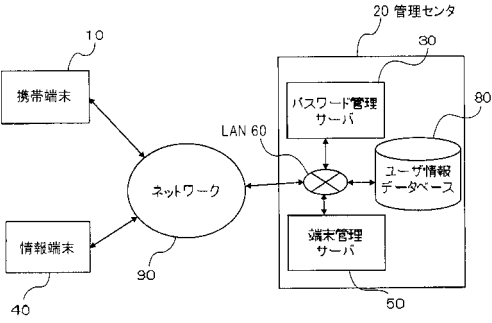
10 携帯端末

30 パスワード管理サーバ

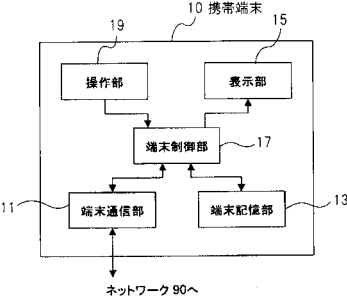
40 情報端末

50 端末管理サーバ

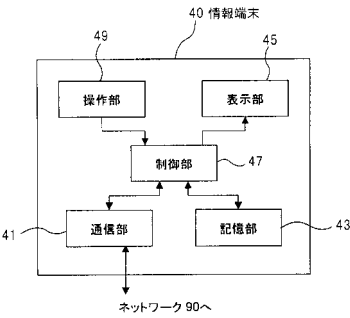
【図 1】



【図 2】



【図 3】



【図 4】

端末ID	利用者ID	初期パスワード	利用開始フラグ	利用停止フラグ	通知機能	通知先アドレス
AZD0001	0123456	saftcityras	○	x	ON	x x x x @○○
AZD0003	1234567	lucappl	x	○	OFF	-
YRQ2358	2345678	lsr7ned	○	○	ON	△△△△@x x x

(a)

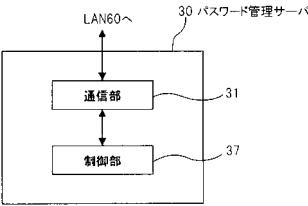
端末ID	登録パスワード	利用サービス
AZD0001	QWERTY	プロバイダログイン
AZD0001	ASDFGHJ	○○銀行Web通帳
AZD0001	null	○○クレジットカード

(b)

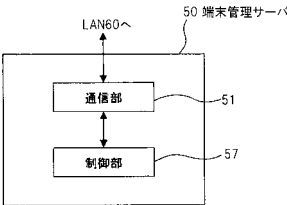
セッションID	端末ID	利用サービス	利用年月日	利用時刻
00001	AZD0001	プロバイダログイン	2007/8/10	12:35:17
00002	AZD0001	○○銀行Web通帳	2007/9/12	22:24:50
00003	AZD0001	○○クレジットカード	2007/9/25	12:00:45

(c)

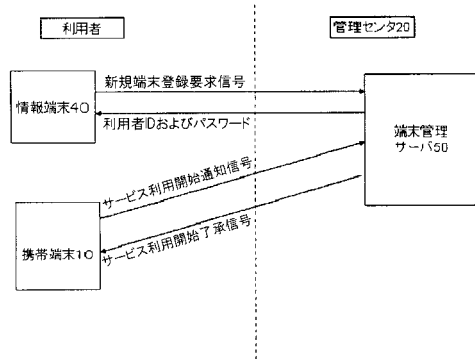
【図 5】



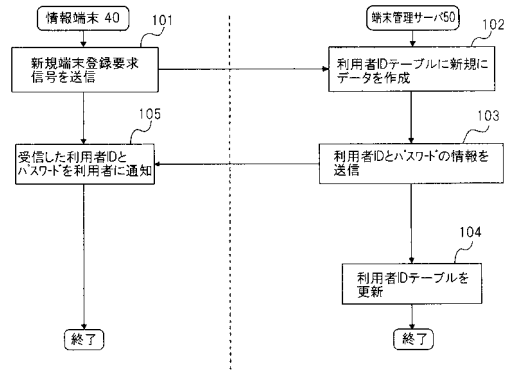
【図 6】



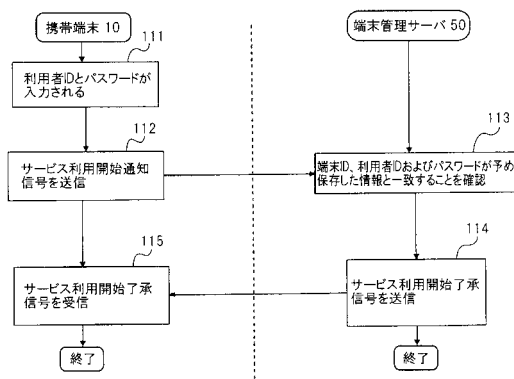
【図 7】



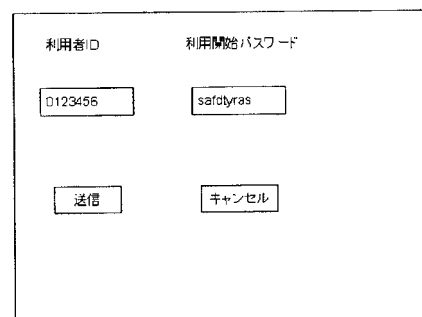
【図 8】



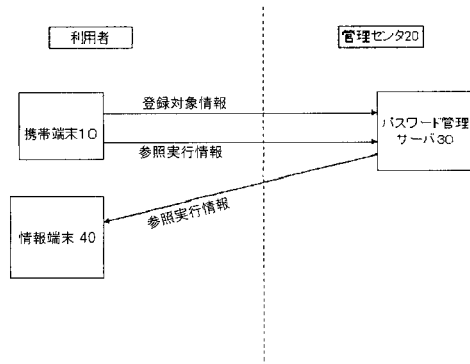
【図 9】



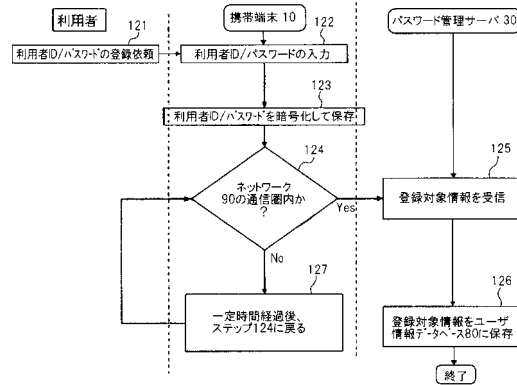
【図 10】



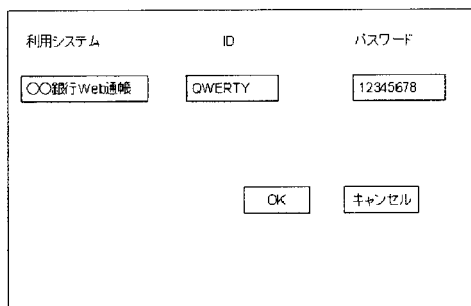
【図 1 1】



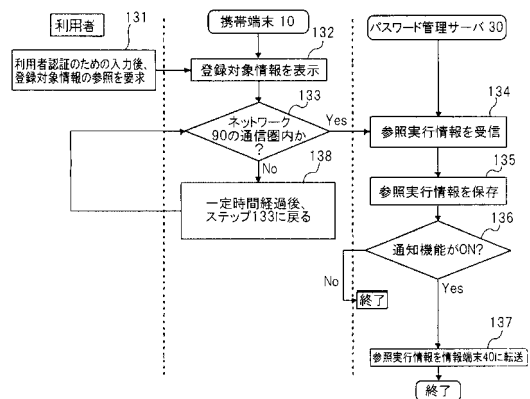
【図 1 2】



【図 1 3】



【図 1 4】



【図 15】

利用システム

ID

パスワード

〇〇銀行Web通帳 ▼

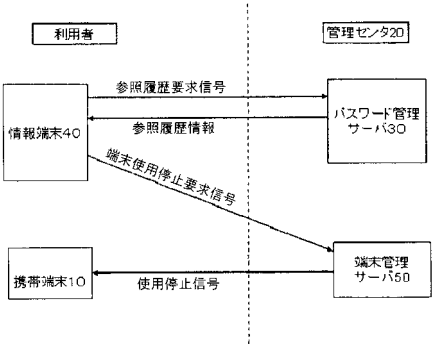
QWERTY

12345678

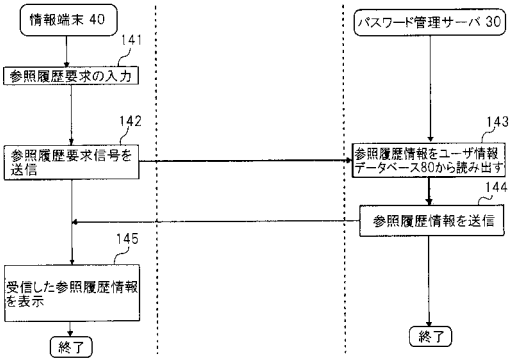
OK

キャンセル

【図 16】



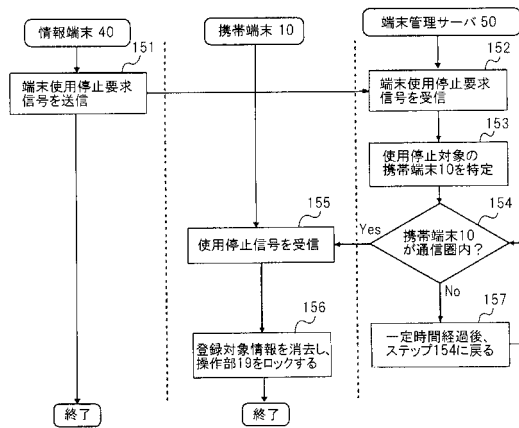
【図 17】



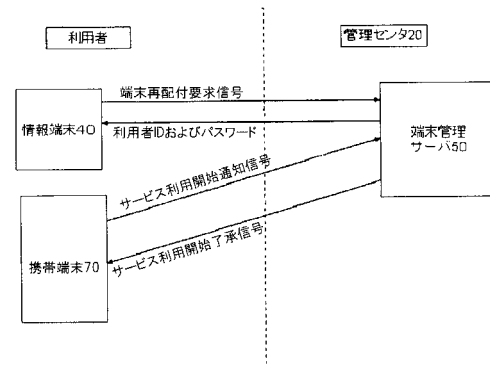
【図 18】

表示日	表示時刻	表示システム	表示ID
2007/08/12	10:42	××銀行CD	パスワードのみ
2007/08/12	11:42	〇〇銀行Web通帳	ABCDEFG
2007/08/12	15:31	△△システムWebメール	12AB4ZD
2007/08/13	8:25	会社ドメインログイン	QWERTY
2007/08/13	18:00	JR Suicaチャージ	パスワードのみ
2007/08/13	21:34	□□クレジット会員サイト	asdzxc

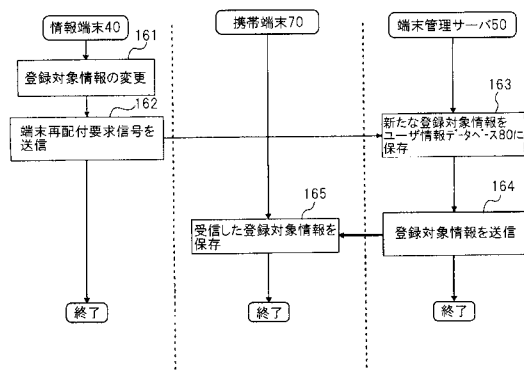
【図 19】



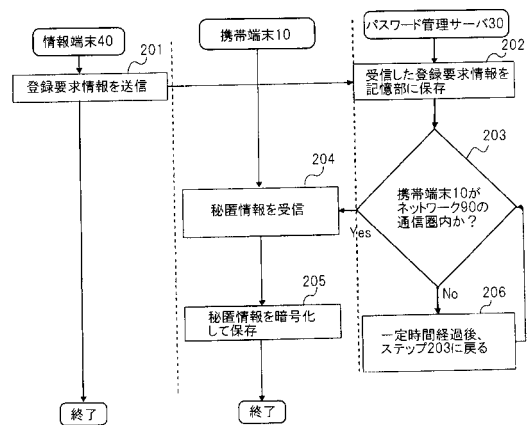
【図 20】



【図 21】



【図 22】



フロントページの続き

- (56)参考文献 特開2002-222274 (JP, A)
特開2007-265176 (JP, A)
特開2003-323344 (JP, A)
特開2004-295711 (JP, A)
特開2000-270376 (JP, A)
特開2000-22839 (JP, A)
中井 奨, リスク高まる端末の紛失・盗難 拡充進むセキュリティ対策を見る, 日経コミュニケーション, 日本, 日経BP社, 2007年 2月15日, 第480号, p.84-89

- (58)調査した分野(Int.Cl., DB名)
G06Q 10/00-50/00
G06F 21/20