(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3659019号
(P3659019)
(45)発行日　平成17年6月15日(2005.6.15)　(24)登録日　平成17年3月25日(2005.3.25)

(51)Int.Cl.[7]　F I
G06F 15/00　G06F 15/00　330G

請求項の数 6　(全 11 頁)

(21)出願番号　特願平10-274552
(22)出願日　平成10年9月29日(1998.9.29)
(65)公開番号　特開2000-105747(P2000-105747A)
(43)公開日　平成12年4月11日(2000.4.11)
審査請求日　平成13年9月20日(2001.9.20)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　齋藤　洋子
神奈川県横浜市戸塚区戸塚町５０３０番地
株式会社日立製作所　ソフトウェア事業部内

審査官　中野　裕二

最終頁に続く

(54)【発明の名称】可搬媒体を用いたシングルログイン制御方法および該方法を実現するためのプログラムを格納した記録媒体および装置

(57)【特許請求の範囲】

【請求項１】

クライアント、業務サーバおよび統合認証サーバが接続したシステムにおける可搬媒体を用いたシングルログイン制御方法であって、

前記クライアントは、ユーザから認証情報と可搬媒体を用いたログイン処理とを受け付け、

前記認証情報と可搬媒体を用いたログイン処理とに基づき、クライアントで認証し、

前記認証の結果に応じて、前記クライアントが、前記可搬媒体に格納された前記業務サーバ及び前記統合サーバへのログイン情報を取得し、該ログイン情報を用いて前記業務サーバおよび前記統合認証サーバへのログイン処理を行うことを特徴とする可搬媒体を用いたシングルログイン制御方法。

【請求項２】

前記クライアントでの認証処理の結果、前記可搬媒体での認証を許可できない場合に、前記可搬媒体を無効とすることを特徴とする請求項１記載の可搬媒体を用いたシングルログイン制御方法。

【請求項３】

クライアント、業務サーバおよび統合認証サーバが接続したシステムにおける可搬媒体を用いたシングルログイン制御方法を実現するプログラムを格納した記録媒体であって、

前記クライアントは、ユーザから認証情報と可搬媒体を用いたログイン処理とを受け付け、

前記認証情報と可搬媒体を用いたログイン処理とに基づき、クライアントで認証処理を行い、
前記認証処理の結果に応じて、前記クライアントが、前記可搬媒体に格納された前記業務サーバ及び前記統合サーバへのログイン情報を取得し、該ログイン情報を用いて前記業務サーバおよび前記統合認証サーバへのログイン処理を行うことを特徴とする可搬媒体を用いたシングルログイン制御方法を実現するプログラムを格納した記録媒体。
【請求項４】
クライアント、業務サーバおよび統合認証サーバが接続したシステムにおける可搬媒体を用いたシングルログイン制御装置であって、
前記クライアントは、ユーザから認証情報と可搬媒体を用いたログイン処理とを受け付ける情報入出力制御部と、
前記認証情報と可搬媒体を用いたログイン処理とに基づき、クライアントで認証処理を行い、
前記認証処理の結果に応じて、前記可搬媒体に格納された前記業務サーバ及び前記統合サーバへのログイン情報を取得し、該ログイン情報を用いて前記業務サーバおよび前記統合認証サーバへのログイン処理を行う認証クライアントを有することを特徴とする可搬媒体を用いたシングルログイン制御装置。
【請求項５】
請求項１または２記載のシングルログイン制御方法において、
前記クライアントは、前記可搬媒体に格納された前記業務サーバ及び前記統合サーバへのログイン情報を前記可搬媒体から読み取る可搬媒体読み取り装置を有し、
前記可搬媒体を前記読み取り装置から外されることにより、前記クライアントは前記業務サーバ及び前記統合サーバへの業務処理を終了する
ことを特徴とする請求項１または２記載のシングルログイン制御方法。
【請求項６】
請求項４記載のシングルログイン制御装置において、
前記クライアントは、前記可搬媒体に格納された前記業務サーバ及び前記統合サーバへのログイン情報を前記可搬媒体から読み取る可搬媒体読み取り装置を有し、
前記可搬媒体を前記読み取り装置から外されることにより、前記クライアントは前記業務サーバ及び前記統合サーバへの業務処理を終了する
ことを特徴とする請求項４記載のシングルログイン制御装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
従来の企業情報システムでセキュリティ管理機能を提供すると、エンドユーザは、OSやアプリケーションシステムごとにログイン操作が要求された。例えば、モバイル端末から社内の業務サーバ内のAPを起動する場合には、まずVPN、次にグループウェア、さらには使用する業務AP、流通APやユーザAPごとにログインしなければならなかった。Windows（登録商標）NTサーバを使ってドメイン内のユーザ情報を管理している場合には、NTドメインへのログインも要求された。これは、エンドユーザにとっては大変な負担であり、覚えきれないパスワードをメモ書きして机上に貼っておくことにより、結果的にセキュリティレベルを低下させる危険もはらんでいた。
【０００２】
このようなセキュリティ運用負荷を軽減させるためには、シングルログインを実現するユティリティとAP開発環境及び実行環境の提供が重要である。本発明は、可搬媒体を利用して広域ネットワークシステムでシングルログインを実現するための画面制御方法に関わるもので、先願発明(特願平9-76954)で提案した統合認証サーバとの連携を実現するユーザ認証方法を対象とする。
【０００３】
【従来の技術】

既に述べたように、セキュリティ運用負荷を軽減させるためには、シングルログインを実現するユティリティとAP開発環境及び実行環境の提供が重要である。シングルログイン方式としては、従来業務ごとに必要だったユーザIDとパスワードを、１つのユーザIDとパスワードに集約する方法がある。すなわち、ユーザが1回ログイン情報を入力すれば、以降全ての業務へのログインを可能とする。確かに、これは、セキュリティの運用負荷を軽減する方式ではあるが、同時にセキュリティを弱めてしまう危険もはらんでいる。もしも、前記集約したユーザIDとパスワードが破られてしまったら、悪意を持った第3者は以前より容易にシステム侵入ができ、これにより企業の機密情報が危険にさらされてしまうからである。

【０００４】

一回のログインにより企業情報システムの資源にアクセスさせるシングルログインは、強固なユーザ認証基盤の提供の上に初めて実現できる。従って、ログイン情報をきちんと管理する基盤として先願発明(特願平9-76954)の技術を用いた上での、シングルログイン方式の提供が必要と考えた。特に、知っている情報による認証から持っている情報、さらには生物的な情報（指紋や網膜、DNA情報等）を視野にいれた技術の適用が要求される。

【０００５】

【発明が解決しようとする課題】

本発明の目的は、企業情報システムにおいて、可搬媒体を利用したシングルログインを実現することである。特願平9-76954の方式では、1枚の証明証の情報で企業情報システムの中でシングルログインを実現するために、統合認証サーバで前記証明証の情報を確認しユーザ認証をする。同様のユーザ認証処理をクライアント側で実現することが本発明の課題である。クライアント側にログイン情報を管理するためには、セキュリティや運用の観点からPCのハードディスクに置くことはできない。そのため、セキュアな可搬媒体の利用が必須となっている。現在では、可搬媒体としてFDやICカードが主流かもしれないが、指輪やネクタイピン、イヤリングなどを用いたり、指紋や網膜等の生物的な情報との併用も課題となっている。

【０００６】

【課題を解決するための手段】

本発明によれば、クライアント、業務サーバおよび統合認証サーバが接続したシステムにおける可搬媒体を用いたシングルログイン制御方法であって、前述のクライアントは、ユーザから認証情報と可搬媒体を用いたログイン処理とを受け付け、前述の認証情報と可搬媒体を用いたログイン処理とに基づき、クライアントで認証し、前述の認証の結果に応じて、前述の可搬媒体に格納されたログイン情報を取得し、前述の業務サーバおよび前記統合認証サーバへのログイン処理を行うことを特徴とする。

また、本発明によれば、クライアント、業務サーバおよび統合認証サーバが接続したシステムにおける可搬媒体を用いたシングルログイン制御装置であって、前述のクライアントは、ユーザから認証情報と可搬媒体を用いたログイン処理とを受け付ける情報入出力制御部と、前述の認証情報と可搬媒体を用いたログイン処理とに基づき、クライアントで認証処理を行い、前述の認証処理の結果に応じて、前述の可搬媒体に格納されたログイン情報を取得し、前述の業務サーバおよび前述の統合認証サーバへのログイン処理を行う認証クライアントを有することを特徴とする。

【０００７】

ユーザに可搬媒体を発行するために、可搬媒体発行申請画面をユーザに表示する手段、ユーザが前記可搬媒体申請画面に入力した情報を統合認証サーバに送信する手段、前記統合認証サーバが発行する可搬媒体を受け取る手段を備える。

【０００８】

アクセス可否判定手段によりアクセスが拒否されたユーザが再度可搬媒体を用いた認証処理を利用したいユーザに対しては、可搬媒体再利用申請画面を表示する手段、ユーザが前記可搬媒体再利用申請画面に入力した情報を統合認証サーバに送信する手段、前記統合認証サーバにより前記ユーザに対する可搬媒体を用いたユーザ認証処理を許可する手段を備

える。
【０００９】
さらに、可搬媒体による処理を業務処理と連携させることも可能で、アクセスが許可されたユーザに対して、自動的に業務を開始する手段、前記ユーザが可搬媒体をはずした時に、自動的に業務を終了する手段も提供する。
【００１０】
【発明の実施の形態】
以下本発明の一実施形態について図面を用いて説明する。
【００１１】
図１は、本実施形態のネットワークシステムの構成図である。インターネットのような広域ネットワーク10には、企業ネットワークシステム１と他企業ネットワークシステム9が接続される。企業ネットワークシステム１には、クライアント8の他に、統合認証サーバ２，セキュリティ情報を管理するサーバ3、アクセス制御サーバ50、データベース(DB)サーバ5、業務サーバ6、グループウェアサーバ４，鍵管理サーバ17，証明証発行サーバ18等のサーバが接続される。DBサーバ5および業務サーバ6は、クライアント8からアクセスされ、業務処理のために利用されるサーバである。グループウェアサーバ4は、クライアント8へ最初の業務メニュー画面を送ったり、クライアント8の電子メールの送受信管理をしたり、ユーザのスケジュールを管理したりするサーバである。他企業ネットワークシステム9には、クライアント20が接続しており、クライアント8のユーザ11とクライアント20のユーザ14は、電子取り引き等の特定の業務を証明証や外部発行証明書を用いて行うものとする。ユーザ11及びユーザ14は、FD，ICカード、腕輪、指輪、ネクタイピン等の可搬媒体700を携帯し、可搬媒体700を用いた認証処理を行なう。サーバ3は、DBサーバ5および業務サーバ6または他企業ネットワークシステム9へのアクセスを制御する情報と業務に応じた証明証の情報を含むユーザの認証情報からなるセキュリティ情報を一元的に管理するサーバである。特願平9-76954の発明では、統合認証サーバ2は、クライアント8から送られる証明証を確認し、サーバ3からセキュリティ情報を取得してユーザが企業ネットワークシステム１にログインする資格を持つかどうか調べていた。しかし、本発明では、クライアント側に認証クライアント22を設けることにより、ログイン情報(証明証あるいはユーザ識別情報等)による認証処理を行なう。アクセス制御サーバ50は、各業務でのユーザのアクセス権限について管理するサーバ、鍵管理サーバ17は、企業ネットワークシステム1内での暗号化通信や認証処理で使用する通信当事者の鍵(秘密鍵と公開鍵の対)を生成するサーバである。広域ネットワーク10には、外部証明書発行サーバ7が接続されている。この外部証明書発行サーバ7は、所定の手順に従って外部証明書を発行するサーバである。なお、いわゆるディレクトリサーバと呼ばれるサーバがサーバ3の情報を有していても良い。
【００１２】
図２には、ユーザ11が可搬媒体700を用いてクライアント8からログインする処理シーケンスを示す。特願平9-76954の発明では、クライアント側のユーザが証明証10を入力し、統合認証サーバで前記証明証10を確認することによりユーザ認証を行なっていた。しかし、本実施例の図２では同様の証明証の確認処理を認証クライアント22で行なう点で異なる。本来であれば、ユーザ11がクライアント8の表示する認証情報入力画面にICカード内の証明証10を入力することが必要であるが、可搬媒体700という特徴を活かし、可搬媒体700にアクセスできる人が正当はユーザと判定することにする。可搬媒体700については常にユーザ本人が所持する運用形態とし、ユーザしか知らないパスワードや生物的な情報によってアクセスが保護されている前提である。可搬媒体700は物理的にもセキュアである必要があり、悪意を持った第3者による不正な情報読み取りに対しても頑強であり、情報自体を暗号化して格納しておいたり、アクセス許可されていない読み取りに対して格納情報を消去するようなしかけを提供している。
【００１３】
まず、ユーザ11は、可搬媒体を可搬媒体読み取り装置705に取り付けると(2001)、認証情

報入力画面(2002)が表示されるので、パスワードあるいは指紋や網膜などの生物的情報を入力する(2003)。すると、前記パスワードあるいは指紋や網膜などの生物的情報を確認することによりアクセス可否の判定をする(2004)。ユーザが正当なユーザ11であると判定した場合には、以降の業務認証処理についてシングルログインの処理を提供するが、そうでない場合には、認証クライアント22の公開鍵を用いて当可搬媒体700を無効にし(2005)、アクセス不可通知をユーザ11に送る(2006)。例えば、3回までの不正なパスワード入力を許すような運用も考えられる。可搬媒体700上あるいは可搬媒体700と連動する位置に、生物的情報による認証装置701を設けている場合には、生物的情報による認証装置701の精度を考慮してアクセス判定の失敗許容回数を設定する必要がある。いずれにしても、正当なユーザ11と判定されなかった場合には、可搬媒体700を以降使えなくする必要があるので、可搬媒体内の情報を参照不可能な状態にする。

【００１４】

図2に示すように、正当なユーザに対しては、以降、本来なら業務ごとに要求されるユーザ認証画面は表示しない。ユーザ11が業務サーバ6に対して業務要求をすると(2007)、業務サーバ6からユーザ認証画面が送られるが(2008)、認証クライアント22は前記画面への情報入力をユーザ11に要求せず、可搬媒体700の中から必要なログイン情報を取り出してその情報を前記業務サーバ6に送る(2009)。同様に、次にユーザ11がDBサーバ5に対してアクセスしたい場合には(2014)、DBサーバ5からユーザ認証画面が送られるが(2015)、認証クライアント22は前記画面への情報入力をユーザ11に要求せず、可搬媒体700の中から必要なログイン情報を取り出してその情報をDBサーバ5に送る(2016)。特願平9-76954の発明では、統合認証サーバ2がサーバ3からセキュリティ情報（業務ごとのログイン情報等）を取得してユーザ11が企業ネットワークシステム１にログインする資格を持つかどうか調べていた。しかし、本実施例では、可搬媒体700内に前記セキュリティ情報を含むことができるので、必ずしもサーバ3に問い合わせに行く必要はない。但し、業務の詳細についてのアクセス制御情報まで可搬媒体700に含めることができない場合もあるので、そのような時には、サーバ３あるいはアクセス制御サーバ50との連携が要求される。

【００１５】

ユーザ11が業務終了を要求すると(2012、2019)、業務終了が通知され(2013、2020)、クライアント8内の可搬媒体読み取り装置705から可搬媒体700が取り外される(2021)。

【００１６】

可搬媒体700を用いないユーザは、図３に示すような従来の認証処理をしなければならない。すなわち、ユーザは、業務ごとに要求されるユーザ認証画面(3003、3010)に自分でログイン情報を入力する必要がある(3004、3011)。

【００１７】

次に、可搬媒体700の発行要求シーケンスについて図４で示す。ユーザ14が可搬媒体700の発行要求をすると(4001)、認証クライアント22は可搬媒体発行申請画面を表示する(4002)。前記可搬媒体発行申請画面には、ユーザの識別情報、所属情報、職務権限情報等様々な情報の指定が必要であるが、基本的にこれらの情報はサーバ３で管理されているため、最低限ユーザに識別情報を入力する(4003)。認証クライアント22は、前記入力された情報を統合認証サーバ2に送信すると、統合認証サーバ2では、サーバ3にユーザ14に関するセキュリティ情報を問い合わせることにより、ユーザ14の権限を確認する(4004)。そして、前記権限情報に基づいてユーザ14のためのログイン情報を作成し(4005)、統合認証サーバ2の公開鍵で暗号化し(4006)、可搬媒体700に格納する。統合認証サーバ2と認証クライアント22間でセキュアな通信をすることにより、認証クライアント22側の可搬媒体に前記ユーザ14のためのログイン情報を書き込むことも可能であるし(4007)、可搬媒体自体を通信以外の方法で配送することもできる(4013)。いずれにしても、可搬媒体をユーザ14が受け取ったら、可搬媒体700についてのパスワード設定要求が出されるので(4014)、ユーザ14はパスワードを指定しなければならない。そして、前記パスワード情報は認証クライアント22及び統合認証サーバ2にも送付される(4015)。

【００１８】

図５では、可搬媒体700へのアクセスを拒否されたユーザが再度可搬媒体700を利用可能とするための処理について説明する。ここでは、ユーザ11がアクセスを拒否されたとしよう。ユーザ11は、可搬媒体700の可搬媒体再利用要求をすると(5001)、認証クライアント22は可搬媒体再利用要求画面を表示する(5002)。基本的には、前記可搬媒体発行申請画面に必要だった情報を入力する必要があるが、別の手段により、前記可搬媒体再利用要求をしているユーザが正当なユーザ11であることを確かめることもできる。例えば、ユーザ11しか知らない情報やユーザ11しか持っていない情報を入力させれば本人であることがわかるので、可搬媒体のパスワードをユーザ11の秘密鍵(証明証内の公開鍵に対応)で暗号して送信させるような手順も有効である(5004)。このようにして、正しいユーザ11であると確認できた場合には(5006)、統合認証サーバ2から認証クライアント22に可搬媒体700を再度利用可能な状態にするように指示する。図２の処理2005でも説明したように、可搬媒体700内の情報は認証クライアント22の公開鍵を用いて参照不可能な状態にされているので、それを解除するためには、ユーザ11本人のパスワードと認証クライアント22の秘密鍵が必要である。認証クライアント22は、ユーザ11のパスワードと前記秘密鍵を入力することにより、可搬媒体700を参照可能な状態に戻す(5007)。そして、可搬媒体700の無効化解除の通知をユーザ11に送る(5008)。

【００１９】

ユーザの業務運用を簡易化するという観点から、図６に示す業務との連携機能も実現できる。これは、特定の業務向けにカスタマイズした運用とも考えられる。前記アクセス可否の判定(6004)によりアクセスが許可されたユーザに対して、あらかじめスケジューリングされたとおりに業務を自動的に開始する。図６の例では、業務サーバ6に対する一連の処理を終えた後、それとは関連のないDBサーバ5の更新処理を行なった後で自動的に業務を終了するような運用情報があらかじめ可搬媒体700の中に入れられている。図6の処理6001から処理6006までは、図2と同様であるが、処理6007による業務サーバ6への処理要求が可搬媒体700から出されている点が図2の処理2007とは異なる。上述のように、可搬媒体700には、ユーザ11から次の業務要求が出されたら(6012)、業務サーバ6に対して業務終了通知を出し(6013)、次の業務であるDBサーバ5に対する業務要求を出す(6014)ように指定されている。従って、ユーザ11が業務サーバ6に対する業務終了要求やDBサーバ5に対する業務要求をする必要はない。同様に、可搬媒体700を取り出したら(6019)、DBサーバ5に対して業務終了通知を出すように指定されているので(6020)、ユーザ11がDBサーバ5に対する業務終了要求を出す必要はない。このようにして、可搬媒体700を読み取り装置からはずすと自動的に処理が終了するしかけになっているので、席を一時的にはずす時には、可搬媒体は抜かれることになりその分業務のセキュリティが高まることが期待される。

【００２０】

図７に、前記図２から図６までの処理手順や運用例を実現するための可搬媒体700、クライアント内の可搬媒体読み取り装置705、生物的情報による認証装置701、及びクライアント内の認証クライアント22との関係について説明をする。可搬媒体700は、情報制御部7010とアクセス可否判定部7020から構成される。情報制御部7010ではログイン情報7011、運用情報7012及び可搬媒体状態情報7013を管理する。情報制御部7010では、可搬媒体の状態（有効・無効など）を管理しており、可搬媒体が無効な状態になっている場合には、可搬媒体読み取り装置705を介した情報の読み取りを禁止し、認証クライアント22からの無効化解除機能7222や情報書き込み機能7223により可搬媒体を有効な状態にする。また、アクセス可否判定部7020は、ユーザが入力したパスワードや生物的情報を判定する部分である。

【００２１】

可搬媒体読み取り装置705は、可搬媒体700を挿入し、そこから情報を読み取る装置であり、情報読み取り部7110と挿入状態監視部7120から構成される。

【００２２】

認証クライアント22は、画面制御部7210、可搬媒体制御部7220、情報入出力制御部7230から構成される。画面制御部7210は、可搬媒体の利用時や申請時に必要な認証情報入力画面

7211、可搬媒体発行申請画面7212及び可搬媒体再利用要求画面7213、ユーザの業務要求時に必要なユーザ認証画面7212などを管理する。また、可搬媒体制御部7220では、可搬媒体の無効化機能7221、可搬媒体の無効化解除機能7222、可搬媒体への情報書き込み機能7223、パスワード管理機能7224などを含む。情報入出力制御部7230は、ユーザからの入力情報の受け付け機能7231、生物的情報による認証装置701とのインタフェース7232、ユーザへの情報表示機能7233を備える。クライアントの中に、前記認証クライアント22と可搬媒体読み取り装置705がある。

【００２３】

【発明の効果】

以上述べたように、本発明によれば、企業情報システムで可搬媒体を利用したシングルログインを実現できる。先願発明(特願平9-76954)で提案した強固なユーザ認証及びアクセス制御の基盤を利用し、さらに、クライアント側に可搬媒体利用の画面制御手段、生物学情報による認証手段を設けることによりユーザを厳密に認証できる。アクセス可否判定の結果、不当なユーザに対しては可搬媒体を無効にするので高度なセキュリティが保証されている。ユーザは可搬媒体を用いない従来の認証処理も利用できるが、可搬媒体の利用申請や無効となった可搬媒体を再度利用可能にする処理も可能である。可搬媒体の利用と業務を連携させれば、ユーザの業務運用の簡易化や特定の業務向けに運用のカスタマイズ化もできる。

【図面の簡単な説明】

【図１】実施形態のネットワークシステムの構成図である。

【図２】実施形態のユーザ11が可搬媒体700を用いてクライアント8からログインする処理手順を示す図である。

【図３】従来の認証処理手順を示す図である。

【図４】実施形態のユーザ14による可搬媒体700の発行要求処理の手順を示す図である。

【図５】実施形態の可搬媒体700へのアクセスを拒否されたユーザが再度可搬媒体700を利用可能とする処理手順を示す図である。

【図６】実施形態の可搬媒体700を業務と連携させることによる特定の業務向けにカスタマイズした運用の一例である。

【図７】実施形態の図２から図６までの処理手順や運用例を実現するための可搬媒体700、クライアント内の可搬媒体読み取り装置705、生物的情報による認証装置701、及びクライアント内の認証クライアント22との関係について説明をする構成図である。

【符号の説明】

企業ネットワークシステム１、他企業のネットワークシステム9、広域ネットワークシステム10…ネットワークシステム

FW60,FW61…ファイアウォール装置

統合認証サーバ２，セキュリティ情報を管理するサーバ３，グループウェアサーバ４，ＤＢサーバ５，業務サーバ６,外部証明書発行サーバ７,鍵管理サーバ17,証明証発行サーバ18、証明証取り消しリスト管理サーバ54,アクセス制御サーバ50,ネットワーク管理サーバ41…サーバシステム

クライアント８、クライアント20…クライアント

認証クライアント22…統合認証サーバ2と連携してユーザ認証処理を行なうクライアント上のプログラム

ユーザ11,ユーザ14…ユーザ

可搬媒体700…FD，ICカード、腕輪、指輪、ネクタイピン等の可搬媒体

可搬媒体読み取り装置705…可搬媒体700の内容を読み取るクライアント上の装置生物的情報による認証装置701…指紋、網膜、DNA情報等を利用してユーザを認証する装置

2001～2021…図２の処理内容

3001～3014…図３の処理内容

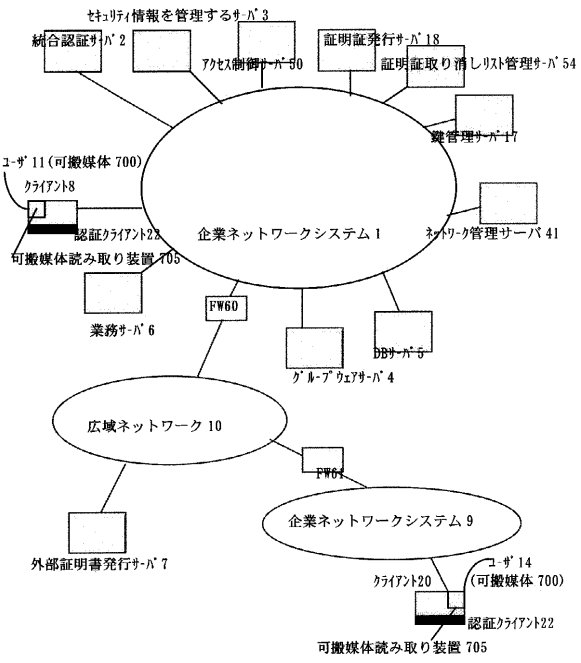
4001～4016…図４の処理内容

5001～5008…図５の処理内容

6001～6020…図６の処理内容
情報制御部7010、ログイン情報7011、運用情報7012、可搬媒体状態情報7013、アクセス可否判定部7020…可搬媒体700の構成要素
情報読み取り部7110、挿入状態監視部7120…可搬媒体読み取り装置705の構成要素
画面制御部7210、認証情報入力画面7211、可搬媒体発行申請画面7212、可搬媒体再利用要求画面7213、ユーザ認証画面7212、可搬媒体制御部7220、可搬媒体の無効化機能7221、可搬媒体の無効化解除機能7222、可搬媒体への情報書き込み機能7223、パスワード管理機能7224、情報入出力制御部7230、入力情報の受け付け機能7231、生物的情報による認証装置701とのインタフェース7232、情報表示機能7233…証クライアント22の構成要素

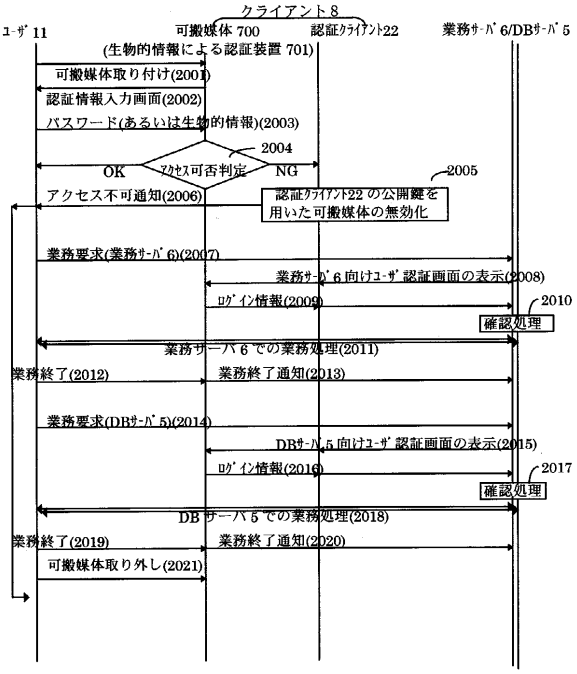
【図１】

図　１



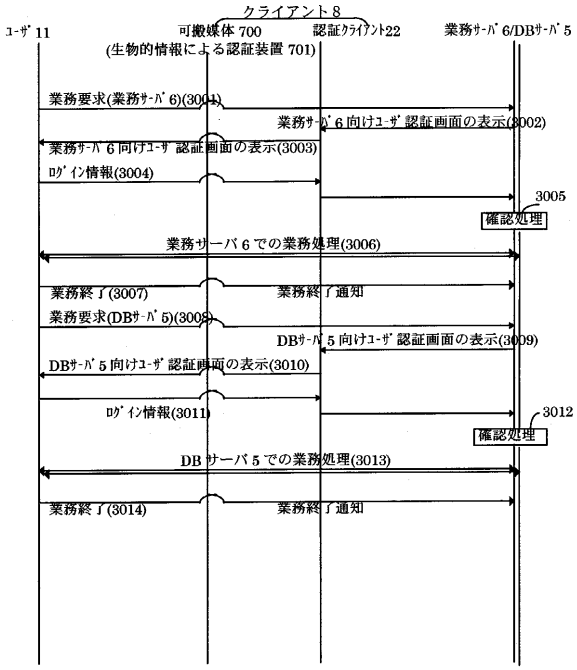
【図２】

図　２



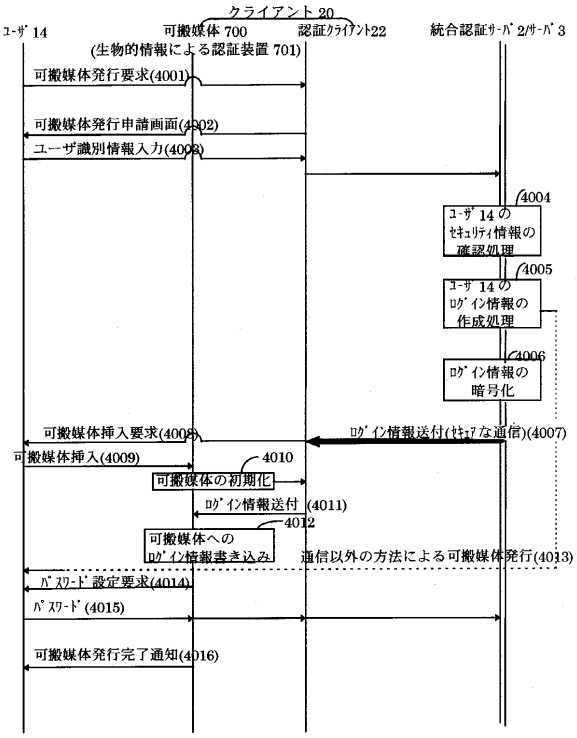
【図３】

図 3



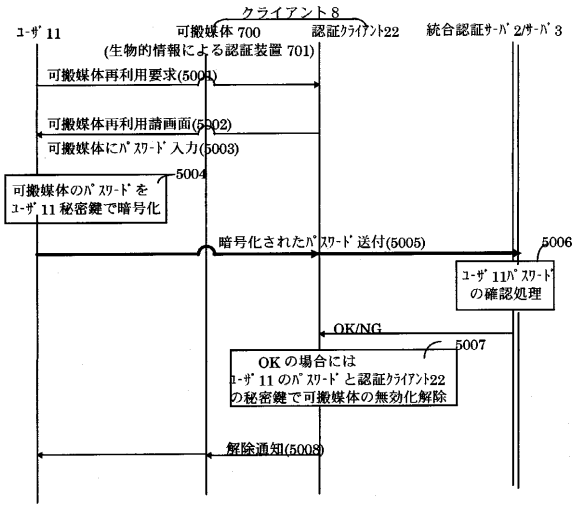
【図４】

図 4



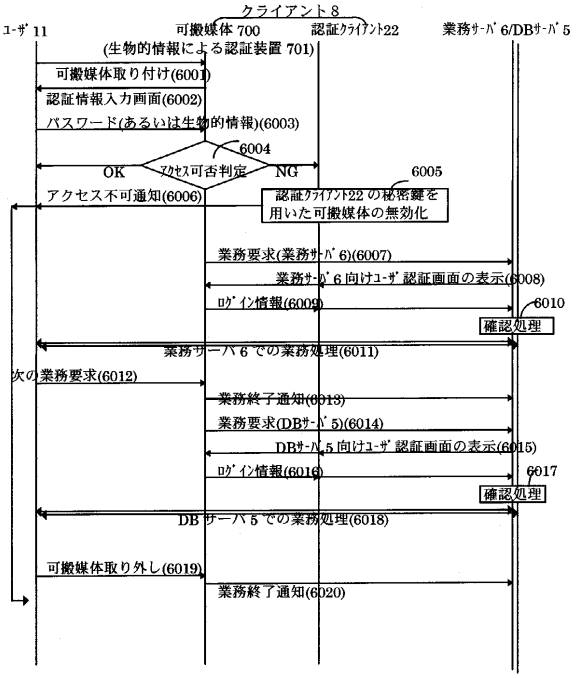
【図５】

図 5



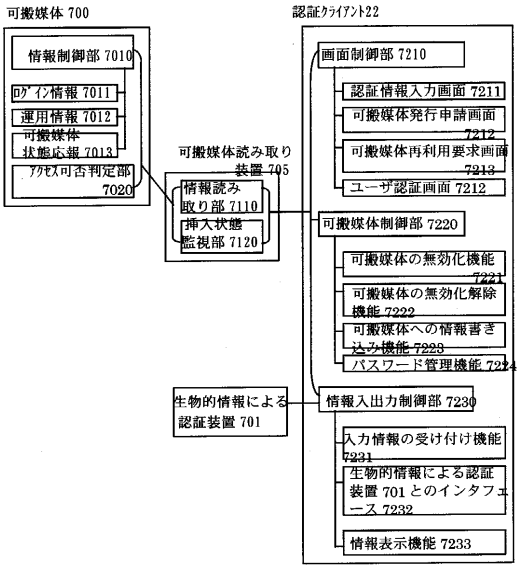
【図６】

図 6



【図７】

図 7


可搬媒体 700
情報制御部 7010
ログイン情報 7011
運用情報 7012
可搬媒体状態応報 7013
アクセス可否判定部 7020
可搬媒体読み取り装置 705
情報読み取り部 7110
挿入状態監視部 7120
認証クライアント22
画面制御部 7210
認証情報入力画面 7211
可搬媒体発行申請画面 7212
可搬媒体再利用要求画面 7213
ユーザ認証画面 7212
可搬媒体制御部 7220
可搬媒体の無効化機能 7221
可搬媒体の無効化解除機能 7222
可搬媒体への情報書き込み機能 7223
パスワード管理機能 7224
生物的情報による認証装置 701
情報入出力制御部 7230
入力情報の受け付け機能 7231
生物的情報による認証装置 701 とのインタフェース 7232
情報表示機能 7233

フロントページの続き

(56)参考文献 特開２０００－０１０９３０（ＪＰ，Ａ）
特開平１１－２８２９８２（ＪＰ，Ａ）
特開平１１－１８４８１８（ＪＰ，Ａ）
特開平１０－１７７５５４（ＪＰ，Ａ）
特開平１０－０２７１６０（ＪＰ，Ａ）
特開昭６３－２５０７６１（ＪＰ，Ａ）
特開２０００－１０５７４６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G06F 15/00
G06F 13/00
JSTPLUS,JST7580ファイル(JOIS)