(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2006-155196
(P2006-155196A)
(43)公開日　平成18年6月15日(2006.6.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	5B085
H04L 9/32	(2006.01)	H04L	9/00	673D	5J104

審査請求 未請求　請求項の数 39　ＯＬ　（全 22 頁）

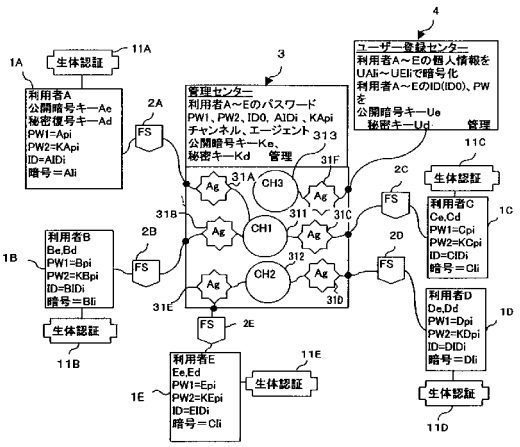
(21)出願番号　特願2004-344277 (P2004-344277)
(22)出願日　平成16年11月29日 (2004.11.29)

(71)出願人　504439757
インテリジェントディスク株式会社
神奈川県横浜市港北区新横浜３－２－６
新横浜ビジネスセンタービル６Ｆ
(71)出願人　000003687
東京電力株式会社
東京都千代田区内幸町１丁目１番３号
(74)代理人　100081710
弁理士　福山　正博
(72)発明者　重富　孝士
横浜市港北区新横浜３－２－６
新横浜ビジネスセンタービル６Ｆ
インテリジェントディスク株式会社内

最終頁に続く

(54)【発明の名称】ネットワークアクセスシステム、方法及び記憶媒体

(57)【要約】
【課題】予めネットワーク側に登録された利用者のみがきわめて高いセキュリティを維持しつつ当該ネットワークにアクセス可能とする。
【解決手段】利用者１Ａの生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が、ディスクに搭載された電子回路のメモリ（外付け記憶媒体）に格納される。ディスク駆動時に、生体認証手段１１Ｅにより、利用者から生体認証情報を取得し、電子回路（外付け記憶媒体）に格納されている生体認証情報と比較し、両情報が一致したとき電子回路（外付け記憶媒体）に格納されているアクセス認証情報をネットワーク側に送出する。ネットワーク側では、受信したアクセス認証情報に基づいて利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときに、利用者端末のサービスコミュニティへの接続を許可する。
【選択図】図１



【特許請求の範囲】
【請求項１】
利用者端末が、ネットワークに接続されているサービス提供側に設けられたサービスコミュニティにアクセスして接続するネットワークアクセスシステムにおいて、
利用者の生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が、ディスクに搭載された電子回路のメモリに格納され、
前記ディスク駆動時に、生体認証手段により、利用者から前記生体認証情報に関する生体情報を取得し、前記電子回路に格納されている生体認証情報と比較し、両情報が一致したとき前記電子回路に格納されている前記アクセス認証情報を前記ネットワーク側に送出し、
前記ネットワーク側には、アクセス認証手段により、受信した前記アクセス認証情報に基づいて前記利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときには、前記利用者端末の前記サービスコミュニティへの接続を許可することを特徴とするネットワークアクセスシステム。
【請求項２】
利用者端末が、ネットワーク側に接続されているサービス提供側に設けられたサービスコミュニティにアクセスして接続するネットワークアクセスシステムにおいて、
利用者の生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が、前記利用者端末に接続され、信号処理機能を有する外付け記憶媒体に格納され、
生体認証手段により、利用者から前記生体認証情報に関する生体情報を取得し、前記外付け記憶媒体に格納されている生体認証情報と比較し、両情報が一致したとき前記外付け記憶媒体に格納されている前記アクセス認証情報を前記ネットワーク側に送出し、
前記ネットワーク側には、アクセス認証手段により、受信した前記アクセス認証情報に基づいて前記利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときには、前記利用者端末の前記サービスコミュニティへの接続を許可することを特徴とするネットワークアクセスシステム。
【請求項３】
前記電子回路または外付け記憶媒体にはアクセス先情報が格納され、前記アクセス先情報が送出されることを特徴とする請求項１または２に記載のネットワークアクセスシステム。
【請求項４】
前記ネットワーク側には、前記利用者のアクセス認証情報を含む情報を管理する管理センターを備え、前記アクセス認証手段による判断は、前記管理センターに管理されているアクセス認証情報との比較により行われることを特徴とする請求項１乃至３のいずれかに記載のネットワークアクセスシステム。
【請求項５】
ネットワークを介して利用者端末のアクセスによって、管理センターにより管理されているサーバーにするソサイエティを含むコミュニティへの接続を行うネットワークアクセスシステムにおいて、
前記管理センターには、接続を許可された利用者のアクセス認証情報が格納され、
前記利用者端末に内蔵され、または接続された利用者の生体認証情報を検出する生体認証情報検出手段と、
前記利用者端末に接続されたディスクドライブと、
を備え、
前記ディスクドライブで駆動されるディスクには、前記利用者の生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が格納された電子回路が搭載され、
前記ディスクドライブによる前記ディスクの駆動時に、前記生体認証情報検出手段により利用者から検出した生体認証情報と、前記電子回路に格納されている生体認証情報とを

比較し、両情報が一致したとき、前記電子回路に格納されている前記アクセス認証情報が前記利用者端末を介して前記管理センターに送出され、
前記管理センターでは、受信した前記アクセス認証情報が、予め格納されているアクセス認証情報と一致する場合に、前記利用者を登録されている正規な利用者であると判断し、前記利用者端末を前記コミュニティへの接続を許可することを特徴とするネットワークアクセスシステム。
【請求項６】
ネットワークを介して利用者端末のアクセスによって、管理センターにより管理されているサーバーにするソサイエティを含むコミュニティへの接続を行うネットワークアクセスシステムにおいて、
前記管理センターには、接続を許可された利用者のアクセス認証情報が格納され、
前記利用者端末に内蔵され、または接続された利用者の生体認証情報を検出する生体認証情報検出手段と、
前記利用者端末に接続され、前記利用者の生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が格納され、信号処理機能を有する外付け記憶媒体と、
前記生体認証情報検出手段により利用者から検出した生体認証情報と、前記外付け記憶媒体に格納されている生体認証情報とを比較し、両情報が一致したとき、前記外付け記憶媒体に格納されている前記アクセス認証情報が前記利用者端末を介して前記管理センターに送出され、
前記管理センターでは、受信した前記アクセス認証情報が、予め格納されているアクセス認証情報と一致する場合に、前記利用者を登録されている正規な利用者であると判断し、前記利用者端末を前記コミュニティへの接続を許可することを特徴とするネットワークアクセスシステム。
【請求項７】
前記電子回路または外付け記憶媒体にはアクセス先情報が格納され、前記アクセス先情報が送出されることを特徴とする請求項５または６に記載のネットワークアクセスシステム。
【請求項８】
前記管理センターは、内蔵され、または接続されたユーザー登録センターを有し、前記ユーザー登録センターには前記利用者の個人情報や前記アクセス認証情報が格納されていることを特徴とする請求項５または６に記載のネットワークアクセスシステム。
【請求項９】
前記アクセス認証情報は、利用者のＩＤとパスワードを含むことを特徴とする請求項１乃至８のいずれかに記載のネットワークアクセスシステム。
【請求項１０】
前記利用者の前記ネットワーク側での情報授受は、前記利用者に対して予め付与されたニックネームによって行われることを特徴とする請求項１乃至９のいずれかに記載のネットワークアクセスシステム。
【請求項１１】
前記アクセス認証情報は、前記利用者端末側から暗号化されて出力され、前記ネットワーク側では、受信した暗号化されたアクセス認証情報を復号化することを特徴とする請求項１乃至１０のいずれかに記載のネットワークアクセスシステム。
【請求項１２】
前記アクセス認証情報は、利用者によるアクセス毎に変化されることを特徴とする請求項１乃至１１のいずれかに記載のネットワークアクセスシステム。
【請求項１３】
前記変化するアクセス認証情報は、前記利用者端末側と前記ネットワーク側のみが知り得るように公開暗号キーと秘密復号キーに基づいて処理されていることを特徴とする請求項１乃至１２のいずれかに記載のネットワークアクセスシステム。

【請求項１４】
前記ネットワーク側は、前記利用者の次回アクセス用のアクセス認証情報を生成し暗号化して前記利用者端末側に送出し、前記利用者端末側からの次回アクセス時には、前記ネットワーク側から受信した前記アクセス認識情報を送出することを特徴とする請求項１乃至１３のいずれかに記載のネットワークアクセスシステム。
【請求項１５】
前記ネットワーク側に格納されている利用者に関する情報は、前記利用者毎に付与されている基礎コードにより管理され、前記利用者を特定した利用者情報は、前記利用者側の前記電子回路で生成された補助コードと前記基礎コードを組み合わせた基本コードによってのみ読み込み、書き込みを可能とすることを特徴とする請求項１乃至１４のいずれかにに記載のネットワークアクセスシステム。
【請求項１６】
前記ネットワーク側に格納されている利用者に関する情報は、前記利用者毎に付与されている基礎コードにより管理され、前記利用者を特定した利用者情報は、前記利用者側の前記外付け記憶媒体で生成された補助コードと前記基礎コードを組み合わせた基本コードによってのみ読み込み、書き込みを可能とすることを特徴とする請求項１乃至１４のいずれかにに記載のネットワークアクセスシステム。
【請求項１７】
前記補助コードは公開暗号キーによって暗号化されて前記利用者端末側から送出され、前記ネットワーク側では、前記公開暗号キーに対応する秘密復号キーにより復号化して得られた補助コードとして利用されることを特徴とする請求項１５または１６に記載のネットワークアクセスシステム。
【請求項１８】
前記利用者側と前記ネットワーク側間での情報授受は、公開暗号キーを用いた暗号化と、前記公開暗号キーに対応する秘密復号キーによる復号化処理を介して実行されることを特徴とする請求項１乃至１７のいずれかに記載のネットワークアクセスシステム。
【請求項１９】
前記生体認証情報は、指紋認証、顔認証、声紋認証または瞳の虹彩認証情報であることを特徴とする請求項１乃至１８のいずれかに記載のネットワークアクセスシステム。
【請求項２０】
前記ディスクは、光ディスクであることを特徴とする請求項３乃至５、７乃至１５、１７乃至１９のいずれかに記載のネットワークアクセスシステム。
【請求項２１】
利用者端末からのアクセスにより、ネットワーク側に接続されているサービス系に接続するネットワークアクセス方法において、
ディスクに搭載された電子回路のメモリに利用者の生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報を格納しておき、
前記ディスク駆動時に、前記利用者から検出手段により取得した生体認証情報と、前記電子回路に格納されている生体認証情報とを比較し、両情報が一致したとき前記電子回路に格納されている前記アクセス認証情報を前記ネットワーク側に送出し、
前記ネットワーク側では、受信した前記アクセス認証情報に基づいて前記利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときに、前記利用者端末の前記サービス系への接続を許可することを特徴とするネットワークアクセス方法。
【請求項２２】
利用者端末からのアクセスにより、ネットワーク側に接続されているサービス系に接続するネットワークアクセス方法において、
前記利用者端末に接続され、信号処理機能を有する外付け記憶媒体に利用者の生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報を格納しておき、
前記利用者から検出手段により取得した生体認証情報と、前記外付け記憶媒体に格納さ

れている生体認証情報とを比較し、両情報が一致したとき前記外付け記憶媒体に格納されている前記アクセス認証情報を前記ネットワーク側に送出し、
前記ネットワーク側では、受信した前記アクセス認証情報に基づいて前記利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときに、前記利用者端末の前記サービス系への接続を許可することを特徴とするネットワークアクセス方法。
【請求項２３】
前記電子回路または外付け記憶媒体にはアクセス先情報が格納され、前記アクセス先情報が送出されることを特徴とする請求項２１または　２２に記載のネットワークアクセスシステム。
【請求項２４】
利用者端末のアクセスによりネットワークを介して、接続を許可された利用者のアクセス認証情報が格納された管理センターにより管理されているサーバーに接続するネットワークアクセス方法であって、
ディスクドライブで駆動され、前記利用者の生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が格納された電子回路が搭載されたディスクの駆動時に、前記利用者端末側の生体認証手段により得られた前記利用者の生体認証情報と、前記ディスクの電子回路に格納された生体認証データとを比較し、両情報が一致したとき、前記電子回路に格納されている前記アクセス認証情報が前記利用者端末を介して前記管理センターに送出し、
前記管理センターは、受信した前記アクセス認証情報を、予め格納されているアクセス認証情報と比較し、両情報が一致したときのみ前記利用者端末の接続を許可することを特徴とするネットワークアクセス方法。
【請求項２５】
利用者端末のアクセスによりネットワークを介して、接続を許可された利用者のアクセス認証情報が格納された管理センターにより管理されているサーバーに接続するネットワークアクセス方法であって、
前記利用者の生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報を、信号処理機能を有する外付け記憶媒体に格納し、前記利用者端末側の生体認証手段により得られた生体認証情報と、前記外付け記憶媒体に格納された生体認証データとを比較し、両情報が一致したとき、前記外付け記憶媒体に格納されている前記アクセス認証情報が前記利用者端末を介して前記管理センターに送出し、
前記管理センターは、受信した前記アクセス認証情報を、予め格納されているアクセス認証情報と比較し、両情報が一致したときのみ前記利用者端末の接続を許可することを特徴とするネットワークアクセス方法。
【請求項２６】
前記電子回路または外付け記憶媒体にはアクセス先情報が格納され、前記アクセス先情報が送出されることを特徴とする請求項２４または２５に記載のネットワークアクセスシステム。
【請求項２７】
前記利用者の前記ネットワーク側での情報授受を、前記利用者に対して予め付与されたニックネームによって行うことを特徴とする請求項２１乃至２６のいずれかに記載のネットワークアクセス方法。
【請求項２８】
前記ネットワーク側には、前記利用者の個人情報や前記アクセス認証情報が格納されていることを特徴とする請求項２１乃至２７のいずれかに記載のネットワークアクセス方法。
【請求項２９】
前記アクセス認証情報は、利用者のＩＤとパスワードを含むことを特徴とする請求項２１乃至２８のいずれかに記載のネットワークアクセス方法。
【請求項３０】

前記アクセス認証情報は、前記利用者端末側から暗号化されて出力し、前記ネットワーク側では、受信した暗号化されたアクセス認証情報を復号化することを特徴とする請求項２１乃至２９のいずれかに記載のネットワークアクセス方法。

【請求項３１】

前記アクセス認証情報は、利用者によるアクセス毎に変化させることを特徴とする請求項２１乃至３０のいずれかに記載のネットワークアクセス方法。

【請求項３２】

前記変化するアクセス認証情報は、前記利用者端末側と前記ネットワーク側のみが知り得るように公開暗号キーと秘密復号キーに基づいて処理することを特徴とする請求項２１乃至３１のいずれかに記載のネットワークアクセス方法。

【請求項３３】

前記ネットワーク側は、前記利用者の次回アクセス用のアクセス認証情報を生成し暗号化して前記利用者端末側に送出し、前記利用者端末側からの次回アクセス時には、前記ネットワーク側から受信した前記アクセス認識情報を送出することを特徴とする請求項２１乃至３２のいずれかに記載のネットワークアクセス方法。

【請求項３４】

前記ネットワーク側に格納されている利用者に関する情報は、前記利用者毎に付与されている基礎コードにより管理し、前記利用者を特定した利用者情報は、前記利用者側の前記電子回路で生成された補助コードと前記基礎コードを組み合わせた基本コードによってのみ読み込み、書き込みを可能とすることを特徴とする請求項２１乃至３３のいずれかに記載のネットワークアクセス方法。

【請求項３５】

前記ネットワーク側に格納されている利用者に関する情報は、前記利用者毎に付与されている基礎コードにより管理し、前記利用者を特定した利用者情報は、前記利用者側の前記外付け記憶媒体で生成された補助コードと前記基礎コードを組み合わせた基本コードによってのみ読み込み、書き込みを可能とすることを特徴とする請求項２１乃至３３のいずれかに記載のネットワークアクセス方法。

【請求項３６】

前記補助コードを公開暗号キーによって暗号化されて前記利用者端末側から送出し、前記ネットワーク側では、前記公開暗号キーに対応する秘密復号キーにより復号化して得られた補助コードとして利用することを特徴とする請求項３４に記載のネットワークアクセス方法。

【請求項３７】

前記利用者側と前記ネットワーク側間での情報授受は、公開暗号キーを用いた暗号化と、前記公開暗号キーに対応する秘密復号キーによる復号化処理を介して実行することを特徴とする請求項２１乃至３５のいずれかに記載のネットワークアクセス方法。

【請求項３８】

前記生体認証情報は、指紋認証、顔認証、声紋認証または瞳の虹彩認証情報であることを特徴とする請求項２１乃至３７のいずれかに記載のネットワーク方法。

【請求項３９】

請求項２１乃至３８のいずれかに記載の処理をコンピュータに実行させるためのプログラムを格納した記憶媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はネットワークアクセスシステム、方法及び記憶媒体に関し、特にきわめて高度なセキュリティを維持できるネットワークアクセスシステム、方法及び記憶媒体に関する。

【背景技術】

【０００２】

インターネット及びブロードバンド環境の急速な普及により、インターネットを介して個人は、各種のサービスを享受できるようになっている。利用者個人は、自宅に居ながらパソコンを用いて、または携帯端末を用いてネットサービスに簡単にアクセスできる。

【０００３】

この種のサービスは、一方的に情報を受けるだけであれば、当該情報のダウンロードだけで済み、利用者の個人情報が漏れる心配はないが、ネットオークション、商品購買等の電子商取引では、利用者個人情報を開示しなければならないため、情報漏洩の危険がある。この種の電子商取引システムは、例えば、特許文献１に開示されている。

【０００４】

【特許文献１】特開２００４－３１８４９７（図１、段落番号〔０００９〕～〔００１６〕）

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかし、電子商取引では、利用者のクレジットカード番号や有効期限、個人銀行口座、住所、氏名、生年月日等の個人情報を開示しなければならないケースが多い。また、ネットに入力された個人情報は、相手方の利用処理に委ねられ、個人情報のセキュリティ確保の保証がなく、更に当該個人情報はネットを無制約に飛び交い、いつ何時に個人情報が他人に渡るか不安も大きいものである。

【０００６】

そこで、セキュリティを確保するため、利用者本人であることを認証する種々の認証手段（ＩＤやパスワード）を利用するシステムが一般的に実用化されている。しかし、認証システムは必ず抜け道があり、システムの脆弱性を突いて個人情報を盗んだり、情報改ざんが行われることもある。認証システムのセキュリティをより向上させるためには、利用するサービス毎にＩＤやパスワードを設定することも有用であるが、その管理のための費用は利用者負担となることが多く、コスト面での問題が残る。

【０００７】

また、当該個人情報を利用して利用者になりすまして電子商取引が行われる危険性も大きい。利用者個人へのなりすましだけでなく、信頼を前提としたｅコマースに悪意の業者が参入して有名サイトでもなりすましの危険もある。

【０００８】

更に、ネットサービスの一環としてのメールによるコミュニティに参加するサービスもあるが、かかるサービスでは、利用者のメールアドレスが第３者に開示され、いつの間にか迷惑メールの攻撃に晒される恐れもある。

【０００９】

本発明は、従来技術の上述した課題に鑑みなされたものであり、斯かる課題を克服できるネットワークアクセスシステム、方法及び記憶媒体を提供することを主たる目的とする。

【課題を解決するための手段】

【００１０】

前述の課題を解決するため本発明によるネットワークアクセスシステム、方法及び記憶媒体は、以下のような特徴的な構成を採用している。

【００１１】

（１）利用者端末が、ネットワークに接続されているサービス提供側に設けられたサービスコミュニティにアクセスして接続するネットワークアクセスシステムにおいて、

利用者の生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が、ディスクに搭載された電子回路のメモリに格納され、

前記ディスク駆動時に、生体認証手段により、利用者から前記生体認証情報に関する生体情報を取得し、前記電子回路に格納されている生体認証情報と比較し、両情報が一致したとき前記電子回路に格納されている前記アクセス認証情報を前記ネットワーク側に送出

し、
前記ネットワーク側には、アクセス認証手段により、受信した前記アクセス認証情報に基づいて前記利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときには、前記利用者端末の前記サービスコミュニティへの接続を許可するネットワークアクセスシステム。
（２）利用者端末が、ネットワーク側に接続されているサービス提供側に設けられたサービスコミュニティにアクセスして接続するネットワークアクセスシステムにおいて、
利用者の生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が、前記利用者端末に接続され、信号処理機能を有する外付け記憶媒体に格納され、
生体認証手段により、利用者から前記生体認証情報に関する生体情報を取得し、前記外付け記憶媒体に格納されている生体認証情報と比較し、両情報が一致したとき前記外付け記憶媒体に格納されている前記アクセス認証情報を前記ネットワーク側に送出し、
前記ネットワーク側には、アクセス認証手段により、受信した前記アクセス認証情報に基づいて前記利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときには、前記利用者端末の前記サービスコミュニティへの接続を許可するネットワークアクセスシステム。
（３）前記電子回路または外付け記憶媒体にはアクセス先情報が格納され、前記アクセス先情報が送出される上記（１）または（２）のネットワークアクセスシステム。
（４）前記ネットワーク側には、前記利用者のアクセス認証情報を含む情報を管理する管理センターを備え、前記アクセス認証手段による判断は、前記管理センターに管理されているアクセス認証情報との比較により行われる上記（１）乃至（３）のいずれかのネットワークアクセスシステム。
（５）ネットワークを介して利用者端末のアクセスによって、管理センターにより管理されているサーバーにするソサイエティを含むコミュニティへの接続を行うネットワークアクセスシステムにおいて、
前記管理センターには、接続を許可された利用者のアクセス認証情報が格納され、
前記利用者端末に内蔵され、または接続された利用者の生体認証情報を検出する生体認証情報検出手段と、
前記利用者端末に接続されたディスクドライブと、
を備え、
前記ディスクドライブで駆動されるディスクには、前記利用者の生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が格納された電子回路が搭載され、
前記ディスクドライブによる前記ディスクの駆動時に、前記生体認証情報検出手段により利用者から検出した生体認証情報と、前記電子回路に格納されている生体認証情報とを比較し、両情報が一致したとき、前記電子回路に格納されている前記アクセス認証情報が前記利用者端末を介して前記管理センターに送出され、
前記管理センターでは、受信した前記アクセス認証情報が、予め格納されているアクセス認証情報と一致する場合に、前記利用者を登録されている正規な利用者であると判断し、前記利用者端末を前記コミュニティへの接続を許可するネットワークアクセスシステム。
（６）ネットワークを介して利用者端末のアクセスによって、管理センターにより管理されているサーバーにするソサイエティを含むコミュニティへの接続を行うネットワークアクセスシステムにおいて、
前記管理センターには、接続を許可された利用者のアクセス認証情報が格納され、
前記利用者端末に内蔵され、または接続された利用者の生体認証情報を検出する生体認証情報検出手段と、
前記利用者端末に接続され、前記利用者の生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が格納され、信号処理機能を有する外付け記

憶媒体と、
前記生体認証情報検出手段により利用者から検出した生体認証情報と、前記外付け記憶媒体に格納されている生体認証情報とを比較し、両情報が一致したとき、前記外付け記憶媒体に格納されている前記アクセス認証情報が前記利用者端末を介して前記管理センターに送出され、
前記管理センターでは、受信した前記アクセス認証情報が、予め格納されているアクセス認証情報と一致する場合に、前記利用者を登録されている正規な利用者であると判断し、前記利用者端末を前記コミュニティへの接続を許可するネットワークアクセスシステム。
（７）前記電子回路または外付け記憶媒体にはアクセス先情報が格納され、前記アクセス先情報が送出される上記（５）または（６）のネットワークアクセスシステム。
（８）前記管理センターは、内蔵され、または接続されたユーザー登録センターを有し、前記ユーザー登録センターには前記利用者の個人情報や前記アクセス認証情報が格納されている上記５または６のネットワークアクセスシステム。
（９）前記アクセス認証情報は、利用者のＩＤとパスワードを含む上記１乃至８のいずれかのネットワークアクセスシステム。
（１０）前記利用者の前記ネットワーク側での情報授受は、前記利用者に対して予め付与されたニックネームによって行われる上記（１）乃至（９）のいずれかのネットワークアクセスシステム。
（１１）前記アクセス認証情報は、前記利用者端末側から暗号化されて出力され、前記ネットワーク側では、受信した暗号化されたアクセス認証情報を復号化する上記（１）乃至（１０）のいずれかのネットワークアクセスシステム。
（１２）前記アクセス認証情報は、利用者によるアクセス毎に変化される上記（１）乃至（１１）のいずれかのネットワークアクセスシステム。
（１３）前記変化するアクセス認証情報は、前記利用者端末側と前記ネットワーク側のみが知り得るように公開暗号キーと秘密復号キーに基づいて処理されている上記（１）乃至（１２）のいずれかのネットワークアクセスシステム。
（１４）前記ネットワーク側は、前記利用者の次回アクセス用のアクセス認証情報を生成し暗号化して前記利用者端末側に送出し、前記利用者端末側からの次回アクセス時には、前記ネットワーク側から受信した前記アクセス認識情報を送出する上記（１）乃至（１３）のいずれかのネットワークアクセスシステム。
（１５）前記ネットワーク側に格納されている利用者に関する情報は、前記利用者毎に付与されている基礎コードにより管理され、前記利用者を特定した利用者情報は、前記利用者側の前記電子回路で生成された補助コードと前記基礎コードを組み合わせた基本コードによってのみ読み込み、書き込みを可能とする上記（１）乃至（１４）のいずれかにのネットワークアクセスシステム。
（１６）前記ネットワーク側に格納されている利用者に関する情報は、前記利用者毎に付与されている基礎コードにより管理され、前記利用者を特定した利用者情報は、前記利用者側の前記外付け記憶媒体で生成された補助コードと前記基礎コードを組み合わせた基本コードによってのみ読み込み、書き込みを可能とする上記（１）乃至（１４）のいずれかにのネットワークアクセスシステム。
（１７）前記補助コードは公開暗号キーによって暗号化されて前記利用者端末側から送出され、前記ネットワーク側では、前記公開暗号キーに対応する秘密復号キーにより復号化して得られた補助コードとして利用される上記（１５）または（１６）のネットワークアクセスシステム。
（１８）前記利用者側と前記ネットワーク側間での情報授受は、公開暗号キーを用いた暗号化と、前記公開暗号キーに対応する秘密復号キーによる復号化処理を介して実行される上記（１）乃至（１７）のいずれかのネットワークアクセスシステム。
（１９）前記生体認証情報は、指紋認証、顔認証、声紋認証または瞳の虹彩認証情報である上記（１）乃至（１８）のいずれかのネットワークアクセスシステム。

（２０）前記ディスクは、光ディスクである上記（３）乃至（５）、（７）乃至（１５）、（１７）乃至（１９）のいずれかのネットワークアクセスシステム。

（２１）利用者端末からのアクセスにより、ネットワーク側に接続されているサービス系に接続するネットワークアクセス方法において、

ディスクに搭載された電子回路のメモリに利用者の生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報を格納しておき、

前記ディスク駆動時に、前記利用者から検出手段により取得した生体認証情報と、前記電子回路に格納されている生体認証情報とを比較し、両情報が一致したとき前記電子回路に格納されている前記アクセス認証情報を前記ネットワーク側に送出し、

前記ネットワーク側では、受信した前記アクセス認証情報に基づいて前記利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときに、前記利用者端末の前記サービス系への接続を許可するネットワークアクセス方法。

（２２）利用者端末からのアクセスにより、ネットワーク側に接続されているサービス系に接続するネットワークアクセス方法において、

前記利用者端末に接続され、信号処理機能を有する外付け記憶媒体に利用者の生体認証のための生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報を格納しておき、

前記利用者から検出手段により取得した生体認証情報と、前記外付け記憶媒体に格納されている生体認証情報とを比較し、両情報が一致したとき前記外付け記憶媒体に格納されている前記アクセス認証情報を前記ネットワーク側に送出し、

前記ネットワーク側では、受信した前記アクセス認証情報に基づいて前記利用者が正規な利用者であるか否かを判断し、正規な利用者であると判断されたときに、前記利用者端末の前記サービス系への接続を許可するネットワークアクセス方法。

（２３）前記電子回路または外付け記憶媒体にはアクセス先情報が格納され、前記アクセス先情報が送出される上記（２１）または（２２）のネットワークアクセスシステム。

（２４）利用者端末のアクセスによりネットワークを介して、接続を許可された利用者のアクセス認証情報が格納された管理センターにより管理されているサーバーに接続するネットワークアクセス方法であって、

ディスクドライブで駆動され、前記利用者の生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報が格納された電子回路が搭載されたディスクの駆動時に、前記利用者端末側の生体認証手段により得られた前記利用者の生体認証情報と、前記ディスクの電子回路に格納された生体認証データとを比較し、両情報が一致したとき、前記電子回路に格納されている前記アクセス認証情報が前記利用者端末を介して前記管理センターに送出し、

前記管理センターは、受信した前記アクセス認証情報を、予め格納されているアクセス認証情報と比較し、両情報が一致したときのみ前記利用者端末の接続を許可するネットワークアクセス方法。

（２５）利用者端末のアクセスによりネットワークを介して、接続を許可された利用者のアクセス認証情報が格納された管理センターにより管理されているサーバーに接続するネットワークアクセス方法であって、

前記利用者の生体認証情報と、利用者毎に定められているネットアクセス時に必要なアクセス認証情報を、信号処理機能を有する外付け記憶媒体に格納し、前記利用者端末側の生体認証手段により得られた生体認証情報と、前記外付け記憶媒体に格納された生体認証データとを比較し、両情報が一致したとき、前記外付け記憶媒体に格納されている前記アクセス認証情報が前記利用者端末を介して前記管理センターに送出し、

前記管理センターは、受信した前記アクセス認証情報を、予め格納されているアクセス認証情報と比較し、両情報が一致したときのみ前記利用者端末の接続を許可するネットワークアクセス方法。

（２６）　前記電子回路または外付け記憶媒体にはアクセス先情報が格納され、前記アクセス先情報が送出される上記（２４）または（２５）のネットワークアクセスシステム

。

（２７）前記利用者の前記ネットワーク側での情報授受を、前記利用者に対して予め付与されたニックネームによって行う上記（２１）乃至（２６）のいずれかのネットワークアクセス方法。

（２８）前記ネットワーク側には、前記利用者の個人情報や前記アクセス認証情報が格納されている上記（２１）乃至（２７）のいずれかのネットワークアクセス方法。

（２９）前記アクセス認証情報は、利用者のＩＤとパスワードを含む上記（２１）乃至（２８）のいずれかのネットワークアクセス方法。

（３０）前記アクセス認証情報は、前記利用者端末側から暗号化されて出力し、前記ネットワーク側では、受信した暗号化されたアクセス認証情報を復号化する上記（２１）乃至（２９）のいずれかのネットワークアクセス方法。

（３１）前記アクセス認証情報は、利用者によるアクセス毎に変化させる上記（２１）乃至（３０）のいずれかのネットワークアクセス方法。

（３２）前記変化するアクセス認証情報は、前記利用者端末側と前記ネットワーク側のみが知り得るように公開暗号キーと秘密復号キーに基づいて処理する上記（２１）乃至（３１）のいずれかのネットワークアクセス方法。

（３３）前記ネットワーク側は、前記利用者の次回アクセス用のアクセス認証情報を生成し暗号化して前記利用者端末側に送出し、前記利用者端末側からの次回アクセス時には、前記ネットワーク側から受信した前記アクセス認識情報を送出する上記（２１）乃至（３２）のいずれかのネットワークアクセス方法。

（３４）前記ネットワーク側に格納されている利用者に関する情報は、前記利用者毎に付与されている基礎コードにより管理し、前記利用者を特定した利用者情報は、前記利用者側の前記電子回路で生成された補助コードと前記基礎コードを組み合わせた基本コードによってのみ読み込み、書き込みを可能とする上記（２１）乃至（３３）のいずれかのネットワークアクセス方法。

（３５）前記ネットワーク側に格納されている利用者に関する情報は、前記利用者毎に付与されている基礎コードにより管理し、前記利用者を特定した利用者情報は、前記利用者側の前記外付け記憶媒体で生成された補助コードと前記基礎コードを組み合わせた基本コードによってのみ読み込み、書き込みを可能とする上記（２１）乃至（３３）のいずれかのネットワークアクセス方法。

（３６）前記補助コードを公開暗号キーによって暗号化されて前記利用者端末側から送出し、前記ネットワーク側では、前記公開暗号キーに対応する秘密復号キーにより復号化して得られた補助コードとして利用する上記（３４）のネットワークアクセス方法。

（３７）前記利用者側と前記ネットワーク側間での情報授受は、公開暗号キーを用いた暗号化と、前記公開暗号キーに対応する秘密復号キーによる復号化処理を介して実行する上記（２１）乃至（３５）のいずれかのネットワークアクセス方法。

（３８）前記生体認証情報は、指紋認証、顔認証、声紋認証または瞳の虹彩認証情報である上記（２１）乃至（３７）のいずれかのネットワーク方法。

（３９）上記（２１）乃至（３８）のいずれかの処理をコンピュータに実行させるためのプログラムを格納した記憶媒体。

【発明の効果】

【００１２】

本発明によれば、光ディスク（光ディスクに限らず一般的なディスク記憶媒体）に格納されている利用者個人の情報は、暗号化されて光ディスクに搭載されている電子回路のメモリに保存され、一方、サービスを提供するサイドにも当該利用者の個人情報が暗号化されて保存され、それぞれの個人情報は、利用者側とサービス提供者サイド（ネットワーク側）のみが知っている暗号キーや復号キーでしか暗号化、復号化処理ができないためセキュリティは格段に向上する。つまり、利用者が保持する光ディスクは、利用者のネット社会に対するパスポートとしての機能を有する。したがって、利用者が必要と判断する相手に対してのみ情報を制限を付けて提供することができる。また、利用者は、ネットサービ

スを受ける際（ネットへのアクセス時）、認証のための情報（ＩＤやパスワード）を入力する手間が不要で、駆動された光ディスク側から自動的に認証のための情報が生成されるため、しかもその情報は利用者側とサービス提供（管理サーバー）側のみ復号化可能とされ、更には、双方向ワンタイムパスワードを送出しているため、ネットワークアクセス時のセキュリティが確保される。サービスへの参加、所属、脱退も利用者本人の意思で高度なセキュリティを維持しつつ行うことができる。そして、利用者がネット社会で開示するのは、本人の氏名ではなくニックネームであるため、個人情報の開示の問題はなくなる。このように本発明によれば、利用者個人毎に光ディスク搭載電子回路に格納されている情報によって、インターネットにアクセスしており、たとえニックネームによる開示であっても、その利用者の実在が保証されているため、きわめてセキュリティの高いインターネットへのアクセス、サービスの提供を受けることができる。

【実施例】

【００１３】

以下、本発明によるネットワークアクセスシステム、方法及び記憶媒体の好適実施例の構成及び動作について添付図面を参照して詳細に説明する。図１は、本発明によるネットワークアクセスシステムの一実施例の基本システム構成図である。

【００１４】

なお、以下の説明では、ＣＰＵ機能やメモリ等を有する電子回路を搭載した光ディスクを利用しているが、光ディスクに限らず任意のディスク、記憶媒体にも本発明が適用可能であることは勿論である。また、本発明を実施するための構成は、以下に述べるような構成に限定されず、任意の公知の構成を用いることができ任意であり、同様な機能を達成できる構成を採用することができる。

【００１５】

図２は本実施例における光ディスクをディスクドライブで駆動する構成を示す図である。図２の構成においては、ディスクドライブ１００を用いて光ディスクを回転させて光ディスクからデータを読み出したり、データを書き込んだりする。光ディスクの一面に設けられたデータ記憶部には所望のデータ（コンテンツ等のデータ）が記憶されている。光ディスクのデータ記憶部が形成されている面とは反対面には所定の信号処理を実行する電子回路（ＣＰＵ）１１０が搭載されている。電子回路１１０は、受発信部１１１、信号処理部１１２、メモリ１１３を備える。また、電子回路１１０での信号処理結果や外部からの情報は、例えば、無線信号としてディスクドライブの無線部（受発信部）１１１を介して外部回路との間で送出／受信される。

【００１６】

ディスクドライブ１００には光ディスクを挿入する挿入口（図示せず）が設けられ、挿入された光ディスクは所定速度で回転される。光ディスクの回転状態で、光ピックアップから光ディスク表面に向けてレーザ光を照射し、その反射光を光ピックアップを介して検出することにより光学的に記録されているデータを読み出す。また、光ピックアップからレーザ光を照射してデータを記録する。

【００１７】

ディスクドライブ１００は、光ディスクを回転駆動するための駆動部１３０とメモリ１４０（必須ではないことは勿論である）を備える。光ディスクは、その一面は音楽情報、映像情報、プログラム情報等のデータが書き込まれたＲＯＭ領域と、任意のデータの書き込みが可能なＲＡＭ領域の少なくともいずれかを有する光データ記憶部１２０を備え、他面はＣＰＵ機能を有する電子回路１１０を備える。電子回路１１０は、例えばＲＦＩＤ（Radio Frequency Identification）部として形成することができる。勿論、電子回路１１０は上記一面に設けることもできる。

【００１８】

ＲＦＩＤ部は、一般に、電磁波を使った非接触通信を可能とするもので、半導体メモリ（ＩＣチップ）内のデータを非接触の状態で通信（読み書き）可能とし、ＲＦＩＤ部は、通常、ＩＣチップとそれに接続したコイル状のアンテナから構成される。

【００１９】
受発信装置２００は、リーダ／ライタ機能を有し、上記光ディスク面に配設された電子回路１１０としてのＲＦＩＤ部のＩＣチップ内の受発信部１１１との間で無線通信によりデータ授受を行う。受発信装置２００と、電子回路１１０の受発信部１１１との間のデータ通信は、例えば１０６ｋｂｐｓの伝送速度で行われる。
【００２０】
電子回路１１０（ＲＦＩＤ部）内のアンテナ（受発信部１１１）が受発信装置２００からの電波を受信すると、共振作用により起電力が発生（電磁誘導等）するので、この起電力を電源整流部で整流して電子回路１１０の電源として用いる。この電源によりＲＦＩＤ部内のＩＣチップが起動される。
電源供給は、かかる構成に限定されるものではないことは勿論である。
【００２１】
パソコン３００は、ＯＳ等の基本情報が格納されているＲＯＭ部（蓄積部）３１０、書き換え可能な記憶部としてのＲＡＭ部３２０、ＣＰＵ等の演算処理部３３０、液晶等の表示部３４０を備え、ディスクドライブ１００との間でデータ授受を行い、所望の信号処理を行う。
【００２２】
生体認証装置４００は、本システムの起動、動作を許可された利用者のみに限定するためのもので、指紋認証、顔認証、声紋認証、瞳の虹彩認証等の生体系パラメータが考えられる。ディスクドライブ１００の起動時（パソコン３００に接続しておき、その起動時でも同様）、生体認証装置４００の、例えば、指紋認証のための指紋読取部に利用者は所定の指を接触させて光学的に読み取り、予め記憶、登録されている利用者の指紋と照合し、両者が一致したときのみ正規な利用者としえ使用を許可する。
【００２３】
さて、以上のような構成を前提とし、本実施例では、不正なりすましによる侵入や個人情報の漏洩を防止するための種々の方策を採用している。
【００２４】
先ず、メモリを有する電子回路１１０が搭載された光ディスクが利用者毎に用意されており、または利用者の利用を希望するコミュニティへの参加毎に用意される。電子回路１１０のメモリには、利用者のＩＤやアクセスに必要な情報が格納されている。これらの情報（例えば、ＩＤ、パスワード等）は、利用者によるアクセスの都度、変更され、しかも、これらの情報は暗号化処理が施されており、利用者と、サービス提供側に設置されている管理センター側だけでしか知り得ないような形態とされている。電子回路のメモリには、また、利用者の認証のための認証データが格納されている。本実施例では、生体認証データが用いられ、例えば指紋データが格納されている。
【００２５】
ディスクドライブ装置１００には、生体認証装置４００としての指紋検出装置が接続（または内蔵）されており、利用者が、自己の光ディスクをディスクドライブ装置に挿入すると、ディスクドライブ装置は、指紋検出装置で得られた指紋データと光ディスクの電子回路のメモリに格納されている指紋データとを照合し、両データが一致していると判断したときに、正規な利用者であると判断して、次なる処理ステップに移行する。
【００２６】
図１を参照すると、本実施例は、予め登録された一人または複数の利用者Ａ～Ｄが、それぞれ使用するパソコン等の利用者端末１Ａ～１Ｄ（図２のパソコン３００）、・・・を使用して、例えば、インターネット等のネットワークを介してサービス提供者としての管理センター３が管理するコミュニティに参加する場合に本発明を適用した実施例である。
【００２７】
管理センター３が管理するコミュニティには、多くのソサイエティ（図では、チャネル（ＣＨ１～ＣＨ３）３１１～３１３が設けられており、利用者は、自分が希望するソサイエティへの加入、参加をフロントエンドサービス２Ａ～２Ｄ、・・・等を介して管理セン

ター３に要求することにより行う。

【００２８】

本実施例においては、利用者は、予め管理センター３を運営する組織に登録され（ユーザー登録センター４）、登録された利用者のみが管理センター３の管理するネットワークサービス（ソサイエティへの参加等）を受けることができる。すなわち、登録された利用者の利用者コードＩＤ、パスワードＰＷ等を付与された利用者が、これら情報を管理センター３に送出し、管理センター３側で正規に登録された利用者と認定された者のみをアクセス可能とし、上記サービスを享受できるような構成を採用している。

【００２９】

管理センター３は、多数のエージェント（Ａｇ）３１Ａ～３１Ｅ、・・・を有し、外部（フロントエンドサービス等）とソサイエティ（チャネルＣＨ１（３１１）、ＣＨ２（３１１）、ＣＨ３（３１３）・・）との接続を制御する。図１では、各利用者端末１Ａ～１Ｅには、対応してエージェント３１Ａ～３１Ｅが設けられている。

【００３０】

管理センター３側には、内蔵して、またはエージェント３１Ｆを介してユーザー登録センター４が接続され、そこに利用者情報が格納されている。ユーザー登録センター４は、利用者の情報として個人情報、ＩＤ情報、パスワード（ＰＷ）等を、必要により暗号化して格納、管理している。例えば、利用者Ａ～Ｅの免許証、住基カード等の個人情報は、それぞれの暗号化キー（ＵＡＩ１～ＵＥＩ１）で暗号化されてメモリに格納され、また、各利用者毎に割り当てられている識別ＩＤとパスワードＰＷが管理されている。ここで、Ｕは利用者を、Ａ、Ｅは個々の利用者を、Ｉは個人情報を、最後に付された数字は何回目のアクセス、処理であるかを示す数字を、それぞれ示している。

【００３１】

ユーザー登録センター４は、各種情報を管理しており、利用者Ａ～ＥのパスワードＰＷ１、ＰＷ２、ＩＤ情報（ＩＤ０、ＡＩＤｉ）、管理センター３のパスワードＫＡｐｉの管理、チャネルやエージェントの管理、公開暗号キーＫｅや秘密復号キーＫｄ等の種々情報を管理している。ユーザー登録センター４は、エージェント３１Ｆを介して管理センター３に接続され、情報の授受が行われる。

【００３２】

フロントエンドサービス２Ａ～２Ｅは、エージェント３１Ａ～３１Ｆに接続され、これらエージェントを介して、互いに接続されるべき所望のフロントエンドサービスとの接続が直接的に行われる。これは、通常のインターネット接続が、接続されるべき両者のＩＰアドレスを用いてＩＰネットワークで接続されるのとは異なる。

【００３３】

以上の構成において、利用者端末１Ａ～１Ｅと管理センター３（ユーザー登録センター４）との間の信号の授受の際は、セキュリティ確保のために各種暗号化処理と復号化処理が施される。この暗号化は公開暗号キーにより行われる。復号化処理は、公開暗号キーに対応する秘密復号キーにより実行される。

【００３４】

次に、本実施例における利用者情報のユーザー登録センター４及び管理センター３への登録処理、更にはソサイエティへの参加形成処理について説明する。

【００３５】

先ず、これら処理で使用される記号の意味について説明する。（ここでは、利用者Ａについて説明する）。

【００３６】

Ａｅ[ＩＤ０,Ａｐ０,ＡＩ０]は、利用者Ａの“０”番目（最初）のＩＤ（ＩＤ０：基礎コード）、パスワード（Ａｐ０）及び暗号キー（ＡＩ０）の情報を公開暗号キーＡｅで暗号化された情報を示す。

また、Ａｄ{Ａｅ[ＩＤ０,Ａｐ０,ＡＩ０]}は、上記Ａｅ[ＩＤ０,Ａｐ０,ＡＩ０]を秘密復号キーＡｄで復号化された情報を示す。

【００３７】
ＫｅとＫｄは、管理センター３で管理されている公開暗号キーと秘密復号キーを示し、予め管理センター３で事前に作成される。ユーザー登録センター４の公開暗号キーＵｅと秘密復号キーＵｄも同様に事前に作成される。
ＵＡＩ０は、ユーザー登録センター４が発行した利用者Ａの初期暗号キーで、ユーザー登録センター４は利用者Ａの個人情報を利用者Ａの初期暗号キーＵＡＩ０で暗号化し、予め付与された後述する基礎コードＩＤ０の名前がついたホルダーに格納して管理する。
【００３８】
基礎コードＩＤ０は、ユーザー登録センター４が発行する唯一つしか存在しないユニークなコードであり、例えば、Ｐ４ＫＹＵ％７のような唯一コードが割り当てられる。基礎コードＩＤ０としては、実際には、ユニークであろうと推察されるコードが割り当てられる。ユーザー登録センター４は、基礎コードＩＤ０で利用者の個人情報等を管理し、この基礎コードＩＤ０に基づいて情報の読み出し、書き込みが行われる。しかし、ユーザー登録センター４は、基礎コードＩＤ０に対応する情報を管理できるだけで、利用者自身を特定した情報を得ることはできない。
【００３９】
Ｋｄ{Ｋｅ[ＩＤ０,Ａｐ０]}は、管理センター３Ａの公開暗号キーＫｅで[ＩＤ０,Ａｐ０]が暗号化された情報Ｋｅ[ＩＤ０,Ａｐ０]を、管理センター３側の秘密復号キーＫｄで復号した情報を意味する。
Ａｄ{Ａｅ[ＩＤ０,Ａｐ０]}は、利用者Ａの公開暗号キーＡｅで情報[ＩＤ０,Ａｐ０]が暗号化された情報Ａｅ[ＩＤ０,Ａｐ０]を、利用者の秘密復号キーＡｄで復号した情報を意味する。
【００４０】
ＡＩＤ１は、基本コードと称され、基礎コードＩＤ０と補助コードＡＡＩＤ１から成り、ＡＩＤ１＝ＩＤ０（基礎コード）＋ＡＡＩＤ１（補助コード）で表され、補助コードＡＡＩＤ１は利用者の所持する光ディスクに搭載された電子回路で作成される。
【００４１】
利用者Ａの情報（個人情報に限らず必要なすべての情報）は、上記基本コードの介在なしでは、取得できない。すなわち、基礎コードＩＤ０や補助コードＡＡＩＤ１それぞれ単独では、利用者Ａを特定した情報にはアクセスできず、両者がそろった基本コードＡＩＤ１によってのみアクセスできる。その結果、前述のように、ユーザー登録センター４では、利用者Ａを特定した情報にはアクセスできない。
【００４２】
基本コードＡＩＤ１としては、例えば、基礎コードＩＤ０をＯＰ４ＫＹＵ％７とし、補助コードＡＡＩＤ１をＱＳＣ５６ＶＢＡとすると、
ＡＩＤ１＝ＯＰ４ＫＹＵ％７＋ＱＳＣ５６ＶＢＡ
のように表わすことができる。
Ｕｄ{Ｕｅ[ＩＤ０,ＵＡＩ１,Ａｐ１]}は、（ＩＤ０,ＵＡＩ１,Ａｐ１）をユーザー登録センター４の公開暗号キーＵｅで暗号化した情報を、秘密復号キーＵｄで復号化した情報を示す。
Ｋｅ[ＩＤ０，ＡＩＤ１，Ａｐ１、ニックネーム]は、（ＩＤ０，ＡＩＤ１，Ａｐ１、ニックネーム）を管理センター３の公開暗号キーＫｅで暗号化した情報を示す。
Ｋｄ{Ｋｅ[ＩＤ０，ＡＩＤ１，Ａｐ１,ニックネーム]}は、（ＩＤ０，ＡＩＤ１，Ａｐ１,ニックネーム）を管理センター３の公開暗号キーＫｅで暗号化した情報を、管理センター３の秘密復号キーＫｄで復号化した情報を示す。
【００４３】
次に、図２のフローチャートを参照しながら＜ユーザー登録センター４及び管理センター３への登録処理＞について説明する。
【００４４】
先ず、利用者が免許証、住基カード等の個人を証明できる書類をユーザー登録センター

４に持参する（ステップＳ１０１）。ユーザー登録センター４では、利用者情報としてのＩＤ（ＩＤ０：基礎コード）とパスワードＰＷ１（Ａｐ０：利用者Ａの初期パスワード）と初期暗号キー（ＡＩ０）を利用者Ａの公開暗号キー（Ａｅ）で暗号化し、利用者Ａの光ディスク搭載電子回路に登録する（ステップＳ１０２）とともに、免許証、住基カード等の個人情報をユーザー登録センター４の初期暗号キーＵＡＩ０で暗号化してサーバー（メモリ）に登録、格納する（ステップＳ１０３）。

【００４５】

ユーザー登録センター４は、また管理センター３で用意されている公開暗号キーＫｅで利用者Ａの情報ＩＤ（ＩＤ０）とパスワードＰＷ１（Ａｐ０）を暗号化し、管理センター３に送出する（ステップＳ１０４）。

【００４６】

管理センター３は、ユーザー登録センター４から受信した情報ＩＤ（ＩＤ０）とパスワードＰＷ１（Ａｐ０）を管理センター３側で用意されている秘密復号キーＫｄで復号化して保存するとともに、管理センター３側のパスワードＰＷ２（ＫＡｐ０）を作成する（ステップＳ１０５）。

【００４７】

さて、利用者Ａが実際にアクセスするときには、パソコンや周辺装置の電源をＯＮし、生体認証装置１１Ａ（図２における生体認証装置４００）を用いて生体認証を行い、正しい利用者であることが確認された後、光ディスクを起動し（ステップＳ１０６）、光ディスクやパソコンにインストールされているフロントエンドサービス２Ａを起動する（ステップＳ１０７）。

【００４８】

次に、電子回路は、ユーザー登録センター４で光ディスクに登録されたＩＤ（基礎コードＩＤ０）とパスワードＰＷ１(Ａｐ０)を、予め用意されている秘密復号キーＡｄで復号化して確認する（ステップＳ１０８）。また、電子回路は、補助コード（ＡＡＩＤ１）を発生し、光ディスクに登録されている基礎コードＩＤ０に加算し、基本コードＡＩＤ１（ＡＩＤ１＝ＩＤ０＋ＡＡＩＤ１）を作成する（ステップＳ１０９）。このとき、電子回路は、ユーザー登録センター４で登録された初期暗号キーＵＡＩ０に基づいて、ユーザー登録センター４での暗号化に用いられる利用者Ａの暗号キーＵＩＡＩ１、暗号キーＡＩ１及びパスワードＰＷ（Ａｐ１）を作成する（ステップＳ１１０）。利用者端末１Ａの電子回路では、利用者Ａの公開暗号キーＡｅ、秘密復号キーＡｄ、パスワードＰＷ１、管理センター３側で用いるパスワードＰＷ２、ＩＤ（基本コードＡＩＤ１）、暗号ＡＩｉ等の情報を作成する。他の利用者端末１Ｂ～１Ｅも、同様な情報を作成する。

【００４９】

利用者端末１Ａ側では、ユーザー登録センター４の公開暗号キー（Ue）で基礎コードＩＤ０、暗号キーＵＡＩ1、パスワードＰＷ（Ａｐ１）を暗号化し、ユーザー登録センター４に送出する（ステップＳ１１１）。

【００５０】

ユーザー登録センター４は、受信した情報を、用意されている秘密復号キーＵｄで復号化し、基礎コードＩＤ０の名前が付されているホルダーの個人情報を読み込んで暗号キーＵＡＩ０に対応する復号キーで復号化後　暗号キーＵＡＩ1で暗号化して更新、保存する。また、パスワードＰＷ（Ａｐ１）も同一ホルダーに更新、保存する（ステップＳ１１２）。

【００５１】

利用者端末１Ａでは、管理センター３の公開暗号キー（Ｋｅ）でアクセスコードとしての基礎コードＩＤ０、基本コードＡＩＤ１、パスワードＰＷ（Ａｐ１）、利用者Ａに任意に付与されているニックネームを暗号化し、管理センター３に送出する（ステップＳ１１３）。

【００５２】

管理センター３は、利用者端末１Ａから受信した情報を、用意されている秘密復号キー

Ｋｄで復号化し、基礎コードＩＤ０対応のホルダーに、
（１）利用者Ａの更新された基本コードＡＩＤ１
（２）利用者Ａの更新されたパスワードＰＷ（Ａｐ１）
（３）管理センターから利用者Ａに送出されたパスワードＰＷ（ＫＡｐ０）
（４）利用者Ａのニックネーム、
を保存する（ステップＳ１１４）。

【００５３】

ステップＳ１１０の処理後、利用者端末１Ａ側の光ディスクに搭載されている電子回路には、
（１）ＡＩ１で再度暗号化した免許証、住基カード等の個人情報
（２）ＡＩ１で暗号化された基礎コードＩＤ０とＡＩＤ１
（３）ＡＩ１で暗号化した管理センター３からのパスワードＰＷ（ＫＡｐ０）
（４）利用者Ａのニックネーム
（５）ユーザー登録センター４の暗号キーＵＡＩ１
を保存する（ステップＳ１１５）。

【００５４】

ステップＳ１１２、Ｓ１１４及びＳ１１５の処理の後、以降、ｉ番目の各暗号キー、基本コード、パスワード：ＵＡＩｉ、ＡＩＤｉ、ＰＷ(Ａｐｉ)が逐次利用者Ａの光ディスクの電子回路で更新され、同時に管理センター３及びユーザー登録センター４のＩＤ０のホルダーに格納されている情報もその都度更新される（ステップＳ１１６）。

【００５５】

以上説明したように、本実施例では、インターネットへのアクセス時に必要な利用者のＩＤとパスワードが２元的に自動的に生成されて、しかも次回アクセス時のＩＤとパスワードを相互に毎回変化させて生成している。生成されたＩＤとパスワードは、暗号化され、それぞれでしか復号できないような構成となっている。

【００５６】

次に、図３のフローチャートを参照して＜ソサィティ（場、チャネル）の形成処理＞について説明する。

【００５７】

先ず、利用者Ａは、パソコンや周辺装置の電源をＯＮし、指紋認証装置１１Ａを用いて生体認証を行い、正規な利用者であることが確認されると、光ディスクをディスクドライブで起動し（ステップＳ２０１）、フロントエンドサービス２Ａを起動する（ステップＳ２０２）。このフロントエンドサービス２Ａは、光ディスクにインストールされている（設定されている）、利用者単位で設定されている特殊プログラム処理により、ネット接続のための特定プログラムとすることができる。この特定プログラムは、サービス提供側の管理センター３に設けられている、利用者が希望するソサィティ（場、チャネル：ＣＨ１、ＣＨ２、ＣＨ３、・・・）への接続を行うための処理を、予め光ディスクに格納されている利用者特有の情報に基づいて実行させるためのものである。

【００５８】

すなわち、利用者端末１Ａでは、ユーザー登録センター４で光ディスクに登録されているＩＤ(基本コードＡＩＤ１)、パスワードＰＷ(Ａｐ１)を暗号キーＡＩ１に対応する復号キーで復号化し、所属したいチャネル（本例では、チャネルＣＨ１とする）とともに管理センター３の公開暗号キーＫｅで暗号化して送出する（ステップＳ２０３）。フロントエンドサービス（ＦＳ）２Ａは、利用者端末１Ａから受信した情報をソサイティへの接続を制御するエージェント３１Ａに受け渡し（ステップＳ２０４）、エージェント３１Ａは、管理センター３にそれを送出する（ステップＳ２０５）。

【００５９】

管理センター３は、秘密復号キーＫｄで、希望チャネル（ＣＨ１）、暗号キーＡＩ１、基本コードＡＩＤ１及びパスワードＡｐ１を復号化する（ステップＳ２０６）。利用者端末１Ａでは、管理センター３側が持っている利用者Ａの暗号キーで暗号化された基本コー

ドＡＩＤ１及びパスワードの初期値Ａｐ０を、復号（秘密）キーＡｄで復号して基本コードＡＩＤ１と、管理センター３側のパスワードＫＡｐ０を入手する（ステップＳ２０７）。

【００６０】

次に、こうして得られた利用者ＡのＩＤと、パスワードＰＷとを比較し（ステップＳ２０８）、一致していなければ、管理センター３は、利用者Ａに再度ＩＤとパスワードＰＷの送付を依頼し（ステップＳ２０９）、管理センター３は、利用者Ａの公開暗号キーＡｅで暗号化された基本コードＡＩＤ１と管理センター３の利用者Ａ用のパスワードＰＷ（ＫＡｐ０）を添付して利用者端末１Ａの電子回路に対して再送付を依頼する（ステップＳ２１０）。そうすると、利用者Ａは、秘密復号キーＡｄで基本コードＡＩＤ１と管理センター３のパスワードＫＡｐ０を復号化して入手し、基本コードＡＩＤ１と管理センター３のパスワードＫＡｐ０と利用者Ａの有するコードとを比較し、管理センター３からのものであることを認証する（ステップＳ２１１）。その後、ステップＳ２０３の処理に戻る。

【００６１】

ステップＳ２０８における比較の結果、ＩＤとパスワードＰＷの両者が一致していると判定されると、利用者ＡのＩＤ(ＡＩＤ１)とパスワードＰＷ（Ａｐ１）で利用者Ａを認証し、管理センター３は利用者Ａの希望するチャネルＣＨ１を繋ぐようにエージェント３１Ａに命令する（ステップＳ２１２）。

【００６２】

エージェント３１Ａは、利用者Ａのフロントエンドサービス（ＦＳ）２ＡとチャネルＣＨ１をエージェント３１Ａを介して接続する（ステップＳ２１３）。

【００６３】

同様に、利用者端末１Ｂや１Ｃ等、希望する利用者端末も接続し、チャネルＣＨ１のソサィティを形成する（ステップＳ２１４）。

【００６４】

利用者端末１Ａの光ディスク搭載電子回路は、新規の（２回目のアクセス）パスワードＡｐ２と暗号キーＡＩＤ２とを作成し、ＩＤ０とともに管理センター３の公開暗号キーＫｅで暗号化して送出する（ステップＳ２１５）。

【００６５】

管理センター３は、パスワードＫＡｐ１を作成し、作成したパスワードＫＡｐ１を利用者Ａの公開暗号キーＡｅで暗号化して利用者端末１Ａに送出する（ステップＳ２１６）。利用者Ａは、ソサィティでのコミュニケーション、サービスを受け（ステップＳ２１７）、サービス終了後、利用者Ａは、エージェント３１Ａに切断を要求する（ステップＳ２１８）。

【００６６】

ステップＳ２１８の処理後、利用者ＡのＩＤ(ＩＤ１)とパスワードＰＷ（Ａｐ１）で利用者Ａを認証し、認証されると、管理センター３は、利用者Ａの希望するチャネルＣＨ１を切断するようにエージェント３１Ａに命令する（ステップＳ２２１）。管理センター３は、利用者ＡのＩＤを新たに作成された基本コードＡＩＤ２、パスワードＰＷを、新たに作成されたパスワードＡｐ２に更新して保存する（ステップＳ２２２）。そして、エージェント３１Ａは、利用者ＡのフロントエンドサービスＦＳ）２ＡとチャネルＣＨ１）を切断する（ステップＳ２２３）。

【００６７】

一方、ステップＳ２１５の処理後、ユーザー登録センター４に対して利用者Ａの２回目アクセス時のパスワードＡＰ２と基礎コードＩＤ０を、公開暗号キーＵｅで暗号化してユーザー登録センター４に送出し（ステップＳ２１９）、ユーザー登録センター４では、秘密復号キーＵｄで復号化して得られたパスワードＡＰ２を更新し、保存する（ステップＳ２２０）。

【００６８】

以上と同様な処理を経て他の利用者も任意のチャネルに接続され、所望のサービスの提

供を受ける。

【００６９】

こうして複数の利用者が所定のソサイティに参加できるようになる。ソサイティに参加している利用者（Ａ）が使用しているパソコンのディスプレイ画面には、参加しているソサイティの掲示板が表示され、利用者Ａを含め参加している利用者のニックネームが表示される。また、同掲示板には、図４に示すように、利用者（Ａ）の利用できる（ＲＥＡＤ、ＷＲＩＴＥ）機能とサービス（チャット、電話、ホームページ、アンケート調査等）が表示されている。

【００７０】

本実施例では、互いに接続されるべき所望のフロントエンドサービスとは、ＩＰネットワークやメールアドレスではなく、直接的に接続されているので、これらの個人情報を開示せずとも、メールマガジンサービス業者が設置した利用者端末からメールマガジン等を受信することができる。

【００７１】

また、利用者端末を銀行や配送業者側に設置された端末とすれば、ネットショッピングによる口座振替指示を銀行側の端末に対して行えば業者にクレジットカード情報を開示せずに決済が行えるし、運送業者には住所のみを開示すれば良く個人情報の無制限な開示を避けることができ、セキュリティが向上する。

【００７２】

上述実施例における各処理は、プログラムとして記述され、このプログラムに基づく処理をコンピュータによって実行させることができることは勿論であり、当該プログラムは記憶媒体に格納される。

【００７３】

以上、本発明の好適実施例の構成及び動作を詳述した。しかし、斯かる実施例は、本発明の単なる例示に過ぎず、何ら本発明を限定するものではないことに留意されたい。本発明の要旨を逸脱することなく、特定用途に応じて種々の変形変更が可能であること、当業者には容易に理解できよう。例えば、電子回路は光回路としても良いし、情報は電子回路または／及びディスクに格納させることもできることは勿論である。また、ディスクの代わりにＵＳＢメモリのように外部から取り外し可能に接続される記憶媒体であれば、どのようなものでも使用できることも勿論である。

【図面の簡単な説明】

【００７４】

【図１】本発明によるネットワークアクセスシステムの好適実施例の基本構成ブロック図である。

【図２】本発明の実施例における光ディスクをディスクドライブで駆動する構成を示す図である。

【図３】本発明の実施例におけるユーザー登録センター４及び管理センター３への登録処理手順を示すフローチャートである。

【図４】本発明の実施例における利用者が参加するソサィティ（場、チャネル）の形成処理手順を示すフローチャートである。

【図５】本発明の実施例において利用者のディスプレイに表示される利用可能機能とサービス内容例を示す図である。

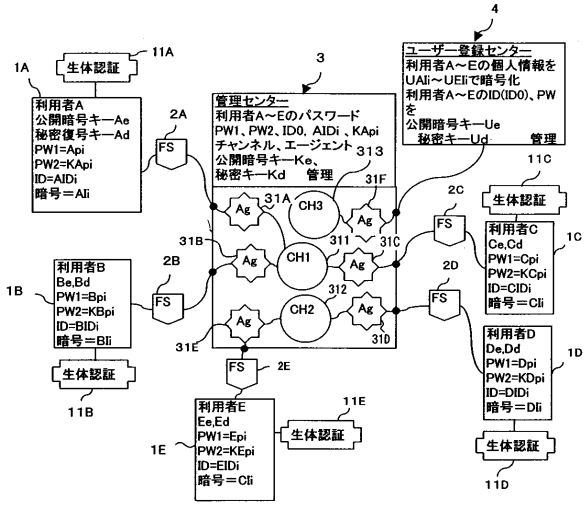
【符号の説明】

【００７５】

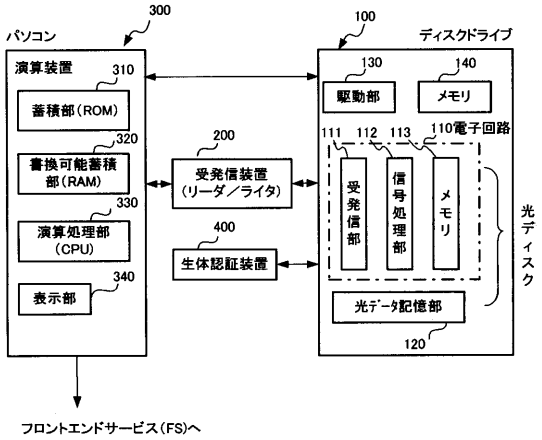
１Ａ～１Ｅ	利用者端末
２Ａ～２Ｅ	フロントエンドサービス
３	管理センター
４	ユーザー登録センター
１１Ａ～１１Ｅ	生体認証部
３１Ａ～３１Ｆ	エージェント

３１１～３１３	チャネルＣＨ１～ＣＨ３
１００	ディスクドライブ
１１０	電子回路
１１１	受発信部
１１２	信号処理部
１１３	メモリ
１２０	光データ記憶部
１３０	駆動部
１４０	メモリ
２００	受発信装置
３００	パソコン
３１０	ＲＯＭ部
３２０	ＲＡＭ部
３３０	演算処理部
３４０	表示部
４００	生体認証装置

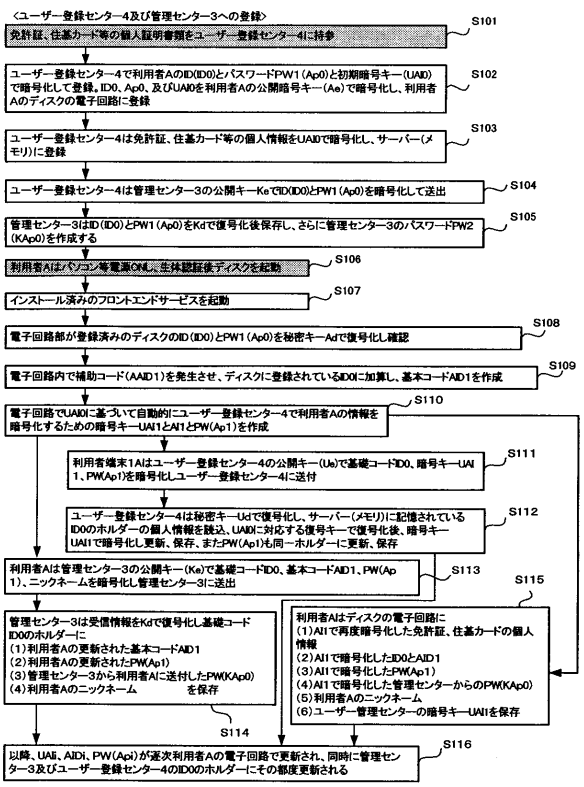
【図１】



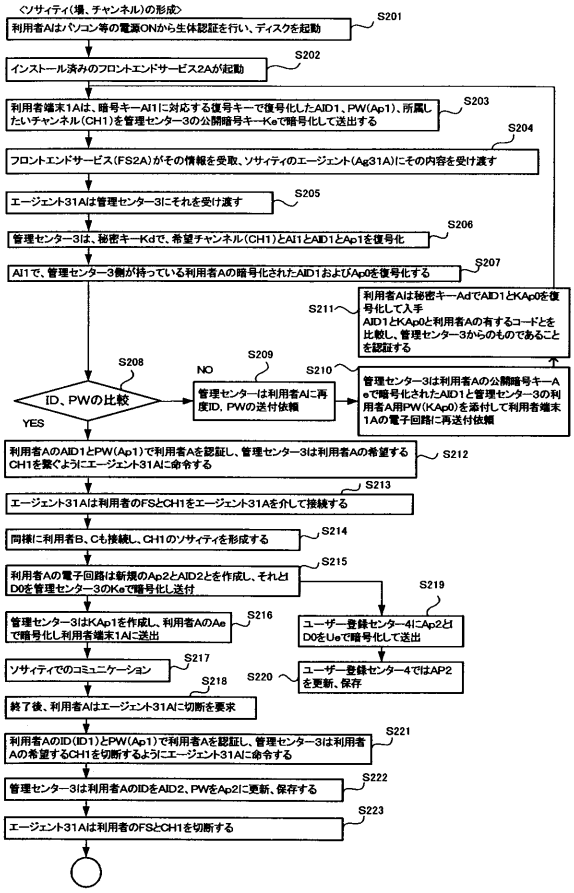
【図２】



【図３】



【図４】



【図５】

READ	WRITE	
○	○	チャット、電話
○	×	ホームページ
×	○	アンケート調査

フロントページの続き

(72)発明者　刈本　博保
横浜市港北区新横浜３－２－６　新横浜ビジネスセンタービル６Ｆ
インテリジェントディスク株式会社内
(72)発明者　中村　正規
東京都千代田区内幸町１丁目１番３号　東京電力株式会社内

Ｆターム(参考) 5B085 AE02 AE03 AE25 AE26 AE27
5J104 AA07 KA01 KA04 KA16 NA02 NA05 NA38 PA07